ПЕРЕСТАНОВОЧНОЕ ДЕКОДИРОВАНИЕ БЧХ-КОДОВ С МИНИМАЛЬНЫМ РАССТОЯНИЕМ 7

Липницкий В.А., Конопелько В.К.

Белорусский государственный университет информатики и радиоэлектроники
Беларусь, 220600, г. Минск, ул. П. Бровки, 6
Тел: (0172) 32-42-00, E-mail: kafsiut@gw.bsuir.unibel.by

Реферат: Разработана теория норм синдромов для БЧХ-кодов с d=7. Нормы синдромов инварианты относительно группы циклических сдвигов Г, которая разбивает весь спектр векторов-ошибок на классы эквивалентности – Г-орбиты. Классы эквивалентности векторов-ошибок веса 1, 2, 3 в названных БЧХ-кодах имеют попарно-различные нормы. Тем самым обеспечивается перестановочный метод коррекции ошибок БЧХ-кодами: по синдрому принятого сообщения, вычисляется норма, по ней идентифицируется класс ошибки и следовательно, образующий этот класс вектор ошибок, который с помощью циклических сдвигов преобразуется в искомый.

1. Введение

Основным препятствием использования помехоустойчивых кодов в качественных цифровых сетях связи является “проблема селектора” [1, 2]: сложность вычислительной реализации решения уравнений степени t>2 в полях Галуа (t кратность корректируемых ошибок). Известны различные методы решения проблемы [1-3], которые приводят к низкоскоростным алгоритмам коррекции ошибок.

В [4] предложен перестановочный метод декодирования БЧХ-кодов с d=5 позволяющий устранить названное препятствиеа также расширить спектр декодируемых данным кодом ошибок. Ниже предлагается развитие перестановочного метода на БЧХ-коды с кодовым расстоянием 7.

2. Необходимые сведения о О БЧХ-кодах

Пусть α — фиксированный примитивный элемент поля Галуа $GF(2^m)$, где m>1. Тогда элементы этого поля $1,\alpha,\alpha^2,...,\alpha^{m-1}$ образуют базис векторного пространства $GF(2^m)$ над полем GF(2). В дальнейшем, в зависимости от контекста, будем рассматривать величины α^i, $0\le i\le n-1$ для $n=2^m-1$, либо как элементы $GF(2^m)$, либо как столбцы из m координат в названном базисе. Поэтому запись: $H=(\alpha^i,\alpha^{3i},\alpha^{5i})^T$, $0\le i\le n-1$, есть компактное представление двоичной 3m×n-матрицы с элементами 0,1 из GF(2). При m≥4 число ее строк 3m≤n.

Как известно [2], линейный (n,k)-код C с проверочной матрицей $H=(\alpha^i,\alpha^{3i},\alpha^{5i})^T$, $0\le i\le n-1$, называется двоичным примитивным БЧХ-кодом. Это циклический код. При m≥4 его кодовое расстояние d≥7 [2].

Для произвольного вектора $\bar{e}\in V_n$ его синдром в БЧХ-коде C есть двоичный вектор $\bar{s}=S(\bar{e})=H\cdot\bar{e}^T$ с 3m координатами. Сгруппировав эти координаты последовательно в три группы по m координат в каждой, $\bar{s}$ можно записать как вектор (s_1,s_2,s_3) с координатами $s_1,s_2,s_3\in GF(2^m)$.

Лемма 1. Множество $\Sigma=S(V_n)$ синдромов всех векторов-ошибок в БЧХ-коде образует трехмерное векторное пространство над полем $GF(2^m)$, то есть для любого вектора (s_1,s_2,s_3), где $s_1,s_2,s_3\in GF(2^m)$, найдется вектор-ошибка $\bar{e}\in V_n$, что $S(\bar{e})=(s_1,s_2,s_3)$.

Следствие. Мощность множества $\Sigma=S(V_n)$ равна $(2^m)^3=2^{3m}=(n+1)^3$.

Лемма 2. Синдромы векторов-ошибок веса 1,2,3 в коде C попарно различны.

3. Классификация ошибок двоичных кодов

Код C является циклическим кодом. Следовательно, группа Г циклических сдвигов является подгруппой группы автоморфизмов кода C. Под действием Г пространство всех возможных векторов-ошибок – n-мерное пространство двоичных векторов – разбивается на классы эквивалентности – Г-орбиты (детали см. в [4,5], в частности, описание Г-орбит ошибок веса 1,2). Они содержат по n векторов, переходящих друг в друга под действием циклических сдвигов.

Иногда Г-орбиты содержат k векторов, где k делит n, если они содержит векторы с внутренней симметрией.

Определение. Вектор-ошибка $\bar{e}=(e_1, e_2,\ldots, e_n)$ из пространства E_n называется b-периодической для делителя b числа n, если ее координаты удовлетворяют условию:

$$e_{ib+j}=e_j \qquad (1)$$

для произвольных целых i и j, где $1\le j\le b$, $1\le i\le r-1$, $rb=n$.

Лемма 3. Пусть $\bar{e}$ - b-периодическая вектор-ошибка, m-вектор из E_n, у которого первые b координат совпадают с координатами вектора $\bar{e}$, а остальные равны нулю. Тогда

$$\bar{e}=\bar{m}+\sigma^b(\bar{m})+\sigma^{2b}(\bar{m})+\ldots\sigma^{(r-1)b}(\bar{m}) \qquad (2)$$

Лемма 4. Пусть в условиях леммы 3 $\bar{m}_1$ – вектор с b координатами, получаемый из вектора m отбрасыванием (b+1)-ой и воследующих координат. Пусть $\sum$ - оператор циклического сдвига координат на пространстве ошибок E_b. Пусть $1\le\lambda<b$ и $\sum^{\lambda}(\bar{m})$ – вектор из E_n, у которого первые b координат совпадают с соответствующими координатами вектора $\sum^{\lambda}(m_1)$, а остальные равны 0. Пусть

@2001, электронная версия подготовлена ЗАО АВТЭКС Санкт-Петербург, http://www.autex.spb.ru

$$\bar{f}_\lambda = \sum^\lambda(\overline{m}) + \sigma^b(\sum^\lambda(\overline{m})) + \ldots + \sigma^{(r-1)b}(\sum^\lambda(\overline{m})).$$

Тогда $\sigma^\lambda(\overline{e}) = \bar{f}_\lambda$.

Доказательство непосредственно вытекает из структуры векторов $\overline{e}$ и $\bar{f}_\lambda$.

Предложение 1. В пространстве векторов-ошибок E_n существуют неполные Г-орбиты мощности b тогда и только тогда, когда n делится на b. Если n=br, то всякая Г-орбита J мощности b состоит из b-периодических векторов-ошибок веса δr, где 1≤δ<b для b>1, и диаметра Д≥(r-1)b+1.

Следствие 1. Если вектор-ошибка g не является периодической, то Г-орбита <g> является полной.

Следствие 2. Пусть b – делитель числа n. Количество Г-орбит мощности b в пространстве E_n равно количеству классов эквивалентности мощности b в пространстве векторов-ошибок длины b.

Следствие 3. В любом пространстве E_n имеются лишь две Г-орбиты мощности 1 – это <0> и <1>. Если n=p – число простое, то все остальные Г-орбиты являются полными (то есть содержат по n векторов). Всего в пространстве E_p имеется $\Pi_p = \dfrac{2^P - 2}{p}$ полных Г-орбит.

Заметим, что согласно малой теореме Ферма 2^{p-1} сравнимо с 1 по модулю p [6] и потому величина $\dfrac{2(2^{P-1}-1)}{p} = \Pi_p$ есть число целое.

Пример 1. В пространстве E_3 согласно следствию 3 число $\Pi_3 = \dfrac{2^3 - 2}{3} = 2$; в пространстве E_5 величина $\Pi_5 = \dfrac{2^5 - 2}{5} = 6$. Следовательно, в E_{15} имеются две Г-орбиты мощности 1, две Г-орбиты мощности 3 (это <(100 100 100 100 100)> и <(110 110 110 110 110)>); шесть Г-орбит мощности 5, порожденных следующими 5-модульными ошибками: (10000), (11000), (11100), (11110), (10100), (11010). Названные классы эквивалентности содержат 38 векторов-ошибок. В силу следствия 2 перечисленные г-орбиты исчерпывают весь список классов эквивалентности пространства E_{15}, мощность которых меньше 15. Следовательно, оставшиеся 2^{15} –38 векторов-ошибок распределяются по 2182 полным Г-орбитам. Из них одна содержит все ошибки веса 1 и 7 – ошибки веса 2.

Следствие 4. I. Периодическая вектор-ошибка может иметь вес 2 тогда и только тогда, когда n=2к – четно. При этом имеется одна Г-орбита таких векторов. Это <(1, k+1)>. Ее мощность равна n/2.

II. Периодическая вектор-ошибка может иметь вес 3 тогда и только тогда, когда n=3к. При этом имеется лишь одна Г-орбита таких векторов. Это <(1, k+1, 2k+1)>. Его мощность равна n/3.

Следующее утверждение описывает Г-орбиты ошибок веса 3.

Предложение 2. На двоичных кодовых словах длиной n возможно C_n^3 =n(n-1)(n-2)/6 различных ошибок веса 3. Они разбиваются на (n-1)(n-2)/6 полных Г-орбит для n, не делящихся на 3, а для n=3t они разбиваются на [C_n^3 /n] полных Г-орбит ([F] – целая часть числа F) плюс один класс эквивалентности из t векторов-ошибок, порождённый ошибкой на позициях 1, t+1, 2t+1.

4. Теория норм синдромов для БЧХ-кодовс D=7

Векторы, принадлежащие одной Г-орбите, имеют жестко связанные друг с другом синдромы в БЧХ-коде C.

Теорема 1. Пусть $\bar{e}$ – вектор-ошибка $\bar{e}=(e_1,\ldots,e_n)$; $\sigma(\bar{e}) = (e_n, e_1, e_2, \ldots, e_{n-1})$. Пусть синдром $S(\bar{e}) = (S_1, S_2, S_3)$. Тогда $S(\sigma^\lambda(\bar{e})) = (\alpha^\lambda S_1, \alpha^{3\lambda} S_2, \alpha^{5\lambda} S_3)$ для всякого целого λ.

Следствие 1. Вектор $N(S(\bar{e})) = (S_2/S_1^3, S_3/S_1^5, S_5^3/S_3^5)$ не меняется при циклических сдвигах вектора $\bar{e}$.

Отсюда непосредственно вытекает

Следствие 2. Для всех векторов из данной Г-орбиты вектор $N(S(\bar{e}))$ одинаков, если только он существует.

Вектор $N(S(\bar{e}))$ естественно назвать нормой синдрома $S(\bar{e})$, а также нормой Г-орбиты J, которую порождает вектор $\bar{e}$. (Отметим, что при $S_1=0$, $S_2\neq 0$ величина $N_1=\infty$; если $S_1=0$, $S_2=0$ то N не существует и т.д.).

Теорема 2. Норма синдрома в БЧХ-коде C принимает $(n+1)^2 + n + 3$ различных значений, где n – длина кодовых слов.

Теорема 3. Г-орбиты одиночных, двойных и тройных ошибок имеют попарно-различные нормы в БЧХ-коде C.

Важным свойством синдромов является их равномерное распределение по нормам в следующем смысле.

Теорема 4. Пусть I и J – две Г-орбиты векторов-ошибок с одинаковой нормой в коде С. Пусть I – полная Г-орбита (содержит n векторов) и спектр ее синдромов полный (синдромы попарно-различны) тогда для всякого вектора $\bar{f} \in J$ найдется такой вектор $\bar{e} \in I$, что их синдромы совпадают: $S(\bar{f}) = S(\bar{e})$.

Следствие. Векторы, принадлежащие Г-орбитам с различными нормами, имеют попарно различные синдромы.

Построенная теория позволяет доказать следующее утверждение.

Теорема 5. Пусть К – произвольная, но фиксированная совокупность Г-орбит векторов-ошибок с попарно-различными нормами в коде С. Если принятое сообщение содержит вектор-ошибку из К, то код С ее однозначно декодирует.

Доказательство фактически вытекает из следствия теоремы 4: синдромы всех векторов-ошибок из совокупности К попарно-различны.

Статистика ошибок в цифровых системах передачи информации показывает, что наряду со случайными ошибками малого веса вероятны зависимые ошибки типа модульных или пакетных. Для борьбы с этими ошибками разрабатываются специальные коды (например, диффузные). Естественно было бы производить совместную коррекцию совокупностей К, содержащих Кодт и классы зависимых ошибок, на отднотипных декодерах.

5. Перестановочный метод декодирования и его возможности

Классический метод коррекции двойных ошибок связан с решеним квадратных уравнений. Это достаточно трудоёмкая процедура. Использование норм синдромов позволяет предложить процедуру коррекции ошибок, удобную при использовании параллельных вычислений и имеющую потенциально большие возможности по сравнению с классическим методом. Из доказательства теоремы 3 вытекает метод декодирования ошибок, который естественно назвать норменным. Суть метода в следующем: вычислив синдром ошибок $S(\bar{x}) = S(\bar{e})$ принятого сообщения $\bar{x} = \bar{e} + \bar{y}$, где $\bar{y}$ - истинное кодовое слово, $\bar{e}$ - вектор ошибок, находим норму этого синдрома $N(S(\bar{x})) = N$. Норма N указывает Г-орбиту J, котрый принадлежит $\bar{e}$. Элементы любой Г-орбиты являются звеньями своеобразного замкнутого кольца, переходящими друг в друга под действием циклических сдвигов. Если в Г-орбите J зафиксировать один элемент $\bar{e}_J$, то сравнив синдромы $S(\bar{e})$ и $S(\bar{e}_J)$ определяем величину циклического сдвига, переводящего $\bar{e}_J$ в $\bar{e}$. Тем самым $\bar{e}$ однозначно определена .

Предложенный перестановочный метод коррекции ошибок реализуется с помощью ПЗУ или на программируемых логических матрицах (ПЛМ). Работа таких декодеров аналогична описанным в [4,5].

Реально применяемая совокупность К должна, естественно, содержать как подмножество совокупность Кодт всех Г-орбит одиночных, двойных и тройных ошибок.

Пример 2. На длине n=31 совокупность Кодт состоит из 15 классов эквивалентности двойных ошибок, 1-го одиночных n из 145 Г-орбит тройных ошибок, содержащих в общем 161*31=4991 вектор-ошибку.

Вычисления показывают, что в БЧХ-коде С над полем GF(32) с α – корнем полинома $x^5+x^3+x^2+x+1$ – все 16 Г-орбит циклических пакетов ошибок длины 4, 5, 6 имеют попарно различные нормы синдромов, отличные от норм синдромов Г-орбит из Кодт. По теореме 4 их можно объединить в одну корректируемую совокупность векторов-ошибок К.

Количество корректируемых ошибок при данном способе декодирования увеличивается примерно на 10% по сравнению с традиционными методами.

Класс Кодт содержит примерно шестую часть названного теоремой 5 количества различных ошибок. Следовательно, перестановочный метод позволяет, в принципе, корректировать большее (до 6 раз) количество векторов-ошибок по сравнению с традиционными методами декодирования.

Литература

1. Блох Э.Л., Зяблов В.В.. Линейные каскадные коды. М.: Наука, 1982, - 230 с.

2. Мак-Вильямс Ф.Дж., Слоэн Н.Дж А. Теория кодов, исправляющих ошибки. М.: Связь, 1979, -744 с.

3. Поваляев Э.И., Щербаков Н.И. Аппаратурно-ориентированный метод решения системы уравнений двоичных кодов Боуза-Чоудхури–Хоквингема для процедуры параллельной коррекции трехкратных ошибок. Автоматика и вычислительная техника, 1987, № 3, с. 66-71.

4. Липницкий В.А., Конопелько В.К. Перестановочный метод декодирования БЧХ-кодов и его возможности. 1-ая Международная конференция “Цифровая обработка сигналов и ее применения”, 30 июня – 3 июля 1998, Москва, Доклады, т.II, с. 79-86.

5. Липницкий В.А., Конопелько В.К. Перестановочный метод декодирования реверсивных кодов и его возможности. 2-ая Международная конф. “Цифровая обработка сигналов и её применения”, 21-24 сент. 1999г., Москва, Доклады, т.I, с. 158-163.

6. Виноградов И.М. Основы теории чисел. М.: Наука, 1972, -168с.

PERMUTATION DECODING OF BCH CODES WITH MINIMAL DISTANCE 7

Lipnitsky V.K., Konopelko V.K.

Belorussian State University of informatics and radioelectronics.
Belarus, 220600, s.Minsk, P. Brovka str., 6
Tel: (0172) 32-42-00, E-mail: kafsiut@gw.bsuir.unibel.by

Abstract: The theory of syndrom norms for BCH-codes with d=7 have been constructed. This norms are the invariantes of cyclical shifts group Γ, which divides the all spectrum of error-vectors into the equivalence classes that are Γ-orbits. The equivalence classes of error-vectors with weight 1, 2, 3 in these BCH-codes have a pare-vice distinct norms. This provides a new permutation method for error correcting by BCH-codes: after the syndrom of accepted message a norme is evaluated, then the error class is recieved, that gives the error-vector, generating this class, which by means of cyclic shifts is converted into desired**.**

The main obstruction for use of noise resistant codes in digital communication nets is a "selector problem" [1, 2]: the complexity of computational implementation of equation with degree t>2 solving in Galois filds (t is a multiplicity of corrected errors). We know a various methods for this problem solving [1 –3], that gives a low speed algorithms for error correcting.

In [4] a permutation method for BCH codes with d=5 decoding that allows to remove this difficulty as well as to increase the spectrum of errors decoded by this code. Below we will suggest an extension of permutation method for BCH codes with d=7.

Here the code C with a length $n=2^m-1$ that have a parity check matrix $H=(\alpha^i, \alpha^{3i}, \alpha^{5i})^T$, $0 \le i \le n-1$, is considered, where α is a primitive element of Galois field $GF(2^m)$, that is a root of fixed primitive polynomial of degree m over GF(2). This code have a minimal distance 7 and belongs to the cyclical codes class. Hence cyclical shifs group Γ is a subgroup of athe group of code C automorphisms. Under Γ- action the space of all possible error vectors is devided into the equivalence classes – Γ-orbits. They contain n vectors each other that turn off one to another under the cyclical shifs action. Sometimes Γ-orbit contain k vectors, where k is divisor od n, if it contains vectors with internal symmetry. All vectors of single Γ-orbit have a rigidly dependent to each other syndroms in the code C.

Theorem 1. Let $\bar{e}$ – error vector $\bar{e}=(e_1,\ldots,e_n)$; $\sigma(\bar{e}) = (e_n, e_1, e_2,\ldots,e_{n-1})$. Let the syndrom $S(\bar{e}) = (S_1, S_2, S_3)$. Then $S(\sigma^\lambda(\bar{e})) = (\alpha^\lambda S_1, \alpha^{3\lambda} S_2, \alpha^{5\lambda} S_3)$ for any integer λ.

Consequence 1. *(The vector $\check{N}(S(\bar{e})) = (S_2/S_1^3, S_3/S_1^5, S_5^3/S_3^5)$ is not changed under a cyclical shifs of vector $\bar{e}$.*

Thus we. have

Consequence 2 . For all vectors of given Γ-orbit the vector $N(S(\bar{e}))$ is constant, if only it exists.

Vector $N(S(\bar{e}))$ we call a norm of syndrom $S(\bar{e})$, as well as a norm of Γ-orbit J, thatis generated by vector $\bar{e}$. (Note that if $S_1=0$, $S_2\neq 0$ then the value $N_1=\infty$; if $S_1=0$, $S_2=0$ тhen N does not exist and so on).

Theorem 2. Γ-orbits of single, double and of tripple errors have pare vice distinct norms in BCH code C.

An important property of syndroms is their uniform distribution to norms in the next sence

Theorem 3. Let I and J are two Γ-orbitsof error vectors with the same norm in code C. Let I is a whole Γ-orbit (containing n vectors) and the spectrum of their syndroms is full (all syndroms are pare vice distinct). Then for any vector $f \in J$ there exists such a vector $\bar{e} \in I$ that their norms are coincide: $S(f)=S(\bar{e})$.

Corollary. All vectors belonging to Γ-orbits with distinct norms, have pare vice distinct syndroms.

The constructed theory give rise to the next statement.

Theorem 4. Let K be an arbitrary bur fixed set of Γ-orbits of error vectors with a pare vice distinct norms in the code C. If the recieved message contains error vector in K, then the code C decodes it be uniq way.

Proof follows from corollary of theorem 3: the syndroms of all error vectors in the set K are pare vice distinct.

The statistics of errors in digital systems of data transmission shows that with a random errors of little weight may be also a dependent errors like modules and bursts. For correcting of these errors one develops a special codes (for example, diffusion codes). It is naturally to do the common correction of sets K, that contain both Ksdt and dependent error classes by decoders of the same type.

A really decoded set K must contain as a subset the set Ksdt of all Γ-orbits of single, double and of tripple errors.

If the length n=31 then the set Ksdt consists from 15 equivalence classes of double errors, from one single error class and from 145 Γ-orbits of tripple errors, containing in total 161*32=4991 error vector.

The computations shows thet in BCH code C over the field GF(32) with α be the root of polynomial $x^5+x^3+x^2+x+1$ all 16 Γ-orbits of cyclic error bursts of lengts 4, 5, 6 have the pare vice distinct syndrom norms, that differ from the syndrome norms of Γ-orbits in Ksdt. Under theorem 4 we may to join them into the single correctable set of error vectors K.

The number of corrected errors by given method of decoding increases up to 10% more then by the traditional methods.

Theorem 5. A syndrom norm in BCH code of length $N=2^m-1$ admits $(n+1)^2 + n + 3$ distinct values.

The class Ksdt contains roughly a sixth part of claimed by theorem 5 number of distinct errors.

Hence a permutation method allows, in principle, to correct a biggest (up to 6 times) number of error vectors then the traditional decoding methods.

REFERENCES

1. Bloch E.L., Zjablov V.V.. Linear cascade codes (in russian). M.: Science, 1982, - 230 pp.

2. Mac-Williams F.J., Sloane N.J.A. The Theory of error correcting codes. NIIC. USA, 1997. –744pp.

3. Povaljaev E.I., Scherbakov N.I. Apparature-oriented method for solving the equation system of binary BCH codes for the procedure of parallel tripple error correcting (in russian). Automatics and computation techniquess, 1987, № 3, pp. 66-71.

4. Lipnitsky V. and Konopelko V. Permutation method of BCH codes decoding anf its capability. The 1st Int. conf. “Digital signal processing and its applications” June 30 – July 3, 1998, Moscow, Proceedings, Vol. II-E, p. 59-62.