УДК 004.056.55

ОПРЕДЕЛЕНИЕ ВЕСА ОШИБКИ В ПРИМИТИВНЫХ БЧХ-КОДАХ

Н.В. СПИЧЕКОВА, В.А. ЛИПНИЦКИЙ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Военная академия Республики Беларусь
Минск-57, 220057, Беларусь

Поступила в редакцию 24 сентября 2015

Исследованы свойства синдромов ошибок весом 1-4 в примитивных БЧХ-кодах C_9, приведен алгоритм определения кратности возникшей ошибки по ее синдрому, показана связь между предлагаемым алгоритмом и методом определителей Блейхута.

Ключевые слова: помехоустойчивое кодирование, БЧХ-код, синдром ошибки, вес ошибки, метод определителей Блейхута.

Введение

Современные цифровые телекоммуникационные системы (ТКС), за исключением волоконно-оптических, функционируют с непременным кодированием информации помехоустойчивыми кодами. Это позволяет синхронно исправлять ошибки, возникающие в процессе передачи этой информации в каналах, как правило, насыщенных разного рода шумами и помехами.

Самый массовый вид ТКС – системы мобильной связи. На сегодняшний день они обеспечивают исправление двойных ошибок на блок передаваемой информации. Потребности увеличения информационных потоков и их скорости сталкиваются с необходимостью исправлять ошибки кратностью, большей двух. При любом методе коррекции ошибок – будь то метод алгебраических уравнений [1], перестановочные норменные методы [2], или иные – знание веса возникшей ошибки делают процедуру ее исправления более целенаправленной.

Единственным и исчерпывающим свидетельством наличия ошибки в принятом блоке-сообщении является ее синдром, непременно вычисляемый на входе каждого приемного устройства ТКС. Данная работа посвящена методикам определения кратности ошибки по ее синдрому в БЧХ-кодах, конструктивно рассчитанных на коррекцию 4-кратных ошибок.

Краткие сведения о БЧХ-кодах

Пусть C_9 – примитивный БЧХ-код длиной $n = 2^m - 1$ с проверочной матрицей $H = (\alpha^i, \alpha^{3i}, \alpha^{5i}, \alpha^{7i})^T$, двоичной, порядка $4m \times n$, для примитивного элемента α поля Галуа $GF(2^m)$ характеристики 2 из 2^m элементов [2, 3]. Такой код имеет конструктивное расстояние 9 (то есть минимальный вес ненулевых кодовых слов равен 9) и потому гарантированно исправляет ошибки весом ϖ, $1 \le \varpi \le 4$. Реальное минимальное расстояние d таких кодов может быть и большим. Так, у кода C_9 длиной 31 $d = 11$ ([3], с. 204).

Пусть $\bar{e}$ – вектор-ошибка, который наложился на очередной блок-сообщение $\bar{c}$ – двоичный вектор длиной n (т.е. с n координатами). Тогда на приемном конце ТКС будет принят вектор $\bar{x} = \bar{c} + \bar{e}$. О наличии ошибки в этом сообщении свидетельствует ее синдром

$S(\bar{x}) = H \cdot \bar{x}^T = S(\bar{e}) = H \cdot \bar{e}^T$, равный сумме столбцов матрицы H, номера которых совпадают с номерами ненулевых координат вектора $\bar{e}$. В силу структуры матрицы H синдром $S(\bar{e}) = H \cdot \bar{e}^T = (s_1, s_2, s_3, s_4)^T$, где компоненты синдрома s_1, s_2, s_3, s_4 являются некоторыми элементами поля Галуа $GF(2^m)$.

Синдромы всех ошибок весом ϖ, $1 \le \varpi \le 4$, попарно различны в коде C_9. Это обстоятельство является основой синдромных методов коррекции ошибок, например, метода алгебраических уравнений. Однако для высокоскоростных систем связи, в частности, для мобильных, такой метод не подходит – слишком медленный. Не спасает и метод Берлекэмпа-Месси [3, 4] решения уравнений степени 4 и выше. А если реальное минимальное расстояние больше конструктивного, то метод уравнений для коррекции ошибок кратностью, большей 4, и вовсе неприменим.

Теория норм синдромов (ТНС) в возникшей ситуации является единственным реальным и конструктивным средством коррекции многократных ошибок. Правда, адаптация ее к конкретным условиям требует отдельной серьезной работы. Первым и весьма желательным шагом здесь, как и в случае любого синдромного метода, является определение веса возникшей ошибки.

Свойства синдромов однократных и двукратных ошибок

Из сказанного выше следует, что вектор-ошибка $\bar{e}$ имеет вес 1 тогда и только тогда, когда ее синдром $S(\bar{e}) = H \cdot \bar{e}^T = (s_1, s_2, s_3, s_4)^T$ совпадает с одним из столбцов матрицы H, т.е. тогда и только тогда, когда

$$s_2 = s_1^3;\ s_3 = s_1^5;\ s_4 = s_1^7. \qquad (1)$$

Для двукратных ошибок имеет место следующая зависимость между компонентами их синдромов.

Теорема 1. *Пусть $\bar{e} = (i, j)$ – ошибка веса 2 на неизвестных позициях i и j. Пусть $S(\bar{e}) = (s_1, s_2, s_3, s_4)^T$ – ее синдром. Тогда $s_1 \neq 0$, а компоненты s_3 и s_4 алгебраически выражаются через первые две компоненты синдрома по формулам*:

$$\begin{aligned} s_3 &= s_1^5 + s_1^2 s_2 + \frac{s_2^2}{s_1}, \\ s_4 &= s_1^7 + s_1 s_2^2 + \frac{s_2^3}{s_1^2}. \end{aligned} \qquad (2)$$

Доказательство. Введем обозначения: $x = \alpha^{i-1}, y = \alpha^{j-1}$

Пусть $s_1 = 0$. Тогда $x + y = 0$. Отсюда $x = y$ и $i = j$. Однако это невозможно.

Для ошибки $\bar{e} = (i, j)$ выполняется: $x + y = s_1$, $x^3 + y^3 = s_2$, $x^5 + y^5 = s_3$, $x^7 + y^7 = s_4$. Подставляя выражения для компонент синдрома $S(\bar{e})$ в (2), получим:

$$x^5 + y^5 = (x+y)^5 + (x+y)^2 (x^3 + y^3) + \frac{(x^3 + y^3)^2}{x+y},$$

$$x^7 + y^7 = (x+y)^7 + (x+y)(x^3 + y^3)^2 + \frac{(x^3 + y^3)^3}{(x+y)^2}.$$

Преобразуем правые части полученных равенств:

$$(x+y)^5+(x+y)^2(x^3+y^3)+\frac{(x^3+y^3)^2}{x+y}=(x+y)^2\left((x+y)^3+(x^3+y^3)\right)+\frac{(x+y)^2(x^2+xy+y^2)^2}{x+y}=$$

$$=(x+y)^2(x^3+x^2y+xy^2+y^3+x^3+y^3)+(x+y)(x^2+xy+y^2)^2=$$

$$=(x+y)^2(x^2y+xy^2)+(x+y)(x^2+xy+y^2)^2=(x+y)\left((x+y)(x^2y+xy^2)+(x^2+xy+y^2)^2\right)=$$

$$=(x+y)(x^3y+x^2y^2+x^2y^2+xy^3+x^4+x^2y^2+y^4)=(x+y)(x^3y+xy^3+x^4+x^2y^2+y^4)=$$

$$=x^4y+x^2y^3+x^5+x^3y^2+xy^4+x^3y^2+xy^4+x^4y+x^2y^3+y^5=x^5+y^5,$$

$$(x+y)^7+(x+y)(x^3+y^3)^2+\frac{(x^3+y^3)^3}{(x+y)^2}=(x+y)^7+(x+y)^3(x^2+xy+y^2)^2+$$

$$+\frac{(x+y)^3(x^2+xy+y^2)^3}{(x+y)^2}=(x+y)^3\left((x+y)^4+(x^2+xy+y^2)^2\right)+(x+y)(x^2+xy+y^2)^3=$$

$$=(x+y)^3(x^4+y^4+x^4+x^2y^2+y^4)+(x+y)(x^2+xy+y^2)^3=(x+y)^3x^2y^2+(x+y)(x^2+xy+y^2)^3=$$

$$=(x+y)\left((x+y)^2x^2y^2+(x^2+xy+y^2)^2(x^2+xy+y^2)\right)=$$

$$=(x+y)\left((x^2+y^2)x^2y^2+(x^4+x^2+y^2+y^4)(x^2+xy+y^2)\right)=$$

$$=(x+y)(x^4y^2+x^2y^4+x^6+x^5y+x^4y^2+x^4y^2+x^3y^3+x^2y^4+x^2y^4+xy^5+y^6)=$$

$$=(x+y)(x^6+x^5y+x^4y^2+x^3y^3+x^2y^4+xy^5+y^6)=x^7+x^6y+x^5y^2+x^4y^3+x^3y^4+x^2y^5+xy^6+$$

$$+x^6y+x^5y^2+x^4y^3+x^3y^4+x^2y^5+xy^6+y^7=x^7+y^7.$$

Доказательство завершено.

Теорема 2. *Пусть* $S(\bar{e})=(s_1,s_2,s_3,s_4)^T$ *– синдром ошибки* $\bar{e}$ *веса* ϖ, $1\le\varpi\le4$, $s_1\neq0$, *и выполняется первое из соотношений* (2). *Тогда* $\varpi=1$ *или* $\varpi=2$.

Доказательство. Отметим, что если $\bar{e}$ – ошибка веса 1, то для ее синдрома выполняется (1). Подставив $s_2=s_1^3, s_3,=s_1^5, s_4=s_1^7$ в (2), получим тождества.

Предположим, что $\bar{e}=(i,j,k)$ – ошибка веса 3. Тогда $\alpha^{i-1}+\alpha^{j-1}+\alpha^{k-1}=s_1$, $\alpha^{3(i-1)}+\alpha^{3(j-1)}+\alpha^{3(k-1)}=s_3$, $\alpha^{5(i-1)}+\alpha^{5(j-1)}+\alpha^{5(k-1)}=s_3$. Введем обозначения: $x=\alpha^{i-1}$, $y=\alpha^{j-1}$, $z=\alpha^{k-1}$. Подставляя выражения для s_1,s_2,s_3 в первую формулу в (2), в новых переменных получим: $\frac{xyz(x+y)(x+z)(y+z)}{x+y+z}=0$. Из последнего равенства следует выполнение одного из следующих условий: $x=0$, $y=0$, $z=0$, $x=y$, $x=z$, $y=z$. Однако это невозможно.

Пусть теперь $\bar{e}=(i,j,k,u)$ – ошибка веса 4. Тогда: $\alpha^{i-1}+\alpha^{j-1}+\alpha^{k-1}+\alpha^{u-1}=s_1$, $\alpha^{3(i-1)}+\alpha^{3(j-1)}+\alpha^{3(k-1)}+\alpha^{3(u-1)}=s_2$, $\alpha^{5(i-1)}+\alpha^{5(j-1)}+\alpha^{5(ik-1)}+\alpha^{5(u-1)}=s_3$. Введем обозначения $x=\alpha^{i-1}$, $y=\alpha^{j-1}$, $z=\alpha^{k-1}$, $w=\alpha^{u-1}$. Подставляя выражения для s_1,s_2,s_3 в первую формулу в (2), в новых переменных получим: $\frac{(x+y)(x+z)(y+z)(x+w)(y+w)(z+w)}{x+y+z+w}=0$. Из последнего равенства следует выполнение одного из следующих условий: $x=y$, $x=z$, $y=z$, $x=w$, $y=w$, $z=w$. Однако это невозможно. Доказательство завершено.

Свойства синдромов трехкратных ошибок

Пусть $\sigma_1=x_1+x_2+x_3$, $\sigma_2=x_1x_2+x_1x_3+...+x_{n-1}x_n$, …, $\sigma_3=x_1x_2...x_n$ – элементарные симметрические многочлены от n переменных. Для степенных сумм $f_k=x_1^k+x_2^k+x_3^k$, $k=1,2,...,$ Ньютоном были установлены следующие реккурентные формулы:

$$f_k - f_{k-1}\sigma_1 + f_{k-2}\sigma_2 - \ldots + (-1)^{k-1} f_1\sigma_{k-1} + (-1)^k k\sigma_k = 0, k \le n, \quad (3)$$

$$f_k - f_{k-1}\sigma_1 + f_{k-2}\sigma_2 - \ldots + (-1)^n f_{k-n}\sigma_n = 0, k > n. \quad (4)$$

Очевидно,

$$f_1 = \sigma_1. \quad (5)$$

Рассмотрим формулы (3) и (4) в поле $GF(2^p)$ при $n = 3$. Если $k = 2$, то формула (3) имеет вид: $f_2 = f_1\sigma_1$, откуда $f_2 = \sigma_1^2$. При $k = 3$ из (3) следует: $f_3 + f_2\sigma_1 + f_1\sigma_2 + \sigma_3 = 0$. Подстановкой в это уравнение найденных выражений для f_1 и f_2 получаем:

$$\sigma_3 = f_3 + \sigma_1^3 + \sigma_1\sigma_2. \quad (6)$$

Если $k = 4$, то формула (4) имеет вид: $f_4 + f_3\sigma_1 + f_2\sigma_2 + f_1\sigma_3 = 0$. Подставляя в это уравнение выражения для f_1, f_2 и σ_3, получаем: $f_4 = \sigma_1^4$. При $k = 5$ из (4) следует: $f_5 + f_4\sigma_1 + f_3\sigma_2 + f_2\sigma_3 = 0$. Подстановкой в это уравнение найденных выражений для f_1, f_2, f_4 и σ_3, получаем: $\sigma_2(f_3 + \sigma_1^3) + f_5 + \sigma_1^2 f_3 = 0$. Если $f_3 + \sigma_1^3 \ne 0$, то из последнего равенства следует:

$$\sigma_2 = \frac{f_5 + \sigma_1^2 f_3}{f_3 + \sigma_1^3}. \quad (7)$$

Если $k = 6$, то формула (4) имеет вид: $f_6 + f_5\sigma_1 + f_4\sigma_2 + f_3\sigma_3 = 0$. Подставляя в это уравнение выражения для f_1, f_2, f_4, σ_2, σ_3, получаем: $f_6 = f_3^2$. При $k = 7$ из (4) следует: $f_7 + f_6\sigma_1 + f_5\sigma_2 + f_4\sigma_3 = 0$. Подстановкой в это уравнение найденных выражений для f_4, f_6 получаем:

$$f_7 = f_3^2\sigma_1 + f_5\sigma_2 + \sigma_1^4\sigma_3. \quad (8)$$

Теорема 3. *Пусть* $\bar{e} = (i, j, k)$ *– ошибка веса* 3 *на неизвестных позициях* i, j, k, $S(\bar{e}) = (s_1, s_2, s_3, s_4)^T$ *– ее синдром. Тогда* $s_1^3 + s_2 \ne 0$ *и*

$$s_4 = \sigma_1 s_2^2 + \sigma_2 s_3 + \sigma_1^4\sigma_3, \quad (9)$$

где

$$\sigma_1 = s_1, \sigma_2 = \frac{\sigma_1^2 s_2 + s_3}{\sigma_1^3 + s_2}, \sigma_3 = \sigma_1^3 + s_2 + \sigma_1\sigma_2. \quad (10)$$

Доказательство. Пусть для ошибки $\bar{e} = (i, j, k)$ веса 3 выполняется $s_1^3 + s_2 = 0$. Введем обозначения: $x = \alpha^{i-1}, y = \alpha^{j-1}, z = \alpha^{k-1}$. В новых переменных равенство $s_1^3 + s_2 = 0$ перепишется в виде: $(x + y + z)^3 + x^3 + y^3 + z^3 = 0$. Раскрывая скобки в левой части равенства, получим:

$$(x^2 + y^2 + z^2)(x + y + z) + x^3 + y^3 + z^3 = x^3 + x^2y + x^2z + xy^2 + y^3 + y^2z + xz^2 +$$
$$+ yz^2 + z^3 + x^3 + y^3 + z^3 = x^2y + x^2z + xy^2 + y^2z + xz^2 + yz^2 =$$
$$= x^2(y + z) + x(y^2 + z^2) + yz(y + z) = x^2(y + z) + x(y + z)^2 + yz(y + z) =$$
$$= (y + z)\left(x^2 + x(y + z) + yz\right) = (y + z)\left(x^2 + xy + xz + yz\right) = (y + z)\left(x(x + y) + z(x + y)\right) =$$
$$= (y + z)(x + y)\left(x + z\right).$$

Из равенства $(y + z)(x + y)\left(x + z\right) = 0$ следует выполнение одного из следующих условий: $x = y, x = z, y = z$. Однако это невозможно.

Для компонент синдрома $S(\bar{e})$ выполняется: $s_1 = x + y + z = f_1$, $s_2 = x^3 + y^3 + z^3 = f_3$, $s_3 = x^5 + y^5 + z^5 = f_5$, $s_4 = x^7 + y^7 + z^7 = f_7$, где f_1, f_3, f_5, f_7 – степенные суммы трех переменных x, y, z. Подставляя в (5)-(7) вместо f_1, f_3, f_5 соответственно s_1, s_2, s_3, получим (10). Подставляя в (8) вместо f_3, f_5, f_7 соответственно s_2, s_3, s_4, получим (9). Доказательство завершено.

Теорема 4. *Пусть* $S(\bar{e}) = (s_1, s_2, s_3, s_4)^T$ – *синдром ошибки* $\bar{e}$ *веса* ϖ, $1 \le \varpi \le 4$, $s_1^3 + s_2 \ne 0$, *и выполняется соотношение* (9), *где* $\sigma_1, \sigma_2, \sigma_3$ *определяются по формулам* (10). *Тогда* $\varpi = 2$ *или* $\varpi = 3$.

Доказательство. Из (1) следует, что для ошибки веса 1 выполняется $s_1^3 + s_2 = 0$.

Пусть $\bar{e} = (i, j)$ – ошибка веса 2. Введем обозначения: $x = \alpha^{i-1}, y = \alpha^{j-1}$. Тогда $x + y = s_1$, $x^3 + y^3 = s_2$, $x^5 + y^5 = s_3$, $x^7 + y^7 = s_4$. Подставив выражения для s_1, s_2, s_3, s_4 в (10), найдем: $\sigma_1 = x + y, \sigma_2 = xy, \sigma_3 = 0$. Подставляя полученные выражения в (9), получим: $s_4 = x^7 + y^7$ – тождество.

Если $\bar{e}$ – ошибка веса 3, то соотношение (4) выполняются в силу теоремы 4.

Пусть $\bar{e} = (i, j, k, u)$ – ошибка веса 4. Введем обозначения: $x = \alpha^{i-1}, y = \alpha^{j-1}, z = \alpha^{k-1}, v = \alpha^{u-1}$. Тогда $x + y + z + v = s_1$, $x^3 + y^3 + z^3 + v^3 = s_2$, $x^5 + y + z^5 + v^5 = s_3$, $x^7 + y^7 + z^7 + v^7 = s_4$. Подставляя выражения для s_1, s_2, s_3, s_4 в (10), найдем $\sigma_1, \sigma_2, \sigma_3$. Подставляя найденные выражения в (9), получим $\dfrac{xyzv(x+y)(x+z)(y+z)(x+v)(y+v)(z+v)}{s_1^3 + s_2} = 0$. Из последнего равенства следует выполнение одного из следующих условий: $x = 0$, $y = 0$, $z = 0$, $v = 0$, $x = y$, $x = z, y = z, x = v, y = v, z = v$. Однако это невозможно. Доказательство завершено.

Свойства синдромов с нулевыми компонентами

Теорема 5. *В коде* C_9 *не существует ошибки* $\bar{e}$ *веса* ϖ, $1 \le \varpi \le 4$, *синдром* $S(\bar{e})$ *которой был бы равен* $S(\bar{e}) = (0, 0, s_3, s_4)^T$ *для некоторых* $s_3, s_4 \in GF(2^m)$.

Доказательство. Пусть синдром $S(\bar{e})$ ошибки $\bar{e}$ веса ϖ, $1 \le \varpi \le 4$, равен $S(e) = (s_1, s_2, s_3, s_4)^T$.

При $\varpi = 1$ равенство $s_1 = 0$ невозможно. При $\varpi = 2$ равенство $s_1 = 0$ невозможно в силу теоремы 2. Если $\bar{e}$ – ошибка веса 3, для которой $s_1 = 0$, то в силу теоремы 4 $s_2 \ne 0$.

Пусть $\bar{e} = (i, j, k, u)$ – ошибка веса 4, для которой $s_1 = s_2 = 0$. Введем обозначения: $x = \alpha^{i-1}, y = \alpha^{j-1}, z = \alpha^{k-1}, v = \alpha^{u-1}$. Из равенств $s_1 = s_2 = 0$ следует: $x + y + z + v = 0$, $x^3 + y^3 + z^3 + v^3 = 0$. Из первого равенства следует: $v = x + y + z$. Подставляя это выражение во второе равенство, найдем: $x^3 + y^3 + z^3 + (x + y + z)^3 = 0$. Преобразуем левую часть полученного соотношения:

$$x^3 + y^3 + z^3 + (x + y + z)^3 = x^3 + y^3 + z^3 + (x + y + z)(x + y + z)^2 =$$
$$= x^3 + y^3 + z^3 + (x + y + z)(x^2 + y^2 + z^2) = x^3 + y^3 + z^3 + x^3 + xy^2 + xz^2 +$$
$$+ x^2 y + y^3 + yz^2 + x^2 z + y^2 z + z^3 = x(y^2 + z^2) + x^2(y + z) + yz(y + z) =$$
$$= x(y + z)^2 + x^2(y + z) + yz(y + z) = (y + z)(x(y + z) + x^2 + yz) =$$
$$= (y + z)(xy + xz + x^2 + yz) = (y + z)(xy + x^2 + xz + yz) =$$
$$= (y + z)(x(x + y) + z(x + y)) = (y + z)(x + y)(x + z).$$

Из условия $(y+z)(x+y)(x+z)=0$ следует выполнение одного из следующих равенств: $x=y, x=z, y=z.$ Однако это невозможно. Доказательство завершено.

Теорема 6. *Пусть* $S(\bar{e})=(0,s_2,s_3,s_4)^T$, $s_2\neq 0$, *– синдром ошибки* $\bar{e}$ *веса* ϖ, $1\le\varpi\le 4$. *Тогда* $\varpi=3$, *если выполняется соотношение* (9), *и* $\varpi=4$ *в противном случае.*

Доказательство. Из формулы (1) и теоремы 1 следует, что при $\varpi=1$ и $\varpi=2$ равенство $s_1=0$ невозможно. Из теорем 3 и 4 следует, что при $3\le\varpi\le 4$ равенство (9) имеет место лишь в случае, если $\varpi=3$. Доказательство завершено.

Теорема 7. *Пусть* $S(\bar{e})=(s_1,s_2,s_3,s_4)^T$, *где* $s_1^3+s_2=0$, *– синдром ошибки* $\bar{e}$ *веса* ϖ, $1\le\varpi\le 4$. *Тогда* $\varpi=1$, *если выполняется соотношение* (1), *и* $\varpi=4$ *в противном случае.*

Доказательство. Пусть $\varpi=2$ и $\bar{e}=(i,j)$. Тогда $\alpha^{i-1}+\alpha^{j-1}=s_1$, $\alpha^{3(i-1)}+\alpha^{3(j-1)}=s_2$. Равенство $s_1^3=s_2$ равносильно тому, что $\alpha^{i-1}\alpha^{j-1}(\alpha^{i-1}+\alpha^{j-1})=0$, т.е. $i=j$. Однако это невозможно.

В силу теоремы 3 равенство $s_1^3+s_2=0$ невозможно при $\varpi=3$. Следовательно, $\varpi=1$ или $\varpi=4$. Для завершения доказательства необходимо учесть, что (1) выполняются только при $\varpi=1$. Доказательство завершено.

Теоремы 1-7 служат обоснованием корректности следующего алгоритма определения в коде C_9 веса ϖ ошибки $\bar{e}$ по ее синдрому $S(\bar{e})=(s_1,s_2,s_3,s_4)^T$ в случае, когда $1\le\varpi\le 4$.

Алгоритм определения веса ϖ ошибки в коде C_9

1. Проверяем, выполняется ли равенства (1).
   1.1. Пусть (1) выполняется. Тогда $\varpi=1$ и алгоритм закончил работу.
   1.2. Пусть (1) не выполняется.
      1.2.1. Пусть $s_1\neq 0$. Проверяем, выполняется ли первое соотношение в (2).
         1.2.1.1. Пусть первое соотношение в (2) выполняется. Тогда $\varpi=2$ и алгоритм закончил работу.
         1.2.1.2. Пусть первое соотношение в (2) не выполняется.
            1.2.1.2.1. Пусть $s_1^3+s_2\neq 0$. Проверяем, выполняется ли соотношение (9).
               1.2.1.2.1.1. Пусть (9) выполняется. Тогда $\varpi=3$ и алгоритм закончил работу.
               1.2.1.2.1.2. Пусть (9) не выполняется. Тогда $\varpi=4$ и алгоритм закончил работу.
            1.2.1.2.2. Пусть $s_1^3+s_2=0$. Тогда $\varpi=4$ и алгоритм закончил работу.
      1.2.2. Пусть $s_1=0$. Проверяем, выполняется ли соотношение (9).
         1.2.2.1. Пусть (9) выполняется. Тогда $\varpi=3$ и алгоритм закончил работу.
         1.2.2.2. Пусть (9) не выполняется. Тогда $\varpi=4$ и алгоритм закончил работу.

Связь с методом определителей Блейхута

В [1] описан метод определения веса ошибки в БЧХ-коде на основании ее синдрома. Суть метода заключается в следующем.

Для БЧХ-кода C_{2t+1}, гарантированно исправляющего ошибки веса $\varpi, 1 \le \varpi \le t,$ и ошибки $\bar{e} = (i_1,...,i_\varpi)$ с синдромом $S(\bar{e}) = (s_1,\ldots,s_t)$ рассматривается матрица $M_\mu = \begin{pmatrix} S_1\ S_2 \ldots S_\mu \\ S_2\ S_3 \ldots S_{\mu+1} \\ \ldots \\ S_\mu\ S_{\mu+1} \ldots S_{2\mu-1} \end{pmatrix}$ порядка μ. Для двоичных БЧХ-кодов: $S_{2j} = S_j^2,\ S_{2j-1} = s_j,\ j \ge 1.$

Доказано (см. [1] с. 197), что $\det M_\mu \ne 0$, если μ равно весу ϖ произошедшей в действительности ошибки. Если же $\mu > \varpi$, то $\det M_\mu = 0$. При определении веса ϖ произошедшей в действительности ошибки поступают следующим образом. В качестве пробного значения берут $\varpi = t$ и вычисляют $\det M_\mu$. Если $\det M \ne 0$, то найдено правильное значение для ϖ. Если же $\det M_\mu = 0$, то уменьшают значение $\varpi = t$ на 1 и повторяют процедуру. Поступают таким образом до тех пор, пока не будет получен определитель, отличный от 0.

Рассмотрим код C_9. Предположим, что произошла ошибка $\bar{e} = (i_1,...,i_\varpi)$ веса $\varpi,$ $1 \le \varpi \le 4,$ с синдромом $s(\bar{e}) = (s_1, s_2, s_3, s_4)$. Тогда:

$$\det M_4 = \begin{vmatrix} s_1 & s_1^2 & s_2 & s_1^4 \\ s_1^2 & s_2 & s_1^4 & s_3 \\ s_2 & s_1^4 & s_3 & s_3^2 \\ s_1^4 & s_3 & s_3^2 & s_4 \end{vmatrix} =$$

$$= (s_1^6 + s_1^3 s_2 + s_2^2 + s_1 s_3)(s_1^{10} + s_1^7 s_2 + s_1 s_2^3 + s_1^5 s_3 + s_1^2 s_2 s_3 + s_3^2 + (s_1^3 + s_2)s_4);$$

$$\det M_3 = \begin{vmatrix} s_1 & s_1^2 & s_2 \\ s_1^2 & s_2 & s_1^4 \\ s_2 & s_1^4 & s_3 \end{vmatrix} = (s_1^3 + s_2)(s_1^6 + s_1^3 s_2 + s_2^2 + s_1 s_3);$$

$$\det M_2 = \begin{vmatrix} s_1 & s_1^2 \\ s_1^2 & s_2 \end{vmatrix} = s_1(s_1^3 + s_2);$$

$$\det M_1 = |s_1| = s_1.$$

В соответствии с методом определителей Блейхута:

- если выполняется (1), то $\det M_1 = s_1 \ne 0, \det M_2 = \det M_3 = \det M_4 = 0$ и $\varpi = 1$;

- если (1) не выполняется, $s_1 \ne 0$ и имеет место первое соотношение из (3), то $\det M_2 = s_1(s_1^3 + s_2) \ne 0, \det M_3 = \det M_4 = 0$ и $\varpi = 2$;

- если $s_1 \ne 0$, (1) и первое соотношение из (3) не выполняются, $s_1^3 + s_2 \ne 0$ и справедливо (4), тогда $\det M_3 = s_1(s_1^3 + s_2)(s_1^5 + s_1^2 s_2 + \frac{s_2^2}{s_1} + s_3) \ne 0, \det M_4 = 0$ и $\varpi = 3$;

- если $s_1 \ne 0$, (1) и первое соотношение из (3) не выполняются, $s_1^3 + s_2 \ne 0$ и равенство (4) не имеет места, то $\det M_4 = s_1(s_1^3 + s_2)(s_1^5 + s_1^2 s_2 + \frac{s_2^2}{s_1} + s_3)(\sigma_1 s_2^2 + \sigma_2 s_3 + \sigma_3 s_1^4 + s_4) \ne 0$, где $\sigma_1, \sigma_2, \sigma_3$ задаются формулами (5), и $\varpi = 4$;

- если $s_1 \ne 0$, (1) и первое соотношение из (3) не выполняются и $s_1^3 + s_2 = 0$, то $\det M_4 = s_1(s_1^5 + s_3) \ne 0$ и $\varpi = 4$;

- если (1) не выполняется, $s_1 = 0$ и справедливо (4), то $\det M_3 = s_2^3 \neq 0$, $\det M_4 = 0$ и $\varpi = 3$;

- если $s_1 = 0$ и (1) и (4) не выполняются, то $\det M_4 = s_2^2(s_3^2 + s_2 s_4) \neq 0$ и $\varpi = 4$.

Таким образом, алгоритм определения веса ошибки в коде C_9, изложенный в предыдущем пункте, эквивалентен методу определителей Блейхута.

Заключение

Определители Блейхута дают возможность определения кратности ошибки в коде. Но их применение требует введения дополнительных параметров и достаточно громоздкой процедуры вычисления самих определителей. Предложенный в работе алгоритм является прямым и непосредственным средством быстрого определения кратности ошибок ограниченного веса.

DETECTION OF ERROR WEIGHT IN THE PRIMITIVE BCH-CODE

N.V. SPICHEKOVA, V.A. LIPNITSKI

Abstract

The properties of the syndromes for errors of weight 1-4 in the primitive BCH-code C_9 are investigated. An algorithm to determine the multiplicity of an error based on its syndrome is described. The relationship between the proposed algorithm and Blahut's method of determinants is shown.

Список литературы

1. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М., 1986.
2. *Липницкий В.А.*, *Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Мн., 2007.
3. *Мак-Вильямс Ф.Дж.*, *Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М., 1979.
4. *Лидл Р., Нидеррайтер Г.* Конечные поля. М., 1988.