SAT-2G.302-2-CSNT-01

Encoding using (15,9) Reed-Solomon codes, based on Galois field GF(2^4), correcting three-symbol errors

Adriana Borodzhieva

Кодиране с код на Рийд-Соломон (15,9), базиран на полето на Галоа GF(2^4), коригиращ трисимволна грешка

Адриана Бороджиева

Abstract: *The paper describes the process of encoding a message using (15,9) 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 three symbols of the codeword. The process of encoding a 36-bit information word is 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.*

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

ВЪВЕДЕНИЕ

Кодовете на Рийд-Соломон са създадени през 1960 г., от Irving S. Reed и Gustave Solomon. Описани са в тяхната публикация „Полиномиални кодове над някои крайни полета". Тогава не е бил известен все още ефективен алгоритъм за тяхното декодиране. Решение на този проблем е открит по-късно, през 1969 г., от Elwyn Berlekamp и James Massey, наречен впоследствие на името на своите откриватели (алгоритъм за декодиране на Берлекемп-Меси) [1, 3, 4].

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 на кодовете на Рийд-Соломон в масово-произвеждани потребителски продукти е през 1982 г., в компакт-дисковете, където се използва съчетаването 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, 4].

При тези кодове се използват 2^m различни символа, представляващи *m*-битови последователности, които се разглеждат като елементи на полето на Галоа $GF\left(2^m\right)$. Кодовете на Рийд-Соломон (*n*, *k*) съществуват за всяко *n* и *k*, за които [1, 2, 3, 4]:

$$0 < k < n < 2^m + 2, \tag{1}$$

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, 2, 3, 4].

За кодовете на Рийд-Соломон е в сила:

$$(n,k) = \left(2^m - 1, 2^m - 1 - 2.t\right), \tag{2}$$

където *t* е броят на грешките, които кодът може да коригира; $r = n - k = 2t$ е броят на контролните символи [1, 2, 3, 4].

КОДИРАНЕ С ИЗПОЛЗВАНЕ НА КОД НА РИЙД-СОЛОМОН

Въз основа на описания в [2, 3] алгоритъм за построяване на код на Рийд-Соломон с дължина $n = 7$, коригиращ грешки в два символа, базиран на полето на Галоа $GF\left(2^3\right)$, 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 $n=15$, коригиращ трисимволна грешка, който е базиран на полето на Галоа $GF(2^4)$, породено от примитивния неразложим полином от четвърта степен $f(x)=x^4+x+1$. Илюстриран е процесът на кодиране на зададена информационна дума при използване на разглеждания код на Рийд-Соломон. По условие, кодът може да коригира грешки в три символа, т.е. $t=3$. 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. Операциите в полето се извършват по модул $f(x)=x^4+x+1$.

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}

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

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

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:

$$
\begin{aligned}
P(x) &= (x-\alpha).\left(x-\alpha^2\right).\left(x-\alpha^3\right).\left(x-\alpha^4\right).\left(x-\alpha^5\right).\left(x-\alpha^6\right)= \\
&= \left(x^2-\alpha x-\alpha^2 x+\alpha^3\right).\left(x^2-\alpha^3 x-\alpha^4 x+\alpha^7\right).\left(x^2-\alpha^5 x-\alpha^6 x+\alpha^{11}\right)= \\
&= \left[x^2-\left(\alpha^1+\alpha^2\right)x+\alpha^3\right].\left[x^2-\left(\alpha^3+\alpha^4\right)x+\alpha^7\right].\left[x^2-\left(\alpha^5+\alpha^6\right)x+\alpha^{11}\right]= \\
&= \left(x^2-\alpha^5 x+\alpha^3\right).\left(x^2-\alpha^7 x+\alpha^7\right).\left(x^2-\alpha^9 x+\alpha^{11}\right)= \\
&= \left(x^4-\alpha^7 x^3+\alpha^7 x^2-\alpha^5 x^3+\alpha^{12}x^2-\alpha^{12}x+\alpha^3 x^2-\alpha^{10}x+\alpha^{10}\right)\left(x^2-\alpha^9 x+\alpha^{11}\right)= \\
&= \left[x^4-\left(\alpha^7+\alpha^5\right)x^3+\left(\underbrace{\alpha^7+\alpha^{12}}_{\alpha^2}+\alpha^3\right)x^2-\left(\alpha^{12}+\alpha^{10}\right)x+\alpha^{10}\right]\left(x^2-\alpha^9 x+\alpha^{11}\right)= \qquad (4) \\
&= \left(x^4+\alpha^{13}x^3+\alpha^6 x^2+\alpha^3 x+\alpha^{10}\right)\left(x^2+\alpha^9 x+\alpha^{11}\right)=x^6+\alpha^{13}x^5+\alpha^6 x^4+\alpha^3 x^3+\alpha^{10}x^2+ \\
&+\alpha^9 x^5+\alpha^{22}x^4+\alpha^{15}x^3+\alpha^{12}x^2+\alpha^{19}x+\alpha^{11}x^4+\alpha^{24}x^3+\alpha^{17}x^2+\alpha^{14}x+\alpha^{21}= \\
&= x^6+\left(\alpha^{13}+\alpha^9\right)x^5+\left(\underbrace{\alpha^6+\alpha^7}_{\alpha^{10}}+\alpha^{11}\right)x^4+\left(\underbrace{\alpha^3+\alpha^0}_{\alpha^{14}}+\alpha^9\right)x^3+\left(\underbrace{\alpha^{10}+\alpha^{12}}_{\alpha^3}+\alpha^2\right)x^2+ \\
&+\left(\alpha^4+\alpha^{14}\right)x+\alpha^6=x^6+\alpha^{10}x^5+\alpha^{14}x^4+\alpha^4 x^3+\alpha^6 x^2+\alpha^9 x+\alpha^6.
\end{aligned}
$$

При пресмятането е използвано, че операцията изваждане е еквивалентна на операцията събиране в полето на Галоа $GF\left(2^4\right)$ с основа 2. Събирането в полето на Галоа $GF\left(2^4\right)$ се осъществява съгласно таблица 2, а умножението се извършва съгласно правилото:

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

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 при кодовете на Рийд-Соломон ще бъде пояснен като се използва даденият по-долу пример.

Тъй като $t=3$, то разглежданият код на Рийд-Соломон може да открива и коригира всички трикратни грешки в кодовите думи. За коригиране на трисимволна грешка е необходимо да се определят стойностите на шест неизвестни – три от тях се отнасят за разположението на грешката, а другите три – за нейната стойност. За разлика 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 обратно, 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 шест неизвестни, следователно са необходими шест уравнения, за да се определят неизвестните. Следователно, броят на контролните символи е $r = 2t = 6$.

При $n = 15$, броят на информационните символи е $k = 9$, като всеки от тях представлява четирибитов вектор-стълб, който се разглежда като елемент на $GF\left(2^4\right)$. След тези уточнения, алгоритъмът за кодиране на битовете на съобщението 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 36 информационни бита (ASCII-кодовете на съобщението "ASCII", т.е. 5 x 7 = 35 бита, допълнени с един бит, формиращ контрол по нечетност):

1000001 1010011 1000011 1001001 1001001 + **0**.

Тези 36 бита се групират в 9 четирибитови символа:

1000 0011 0100 1110 0001 1100 1001 1001 0010.

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

$$\begin{bmatrix}0\\0\\0\\1\end{bmatrix}=\alpha^3,\begin{bmatrix}1\\1\\0\\0\end{bmatrix}=\alpha^4,\begin{bmatrix}0\\0\\1\\0\end{bmatrix}=\alpha^2,\begin{bmatrix}0\\1\\1\\1\end{bmatrix}=\alpha^{11},\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=\alpha^0,\begin{bmatrix}0\\0\\1\\1\end{bmatrix}=\alpha^6,\begin{bmatrix}1\\0\\0\\1\end{bmatrix}=\alpha^{14},\begin{bmatrix}1\\0\\0\\1\end{bmatrix}=\alpha^{14},\begin{bmatrix}0\\1\\0\\0\end{bmatrix}=\alpha^1. \qquad (6)$$

Стъпка 2. За разглеждания код на Рийд-Соломон, генераторният полином, съгласно формула (4), е $P(x) = x^6 + \alpha^{10}x^5 + \alpha^{14}x^4 + \alpha^4x^3 + \alpha^6x^2 + \alpha^9x + \alpha^6$.

Стъпка 3. На информационната дума 1000 0011 0100 1110 0001 1100 1001 1001 0010 съответства полиномът:

$$A(x) = \alpha^3.\,x^8 + \alpha^4.\,x^7 + \alpha^2.\,x^6 + \alpha^{11}.\,x^5 + \alpha^0.\,x^4 + \alpha^6.\,x^3 + \alpha^{14}.\,x^2 + \alpha^{14}.\,x + \alpha^1. \qquad (7)$$

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^6, така че информационните символи ще заемат най-старшите девет позиции на полинома, съответстващ на разрешената кодова дума. След това, $A(x).x^6$ 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 $GF\left(2^4\right)$ операциите изваждане и събиране се изпълняват по модул 2 и по тази причина са еквивалентни) [3, 4].

информация

1	α^3	α^4	α^2	α^{11}	α^0	α^6	α^{14}	α^{14}	α^1	0	0	0	0	0	0
2	α^3	α^{13}	α^{17}	α^7	α^9	α^{12}	α^9								
3		α^{11}	0	α^8	α^7	α^4	α^4	α^{14}							
4		α^{11}	α^{21}	α^{25}	α^{15}	α^{17}	α^{20}	α^{17}							
5			α^6	α^1	α^9	α^{10}	α^8	α^{13}	α^1						
6			α^6	α^{16}	α^{20}	α^{10}	α^{12}	α^{15}	α^{12}						
7				0	α^6	0	α^9	α^6	α^{13}	0	0				
8					α^6	α^{16}	α^{20}	α^{10}	α^{12}	α^{15}	α^{12}				
9						α^1	α^6	α^7	α^1	α^0	α^{12}	0			
10						α^1	α^{11}	α^{15}	α^5	α^7	α^{10}	α^7			
11							α^1	α^9	α^2	α^9	α^3	α^7	0		
12							α^1	α^{11}	α^{15}	α^5	α^7	α^{10}	α^7		
13								α^2	α^8	α^6	α^4	α^6	α^7	0	
14								α^2	α^{12}	α^{16}	α^6	α^8	α^{11}	α^8	
15									α^9	α^{11}	α^{12}	α^{14}	α^8	α^8	0
16									α^9	α^{19}	α^{23}	α^{13}	α^{15}	α^{18}	α^{15}
17										α^{13}	α^9	α^2	α^2	α^{13}	α^0

α^0	α^{10}	α^{14}	α^4	α^6	α^9	α^6		
α^3	α^{11}	α^6	0	α^6	α^1	α^1	α^2	α^9

частно

остатък

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

Вижда се, че остатъкът от делението на $A(x).x^6$ с генераторния полином $P(x)$ е $R(x)=\alpha^{13}.x^5+\alpha^9.x^4+\alpha^2.x^3+\alpha^2.x^2+\alpha^{13}.x+\alpha^0$.

Трябва да се отбележи, че коефициентите на редове 3, 5, 7, 9, 11, 13, 15 и 17 (фиг. 1) се получават чрез 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:

$$\alpha^4+\alpha^{13}=\alpha^{11};\ \alpha^2+\alpha^{17}=\alpha^2+\alpha^2=0;\ \alpha^{11}+\alpha^7=\alpha^8;$$
$$\alpha^0+\alpha^9=\alpha^7;\ \alpha^6+\alpha^{12}=\alpha^4;\ \alpha^{14}+\alpha^9=\alpha^4; \qquad \text{(за ред № 3)} \qquad (8);$$

$$0+\alpha^{21}=0+\alpha^6=\alpha^6;\ \alpha^8+\alpha^{25}=\alpha^8+\alpha^{10}=\alpha^1;$$
$$\alpha^7+\alpha^{15}=\alpha^7+\alpha^0=\alpha^9;\ \alpha^4+\alpha^{17}=\alpha^4+\alpha^2=\alpha^{10}; \qquad \text{(за ред № 5);} \qquad (9)$$
$$\alpha^4+\alpha^{20}=\alpha^4+\alpha^5=\alpha^8;\ \alpha^{14}+\alpha^{17}=\alpha^{14}+\alpha^2=\alpha^{13};$$

$$\alpha^1+\alpha^{16}=\alpha^1+\alpha^1=0;\ \alpha^9+\alpha^{20}=\alpha^9+\alpha^5=\alpha^6;\ \alpha^{10}+\alpha^{10}=0;$$
$$\alpha^8+\alpha^{12}=\alpha^9;\ \alpha^{13}+\alpha^{15}=\alpha^{13}+\alpha^0=\alpha^6;\ \alpha^1+\alpha^{12}=\alpha^{13}; \qquad \text{(за ред № 7);} \qquad (10)$$

$$0+\alpha^{16}=0+\alpha^1=\alpha^1;\ \alpha^9+\alpha^{20}=\alpha^9+\alpha^5=\alpha^6;\ \alpha^6+\alpha^{10}=\alpha^7;$$
$$\alpha^{13}+\alpha^{12}=\alpha^1;\ 0+\alpha^{15}=0+\alpha^0=\alpha^0;\ 0+\alpha^{12}=\alpha^{12}; \qquad \text{(за ред № 9);} \qquad (11)$$

$$\alpha^6+\alpha^{11}=\alpha^1;\ \alpha^7+\alpha^{15}=\alpha^7+\alpha^0=\alpha^9;\ \alpha^1+\alpha^5=\alpha^2;$$
$$\alpha^0+\alpha^7=\alpha^9;\ \alpha^{12}+\alpha^{10}=\alpha^3;\ 0+\alpha^7=\alpha^7; \qquad \text{(за ред № 11);} \qquad (12)$$

$$\alpha^9+\alpha^{11}=\alpha^2;\ \alpha^2+\alpha^{15}=\alpha^2+\alpha^0=\alpha^8;\ \alpha^9+\alpha^5=\alpha^6;$$
$$\alpha^3+\alpha^7=\alpha^4;\ \alpha^7+\alpha^{10}=\alpha^6;\ 0+\alpha^7=\alpha^7; \qquad \text{(за ред № 13);} \qquad (13)$$

$$\alpha^8+\alpha^{12}=\alpha^9;\ \alpha^6+\alpha^{16}=\alpha^6+\alpha^1=\alpha^{11};\ \alpha^4+\alpha^6=\alpha^{12};$$
$$\alpha^6+\alpha^8=\alpha^{14};\ \alpha^7+\alpha^{11}=\alpha^8;\ 0+\alpha^8=\alpha^8; \qquad \text{(за ред № 15);} \qquad (14)$$

$$\alpha^{11}+\alpha^{19}=\alpha^{11}+\alpha^4=\alpha^{13};\ \alpha^{12}+\alpha^{23}=\alpha^{12}+\alpha^8=\alpha^9;$$
$$\alpha^{14}+\alpha^{13}=\alpha^2;\ \alpha^8+\alpha^{15}=\alpha^8+\alpha^0=\alpha^2; \qquad \text{(за ред № 17).} \qquad (15)$$
$$\alpha^8+\alpha^{18}=\alpha^8+\alpha^3=\alpha^{13};\ 0+\alpha^{15}=0+\alpha^0=\alpha^0.$$

За да се дели полиномът на разрешената кодова комбинация без остатък на генераторния полином $P(x)$, към $A(x).x^6$ 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:

$$\begin{aligned} C(x) &= A(x).x^6 + R(x) = \alpha^3.x^{14} + \alpha^4.x^{13} + \alpha^2.x^{12} + \alpha^{11}.x^{11} + \alpha^0.x^{10} + \alpha^6.x^9 + \\ &+ \alpha^{14}.x^8 + \alpha^{14}.x^7 + \alpha^1.x^6 + \alpha^{13}.x^5 + \alpha^9.x^4 + \alpha^2.x^3 + \alpha^2.x^2 + \alpha^{13}.x + \alpha^0 = \\ &= \begin{bmatrix}0\\0\\0\\1\end{bmatrix}.x^{14} + \begin{bmatrix}1\\1\\0\\0\end{bmatrix}.x^{13} + \begin{bmatrix}0\\0\\1\\0\end{bmatrix}.x^{12} + \begin{bmatrix}0\\1\\1\\1\end{bmatrix}.x^{11} + \begin{bmatrix}1\\0\\0\\0\end{bmatrix}.x^{10} + \begin{bmatrix}0\\0\\1\\1\end{bmatrix}.x^{9} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix}.x^{8} + \\ &+ \begin{bmatrix}1\\0\\0\\1\end{bmatrix}.x^{7} + \begin{bmatrix}0\\1\\0\\0\end{bmatrix}.x^{6} + \begin{bmatrix}1\\0\\1\\1\end{bmatrix}.x^{5} + \begin{bmatrix}0\\1\\0\\1\end{bmatrix}.x^{4} + \begin{bmatrix}0\\0\\1\\0\end{bmatrix}.x^{3} + \begin{bmatrix}0\\0\\1\\0\end{bmatrix}.x^{2} + \begin{bmatrix}1\\0\\1\\1\end{bmatrix}.x + \begin{bmatrix}1\\0\\0\\0\end{bmatrix}. \end{aligned} \tag{16}$$

Следователно, информационната дума 1000 0011 0100 1110 0001 1100 1001 1001 0010 се допълва с още 24 бита, представляващи 6 четирибитови контролни символа и в комуникационния канал се излъчва кодовата дума 1000 0011 0100 1110 0001 1100 1001 1001 0010 1101 1010 0100 0100 1101 0001, т.е. относителната скорост на предаване на информацията за разглеждания код е $9/15$.

ПРИЛОЖЕНИЕ НА МЕТОДИКАТА В УЧЕБНИЯ ПРОЦЕС

С цел по-добро усвояване на преподавания материал се прилагат активни методи на обучение, като на всеки студент се задава индивидуално задание, включващо неразложим примитивен полином от 3-та степен и зададено 9-битово съобщение за кодиране. По време на практическото упражнение, студентът трябва да реши своето задание на предварително изготвена бланка, публикувана в платформата за електронно обучение на Русенски университет „Ангел Кънчев” [3], и да представи на преподавателя в края на часа. Представената методика за синтез на код на Рийд-Соломон се използва от учебната 2011-2012 година в учебния процес по дисциплината „Кодиране в телекомуникационните системи”, включена като избираема в учебния план на специалността „Телекомуникационни системи”, за студенти от образователно-квалификационна степен „Бакалавър”, като резултатите от текущия контрол се публикуват в сайта за електронно обучение [3].

По време на практическото упражнение върху темата за кодове на Рийд-Соломон, студентите трябва да построят генераторния полином на код на Рийд-Соломон с параметри $n = 7$, $k = 3$, който открива и коригира двукратна грешка. При синтеза трябва да се използва неразложимият примитивен полином $f(x) = x^3 + x + 1$.

На любознателните студенти се дава възможност и за допълнителна самостоятелна работа – извеждане на генераторния полином на кодове на Рийд-Соломон с параметри $n = 15$, $k = 11$ или $k = 9$, който открива и коригира двукратна или трикратна грешка, базиран на полето на Галоа $GF(2^4)$, породено от неразложимия примитивен полином от четвърта степен $f(x) = x^4 + x + 1$ или $f(x) = x^4 + x^3 + 1$. Както се вижда, процесите на синтезиране на генераторния полином и на кодиране на съобщението за разглеждания код на Рийд-Соломон е доста времеотнемащ и най-често продължителността на упражнението от 90 минути е твърде недостатъчна за цялостното решаване на подобна задача в рамките на упражнението. Но определянето на кодовата дума при изведени генераторен полином и таблица за събиране в полето на Галоа (таблица 2) вече е по силите на отличните студенти.

ЗАКЛЮЧЕНИЕ

В публикацията е представена методика за построяване на код на Рийд-Соломон с дължина $n = 15$, коригиращ трисимволна 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. Илюстриран е процесът на кодиране на зададена информационна дума при използване на разглеждания код на Рийд-Соломон. 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] Sklar, B. Digital Communications. Fundamental and Applications (Second Edition). Prentice Hall PTR, 2002.

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

[4] en.wikipedia.org/wiki/Reed–Solomon_error_correction

За контакти:

гл. ас. д-р Адриана Бороджиева, Катедра „Телекомуникации", Русенски университет „Ангел Кънчев", тел.: 082-888 734, e-mail: aborodzhieva@uni-ruse.bg.