УДК 519.95

Ф.Г. Фейзиев, д-р физ.-мат. наук,
Сумгаитский госуниверситет
(Азербайджан, AZ-5008, Сумгаит, 43 квартал,
тел. (+99418) 6483887, e-mail: FeyziyevFG@mail.ru)

Модификация алгоритма Питерсона—Горенстейна—Цирлера и ее эффективная реализация

Предложена модификация алгоритма Питерсона—Горенстейна—Цирлера на основе метода Гаусса и описан эффективный способ реализации модифицированного алгоритма ускоренного обнаружения и исправления ошибок в принятых двоичных сообщениях. Применены таблицы операций над элементами конечного поля, в которых вместо элемента предложено использовать показатель степени представления выбранного примитивного элемента поля. Приведен алгоритм декодирования принятых двоичных сообщений.

Запропоновано модифікацію алгоритма Пітерсона—Горенстейна—Цирлера на основі методу Гауса та описано ефективний спосіб реалізації модифікованого алгоритма прискореного виявлення і виправлення похибок в отриманих двоїчних повідомленнях. Застосовано таблиці операцій над елементами кінцевого поля, в яких замість елемента запропоновано використовувати показник ступеня представлення обраного примітивного елемента поля. Наведено алгоритм декодування отриманих двоїчних повідомлень.

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

В настоящее время для защиты данных в компьютерных системах и сетях широко применяются методы теории кодирования, криптографии и др. [1—3]. Эффективными помехоустойчивыми кодами являются коды Боуза—Чоудхури—Хоквингема (БЧХ) [1, 3, 4], для декодирования которых, т.е. обнаружения и исправления ошибки в принятых сообщениях, и выделения из них информационных сообщений используются различные методы и алгоритмы, например алгоритм Питерсона—Горенстейна—Цирлера (ПГЦ). Этот алгоритм основан на решении специальной системы линейных алгебраических уравнений (СЛАУ) относительно неизвестных локаторов ошибок методом обращения матрицы.

В предлагаемой модификации алгоритма ПГЦ вместо метода обращения матрицы применен метод Гаусса. Поскольку элементы матрицы

системы суть элементы конечного поля [4], т.е. многочлены, каждый из которых является степенью примитивного элемента конечного поля, выполнение операций над ними можно ускорить посредством выполнения операций над показателями соответствующих степеней примитивного элемента [1].

Постановка задачи. Пусть α — примитивный элемент поля $GF(2^m)$ [4], т.е. элемент порядка $n=2^m-1$, где m — заданное натуральное число. Для натурального числа t код БЧХ, исправляющий t ошибок, является циклическим кодом длины n с порождающим многочленом $g(x)$, равным наименьшему общему кратному $[f_1(x), f_2(x), ..., f_{2t}(x)]$, где $f_\beta(x)$ — минимальный многочлен элемента $\alpha^\beta \in GF(2^m)$, $\beta=\overline{1,2t}$. Пусть $k=n-\deg g(x)$ и $i=(i_0, i_1, ..., i_{k-1})$ есть k-мерный произвольный информационный вектор над полем $GF(2)$. Тогда информационный вектор i может быть закодирован посредством операции $c(x)=i(x)g(x)$ в кодовый многочлен $c(x)=c_{n-1}x^{n-1}+...+c_1x+c_0$, где $i(x)=i_{k-1}x^{k-1}+...+i_1x+i_0$. Заметим, что для чисел n, k и t должно быть удовлетворено соотношение $2t \le n-k$ [4].

Пусть по каналу связи передан многочлен $c(x)$, а на другом конце принят многочлен $\upsilon(x)=\upsilon_{n-1}x^{n-1}+...+\upsilon_1x+\upsilon_0$. Пусть $e(x)=e_{n-1}x^{n-1}+...$ $...+e_1x+e_0$ есть многочлен ошибок, т.е. $e(x)=\upsilon(x)+c(x)$, $GF(2)$, и не более t коэффициентов равны единице (здесь $GF(2)$ указывает, что многочлены $\upsilon(x)$ и $c(x)$ слагаются над полем $GF(2)$). Предположим, что в данный момент произошло ν ошибок, где $0 \le \nu \le t$, и что этим ошибкам соответствуют неизвестные позиции $p_1, p_2, ..., p_\nu$. В этом случае многочлен ошибок $e(x)$ можно записать в виде $e(x)=x^{p_1}+...+x^{p_v}$, где показатели степеней $p_1, p_2, ..., p_\nu$ и число v неизвестны. Для обнаружения и исправления ошибок необходимо найти эти неизвестные.

Для нахождения значений v и $p_1, p_2, ..., p_\nu$ в [1] предлагается использовать компоненты синдрома S_β, $\beta=\overline{1,2t}$, где $S_\beta=\upsilon(\alpha^\beta)$. Поскольку $c(x)=i(x)g(x)$ и α^β, $\beta=\overline{1,2t}$, есть корни порождающего многочлена $g(x)$, то $c(\alpha^\beta)=0$, $\beta=\overline{1,2t}$. С учетом этого факта получим следующую формулу для определения S_β, $\beta=\overline{1,2t}$:

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

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

Примитивный многочлен над полем $GF(2)$ степени m, с помощью которого построено поле $GF(2^m)$, обозначим через $P(x)$. Заметим, что в поле $GF(2^m)$ примитивному элементу α соответствует многочлен x [1].

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

Пусть $X_\ell = a^{p_\ell}$ (локаторы ошибок), $\ell = 1, ..., \nu$. Поскольку порядок элемента α равен n, все локаторы рассматриваемой конфигурации ошибок различны. Для каждого $\beta \in \{1, ..., 2t\}$ из формулы (1) находим $S_\beta = \upsilon(\alpha^\beta) = X_1^\beta + X_2^\beta + ... + X_\nu^\beta$. Таким образом, получаем следующую систему $2t$ уравнений относительно неизвестных локаторов ошибок $X_1, ..., X_\nu$:

$$S_\beta = X_1^\beta + X_2^\beta + ... + X_\nu^\beta, \ \beta = \overline{1,2t}. \qquad (2)$$

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

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

Здесь $A = (a_{\rho,\beta})$, $\rho = \overline{1,\nu}$, $\beta = \overline{1,\nu}$, где $a_{\rho,\beta} = S_{\rho-1+\beta}$. Известно, что если матрица A невырожденная, то эта система имеет единственное решение относительно $\Lambda_1, \Lambda_2, ..., \Lambda_\nu$. Доказано также [1], что:

1) если произошло ν ошибок, то матрица A — невырожденная;

2) если $M = (S_{\rho-1+\beta})$, $\rho = \overline{1,\mu}$, $\beta = \overline{1,\mu}$, и если μ равно числу ν произошедших ошибок, то матрица M — невырожденная, а если μ больше ν, то матрица M — вырождена.

На основе этих фактов в [1] построен алгоритм декодирования, с помощью которого СЛАУ (3) решается обращением матрицы A.

Опишем модификацию алгоритма ПГЦ на основе метода Гаусса.

А л г о р и т м 1.

Ш а г 0. На основе принятого многочлена $\upsilon(x)$ вычислить $S_\beta = \upsilon(\alpha^\beta)$, $\beta = \overline{1,2t}$, по формуле (1).

Ш а г 1. $\nu = t$.

Ш а г 2. Построить матрицу $A = (a_{\rho,\beta})$, $\rho = \overline{1,\nu}$, $\beta = \overline{1,\nu}$, где $a_{\rho,\beta} = S_{\rho-1+\beta}$. Если в матрице A существуют нулевые строки и столбцы, то перейти к шагу 4, иначе — привести следующую систему алгебраических уравнений к треугольному виду:

$$A\,\mathrm{col}(\Lambda_\nu, \Lambda_{\nu-1}, ..., \Lambda_1) = \mathrm{col}(S_{\nu+1}, S_{\nu+2}, ..., S_{2\nu}). \qquad (4)$$

Ш а г 3. Если в процессе приведения матрицы A к треугольному виду стало известно, что A — вырожденная матрица, то перейти к шагу 4, в противном случае — к шагу 5.

Ш а г 4. $\nu := \nu - 1$. Перейти к шагу 2.

Ш а г 5. Решить систему алгебраических уравнений $A_1 \mathrm{col}(\Lambda_\nu, \Lambda_{\nu-1}, ..., \Lambda_1) = b$ и определить коэффициенты $\Lambda_1, \Lambda_2, ..., \Lambda_\nu$ многочлена $\Lambda(x)$, где вектор-столбец b получается из вектора-столбца $\mathrm{col}(S_{\nu+1}, S_{\nu+2}, ..., S_{2\nu})$ в результате приведения системы (4) к треугольному виду; A_1 — треугольный вид матрицы A.

Ш а г 6. Найти корни $x_1, ..., x_\nu$ многочлена локаторов ошибок $\Lambda(x)$ и локаторы ошибок по формуле $X_\beta = x_\beta^{-1}$, $\beta = 1, ..., \nu$.

Ш а г 7. Найти значения индексов $p_1, ..., p_\nu$ и исправить ошибки по формуле $\upsilon_{p_\ell} := \upsilon_{p_\ell} + 1$, $\ell = 1, ..., \nu$, $GF(2)$.

Ш а г 8. Определить информационный многочлен по формуле $i(x) = \upsilon(x)/g(x)$.

Ш а г 9. Конец.

Элементы матрицы A в (4) являются элементами поля $GF(2^m)$, т.е. многочленами над полем $GF(2)$. Каждый ненулевой элемент поля $GF(2^m)$ является степенью примитивного элемента. Для выполнения операций сложения и умножения элементов поля $GF(2^m)$ можно использовать соответствующие заготовленные таблицы, что позволит сократить время выполнения этих операций.

Эффективная реализация процесса обнаружения и исправления ошибок. Рассмотрим реализацию отдельных шагов описанного алгоритма. По определению справедливо: $S_\beta = \upsilon_0 + \upsilon_1 \alpha^\beta + \upsilon_2 \alpha^{2\beta} + ... + \upsilon_{n-2} \alpha^{(n-2)\beta} + \upsilon_{n-1} \alpha^{(n-1)\beta}$. Тогда по схеме Горнера получим $S_\beta = (...((\upsilon_{n-1} \alpha^\beta + \upsilon_{n-2}) \alpha^\beta + \upsilon_{n-3}) \alpha^\beta + ... + \upsilon_1) \alpha^\beta + \upsilon_0$. Поэтому для нахождения S_β, $\beta = 1, ..., 2t$, можно использовать следующий алгоритм:

А л г о р и т м 2.

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

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

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

Ш а г 3. Конец.

В этом алгоритме оператор $R_{P(\alpha)}[\varphi(\alpha)]$ используется для нахождения многочлена остатка от деления многочлена $\varphi(\alpha)$ на многочлен $P(\alpha)$. Компоненты S_β, $\beta = 1, ..., 2t$, принимают значения из конечного поля $GF(2^m)$. Поэтому каждый из них является либо нулевым элементом, либо степенью примитивного элемента α. Введем числа N_β, $\beta = 1, ..., 2t$:

$$N_\beta = \begin{cases} -1, \text{если } S_\beta = 0, \\ k, \text{ если } S_\beta = \alpha^k, k \in \{0, ..., 2^m - 2\}. \end{cases} \quad (5)$$

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

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

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

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

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

$$x * y = \begin{cases} -1, \text{если } x = -1 \text{ или } y = -1, \\ x + y - (2^m - 1), \text{если } x \neq -1, y \neq -1, x + y \geq 2^m - 1, \\ x + y, \text{если } x \neq -1, y \neq -1, x + y < 2^m - 1. \end{cases} \quad (6)$$

Построив предварительно массивы $M1$ и $M2$ согласно алгоритму 2, можно вычислить N_β, $\beta = \overline{1, 2t}$, с помощью следующего алгоритма:

А л г о р и т м 3.

Ш а г 0. $N_\beta := M1(\upsilon_{n-1}, \beta, \upsilon_{n-2})$, $\gamma = 1$.

Ш а г 1. $N_\beta := M2((N_\beta * \beta), \upsilon_{n-2-\gamma})$.

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

Ш а г 3. Конец.

Если числа N_β, $\beta = \overline{1, 2t}$, вычислены по алгоритму 3, то

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

Поэтому далее вместо S_β, $\beta = 1, ..., 2t$, можно использовать N_β, $\beta = 1, ..., 2t$.

Рассмотрим приведение СЛАУ (4) к треугольному виду. Для этого введем матрицу $A = (a_{\rho,\beta})$, $\rho = \overline{1, v}$, $\beta = \overline{1, v}$, и вектор $b = (b_1, ..., b_v)$: $a_{\rho,\beta} = S_{\rho-1+\beta}$,

$\rho = \overline{1, v}$, $\beta = \overline{1, v}$; $b_\rho = S_{\rho+v}$, $\rho = \overline{1, v}$. Наименьший элемент множества $Q = \{\xi \mid \xi \in \{1, ..., v\}, a_{\xi 1} \neq 0\}$ обозначим через σ. В случае $\sigma \neq 1$ поменяем местами первую и σ-ю строки матрицы A и первый и σ-й компоненты вектора b, т.е. примем $c = a_{1\beta}$, $a_{1\beta} = a_{\sigma\beta}$, $a_{\sigma\beta} = c$, $\beta = 1, ..., v$; $c = b_1$, $b_1 = b_\sigma$, $b_\sigma = c$.

Таким образом, в полученной новой матрице A $a_{11} \neq 0$. К строкам матрицы A 2, ..., v-й, умноженным на a_{11}, прибавляем первую строку, умноженную соответственно на $a_{21}, ..., a_{v1}$. Затем в векторе b к компонентам 2, ..., v-й, умноженным на a_{11}, прибавляем первые компоненты, умноженные соответственно на $a_{21}, ..., a_{v1}$. Тогда получим

$$A' = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1v} \\ 0 & a'_{22} & \cdots & a'_{2v} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & a'_{v2} & \cdots & a'_{vv} \end{pmatrix}, \quad b' = \mathrm{col}(b_1, b'_2, ..., b'_v),$$

где

$$a'_{\rho\beta} = a_{\rho\beta} a_{11} + a_{1\beta} a_{\rho 1}, \quad \beta = 2, ..., v, \quad \rho = 2, ..., v; \tag{7}$$

$$b'_\rho = b_\rho a_{11} + b_1 a_{\rho 1}, \quad \rho = 2, ..., v. \tag{8}$$

Если в подматрице $A'_1 = (a'_{\rho,\beta})$, $\rho = \overline{2, v}$, $\beta = \overline{2, v}$, существует нулевая строка или столбец, то матрица A' является вырожденной, и приведение ее к треугольному виду прекращаем. В противном случае наименьший элемент множества $Q_2 = \{\xi \mid \xi \in \{2, ..., v\}, a_{\xi 2} \neq 0\}$ обозначим через σ. В случае $\sigma \neq 2$ поменяем местами вторую и σ-ю строки матрицы A' и второй и σ-й компоненты вектора b'. В матрице A' к строкам 3, ..., v-й, умноженным на a'_{22}, прибавляем вторую строку, умноженную соответственно на $a'_{31}, ..., a'_{v1}$. Затем, в векторе b' к компонентам 3, ..., v-й, умноженным на a'_{22}, прибавляем вторую компоненту, умноженную соответственно на $a'_{31}, ..., a'_{v1}$ и так далее.

Продолжая описанную процедуру, либо выясняем, что матрица A — вырожденная, и поэтому прекращаем приведение ее к треугольному виду, либо на шаге $(v-1)$ получаем

$$A^{(v-1)} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1v} \\ 0 & a'_{22} & a'_{23} & \cdots & a'_{2v} \\ 0 & 0 & a''_{33} & \cdots & a''_{3v} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & a_{vv}^{(v-1)} \end{pmatrix}, \quad b^{(v-1)} = \begin{pmatrix} b_1 \\ b'_2 \\ b''_3 \\ \vdots \\ b_v^{(v-1)} \end{pmatrix},$$

где

$$a_{\rho\beta}^{(\ell)} = a_{\rho\beta}^{(\ell-1)} a_{\ell\ell}^{(\ell-1)} + a_{\ell\beta}^{(\ell-1)} a_{\rho\ell}^{(\ell-1)},\ \beta = \ell+1,...,v,\ \rho = \ell+1,...,v;$$
$$b_{\rho}^{(\ell)} = b_{\rho}^{(\ell-1)} a_{\ell\ell}^{(\ell-1)} + b_{\ell}^{(\ell-1)} a_{\rho\ell}^{(\ell-1)},\ \ \rho = \ell+1,...,v;\ \ \ell = 2,...,v-1. \tag{9}$$

В матрице $A^{(v-1)}$ суть $a_{11} \neq 0$, $a'_{22} \neq 0$, ..., $a_{v-1,v-1}^{(v-2)} \neq 0$. Если $a_{v,v}^{(v-1)} = 0$, то матрица $A^{(v-1)}$ — вырожденная и СЛАУ не имеет решения при данном значении v. В случае $a_{v,v}^{(v-1)} \neq 0$ решение задачи (4) сводится к решению задачи с треугольной матрицей:

$$A^{(v-1)} \mathrm{col}(\Lambda_v, \Lambda_{v-1}, ..., \Lambda_1) = b^{(v-1)}. \tag{10}$$

Из последнего уравнения системы (10) определяем Λ_1 по формуле

$$\Lambda_1 = (a_{v,v}^{(v-1)})^{-1} b_v^{(v-1)}. \tag{11}$$

Учитывая (11) в предпоследнем уравнении системы (10) и решая это уравнение, определяем неизвестный коэффициент Λ_2 и так далее. Если $\Lambda_1, \Lambda_2, ..., \Lambda_{\rho-1}$ найдены, то неизвестный коэффициент Λ_ρ можно определить из $[v-(\rho-1)]$-го уравнения системы (10):

$$a_{v-\rho+1,v-\rho+1}^{(v-\rho)} \Lambda_\rho + a_{v-\rho+1,v-\rho+2}^{(v-\rho)} \Lambda_{\rho-1} + ... + a_{v-\rho+1,v}^{(v-\rho)} \Lambda_1 = b_{v+\rho+1}^{(v-\rho)}, \tag{12}$$

где коэффициенты неизвестных $\Lambda_v, ..., \Lambda_{\rho+1}$ — нулевые, поэтому эти неизвестные здесь отсутствуют. Из (12) находим

$$\Lambda_\rho = (a_{v-\rho+1,v-\rho+1}^{(v-\rho)})^{-1} \left\{ b_{v-\rho+1}^{(v-\rho)} + \sum_{\sigma=1}^{\rho-1} a_{v-\rho+1,v-\rho+1+\sigma}^{(v-\rho)} \Lambda_{\rho-\sigma} \right\},\quad \rho = 2,3,...,v. \tag{13}$$

Формулы (11), (13) являются рекуррентными соотношениями для решения задачи (10). В формулах (7)—(13) 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 введем матрицу $Z = (z_{\rho\beta})$, $\rho = \overline{1,v}$, $\beta = \overline{1,v}$, а на основе вектора b — v-мерный вектор $\eta = \mathrm{col}(\eta_1, ..., \eta_v)$, где

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

$$\eta_\rho = \begin{cases} -1, \text{ если } b_\rho = 0, \\ \sigma, \ \text{ если } b_\rho = \alpha^\sigma, \sigma \in \{0,...,2^m-2\}. \end{cases} \tag{15}$$

Используя (5) можно определить $z_{\rho,\beta}$, $\rho=\overline{1,v}$, $\beta=\overline{1,v}$, и η_ρ, $\rho=\overline{1,v}$, с помощью формул $z_{\rho,\beta}=N_{\rho-1+\beta}$ и $\eta_\rho=N_{\rho+v}$. На основе матрицы $Z^{(v-1)}$ и вектора $\eta^{(v-1)}$ введем следующие матрицы и векторы:

$$Z^{(v-1)}=\begin{pmatrix} z_{11} & z_{12} & z_{13} & \cdots & z_{1v} \\ -1 & z'_{22} & z'_{23} & \cdots & z'_{2v} \\ -1 & -1 & z''_{33} & \cdots & z''_{3v} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ -1 & -1 & -1 & \cdots & z_{vv}^{(v-1)} \end{pmatrix}, \quad \eta^{(v-1)}=\begin{pmatrix} \eta_1 \\ \eta'_2 \\ \eta''_3 \\ \vdots \\ \eta_v^{(v-1)} \end{pmatrix},$$

где

$$z_{\rho,\beta}^{(\ell)}=\begin{cases} -1, \text{ если } a_{\rho,\beta}^{(\ell)}=0, \\ \sigma, \text{ если } a_{\rho,\beta}^{(\ell)}=\alpha^\sigma, \sigma\in\{0,...,2^m-2\}, \end{cases} \quad \beta=\ell+1,...,v,\ \rho=\ell+1,...,v, \quad (16)$$

$$\eta_\rho^{(\ell)}=\begin{cases} -1, \text{ если } b_\rho^{(\ell)}=0, \\ \sigma, \text{ если } b_\rho^{(\ell)}=\alpha^\sigma, \sigma\in\{0,...,2^m-2\}, \end{cases} \quad \rho=\ell+1,...,v, \quad (17)$$

$$\ell=1,...,v-1.$$

Используя примитивный элемент α, формулы (7), (8) с учетом (14) и (15) можно записать в виде $\alpha^{z'_{\rho\beta}}=\alpha^{z_{\rho\beta}}\alpha^{z_{11}}+\alpha^{z_{1\beta}}\alpha^{z_{\rho 1}}$, $\alpha^{\eta'_\rho}=\alpha^{\eta_\rho}\alpha^{z_{11}}+\alpha^{\eta_1}\alpha^{z_{\rho 1}}$, откуда вытекает

$$z'_{\rho,\beta}=MC\,(z_{\rho,\beta}*z_{11}, z_{1\beta}*z_{\rho 1}),\ \beta=\overline{2,v},\ \rho=\overline{2,v}, \quad (18)$$

$$\eta'_\rho=MC\,(\eta_\rho*z_{11}, \eta_1*z_{\rho 1}),\ \rho=\overline{2,v}, \quad (19)$$

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

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

Аналогично по формулам (18), (19) на основе (9) и (16), (17) получаем

$$z_{\rho\beta}^{(\ell)}=MC\,(z_{\rho\beta}^{(\ell-1)}*z_{\ell\ell}^{(\ell-1)}, z_{\ell\beta}^{(\ell-1)}*z_{\rho\ell}^{(\ell-1)}),\ \beta=\ell+1,...,v,$$

$$\eta_\rho^{(\ell)}=MC\,(\eta_\rho^{(\ell-1)}*z_{\ell\ell}^{(\ell-1)}, \eta_\ell^{(\ell-1)}*z_{\rho\ell}^{(\ell-1)}),\ \rho=\ell+1,...,v,\ \ell=1,...,v-1.$$

Составив предварительно массив $MC\,(x,y)$ для всех $x,y\in GF\,(2^m)$, с помощью (11), (13) ((18), (19)) можно вычислить $z'_{\rho,\beta}$ и η'_ρ ($z_{\rho,\beta}^{(\ell)}$ и $\eta_\rho^{(\ell)}$) быстрее чем $a'_{\rho,\beta}$ и b'_ρ ($a_{\rho,\beta}^{(\ell)}$ и $b_\rho^{(\ell)}$).

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

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

Из (11) получим $\lambda_1 = (2^m - 1 - z_{vv}^{(v-1)}) * \eta_v^{(v-1)}$, где множитель $2^m - 1 - z_{vv}^{(v-1)}$ свидетельствует о том, что если $a_{vv}^{(v-1)} = \alpha^{z_{vv}^{(v-1)}}$, то $(a_{vv}^{(v-1)})^{-1} = \alpha^{2^m - 1 - z_{vv}^{(v-1)}}$. Действительно, $\alpha^{z_{vv}^{(v-1)}} \alpha^{q^m - 1 - z_{vv}^{(v-1)}} = \alpha^{2^m - 1} = 1$. В правой части (13) выражение

$$J_\rho = \sum_{\sigma=1}^{\rho-1} a_{v-\rho+1, v-\rho+1-\sigma}^{(v-1)} \Lambda_{\rho-\sigma}$$

можно вычислить рекуррентно: $J_\rho := 0$; $J_\rho := J_\rho + a_{v-\rho+1, v-\rho+1-\sigma}^{(v-\rho)} \Lambda_{\rho-\sigma}$, $\sigma = 1, ..., \rho - 1$. Поэтому если $J_\rho = \alpha^{\gamma_\rho}$, то показатель γ_ρ также может быть определен рекуррентно:

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

Следовательно, согласно (13)

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

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

$$\Lambda_0 := 1, \ \Lambda(x) := \Lambda_v x + \Lambda_{v-1}, \ \Lambda(x) := \Lambda(x) x + \Lambda_\ell, \ \ell = v - 2, v - 1, ..., 0. \quad (20)$$

Для ускорения вычисления вместо x можно использовать его описание в виде $x = \alpha^\beta$. Тогда схему (20) запишем в виде

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

$$\ell = v - 2, \ v - 1, ..., 0,$$

где

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

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

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

Эффективность предложенных методик. Поскольку все вычисления связаны с элементами матрицы $A = (a_{\rho,\beta})$, $\rho = \overline{1, v}$, $\beta = \overline{1, v}$, и вектора $b = (b_1, ..., b_v)$, где $\alpha_{\rho,\beta} = S_{\rho-1+\beta}$ и $b_\rho = S_{\rho+v}$, согласно формуле (1) можно полагать, что все указанные элементы суть многочлены от примитивного элемента α, имеющие степень меньше m. Следовательно, они также являются элементами поля $GF(2^m)$.

Пусть $\varphi(\alpha), \psi(\alpha) \in GF(2^m)$ и $\varphi(\alpha) = \varphi_\ell \alpha^\ell + ... + \varphi_1 \alpha + \varphi_0$, $\psi(\alpha) = \psi_r \alpha^r + ... + \psi_1 \alpha + \psi_0$, где $\ell, r < m$. Пусть $h(\alpha) = h_{\ell+r} \alpha^{\ell+r} + ... + h_1 \alpha + h_0$ и ее коэффициенты определяются по формуле

$$h_\xi = \sum_{(\sigma, j) \in \Omega_\xi} \varphi_\sigma \psi_j, \quad GF(2),$$

где $\Omega_\xi = \{(\sigma, j) | \sigma + j = \xi\}$. Для вычисления всех коэффициентов $h(\alpha)$ необходимо выполнение операций умножения и сложения в количестве $2\sum_{\xi=0}^{\ell+r} |\Omega_\xi|$, где $|\Omega_\xi|$ — число элементов в множестве Ω_ξ.

По определению коэффициентов видно, что многочлен $h(\alpha)$ суть обычное произведение многочленов $\varphi(\alpha)$ и $\psi(\alpha)$, а степень $h(\alpha)$ может быть меньше $r + \ell$. Произведение $\varphi(\alpha)$ и $\psi(\alpha)$ над полем $GF(2^m)$ определяется по формуле $\varphi(\alpha)\psi(\alpha) = R_{P(\alpha)}[h(\alpha)]$.

Находим число операций для вычисления $R_{P(\alpha)}[h(\alpha)]$. Предположим, что $P(\alpha) = P_m \alpha^m + ... + P_1 \alpha + P_0$, где $P_m = 1$, и реальная степень многочлена $h(\alpha)$ есть N. Если $N < m$, то при делении на многочлен $P(\alpha)$ полученный остаточный многочлен есть $h(\alpha)$, следовательно, $\varphi(\alpha)\psi(\alpha) = h(\alpha)$. Если N не меньше m, то для деления $h(\alpha)$ на $P(\alpha)$ можно использовать следующие рекуррентные соотношения:

$$y_\alpha[0] = h_\alpha, \ \alpha = 0, 1, ..., N; \tag{21}$$

$$\begin{aligned} &y_{N+1-\beta-\alpha}[\beta] = y_{N+1-\beta-\alpha}[\beta-1] - y_{N+1-\beta}[\beta-1] P_{m-\alpha}, \alpha = 1, ..., m, \ GF(2), \\ &y_{N+1-\beta-\alpha}[\beta] = y_{N+1-\beta-\alpha}[\beta-1], \ \alpha = m+1, ..., N+1-\beta, \ \beta = 1, 2, ..., N-m; \end{aligned} \tag{22}$$

$$y_{m-\alpha}[N+1-m] = y_{m-\alpha}[N-m] - y_m[N-m] P_{m-\alpha}, \ \alpha = 1, ..., m, \ GF(2). \tag{23}$$

После завершения вычисления коэффициенты остаточного многочлена с убывающей последовательностью значений индексов являются значениями элементов соответственно $y_{m-1}[N+1-m], y_{m-2}[N+1-m], ..., y_0[N+1-m]$.

Согласно (21) требуется $KO_1 = N+1$ операций типа присваивание. В (22) первая и вторая формулы выполняются вместе циклически $N-m$ раз. В первой формуле есть две операции. Учитывая, что первая формула в отдельности выполняется циклически m раз, получаем $2m$ операций. Вторая формула выполняется циклически $N+1-\beta-m$ раз, и каждый раз выполняется одна операция присваивания, поэтому всего получаем $N+1-\beta-m$ операций. Таким образом, для (21) число выполняемых операций составляет

$$KO_2 = \sum_{\beta=1}^{N-m}(2m+N+1-\beta-m) = \sum_{\beta=1}^{N-m}(m+N+1-\beta) = \frac{N^2-3m^2+2Nm+N-m}{2}.$$

Согласно (23) вычисления проводятся циклически m раз, и каждый раз выполняются две операции. Следовательно, требуется $KO_3 = 2m$ операций. Таким образом, для деления $h(\alpha)$ на $P(\alpha)$ требуется KO_D операций:

$$KO_D = KO_2 + KO_2 + KO_2 = N+1+2m+\frac{N^2-3m^2+2Nm+N-m}{2}.$$

Число операций для вычисления $\varphi(\alpha)\psi(\alpha) = R_{P(\alpha)}[h(\alpha)]$ составит

$$KO = \begin{cases} 2\sum_{\xi=0}^{\ell+r}|\Omega_\xi|, & N \le m, \\ 2\sum_{\xi=0}^{\ell+r}|\Omega_\xi| + N+1+2m+\frac{N^2-3m^2+2Nm+N-m}{2}, & N > m, \end{cases}$$

откуда видно, что для вычисления произведения $\varphi(\alpha)$ и $\psi(\alpha)$ над полем $GF(2^m)$ требуется выполнение большего числа операций.

Теперь предположим, что $\varphi(\alpha) = \alpha^{\ell}$ и $\psi(\alpha) = \alpha^{r}$. Тогда для вычисления произведения $\varphi(x)$ и $\psi(x)$ над полем $GF(2^m)$ можно использовать операцию $\ell * r$, определенную формулой (6). Эта операция проводится на основе предварительно составленной соответствующей таблицы. Следовательно, используя значения ℓ и r, с помощью одного подходящего оператора языка программирования из таблицы можно выбрать показатель степени α, соответствующий $\varphi(\alpha)\psi(\alpha) = R_{P(\alpha)}[h(\alpha)]$. Таким образом, намного быстрее вычисляется $\varphi(\alpha)\psi(\alpha) = R_{P(\alpha)}[h(\alpha)]$. Следует заметить, что, кроме нулевого элемента, все многочлены над $GF(2^m)$ могут

быть представлены в виде α^{ξ}, где $0 \le \xi \le n$, а в вычислениях для нулевого элемента формально используется показатель степени -1.

Аналогично можно показать, что использование предварительно составленных таблиц, основанных на значении показателя степени примитивного элемента, может привести к многократному уменьшению времени выполнения сложения элементов над полем $GF(2^m)$.

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

А л г о р и т м 4.

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 $n - 2 - \gamma \ge 0$, то перейти к шагу 2, иначе — к шагу 4.

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

Ш а г 5. Если числа $N_1, N_2, ..., N_{2t}$ равны -1, то перейти к шагу 36, иначе — к шагу 6.

Ш а г 6. $v = t$.

Ш а г 7. Построить матрицу $D = (z_{\rho,\beta})$, $\rho = \overline{1, v}$, $\beta = \overline{1, v}$, где $z_{\rho,\beta} = N_{\rho-1+\beta}$, $\beta = \overline{1, v}$, $\rho = \overline{1, v}$. Построить вектор $\eta = (\eta_1, \eta_2, ..., \eta_v)$, где $\eta_\rho = N_{\rho+v}$, $\rho = \overline{1, v}$.

Ш а г 8. $\ell = 1$.

Ш а г 9. Если в матрице $D_1 = (z_{\rho,\beta})$, $\rho = \overline{\ell, v}$, $\beta = \overline{\ell, v}$, существуют нулевые строки и столбцы, то перейти к шагу 19, иначе найти $\sigma = \min\{\xi \mid \xi \in \{\ell, ..., 1\}, z_{\xi\ell} \ne -1\}$. Если $\sigma \ne \ell$, то перейти к шагу 10, иначе — к шагу 13.

Ш а г 10. $\beta = \ell$.

Ш а г 11. Последовательно принимать: $c = z_{\ell,\beta}$, $z_{\ell,\beta} = z_{\sigma,\beta}$, $z_{\sigma,\beta} = c$.

Ш а г 12. $\beta := \beta + 1$. Если $\beta \le \nu$, то перейти к шагу 11, иначе принимать последовательно $c = \eta_\ell$, $\eta_\ell = \eta_\sigma$, $\eta_\sigma = c$ и перейти к шагу 13.

Ш а г 13. $\rho = \ell + 1$. Если $\rho > \nu$, то перейти к шагу 18, иначе — к шагу 14.

Ш а г 14. $\beta = \ell$.

Ш а г 15. $z_{\rho,\beta} := MC(z_{\rho,\beta} * z_{\ell,\ell}, z_{\ell,\beta} * z_{\rho,\ell})$.

Ш а г 16. $\beta := \beta + 1$. Если $\beta \le \nu$, то перейти к шагу 15, иначе — принимать $\eta_\rho := MC(\eta_\rho * z_{\ell,\ell}, \eta_\ell * z_{\rho,\ell})$ и перейти к шагу 17.

Ш а г 17. $\rho := \rho + 1$. Если $\rho \le \nu$, то перейти к шагу 14, иначе — к шагу 18.

Ш а г 18. $\ell := \ell + 1$. Если $\ell \le \nu$, то перейти к шагу 9, иначе — к шагу 20.

Ш а г 19. $v := v - 1$. Перейти к шагу 7.

Ш а г 20. $\lambda_1 = (2^m - 1 - z_{vv}) * \eta_v$.

Ш а г 21. $\rho := 2$.

Ш а г 22. $\gamma := -1; \sigma = 1$.

Ш а г 23. $\gamma := MC(\gamma, z_{v-\rho+1, v-\rho+1+\sigma} * \lambda_{\rho-\sigma})$.

Ш а г 24. $\sigma := \sigma + 1$. Если $\sigma \le \rho - 1$, то перейти к шагу 23, иначе — к шагу 25.

Ш а г 25. $\lambda_\rho := (2^m - 1 - z_{v-\rho+1, v-\rho+1}) * MC(\eta_{v-\rho+1}, \gamma)$.

Ш а г 26. $\rho := \rho + 1$. Если $\rho \le \nu$, то перейти к шагу 23, иначе — к шагу 27.

Ш а г 27. $\beta = -1, \lambda_0 = 0, \sigma = 0$.

Ш а г 28. $\lambda(\beta) := MC((\lambda_\nu * \beta), \lambda_{v-1}), \ell = v - 2$.

Ш а г 29. $\lambda(\beta) := MC((\lambda(\beta) * \beta), \lambda_\ell)$.

Ш а г 30. $v := v - 1$. Если $\ell \ge 0$, то перейти к шагу 29, иначе — к шагу 31.

Ш а г 31. Если $\lambda(\beta) \ne -1$, то перейти к шагу 33, иначе — к шагу 32.

Ш а г 32. $\sigma := \sigma + 1$, $x_\sigma = \beta$. Если $\sigma \ge v$, то перейти к шагу 34, иначе — к шагу 33.

Ш а г 33. $\beta := \beta + 1$. Если $\beta \le 2^m - 2$, то перейти к шагу 28, иначе — к шагу 34.

Ш а г 34. Для каждого $\ell = 1, ..., v$ определить p_ℓ по формуле $p_\ell = 2^m - 1 - x_\ell$.

Ш а г 35. Принимать: $\upsilon_{p_\ell} := \upsilon_{p_\ell} + 1, GF(2), \ell = 1, ..., v$.

Ш а г 36. Делить многочлен $\upsilon(x)$ на многочлен $g(x) = g_{n-k} x^{n-k} + ... + g_1 x + g_0$ по следующей схеме [5]:

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

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

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

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

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

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

Ш а г 37. Определить компоненты информационного вектора по формуле $i_{k-\beta} = I_{k-\beta}[\beta], \ \beta = 1, 2, ..., k$.

Ш а г 38. Конец.

Выводы

Таким образом, на основе метода Гаусса и использования специальных таблиц достигнуто ускорение выполнения алгоритма ПГЦ для обнаружения и исправления ошибок в принятом многочлене. Этот алгоритм 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., 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

ON ONE MODIFICATION OF THE PETERSON-GORENSTEIN-ZIERLER ALGORITHM AND ITS EFFECTIVE REALIZATION

A modification of the Peterson-Gorenstein-Zierler algorithm based on the Gauss method is proposed. The effective method for realization of the modified algorithm is proposed to accelerate the detection and correction of errors in the binary Bose-Chaudhuri-Hocquenghem codes. The tables of operations over the elements of the finite field were used and it was offered to use the exponent of a power of the chosen primitive element representation instead of the element. The detailed description of decoding algorithm of the received messages is given.

K e y w o r d s: Bose-Choudhuri-Hockwinham code, Peterson-Gorenstein-Zierler algorithms, primitive element of finite field, error locator.

REFERENCES

1. Bleikhut, R. (1986), *Teoriya i praktika kodov kontroliruyushchikh oshibk*i [Theory and practice of codes controlling errors], Mir, Moscow, Russia.
2. Ivanov, M.A. (2001), *Kriptograficheskie 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. and Vera, P. (2003), Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, U.K.
4. Birkgof, G. and Barti, T. (1976), *Sovremennaya prikladnaya algebra* [Modern applied algebra], Mir, Moscow, Russia.
5. Feyziyev, F.G. and Megrdad Babavand (2012*),* "Description of decoding of cyclic codes in the klass of successeve machines based on Meggitt theorem", *Avtomatika i vychislitelnaya tekhnika*, no. 4, pp. 26-33.

Поступила 06.11.14

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