

УДК 681.3

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

## **ВЛИЯНИЕ ПАРАМЕТРОВ КОДА РИДА-СОЛОМОНА НА ИЗБЫТОЧНОСТЬ КОДА**

Рассмотрено влияние параметров кодов Рида-Соломона на избыточность, корректирующие возможности и скорость кодов, а также на аппаратные затраты их реализации.

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

### ***Введение***

При проектировании современных систем коммуникаций одной из важнейших является задача обеспечения высокой достоверности передачи информации, а также её хранение и обработка. Для обеспечения помехоустойчивости информации применяют коды, обнаруживающие и исправляющие ошибки, возникающие в ходе работы системы и её элементов.

Коды Рида-Соломона — циклические коды, позволяющие исправлять ошибки в блоках данных. Элементами кодового слова являются не биты, а группы битов (блоки). В настоящее время широко используются коды Рида-Соломона для космической связи NASA, цифрового телевидения высокого разрешения (формат HDTV), в системах восстановления данных с компакт-дисков, в контроллерах оперативной памяти, в модемах, в жестких дисках, при создании архивов с информацией для восстановления в случае повреждений и т.д. [1-2]. А также они не исчерпали свои возможности и преимущества и в других приложениях, таких, как например, задачи криптографии, устройствах компактного тестирования и т.д.

Вместе с тем, несмотря на известные схемотехнические решения построения кодов, а также кодирующих и декодирующих устройств, их реализующих, информация о них - платная. Например – исправление ошибок в CD дисках.

Популярность этих кодов заключается в высоких корректирующих возможностях - исправление пакетов и множественных пакетов ошибок.

Данная работа посвящена рассмотрению влияния параметров кода Рида-Соломона на избыточность кода.

## **Порождающие полиномы кодов Рида-Соломона**

Коды Рида-Соломона являются частным случаем кодов БЧХ. Главное отличие кодов Рида-Соломона заключается в том, что в качестве символа выступает не двоичный символ (один бит), а элемент поля Галуа (несколько битов).

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

$$\{\alpha_0^{j_0}, \alpha_0^{j_0+1}, \alpha_0^{j_0+2}, \dots, \alpha_0^{j_0+2s-1}\},$$

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, возникающие под действием помех при передаче кодов по каналам связи. 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]. Для циклических кодов метод перемежения приводит к циклическим кодам.

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.

### **Влияние параметров кодов Рида-Соломона на избыточность**

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. Зависимость избыточности кода от его параметров представлены в таблице 1 и на рисунке 1.

Таблица 1. Зависимость параметров кода и избыточности кода при постоянном значении  $s=1$

| GF      | $p$ | $n$ | $R$   |
|---------|-----|-----|-------|
| GF(4)   | 2   | 3   | 0,67  |
| GF(8)   | 2   | 7   | 0,29  |
| GF(16)  | 2   | 15  | 0,13  |
| GF(32)  | 2   | 31  | 0,065 |
| GF(64)  | 2   | 63  | 0,032 |
| GF(128) | 2   | 127 | 0,016 |
| GF(256) | 2   | 255 | 0,008 |

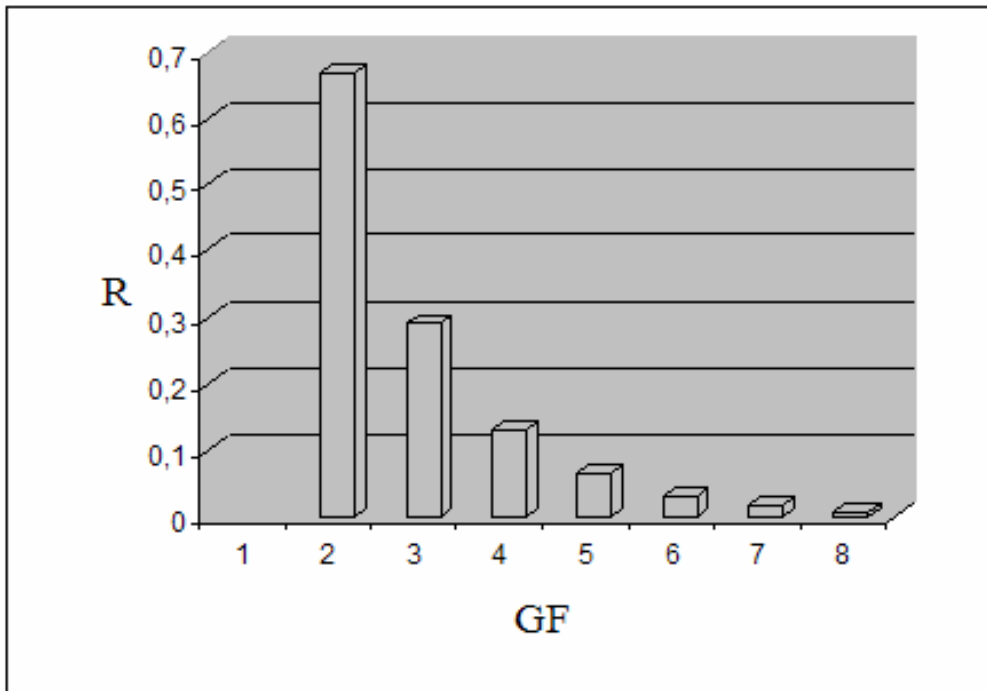


Рисунок 1 - Диаграмма зависимости изменения параметров поля Галуа на избыточность кода

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  $s=1$  не рационально; 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, в особенности, на носителях информации (радиальные царапины на CD-дисках, дефекты в запоминающих устройствах и др.), ошибки сгруппированы в одиночные пакеты.

На рисунке 2-5 представлены примеры схемной реализации декодеров кодов Рида-Соломона с полем Галуа  $GF(8)$  и  $GF(16)$ , исправляющих одиночные или двойные ошибки (параметры  $s=1$  и  $s=2$ ), без перемежения и с параметром перемежения  $j=2$  при  $s=2$ .

Кодеры для соответствующих кодов аналогичны по построению декодерам кодов Рида-Соломона, а также кодерам циклического кода Хэмминга и кодерам кода BCH.

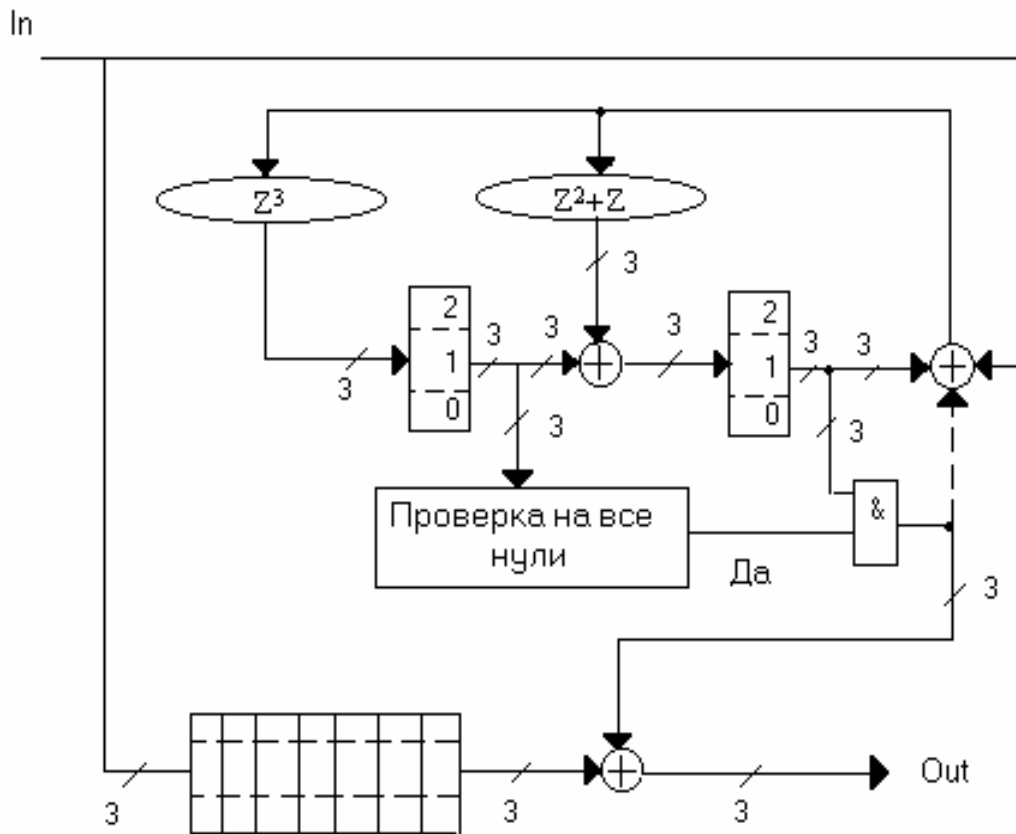


Рисунок 2 - Декодер кода Рида-Соломона для поля Галуа GF(8) при s=1

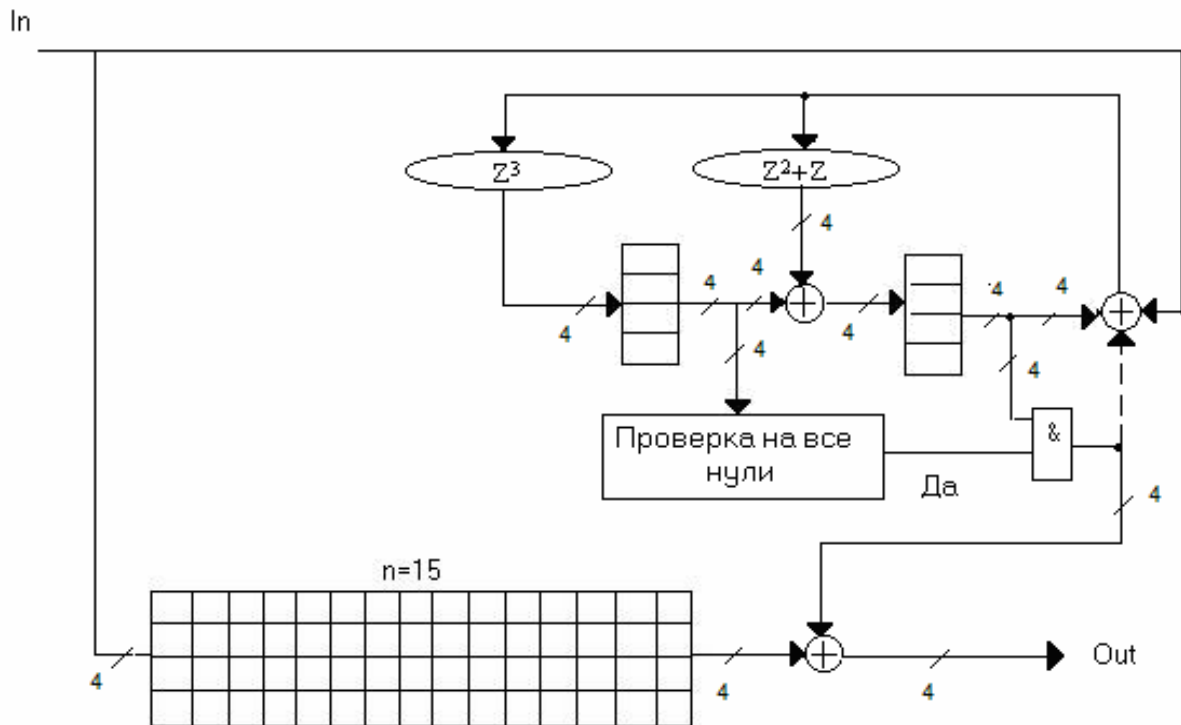


Рисунок 3 - Декодер кода Рида-Соломона для поля Галуа GF(8) при s=1

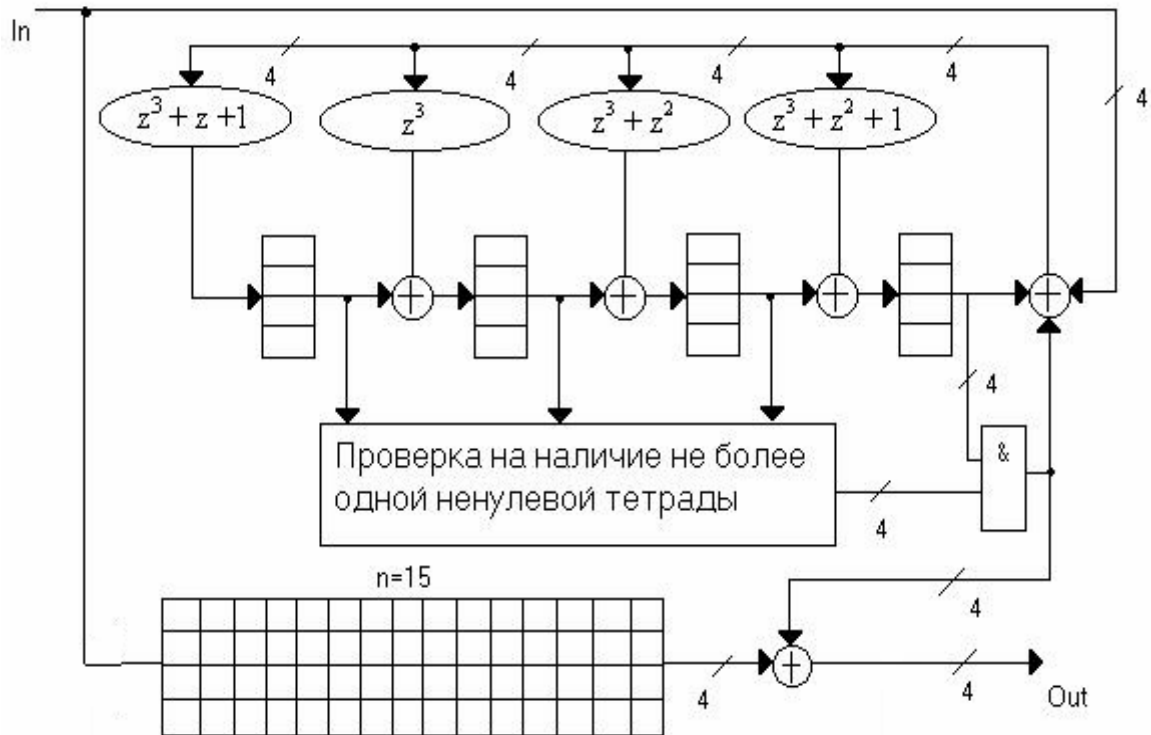


Рисунок 4 - Декодер кода Рида-Соломона для поля Галуа GF(16) при  $s=2$

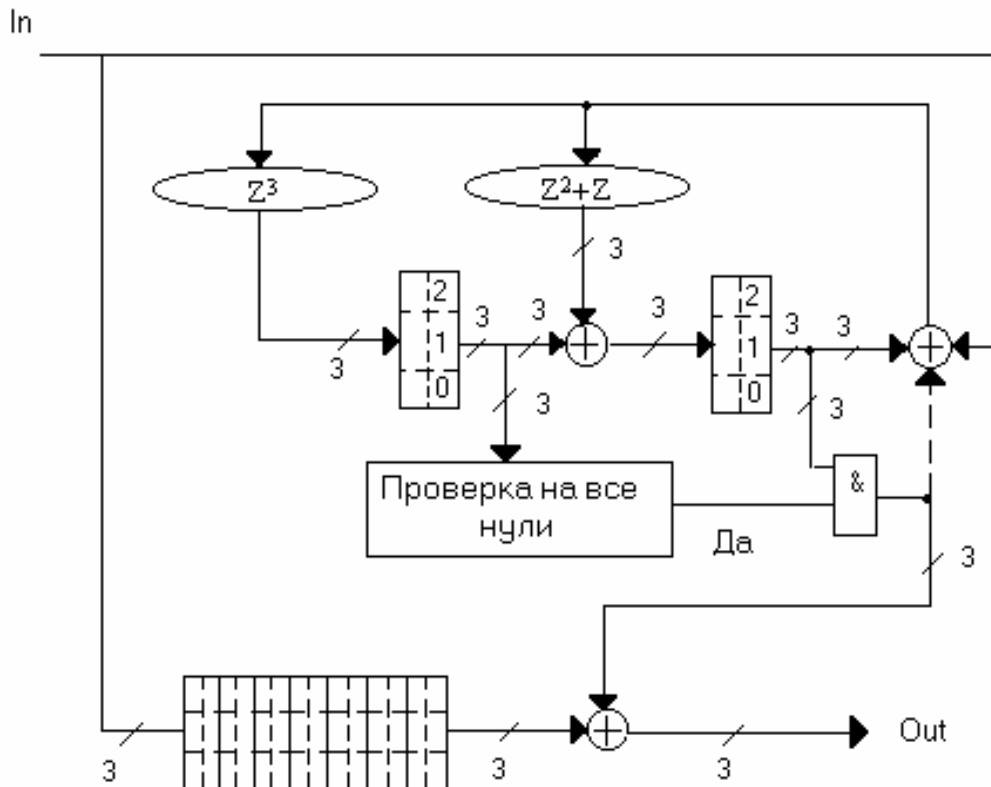


Рисунок 5 - Декодер кода Рида-Соломона для поля Галуа GF(8) и  $j=2$

## **Выводы**

Применение кодов Рида-Соломона, исправляющих одиночную ошибку, для исправления пакетов ошибок рационально только в случае их посимвольного перемежения.

Увеличение параметра  $b$  поля Галуа  $GF(2^b)$ , на основе которого строится код Рида-Соломона, уменьшает избыточность. Метод посимвольного перемежения не изменяет избыточность кода.

При перемежении для кодов Рида-Соломона, исправляющих одиночную ошибку, появляются, а для кодов Рида-Соломона, исправляющих двойную ошибку, увеличиваются дополнительные возможности исправления множественных пакетов ошибок. Однако при построении кодов следует ориентироваться на максимальную длину гарантированно исправляемого пакета ошибок.

## **Список литературы**

1. Robert H. Morelos-Zaragoza. The Art of Error Correcting Coding. First Edition, John Wiley & Sons, 2002. – 221p.
2. Код Рида-Соломона. Википедия, свободная энциклопедия. Электронный ресурс. Режим доступа: [http://ru.wikipedia.org/wiki/Код\\_Рида\\_—\\_Соломона](http://ru.wikipedia.org/wiki/Код_Рида_—_Соломона)
3. Richard E. Blahut. Theory and Practice of Error Control Codes. Addison-Wesley Publishing Company, Massachusetts, 1984. – 576p.

*Надійшла до редколегії 28.09.2009р. Рецензент: к.т.н., доц. Зінченко Ю.Є.*

**О.М. Дяченко, І.В. Юр'єв**

Донецький національний технічний університет

**Вплив параметрів коду Ріда-Соломона на надлишковість коду.** Розглянутий вплив параметрів кодів Ріда-Соломона на надлишковість, коригувальні можливості і швидкість кодів, а також на апаратні витрати та їх реалізацію.

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

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

Donetsk National Technical University

**Influence of parameters of Reed–Solomon code on redundancy.** Influence of parameters of Reed-Solomon codes on redundancy, correcting possibilities and speed of codes, and also on hardware and their implementation is considered.

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