ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ КОДОВ РИДА-СОЛОМОНА В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Егоров С.И.

Курский государственный технический университет

I. ВВЕДЕНИЕ

Коды Рида-Соломона (РС-коды) характеризуются параметрами (n,k,d), где n – длина кодового слова, k - количество информационных символов в кодовом слове и d – минимальное кодовое расстояние. При этом количество проверочных символов в слове $r = (n-k)$, и $d = r+1$. Символы кодового слова представляют собой элементы поля Галуа $GF(q)$.

Известно [1], что коды Рида-Соломона (РС) могут гарантированно исправлять любой набор из t ошибочных символов, тогда и только тогда, когда выполняется условие $2t+1 \le d$. Основываясь на алгоритме Берлекэмпа-Месси Блейхут [1] разработал процедуру декодирования для РС-кодов, позволяющую во многих случаях исправлять $t+1$ ошибочных символов. Недавно эта процедура была усовершенствована Егоровым и Маркаряном [2]. В представленной работе предлагается упрощение аппаратной реализации модифицированной процедуры Блейхута, приводятся результаты исследования эффективности исправления ошибок.

II. МОДИФИЦИРОВАННАЯ ПРОЦЕДУРА БЛЕЙХУТА ДЛЯ ДЕКОДИРОВАНИЯ РС-КОДОВ

Модифицированная процедура для исправления $t+1$ ошибочных символов в кодовом слове РС-кода с минимальным расстоянием $d=2t+1$ [2], состоит из следующих этапов:

1) Вычисление полинома синдромов $S(x)$.

2) Получение полинома локаторов $\Lambda^{(2t)}(x)$, вспомогательного полинома $B^{(2t)}(x)$ и формальной степени полинома локаторов L_{2t} с использованием алгоритма Берлекэмпа-Месси.

3) Вычисление преобразования Фурье полиномов $\Lambda^{(2t)}(x)$ и $B^{(2t)}(x)$, когда $L_{2t} = t$ или $L_{2t} = t+1$.

4a) Вычисление коэффициентов $C_i = B^{(2t)}(\alpha^{-i})/\Lambda^{(2t)}(\alpha^{-i})$, когда $L_{2t} = t$, или $D_i = \Lambda^{(2t)}(\alpha^{-i})/ (B^{(2t)}(\alpha^{-i})\cdot\alpha^{-2i})$, когда $L_{2t} = t+1$ (α – примитивный элемент поля $GF(q)$).

4b) Вычисление последовательностей S_i возможных значений $\Delta^{i,j}_{2t+1}$ невязки Δ_{2t+1} для каждого значения $i \in \{0,\ldots,n-1-t\}$ ($j=i+1,\ldots,n-1$) и поиск значений Δ_{2t+1}, которые встречаются точно t раз в какой-то из этих последовательностей, где

$$S_i = \{ \Delta^{i,j}_{2t+1} = \frac{\alpha^i - \alpha^j}{C_i - C_j}; j = i+1,\ldots,n-1; \Lambda^{(2t)}(a^{-j}) \neq 0 \}; i = 1,\ldots,n-1-t; \Lambda^{(2t)}(a^{-i}) \neq 0, \quad (1)$$

когда $L_{2t}=t$, или

$$S_i = \{ \Delta^{i,j}_{2t+1} = \frac{D_i - D_j}{\alpha^i - \alpha^j}; j = i+1,\ldots,n-1; B^{(2t)}(a^{-j}) \neq 0 \}; \; i = 1,\ldots,n-1-t; B^{(2t)}(a^{-i}) \neq 0, \quad (2)$$

когда $L_{2t} = t+1$.

4c) Повторное вычисление последовательностей S_i для найденного значения i и фиксация локаторов ошибок в моменты времени равенства невязки Δ_{2t+1} значениям $\Delta^{i,j}_{2t+1}$.

5) Получение полинома $\Lambda^{(2t+2)}(x)$, вычисление значений ошибок и их исправление.

Представленная процедура основывается на эффективном методе поиска неизвестных невязок аналитического продолжения алгоритма Берлекэмпа-Месси [2]. Этот метод позволяет сократить в $2(q-1)n/((n+t+1)(n-t))$ раз по сравнению с алгоритмом Блейхута число тактов самого сложного этапа алгоритма декодирования: поиска неизвестных невязок.

III. УПРАЩЕНИЕ АППАРАТНОЙ РЕАЛИЗАЦИИ ПРОЦЕДУРЫ ДЕКОДИРОВАНИЯ

Структурная схема декодера РС-кода, реализующего модифицированную процедуру Блейхута приведена на рисунке 1. Декодер содержит: буфер данных, вычислитель синдрома, процессор Галуа, модуль дискретного преобразования Фурье (DFT) и модуль нахождения локаторов $t+1$ ошибки.

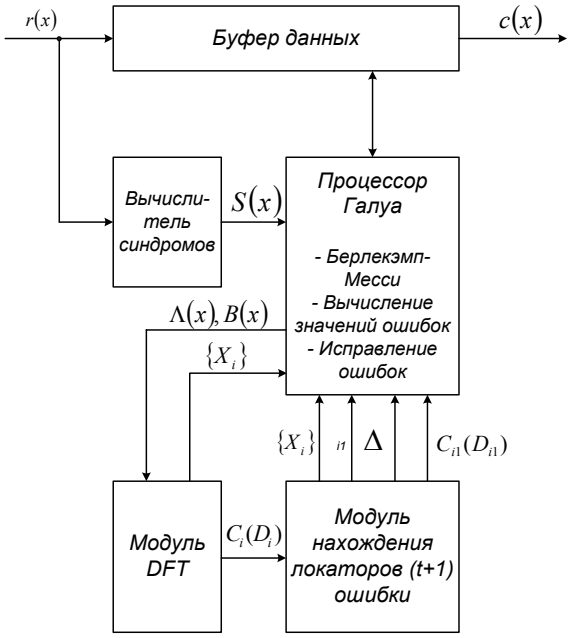

Рис.1. Структурная схема декодера

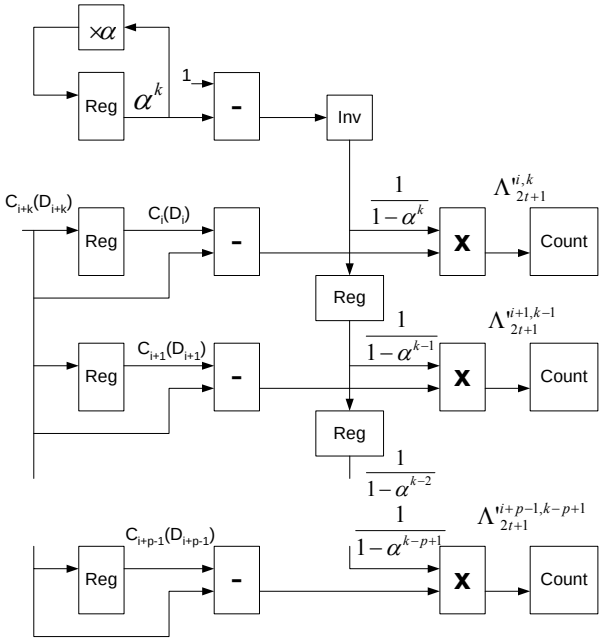

Рис.2. Структурная схема модуля нахождения локаторов t+1 ошибки

Процессор Галуа реализует алгоритм Берлекэмпа-Месси, вычисляя в соответствии с ним многочлены $\Lambda^{(2t)}(x)$ и $B^{(2t)}(x)$. Кроме того, на основе информации, полученной от модуля вычисления локаторов ошибок веса t+1, он вычисляет значения Δ_{2t+1}, Δ_{2t+2} и затем $\Lambda^{(2t+2)}(x)$. Используя многочлены $\Lambda(x)$, $S(x)$ и локаторы ошибочных символов, процессор Галуа вычисляет многочлен значений ошибок $\Omega(x)$, а затем вычисляет значения ошибок для уже известных позиций ошибочных символов.

Модуль DFT вычисляет преобразование Фурье многочленов $\Lambda^{(2t)}(x)$ и $B^{(2t)}(x)$. Кроме того в зависимости от режима работы он вычисляет коэффициенты C_i или D_i. Этот же модуль вычисляет величины, обратные к корням полинома $\Lambda^{(2t)}(x)$, и контролирует их число, если $L_{2t} \le t$.

Модуль нахождения локаторов ошибок веса t+1 в зависимости от режима работы использует коэффициенты C_i или коэффициенты D_i. Он находит набор локаторов ошибок $\{X_i\}$ веса t+1 и соответствующие им значения Δ, i_1, C_{i_1} (или D_{i_1}).

Представленный декодер работает по конвейерному принципу: все основные его модули работают параллельно, обрабатывая последовательно принятые из канала различные кодовые слова. Задержка декодирования составляет пять кодовых слов.

Поиск неизвестных невязок в модуле нахождения локаторов ошибок осуществляется в соответствии с простыми формулами (1) и (2). Одной итерации соответствуют четыре операции: два вычитания в поле Галуа (эквивалентны сложению в GF(2^m)), одно деление в поле Галуа и инкремент небольшого целого. Хотя на каждой итерации выполняется небольшое число операций, значительное количество итераций, требуемое для декодирования кодового слова, делает модуль нахождения локаторов ошибок наиболее ресурсоемкой частью декодера.

Для конвейерного декодера важно уменьшить время обработки кодового слова в модуле нахождения локаторов ошибок до времени приема слова из канала. Этого можно достигнуть параллельной организацией поиска невязок. Архитектура модуля нахождения локаторов ошибок с параллельной организацией поиска невязок показана на рисунке 2. Особенность этой архитектуры заключается в том, что она позволяет заменить деления в конечном поле (1,2) на значительно более простые операции умножения с добавлением одной единственной схемы нахождения обратного элемента в поле Галуа.

Математическое обоснование предложенной архитектуры основывается на следующем утверждении.

Утверждение: Если $L_{2t} = t$, то последовательности значений $\Delta'^{i,j}_{2t+1} = \Delta^{-1^{i,j}}_{2t+1} \cdot \alpha^{i}$, полученные для пар i и $j = i + k$, будут иметь вид:

$$S_i = \{ \Delta'^{i,k}_{2t+1} = (C_i - C_{i+k}) \cdot (1-\alpha^k)^{-1};\ k = 1,...,n\text{-}1\text{-}i;\ \Lambda^{(2t)}(a^{-i-k}) \neq 0 \},\ i = 1,...,\ n\text{-}1\text{-}t,\ \Lambda^{(2t)}(a^{-i}) \neq 0. \quad (3)$$

Если $L_{2t} = t + 1$, то последовательности значений $\Delta'^{i,j}_{2t+1} = \Delta^{i,j}_{2t+1} \cdot \alpha^{i}$ будут иметь вид:

$$S_i = \{ \Delta'^{i,k}_{2t+1} = (D_i - D_{i+k}) \cdot (1-\alpha^k)^{-1},\ k = 1,...,n\text{-}1\text{-}i,\ B^{(2t)}(a^{-i-k}) \neq 0 \},\ i = 1,...,\ n\text{-}1\text{-}t,\ B^{(2t)}(a^{-i}) \neq 0. \quad (4)$$

Доказательство: (3) и (4) следует из (1) и (2) после замены переменной j на $k = j - i$ с учетом $\alpha^i - \alpha^{i+k} = \alpha^i \cdot (1 - \alpha^k)$.

Можно заметить, что компоненты α^i в (1) и (2) не зависят от конфигурации ошибок в принятом кодовом слове и не меняются в S_i. При использовании (3) или (4) вместо (1) или (2) подсчет Δ'_{2t+1} заменяет подсчет Δ_{2t+1}.

После нахождения требуемого значения Δ'_{2t+1} значение Δ_{2t+1} может быть найдено следующим образом: $\Delta_{2t+1} = (\Delta'_{2t+1})^{-1} \cdot \alpha^{iI}$, если $L_{2t} = t$, или $\Delta_{2t+1} = \Delta'_{2t+1} \cdot \alpha^{-iI}$, если $L_{2t} = t + 1$.

Формулы (3) и (4) позволяют распараллелить поиск невязок с сокращенной аппаратной сложностью. Так как правый множитель в этих формулах не зависит i, он может быть использован одновременно для вычисления Δ'_{2t+1} различных последовательностей S_i. Деление заменяется умножением на каждом такте. Дополнительно требуется одна схема нахождения обратного элемента в поле Галуа.

Число инверсий, необходимых для обработки принятого слова, обратно пропорционально числу блоков, которые одновременно вычисляют Δ'_{2t+1}. Использование формул (3,4) значительно сокращает аппаратные затраты самого сложного блока декодера даже при небольшой степени распараллеливания.

В таблице 1 приводятся значения пропускной способности и аппаратной сложности модуля нахождения локаторов ошибок для РС-кода (204,188,8), используемого в DVB. Тактовая частота СБИС равняется 100 МГц.

IV. ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ КОРРЕКЦИИ ОШИБОК

Эффект от исправления дополнительных ошибок в словах различных кодов Рида-Соломона был исследован путем имитационного моделирования. Все эти коды определены над полем $GF(2^8)$, заданным полиномом $p(x) = x^8 + x^4 + x^3 + x^2 + 1$. При моделировании использовалась модель канала с Гауссовским шумом (AWGN) и модуляция BPSK.

На графике рисунка 3 приведены доли исправляемых конфигураций ошибок веса t+1 по отношению ко всем возможным конфигурациям ошибок этого веса для РС-кодов с различными длинами и минимальными кодовыми расстояниями. РС-коды различной длины получаются за счет укорочения базового РС-кода с n = 255.

Табл.1. Быстродействие и сложность реализации модуля нахождения (t+1) ошибки

p	Проп. спос. Мбит/с	RAM (ROM) бит	Число вент.
1	3.9	13088	2147
6	22.9	24864	6542
12	44.4	36896	11819
17	61.5	43808	16139

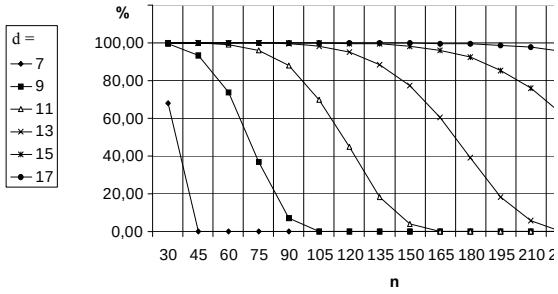

Рис.3. Процент исправляемых ошибок веса (t+1)

Таблица 2 показывает выигрыш от исправления дополнительной ошибки с использованием модифицированной процедуры декодирования для ряда РС-кодов, используемых в телекоммуникационных системах. Столбцы таблицы, обозначенные t, содержат значения BER (Bit Error Ratio) на выходе обычной процедуры декодирования, столбцы, обозначенные t+1, содержат значения BER на выходе модифицированной процедуры. В таблице 2 E_b/No обозначает отношение энергии сигнала на информационный бит к односторонней спектральной плотности шума.

При передаче данных на большие расстояния в волоконно-оптических сетях используется РС-код с параметрами (n=255, k=239, t=8). Для этого кода уровень ошибок на выходе декодера при использовании модифицированной процедуры декодирования уменьшается в 2,9 раза при E_b/No = 7.0 dB.

В стандарте DVB используется РС-код с параметрами (n=204, k=188, t=8). Для этого кода BER уменьшается в 4,6 раза при E_b/No = 7.0 dB.

В стандарте для сетей с беспроводным доступом IEEE 802.16 используется РС-код с параметрами (n=24, k=18, t=3). Для этого кода BER уменьшается в 4,2 раза при E_b/No = 7.4 dB

Результаты имитационного моделирования показывают, что эффект от исправления дополнительных ошибок возрастает при укорочении кода. В общем случае он увеличивается при уменьшении d при условии, что почти все ошибки веса t+1 остаются корректируемыми.

Табл.2. Значения BER на выходе обычного и предлагаемого РС-декодера

E_b/N_0 (dB)	BER (* - моделирование не завершилось)					
	(255,239) РС-код		(204,188) РС-код		(24,18) РС-код	
	t	t +1	t	t +1	t	t +1
6.2	4.14×10^{-4}	3.16×10^{-4}	2.49×10^{-4}	$9.28\cdot10^{-5}$	6.01×10^{-4}	2.88×10^{-4}
6.4	1.56×10^{-4}	8.83×10^{-5}	7.75×10^{-5}	$3.99\cdot10^{-5}$	3.77×10^{-4}	1.34×10^{-4}
6.6	4.20×10^{-5}	2.52×10^{-5}	2.15×10^{-5}	5.42×10^{-6}	1.88×10^{-4}	6.47×10^{-5}
6.8	1.08×10^{-5}	4.52×10^{-6}	5.46×10^{-6}	1.21×10^{-6}	1.06×10^{-4}	3.26×10^{-5}
7.0	2.24×10^{-6}	7.75×10^{-7}	9.18×10^{-7}	1.98×10^{-7}	5.77×10^{-5}	1.63×10^{-5}
7.2	*	*	*	*	2.40×10^{-5}	6.18×10^{-6}
7.4	*	*	*	*	1.24×10^{-5}	2.98×10^{-6}

V. ВЫВОДЫ

Усовершенствованная процедура декодирования позволяет повысить эффективность применения РС-кодов в телекоммуникационных системах. При этом не требуется изменять существующие стандарты. Предложенная архитектура модуля нахождения локаторов ошибок позволяет реализовать РС-декодер с небольшими аппаратными затратами.

Литература

1. Блейхут Р.Э. Теория и практика кодов, контролирующих ошибки: Пер. с англ. М.: Мир, 1986. – 576 с.

2. Egorov S., Markarian G., Pickavance K. A Modified Blahut Algorithm for Decoding Reed-Solomon Codes Beyond Half the Minimum Distance // IEEE Trans. on Commun., vol. 52, no. 12, December. 2004, pp. 2052-2056.

INCREASING OF REED-SOLOMON CODES EFFICIENCY IN COMMUNICATION SYSTEMS

Egorov S.

Kursk State Technical University

A Reed-Solomon (RS) code is described as an (n, k) code, where the codeword consists of n symbols from a Galois Field (GF) of q elements, k of which are information symbols. It is known that RS codes can correct any pattern of t errors or less iff $2t+1\le d$ (d - minimum distance). A procedure providing t+1 error correction for RS codes was developed by Blahut based on the Berlekamp-Massey (BM) algorithm. This procedure was improved recently by Egorov and Markarian. In this correspondence the RS decoder with modest hardware complexity based on the modified Blahut procedure is proposed. This decoder allows the coding gain of the RS codes to increase for communication systems.

First in this correspondence modified Blahut decoding procedure is described. This procedure provides correction of t+1 errors by analytical continuation of the BM algorithm through two more iterations.

Then new procedure for searching for unknown discrepancies is introduced. An architecture of a searcher for the unknown discrepancies is given. The mathematical foundation of this procedure is based on the following proposition.

Let α denotes primitive element of GF, $C_i = B^{(2t)}(\alpha^{-i})/\Lambda^{(2t)}(\alpha^{-i})$, $D_i = \Lambda^{(2t)}(\alpha^{-i})/ (B^{(2t)}(\alpha^{-i})\cdot\alpha^{-2i})$, where $\Lambda^{(2t)}(x)$ is the locator polynomial, $B^{(2t)}(x)$ is the auxiliary polynomial, obtained as the outputs of the Berlekamp-Massey algorithm after $2t$ iterations. Then following proposition will be true.

Proposition: If the degree of $\Lambda^{(2t)}(x)$ $L_{2t} = t$, then the sequences S_i of possible values of $\Delta'^{i,j}_{2t+1} = \Delta^{-1^{i,j}}_{2t+1}\cdot\alpha^{i}$ of modified Δ_{2t+1} obtained for the pairs of i and $j = i + k$ are given as follows:

$S_i = \{\, \Delta'^{i,k}_{2t+1} = (C_i - C_{i+k})\cdot(1-\alpha^{k})^{-1};\ k = 1,...,n\text{-}1\text{-}i;\ P(a^{-i-k}) \neq 0 \,\}$, $i = 1,...,\ n\text{-}1\text{-}t$, $P(a^{-i}) \neq 0$.