Механика Транспорт Комуникации

Научно списание **http://www.mtc-aj.com**

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
том 14, брой 2, 2016 г.
статия № 1284

КОДИРАНЕ И ДЕКОДИРАНЕ С КОД НА РИЙД-СОЛОМОН (15,11), БАЗИРАН НА ПОЛЕТО НА ГАЛОА $GF(2^4)$, ПРИ ВЪВЕЖДАНЕ НА ДВУСИМВОЛНА ГРЕШКА

Адриана Бороджиева
aborodjieva@ecs.uni-ruse.bg

Русенски университет „Ангел Кънчев", 7017 Русе,
ул. „Студентска" № 8
БЪЛГАРИЯ

Ключови думи: *Кодиране, декодиране, кодове на Рийд-Соломон, откриване и коригиране на грешки.*

Резюме: *В публикацията се описват процесите на кодиране и декодиране с код на Рийд-Соломон (15,11), базиран на полето на Галоа $GF(2^4)$, породено от неразложимия примитивен полином $f(x) = x^4 + x + 1$. Даден е пример за построяване на генераторен полином на кода на Рийд-Соломон, чрез който ще се откриват и коригират грешки, възникнали в два символа на кодовата дума, като тези символи може да са поредни, т.е. в поредица от 8 последователни бита. Илюстриран е процесът на кодиране на 44-битова информационна дума. След въвеждане на грешки в два символа се илюстрират и процесите на откриване и коригиране на грешките, както и декодирането. Материалът намира приложение в учебния процес по дисциплината „Кодиране в телекомуникационните системи", включена като избираема в учебния план на специалност „Телекомуникационни системи" за образователно-квалификационна степен „Бакалавър".*

ВЪВЕДЕНИЕ

Кодовете на Рийд-Соломон са създадени през 1960 г., от Irving S. Reed и Gustave Solomon, работещи по това време в MIT Lincoln Laboratory. Описани са в тяхната публикация „Полиномиални кодове над някои крайни полета" (Reed & Solomon, 1960). Тогава не е бил известен все още ефикасен алгоритъм за тяхното декодиране. Решение на този проблем е открит по-късно, през 1969 г., от Elwyn Berlekamp и James Massey, наречен по-късно на името на своите откриватели (алгоритъм за декодиране на Берлекемп-Меси). Кодовете на Рийд-Соломон са недвоични кодове, намиращи широко приложение в съвременните комуникационно-информационни системи. През 1977 г., кодовете на Рийд-Соломон са били имплементирани в програмата Voyager под формата на свързани кодове. Първото комерсиално приложение в масово-произвеждани потребителски продукти на кодовете на Рийд-Соломон е през 1982 г., в компакт-дисковете, където се използва съчетаването (преплитането) на два кода на Рийд-Соломон. Днес, кодовете на Рийд-Соломон широко се прилагат в цифровите устройства

за съхраняване на данни и в цифровите комуникационни стандарти, например, в стандарта за цифрово видео-разпръскване (digital video broadcasting, DVB) [2, 3, 6, 7].

При тези кодове се използват 2^m различни символа, представляващи m-битови последователности, които се разглеждат като елементи на полето на Галоа $GF(2^m)$. Кодовете на Рийд-Соломон (n, k) съществуват за всяко n и k, за които:

(1) $0 < k < n < 2^m + 2$,

където k е броят на информационните символи, подлежащи на кодиране; n е броят на символите в една кодова дума; 2^m е броят на символите в кодовата азбука [1, 4, 5, 7].

За кодовете на Рийд-Соломон е в сила:

(2) $(n,k) = (2^m - 1, 2^m - 1 - 2.t)$,

където t е броят на грешките, които кодът може да коригира; $r = n - k = 2t$ е броят на контролните символи [1, 4, 5, 6].

КОДИРАНЕ И ДЕКОДИРАНЕ С ИЗПОЛЗВАНЕ НА КОД НА РИЙД-СОЛОМОН

Въз основа на описания в [4, 5, 6] алгоритъм за построяване на код на Рийд-Соломон с дължина $n = 7$, коригиращ грешки в два символа, базиран на полето на Галоа $GF(2^3)$, породено от примитивния неразложим полином $f(x) = x^3 + x + 1$, в настоящата публикация този алгоритъм е адаптиран с цел построяване на код на Рийд-Соломон с дължина $n = 15$, отново коригиращ двусимволна грешка, който е базиран на полето на Галоа $GF(2^4)$, породено от примитивния неразложим полином от четвърта степен $f(x) = x^4 + x + 1$. Илюстрирани са процесите на кодиране на зададена информационна дума при използване на разглеждания код на Рийд-Соломон и на декодиране, при въвеждане на грешка в два символа.

По условие, кодът може да коригира грешки в два символа, т.е. $t = 2$. Тъй като $n = 15$, то се използва полето на Галоа $GF(2^4)$, породено от примитивния неразложим полином $f(x) = x^4 + x + 1$. Елементите на полето $GF(2^4)$ са дадени в таблица 1 [7]. Операциите в полето се извършват по модул $f(x) = x^4 + x + 1$.

Тъй като кодовете на Рийд-Соломон са подклас на БЧХ-кодовете, те могат да се разглеждат като циклични кодове с генераторен полином $P(x)$ от вида:

(3) $P(x) = (x - \alpha).(x - \alpha^2)...(x - \alpha^{2t})$.

Вижда се, че степента на полинома $P(x)$ е $2t$, защото са необходими $r = 2t$ контролни разряди, за да се коригират t грешки.

В случая, генераторният полином на кода на Рийд-Соломон се получава:

$$
\begin{aligned}
&P(x) = (x - \alpha).(x - \alpha^2).(x - \alpha^3).(x - \alpha^4) = \\
&= (x^2 - \alpha x - \alpha^2 x + \alpha^3).(x^2 - \alpha^3 x - \alpha^4 x + \alpha^7) = \\
&= [x^2 - (\alpha^1 + \alpha^2)x + \alpha^3].[x^2 - (\alpha^3 + \alpha^4)x + \alpha^7] = (x^2 - \alpha^5 x + \alpha^3).(x^2 - \alpha^7 x + \alpha^7) = \\
&= x^4 - \alpha^7 x^3 + \alpha^7 x^2 - \alpha^5 x^3 + \alpha^{12} x^2 - \alpha^{12} x + \alpha^3 x^2 - \alpha^{10} x + \alpha^{10} = \\
&= x^4 - (\alpha^7 + \alpha^5)x^3 + \left(\underbrace{\alpha^7 + \alpha^{12}}_{\alpha^2} + \alpha^3 \right) x^2 - (\alpha^{12} + \alpha^{10})x + \alpha^{10} = \\
&= x^4 + \alpha^{13} x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^{10}.
\end{aligned}
\tag{4}
$$

При пресмятането е използвано, че операцията изваждане е еквивалентна на операцията събиране в полето на Галоа $GF(2^4)$ с основа 2. Събирането в полето на

Галоа $GF(2^4)$ се осъществява съгласно таблица 2, а умножението се извършва съгласно правилото:

(5) $\alpha^x.\alpha^y = \alpha^{(x+y) \bmod 15}$.

Таблица 1. Елементи на полето $GF(2^4)$, породено от $f(x) = x^4 + x + 1$

№	Полином от трета степен	Наредена *n*-торка	Степени на $\alpha = x$
0	$0.x^3 + 0.x^2 + 0.x + 0$	0 0 0 0	0
1	$0.x^3 + 0.x^2 + 0.x + 1$	0 0 0 1	α^0
2	$0.x^3 + 0.x^2 + 1.x + 0$	0 0 1 0	α^1
3	$0.x^3 + 0.x^2 + 1.x + 1$	0 0 1 1	α^4
4	$0.x^3 + 1.x^2 + 0.x + 0$	0 1 0 0	α^2
5	$0.x^3 + 1.x^2 + 0.x + 1$	0 1 0 1	α^8
6	$0.x^3 + 1.x^2 + 1.x + 0$	0 1 1 0	α^5
7	$0.x^3 + 1.x^2 + 1.x + 1$	0 1 1 1	α^{10}
8	$1.x^3 + 0.x^2 + 0.x + 0$	1 0 0 0	α^3
9	$1.x^3 + 0.x^2 + 0.x + 1$	1 0 0 1	α^{14}
10	$1.x^3 + 0.x^2 + 1.x + 0$	1 0 1 0	α^9
11	$1.x^3 + 0.x^2 + 1.x + 1$	1 0 1 1	α^7
12	$1.x^3 + 1.x^2 + 0.x + 0$	1 1 0 0	α^6
13	$1.x^3 + 1.x^2 + 0.x + 1$	1 1 0 1	α^{13}
14	$1.x^3 + 1.x^2 + 1.x + 0$	1 1 1 0	α^{11}
15	$1.x^3 + 1.x^2 + 1.x + 1$	1 1 1 1	α^{12}

Таблица 2. Сумиране в поле $GF(2^4)$, породено от $f(x) = x^4 + x + 1$

	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
α^0	0	α^4	α^8	α^{14}	α^1	α^{10}	α^{13}	α^9	α^2	α^7	α^5	α^{12}	α^{11}	α^6	α^3
α^1	α^4	0	α^5	α^9	α^0	α^2	α^{11}	α^{14}	α^{10}	α^3	α^8	α^6	α^{13}	α^{12}	α^7
α^2	α^8	α^5	0	α^6	α^{10}	α^1	α^3	α^{12}	α^0	α^{11}	α^4	α^9	α^7	α^{14}	α^{13}
α^3	α^{14}	α^9	α^6	0	α^7	α^{11}	α^2	α^4	α^{13}	α^1	α^{12}	α^5	α^{10}	α^8	α^0
α^4	α^1	α^0	α^{10}	α^7	0	α^8	α^{12}	α^3	α^5	α^{14}	α^2	α^{13}	α^6	α^{11}	α^9
α^5	α^{10}	α^2	α^1	α^{11}	α^8	0	α^9	α^{13}	α^4	α^6	α^0	α^3	α^{14}	α^7	α^{12}
α^6	α^{13}	α^{11}	α^3	α^2	α^{12}	α^9	0	α^{10}	α^{14}	α^5	α^7	α^1	α^4	α^0	α^8
α^7	α^9	α^{14}	α^{12}	α^4	α^3	α^{13}	α^{10}	0	α^{11}	α^0	α^6	α^8	α^2	α^5	α^1
α^8	α^2	α^{10}	α^0	α^{13}	α^5	α^4	α^{14}	α^{11}	0	α^{12}	α^1	α^7	α^9	α^3	α^6
α^9	α^7	α^3	α^{11}	α^1	α^{14}	α^6	α^5	α^0	α^{12}	0	α^{13}	α^2	α^8	α^{10}	α^4
α^{10}	α^5	α^8	α^4	α^{12}	α^2	α^0	α^7	α^6	α^1	α^{13}	0	α^{14}	α^3	α^9	α^{11}
α^{11}	α^{12}	α^6	α^9	α^5	α^{13}	α^3	α^1	α^8	α^7	α^2	α^{14}	0	α^0	α^4	α^{10}
α^{12}	α^{11}	α^{13}	α^7	α^{10}	α^6	α^{14}	α^4	α^2	α^9	α^8	α^3	α^0	0	α^1	α^5
α^{13}	α^6	α^{12}	α^{14}	α^8	α^{11}	α^7	α^0	α^5	α^3	α^{10}	α^9	α^4	α^1	0	α^2
α^{14}	α^3	α^7	α^{13}	α^0	α^9	α^{12}	α^8	α^1	α^6	α^4	α^{11}	α^{10}	α^5	α^2	0

Алгоритъмът за кодиране и декодиране при кодовете на Рийд-Соломон ще бъде пояснен като се използва дадения пример.

Тъй като $t = 2$, то разглежданият код на Рийд-Соломон може да открива и коригира всички двойни грешки в кодовите думи. За коригиране на двусимволна

грешка е необходимо да се определят стойностите на четири неизвестни – две от тях се отнасят за разположението на грешката, а другите две – за нейната стойност. Тук трябва да се отбележи разликата от двоичното кодиране, където е необходимо само да се знае мястото на грешката и е достатъчно да се промени бита от 0 в 1 или обратното, докато при недвоичното кодиране трябва не само да се разбере къде е грешката, но и да се определи правилната стойност на символа на това място. В дадения пример има четири неизвестни, следователно са необходими четири уравнения, за да се определят неизвестните. Следователно, броят на контролните символи е $r = 2t = 4$.

При $n = 15$, броят на информационните символи е $k = 11$, като всеки от тях преставлява четирибитов вектор-стълб, който се разглежда като елемент на $GF(2^4)$. След тези уточнения, алгоритъмът за кодиране при разглеждания код на Рийд-Соломон, е следният:

Стъпка 1. Нека в *i*-тия такт от работа на кодера източникът на информация е формирал следните 44 информационни бита (ASCII-кодовете на съобщението "EBCDIC", т.е. 6 x 7 = 42 бита, допълнени с два бита, първият, формиращ контрол по нечетност, а вторият – контрол по четност):

1000101 1000010 1000011 1000100 1001001 1000011 + 1 +0.

Тези 44 бита се групират в 11 четирибитови символа:

1000 1011 0000 1010 0001 1100 0100 1001 0011 0000 1110.

Като се използва таблица 1 се установява, че на посочените четирибитови символи съответстват следните елементи от $GF(2^4)$:

$$\text{(6a)} \quad \begin{bmatrix}0\\0\\0\\1\end{bmatrix} = \alpha^3, \begin{bmatrix}1\\1\\0\\1\end{bmatrix} = \alpha^7, \begin{bmatrix}0\\0\\0\\0\end{bmatrix} = 0, \begin{bmatrix}0\\1\\0\\1\end{bmatrix} = \alpha^9, \begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \alpha^0, \begin{bmatrix}0\\0\\1\\1\end{bmatrix} = \alpha^6,$$

$$\text{(6b)} \quad \begin{bmatrix}0\\0\\1\\0\end{bmatrix} = \alpha^2, \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \alpha^{14}, \begin{bmatrix}1\\1\\0\\0\end{bmatrix} = \alpha^4, \begin{bmatrix}0\\0\\0\\0\end{bmatrix} = 0, \begin{bmatrix}0\\1\\1\\1\end{bmatrix} = \alpha^{11}.$$

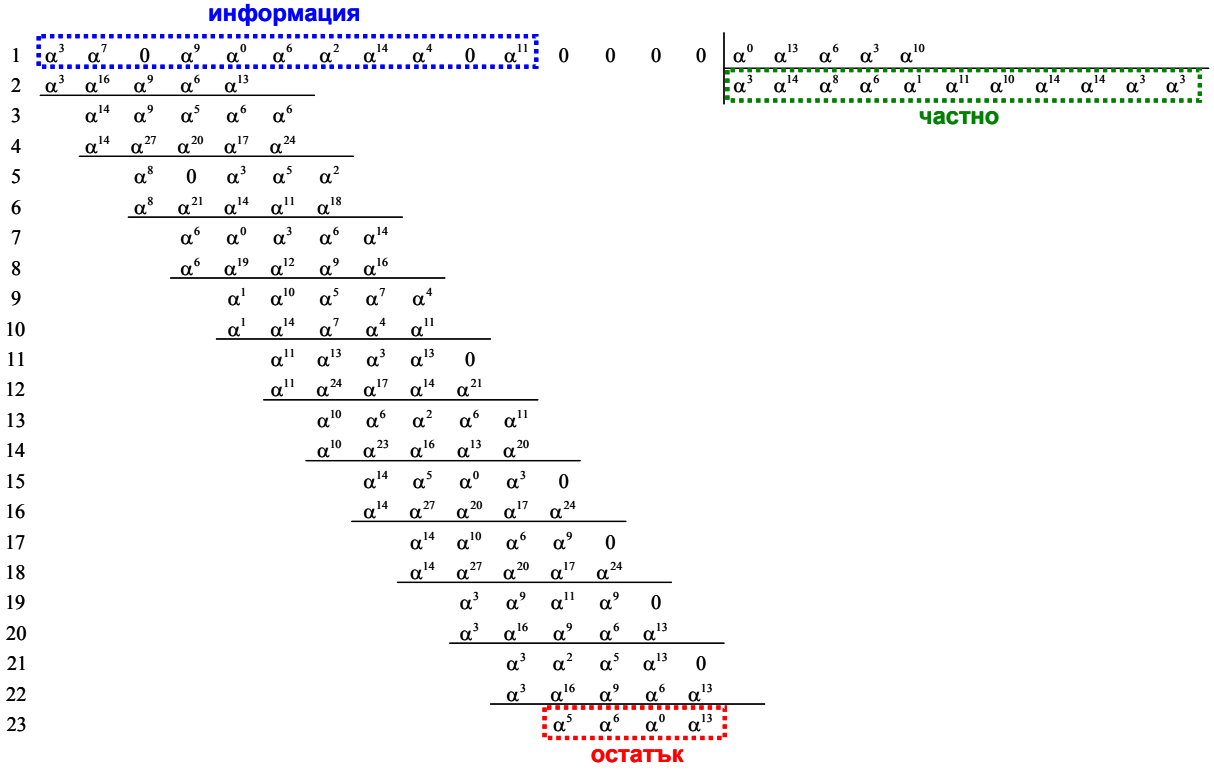
Стъпка 2. За разглеждания код на Рийд-Соломон, генераторният полином, съгласно формула (4), е $P(x) = x^4 + \alpha^{13}x^3 + \alpha^6x^2 + \alpha^3x + \alpha^{10}$.

Стъпка 3. На информационната дума 1000 1011 0000 1010 0001 1100 0100 1001 0011 0000 1110 съответства полиномът:

$$\text{(7)} \quad \begin{aligned} A(x) &= \alpha^3 . x^{10} + \alpha^7 . x^9 + 0 . x^8 + \alpha^9 . x^7 + \alpha^0 . x^6 + \\ &+ \alpha^6 . x^5 + \alpha^2 . x^4 + \alpha^{14} . x^3 + \alpha^4 . x^2 + 0 . x + \alpha^{11}. \end{aligned}$$

Разрешените кодови комбинации, които се изпращат от предавателя към приемника, се изчисляват, като се вземат коефициентите на полиномиалното произведение $C(x) = A(x) . P(x)$. Този подход се нарича несистематично кодиране. При систематичното кодиране, в разрешените кодови думи първо се разполагат информационните символи, а контролните символи заемат последните позиции. Предимството на систематичното кодиране е в това, че ако няма грешки в приетите кодови думи, т.е. синдромът е 0, тогава първите символи на приетите кодови думи директно се извличат като вярна информация. Ето защо в разглеждания пример ще бъде използвано систематично кодиране, при което полиномът на информационната дума $A(x)$ се умножава с x^4, така че информационните символи ще заемат най-старшите единадесет позиции на

полинома, съответстващ на разрешената кодова дума. След това, $A(x).x^4$ се дели на генераторния полином $P(x)$, като се използват таблица 2 и формула (5) (в изчисленията по-долу се използва, че в полето на Галоа $GF(2^4)$ операциите изваждане и събиране се изпълняват по модул 2 и по тази причина са еквивалентни).



Фиг. 1. Илюстриране на процеса на кодиране чрез код на Рийд-Соломон, чрез деление на полиноми

Вижда се, че остатъкът от делението на $A(x).x^4$ с генераторния полином $P(x)$ е $R(x)=\alpha^5.x^3+\alpha^6.x^2+\alpha^0.x+\alpha^{13}$.

За да се дели полиномът на разрешената кодова комбинация без остатък на генераторния полином $P(x)$, към $A(x).x^4$ се прибавя остатъкът $R(x)$ (в полето на Галоа $GF(2^4)$ операциите изваждане и събиране се изпълняват по модул 2 и по тази причина са еквивалентни) и резултатът е:

$$C(x)=A(x).x^4+R(x)=\alpha^3.x^{14}+\alpha^7.x^{13}+0.x^{12}+\alpha^9.x^{11}+\alpha^0.x^{10}+$$
$$+\alpha^6.x^9+\alpha^2.x^8+\alpha^{14}.x^7+\alpha^4.x^6+0.x^5+\alpha^{11}.x^4+\alpha^5.x^3+\alpha^6.x^2+\alpha^0.x+\alpha^{13}=$$

(8)
$$=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}.x^{14}+\begin{bmatrix}1\\1\\0\\1\end{bmatrix}.x^{13}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{12}+\begin{bmatrix}0\\1\\0\\1\end{bmatrix}.x^{11}+\begin{bmatrix}1\\0\\0\\0\end{bmatrix}.x^{10}+\begin{bmatrix}0\\0\\1\\1\end{bmatrix}.x^9+\begin{bmatrix}0\\0\\1\\0\end{bmatrix}.x^8+$$
$$+\begin{bmatrix}1\\0\\0\\1\end{bmatrix}.x^7+\begin{bmatrix}1\\1\\0\\0\end{bmatrix}.x^6+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^5+\begin{bmatrix}0\\1\\1\\1\end{bmatrix}.x^4+\begin{bmatrix}0\\1\\1\\0\end{bmatrix}.x^3+\begin{bmatrix}0\\0\\1\\1\end{bmatrix}.x^2+\begin{bmatrix}1\\0\\0\\0\end{bmatrix}.x+\begin{bmatrix}1\\0\\1\\1\end{bmatrix}.$$

Следователно, информационната дума 1000 1011 0000 1010 0001 1100 0100 1001 0011 0000 1110 се допълва с още 16 бита, представляващи 4 четирибитови контролни символа и в комуникационния канал се излъчва кодовата дума 1000 1011 0000 1010 0001 1100 0100 1001 0011 0000 1110 0110 1100 0001 1101, т.е. относителната скорост на предаване на информацията за разглеждания код е $11/15$.

Трябва да се отбележи, че коефициентите на редове 3, 5, 7, 9, 11, 13, 15, 17, 19, 21 и 23 (фиг. 1) се получават въз основа на събиране на съответните коефициенти в предходните два реда и спазване на правилата, посочени в таблица 2, както и редуцирането на степенния показател на α, а именно:

(9) $\alpha^7+\alpha^{16}=\alpha^7+\alpha^1=\alpha^{14};\ 0+\alpha^9=\alpha^9;\ \alpha^9+\alpha^6=\alpha^5;\ \alpha^0+\alpha^{13}=\alpha^6;$ (за ред № 3);

(10) $\alpha^9+\alpha^{27}=\alpha^9+\alpha^{12}=\alpha^8;\ \alpha^5+\alpha^{20}=\alpha^5+\alpha^5=0;$
$\alpha^6+\alpha^{17}=\alpha^6+\alpha^2=\alpha^3;\ \alpha^6+\alpha^{24}=\alpha^6+\alpha^9=\alpha^5;$ (за ред № 5);

(11) $0+\alpha^{21}=0+\alpha^6=\alpha^6;\ \alpha^3+\alpha^{14}=\alpha^0;\ \alpha^5+\alpha^{11}=\alpha^3;\ \alpha^2+\alpha^3=\alpha^6;$ (за ред № 7);

(12) $\alpha^0+\alpha^{19}=\alpha^0+\alpha^4=\alpha^1;\ \alpha^3+\alpha^{12}=\alpha^{10};$
$\alpha^6+\alpha^9=\alpha^5;\ \alpha^{14}+\alpha^{16}=\alpha^{14}+\alpha^1=\alpha^7;$ (за ред № 9);

(13) $\alpha^{10}+\alpha^{14}=\alpha^{11};\ \alpha^5+\alpha^7=\alpha^{13};\ \alpha^7+\alpha^4=\alpha^3;\ \alpha^4+\alpha^{11}=\alpha^{13};$ (за ред № 11);

(14) $\alpha^{13}+\alpha^{24}=\alpha^{13}+\alpha^9=\alpha^{10};\ \alpha^3+\alpha^{17}=\alpha^3+\alpha^2=\alpha^6;$
$\alpha^{13}+\alpha^{14}=\alpha^2;\ 0+\alpha^{21}=0+\alpha^6=\alpha^6;$ (за ред № 13);

(15) $\alpha^6+\alpha^{23}=\alpha^6+\alpha^8=\alpha^{14};\ \alpha^2+\alpha^{16}=\alpha^2+\alpha^1=\alpha^5;$
$\alpha^6+\alpha^{13}=\alpha^0;\ \alpha^{11}+\alpha^{20}=\alpha^{11}+\alpha^5=\alpha^3;$ (за ред № 15);

(16) $\alpha^5+\alpha^{27}=\alpha^5+\alpha^{12}=\alpha^{14};\ \alpha^0+\alpha^{20}=\alpha^0+\alpha^5=\alpha^{10};$
$\alpha^3+\alpha^{17}=\alpha^3+\alpha^2=\alpha^6;\ 0+\alpha^{24}=0+\alpha^9=\alpha^9;$ (за ред № 17);

(17) $\alpha^{10}+\alpha^{27}=\alpha^{10}+\alpha^{12}=\alpha^3;\ \alpha^6+\alpha^{20}=\alpha^6+\alpha^5=\alpha^9;$
$\alpha^9+\alpha^{17}=\alpha^9+\alpha^2=\alpha^{11};\ 0+\alpha^{24}=0+\alpha^9=\alpha^9;$ (за ред № 19);

(18) $\alpha^9+\alpha^{16}=\alpha^9+\alpha^1=\alpha^3;\ \alpha^{11}+\alpha^9=\alpha^2;\ \alpha^9+\alpha^6=\alpha^5;\ 0+\alpha^{13}=\alpha^{13};$ (за ред № 21);

(19) $\alpha^2+\alpha^{16}=\alpha^2+\alpha^1=\alpha^5;\ \alpha^5+\alpha^9=\alpha^6;\ \alpha^{13}+\alpha^6=\alpha^0;\ 0+\alpha^{13}=\alpha^{13};$ (за ред № 23).

Нека при предаване на кодовата дума два символа са повредени от шумовете и са приети с грешка. Този брой на грешките съответства на максималната възможност на кода да коригира грешки. При използване на 15-символна кодова дума, моделът на грешката може да се представи във вида $E(x)=\sum_{k=0}^{14} e_k.x^k$. За определеност нека двусимволната грешка се представя с полинома:

$$E(x)=\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{14}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{13}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{12}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{11}+\begin{bmatrix}0\\1\\0\\1\end{bmatrix}.x^{10}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{9}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{8}+$$

(20)
$$+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{7}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{6}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{5}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{4}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{3}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{2}+\begin{bmatrix}1\\1\\1\\1\end{bmatrix}.x+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}=$$
$$=0.x^{14}+0.x^{13}+0.x^{12}+0.x^{11}+\alpha^{9}.x^{10}+0.x^{9}+0.x^{8}+$$
$$+0.x^{7}+0.x^{6}+0.x^{5}+0.x^{4}+0.x^{3}+0.x^{2}+\alpha^{12}.x+0.$$

С други думи, сгрешени са първият (най-старшият) бит и третият бит на петия информационен символ (представено като α^9) и четирите бита на третия контролен символ на съобщението (представено като α^{12}).

Следователно, полиномът на грешно приетата кодова дума е:

$$B(x)=C(x)+E(x)=$$

$$=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}.x^{14}+\begin{bmatrix}1\\1\\0\\1\end{bmatrix}.x^{13}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{12}+\begin{bmatrix}0\\1\\0\\1\end{bmatrix}.x^{11}+\begin{bmatrix}1\\1\\0\\1\end{bmatrix}.x^{10}+\begin{bmatrix}0\\0\\1\\1\end{bmatrix}.x^{9}+\begin{bmatrix}0\\0\\1\\0\end{bmatrix}.x^{8}+$$

(21)
$$+\begin{bmatrix}1\\0\\0\\1\end{bmatrix}.x^{7}+\begin{bmatrix}1\\1\\0\\0\end{bmatrix}.x^{6}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.x^{5}+\begin{bmatrix}0\\1\\1\\1\end{bmatrix}.x^{4}+\begin{bmatrix}0\\1\\1\\0\end{bmatrix}.x^{3}+\begin{bmatrix}0\\0\\1\\1\end{bmatrix}.x^{2}+\begin{bmatrix}0\\1\\1\\1\end{bmatrix}.x+\begin{bmatrix}1\\0\\1\\1\end{bmatrix}=$$
$$=\alpha^{3}.x^{14}+\alpha^{7}.x^{13}+0.x^{12}+\alpha^{9}.x^{11}+\alpha^{7}.x^{10}+\alpha^{6}.x^{9}+\alpha^{2}.x^{8}+$$
$$+\alpha^{14}.x^{7}+\alpha^{4}.x^{6}+0.x^{5}+\alpha^{11}.x^{4}+\alpha^{5}.x^{3}+\alpha^{6}.x^{2}+\alpha^{11}.x+\alpha^{13}.$$

Проверката на приетите комбинации се извършва чрез изчисляване на синдрома. Ако синдромът S има стойност 0, тогава се счита, че няма грешка в приетата кодова дума. Всяка друга стойност на синдрома, различна от 0, е показател за възникнала в комуникационния канал грешка. Както и в двоичния случай, синдромът се състои от $(n-k)$ символи. За разглеждания пример, синдромът има 4 символа, които се получават:

$$S_1=r(\alpha)=B(\alpha)=\alpha^{3}.\alpha^{14}+\alpha^{7}.\alpha^{13}+0.\alpha^{12}+\alpha^{9}.\alpha^{11}+\alpha^{7}.\alpha^{10}+\alpha^{6}.\alpha^{9}+\alpha^{2}.\alpha^{8}+$$
$$+\alpha^{14}.\alpha^{7}+\alpha^{4}.\alpha^{6}+0.\alpha^{5}+\alpha^{11}.\alpha^{4}+\alpha^{5}.\alpha^{3}+\alpha^{6}.\alpha^{2}+\alpha^{11}.\alpha+\alpha^{13}=$$

(22)
$$=\alpha^{17}+\alpha^{20}+0+\alpha^{20}+\alpha^{17}+\alpha^{15}+\alpha^{10}+\alpha^{21}+\alpha^{10}+0+\alpha^{15}+\alpha^{8}+\alpha^{8}+\alpha^{12}+\alpha^{13}=$$
$$=\alpha^{2}+\alpha^{5}+0+\alpha^{5}+\alpha^{2}+\alpha^{0}+\alpha^{10}+\alpha^{6}+\alpha^{10}+0+\alpha^{0}+\alpha^{8}+\alpha^{8}+\alpha^{12}+\alpha^{13}=$$
$$=\alpha^{6}+\alpha^{12}+\alpha^{13}=\alpha^{4}+\alpha^{13}=\alpha^{11}\neq 0;$$

$$S_2 = r(\alpha^2) = B(\alpha^2) = \alpha^3.\alpha^{28} + \alpha^7.\alpha^{26} + 0.\alpha^{24} + \alpha^9.\alpha^{22} + \alpha^7.\alpha^{20} + \alpha^6.\alpha^{18} + \alpha^2.\alpha^{16} +$$
$$+ \alpha^{14}.\alpha^{14} + \alpha^4.\alpha^{12} + 0.\alpha^{10} + \alpha^{11}.\alpha^8 + \alpha^5.\alpha^6 + \alpha^6.\alpha^4 + \alpha^{11}.\alpha^2 + \alpha^{13} =$$
(23) $$= \alpha^{31} + \alpha^{33} + 0 + \alpha^{31} + \alpha^{27} + \alpha^{24} + \alpha^{18} + \alpha^{28} + \alpha^{16} + 0 + \alpha^{19} + \alpha^{11} + \alpha^{10} + \alpha^{13} + \alpha^{13} =$$
$$= \alpha^1 + \alpha^3 + 0 + \alpha^1 + \alpha^{12} + \alpha^9 + \alpha^3 + \alpha^{13} + \alpha^1 + 0 + \alpha^4 + \alpha^{11} + \alpha^{10} + \alpha^{13} + \alpha^{13} =$$
$$= \alpha^{12} + \alpha^9 + \alpha^1 + \alpha^4 + \alpha^{11} + \alpha^{10} + \alpha^{13} = \alpha^8 + \alpha^0 + \alpha^{14} + \alpha^{13} = \alpha^2 + \alpha^2 = 0;$$
$$S_3 = r(\alpha^3) = B(\alpha^3) = \alpha^3.\alpha^{42} + \alpha^7.\alpha^{39} + 0.\alpha^{36} + \alpha^9.\alpha^{33} + \alpha^7.\alpha^{30} + \alpha^6.\alpha^{27} + \alpha^2.\alpha^{24} +$$
$$+ \alpha^{14}.\alpha^{21} + \alpha^4.\alpha^{18} + 0.\alpha^{15} + \alpha^{11}.\alpha^{12} + \alpha^5.\alpha^9 + \alpha^6.\alpha^6 + \alpha^{11}.\alpha^3 + \alpha^{13} =$$
(24) $$= \alpha^{45} + \alpha^{46} + 0 + \alpha^{42} + \alpha^{37} + \alpha^{33} + \alpha^{26} + \alpha^{35} + \alpha^{22} + 0 + \alpha^{23} + \alpha^{14} + \alpha^{12} + \alpha^{14} + \alpha^{13} =$$
$$= \alpha^0 + \alpha^1 + 0 + \alpha^{12} + \alpha^7 + \alpha^3 + \alpha^{11} + \alpha^5 + \alpha^7 + 0 + \alpha^8 + \alpha^{14} + \alpha^{12} + \alpha^{14} + \alpha^{13} =$$
$$= \alpha^0 + \alpha^1 + \alpha^3 + \alpha^{11} + \alpha^5 + \alpha^8 + \alpha^{13} = \alpha^4 + \alpha^5 + \alpha^4 + \alpha^{13} = \alpha^7 \neq 0;$$
$$S_4 = r(\alpha^4) = B(\alpha^4) = \alpha^3.\alpha^{56} + \alpha^7.\alpha^{52} + 0.\alpha^{48} + \alpha^9.\alpha^{44} + \alpha^7.\alpha^{40} + \alpha^6.\alpha^{36} + \alpha^2.\alpha^{32} +$$
$$+ \alpha^{14}.\alpha^{28} + \alpha^4.\alpha^{24} + 0.\alpha^{20} + \alpha^{11}.\alpha^{16} + \alpha^5.\alpha^{12} + \alpha^6.\alpha^8 + \alpha^{11}.\alpha^4 + \alpha^{13} =$$
(25) $$= \alpha^{59} + \alpha^{59} + 0 + \alpha^{53} + \alpha^{47} + \alpha^{42} + \alpha^{34} + \alpha^{42} + \alpha^{28} + 0 + \alpha^{27} + \alpha^{17} + \alpha^{14} + \alpha^{15} + \alpha^{13} =$$
$$= \alpha^{14} + \alpha^{14} + 0 + \alpha^8 + \alpha^2 + \alpha^{12} + \alpha^4 + \alpha^{12} + \alpha^{13} + 0 + \alpha^{12} + \alpha^2 + \alpha^{14} + \alpha^0 + \alpha^{13} =$$
$$= \alpha^8 + \alpha^4 + \alpha^{12} + \alpha^{14} + \alpha^0 = \alpha^5 + \alpha^5 + \alpha^0 = \alpha^0 \neq 0;$$

Резултатът показва, че в приетата кодова комбинация се съдържа грешка. Това налага решаването на системата уравнения [5, 6]:

$$r(\alpha) = e_1.X_1 + e_2.X_2 + ... + e_i.X_i + ... + e_t.X_t,$$
$$r(\alpha^2) = e_1.X_1^2 + e_2.X_2^2 + ... + e_i.X_i^2 + ... + e_t.X_t^2,$$
(26) $$r(\alpha^3) = e_1.X_1^3 + e_2.X_2^3 + ... + e_i.X_i^3 + ... + e_t.X_t^3,$$
$$.....$$
$$r(\alpha^{2t}) = e_1.X_1^{2t} + e_2.X_2^{2t} + ... + e_i.X_i^{2t} + ... + e_t.X_t^{2t},$$

като в разглеждания случай $t = 2$. Това е трудна изчислителна задача дори за много мощен компютър, тъй като възможните стойности на неизвестните, които трябва да бъдат проверени, са q^{2t}, като тук $q = 2^m$ е броят на елементите в използваното поле на Галоа, $2t$ е броят на неизвестните. Изход от тази сложна ситуация са намерили Берлекемп и Меси, които са въвели т.нар. полином на локатора на грешката [5, 6, 7]:

(27) $$\sigma(x) = (1 - X_1.x).(1 - X_2.x)...(1 - X_{2t}.x) = 1 + \sigma_1.x + \sigma_2.x^2 + ... + \sigma_{2t}.x^{2t}.$$

Тук знаците „–” са заменени навсякъде с „+”, защото в полетата на Галоа $GF(2^m)$, операциите изваждане и събиране се изпълняват по модул 2 и по тази причина са еквивалентни. Както се вижда, нулите на полинома $\sigma(x)$ са реципрочните стойности $X_1^{-1}, X_2^{-1}, \ldots, X_{2t}^{-1}$ на елементите $X_1, X_2, \ldots, X_{2t}$, които са решение на системата уравнения за $r(\alpha^i)$. Ползата от въвеждането на полином на локатора на грешката $\sigma(x)$ е в това, че Берлекемп и Меси са доказали метод за просто изчисляване на коефициентите на $\sigma(x)$. По-конкретно, в сила е следната система от уравнения, която за краткост е записана в матрична форма:

$$(28)\qquad \begin{bmatrix} S_1 & S_2 & S_3 & \ldots & S_{t-1} & S_t \\ S_2 & S_3 & S_4 & \ldots & S_t & S_{t+1} \\ \ldots & \ldots. & \ldots. & \ldots. & \ldots. & \ldots. \\ S_{t-1} & S_t & S_{t+1} & \ldots & S_{2t-3} & S_{2t-2} \\ S_t & S_{t+1} & S_{t+2} & \ldots & S_{2t-2} & S_{2t-1} \end{bmatrix} . \begin{bmatrix} \sigma_t \\ \sigma_{t-1} \\ \ldots \\ \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} -S_{t+1} \\ -S_{t+2} \\ \ldots \\ -S_{2t-1} \\ -S_{2t} \end{bmatrix}$$

В разглеждания случай, при метода на Берлекемп-Меси се получава:

$$(29)\qquad \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} . \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} S_3 \\ S_4 \end{bmatrix}, \text{т.е.} \begin{bmatrix} \alpha^{11} & 0 \\ 0 & \alpha^7 \end{bmatrix} . \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^7 \\ \alpha^0 \end{bmatrix}.$$

За да се реши последното матрично уравнение е необходимо да се изчисли обратната матрица на матрицата на коефициентите. Както е известно, ако $\boldsymbol{A}$ е квадратна матрица от ред t, нейната обратна матрица се изчислява по формулата:

$$(30)\qquad \boldsymbol{A}^{-1} = \frac{1}{\det \boldsymbol{A}} \begin{bmatrix} A_{11} & A_{21} & \ldots & A_{t1} \\ A_{12} & A_{22} & \ldots & A_{t2} \\ \ldots & \ldots & \ldots & \ldots \\ A_{1t} & A_{2t} & \ldots & A_{tt} \end{bmatrix}.$$

Тук $\det \boldsymbol{A}$ е детерминантата на $\boldsymbol{A}$, а A_{ij}, $i = 1,2,\ldots,t$, $j = 1,2,\ldots,t$, е адюнгираното количество (алгебричното допълнение) на елемента на $\boldsymbol{A}$, разположен в i-тия ред и j-тия стълб. За матрицата на коефициентите е изпълнено:

$$(31)\qquad \det \boldsymbol{A} = \det \begin{bmatrix} \alpha^{11} & 0 \\ 0 & \alpha^7 \end{bmatrix} = \alpha^{11}.\alpha^7 - 0.0 = \alpha^{18} - 0 = \alpha^3 \neq 0,$$

$$(32)\qquad \begin{aligned} &A_{11} = (-1)^{1+1}.\alpha^7 = \alpha^7, A_{12} = (-1)^{1+2}.0 = 0, \\ &A_{21} = (-1)^{2+1}.0 = 0, A_{22} = (-1)^{2+2}.\alpha^{11} = \alpha^{11}. \end{aligned}$$

Следователно, за обратната матрица се получава:

$$(33)\qquad \boldsymbol{A}^{-1} = \frac{1}{\alpha^3} \begin{bmatrix} \alpha^7 & 0 \\ 0 & \alpha^{11} \end{bmatrix} = \begin{bmatrix} \alpha^4 & 0 \\ 0 & \alpha^8 \end{bmatrix}.$$

Верността на получения резултат се проверява от равенството:

$$(34)\qquad \boldsymbol{A}.\boldsymbol{A}^{-1} = \begin{bmatrix} \alpha^{11} & 0 \\ 0 & \alpha^7 \end{bmatrix} . \begin{bmatrix} \alpha^4 & 0 \\ 0 & \alpha^8 \end{bmatrix} = \begin{bmatrix} \alpha^{15} & 0 \\ 0 & \alpha^{15} \end{bmatrix} = \begin{bmatrix} \alpha^0 & 0 \\ 0 & \alpha^0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \boldsymbol{E}_2.$$

Следователно:

$$(35)\qquad \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^4 & 0 \\ 0 & \alpha^8 \end{bmatrix} . \begin{bmatrix} \alpha^7 \\ \alpha^0 \end{bmatrix} = \begin{bmatrix} \alpha^{11} + 0 \\ 0 + \alpha^8 \end{bmatrix} = \begin{bmatrix} \alpha^{11} \\ \alpha^8 \end{bmatrix},$$

откъдето следва:

$$(36)\qquad \sigma(x) = 1 + \sigma_1.x + \sigma_2.x^2 = \alpha^0 + \alpha^8.x + \alpha^{11}.x^2.$$

Следователно, нулите на полинома на локатора на грешката могат да се определят най-много след q проверки, което е изключително голямо намаление на сложността на процедурата за откриване и коригиране на грешки при кодовете на Рийд-Соломон (и въобще при произволни циклични кодове) в сравнение с необходимите по принцип q^{2t} проверки за решаване в $GF(2^m)$ на система уравнения с $2t$ неизвестни. Нулите на $\sigma(x)$ са реципрочни на елементите, показващи местата на сгрешените символи. След като се определят нулите на $\sigma(x)$, ще се знае къде са

сгрешените символи. За да се намерят нулите на полинома $\sigma(x)$ се правят 15 проверки с всички елементи на полето $GF(2^m)$. Резултатите за $\sigma(\alpha^i)$, които се получават, са:

(37) $\sigma(\alpha^0)=\alpha^0+\alpha^8.\alpha^0+\alpha^{11}.\alpha^0=\alpha^0+\alpha^8+\alpha^{11}=\alpha^2+\alpha^{11}=\alpha^9\neq 0,$

(38) $\sigma(\alpha^1)=\alpha^0+\alpha^8.\alpha^1+\alpha^{11}.\alpha^2=\alpha^0+\alpha^9+\alpha^{13}=\alpha^7+\alpha^{13}=\alpha^5\neq 0,$

(39) $\sigma(\alpha^2)=\alpha^0+\alpha^8.\alpha^2+\alpha^{11}.\alpha^4=\alpha^0+\alpha^{10}+\alpha^{15}=\alpha^0+\alpha^{10}+\alpha^0=\alpha^{10}\neq 0,$

(40) $\sigma(\alpha^3)=\alpha^0+\alpha^8.\alpha^3+\alpha^{11}.\alpha^6=\alpha^0+\alpha^{11}+\alpha^{17}=\alpha^{12}+\alpha^2=\alpha^7\neq 0,$

(41) $\sigma(\alpha^4)=\alpha^0+\alpha^8.\alpha^4+\alpha^{11}.\alpha^8=\alpha^0+\alpha^{12}+\alpha^{19}=\alpha^{11}+\alpha^4=\alpha^{13}\neq 0,$

(42) $\sigma(\alpha^5)=\alpha^0+\alpha^8.\alpha^5+\alpha^{11}.\alpha^{10}=\alpha^0+\alpha^{13}+\alpha^{21}=\alpha^6+\alpha^6=0\Rightarrow$ грешка,

(43) $\sigma(\alpha^6)=\alpha^0+\alpha^8.\alpha^6+\alpha^{11}.\alpha^{12}=\alpha^0+\alpha^{14}+\alpha^{23}=\alpha^3+\alpha^8=\alpha^{13}\neq 0,$

(44) $\sigma(\alpha^7)=\alpha^0+\alpha^8.\alpha^7+\alpha^{11}.\alpha^{14}=\alpha^0+\alpha^{15}+\alpha^{25}=\alpha^0+\alpha^0+\alpha^{10}=\alpha^{10}\neq 0,$

(45) $\sigma(\alpha^8)=\alpha^0+\alpha^8.\alpha^8+\alpha^{11}.\alpha^{16}=\alpha^0+\alpha^{16}+\alpha^{27}=\alpha^0+\alpha^1+\alpha^{12}=\alpha^4+\alpha^{12}=\alpha^6\neq 0,$

(46) $\sigma(\alpha^9)=\alpha^0+\alpha^8.\alpha^9+\alpha^{11}.\alpha^{18}=\alpha^0+\alpha^{17}+\alpha^{29}=\alpha^0+\alpha^2+\alpha^{14}=\alpha^8+\alpha^{14}=\alpha^6\neq 0,$

(47) $\sigma(\alpha^{10})=\alpha^0+\alpha^8.\alpha^{10}+\alpha^{11}.\alpha^{20}=\alpha^0+\alpha^{18}+\alpha^{31}=\alpha^0+\alpha^3+\alpha^1=\alpha^{14}+\alpha^1=\alpha^7\neq 0,$

(48) $\sigma(\alpha^{11})=\alpha^0+\alpha^8.\alpha^{11}+\alpha^{11}.\alpha^{22}=\alpha^0+\alpha^{19}+\alpha^{33}=\alpha^0+\alpha^4+\alpha^3=\alpha^1+\alpha^3=\alpha^9\neq 0,$

(49) $\sigma(\alpha^{12})=\alpha^0+\alpha^8.\alpha^{12}+\alpha^{11}.\alpha^{24}=\alpha^0+\alpha^{20}+\alpha^{35}=\alpha^0+\alpha^5+\alpha^5=\alpha^0\neq 0,$

(50) $\sigma(\alpha^{13})=\alpha^0+\alpha^8.\alpha^{13}+\alpha^{11}.\alpha^{26}=\alpha^0+\alpha^{21}+\alpha^{37}=\alpha^0+\alpha^6+\alpha^7=\alpha^{13}+\alpha^7=\alpha^5\neq 0,$

(51) $\sigma(\alpha^{14})=\alpha^0+\alpha^8.\alpha^{14}+\alpha^{11}.\alpha^{28}=\alpha^0+\alpha^{22}+\alpha^{39}=\alpha^0+\alpha^7+\alpha^9=\alpha^9+\alpha^9=0$
$\Rightarrow$ грешка.

Както се вижда, $\sigma(\alpha^5)=\sigma(\alpha^{14})=0$, т.е. нулите на полинома на локатора на грешката са α^5 и α^{14}, а за X_1 и X_2 се получава:

(52) $X_1=\dfrac{1}{\alpha^5}=\dfrac{\alpha^{15}}{\alpha^5}=\alpha^{10}, X_2=\dfrac{1}{\alpha^{14}}=\dfrac{\alpha^{15}}{\alpha^{14}}=\alpha^1.$

Оттук следва, че сгрешените символи в приетата кодова дума са коефициентите пред x^{10} и x^1 в израза за $B(x)$.

И така, в разгледания пример бяха открити две грешки в символите, които са коефициентите пред x^{10} и x^1 в израза за $B(x)$. Следва да се открият стойностите на грешките e_1 и e_2, свързани с позициите x^{10} и x^1. За разглеждания случай системата уравнения за $r(\alpha^i)$ се опростява до:

(53) $r(\alpha)=e_1.X_1+e_2.X_2$
$r(\alpha^2)=e_1.X_1^2+e_2.X_2^2$

Тъй като $r(\alpha)=S_1=\alpha^{11}$, $r(\alpha^2)=S_2=0$, $X_1=\alpha^{10}$, $X_2=\alpha^1$, то системата се записва във вида:

(54) $\begin{bmatrix} X_1 & X_2 \\ X_1^2 & X_2^2 \end{bmatrix}.\begin{bmatrix} e_1 \\ e_2 \end{bmatrix}=\begin{bmatrix} S_1 \\ S_2 \end{bmatrix}$, т.е. $\begin{bmatrix} \alpha^{10} & \alpha^1 \\ \alpha^{20} & \alpha^2 \end{bmatrix}.\begin{bmatrix} e_1 \\ e_2 \end{bmatrix}=\begin{bmatrix} \alpha^{11} \\ 0 \end{bmatrix}.$

За да се намерят стойностите на грешките e_1 и e_2 е необходимо да се изчисли обратната матрица на матрицата на коефициентите в последното матрично уравнение. Следователно:

$$B^{-1}=\begin{bmatrix}\alpha^{10} & \alpha^{1}\\ \alpha^{20} & \alpha^{2}\end{bmatrix}^{-1}=\begin{bmatrix}\alpha^{10} & \alpha^{1}\\ \alpha^{5} & \alpha^{2}\end{bmatrix}^{-1}=\frac{\begin{bmatrix}\alpha^{2} & \alpha^{1}\\ \alpha^{5} & \alpha^{10}\end{bmatrix}}{\alpha^{10}.\alpha^{2}-\alpha^{1}.\alpha^{5}}=\frac{\begin{bmatrix}\alpha^{2} & \alpha^{1}\\ \alpha^{5} & \alpha^{10}\end{bmatrix}}{\alpha^{12}-\alpha^{6}}=$$

(55)

$$=\frac{\begin{bmatrix}\alpha^{2} & \alpha^{1}\\ \alpha^{5} & \alpha^{10}\end{bmatrix}}{\alpha^{12}+\alpha^{6}}=\frac{\begin{bmatrix}\alpha^{2} & \alpha^{1}\\ \alpha^{5} & \alpha^{10}\end{bmatrix}}{\alpha^{4}}=\begin{bmatrix}\alpha^{13} & \alpha^{12}\\ \alpha^{1} & \alpha^{6}\end{bmatrix}.$$

Следователно за стойностите на грешките се получават:

$$\begin{bmatrix}e_1\\ e_2\end{bmatrix}=\begin{bmatrix}\alpha^{13} & \alpha^{12}\\ \alpha^{1} & \alpha^{6}\end{bmatrix}.\begin{bmatrix}\alpha^{11}\\ 0\end{bmatrix}=\begin{bmatrix}\alpha^{24}+0\\ \alpha^{12}+0\end{bmatrix}=\begin{bmatrix}\alpha^{9}\\ \alpha^{12}\end{bmatrix}. \quad (56)$$

Следователно, полиномът на грешката е:

$$E(x)=0.x^{14}+0.x^{13}+0.x^{12}+0.x^{11}+\alpha^{9}.x^{10}+0.x^{9}+0.x^{8}+$$
$$+0.x^{7}+0.x^{6}+0.x^{5}+0.x^{4}+0.x^{3}+0.x^{2}+\alpha^{12}.x+0, \quad (57)$$

което съответства на полинома на приетата двусимволната грешка. Тъй като в полето на Галоа $GF(2^4)$ операциите изваждане и събиране се изпълняват по модул 2 и по тази причина са еквивалентни, за да се отстранят грешките е достатъчно полиномът на грешките $E(x)$ да се прибави към полинома $B(x)$ на приетата кодова дума, т.е.:

$$C(x)=B(x)+E(x)=$$
$$=\alpha^{3}.x^{14}+\alpha^{7}.x^{13}+0.x^{12}+\alpha^{9}.x^{11}+\alpha^{7}.x^{10}+\alpha^{6}.x^{9}+\alpha^{2}.x^{8}+$$
$$+\alpha^{14}.x^{7}+\alpha^{4}.x^{6}+0.x^{5}+\alpha^{11}.x^{4}+\alpha^{5}.x^{3}+\alpha^{6}.x^{2}+\alpha^{11}.x+\alpha^{13}+$$
$$+0.x^{14}+0.x^{13}+0.x^{12}+0.x^{11}+\alpha^{9}.x^{10}+0.x^{9}+0.x^{8}+ \quad (58)$$
$$+0.x^{7}+0.x^{6}+0.x^{5}+0.x^{4}+0.x^{3}+0.x^{2}+\alpha^{12}.x+0=$$
$$=\alpha^{3}.x^{14}+\alpha^{7}.x^{13}+0.x^{12}+\alpha^{9}.x^{11}+\alpha^{0}.x^{10}+\alpha^{6}.x^{9}+\alpha^{2}.x^{8}+$$
$$+\alpha^{14}.x^{7}+\alpha^{4}.x^{6}+0.x^{5}+\alpha^{11}.x^{4}+\alpha^{5}.x^{3}+\alpha^{6}.x^{2}+\alpha^{0}.x+\alpha^{13}.$$

Тъй като символите на съобщението се съдържат в първите $k=11$ символа, декодерът ще изведе следното съобщение:

$$\begin{matrix}\alpha^{3}\\ \begin{bmatrix}0\\0\\0\\1\end{bmatrix}\end{matrix}\quad\begin{matrix}\alpha^{7}\\ \begin{bmatrix}1\\1\\0\\1\end{bmatrix}\end{matrix}\quad\begin{matrix}0\\ \begin{bmatrix}0\\0\\0\\0\end{bmatrix}\end{matrix}\quad\begin{matrix}\alpha^{9}\\ \begin{bmatrix}0\\1\\0\\1\end{bmatrix}\end{matrix}\quad\begin{matrix}\alpha^{0}\\ \begin{bmatrix}1\\0\\0\\0\end{bmatrix}\end{matrix}\quad\begin{matrix}\alpha^{6}\\ \begin{bmatrix}0\\0\\1\\1\end{bmatrix}\end{matrix}\quad\begin{matrix}\alpha^{2}\\ \begin{bmatrix}0\\0\\1\\0\end{bmatrix}\end{matrix}\quad\begin{matrix}\alpha^{14}\\ \begin{bmatrix}1\\0\\0\\1\end{bmatrix}\end{matrix}\quad\begin{matrix}\alpha^{4}\\ \begin{bmatrix}1\\1\\0\\0\end{bmatrix}\end{matrix}\quad\begin{matrix}0\\ \begin{bmatrix}0\\0\\0\\0\end{bmatrix}\end{matrix}\quad\begin{matrix}\alpha^{11}\\ \begin{bmatrix}0\\1\\1\\1\end{bmatrix}\end{matrix}\quad\Rightarrow$$

(59)

$$\Rightarrow$$

$$1000\,1011\,0000\,1010\,0001\,1100\,0100\,1001\,0011\,0000\,1110.$$

Това съобщение съответства точно на съобщението, което беше избрано в началото на примера.

ЗАКЛЮЧЕНИЕ

В публикацията е представена методика за построяване на код на Рийд-Соломон с дължина $n=15$, коригиращ двусимволна грешка, който е базиран на полето на Галоа $GF(2^4)$, породено от примитивния неразложим полином $f(x)=x^4+x+1$, като е изведена таблицата за събиране в посоченото поле. Илюстрирани са процесите на кодиране на зададена информационна дума при използване на разглеждания код на

Рийд-Соломон и на декодиране, при въвеждане на грешка в два символа. Материалът намира приложение в учебния процес по избираемата дисциплина „Кодиране в телекомуникационните системи”, включена в учебния план на специалността „Телекомуникационни системи”, образователно-квалификационна степен „Бакалавър”.

ЛИТЕРАТУРА

[1] Блейхут, Р., Теория и практика кодов, контролирующих ошибки. Перевод с англ. И.И. Грушко и В.М. Блиновского, Москва, Мир, 1986.

[2] Пенчева, Е. GSM комуникации, София, Нови знания, 2000.

[3] Попов, М.К. Клетъчни радиотелефонни системи. София, Свети Георги Победоносец, 1998.

[4] Sklar, B. Digital Communications. Fundamental and Applications (Second Edition). Prentice Hall PTR, 2002.

[5] ecet.ecs.uni-ruse.bg/else – факултет ЕЕА, специалност ТКС, дисциплина КТКС.

[6] Бороджиева, А. Кодиране и декодиране с код на Рийд-Соломон (7,3), базиран на полето на Галоа $GF(2^3)$, при въвеждане на двусимволна грешка. Научно списание „Механика, Транспорт, Комуникации”, Том 13, Брой 1/2015, стр. XI-1 – XI-12, ISSN: 1312-3823 (print), 2367-6620 (online).

[7] Clarke, C.K.P. Reed-Solomon error correction. BBC R&D White Paper WHP 031, July, 2002, http://downloads.bbc.co.uk/rd/pubs/whp/whp-pdf-files/WHP031.pdf.

ENCODING AND DECODING USING (15,11) REED-SOLOMON CODES, BASED ON GALOIS FIELD $GF(2^4)$, WITH TWO-SYMBOL ERRORS

Adriana Borodzhieva
aborodjieva@ecs.uni-ruse.bg

University of Ruse “Angel Kanchev”,
7017 Ruse, 8 Studentska Str.
BULGARIA

Key words: *Encoding, decoding, Reed-Solomon codes, error detection and correction.*

Abstract: *The paper describes the processes of encoding and decoding using (15,11) Reed-Solomon code, based on Galois field $GF(2^4)$, generated by a primitive irreducible polynomial $f(x) = x^4 + x + 1$. An example for creating a generator polynomial of the Reed-Solomon code is given. This code will detect and correct errors occurring in two symbols of the codeword, as these symbols may be consecutive, i.e. in a series of 8 consecutive bits. The process of encoding a 44-bit information word is illustrated. After introducing errors in two symbols in the codeword, the processes of detecting and correcting errors in the codeword, and decoding are illustrated. The material is used in the course “Coding in Telecommunication Systems”, included as optional in the curriculum of the specialty “Telecommunication Systems” for the Bachelor degree.*