УДК 621.391.(075.8)

ТЕОРИЯ НОРМ СИНДРОМОВ В ПЕРЕСТАНОВОЧНОМ ДЕКОДИРОВАНИИ ПОМЕХОУСТОЙЧИВЫХ КОДОВ

В.К. КОНОПЕЛЬКО, В.А. ЛИПНИЦКИЙ

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

Поступила в редакцию 19 ноября 2003

Излагаются основные моменты теории норм синдромов — нового направления в перестановочном декодировании помехоустойчивых кодов. Нормы синдромов — инварианты группы циклических сдвигов — разбивают слова-ошибки на непересекающиеся классы, являются идентификаторами этих классов, позволяют существенно сократить вычислительные затраты при декодировании ошибок (что является новым решением проблемы селектора), расширить спектр декодируемых ошибок.

Ключевые слова: помехоустойчивые коды, идентификаторы, декодирование ошибок.

Введение

Помехоустойчивое кодирование является одним из основных методов при передаче, хранении, обработке и распределении информации в современных телекоммуникационных системах и сетях. Волоконно-оптические телекоммуникационные системы можно отнести к разряду идеальных (одна ошибка на несколько десятков минут [1,2]), однако они дороги и относятся к разряду стационарных систем. Телекоммуникационные системы с обратной связью, сущность которой заключается в повторной передаче ошибочно принятых блоков информации, относятся к почтовому типу, где фактор времени не является превалирующим. К названным нельзя отнести постоянно растущее многообразие телекоммуникационных систем – сотовая, пейджинговая, цифровые телевидение и телефон, космическая связь и т.п. Их функционирование базируется на синхронном исправлении возникающих ошибок с помощью помехоустойчивых кодов.

К настоящему времени разработан широкий спектр разнообразных кодов и методов их обработки. Однако на практике реализованы лишь некоторые из них, рассчитанные, как правило, на коррекцию ошибок кратностью $t = 1, 2,$ а также пакетных и модульных ошибок. Это объясняется известной проблемой "селектора", имеющей комбинаторную природу.

Синдромные методы декодирования относятся к числу наиболее популярных в обработке помехоустойчивых кодов. Синдром принятого слова получается умножением принятого слова на проверочную матрицу кода. Синдром однозначно соответствует допущенному вектору-ошибке $\overline{e}$. Код длиной 31, декодирующий двойные ошибки, должен селектировать 496 различных синдромов и соответствующих ошибок. При $n = 127$ и $t = 3$ количество обрабатываемых синдромов вырастает до величины 341 503. Проблема селектора заключается в сложности обработки экспоненциально растущего количества синдромов с увеличением кратности обрабатываемых ошибок и длины кода.

Следует отметить, что проблема селектора имеет более широкое значение — являясь препятствием в защите информации от помех, в то же время служит защите информации от несанкционированного доступа. Недавние исследования показали, что данной проблемой объясняется сложность раскрытия различных криптотекстов [3].

Для решения проблемы "селектора" теория и практика помехоустойчивого кодирования пошли по пути создания сложных кодов — кодов-произведений, итеративных кодов, декодирование которых производится поэтапно, что, однако, приводит к большой избыточности, т.е. большому числу проверочных разрядов. Например, при кратности $t = 4$ использование этих алгоритмов на $1/3$ увеличивает количество проверочных разрядов по сравнению с БЧХ-кодом с аналогичными множеством корректируемых ошибок и числом информационных разрядов. Многоступенчатая система декодирования этих кодов, кроме того, не всегда применима из-за низкой скорости обработки этих кодов.

Кроме того, известные методы обработки кодов не используют полностью все их возможности, т.е. остается большое число неиспользованных синдромов. Например, при $n = 127,\ t = 3$ количество проверочных разрядов равно 21, следовательно, количество синдромов равно $2^{21} = 2\,097\,152,$ а используется лишь 341503 синдромов, т.е. примерно 1/7 их часть. Таким образом, существует проблема использования избыточности синдромов для контроля других типов ошибок (например, модульных и пакетных).

В теории кодирования выработалось мнение о том, что перестановочные методы обработки кодов перспективны для снижения сложности декодирования [4]. Однако усилия здесь сконцентрировались вокруг идеи перестановки ошибочных разрядов из информационной части в проверочную, что дает возможность по весу синдрома определить это состояние. Данный путь оказался весьма трудоемким и не принес ожидаемых результатов из-за необходимости поиска конкретных подстановок для каждого вектора ошибок.

Таким образом, в теории и практике помехоустойчивого кодирования приобрели актуальность следующие задачи:

1) проблема сложности "селектора";

2) разработка методов коррекции, позволяющих использовать избыточность синдромов для исправления ошибок выше корректирующей способности кодов;

3) разработка новых подходов к реализации перестановочных методов декодирования кодов.

2. Основные положения теории норм синдромов

Теория норм синдромов позволяет решить перечисленные выше задачи, провести исследования по вопросам классификации векторов-ошибок с помощью действия различных групп подстановок (циклических, циклотомических, аффинных), дать описание соответствующих классов эквивалентности и их структуры; исследовать спектры синдромов Г-орбит и G-орбит векторов-ошибок для группы Г-циклических сдвигов и группы G-циклических и циклотомических подстановок; найти кодовые инварианты групп циклических сдвигов — нормы синдромов, развить их теорию в кодах Боуза-Чоудхури-Хоквингема (БЧХ-кодах), в реверсивных кодах, кодах Рида-Соломона (РС-кодах); разработать перестановочные методы декодирования названных кодов и их модификаций на основе построенной теории норм синдромов. Норменные методы обладают умеренными вычислительными затратами, благодаря перебору селектором блоков — орбит ошибок, а не отдельных ошибок, позволяют корректировать расширенные (по сравнению с традиционными синдромными методами) спектры ошибок без усложнения алгоритма декодирования, допускают реализацию декодеров на современной элементной базе (ПЛМ, ПЛИС).

Классификация векторов-ошибок – это разбиение их на непересекающиеся классы, объединяемые по какому-то естественному признаку. Группа циклических сдвигов Г на пространстве *n*-мерных векторов состоит из степеней подстановки σ, действующей на каждый вектор по правилу: первая координата ставится на место второй, 2-я на место третьей и так далее, наконец, последняя координата переставляется по циклу на место первой.

Г-орбитой $<\bar{e}>$, порожденной вектором $\bar{e}$, называется множество всех попарно различных векторов-ошибок, получаемых при действии на вектор ē всех подстановок группы Г.

Установлены следующие основные свойства Г-орбит [5].

1. Каждая Г-орбита содержит либо n векторов (полная Г-орбита), либо λ векторов, где λ делит n (неполная Г-орбита), где n — длина кода.

2. Г-орбиты либо совпадают, либо не пересекаются.

3. Каждая Г-орбита имеет циклическую структуру: по одному из представителей Г-орбиты циклическими сдвигами легко получить все остальные (рис.1).

4. Номера ненулевых координат векторов неполных Г-орбит образуют периодическую последовательность (рис. 1).

5. Полные Г-орбиты составляют основную часть всех Г-орбит.

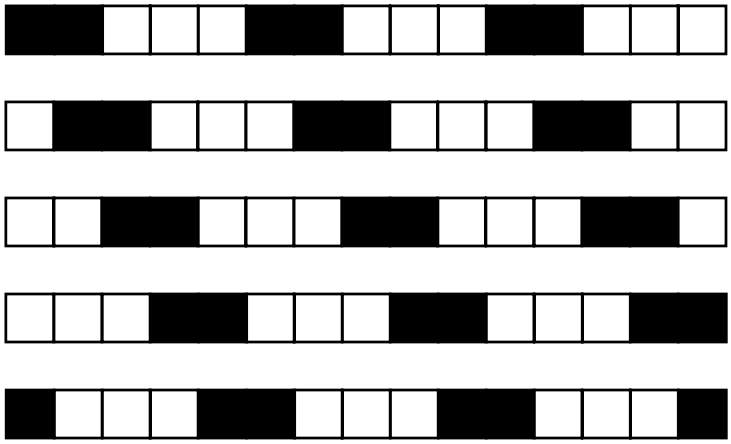

Рис. 1. Схематическое изображение неполной Г-орбиты $<\bar{e}>$ мощностью 5, порожденной вектором $\bar{e} = (110001100011000)$ в 15-мерном двоичном пространстве

Таким образом, группа циклических сдвигов Г обеспечивает разбиение пространства двоичных векторов длиной n (с n координатами) на непересекающиеся блоки – Г-орбиты – примерно по n векторов в каждом. Разбиение на более крупные классы получается применением группы G циклических и циклотомических подстановок. Циклотомические подстановки есть степени подстановки φ, порожденной автоморфизмом Фробениуса поля Галуа $GF(2^m)$. Под действием автоморфизма Фробениуса удваиваются показатели элементов этого поля. Если координаты векторов нумеровать числами 0,1, 2, …, и так далее, то подстановка φ каждую i-ю координату переставляет на место координаты с номером $2i$ по модулю n.

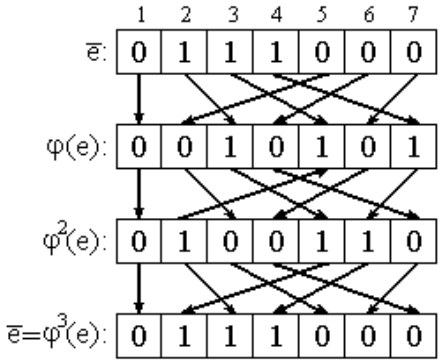

Рис. 2. Действие циклотомической подстановки φ и ее степеней на 7-мерном двоичном пространстве, в частности, на вектор $\bar{e} = (0111000)$

Группа *G* и ее орбиты обладают следующими свойствами [5].

1. Циклическая группа, порожденная степенями подстановки φ, состоит из m элементов, где *m* — наименьшее натуральное число с условием: $2^m - 1$ делится на длину кода *n* (существование которого обеспечено малой теоремой Ферма).

2. Циклотомические подстановки преобразуют Г-орбиты в Г-орбиты.

3. $\varphi\sigma = \sigma^2\varphi$.

4. Порядок группы G равен *mn*.

5. G-орбита $<\bar{e}>_G$, порожденная вектором $\bar{e}$, состоит из всех Г-орбит, получаемых действием циклотомических подстановок на Г-орбиту $<\bar{e}>$, состоит из μ Г-орбит, где μ делит *m* или совпадает с m.

6. Основную часть G-орбит составляют полные G-орбиты, содержащие по *mn* элементов.

Применение циклических и циклотомических подстановок объясняется тем, что они являются автоморфизмами многих линейных кодов.

Спектры синдромов Г-орбит и G-орбит ошибок исследованы в классе произвольных БЧХ-кодов, относящихся к разряду наиболее популярных в теории и практике кодов. Для кодирования обычно используют проверочные матрицы кодов в систематической форме. В [6] дано описание спектра проверочных матриц произвольного линейного кода, а также эквивалентных кодов, установлена взаимосвязь между этими матрицами. Данный факт позволяет для декодирования использовать другие проверочные матрицы. В дальнейшем предполагаем, что БЧХ-коды заданы однородными проверочными матрицами H вида [4]

$$H=\left[\begin{array}{ccc:c} 1 & \beta^{b} & \beta^{2b} & \beta^{(n-1)b} \\ 1 & \beta^{b+1} & \beta^{2(b+1)} & \beta^{(n-1)(b+1)} \\ \hdashline 1 & \beta^{b+\delta-2} & \beta^{2(b+\delta-2)} & \beta^{(n-1)(b+\delta-2)} \end{array}\right] = [\beta^{bi},\beta^{(b+1)i},...,\beta^{(b+\delta-2)i}]^T, \quad (1)$$

где $n-$ длина кода; $\beta-$ примитивный корень $n-$й степени из 1 в поле Галуа $GF(q^m)$ для наименьшего m с условием: $q^m - 1$ делится на n, $q-$ простое число, $b-$ целое число, $\delta-$ конструктивное расстояние, истинное кодовое расстояние $d \geq \delta$. Каждый элемент матрицы H есть двоичный столбец с m координатами — двоичный вектор, представляющий соответствующий элемент поля Галуа $GF(q^m)$ элементов в базисе $1, \beta, ..., \beta^{m-1}$. В соответствии со структурой матрицы H синдром произвольного вектора ошибок $\bar{e}$ можно интерпретировать как вектор $S(\bar{e}) = \bar{e}H^{\mathrm{T}} = (s_1, s_2, ..., s_{\delta-1})$ с компонентами $s_1, s_2, ..., s_{\delta-1} \in GF(q^m)$.

При $n = q^m - 1$ БЧХ-код называют примитивным, поскольку в этом случае $\beta = \alpha -$ примитивный элемент поля Галуа из q^m элементов. Для двоичных БЧХ-кодов $(q = 2,\ b = 1)$ прове-

рочная матрица, благодаря сопряженности элементов поля Галуа и их квадратов, имеет более простую структуру:

$$H = [\alpha^i, \alpha^{3i}, ..., \alpha^{(2i-1)i}]^T, \quad 0 \le i \le n-1, \tag{2}$$

одинаковую для значений $\delta = 2t$ и $\delta = 2t+1$. Данные коды обозначаем через C_{2t+1}. Теорема 1 устанавливает, как под действием циклической подстановки и ее степеней на вектор ошибок изменятся синдромы этих векторов в БЧХ-кодах.

Теорема 1. *Пусть* $\bar{e}$ *— произвольный вектор ошибок в БЧХ-коде* C *с проверочной матрицей (3.1). Пусть* $S(\bar{e}) = (s_1, s_2, ..., s_{\delta-1})$ *— синдром вектора* $\bar{e}$. *Тогда* $S(\sigma(\bar{e})) = (\beta^b s_1, \beta^{b+1} s_2, ..., \beta^{b+i-1} s_i, ..., \beta^{b+\delta-2} s_{\delta-1})$.

Для кода C_{2t+1} $S(\sigma(\bar{e})) = (\beta s_1, \beta^3 s_2, ..., \beta^{2i-1} s_i, ..., \beta^{2t-1} s_t)$.

Из теоремы 1 следуют основные свойства спектров синдромов орбит ошибок.

1. Спектры синдромов Г-орбит, как правило, являются полными, т.е. содержат столько же синдромов, сколько Г-орбиты содержат векторов-ошибок.

2. Спектры синдромов Г-орбит имеют циклическую структуру, адекватную структуре самих Г-орбит (рис. 3).

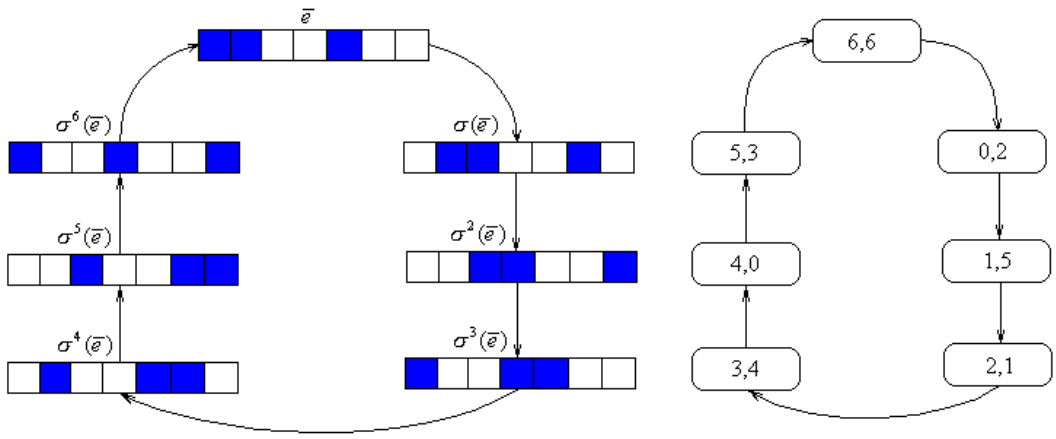

Рис. 3. Взаимно-однозначная зависимость между циклическими сдвигами векторов Г-орбиты $<\bar{e}>=<(1,2,5)>$ в 7-мерном пространстве и соответствующими преобразованиями показателей компонент синдромов в БЧХ-коде C_5

Вычисления показывают, что при действии циклотомической подстановки φ на вектор ошибок компоненты его синдрома возводятся в квадрат как элементы поля Галуа. Отсюда выводится, что спектр синдромов G-орбит также имеет структуру, взаимно однозначно соответствующую структуре самой G-орбиты (рис. 4).

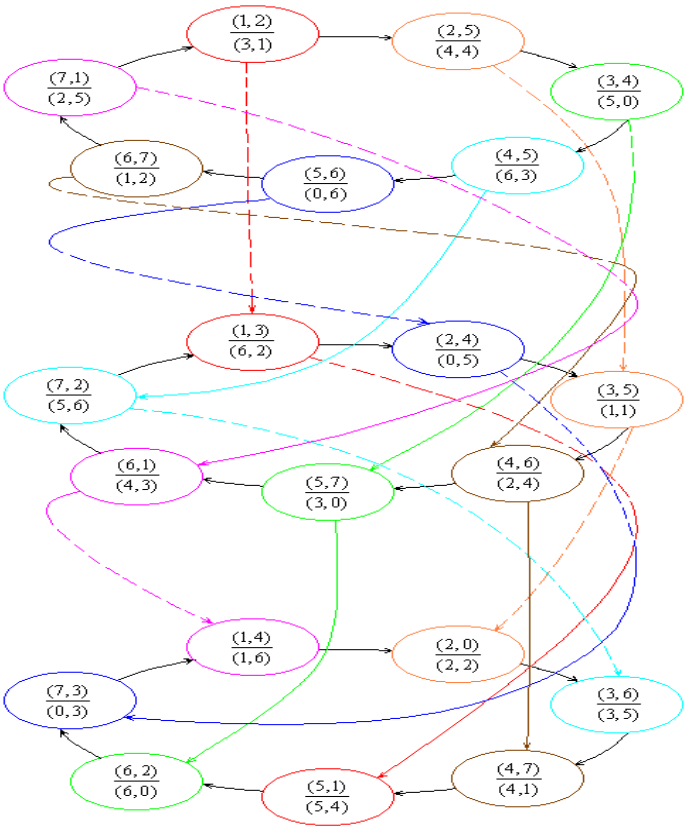

Рис. 4. Структура G-орбиты $<(1,2)>_G$ и спектра ее синдромов в коде C_5 длиной 7

Здесь (рис. 4) знаменатели дробей есть показатели компонент синдрома в БЧХ-коде C_5 с $n=7,\ d=5.$ В силу теоремы 1 эти показатели преобразуются в полном согласии с подстановками группы G.

Понятие нормы синдрома выкристаллизовывалось постепенно [7 – 17]. Для произвольных БЧХ-кодов его определение выглядит следующим образом [16].

Нормой синдрома $S(\bar{e})$ *вектора ошибок* $\bar{e}$ *в БЧХ-коде С с проверочной матрицей (1) называется вектор* $\bar{N}$ *с* $C_{\delta-1}^2$ *координатами* N_{ij}, *которые вычисляются по*

формулам $N_{ij}=s_j^{(b+i-1)/h_{ij}}/s_i^{(b+j-1)/h_{ij}}$, *если* $s_i\neq 0$;

$N_{ij}=\infty$, *если* $s_j\neq 0,\ s_i=0;\ N_{ij}=-$ *(не существует), если* $s_i=s_j=0$.

В двоичных БЧХ-кодах формулы для координат нормы синдрома имеют аналогичную форму [5], но количество координат меньше — C_t^2.

Установлены следующие основные свойства норм синдромов.

1. Циклические сдвиги векторов-ошибок их нормы синдрома не меняют.

2. Если в коде C_{2t+1} у вектора-ошибки $\bar{e}$ первая компонента синдрома $s_1\neq 0$, то все координаты нормы $\bar{N}(S(\bar{e}))$ определяются первыми $t-1$ координатами этой нормы $N_{ij}=\left(N_{1j}\right)^{\frac{2i-1}{h_{ij}}}\Big/\left(N_{1i}\right)^{\frac{2j-1}{h_{ij}}}$.

3. Все векторы каждой Г-орбиты J имеют одинаковую норму. Ее будем называть нормой Г-орбиты и обозначать $\bar{N}(J)$. Это однозначная характеристика – идентификатор, метка каждой Г-орбиты.

4. Спектры синдромов Г-орбит с различными нормами не пересекаются.

5. В двоичном БЧХ-коде с минимальным расстоянием $d = 3t + 1$ количества всех синдромов $(n+1)^t$ и норм синдромов связаны соотношением $n(K_t - 1) + 1 = (n+1)^t.$,

$$K_t = (n+1)^{t-1} + (n+1)^{t-2} + \ldots + (n+1)^2 + (n+1) + 2 = K_{t-1} + (n+1)^{t-1}.$$

6. В примитивном коде C_{2t+1} все синдромы равномерно (по *n* значений) распределяются по значениям норм, кроме нормы $\bar{N} = (-,-,\ldots,-) = \bar{N}(S(\bar{0}))$.

7. Полные Г-орбиты векторов-ошибок с одинаковыми нормами имеют и одинаковые спектры синдромов при условии их полноты.

8. При действии циклотомической подстановки φ на вектор ошибок каждая из координат его нормы синдрома возводится в квадрат.

Теорема 2 (основная теорема теории норм синдромов). *БЧХ-код может декодировать любой вектор ошибок из любой совокупности К Г-орбит ошибок с попарно-различными нормами (спектрами синдромов).*

Совокупность ошибок, допустимых кодовым расстоянием и традиционно декодируемых синдромными методами, удовлетворяет условиям основной теоремы. Но запас норм синдромов существенно больший. Поэтому имеется конструктивная возможность добавлять к названной совокупности другие Г-орбиты и G-орбиты ошибок с отличными нормами. Некоторые из таких возможностей отражает теорема 3

Теорема 3. *Если примитивный элемент* $\alpha \in \mathrm{GF}(2^m)$ *не является корнем полиномов* $x^6 + x^5 + x^2 + x + 1$, $x^6 + x^5 + x^4 + x + 1$ *и равны 1 следы элементов* $\gamma_1 = \dfrac{(\alpha+1)^4 \alpha}{(\alpha^2+\alpha+1)^3}$;

$\gamma_2 = \dfrac{(\alpha+1)^4 \alpha(\alpha^2+\alpha+1)}{(\alpha^3+\alpha^2+1)^3}$; $\gamma_3 = \dfrac{\alpha^2(\alpha+1)^4(\alpha^2+\alpha+1)}{(\alpha^3+\alpha^2+1)^3}$; $\gamma_4 = \dfrac{\alpha(\alpha+1)^2(\alpha^5+1)}{(\alpha^3+\alpha^2+\alpha+1)^3}$, *то код* C_5 *над полем* $GF(2^m)$ *может корректировать наряду с двойными ошибками любой пакет ошибок длиной четыре.*

Суть теоремы в том, что при определенных условиях на примитивный элемент поля Галуа БЧХ-код C_5 с проверочной матрицей, определяемой найденным примитивным элементом, может корректировать наряду с двойными ошибками любой пакет ошибок длиной четыре. Уже на длине 31 такие коды существуют (БЧХ-коды длиной 31 используются, в частности, в сотовой и пейджинговой связи). Подобные расширения можно проводить вплоть до исчерпания всего потенциала синдромов в коде.

Аналогичная теория построена для реверсивных кодов [18-19]. Они задаются проверочными матрицами $H = (\alpha^i, \alpha^{-i})^T, 0 \le i \le n-1.$ Здесь $n = 2^m - 1$, $\alpha -$ примитивный элемент поля $GF(2^m)$. В реверсивном коде синдром $S(\bar{e})$ любого вектора ошибок $\bar{e}$ состоит из двух компонент: $S(\bar{e}) = (s_1, s_2)$, а норма синдрома $N(S(\bar{e})) = s_1 \cdot s_2$ и является скалярной величиной.

Из разработанной теории норм синдромов следуют новые методы коррекции ошибок [20-22]. Их обобщенная схема выглядит следующим образом: по вычисленному синдрому находится его норма, норма определяет Г-орбиту, которой принадлежит искомый вектор-ошибка. По норме и синдрому определяется величина циклического сдвига образующего Г-орбиту вектора для получения искомого вектора ошибок.

Принципиальная новизна норменных методов и декодеров на их основе заключается в следующем:

1) селектируются не отдельные синдромы и ошибки, а нормы синдромов и, следовательно, Г-орбиты ошибок;

2) внутри найденной Г-орбиты координаты искомого вектора ошибок находятся не перебором, а непосредственными вычислениями с учетом установленной взаимосвязи между синдромами и векторами ошибок;

3) имеется конструктивная возможность декодировать расширенные множества векторов-ошибок добавлением Г-орбит ошибок с отличными нормами в соответствии с основной теоремой.

На рис. 5 предложены структурные схемы норменных декодеров с использованием ПЗУ и сумматоров по модулю n для коррекции двойных и тройных ошибок. В отличие от традиции переход от двойных ошибок к тройным отражается только на росте аппаратурной сложности декодера примерно в полтора раза.

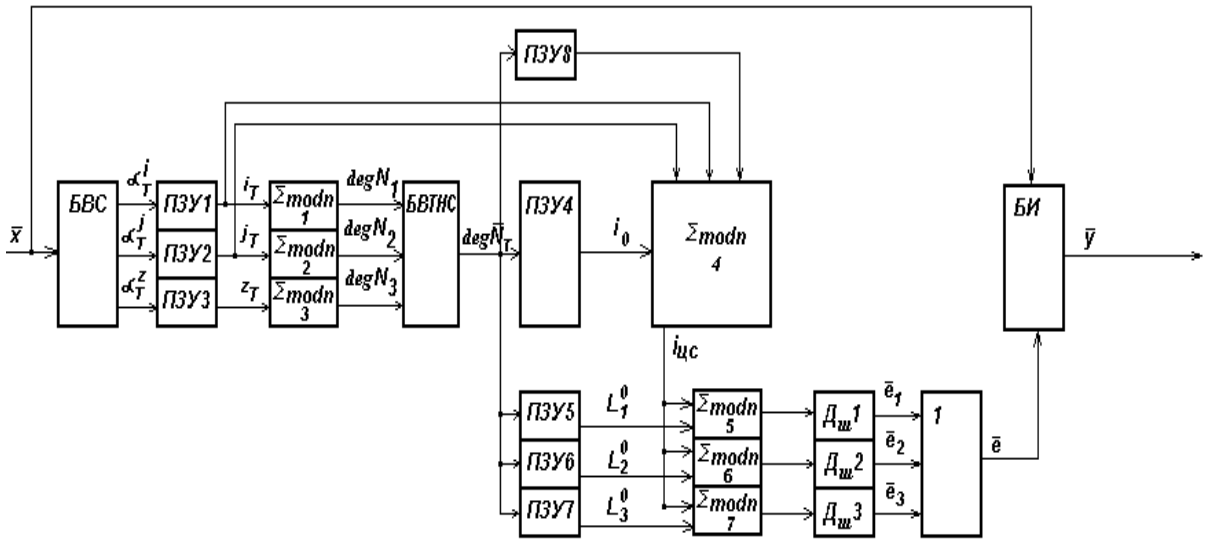

Рис. 5. Структурная схема декодера, использующего ПЗУ для хранения кодов ошибок образующего вектора при $t = 3$

Норменные методы коррекции ошибок в n раз снижают вычислительные затраты по сравнению с традиционными синдромными методами. Однако множество норм все же велико. Разработан метод сжатия норм синдромов [23] путем преобразования декодируемых ошибок в ошибки большего веса, но с синдромами, имеющими нулевые компоненты. Такие векторы имеют ограниченный спектр значений норм синдромов, что в n раз сокращает селекцию норм синдромов и в n^2 раз - вычислительные затраты на коррекцию ошибок, снижающий эти затраты в n^2 раз. Таким образом достигается предельно возможный эффект сжатия норм синдромов в силу равномерности распределения синдромов по нормам.

Теория норм синдромов для кодов Рида-Соломона

Теория норм синдромов развита на коды Рида-Соломона (РС-коды). Это БЧХ-коды над полем $GF(q)$ длиной $n = q - 1$. Это $q-$ичные, а не двоичные коды. Ошибок здесь в $n = q - 1$ раз больше (таблица).

Разработана классификация ошибок с помощью А-групп, состоящих из циклических сдвигов и гомотетий — умножений f_γ на произвольные элементы γ поля Галуа — поля определения РС-кода. А-орбиты состоят из n Г-орбит (рис. 6).

Количество ошибок весом 1–3 и их Г-орбит в РС-кодах на различных длинах

q		$8 = 2^3$	$16 = 2^4$	$32 = 2^5$	$64 = 2^6$
Длина кода N		7	15	31	63
$\omega = 1$	Кол-во ошибок	49	225	961	3969
	Кол-во Г-рбит	7	15	31	63

$\omega = 2$	Кол-во ошибок	1029	23625	446865	5250987
	Кол-во Г-рбит	147	1575	14415	83349
$\omega = 3$	Кол-во ошибок	12005	1535625	133910545	10255177611
	Кол-во Г-рбит	1715	102385	4319695	162780639

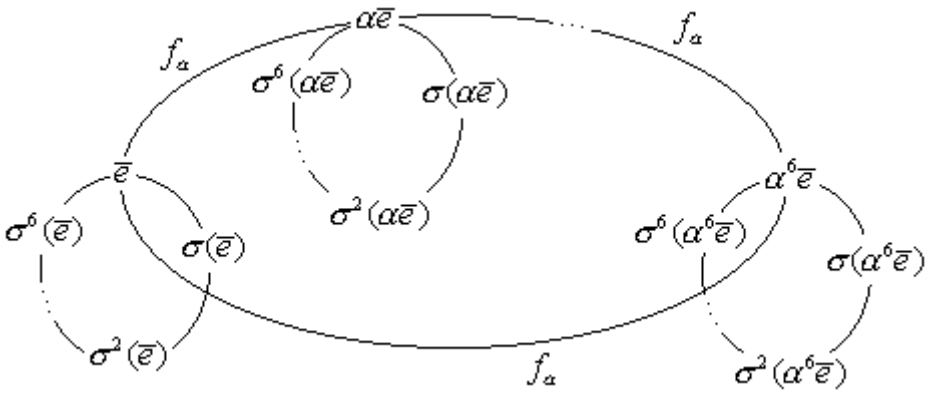

Рис. 6. Схема полной $A-$орбиты в РС-коде длиной 7

Основные факты теории норм синдромов, приведенные выше, справедливы для РС-кодов. Отметим отличительные особенности этой теории для РС-кодов.

Теорема 4. *Если в РС-коде с проверочной матрицей (1), где* $b=1, q=2^m$, *синдром* $S(\bar{e})=(s_1,s_2,...,s_{\delta-1})$, *то синдром* $S(f_\gamma(\bar{e}))=(\gamma s_1,\gamma s_2,...,\gamma s_{\delta-1})=\gamma S(\bar{e})$.

Теорема 5. *Пусть в условиях теоремы 4 в РС-коде норма* $\bar{N}(S(\bar{e}))=(N_{12},N_{13},...,N_{(\delta-2)(\delta-1)})$. *Тогда* $\bar{N}(S(\gamma\bar{e}))=(N_{12}^{\gamma},N_{13}^{\gamma},...,N_{(\delta-2)(\delta-1)}^{\gamma})$, *где* $N_{ij}^{\gamma}=N_{ij}\big/\gamma^{(j-i)/h_{ij}}, 1\le i<j\le\delta-1$.

Следствие 1. *Пусть в условиях теоремы 5* $\delta=5$. *Тогда* $N(S(\bar{e}))=(N_{12},N_{13},N_{14},N_{23},N_{24},N_{34})$ *и* $N_{12}^{\gamma}=N_{12}\big/\gamma$; $N_{13}^{\gamma}=N_{13}\big/\gamma^2$; $N_{14}^{\gamma}=N_{14}\big/\gamma^3$; $N_{23}^{\gamma}=N_{23}\big/\gamma$; $N_{24}^{\gamma}=N_{24}\big/\gamma$; $N_{34}^{\gamma}=N_{34}\big/\gamma$.

Следствие 2. *Норменные спектры А-орбит (множества норм Г-орбит данных А-орбит) либо совпадают, либо не пересекаются.*

Как и в случае БЧХ-кодов, нормы синдромов в РС-кодах позволяют селектировать А-орбиты ошибок вместо отдельных ошибок, что существенно снижает вычислительные затраты при декодировании РС-кодов. В Госкомитет изобретений РБ подана заявка на изобретение декодера на основе норм синдромов [24].

На основе теории норм синдромов обоснованы возможности коррекции модифицированными БЧХ-кодами, реверсивными кодами различных расширенных классов ошибок [25-38]. В частности доказано, что лексикографически упорядоченный реверсивный код с минимальным расстоянием 6 декодирует:

1) произвольную двойную или одиночную ошибку;

2) ошибку весом $t=3$ вида: модульная длиной $b=2$ плюс произвольная одиночная;

3) модульную ошибку длиной $b=4$ с локаторами в одном из модулей длиной 4 (начиная со второго) а также в первом модуле, если след $Tr((1+\alpha+\alpha^2)^{-1})=1$.

Этот результат примерно в 2 раза увеличивает количество корректируемых реверсивным кодом ошибок.

Заключение

Основные результаты проведенных исследований состоят в следующем.

Осуществлена классификация векторов-ошибок линейных кодов, т.е. разбиение их на непересекающиеся легко конструируемые классы — Г-орбиты, G-орбиты, A-орбиты.

Показано, что спектры синдромов Г-орбит и G-орбит имеют структуру, адекватную самим орбитам.

В теорию помехоустойчивого кодирования введена новая характеристика — норма синдрома, являющаяся инвариантом группы циклических сдвигов Г и, следовательно, идентификатором Г-орбит и G-орбит. Исследованы основные свойства норм синдромов.

Доказана возможность декодирования любой совокупности Г-орбит с попарно различными нормами синдромов. Это дает конструктивный способ строить расширенные классы декодируемых ошибок по сравнению с традиционными методами, что позволяет решать проблему избыточности кодов.

Разработаны перестановочные норменные методы коррекции ошибок, которые отличают: перебор крупных блоков — орбит ошибок, возможность исправления дополнительных видов ошибок, снижение вычислительных затрат на реализацию при достаточно высоком быстродействии (n-кратное сокращение вычислительных затрат, n — длина кода).

Разработан метод сжатия норм синдромов, сокращающий в n^2 раз вычислительные затраты по сравнению с классическими синдромными методами. Внесен вклад в решение проблемы селектора за счет предложенных конструктивных алгоритмов сжатия норм синдромов.

Развита теория норм синдромов для РС-кодов, реверсивных кодов. Теория норм синдромов применена к различным кодификациям БЧХ-кодов, позволила в два раза увеличить количество корректируемых ошибок лексикографически упорядоченным реверсивным кодам.

THE THEORY OF SYNDROME NORMS IN THE PERMUTATION DECODING ACTION UNJAMMABLE CODES

V.K. KONOPELKO, V.A. LIPNITSKI

Abstract

The fundamental moments of the theory of norms of syndromes a new direction in the permutation decoding action of unjammable codes are stated. Norms of syndromes groups of cyclic shifts break words — errors into not traversed classes, are identifiers of these classes, allow essentially to reduce computing expenses at decoding action of errors that is the new decision of a problem of the selector) to extend a spectrum декодируемых errors.

Литература

1. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. М., СПб., Киев, 2003.
2. *Уолред Дж.* Телекоммуникационные и компьютерные сети. Вводный курс. М., 2001. 480 с.
3. *Courtois N., Finiasz M., Sendrier N.* How to achieve a McEliece-based Digital Signature Sheme. 2002 // http://www.minrank.org/.
4. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки: Пер. с англ. М., 1979.
5. *Конопелько В.К., Липницкий В.А.* Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Мн.: БГУИР, 2000. 242 с. 2-е изд. М.: Едиториал УРСС, 2004. 176 с.
6. *Липницкий В.А., Конопелько В.К.* О матрицах линейных кодов // VI МНТК "Современные средства связи": Материалы конф., Нарочь, 1 – 5 октября 2001 г. / Изв. Белелорус. инж. акад. 2001. №1(11)/2. С. 19–21.

7. *Конопелько В.К., Липницкий В.А.* Классы эквивалентности и нормы синдромов для БЧХ-кодов // 2-я МНК "Современные средства связи": Материалы конф., Нарочь, Беларусь, 22 – 26 сент. 1997 г. / Изв. Белорус. инж. акад. 1997. №1(3)/1. С. 82 – 85.
8. *Конопелько В.К., Липницкий В.А.* Модифицированные БЧХ-коды с минимальным расстоянием 5 или 6 и их корректирующие возможности // LIII научн. сессия, посв. дню радио: Тез.докл, Москва, 20 – 21 мая 1998 г. С. 207 – 208.
9. *Конопелько В.К., Липницкий В.А.* Перестановочный метод декодирования БЧХ-кодов и его возможности // 1-ая Международная конф. "Цифровая обработка сигналов и ее применение": Доклады, Т. 1, Москва, 30 июня – 3 июля 1998 г. С. 79 – 86.
10. *Конопелько В.К., Липницкий В.А., Лапо Д.А.* Коррекция двойных и пакетной ошибок длины 4 модифицированным БЧХ-кодом // 2-я МНК "Цифровая обработка сигналов и её применения": Доклады, Т. 1, Москва, 21 – 24 сент. 1999 г. / ООО "Инсвязьинвест". М., 1999. С. 156 – 157.
11. *Качановский Д.В., Конопелько В.К., Липницкий В.А.* Декодирование БЧХ-кодов с помощью норм синдромов, циклических и циклотомических перестановок // 2-ая МНК "Цифровая обработка сигналов и её применения": Доклады, Т. 1, Москва, 21 – 24 сент. 1999. / ООО "Инсвязьинвест". М., 1999. С. 146–150.
12. *Липницкий В.А., Конопелько В.К.* Автоморфизм Фробениуса и перестановочный метод декодирования семейства БЧХ-кодов // 4-я МНК "Современные средства связи": Материалы конф., Нарочь, Беларусь, 20 – 24 сент. 1999/ Изв. Белорус. инж. акад. 1999. №1(7) / 1. С. 81 – 83.
13. *Липницкий В.А., Конопелько В.К.* Нормы синдромов в БЧХ-кодах с минимальным расстоянием 7 // "Современные проблемы проектирования и производства радиоэлектронных средств": Сб. материалов Межд. научн.-техн. семинара. Новополоцк. 29 – 31 мая 2000. С. 228 – 231.
14. *Липницкий В.А.* Нормы синдромов и норменный метод коррекции ошибок БЧХ-кодами // VIII Белорусская математическая конф.: Тез. докл., часть IV. Минск. 19 – 24 июня 2000. / НАН РБ. Ин-т математики. Мн., 2000. С. 16.
15. *Липницкий В.А., Конопелько В.К.* Перестановочное декодирование БЧХ-кодов с минимальным расстоянием 7 // 3-я МНК и выставка "Цифровая обработка сигналов и ее применения": Доклады. Т. 1. Москва, 29 ноября – 1 декабря 2000 г. С. 49 – 52.
16. *Липницкий В.А.* Определение нормы синдрома в произвольных БЧХ-кодах // 7-я МНТК "Современные средства связи": Материалы конф., Нарочь, 30 сент. – 4 окт. 2002 г. / Изв. Белорус. инж. акад. 2002. №2(14)/1. С. 102 – 104.
17. *Липницкий В.А.* Нормы синдромов ошибок в произвольных БЧХ-кодах // Электромагнитные волны и электронные системы. 2003. Т. 8, №3. С. 4 – 12.
18. *Конопелько В.К., Липницкий В.А.* Декодирующие возможности реверсивных кодов с минимальным расстоянием 5 // Радиотехника и электроника. 1999. Вып. 24. С. 70 – 74.
19. *Липницкий В.А., Конопелько В.К.* Перестановочный метод декодирования реверсивных кодов и его возможности // 2-я МНК "Цифровая обработка сигналов и её применения": Доклады. Т. 1. Москва, 21 – 24 сент. 1999 г. / ООО "Инсвязьинвест". М., 1999. С. 158 – 163.
20. *Липницкий В.А.* // Докл. БГУИР. 2003. Т. 1, №2/1. С. 107 – 110.
21. *Липницкий В.А., Конопелько В.К., Курилович А.В.* Системотехника БИС помехоустойчивых кодов // Электромагнитные волны и электронные системы. 2002. Т. 6, №3. С. 61 – 66.
22. *Конопелько В.К., Липницкий В.А.* Теория норм синдромов и проблема контроля многократных ошибок в телекоммуникациях // 5-я летняя междунар. школа-семинар "Современные информационные технологии": Материалы семинара. Браслав, Беларусь, 2 – 6 июля 2002 г. / Изв. Белорус. инж. акад. 2002. №1(13)/2. С. 153 – 159.
23. *Конопелько В.К., Липницкий В.А., Курилович А.В.* Метод сжатия норм синдромов для коррекции кратных ошибок // 5-я МНТК "Цифровая обработка сигналов и её применения": Доклады. Т. 1. Москва. 12 – 14 марта. 2003 г. / ООО "Инсвязьинвест". М., 2003. С. 146 – 150.
24. *Липницкий В.А., Земляков А.Л., Конопелько В.К.* Устройство декодирования для коррекции модуля ошибок. Заявка на изобретение в Госкомизобретений РБ. BY. Мн., 2001. №2. С. 58 – 59.
25. *Конопелько В.К., Липницкий В.А., Власова Г.А.* Коррекция двойных, модульных и пакетных ошибок реверсивным кодом // Респ. научн.-техн. семинар "Организация и технология средств связи": Материалы сем., Минск, 27 июня 1996 г. / Веснік сувязі. 1996. №2(10). С. 19.
26. *Липницкий В.А.* // 7-я. Бел. матем. конф.: Тез. докл. Ч.I. Минск, 18 – 22 ноября 1996г. С. 109 – 110.
27. *Липницкий В.А., Конопелько В.К.* Лексикографические реверсивные коды, исправляющие случайные и модульные ошибки // Вторая МНК "Автоматизация проектирования дискретных систем": Материалы конф. Минск, 12-14 ноября 1997 г. Т.2. / НАН Беларуси. Ин-т кибернетики. Мн., 1997. С. 176 – 183.
28. *Липницкий В.А.* Следы в конечных полях и дополнительные корректирующие возможности БЧХ-кодов // I-я МНК и выставка "Компьютерная алгебра в фундаментальных и прикладных исследованиях и образовании": Тез. докл. Минск, 8-11 декабря 1997 г. С. 30 – 33.

29. *Конопелько В.К., Липницкий В.А., Лапо Д.А.* // Интеллектуальные системы: Сб. научн. трудов ИТК НАН Беларуси. Вып. 1. Мн., 1998. С. 187 – 192.
30. *Липницкий В.А., Конопелько В.К.* Контроль пакетов ошибок БЧХ-кодами // Интеллектуальные системы: Сб. научн. трудов ИТК НАН РБ. Вып. 2. 1999. С. 157 – 164.
31. *Конопелько В.К., Липницкий В.А., Земляков А.А.* Однородные коды для БИС коррекции ошибок // Интеллектуальные системы: Сб. научн. трудов ИТК НАН РБ. Вып. 2. 1999. С. 165–169.
32. *Липницкий В.А., Конопелько В.К.* Коррекция ошибок лексикографически упорядоченным реверсивным кодом // Электромагнитные волны и электронные системы. 1999. Т. 4, №3. С. 4 – 9.
33. *Липницкий В.А., Конопелько В.К., Земляков А.Л.* Высокоскоростной декодер кода Рида-Соломона // 4-я МНК "Современные средства связи": Материалы конф. Нарочь, Беларусь, 20 – 24 сент. 1999 г. / Изв. Белорус. инж. акад. 1999. №1(7) / 1. С. 79 – 80.
34. *Липницкий В.А., Конопелько В.К., Власова Г.А., Осипов А.Н.* Двоичные реверсивные коды для контроля байтовых ошибок // Весці НАН Беларусі. Сер. фіз.-мат. навук. 2000. №1. С. 127 – 131.
35. *Земляков А.Л., Конопелько В.К., Липницкий В.А.* Адаптивный декодер кодов БЧХ и Рида-Соломона // 3-я МНК и выставка "Цифровая обработка сигналов и ее применения": Доклады. Т. 1. Москва, 29 ноября – 1 декабря 2000 г. С. 36 – 39.
36. *Земляков А.Л., Конопелько В.К., Липницкий В.А.* Высокоскоростной декодер кода Рида-Соломона для коррекции двойного модуля ошибок // 5-я МНТК "Современные средства связи": Материалы конф., Нарочь, 2000 / Изв. Бел. инж. академии. – 2000. – №1(9) /1. – С. 137 – 139.
37. *Липницкий В.А., Конопелько В.К.* Корректирующие возможности БЧХ-кодов с кодовым расстоянием 5, 6 и их модификаций // Радиотехника и электроника. 2001. Вып. 25. С. 62 – 71.
38. *Липницкий В.А., Конопелько В.К., Курилович А.В.* Декодирование циклических БЧХ-кодов с помощью идентификаторов классов ошибок // VI-я МНТК "Современные средства связи": Материалы конф. Нарочь, 1 -5 октября 2001 г. / Изв. Белорус. инж. акад. 2001. №1(11)/2. С.16 -18.