

НОРМЕННОЕ ДЕКОДИРОВАНИЕ ПОМЕХОУСТОЙЧИВЫХ КОДОВ НА ОСНОВЕ ЦИКЛОТОМИЧЕСКИХ ПЕРЕСТАНОВОК

В.К. КОНОПЕЛЬКО, О.Г. СМОЛЯКОВА

Белорусский государственный университет информатики и радиоэлектроники

П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 11 июля 2008

Предложено норменное декодирование помехоустойчивых кодов на основе циклотомических перестановок, которое позволяет сократить количество селектируемых комбинаций в единицы-десятки раз в зависимости от длины кода и числа корректируемых ошибок, а также метод пошаговой обработки циклотомических классов, сводящий селектируемое множество к одному элементу.

Ключевые слова: БЧХ-код, проверочная матрица, синдром, норма, норменный циклокласс, норменный циклотомический класс.

В телекоммуникационных системах широко используются БЧХ-коды, которые задаются с помощью проверочной матрицы. Проверочная матрица кодов, исправляющих однократные ошибки, задается в следующем виде: $H = [d]$, двукратные — $H = [\alpha^i; \alpha^{3i}]^T$, трехкратные — $H = [\alpha^i; \alpha^{3i}; \alpha^{5i}]^T$, и t -кратные — $H = [\alpha^i; \alpha^{3i}; \alpha^{5i}; \dots; \alpha^{(2t-1)}]^T$, где α^i является элементом поля Галуа, который определяется с помощью примитивного полинома поля $g(x)$ [1]. Например, проверочная матрица H для кодов длиной $n=31$, исправляющих двукратные случайные ошибки ($t=2$), имеет вид

$$H = \begin{bmatrix} \alpha^0 \alpha^1 \alpha^2 \alpha^3 \dots \alpha^{30} \\ \alpha^0 \alpha^3 \alpha^6 \alpha^9 \dots \alpha^{28} \end{bmatrix}.$$

Процедура синдромного декодирования помехоустойчивых кодов состоит в вычислении синдрома $S = A^* \cdot H^T$, где $A^* = A + E$ — принятое слово, H^T — транспонированная проверочная матрица его селектирования для нахождения вектора ошибок E . При увеличении длины кода количество селектируемых комбинаций увеличивается и, как следствие, возрастает сложность декодирования. Так при $t=2$, $n=31, 255, 511, 1023, 2047$ число селектируемых комбинаций соответственно равно 496, 32640, 130305, 522753, 2094081. Из-за высокой сложности селектора в существующих системах связи декодирование по синдрому применяется при коррекции ошибок малой кратности ($t \leq 3$).

Предложенный в [2] метод норменного декодирования позволяет уменьшить сложность этой процедуры в n раз путем классификации векторов ошибок, разбиения их норменные циклоклассы (НЦ) и определения норм синдромов. Под норменным циклоклассом понимается группа векторов ошибок, члены которой представляют собой циклические сдвиги друг друга. Норма N синдрома S является числовым признаком, постоянным для всех синдромов векторов ошибок, которые входят в норменный циклокласс, и его идентифицирующим.

Как показано в [2] для определения группы циклических перестановок векторов ошибок БЧХ-кодов, исправляющих двойные и тройные случайные ошибки, требуется соответственно одна и три нормы, определяемые из выражений

$$N(S) = (j - 3i) \bmod n,$$

где $S = (\alpha^i \ \alpha^j)$ для кода с $d=5$ и для кода с $d=7$ $S = (\alpha^i \ \alpha^j \ \alpha^z)$, $N = (N_1, N_2, N_3)$, где $N_2(S) = (z - 5i) \bmod n$; $N_3(S) = (3z - 5j) \bmod n$.

В табл. 1 приведены значения количества норменных циклоклассов для кодов с $d=5$ и $d=7$.

Таблица 1. Количество норм, циклотомических классов и элементов циклоклассов для кодов с $d=5$ и $d=7$

Длина ко-да, N	Количество НЦ, $t=2$	Количество НЦ, $t=3$	Количество циклотомиче-ских классов	Количество элементов в циклотомическом классе
31	15	145	6	5
127	63	2625	18	7
2047	1023	697345	186	11

Анализ данных табл. 1 показывает, что, несмотря на уменьшение сложности декодирования, проблема сложности селектора остается. Применение циклотомических перестановок позволяет уменьшить число селектируемых комбинаций. Рассмотрим это подробнее.

Циклотомическими перестановками по модулю n над $GF(p)$ называется множество

$$C_S = \{s, sp, sp^2, \dots, sp^{m_s-1}\}, sp^{m_s} \equiv s \bmod n.$$

Множество целых чисел $0 \leq i \leq n-1$ разбивается на подмножество циклотомических классов. Так, для $n=31$ в поле $GF(2)$ существует шесть циклотомических классов (рис. 1).

- 1) $\{1, 2, 4, 8, 16\}$
- 2) $\{3, 6, 12, 24, 17\}$
- 3) $\{5, 10, 20, 9, 18\}$
- 4) $\{7, 14, 28, 25, 19\}$
- 5) $\{11, 22, 13, 26, 21\}$
- 6) $\{15, 30, 29, 27, 23\}$

Рис. 1 Циклотомические классы по модулю 31 над полем $GF(2)$

В [2] показано, что количество норм синдромов двойных ошибок на длине 31 равно 15. В табл. 2 приведены значения норм синдромов двойных ошибок кода на длине $n=31$ для $g(x) = x^5 + x^3 + x^2 + x + 1$.

Анализ данных табл. 2 и рис. 1 показывает, что нормы синдромов двойных ошибок БЧХ-кода принадлежат трем циклотомическим классам ($\{3, 6, 12, 24, 17\}$, $\{7, 14, 28, 25, 19\}$, $\{15, 30, 29, 27, 23\}$), полностью покрывая все множество элементов, входящих в них, и образуя норменные циклотомические классы. Для кодов с $t=2$, задаваемых иными $g(x)$, наблюдается распределение по трем, но по другим циклотомическим классам.

Количество селектируемых комбинаций можно сократить в пять раз для БЧХ-кода с $d=5$ $n=31$, по числу элементов в норменном циклотомическом классе, по сравнению с декодированием на основе норменных циклоклассов, при использовании следующего правила декодирования с применением норменных циклотомических классов и метода полихотомической обработки информации. Рассмотрим это подробнее для $t=2$.

Таблица 2. Образующие векторы двойных ошибок норменных циклоклассов и их нормы

№	$N(e_{обр})$	Вектора ошибок $e_{обр}$
1	3	11000000000000000000000000000000
2	6	10100000000000000000000000000000
3	14	10010000000000000000000000000000
4	12	10001000000000000000000000000000
5	30	10000100000000000000000000000000
6	28	10000010000000000000000000000000
7	19	10000001000000000000000000000000
8	24	10000000100000000000000000000000
9	23	10000000010000000000000000000000
10	29	10000000001000000000000000000000
11	27	10000000000100000000000000000000
12	25	10000000000010000000000000000000
13	15	10000000000001000000000000000000
14	7	10000000000000100000000000000000
15	17	10000000000000010000000000000000

Выберем образующие норменных циклотомических классов и обозначим их как $N_{a.обр}$, $N_{b.обр}$, $N_{c.обр}$. В качестве образующей норменного циклотомического класса может выступать любое число в него входящее, например, $N_{a.обр}=3$, $N_{b.обр}=7$, $N_{c.обр}=15$. Далее производятся следующие вычисления.

1. Вычисляется синдром S и норма $N_{выч}$ принятого слова.

2. Сравнивается вычисленная норма $N_{выч}$ с каждой из образующих $N_{a.обр}$, $N_{b.обр}$, $N_{c.обр}$; совпадение нормы $N_{выч}$ с одним из значений $N_{a.обр}$, $N_{b.обр}$, $N_{c.обр}$ указывает на циклотомический класс, в котором находится вычисленная норма.

3. Если $N_{выч}$ не совпадает ни с одним из значений $N_{a.обр}$, $N_{b.обр}$, $N_{c.обр}$, то осуществляется циклотомический сдвиг нормы и происходит сравнение $N_{выч}$ с образующими норменными циклотомическими классами.

4. Определяется циклотомический класс, к которому принадлежит норма $N_{выч}$. По числу совершенных сдвигов определяется значение нормы $N_{выч}=N_{сдв}$; по таблице истинности находится соответствующий ей образующий вектор ошибки $E_{обр}$.

5. По вычисленному синдрому S и с учетом $N_{выч}$ и $E_{обр}$ вычисляется текущий вектор ошибок [2].

Алгоритм декодирования представлен на рис. 2, где $N_{обр}$ — образующая определенного норменного циклотомического класса, F_1 — функция вычисления исходного значения $N_{выч}$, F_2 — функция вычисления образующего вектора ошибок $E_{обр}$, F_3 — функция вычисления текущего вектора ошибок.

Видно, что количество селектируемых комбинаций уменьшается до числа норменных циклотомических классов без учета неиспользуемых норменных циклотомических классов. Если через $z=5$ сдвигов вычисленной нормы $N_{выч}$ циклотомический класс, которому она принадлежит, не найден, то это означает, что произошла некорректируемая нашим кодом ошибка. В [2] показано, что это свойство можно использовать для коррекции некоторых ошибок большей кратности.

Увеличение числа корректируемых ошибок до $t=3$ для кодов длиной $n=31$ приводит к увеличению числа норменных циклоклассов: 145 — для тройных ошибок, 15 — для двойных, а число норменных циклотомических классов составляет 29 и 3 соответственно (табл. 3).

Рассмотрим применение циклотомических классов для кодов с $d=7$ и $n=31$. Для этого выберем образующие норменных циклотомических классов и обозначим их как $N_{обр}^i = (N_{1..обр}^i, N_{2..обр}^i, N_{3..обр}^i)$, $i = \overline{1, 32}$, например, $N_{обр}^1 = (3, 30, 13)$, $N_{обр}^2 = (11, 13, 15)$ и т.д. Количество селектируемых комбинаций также можно сократить в пять раз, если для кодов, исправляющих тройные случайные ошибки, использовать правило, аналогичное применяемому для кодов с $d=5$. В этом случае вычисленная норма имеет вид $N_{выч} = (N_{1..выч}, N_{2..выч}, N_{3..выч})$; равенство

$N_{выч}$ и $N_{обр}^i$ определяется выражениями $N_{1..выч} = N_{1..обр}^i$, $N_{2..выч} = N_{2..обр}^i$, $N_{3..выч} = N_{3..обр}^i$, $i = \overline{1, 32}$, а циклотомический сдвиг нормы означает циклотомический сдвиг каждой из ее компонент $N_{1..выч}$,

$N_{2.\text{выч}}$, $N_{3.\text{выч}}$. Например, если $N_{\text{выч}} = (24, 12, 9)$, то циклотомический сдвиг значения приводит к $N'_{\text{выч}} = (17, 24, 18)$.

Для кодов длиной $n=127$ и 2047 при $t=2$ количество селектируемых комбинаций уменьшается в 7 и 11 раз (по числу элементов в циклотомическом классе) (табл. 1), однако в этом случае увеличивается число используемых норменных циклотомических классов до 9 и 93 соответственно, что приводит к росту сложности селектора.

Сложность декодирования при использовании норменных циклотомических классов можно уменьшить, применяя правило декодирования на основе метода пошаговой обработки норменных циклотомических классов. Рассмотрим этот метод на примере кода с $n=31$, $t=2$.

Выражение $N_{c.\text{обр}} = (N_{b.\text{обр}} - \Delta) \bmod n = (N_{a.\text{обр}} - 2\Delta) \bmod n$ определяет правило перехода из одного циклотомического класса в другой, Δ — число. Выберем в качестве образующей трех норменных циклотомических классов один из элементов в них входящих и обозначим его как $N_{\text{обр}}$. Тогда правило декодирования с пошаговой обработкой норменных циклотомических классов может осуществляться следующим образом.




Рис. 2. Алгоритм декодирования кодов $n=31$, $t=2$ на основе циклотомических классов

Таблица 3. Норменные циклотомические классы кода с $d=7$

1. Вычисляется синдром S и норма $N_{выч}$ принятого слова.
 2. Выбираем $N_{обр} = N_{a.обр}$.
 3. Сравниваем норму $N_{выч} = N_{обр}$ (совпадение нормы $N_{выч}$ со значением $N_{обр}$ указывает на циклотомический класс, в котором находится вычисленная норма).
 4. Если $N_{выч}$ не совпадает со значением $N_{обр}$, то осуществляется циклотомический сдвиг нормы и происходит сравнение $N_{выч}$ с образующей $N_{обр}$.
 5. Если $N_{выч}$ не совпадает ни с одним элементом циклотомического класса, то значение образующей норменного циклотомического класса $N_{обр}$ увеличивается на Δ и происходит сравнение $N_{выч}$ с $N_{обр}$.
 6. Определяется циклотомический класс, к которому принадлежит норма $N_{выч}$. По числу совершенных сдвигов определяется значение нормы $N_{выч} = N_{сдв}$; по таблице истинности находится соответствующий ей образующий вектор ошибки $E_{обр}$.
 7. По вычисленному синдрому S и с учетом $N_{выч}$ и $E_{обр}$ вычисляется текущий вектор ошибок [2].

Значение Δ выбирается в зависимости от используемых кодом норменных циклотомических классов и осуществляется по модулю n (табл. 4).

Таблица 4. Значение величины Δ для кодов с $d=5$

Используемые норменные циклотомические классы	Δ	$N_{a.\text{обр}}$	$N_{b.\text{обр}}$	$N_{c.\text{обр}}$
{1,2,4,8,16}{3,6,12,24,17}{5,10,20,9,18}	1	16	17	18
{1,2,4,8,16}{3,6,12,24,17}{7,14,28,25,19}	1	6	7	8
{1,2,4,8,16}{3,6,12,24,17}{11,22,13,26,21}	5	6	11	16
{1,2,4,8,16}{3,6,12,24,17}{15,30,29,27,23}	1	15	16	17
{3,6,12,24,17}{5,10,20,9,18}{7,14,28,25,19}	1	17	18	19
{3,6,12,24,17}{5,10,20,9,18}{11,22,13,26,21}	1	10	11	12
{3,6,12,24,17}{5,10,20,9,18}{15,30,29,27,23}	19	10	29	17
{5,10,20,9,18}{7,14,28,25,19}{11,22,13,26,21}	1	19	20	21
{5,10,20,9,18}{7,14,28,25,19}{15,30,29,27,23}	5	20	25	30
{7,14,28,25,19}{11,22,13,26,21}{15,30,29,27,23}	1	13	14	15
{1,2,4,8,16}{3,6,12,24,17}{11,22,13,26,21}	18	16	3	21
{3,6,12,24,17}{5,10,20,9,18}{15,30,29,27,23}	3	12	15	18
{5,10,20,9,18}{7,14,28,25,19}{15,30,29,27,23}	9	5	14	23
{1,2,4,8,16}{5,10,20,9,18}{7,14,28,25,19}	2	14	16	18
{1,2,4,8,16}{5,10,20,9,18}{11,22,13,26,21}	20	5	26	16
{1,2,4,8,16}{5,10,20,9,18}{15,30,29,27,23}	20	27	16	5
{1,2,4,8,16}{7,14,28,25,19}{11,22,13,26,21}	3	16	19	22
{1,2,4,8,16}{7,14,28,25,19}{15,30,29,27,23}	1	14	15	16
{1,2,4,8,16}{11,22,13,26,21}{15,30,29,27,23}	18	11	29	16

Из табл. 4 видно, что число селектируемых комбинаций сокращается до одной. Алгоритм декодирования по этому правилу представлен на рис. 3.

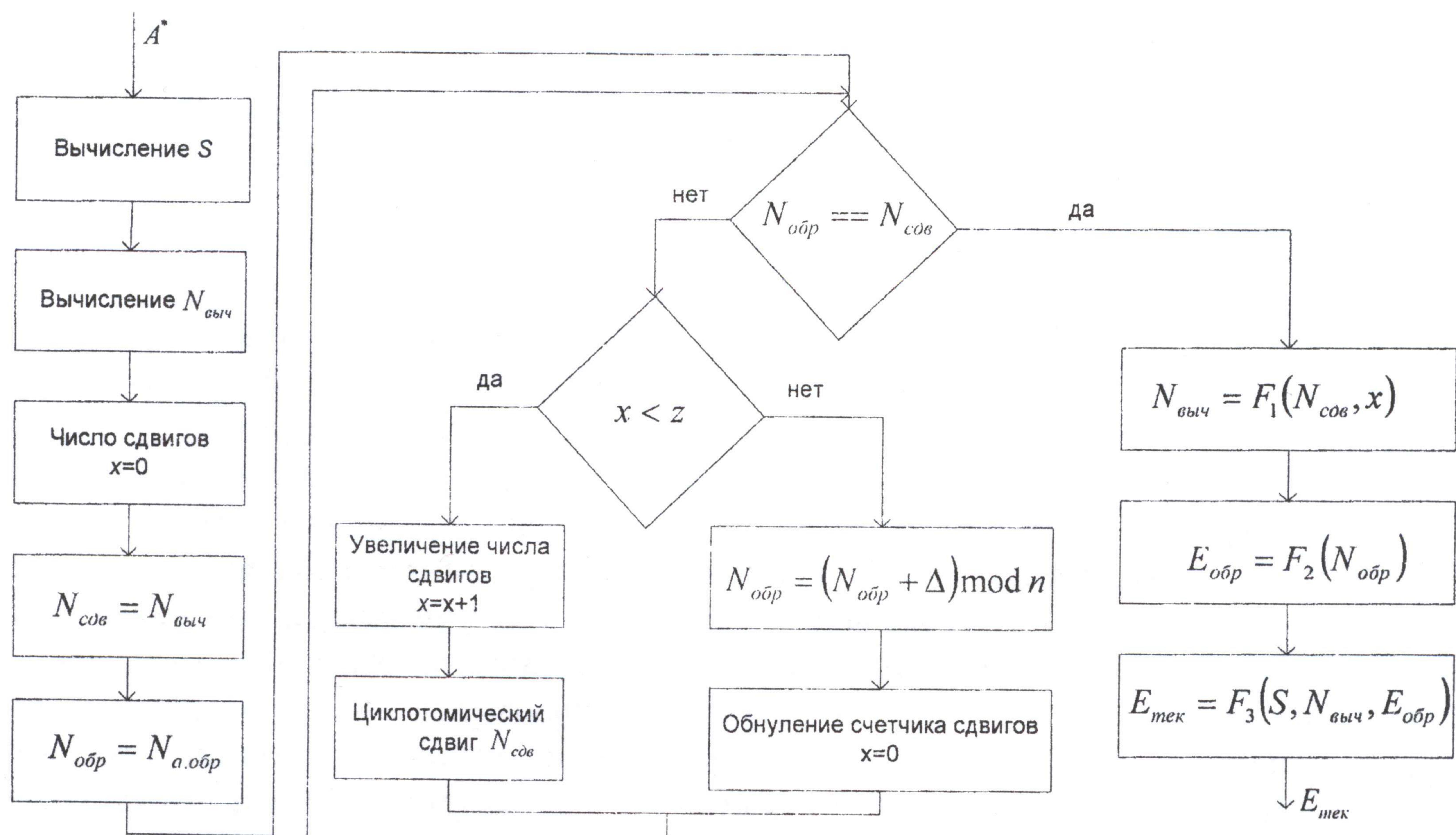


Рис. 3. Алгоритм декодирования на основе пошаговой обработки норменных циклотомических классов кодов с $d=5$, $n=31$

Аналогичным образом может происходить декодирование БЧХ-кодов с большими значениями n и t , благодаря чему число селектируемых комбинаций сводится к одной.

Сложность норменного декодирования высока из-за экспоненциального роста циклотомических классов при увеличении длины кода и числа исправляемых ошибок. Проведенный анализ показал, что использование правила декодирования с применением циклотомических классов и полихотомической обработки информации позволяет сократить количество селектируемых комбинаций в число раз, равное количеству элементов в циклотомическом классе. Показано, что рост сложности декодирования при увеличении значений n и t , приводящий к росту числа циклотомических классов, можно уменьшить до одного за счет перехода от одного циклотомического класса к другому путем соответствующего изменения образующих циклотомических классов.

NORMING DECODING OF NOISEPROOF CODES ON A BASIS CYCLOTOMIC SHIFTS

V.K. KONOPELKO, O.G. SMOLYAKOVA

Abstract

It is offered norming decoding noiseproof of codes on a basis cyclotomic shifts which allows reducing quantity of determinated combinations in units-tens times depending on length of a code and number of corrected errors, and also a method of step-by-step processing the cyclotomic classes, reducing determinated set to one element.

Литература

1. Конопелько В.К., Липницкий В.А., Дворников В.Д. и др. Теория прикладного кодирования / Под ред. В.К. Конопелько. Минск, 2004. Т. 2.
2. Конопелько В.К., Липницкий В.А. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Минск, 2000.