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: FeyziyevFG@mail.ru),
М.Р. Мехтиева, канд. физ.-мат. наук
Бакинский госуниверситет
(Азербайджан, AZ1148, Баку, ул. Академика Захида Халилова, 23,
тел.(+994012) 5390535),
З.А. Самедова, д-р философии по математике
Азербайджанский университет языков
(Азербайджан, AZ1014, Баку, ул. Рашида Бехбудова, 134,
тел.(+994012) 4412278, e-mail: zamina68@hotmail.com)

Модификация метода Питерсона—Горенстейна—Цирлера приведением матрицы к треугольному виду (двоичный случай)

Сформулирована теорема о числе ошибок в принятых сообщениях при передаче по каналам связи двоичных кодов Боуза—Чоудхури—Хоквингема (БЧХ). Для обнаружения и исправления произошедших ошибок в двоичных кодах БЧХ предложена модификация метода Питерсона—Горенстейна—Цирлера, основанная на приведении матрицы к треугольному виду. Разработана методика ускорения вычисления согласно этой модификации. Приведен алгоритм декодирования принятых сообщений на основе предложенной модификации.

Сформульовано теорему про число похибок в прийнятих повідомленнях при передачі по каналах зв'язку двоічних кодів Боуза—Чоудхурі—Хоквінгема (БЧХ). Для виявлення та виправлення похибок, що сталися, в двоїчних кодах БЧХ запропоновано модифікацію методу Пітерсона—Горенстейна—Цирлера, базовану на приведенні матриці до трикутної форми. Розроблено методику прискорення обчислень згідно з цією модифікацією. Наведено алгоритм декодування прийнятих повідомлень на базі запропонованої модифікації.

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

Коды Боуза—Чоудхури—Хоквингема (БЧХ) являются эффективными помехоустойчивыми кодами [1—4]. 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]. Этот метод основан на решении специальной системы линейных алгебраических уравнений (СЛАУ) относительно неизвестных локаторов ошибок с применением обращения матрицы.

В работе [5] 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. Затем 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 предлагаемой новой модификации метода ПГЦ нахождение числа ошибок осуществляется без их последовательного выбора и проверки.

Постановка задачи. Пусть m — заданное натуральные число, α — примитивный элемент поля $GF(2^m)$ [4], т.е. элемент порядка $n = 2^m - 1$, $P(x)$ — примитивный многочлен над полем $GF(2)$ степени m, с помощью которого построено поле $GF(2^m)$. В поле $GF(2^m)$ 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 $GF(2)$. 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 $i(x) = i_{k-1}x^{k-1} + ... + i_1 x + i_0$. Заметим, что для чисел n, k и ℓ должно быть удовлетворено соотношение $2\ell \le n - k$ [4].

Пусть по каналу связи передан многочлен $c(x)$, на другом конце 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 равны единице. Предположим, что в данный момент произошло v ошибок, где $0 \le v \le \ell$, и что этим ошибкам соответствуют неизвестные позиции $p_1, p_2, ..., p_v$. В этом случае $e(x) = x^{p_1} + ... + x^{p_v}$, где показатели степеней $p_1, p_2, ..., p_v$ и число v произошедших ошибок неизвестны. Для обнаружения и исправления ошибок необходимо найти эти неизвестные. Для их нахождения используются компоненты синдрома $S_1, ..., S_{2\ell}$, где [1]

$$S_\beta = \upsilon(\alpha^\beta) = c(\alpha^\beta) + e(\alpha^\beta) = e(\alpha^\beta) = (\alpha^\beta)^{p_1} + (\alpha^\beta)^{p_2} + ... + (\alpha^\beta)^{p_v}. \quad (1)$$

Вычисления S_β по формуле (1) проводятся над полем $GF(2^m)$. Это означает, что после выполнения операций, указанных в правой части равенства, полученный результат делится на многочлен $P(\alpha)$ и берется остаточный многочлен. Из формулы (1) видно, что если $S_\beta = 0, \beta = \overline{1, 2\ell}$, то в принятом сообщении ошибок нет, в противном случае — ошибки (искажения) есть.

Пусть $X_j = \alpha^{p_j}$ (локаторы ошибок), $j = 1, ..., v$. Поскольку порядок элемента α равен n, все локаторы рассматриваемой конфигурации ошибок различны. Для каждого $\beta = 1, ..., 2\ell$ из формулы (1) получаем следующую систему из 2ℓ уравнений относительно неизвестных локаторов ошибок $X_1, ..., X_v$:

$$S_\beta = X_1^\beta + X_2^\beta + ... + X_v^\beta, \ \beta = \overline{1, 2\ell}. \tag{2}$$

Для решения систем нелинейных уравнений (2) используется многочлен локаторов ошибок $\Lambda(x) = \Lambda_v x^v + ... + \Lambda_1 x + 1$, корнями которого являются X_ℓ^{-1}, $\ell = 1, ..., v$ [1]. Если коэффициенты многочлена $\Lambda(x)$ известны, то для вычисления локаторов ошибок необходимо найти его корни. СЛАУ, связывающая компоненты синдрома с коэффициентами многочлена $\Lambda(x)$, имеет следующий матричный вид [1]:

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

Здесь $A = (a_{\rho,\beta})$, $\rho = \overline{1, v}$, $\beta = \overline{1, v}$, где $a_{\rho,\beta} = S_{\rho-1+\beta}$. Если матрица A — невырожденная, то эта система имеет единственное решение относительно $\Lambda_1, \Lambda_2, ..., \Lambda_v$.

Для обнаружения и исправления ошибок сначала находим число произошедших ошибок. Затем уточняем их координаты, т.е. находим номера компонентов принятого слова, которое имеет ошибки, и вносим в них коррективы. Определение числа произошедших ошибок требует достаточно много времени. Чем быстрее определяется число произошедших ошибок, тем эффективнее метод декодирования.

Известно, что если $M = (S_{\rho-1+\beta})$, $\rho = \overline{1, \mu}$, $\beta = \overline{1, \mu}$, и если $\mu = v$, то матрица M — невырожденная, а если $\mu > v$, то матрица M — вырождена [1]. В предлагаемой модификации метода ПГЦ, на основе этого факта и вида матрицы A сформулирована теорема о числе произошедших ошибок в принятых сообщениях.

Модификация метода ПГЦ. Компоненты $S_1, ..., S_{2\ell}$ вычисляем по следующему алгоритму.

А л г о р и т м 1 [5].

Шаг 0. $S_\beta := R_{P(\alpha)}[\upsilon_{n-1}\alpha^\beta + \upsilon_{n-2}]$, $\gamma = 1$.

Шаг 1. $S_\beta := R_{P(\alpha)}[\upsilon_{n-1}\alpha^\beta + \upsilon_{n-2-\gamma}]$.

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

Шаг 3. Конец.

В этом алгоритме оператор $R_{P(\alpha)}[\varphi(\alpha)]$ используется для нахождения многочлена остатка от деления многочлена $\varphi(\alpha)$ на многочлен $P(\alpha)$.

Нетрудно доказать следующие теоремы.

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

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

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

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

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

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

$$\Lambda_1=(d_{vv})^{-1}\vartheta_v,$$

$$\Lambda_\rho=(d_{v-\rho+1,v-\rho+1})^{-1}\left\{\vartheta_{v-\rho+1}+\sum_{\sigma=1}^{\rho-1}d_{v-\rho+1,v-\rho+1+\sigma}\Lambda_{\rho-\sigma}\right\},\ \rho=2,3,\dots,v.$$

На основе теорем 1 и 2, используя методику приведения матрицы к треугольной форме, модификацию метода ПГЦ можно описать с помощью следующего алгоритма.

А л г о р и т м 2.

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 $S_1,\dots,S_{2\ell}$ равны нулю, то перейти к шагу 10, 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 $a_{\rho,\beta}=S_{\rho-1+\beta},\rho,\beta=\overline{1,\ell}$; $b_\rho=S_{\rho+v}$, $\rho=\overline{1,\ell}$. Принять $j=1$ и перейти к шагу 2.

Ш а г 2. Если $j+1\geq\ell$, то принять $v=1$ и перейти к шагу 7, иначе наименьший элемент множества $Q=\{\xi\mid\xi\in\{j,...,\ell\},a_{\xi j}\neq 0\}$ 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 $v=j+1$. Если $v\leq\ell$, то перейти к шагу 3, иначе — к шагу 5.

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

$$a_{v\beta}:=a_{v\beta}+(a_{vj}/a_{jj})\,a_{j\beta},\ \beta=j,...,\ell. \tag{4}$$

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

$$b_v:=b_v+(a_{vj}/a_{jj})b_j. \tag{5}$$

Ш а г 4. Принять $v:=v+1$. Если $v\leq\ell$, 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 вектор-столбец, то принять $v=j$ и перейти к шагу 7, иначе — к шагу 6.

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

Ш а г 7. Решить СЛАУ $\overline{A}\,\mathrm{col}(\Lambda_v,\Lambda_{v-1},...,\Lambda_1)=\overline{b}$ и определить коэффициенты $\Lambda_1,\Lambda_2,...,\Lambda_v$ многочлена $\Lambda(x)$ по формулам

$$\Lambda_1=(a_{vv})^{-1}b_v, \tag{6}$$

$$\Lambda_\rho=(a_{v-\rho+1,v-\rho+1})^{-1}\left\{b_{v-\rho+1}+\sum_{\sigma=1}^{\rho-1}a_{v-\rho+1,v-\rho+1+\sigma}\Lambda_{\rho-\sigma}\right\},\ \ \rho=2,3,...,v, \tag{7}$$

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 многочлена локаторов ошибок по формуле $X_\beta=x_\beta^{-1}$, $\beta=\overline{1,v}$.

Ш а г 9. Найти значения индексов $p_1,...,p_v$ и исправить ошибки по формуле $\upsilon_{p_\beta}:=\upsilon_{p_\beta}+1$, $\beta=1,...,v$, $GF(2)$.

Ш а г 10. Определить информационный многочлен по формуле $i(x)=$ $=\upsilon(x)/g(x)$.

Ш а г 11. Конец.

Методика ускорения вычисления в модификации метода ПГЦ. Элементы матрицы A в (3) есть элементы поля $GF(2^m)$, т.е. они являются многочленами над полем $GF(2)$. Ненулевые элементы поля $GF(2^m)$ являются степенью примитивного элемента. Для выполнения операций сложения и умножения элементов поля $GF(2^m)$ можно использовать соответствующие таблицы, что позволит сократить время выполнения этих операций.

Компоненты $S_1, ..., S_{2\ell}$ принимают значения из конечного поля $GF(2^m)$. Поэтому они являются 0 (нулевым элементом) или степенью примитивного элемента α. Введем числа $N_1, ..., N_{2\ell}$:

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

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

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

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

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

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

$$x * y = \begin{cases} -1, \text{ если } x = -1 \text{ или (и) } y = -1, \\ x + y - (2^m - 1), \text{ если } x \neq -1, y \neq -1, x + y \geq 2^m - 1, \\ x + y, \text{ если } x \neq -1, y \neq -1, x + y < 2^m - 1. \end{cases}$$

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

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

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

В формулах (4)—(7) 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

$$z_{\rho\beta}=\begin{cases}-1, \text{ если } a_{\rho\beta}=0,\\ \sigma, \text{ если } a_{\rho\beta}=\alpha^{\sigma}, \text{где } \sigma\in\{0, ..., 2^m-2\},\end{cases} \tag{8}$$

$$\eta_{\rho}=\begin{cases}-1, \text{ если } b_{\rho}=0,\\ \sigma, \text{ если } b_{\rho}=\alpha^{\sigma}, \text{ где } \sigma\in\{0, ..., 2^m-2\}.\end{cases} \tag{9}$$

Используя примитивный элемент α, можно записать формулы (4) и (5) с учетом (8) и (9) в виде

$$\alpha^{z_{v\beta}}:=\alpha^{z_{v\beta}}+(\alpha^{z_{vj}}/\alpha^{z_{jj}})\alpha^{z_{j\beta}}, \tag{10}$$

$$\alpha^{\eta_v}:=\alpha^{\eta_v}+(\alpha^{z_{vj}}/\alpha^{z_{jj}})\alpha^{\eta_j}. \tag{11}$$

Отсюда

$$z_{v\beta}:=MC\,(z_{v\beta}, (2^m-1-z_{jj})*z_{vj}*z_{j\beta}), \tag{12}$$

$$\eta_v:=MC\,(\eta_v, (2^m-1-z_{jj})*z_{vj}*\eta_j), \tag{13}$$

где $MC\,(x, y)$ — значение показателя суммы $\alpha^x+\alpha^y$,

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

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

$$\lambda_{\rho}=\begin{cases}-1, \text{ если } \Lambda_{\rho}=0,\\ \sigma, \text{ если } \Lambda_{\rho}=\alpha^{\sigma}, \text{ где } \sigma\in\{0, ..., 2^m-2\}.\end{cases} \tag{14}$$

На основе (8)—(14) можно записать формулы (6) и (7) соответственно в виде

$$\lambda_1=(2^m-1-z_{vv}^{(v-1)})*\eta_v^{(v-1)}, \tag{15}$$

$$\lambda_{\rho}=(2^m-1-z_{v-\rho+1,\,v-\rho+1}^{(v-1)})*MC\,(\eta_{v-\rho+1}^{(v-\rho)}, \gamma_{\rho}),\ \rho=2,3, ..., v. \tag{16}$$

Множитель $2^m - 1 - z_{\nu\nu}^{(\nu-1)}$ в правой части (15) указывает на то, что если $a_{\nu\nu}^{(\nu-1)} = \alpha^{z_{\nu\nu}^{(\nu-1)}}$, то $(a_{\nu\nu}^{(\nu-1)})^{-1} = \alpha^{2^m - 1 - z_{\nu\nu}^{(\nu-1)}}$, а в правой части формулы (16) γ_ρ определяется рекуррентно:

$$\gamma_\rho := -1;\ \gamma_\rho := MC\,(\gamma_\rho,\, z_{\nu-\rho+1,\,\nu-\rho+1+\sigma}^{(\nu-\rho)} * \lambda_{\rho-\sigma}),\ \ \sigma = 1, \ldots, \rho - 1.$$

Для определения корней многочлена $\Lambda\,(x)$ после определения коэффициентов $\Lambda_1, \Lambda_2, \ldots, \Lambda_\nu$ для каждого элемента $x \in GF\,(2^m)$ надо вычислить $\Lambda\,(x)$ и выделить те значения x, при которых $\Lambda\,(x)$ равно нулю. На основе схемы Горнера $\Lambda\,(x)$ вычисляется рекуррентно в такой последовательности:

$$\Lambda_0 := -1,\ \ \Lambda(x) := \Lambda_\nu x + \Lambda_{\nu-1},\ \ \Lambda(x) := \Lambda(x)\,x + \Lambda_\xi,\ \ \xi = \nu - 2, \nu - 3, \ldots, 0. \quad (17)$$

Для ускорения вычисления вместо x можно использовать его описание в виде $x = \alpha^\beta$. Тогда схему (17) запишем в виде

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

Здесь

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

По определению для каждого $\ell = 1, \ldots, \nu$

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

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 3.

Ш а г 0. Выбрать $\upsilon_{n-1}, \upsilon_{n-2}, \ldots, \upsilon_1, \upsilon_0$. 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 $N_1, N_2, \ldots, N_{2\ell}$ равны – 1, то перейти к шагу 35, 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 $\eta = (\eta_1, \eta_2, \ldots, \eta_\ell)$, где $\eta_\rho = N_{\rho+\ell}$, $\rho = \overline{1, \ell}$.

Принять $j=1$. Если $j+1>\ell$, то принять $v=1$ и перейти к шагу 19, иначе перейти к шагу 7.

Ш а г 7. 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 $\beta\le\ell$, 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 $v\le\ell$, то перейти к шагу 11, иначе — к шагу 15.

Ш а г 11. Принять $\beta=j$.

Ш а г 12. Принять $z_{v\beta}:=MC\,(z_{v\beta},(2^m-1-z_{jj})*z_{vj}*z_{j\beta})$.

Ш а г 13. Принять $\beta:=\beta+1$. Если $\beta\le\ell$, то перейти к шагу 12, иначе принять $\eta_v:=MC\,(\eta_v,(2^m-1-z_{jj})*z_{vj}*\eta_j)$ и перейти к шагу 14.

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

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

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 $\rho\le\ell$, то перейти к шагу 16, иначе принять $v=j$ и перейти к шагу 19.

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

Ш а г 19. $\lambda_1=(2^m-1-z_{vv})*\eta_v$. 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 $\sigma\le\rho-1$, то перейти к шагу 22, иначе — к шагу 24.

Ш а г 24. $\lambda_\rho:=(2^m-1-z_{v-\rho+1,\,v-\rho+1})*MC\,(\eta_{v-\rho+1},\gamma)$.

Ш а г 25. $\rho:=\rho+1$. Если $\rho\le v$, 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 $\xi\ge0$, 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 $\sigma\ge v$, то перейти к шагу 33, иначе — к шагу 32.

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

Шаг 33. Для каждого $\xi = 1, ..., \nu$ определить p_ξ по формуле $p_\xi = 2^m - 1 - x_\xi$.

Ш а г 34. Принимать: $\upsilon_{p_\xi} := \upsilon_{p_\xi} + 1, GF(2), \xi = 1, ..., \nu$.

Ш а г 35. Делить многочлен $\upsilon(x)$ на многочлен $g(x) = g_{n-k} x^{n-k} + ...$ $... + g_1 x + g_0$ по схеме [6]:

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

$y_{n-\beta-\alpha}[\beta] = y_{n-\beta-\alpha}[\beta-1] + y_{n-\beta}[\beta-1] g_{n-k-\alpha}, \ \alpha = 1, ..., n-1, GF(2),$

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

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

$y_{n-k-\alpha}[k] = y_{n-k-\alpha}[k-1] + y_{n-k}[k-1] g_{n-k-\alpha}, \ \alpha = 1, ..., n-k, GF(2),$

$I_0[k] = y_{n-k}[k-1].$

Ш а г 36. Определить компоненты информационного вектора по формуле $i_{k-\beta} = I_{k-\beta}[\beta], \ \beta = 1, 2, ..., k$.

Ш а г 37. 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 двоичных 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. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. — М. : Кудиц-образ, 2001. — 368 с.
3. *William C.H., Vera P.* Fundamentals of Error-Correcting Codes. — Cambridge University Press, 2003. — 662 p.
4. *Биркгоф Г., Барти Т.* Современная прикладная алгебра. — М. : Мир, 1976. — 400 с.
5. *Фейзиев Ф.Г.* Модификация алгоритма Питерсона—Горенстейна—Цирлера и ее эффективная реализация// Электрон. моделирование. — 2015. — **37**, № 3. — С. 3—16.
6. *Фейзиев Ф.Г., Мегрдад Бабаванд.* Описание декодирования циклических кодов в классе последовательностных машин, основанного на теореме Меггитта// Автоматика и вычислительная техника. — 2012. — № 4. — С. 26—33.

F.G. Feyziyev, M.R. Mekhtiyeva, Z.A. Samedova

MODIFICATION OF PETERSON-GORENSTEIN-ZIERLER METHOD,
BRINGING THE MATRIX TO TRIANGULAR FORM (BINARY CASE)

The theorem on the number of errors, which occurred in the received messages in the case of transmission of the binary Bose-Chaudhuri-Hocquenghem codes over communication channels, has been formulated. A modification of the Peterson-Gorenstein-Zierler method, based on the reduction of the matrix to triangular form, for detecting and correcting errors in the binary Bose-Chaudhuri-Hocquenghem codes has been proposed. The technique has been developed for accelerating calculation in accordance with this modification. A detailed description of the algorithm of decoding the received messages based on the above modifications and techniques is given.

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

REFERENCES

1. Bleykhut, R. (1986), *Teoriya i praktika kodov, kontroliruyushchikh oshibki* [Theory and practice of error control codes], Translated by Grushina, I.I., and Blinov, B.M., Mir, Moscow, Russia.
2. Ivanov, M.A. (2001), *Kriptograficheskiye metody zashchity informatsii v kompyuternykh sistemakh i setyakh* [Cryptographic methods of information protection in computer systems and networks], Kudits-obraz, Moscow, Russia.
3. William, C.H., Vera, P. (2003), Fundamentals of error-correcting codes, Cambridge University Press, Cambridge, UK.
4. Birkgof, G. and Barti, T. (1976), *Sovremennaya prikladnaya algebra* [Modern applied algebra], Translated by Manina, Yu.I., Mir, Moscow, Russia.
5. Feyziyev, F.G. (2015), “On one modification of the Peterson-Gorenstein-Zierler algorithm and its effective realization”, *Elektronnoe modelirovanie*, Vol. 37, no. 3, pp. 3-16.
6. Feyziyev, F.G., and Babavand, A.M. (2012), “Description of decoding of cyclic codes in the class of sequential machines based on the Meggitt theorem”, *Avtomatika i vychislitelnaya tekhika*, no. 4, pp. 26-33.

Поступила 10.05.16

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.

САМЕДОВА Замина Агаш кызы, д-р философии по математике, доцент кафедры информационных технологий Азербайджанского университета языков. В 1994 г. окончила Азербайджанскую государственную нефтяную академию. Область научных исследований — теория конечных автоматов и теоретические вопросы информатики.