УДК 621.396

# Упрощение кодера Рида – Соломона при использовании альтернативных простых полиномов, образующих расширения полей Галуа

Д. В. Клейко, Н. В. Лямин

В работе показаны возможные выигрыши при аппаратной реализации кодера Рида – Соломона, выраженные в количестве логических элементов, которые не требуются в упрощённой схеме. Основа упрощения – использование альтернативных простых образующих полиномов для получения изоморфных расширений поля Галуа GF(2) и вариации различных целочисленных представлений порождающих многочленов кода Рида – Соломона.

*Ключевые слова:* коды Рида – Соломона, полный умножитель, поля Галуа, порождающие многочлены.

## 1. Введение

В современных системах передачи информации помехоустойчивое кодирование играет далеко не последнюю роль, в частности, коды Рида – Соломона. На настоящий момент коды РС имеют очень широкую область применения благодаря их способности обнаруживать и исправлять пакеты ошибок. Они используются при записи и чтении в контроллерах оперативной памяти, при архивировании данных, записи информации на жёсткие, CD/DVD диски. Процессам их кодирования и декодирования посвящено много работ различных авторов. Коды Рида – Соломона строятся в расширениях полей Галуа GF($2^m$), где $m$ – максимальная степень простого полинома, образующего поле. Операции в полях Галуа во многом отличаются от привычных, поэтому их выполнение связано с определёнными сложностями. Ввиду этого актуальны предложения по упрощению аппаратной реализации кодеков Рида – Соломона. В работе показан выигрыш, возможный при аппаратной реализации кодера, выраженный в количестве логических элементов, в случае использования альтернативных простых полиномов для получения полей Галуа и различных целочисленных представлений порождающих многочленов кода Рида – Соломона.

## 2. Коды Рида – Соломона: образование порождающего многочлена

Коды Рида – Соломона – важное и широко используемое подмножество кодов БЧХ, которые примечательны способностью исправлять пакеты ошибок. Это объясняется тем, что коды Рида – Соломона строятся в расширениях полей Галуа GF($2^m$), где $m$ – максимальная степень простого полинома, образующего поле. Построение кодов Рида – Соломона мало отличается от построения двоичных кодов БЧХ и сводится к определению производящего многочлена. Порождающий многочлен кода образуется по правилу

$$(x-\alpha^{j})(x-\alpha^{j+1})(x-\alpha^{j+2})\cdots(x-\alpha^{j+2t-1}),$$

где $j$ может изменяться в пределах от 1 до $2^m-1$, $2t=k-n$ – количество избыточных символов, $\alpha$ – примитивный элемент поля GF($2^m$). Так, для одного и того же кода порождающий многочлен в целочисленном представлении может отличаться для разных значений параметра $j$ и разных простых полиномов, образующих расширение поля GF($2^m$). В связи с этим в [2] говорится о том, что выбирать можно любое значение $j$, но с помощью разумного выбора $j$ иногда удаётся упростить кодер. За счёт чего и в чём можно добиться упрощения?

## 3. Поиск порождающих многочленов

В аппаратной реализации кодера присутствуют умножители. В них коэффициенты порождающего многочлена в целочисленном представлении, которые являются числами в расширении поля GF($2^m$), умножаются на поступающие информационные символы. Коэффициенты записываются в ячейки памяти в двоичном коде, причём требуется $m$ ячеек для записи одного. Так, для расширения GF(256) коэффициенты многочлена могут являться числами от 0 до 255, поэтому требуется по 8 ячеек памяти для записи каждого из коэффициентов в двоичной форме. Однако при изменении параметра $j$ для разных простых полиномов можно найти такие коэффициенты, что все из них находятся в меньшем расширении поля GF(2), по сравнению с тем, в котором строится код. Следовательно, при реализации кодера требуется меньшее количество ячеек памяти для записи образующего многочлена, а также упрощается аппаратная реализация умножителя. Ниже приведены возможные простые полиномы, образующие расширения полей Галуа GF(8), GF(16), GF(32), GF(64), GF(128), GF(256). Причём здесь в качестве основного простого полинома полагается примитивный полином, наиболее часто используемый в реализациях кодов Рида – Соломона (для GF(8) – $x^3+x+1$, для GF(16) – $x^4+x+1$, для GF(256) – $x^8+x^4+x^3+x^2+1$), в качестве альтернативных полиномов – все остальные возможные.

Расширение GF(8): 11, 13.

Расширение GF(16): 19, 25.

Расширение GF(32): 37, 41, 47, 55, 59, 61.

Расширение GF(64): 67, 91, 97, 103, 109, 115.

Расширение GF(128): 137, 145, 157, 167, 171, 185, 191, 193, 203, 211, 213, 229, 239, 241, 247, 253.

Расширение GF(256): 285, 299, 301, 333, 351, 355, 357, 361, 369, 391, 397, 425, 251, 463, 487, 501.

Для кодов, представленных в [3], найдём порождающие многочлены такие, чтобы коэффициенты в целочисленном представлении находились в меньшем расширении, чем то, в котором строится код.

Приведём пример расчёта для кода (7,5) в расширении GF(8). Порождающий многочлен для полинома $x^3+x+1$ и

$$j=1\ \ (x-\alpha^{1})(x-\alpha^{2})=x^2+\alpha^2x+\alpha x+\alpha^3=x^2+\alpha^4x+\alpha^3=x^2+6x+3,$$

для полинома $x^3+x^2+1$

$$j=2\ \ (x-\alpha^{2})(x-\alpha^{3})=x^2+\alpha^3x+\alpha^2x+\alpha^5=x^2+\alpha^0x+\alpha^5=x^2+x+3;$$

коэффициенты можно реализовать с помощью двух двоичных элементов вместо трёх элементов. Результаты расчётов, полученных аналогичным способом, приведём в табл. 1.

Таблица 1. Порождающие многочлены с коэффициентами в меньшем расширении поля

| Код | Образующий полином | Значение параметра $j$ | Порождающий многочлен |
|---|---|---|---|
| (7,3) | $x^3+x+1$ | 1 | $x^4+3x^3+x^2+2x+3$ |
| | ---- | ---- | ------ |
| (15,13) | $x^4+x+1$ | 1 | $x^2+6x+8$ |
| | $x^4+x+1$ | 15 | $x^2+3x+2$ |
| (15,11) | $x^4+x+1$ | 1 | $x^4+13x^3+12x^2+8x+7$ |
| | $x^4+x^3+1$ | 10 | $x^4+2x^3+7x^2+5x+2$ |
| (31,29) | $x^5+x^2+1$ | 1 | $x^2+6x+8$ |
| | $x^5+x^2+1$ | 31 | $x^2+3x+2$ |
| (31,27) | $x^5+x^2+1$ | 1 | $x^4+30x^3+6x^2+9x+17$ |
| | $x^5+x^2+1$ | 13 | $x^4+5x^3+14x^2+8x+11$ |
| (31,25) | $x^5+x^2+1$ | 1 | $x^6+17x^5+26x^4+30x^3+27x^2+30x+24$ |
| | $x^5+x^2+1$ | 2 | $x^6+7x^5+7x^4+11x^3+12x^2+9x+11$ |
| (63,55) | $x^6+x+1$ | 1 | $x^8+55x^7+61x^6+37x^5+48x^4+47x^3+20x^2+6x+22$ |
| | $x^6+x^5+1$ | 54 | $x^8+22x^7+4x^6+27x^5+30x^4+11x^3+17x^2+30x+22$ |
| (255,253) | $x^8+x^4+x^3+$ $+x^2+1$ | 1 | $x^2+6x+8$ |
| | $x^8+x^4+x^3+$ $+x^2+1$ | 255 | $x^2+3x+2$ |
| (255,251) | $x^8+x^4+x^3+$ $+x^2+1$ | 1 | $x^4+30x^3+216x^2+231x+116$ |
| | $x^8+x^4+x^3+$ $+x^2+1$ | 2 | $x^4+60x^3+71x^2+107x+19$ |
| (255,249) | $x^8+x^4+x^3+$ $+x^2+1$ | 1 | $x^6+126x^5+4x^4+158x^3+58x^2+49x+117$ |
| | $x^8+x^4+x^3+$ $+x^2+1$ | 29 | $x^6+100x^5+105x^4+69x^3+118x^2+97x+87$ |
| (255,247) | $x^8+x^4+x^3+$ $+x^2+1$ | 1 | $x^8+227x^7+44x^6+178x^5+71x^4+172x^3+8x^2+$ $+224x+37$ |
| | $x^8+x^5+x^3+$ $+x+1$ | 77 | $x^8+20x^7+6x^6+39x^5+111x^4+90x^3+7x^2+$ $+122x+22$ |
| (255,245) | $x^8+x^4+x^3+$ $+x^2+1$ | 1 | $x^{10}+173x^9+47x^8+140x^7+190x^6+197x^5+30x^4+$ $+188x^3+68x^2+212x+160$ |
| | $x^8+x^4+x^3+$ $+x^2+1$ | 31 | $x^{10}+12x^9+23x^8+66x^7+55x^6+45x^5+2x^4+6x^3+$ $+127x^2+93x+17$ |

## 4. Аппаратная реализация умножителя в поле Галуа

Кодер Рида – Соломона реализуется по схеме, представленной на рис. 1. Он содержит регистры сдвига, сумматоры в поле Галуа и умножители в поле Галуа.

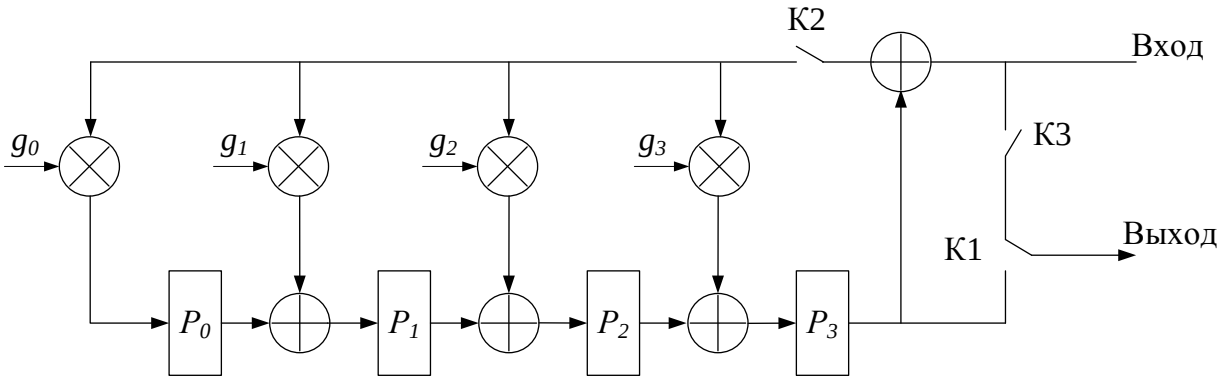


Рис. 1. Кодер Рида – Соломона

Одним из способов реализации элемента умножения в поле Галуа является так называемый полный умножитель, он описан в [3]. Приведём схему такого умножителя для кода (15,11), построенного в поле GF(16). Его аппаратная реализация приведена на рис. 2.

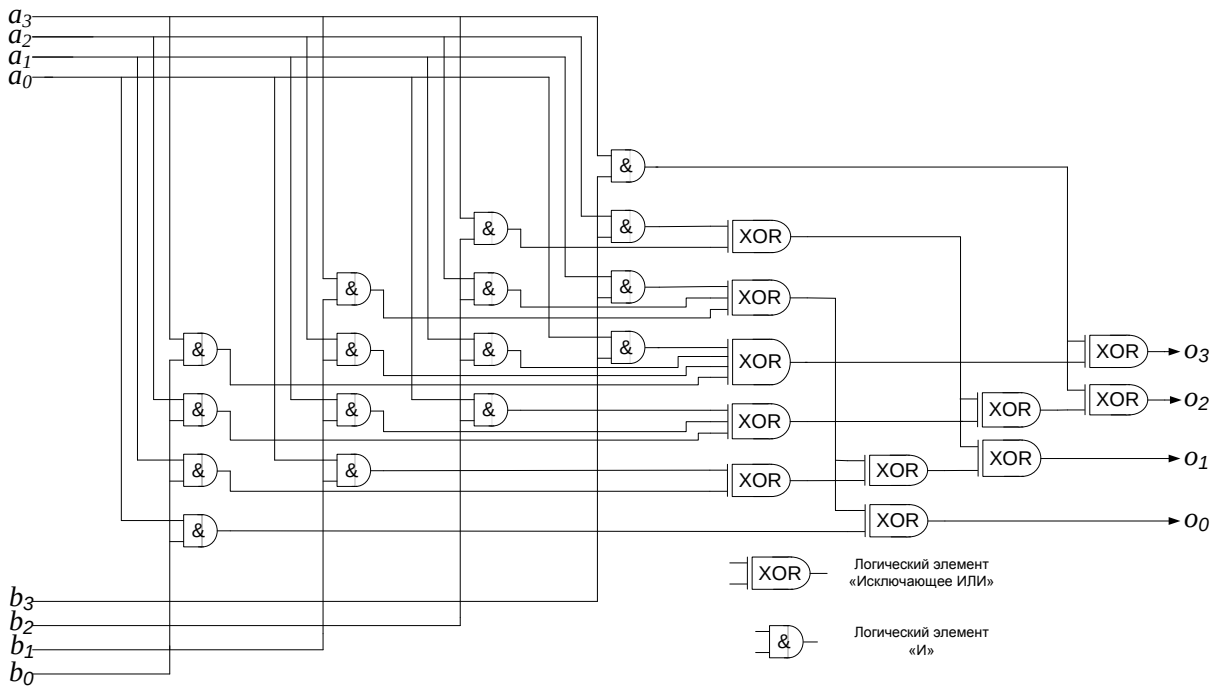


Рис. 2. Умножитель в поле GF(16)

На рисунке $a_i$ – поступающие на вход умножителя двоичные элементы, образующие четырёхбитовый элемент, поскольку умножение происходит в поле GF(16). $b_0b_1b_2b_3$ – элемент поля Галуа в двоичном виде (применительно к нашему случаю – один из числовых коэффициентов порождающего многочлена, представленный в двоичной форме). $o_0$ $o_1$ $o_2$ $o_3$ – результат умножения.

## 5. Упрощение умножителя

Выше показано, что существуют такие порождающие многочлены, у которых все коэффициенты находятся в меньшем расширении поля GF(2). К примеру, в табл. 1 для кода (15,11) найден порождающий многочлен $x^4 + 2x^3 + 7x^2 + 5x + 2$, все коэффициенты которого лежат в поле GF(8). В этом случае схему умножителя можно представить следующим образом.

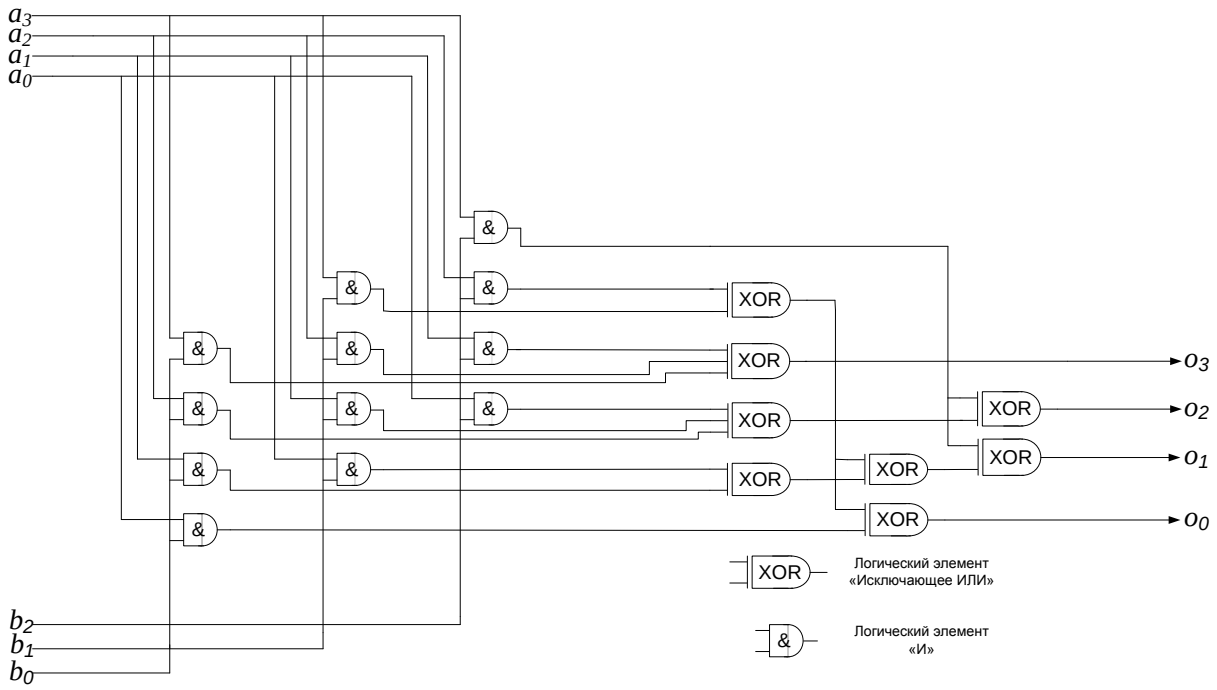


Рис. 3. Упрощённый умножитель в поле GF(16)

Тот факт, что коэффициенты порождающего многочлена лежат в GF(8) (в двоичном представлении трёхбитовые элементы), позволяет упростить схемное решение. В сравнение с предыдущей схемой, из реализации исключены 4 элемента “AND” и 3 элемента “XOR”. Безусловно, умножитель можно реализовать индивидуально для каждого из коэффициентов порождающего многочлена, при этом появится возможность упростить схему при наличии нулевых бит в двоичном представлении коэффициентов. Однако в зависимости от расположения нулей схемное решение будет каждый раз изменяться, а это усложнение в том плане, что для каждого коэффициента необходимо реализовывать свой индивидуальный умножитель. Предложенное в данной работе решение более универсально: достаточно выбрать многочлен, коэффициенты которого лежат в меньшем расширении поля, и однократно упростить схему. Впоследствии данная схема является универсальной для всех коэффициентов многочлена, изменяется только двоичное представление последних. Выигрыши при упрощении умножителей приведены в табл. 2.

Таблица 2. Выигрыш элементов на один умножитель в зависимости от поля Галуа

| Расширение поля | Выигрыш элементов для одного умножителя | |
|---|---|---|
| | AND | XOR |
| GF(16) | 4 | 3 |
| GF(32) | 5 | 4 |
| GF(64) | 6 | 3 |
| GF(128) | 7 | 4 |
| GF(256) | 8 | 3 |

Таким образом, выбор порождающих многочленов кодов Рида – Соломона, коэффициенты которых находятся в меньшем расширении поля GF(2) относительно того, в котом построен код, позволяет упростить реализацию схемы умножителя, исключив $m$ элементов “AND” (где $m$ – расширение поля GF($2^m$), в котором построен код) и $n$ элементов “XOR”, $n$ зависит от конкретного поля.

## Литература

1. Clarke C. K. P. Reed-Solomon error correction, BBC R&D White Paper № 031, 2002. – 47 p.
2. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ./ Под ред. К.Ш. Зигангирова.– М.: Мир, 1986.– 576 с.
3. Макаров А.А., Прибылов В.П. Помехоустойчивое кодирование: основы теории и практические приложения. – Новосибирск: Сиб. гос. ун-т телекоммуникаций и информатики, 2005.– 186 с.

*Статья поступила в редакцию 8.11.2010;*
*переработанный вариант — 17.11.2010*

**Клейко Денис Вячеславович**
студент 4 курса факультета АЭС СибГУТИ (630102, Новосибирск, ул. Кирова, 86),
e-mail: kley3@yandex.ru

**Лямин Никита Владимирович**
студент 4 курса факультета АЭС СибГУТИ (630102, Новосибирск, ул. Кирова, 86),
e-mail: sibsutispds@gmail.com

**Simplification of the Reed-Solomon encoder using alternative simple polynomials forming extensions of Galois fields**

**D. Kleyko, N. Lyamin**

In this paper, we introduce the possible gains in the hardware implementation of a Reed-Solomon encoder, expressed in the number of gates that are required in the simplified scheme. The basis of simplification is the usage of alternative polynomial for isomorphic extensions of the Galois field GF (2), and variations of different integral representations of the code generator polynomial of the Reed-Solomon code.

*Keywords:* Reed-Solomon codes, full multiplier, Galois field, code generator polynomial.