

**О.Н. Дяченко** (канд.техн.наук, доц.), **И.В. Юрьев** (магистрант)  
Донецкий национальный технический университет  
do@cs.dgtu.donetsk.ua

## **КОМПАКТНОЕ ТЕСТИРОВАНИЕ ЦИФРОВЫХ УСТРОЙСТВ НА ОСНОВЕ КОДА РИДА-СОЛОМОНА**

Рассмотрена методика проектирования устройств компактного тестирования, приведен анализ характеристик кодов Рида-Соломона и описание работы устройства компактного тестирования на основе декодера кода Рида-Соломона.

**коды Рида-Соломона, циклические коды, кодер, декодер, коды БЧХ, поле Галуа, избыточность, перемежение, коды Хэмминга**

### ***Введение***

В связи с неуклонным ростом сложности и функциональной насыщенности цифровых устройств (ЦУ), а также необходимости проверки их технического состояния, методы компактного тестирования являются актуальными для решения задач тестовой диагностики ЦУ. Достоинством этих методов является значительное сокращение объема информации, необходимой для проведения тестового эксперимента. При традиционных методах компактного тестирования, контроль проводится по принципу "годен - не годен". При диагностике ЦУ важно определить момент времени, когда на выходе схемы появляется ошибка, то есть локализовать ошибку в выходной тестовой последовательности битов [1].

Существующие методы компактного тестирования с локализацией ошибок и реализующие их устройства основаны на кодах Хэмминга, кодах БЧХ, кодах Файра. Вместе с тем в теории и практике помехоустойчивого кодирования широко используются коды Рида-Соломона. Отсутствие устройств компактного тестирования, построенных на базе этих кодов, по-видимому, связано с тем, что подавляющее большинство публикаций написаны на языке высшей математики [2]. Наиболее полно рассматривается программная реализация помехоустойчивого кодирования с помощью кода Рида-Соломона, а аппаратная (построение кодера и декодера), как правило, либо вовсе не рассматривается, либо в недостаточном объеме.

Целью данной работы является разработка устройств компактного тестирования, построенных на основе кодов Рида-Соломона.

### ***Методика проектирования устройств компактного тестирования***

Методика проектирования устройств компактного тестирования (УКТ) подразумевает следующие этапы:

– анализ объекта диагностики: тип устройства (комбинационный, последовательностный, одновыводной или многовыводной); тип тестирования (зондовое, устройство встроенного контроля); объект диагностики исправный или заведомо неисправный, ошибки, вызванные перемежающимися неисправностями, постоянными неисправностями, случайными сбоями; характер распределения ошибок различной кратности;

– анализ тестовых воздействий: исчерпывающее тестирование (комбинационные схемы), псевдослучайное тестирование, синтезированные тесты, случайные тесты и др. Для синтезируемых тестов вероятность ошибки малой кратности максимальна. Для перемежающихся неисправностей вероятность одиночных ошибок максимальна. Для заведомо исправных объектов вероятность одиночного сбоя максимальна;

– выбор кода для реализации компактного тестирования. Для случайных сбоев и перемежающихся неисправностей достаточно выбрать код Хэмминга. Для постоянных неисправностей целесообразно использовать коды, исправляющие пакеты ошибок (коды Файра или коды Рида-Соломона). Все эти коды относятся к блоковым кодам. Древовидные коды для этих целей неприменимы. Кроме того, неприменимы для этих целей такие коды, как, например, турбо-коды. Хотя они и являются блоковыми, для них используются методы кодирования, разработанные для древовидных кодов;

– разработка УКТ на основе циклических блоковых кодов. Основа УКТ — декодер выбранного кода без буферного регистра не конвейерной реализации. Для локализации ошибок используется счётчик. Перед сжатием тестовых реакций эталонная сигнатура загружается в генератор синдрома. В некоторых случаях не для укороченных кодов целесообразна альтернативная реализация генератора синдрома (схема деления полинома с внешними сумматорами в цепях обратной связи). В зависимости от длины теста используются декодеры для укороченных или неукороченных кодов;

– получение эталонных компактных оценок. Эталонные компактные оценки рассчитываются либо аналитически, либо формируются с помощью заведомо исправного устройства и генератора синдрома выбранного кода. Загрузка эталонной последовательности в УКТ может производиться либо параллельным, либо последовательным способом, как до начала тестирования, так и после, главное чтобы выполнялся принцип суперпозиции, то есть, при совпадении компактных оценок результат посимвольного сложения равен нулю, а при несовпадении отличен от нуля.

– анализ характеристик различных реализаций кодов. Ниже приводится анализ характеристик на примере кодов Рида-Соломона.

### ***Анализ характеристик кодов Рида-Соломона***

Для устройств компактного тестирования важны такие характеристики, как корректирующие способности кода, избыточность кода, скорость кода.

Порождающий полином кода Рида-Соломона, исправляющего  $s$  ошибок, должен содержать  $2s$  корней:

$$\{\alpha_0^j, \alpha_0^{j+1}, \alpha_0^{j+2}, \dots, \alpha_0^{j+2s-1}\},$$

где  $j_0$  – конструктивный параметр.

Как правило,  $j_0$  выбирают равным 1. Тогда множество корней полинома принимает вид  $\{\alpha, \alpha^2, \alpha^3 \dots \alpha^{2s}\}$ .

Для кода Рида-Соломона, исправляющего  $s$  ошибок, порождающий полином имеет следующий вид:

$$RS(X) = (X - \alpha)(X - \alpha^2)(X - \alpha^3) \dots (X - \alpha^{2s}),$$

При таком представлении порождающий полином имеет множество корней  $\{\alpha, \alpha^2, \alpha^3 \dots \alpha^{2s}\}$ .

Сущность помехоустойчивого кодирования заключается во введении в первичные коды избыточности. Поэтому помехоустойчивые коды называют избыточными. Задача помехоустойчивого кодирования заключается в таком добавлении к информационным символам первичных кодов дополнительных символов, чтобы в приемнике информации могли быть найдены и исправлены ошибки. Формула вычисления избыточности имеет вид:  $R=p/n$ , где  $p$  — количество проверочных символов,  $n$ —длина кода. Значение  $p$  вычисляется по следующей формуле  $p=\deg RS(X)=2*s$ .

Длина исправляемого пакета ошибок для последовательного кода без каких-либо ограничений равна  $t=j*b-(b-1)$  для посимвольно перемеженного кода Рида-Соломона поля Галуа  $GF(2^b)$  с параметром перемежения  $j$ .

Схему посимвольно перемеженного кода Рида-Соломона можно получить из схемы исходного кода, вставив дополнительно к каждому элементу памяти  $j-1$  элементов. Например, для поля  $GF(2^3)$  при перемежении с параметром  $j=2$  каждую триаду элементов памяти нужно заменить двумя последовательно включенными триадами.

Чтобы из  $(n, k)$ -кода получить  $(jn, jk)$ -код, выберем из исходного кода  $j$  произвольных кодовых слов и укрупним кодовые слова, чередуя их символы. Если исходный код исправлял произвольный пакет ошибок длины  $d$ , то, очевидно, результирующий код будет исправлять все пакеты ошибок длины  $jd$ . Например, применяя метод перемежения к четырём копиям  $(31, 25)$ -кода, исправляющего пакет ошибок длины 2, получаем  $(124, 100)$  – код, который может исправлять пакет ошибок длины 8 [3].

Предположим, что исходный код порождается полиномом  $g(X)$ . Тогда порождающий полином получаемого перемежением кода равен  $g(X^j)$ . Заметим, что перемежение символов нескольких информационных полиномов с последующим умножением на  $g(X^j)$  даёт то же самое кодовое слово, что и умножение каждого из исходных информационных полиномов на  $g(X)$  с последующим перемежением этих слов  $(n, k)$ -кода.

Избыточность кода и его скорость зависит, прежде всего, от количества исправляемых ошибок, которое задаётся при построении кода.

Для изменения избыточности кода применяют такие подходы:

- 1) изменение параметра  $b$  поля Галуа  $(2^b)$ , на основе которого строится код;
- 2) метод посимвольного перемежения кодов.

Вначале рассмотрим параметры кодов в символах элемента поля Галуа  $GF(2^b)$ .

Для  $s=1$ :  $p=2$ ,  $n=2^b - 1$ ,  $R=p/n=2/(2^b - 1)$ .

Исправляется один  $b$ -битный символ. Чем больше  $b$ , тем меньше избыточность, следовательно, больше скорость кода. Корректирующие возможности и аппаратные затраты увеличиваются.

Для  $s=2$ :  $p=4$ ,  $n=2^b - 1$ ,  $R=p/n=4/(2^b - 1)$ . Избыточность в 2 раза больше, чем для  $s=1$ .

Исправляются два  $b$ -битных символа, расположенных в любых двух символах из кодового слова длины  $2^b - 1$ .

Чем больше  $b$ , тем меньше избыточность, следовательно, больше скорость кода.

Корректирующие возможности увеличиваются в  $C_2^n$  раз (по сравнению с  $s=1$ ), а аппаратные затраты увеличиваются незначительно, так как длина кода  $n$  одинакова для  $s=1$  и  $s=2$ . Однако скорость кода в 2 раза меньше, поскольку избыточность кода  $R$  в 2 раза больше.

Рассмотрим избыточность и корректирующие возможности кодов в символах двоичной последовательности  $b$ -битов (применение кодов Рида-Соломона для исправления пакетов ошибок).

Для случая с ограничением характера расположения ошибок получаем такой же результат, как рассмотренный ранее для символов элементов поля Галуа ( $2^b$ ).

Для произвольного расположения пакетов ошибок: для  $s=1$  длина исправляемого пакета  $t=1$  (всего 1 бит). Это можно пояснить следующим образом. При длине пакета  $t=2$  в наихудшем случае один искаженный бит может оказаться в одном принятом символе кодового слова ( $b$  – двоичных символов), а второй – в другом соседнем символе, что равносильно двойной ошибке для кодов Рида-Соломона. Поскольку код построен для исправления одиночной ошибки, то рассмотренная ошибка неисправима.

В случае кодов Рида-Соломона, исправляющего две ошибки ( $s=2$ ) длина произвольного расположенного исправляемого пакета ошибок  $t=b+1$ . Это объясняется тем, что в наихудшем случае при  $t=b+2$  один искаженный бит может оказаться в одном символе кодового слова ( $b$  – двоичных символов),  $b$  искаженных двоичных битов – во втором символе, и еще один искаженный бит – в третьем символе. Таким образом, получили тройную ошибку, которую декодер кода Рида-Соломона не сможет исправить, поскольку построен для кода, исправляющего двойную ошибку. Вместе с тем, любой пакет ошибок искаженных битов длины  $t=b+1$  не сможет расположиться в трех соседних символах принятого кодового слова кода Рида-Соломона. Поэтому, он будет исправим.

Таким образом, для одиночного исправляемого пакета максимальной длины увеличение  $b$  для  $s=1$  нерационально; для  $s=2$  увеличение длины исправляемого пакета незначительно по сравнению с методом перемежения.

Поэтому применение кодов Рида-Соломона, исправляющих одиночные ошибки, для исправления пакетов ошибок рационально только в случае их посимвольного перемежения.

Для произвольного расположения пакетов ошибок максимальной длины: для  $s=1$   $t=j*b-(b-1)$ ; для  $s=2$   $t=2*(j*b-(b-1))$ , где  $j$  — параметр перемежения. Как видно из приведенных выражений зависимости длины исправляемого пакета ошибок, для обоих вариантов кода Рида-Соломона, допускающих синдромное декодирование, она значительно зависит не только от параметра перемежения  $j$ , но также от параметра  $b$  поля Галуа  $GF(2^b)$ .

Избыточность  $R=j*p/j*n=p/n$  — не изменяется, следовательно, скорость кода также не изменяется, аппаратные затраты возрастают в  $j$  раз.

При посимвольном перемежении для  $s=1$  появляются, а для  $s=2$  увеличиваются дополнительные возможности исправления множественных пакетов ошибок. Однако при построении кодов следует ориентироваться на максимальную длину гарантированно исправляемого пакета ошибок, поскольку в большинстве случаев ошибки сгруппированы в одиночные пакеты.

### ***Описание работы функциональной схемы УКТ***

Наиболее естественным для УКТ, построенного на основе кода Рида-Соломона (рис. 1), является определение ошибочного вектора в выходной тестовой реакции многовыходной тестируемой схемы (если использовать посимвольное перемежение — пакета ошибочных векторов). Однако такие устройства можно использовать и для локализации пакетов ошибок последовательности двоичных символов. Для этого необходимо преобразовать последовательный код в параллельный.

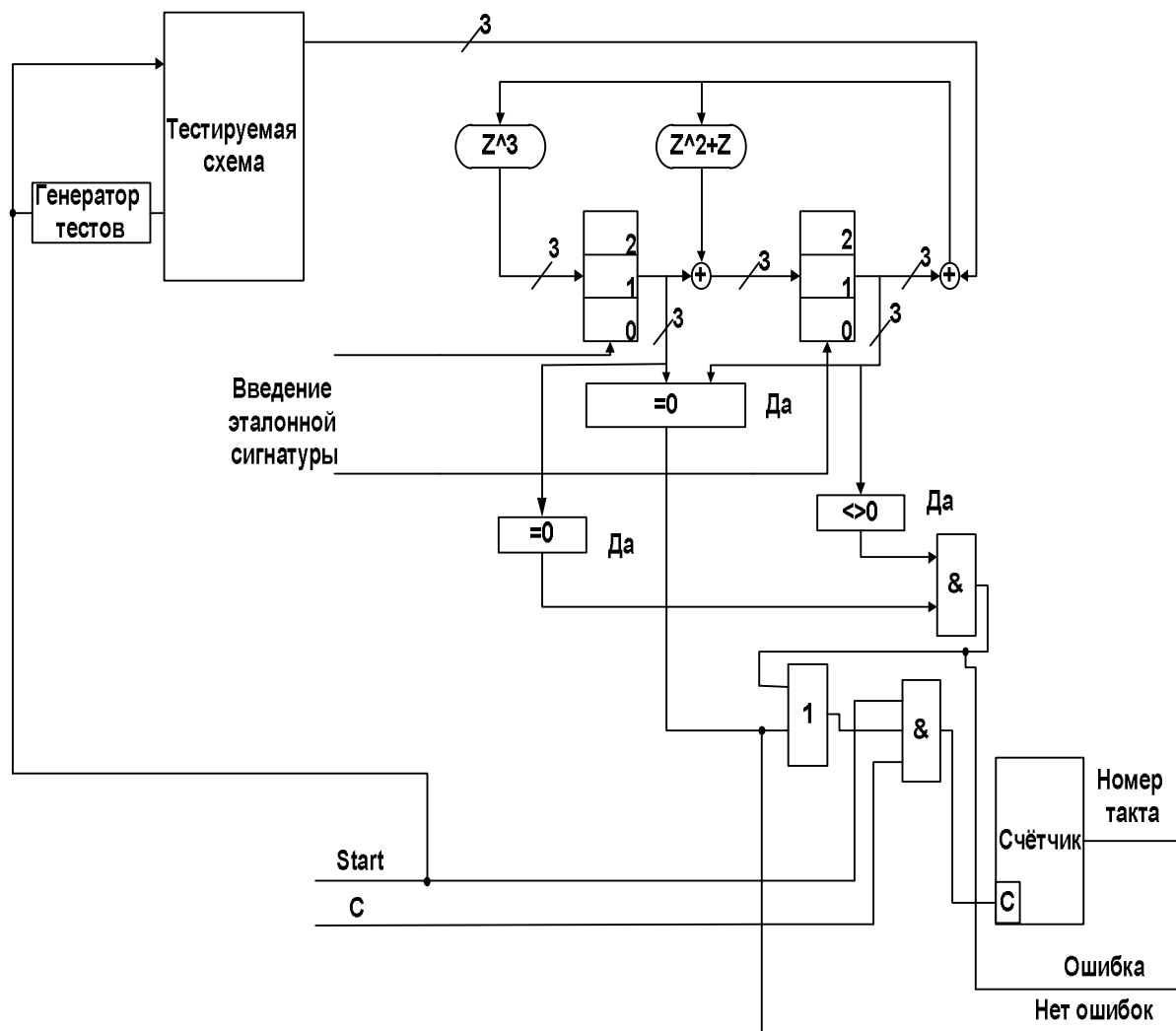


Рисунок 1 — Функциональная схема многовходового УКТ, построенного на основе декодера кода Рида-Соломона для поля Галуа GF(8)

Работа схемы на рисунке 1 начинается с ввода эталонной сигнатуры в элементы памяти генератора синдрома Рида-Соломона, затем по сигналу Start запускается генератор тестов и тестируемая схема. Генератор тестов посылает тестовую последовательность на тестируемую схему. Реакция тестируемой схемы подаётся на генератор синдрома Рида-Соломона, где происходит деление на порождающий полином и посимвольное сложение с эталонной сигнатурой. Затем происходит проверка битов с генератора синдрома Рида-Соломона на нуль, если да (все нули), то выдаётся сигнал “нет ошибок”. Иначе, при обнаружении в одном блоке элементов памяти нулевого значения, а в другом ненулевого в таком порядке, как показано на схеме, выдаётся сигнал об ошибке и счётчик прекращает свою работу на номере того такта, на котором произошла ошибка.

## **Выводы**

Эффективность применения кодов для целей компактного тестирования следует сравнивать по следующим показателям. Во-первых, число проверочных символов  $n-k$  кода должно быть минимальным, в этом случае длина сигнатуры и аппаратные затраты также будут минимальными. Во-вторых, длина кода  $n$ , соответствующая длине анализируемой последовательности, должна быть достаточно большой (чтобы обеспечить требуемую достоверность результатов тестового эксперимента). Преимуществом устройств компактного тестирования, построенных на основе кода Рида-Соломона, по сравнению с аналогичными на основе кода Файра, является возможность их применения для тестирования многовыходных устройств, а также для локализации многократных пакетов ошибок.

## **Список литературы**

1. Дяченко О.Н. Компактное тестирование запоминающих устройств с локализацией пакетов ошибок / О.Н. Дяченко // Электрон. моделирование.- 1996. №6.- С.43-48.
2. Крис Касперски. Могущество кодов Рида-Соломона или информация, воскресшая из пепла / Крис Касперски // [Электронный ресурс] — Режим доступа: [www.insidepro.com/kk/027/027r.shtml](http://www.insidepro.com/kk/027/027r.shtml)
3. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р.Блейхут; пер. с англ. - М.: Мир, 1986. - 576 с.

*Надійшла до редколегії: 12.09.2010*

*Рецензент: канд.техн.наук, доц. Зінченко Ю.Є.*

**О.М. Дяченко, І.В. Юр'єв**

Донецький національний технічний університет

**Компактне тестування цифрових пристроїв на основі коду Ріда-Соломона.** Розглянута методика проектування пристроїв компактного тестування, наведено аналіз характеристик кодів Ріда-Соломона та опис роботи пристрою компактного тестування на основі декодера коду Ріда-Соломона.

**коди Ріда-Соломона, циклічні коди, кодер, декодер, коди BCH, поле Галуа, надлишковість, перемежування, коди Хеммінга**

**O.N. Dyachenko, I.V. Yur'ev**

Donetsk National Technical University

**Compact Testing of Digital Devices Based on Reed-Solomon Code.** Designing technique for devices of the compact testing, the analysis of the characteristics of Reed-Solomon codes and the description of the device compact testing based on the decoder of Reed-Solomon code is considered.

**Reed-Solomon codes, cyclic codes, encoder, decoder, BCH codes, Galois field, redundancy, interleaving, Hamming codes**