## *ИНФОРМАТИКА*

*УДК 621.391 (075.8)*

# УСТРОЙСТВА ОБРАБОТКИ БЧХ-КОДОВ НА ОСНОВЕ НОРМ СИНДРОМОВ

В.А. ЛИПНИЦКИЙ

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

*Поступила в редакцию 9 января 2003*

Теория норм синдромов предоставляет перестановочные алгоритмы коррекции ошибок, позволяющие на порядок снизить “проблему селектора”. Их реализация возможна как с помощью ПЗУ, так и ПЛИС. Первая обладает хорошей аппаратурной экономичностью, вторая – высоким быстродействием.

*Ключевые слова*: помехоустойчивость, БЧХ-коды, синдром ошибок, норма синдрома, декодер, перестановочное декодирование.

### Введение

Одной из прикладных задач общей теории телекоммуникаций является повышение помехоустойчивости цифровой передачи, хранения, обработки и коммутации сообщений [1, 2]. При широком многообразии помехоустойчивых кодов на практике реализован лишь небольшой спектр кодов и методов их декодирования. Это декодеры, базирующиеся на методе максимального правдоподобия, используемые, как правило, для обработки низкоскоростных кодов [3], мажоритарные декодеры, синдромные декодеры для обработки высокоскоростных кодов. Основное препятствие здесь — "проблема селектора" — быстрый рост количества селектируемых векторов с увеличением длины кода или кодового расстояния. Общепризнано считать эффективными перестановочные декодеры, базирующиеся на автоморфизмах кодов [1]. Однако до последнего времени они не нашли практической реализации ввиду отсутствия теоретической базы и, как следствие, сложности алгоритмов коррекции ошибок. Определенным шагом в развитии перестановочных методов обработки кодов является создание теории норм синдромов [4]. Суть теории состоит в следующем. Под действием группы Г векторы-ошибки разбиваются на непересекающиеся классы — Г-орбиты. Каждая Г-орбита имеет четко очерченный спектр векторов и синдромов — зная вектор (синдром вектора) одной Г-орбиты, можно однозначно восстановить все остальные векторы (синдромы ее векторов). Через компоненты синдрома вычисляется норма синдрома [4]. Норма синдрома не зависит от циклических сдвигов, является однозначной характеристикой каждой Г-орбиты; это и есть норма Г-орбиты. Г-орбиты с различными нормами имеют непересекающиеся спектры синдромов. Отсюда следует, что код может корректировать любой набор К Г-орбит векторов-ошибок с попарно различными нормами. Практически в любом коде можно построить совокупность Г-орбит К, содержащий не только произвольные случайные ошибки, допустимые кодовым расстоянием, но и ряд зависимых ошибок, вплоть до полного исчерпания синдромных возможностей кода.

*Норменный метод декодирования*. Изложенная теория предоставляет следующий метод декодирования ошибок: вычисляется синдром ошибок $S(\bar{x}) = S(\bar{e})$ принятого сообщения

$\overline{x} = \overline{e} + \overline{y}$, где $\overline{y}$ — истинное кодовое слово, $\overline{e}$ — вектор ошибок; далее вычисляется норма синдрома $\overline{N}(S(\overline{x})) = \overline{N}$. Норма указывает Г орбиту J, которой принадлежит вектор $\overline{e}$. Если в Г-орбите J зафиксировать один элемент $\overline{e}_j$ в качестве образующего, то, сравнив синдромы $S(\overline{e})$ и $S(\overline{e}_j)$, можно определить величину циклического сдвига, переводящего $\overline{e}_j$ в $\overline{e}$. Тем самым вектор ошибок $\overline{e}$ может быть однозначно определен. Основные этапы этого алгоритма для БЧХ-кода с минимальным расстоянием $d$=5 исправляющего ошибки кратности $t$=2, состоят в следующем.

1. Вычисляется синдром $S = (\alpha^{i_T}, \alpha^{j_T})$ (БВС).

2. Находятся текущие значения степеней $i_T$, $j_T$ элементов поля Галуа (ПЗУ1 и ПЗУ2).

3. Вычисляется показатель нормы синдрома deg $N$=( $j_T - 3\, i_T$ )(mod $n$) (применяется сумматор по модулю n).

4. По показателю deg $N$ находится показатель $i_0$ первой компоненты синдрома образующего вектора ошибок (с применением ПЗУ3).

5. Вычисляется $L_1 = (i_T - i_0)$(mod $n$) номер первого ошибочного разряда (с помощью сумматора по модулю n).

6. Вычисляется номер $L_2$ второго ошибочного разряда — с помощью блока вычисления наблюдаемого вектора ошибок (БВНВО), состоящего из ПЗУ4 и сумматора по модулю $n$, вычисляется диаметр ошибки и, следовательно, положение второй ошибочной позиции.

7. Путем раздельной дешифрации $L_1$ и $L_2$ (с помощью дешифраторов $Д_ш$1 и $Д_ш$2) находятся векторы ошибок $\overline{e}_1$ и $\overline{e}_2$ веса 1.

8. Находится суммарный вектор $\overline{e} = \overline{e}_1 + \overline{e}_2$ в блоке элементов ИЛИ (на рис. 1 — блок 1).

9. Осуществляется коррекция принятого сигнала в блоке инвертирования (БИ).

Декодер, реализующий данный алгоритм , представлен на рис. 1.

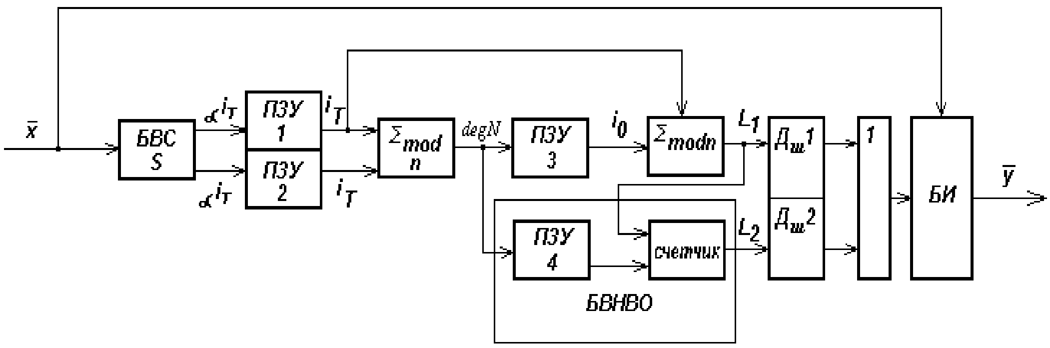


Рис. 1. Структурная схема декодера, использующего ПЗУ и сумматоры по модулю $n$

В сумме аппаратурная сложность данного декодера составляет $(\sum N + 3n)\log_2 n + 3n$ элементов И, ИЛИ, ячеек памяти. Например, для длины кода $n$=127, $t$=2 аппаратурная сложность составляет 3115 элементов. Такая сложность вполне приемлема для современной микроэлектронной базы. Однако декодер отличается неоднородностью входящих блоков; это приводит к большим затратам площади кристаллов, реализующим декодер. Сложность предложенного декодера почти в три раза меньше числа селектируемых комбинаций: $C^1_{121} + C^2_{127}$ =8128 по таблице смежных классов, на реализацию которой потребуется ПЗУ емкостью $2^{2\log_2 n} \cdot 2^{2\log_2 n}$ (при n=127 емкость его примерно равна 64 Кбит) при извлечении из него двух $\log_2 n$ разрядных кодов адресов ошибок. Если декодер реализовать на основе классического метода синдромов с использованием ПЗУ емкостью, равной суммарному числу синдромов, умноженному на длину кода, то для данного примера емкость ПЗУ составит 8128·127≈Мбит.

Анализ показывает, что с увеличением кратности $t$ корректируемых ошибок увеличивается число ПЗУ для преобразования элементов поля в их показатели, количество сумматоров по модулю *n* для нахождения показателей компонент норм синдромов deg $N_i$, ПЗУ для хранения адресов ошибок образующего вектора. Также требуется блок вычисления текущего значения нормы синдрома $\overline{N}_T = (N_1, N_2, \ldots, N_z)$ (при $d \geq 7$ норма синдрома становится вектором [4]. Ясно, что данный блок может быть реализован на элементах И, максимальное число входов у которых равно *t*, а их суммарное число равно количеству норм синдромов, необходимых для декодирования *t*-кратных ошибок.

Анализ рассматриваемого метода декодирования и его реализаций показывает, что операции при вычислениях совершаются с двоичными числами с промежуточными переходами в унитарные коды (в дешифраторах и ПЗУ) и обратно в двоичные. Это приводит к большим задержкам сигналов при преобразованиях, а также к высокой сложности при реализации сумматоров по модулю *n* при их параллельной схеме исполнения, а при последовательной реализации — к низкому быстродействию.

Если реализовать алгоритм декодирования на ПЛИС, то в этом случае происходит преобразование синдрома (двоичного кода) в унитарный код с помощью дешифратора, а далее вычисляется норма N и вектор ошибок $\bar{e}$ в унитарных кодах.

На рис. 2 представлена структурная схема декодера на ПЛМ, реализующая метод декодирования в унитарном коде для БЧХ-кода длиной *n*=7. Каждая точка на пересечении вертикальных и горизонтальных шин логических матриц ЛМ1 и ЛМ2 обозначает элемент 2И. Схема построена на основе таблицы, где представлены все векторы-ошибки веса 1–2, собранные в Г-орбиты

$I_1$–$I_4$, синдромы ошибок в названном коде и показатели норм Г-орбит.

**Перечень векторов Г-орбит ошибок веса 1, 2 и их синдромов в БЧХ- коде длиной 7**

| Г-орбита | $I_1$ | | $I_2$ | | $I_3$ | | $I_4$ | |
|---|---|---|---|---|---|---|---|---|
| $\bar{e}$ и $S(\bar{e})$ | (1) | (1,1) | (1,2) | $(\alpha^3,\alpha^2)$ | (1,3) | $(\alpha^6,\alpha^4)$ | (1,4) | $(\alpha,\alpha^5)$ |
| $\sigma(\bar{e})$ и $S(\sigma(\bar{e}))$ | (2) | $(\alpha,\alpha^6)$ | (2,3) | $(\alpha^4,\alpha)$ | (2,4) | $(1,\alpha^3)$ | (2,5) | $(\alpha^2,\alpha^4)$ |
| $\sigma^2(\bar{e})$ и $S(\sigma^2(\bar{e}))$ | (3) | $(\alpha^2,\alpha^5)$ | (3,4) | $(\alpha^5,1)$ | (3,5) | $(\alpha,\alpha^2)$ | (3,6) | $(\alpha^3,\alpha^3)$ |
| $\sigma^3(\bar{e})$ и $S(\sigma^3(\bar{e}))$ | (4) | $(\alpha^3,\alpha^4)$ | (4,5) | $(\alpha^6,\alpha^6)$ | (4,6) | $(\alpha^2,\alpha)$ | (4,7) | $(\alpha^4,\alpha^2)$ |
| $\sigma^4(\bar{e})$ и $S(\sigma^4(\bar{e}))$ | (5) | $(\alpha^4,\alpha^3)$ | (5,6) | $(1,\alpha^5)$ | (5,7) | $(\alpha^3,1)$ | (5,1) | $(\alpha^5,\alpha)$ |
| $\sigma^3(\bar{e})$ и $S(\sigma^5(\bar{e}))$ | (6) | $(\alpha^5,\alpha^2)$ | (6,7) | $(\alpha,\alpha^4)$ | (6,1) | $(\alpha^4,\alpha^6)$ | (6,2) | $(\alpha^6,1)$ |
| $\sigma^6(\bar{e})$ и $S(\sigma^3(\bar{e}))$ | (7) | $(\alpha^6,\alpha)$ | (7,1) | $(\alpha^2,\alpha^3)$ | (7,2) | $(\alpha^5,\alpha^5)$ | (7,3) | $(1,\alpha^6)$ |
| deg$N(I)$ | 0 | | 5 | | 3 | | 6 | |

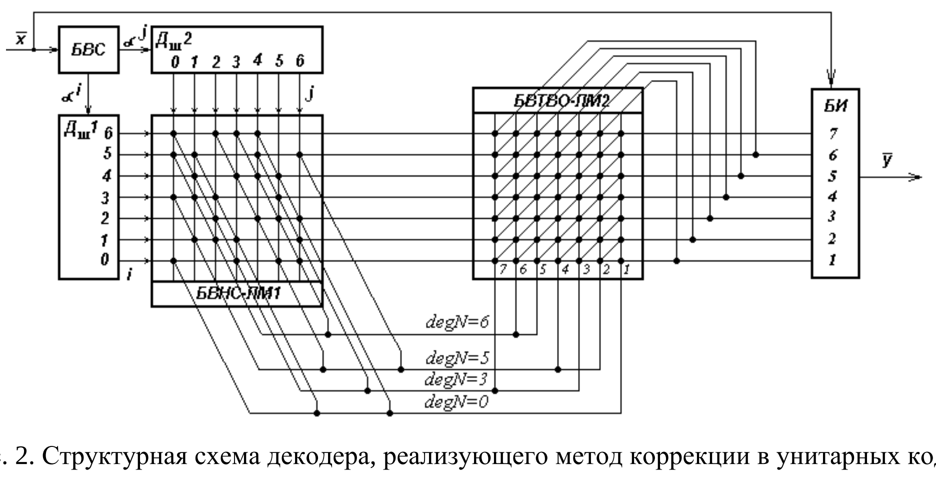


Рис. 2. Структурная схема декодера, реализующего метод коррекции в унитарных кодах

Двоичные коды синдрома с выходов БВС поступают на входы дешифраторов $Д_ш1$ и $Д_ш2$, где преобразуются в унитарные коды. Эти коды поступают на первую логическую матрицу БВНС-ЛМ1, на выходах которой устанавливаются в унитарном коде единичные сигналы в зависимости от вычисленной нормы N; на выходах второй логической матрицы (БВТВО-ЛМ2) — текущие векторы ошибок Таким образом, по сути дела логическая матрица ЛМ2 заменяет функции, БВОВО, БВЦС, БВТВО декодера (рис. 2) и производит циклический сдвиг образующего вектора ошибок $\bar{e}$. Прообразом здесь является работа [5].

### Результаты и обсуждения

Основное преимущество норменного декодера на ПЛИС — высокое быстродействие — обеспечивается как за счет исключения отдельных блоков, так и благодаря регулярной и однородной структуре ЛМ. Так, например, для декодера на рис. 2 сигнал задерживается лишь в трех последовательно соединенных высокоскоростных блоках (дешифраторе и двух ЛМ. Известно, что сумматоры по $\mathrm{mod}\, n$ являются достаточно медленными элементами. Сложность реализации рассматриваемого декодера определяется емкостью двух ЛМ, одна из которых наполовину заполнена ($0{,}5 \cdot n^2$). Это приводит к более высокой сложности устройства. В частности, при длине кода n=127 сложность примерно равна 22 Кбит. Это в семь раз выше сложности декодера на рис. 1, однако примерно в 4 раза соответственно ниже сложности декодера, реализующего декодирование по таблице смежных классов.

### Заключение

Теория норм синдромов предоставляет перестановочные алгоритмы коррекции ошибок, позволяющие на порядок снизить “проблему селектора”. Их реализация возможна как с помощью ПЗУ, так и ПЛИС. Первая обладает хорошей аппаратурной экономичностью, вторая – высоким быстродействием.

## DEVICES FOR BCH CODES DECODING USING SYNDROME NORMS

V.A. LIPNITSKY

### Abstract

The syndrom norm theory provides permutation algorithms for error correcting thus essentially decreasing a “selector problem”. They can be implemented by using RAM and PLIS. The first one has accessible hardware economy, the second one — high speed performance.

### Литература

1. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М., 1979.
2. *Варламова О.* Помехоустойчивые кодеки — будущее цифровой телефонии. Интернет, 2002.
3. *Дворников В.Д., Конопелько В.К., Липницкий В.А.* Теория и практика низкоскоростных кодов. Мн., 2002.
4. *Конопелько В.К., Липницкий В.А.* Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Мн., 2000.
5. *Конопелько В.К.* Устройство декодирования для коррекции двойных ошибок. А.с. № 1833968. 1993. Бюл. изобрет. № 30.