УДК 621.391.037.3

Г.М. Тамразян

СОВРЕМЕННЫЕ МЕТОДЫ АДАПТИВНОГО ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

***Тамразян Георгий Михайлович**, аспирант кафедры «Телекоммуникации» Ульяновского государственного технического университета. Инженер-исследователь ФНПЦ АО «НПО «Марс». Имеет статьи и изобретения в области помехоустойчивого кодирования. [e-mail: mars@mv.ru].*

Аннотация

В данной работе предлагаются оптимальные алгоритмы декодирования избыточных кодов с перестраиваемыми параметрами на примере кодов Рида-Соломона (РС).

Наиболее сложной и ресурсоемкой операцией при декодировании кодов РС является расчет полинома локаторов ошибки. Как правило, он осуществляется с помощью алгоритма iBM, который, однако, имеет такой недостаток, как сложная и нерегулярная структура. Попытки реализации данного алгоритма с динамически перестраиваемыми параметрами для адаптивных кодеков приводят к значительному усложнению декодера и увеличению времени прохождения критического пути.

Временные издержки при поиске полинома локаторов ошибки можно сократить за счет использования конвейерных и параллельных вычислений, а также приведения алгоритма по поиску полинома локаторов ошибки к регулярному виду. При грамотной компоновке решающих устройств и определенной модификации алгоритма iBM длину критического пути возможно сократить и ускорить его выполнение, а регулярная структура такого алгоритма делает возможным его использование в адаптивных системах. Регулярность структуры декодера достигается за счет приведения к общему виду блоков вычисления полинома локаторов ошибок и решения ключевого уравнения. В данной работе представлен способ формирования таких блоков и их использование в адаптивных системах кодирования.

Ключевые слова: коды Рида-Соломона (РС), коды Боуза-Чоудхури-Хоквингема (БЧХ), алгоритм Берлекемпа-Месси (БМА), RiBM, мягкое декодирование.

STATE-OF-THE-ART METHODS FOR ADAPTIVE NOISELESS CODING

***Georgii Mikhailovich Tamrazian,** Postgraduate Student at the Department of Telecommunications of Ulyanovsk State Technical University; Research Engineer of Federal Research-and-Production Center Joint Stock Company 'Research-and-Production 'Mars'; an author of articles and patents in the field of noiseless coding. e-mail: mars@mv.ru.*

Abstract

The article proposes some optimal algorithms of redundant codes decoding with configurable characteristics by the example of Reed-Solomon (RS) codes.

Error locator multinomial computing is one of the main complex and resource-intensive tasks in case of RS codes decoding. Generally, it can be computed with iBM algorithm. iBM have some disadvantages such as complex and irregular structure. Realization of the algorithm with dynamically configurable characteristics for adaptive codecs leads to the significant complexity of the decoder and increasing critical path.

Time costs on the errors costs multinomial search can be reduced with the use of pipeline and parallel computations. The error locator multinomial search algorithm can be also transformed to the regular form. In the context of an appropriate composition of resolvers and some modification of iBM algorithm, the critical path length can be decreased and the algorithm performance can be advanced. The regular structure makes the usage of the algorithms possible for adaptive systems. Decoder structure regularity can be achieved with the transformation of error locator multinominal computational blocks and key equation solution to the general form. The article considers the method of construction such blocks and their usage in adaptive coding systems.

Key words: Reed-Solomon codes, BCH Codes, Berlekamp-Massey algorithm, RiBM, PLIS.RiBM, soft decoding.

Введение

Развитие современных высокоскоростных систем мобильной связи требует динамического изменения информационной емкости канала связи в зависимости от помеховой обстановки. Возможность быстрой подстройки системы помехоустойчивого кодирования (СПК) под постоянно изменяющийся уровень шума в канале связи позволяет такой системе передавать данные на максимальной скорости при заданной достоверности приема. Существуют различные методы реализации адаптивной системы кодирования (АСК), наиболее простым из которых является предварительная подготовка набора кодеков с динамическим переключением между ними. Такой подход не всегда является оптимальным. При переходе с одного кода на другой изменять зачастую необходимо лишь некоторые параметры кода, поэтому гораздо более эффективным методом реализации АСК является динамическая перестройка только тех параметров кода, которые отвечают за его избыточность. Способы поиска и оптимизации таких алгоритмов зависят от вида используемых кодов. В данной работе приведен пример реализации АСК для недвоичных кодов Боуза-Чоудхури-Хоквингема (БЧХ).

Цель работы – оптимизация и унификация процедуры декодирования избыточных кодов с адаптирующимися параметрами на примере недвоичных кодов БЧХ.

Процедура декодирования кодов РС

Классический подход к реализации декодера кодов Рида-Соломона (РС), как правило, сводится к разработке трех основных арифметико-логических устройств (АЛУ):

1. SC-block (Syndrome Computation block). Блок расчета синдромного многочлена. Выполняет вычисления согласно формуле (1).

$$s_i = R(\alpha^i),$$

где $R(z)$ – полином принятых кодовых слов,

α – примитивный элемент поля Галуа.

2. KES-block (Key-Equation block). Блок, решающий ключевое уравнение:

$$\Lambda(z)\cdot S(z) = \Omega(z) \bmod z^{2\cdot t}, \quad (1)$$

где $\Lambda(z)$ – полином локаторов ошибки,

t – корректирующая способность кода.

3. CSEE-block (Chien Search and Error Evaluator block). Блок, выполняющий процедуру Ченя по поиску корней полинома локаторов ошибок путем последовательного перебора всех возможных значений и рассчитывающий значение ошибки согласно алгоритму Форни:

$$Y_j = -\frac{\Omega(z)}{\Lambda'(z)}\bigg|_{z=\alpha^{-j}},$$

где Y – значение ошибки,

$\Lambda'(z)$ – производная от полинома локаторов ошибки,

j – номер позиции в принятом векторе R, на которой произошла ошибка.

Наиболее сложной и ресурсоемкой операцией при данном подходе является расчет полинома локаторов ошибки $\Lambda(z)$. Таким образом, выбор оптимального алгоритма поиска полинома локаторов ошибки является актуальной задачей.

Расчет полинома локаторов ошибок (алгоритм iBM)

Наиболее эффективным, с точки зрения скорости обработки данных, алгоритмом поиска полинома локаторов ошибок считается алгоритм Берлекемпа-Месси (БМА). Его лучше всего рассматривать как итеративный процесс построения линейного сдвигового регистра с обратной связью [1, 2]. Позднее этот алгоритм был доработан, что позволило сократить длину сдвигового регистра до минимальной с сохранением требуемых свойств. Реализация обновленного алгоритма была описана Р. Блейхутом и получила название безинверсионного БМА (iBM). Основан iBM на единообразии расчетов полиномов $\Lambda(z)$ и $\Omega(z)$ через невязку δ^{-1} этих величин [3]. Таким образом, аппаратная реализация KES- блока сводится к разработке двух АЛУ:

- блока расчета невязок (Discrepancy Computation, DC-block),
- блока корректировки полинома локаторов ошибки (Error Locator Update, ELU-block).

Архитектура АЛУ, работающего согласно алгоритму iBM, представлена на рисунке 1.

При проектировании современных высокоскоростных

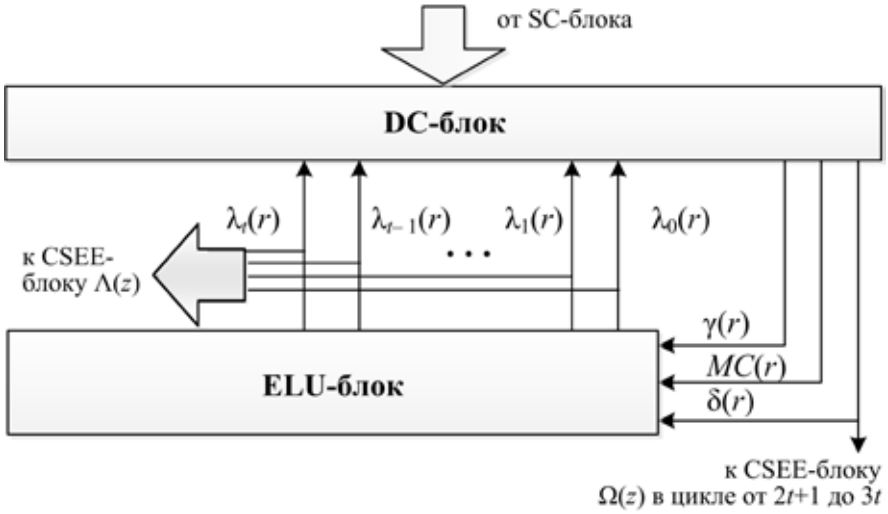

Рис. 1. Схема устройства, работающего по алгоритму iBM

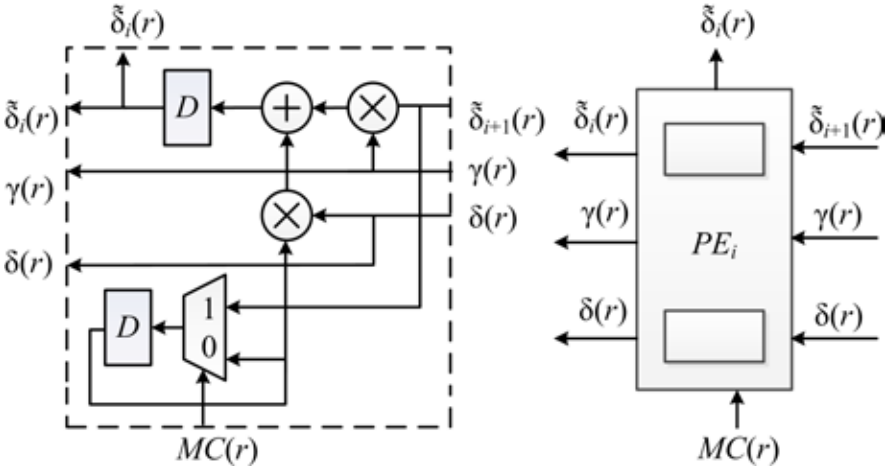

Рис. 2. Внутренняя схема блока PE

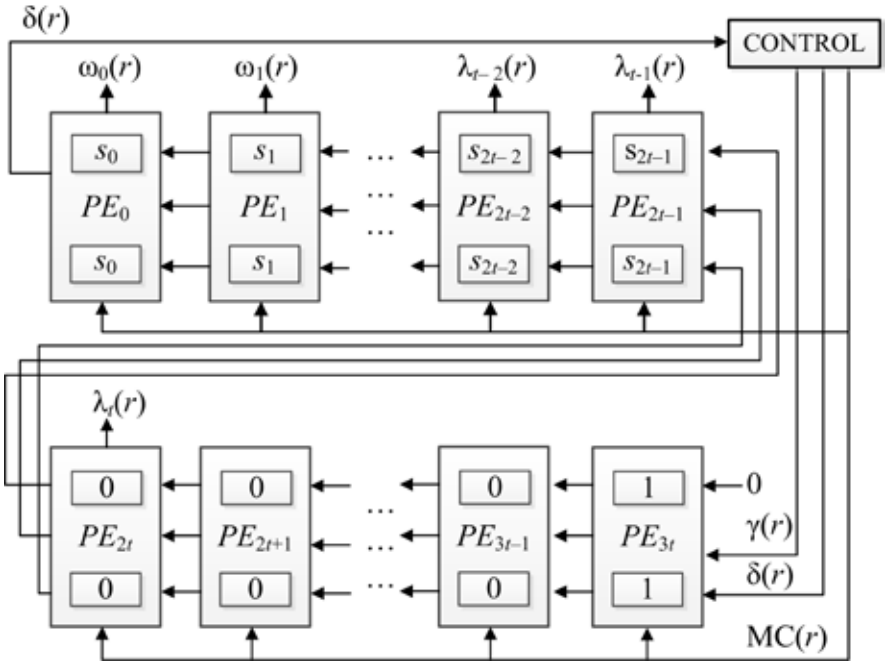

Рис. 3. Схема устройства, работающего по алгоритму RiBM

систем связи важным параметром является длина критического пути, то есть суммарное время, необходимое для выполнения всех требуемых операций в течение одного такта. Чем длиннее критический путь, тем меньшую тактовую частоту можно использовать для данного устройства и тем ниже скорость передачи информации. Критический путь при выборе iBM-архитектуры составляет более $2(T_{mult}+T_{add})$, где T_{mult} и T_{add} – время выполнения операции умножения и сложения в поле Галуа соответственно. Затрачивается на полный прогон этого алгоритма $3t$ тактов.

Оптимальный алгоритм поиска полинома локаторов ошибок (алгоритм RiBM)

Алгоритм iBM имеет сложную и нерегулярную структуру. Попытки реализации данного алгоритма с динамически перестраиваемыми параметрами для адаптивных кодеков приводят к значительному усложнению DC-блока и увеличению критического пути.

В настоящее время удалось значительно сократить временные издержки при поиске полинома локаторов ошибки за счет использования конвейерных и параллельных вычислений, а также привести алгоритм поиска полинома локаторов ошибки к регулярному виду. Подобная модификация алгоритма iBM получила название Reformulated iBM (RiBM). Длина критического пути для этого алгоритма составляет $T_{mult}+T_{add}$, и выполняется он всего за $2t$ тактов. Регулярность структуры алгоритма достигается за счет приведения к общему виду DC- и ELU-блоков [4]. Расчет компонентов необходимых полиномов происходит в специальных вычислительных блоках PE (Processor Element). Архитектура вычислителя PE представлена на рисунке 2. Построение сдвигового регистра длиной $3t$ на PE-блоках позволяет вычислить полином локаторов ошибок $\Lambda(z)$ и полином значений ошибок $\Omega(z)$ внутри одного АЛУ.

Архитектура устройства, работающего согласно алгоритму RiBM, пред-

ставлена на рисунке 3, где показано состояние регистров при стартовой инициализации. Спустя $2t$ тактов работы регистра в памяти вычислителей PE_0–PE_{t-1} будут содержаться коэффициенты полинома $\Omega(z)$, а в вычислителях PE_t–PE_{2t} – коэффициенты $\Lambda(z)$. Эти вычисления ведутся параллельно и не накладываются друг на друга.

Полное описание алгоритма RiBM выглядит следующим образом:

Инициализация:

$\delta_{3t}(0)=1;\ \delta_i(0)=0;$ для $i=2t,\ 2t+1,\ \ldots\ 3t-1.$

$\delta_i(0)=\theta_i(0)=s;$ для $i=0,\ 1,\ldots,\ 2t-1.$

$k(0)=0;\ \gamma(0)=1;$

for $r=0, r\le 2t-1, r=r+1.$

Шаг 1. $\delta_i(r+1)=\gamma(r)\cdot\delta_{i+1}(r)-\delta_0(r)\cdot\theta_i(r),$ $(i=0,\ldots,\ 3t)$

Шаг 2. **if** $\delta_0(r)\neq 0$ **and** $k(r)\ge 0$ **then**

$\theta_i(r+1)=\delta_{i+1}(r),\ (i=0,\ldots,\ 3t)$

$\gamma(r+1)=\delta_0(r)$

$k(r+1)=-[k(r)+1]$

else

$\theta_i(r+1)=\theta_i(r),\ (i=0,\ldots,\ 3t)$

$\gamma(r+1)=\gamma(r)$

$k(r+1)=k(r)+1$

Выход: $\lambda_i(2t)=\delta_{t+i}(2t),\ i=0,\ 1,\ldots,\ t$

$\omega_i(2t)=\delta_i(2t),\ i=0,\ 1,\ldots,\ t-1$

Блок CONTROL выполняет функции расчета регистров управления $\gamma(r)$ и $MC(r)$.

Подобная структура алгоритма позволяет динамически перестраивать его в зависимости от помеховой обстановки в канале связи. Для этого длина сдвигового регистра, представленного на рисунке 3, выбирается равной $3t_{max}$, где t_{max} – количество ошибок, исправляемых наиболее помехоустойчивым кодом из числа реализуемых кодеков внутри данной системы. Блок CONTROL управляет динамической перестройкой СПК за счет переключения связей внутри сдвигового регистра. При этом все основные параметры кодека, такие как: критический путь, аппаратные затраты, скорость работы – будут соответствовать параметрам наиболее избыточного кодека.

Реализация мягких методов декодирования для АСК

При разработке АСК необходимо постоянно оценивать помеховую обстановку в канале связи. Эти данные также удобно использовать при мягком декодировании [5], что поможет значительно повысить помехоустойчивость АСК с минимальным усложнением структуры декодера.

Для мягкого декодирования недвоичных кодов БЧХ необходимо знать многочлен локаторов стираний, вычисляемый следующим образом:

$$\Gamma(z)=\prod_{k=1}^{e}\left(1-z\cdot\alpha^{j_k}\right), \qquad (2)$$

где j_k – номер k-й стертой позиции.

Зная позиции стертых символов, можно вычислить полином $\Gamma(z)$ и подставить на эти позиции произвольные принятые символы, вычислив после этого синдромный многочлен $S(z)$. Такая подстановка может привести к появлению e дополнительных ошибок. Тогда ключевое уравнение (2) преобразуется в уравнение (3) [6]:

$$S(z)\cdot\Lambda(z)\cdot\Gamma(z)=\Omega(z)\bmod z^{2\cdot t}. \qquad (3)$$

Для аппаратной реализации данного алгоритма потребуется незначительная доработка существующей схемы декодера. SC-блок дополнится расчетом полинома локаторов стираний $\Gamma(z)$ согласно (2). В KES-блоке вместо многочлена $\Lambda(z)$ будет использоваться многочлен $\Lambda(z)\cdot\Gamma(z)=\Psi(z)$, степень которого в 2 раза больше, соответственно, увеличится и степень многочлена $\Omega(z)$, что приведет к необходимости увеличения длины сдвигового регистра, представленного на рисунке 3.

Заключение

Рассмотренный подход к реализации АСК позволяет оптимизировать процесс декодирования недвоичных кодов БЧХ, при этом сложность декодера всей системы остается равной сложности наиболее помехоустойчивого декодера и не зависит от числа кодеков, использованных в АСК. Кроме того, использование RiBM-архитектуры для расчета полинома локаторов ошибок позволяет сократить критический путь более чем в 2 раза, а время на выполнение БМА уменьшить в 1,5 раз. Рассмотренная организация процесса декодирования также удобна при работе в канале со стираниями. Использование мягкого декодирования в этом случае увеличивает аппаратные затраты на реализацию декодера незначительно.

СПИСОК ЛИТЕРАТУРЫ

1. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М. : Техносфера, 2005. – 320 с.

2. Скляр Б. Цифровая связь. Теоретические основы и практическое применение – Изд. 2-е, испр., пер. с англ. – М. : Издательский дом «Вильямс», 2003. – 1104 с.

3. Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М. : Мир, 1986. – 576 с.

4. Sarwate D.V., Shanbhag N.R. High-Speed Architectures for Reed-Solomon Decoders. IEEE transactions on VLSI Systems, 2001.

5. Гладких А.А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи. – Ульяновск : УлГТУ, 2010. – 379 с.

6. Кларк Дж., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи : пер. с англ. – М. : Радио и связь, 1987. – 382 с.

REFERENCES

1. Morelos-Zaragoza R. *Iskusstvo pomekhoustoichivogo kodirovaniia. Metody, algoritmy, primenenie* [The Art of Error Correcting Coding]. Moscow, Tekhnosfera Publ., 2005. 320 p.

2. Sklar Bernard. *Tsifrovaia sviaz. Teoreticheskie osnovy i prakticheskoe primenenie*. Izd. 2-e, ispr. per. s angl. [Digital Communication. Fundamentals and Applications. Second corrected Edition]. Moscow, Williams Publ., 2003. 1104 p.

3. Blahut R. *Teoriia i praktika kodov, kontroliruiushchikh oshibki* [Theory and Practice of Error Control Codes]. Moscow, Mir Publ., 1986. 576 p.

4. Sarwate D.V., Shanbhag N.R. High-Speed Architectures for Reed-Solomon Decoders. *IEEE Transactions on VLSI Systems*. 2001.

5. Gladkikh A.A. *Osnovy teorii miagkogo dekodirovaniia izbytochnykh kodov v stiraiushchem kanale sviazi* [Foundations of the Theory of Soft-Decision Decoding of Redundant Codes in Erasure Communication Channels]. Ulyanovsk, UlSTU Publ., 2010. 379 p.

6. Clark G., Cain J. *Kodirovanie s ispravleniem oshibok v sistemakh tsifrovoi sviazi*. Per. s angl. [Error-Correcting Coding for Digital Communication]. Moscow, Radio i sviaz Publ., 1987. 382 p.