Механика Транспорт Комуникации

Научно списание http://www.mtc-aj.com

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
том 13, брой 1, 2015 г.
статия № 1104

КОДИРАНЕ И ДЕКОДИРАНЕ С КОД НА РИЙД-СОЛОМОН (7,3), БАЗИРАН НА ПОЛЕТО НА ГАЛОА *GF*(2^3), 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 (7,3), базиран на полето на Галоа GF(2^3), породено от неразложимия примитивен полином $f(x) = x^3 + x^2 + 1$. 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 6 последователни бита. Илюстриран е процесът на кодиране на 9-битова информационна дума. След въвеждане на грешки в два символа се илюстрира 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 компак-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, 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, 6].

За кодовете на Рийд-Соломон е в сила:

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

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

КОДИРАНЕ И ДЕКОДИРАНЕ С ИЗПОЛЗВАНЕ НА КОД НА РИЙД-СОЛОМОН

Въз основа на описания в [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 $n = 7$, отново коригиращ двусимволна грешка, който е базиран на полето на Галоа $GF(2^3)$, породено от другия възможен примитивен неразложим полином от трета степен $f(x) = x^3 + x^2 + 1$. Илюстрирани са процесите на кодиране на зададена информационна дума (101 001 111) 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 $n = 7$, то се използва полето на Галоа $GF(2^3)$, породено от примитивния неразложим полином $f(x) = x^3 + x^2 + 1$. Елементите на полето $GF(2^3)$ са дадени в таблица 1. Операциите в полето се извършват по модул $f(x) = x^3 + x^2 + 1$.

Таблица 1. Елементи на полето $GF(2^3)$, породено от $f(x) = x^3 + x^2 + 1$

№	Полином от втора степен	Наредена n-торка	Степени на $\alpha = x$
0	$0.x^2 + 0.x + 0$	0 0 0	0
1	$0.x^2 + 0.x + 1$	0 0 1	α^0
2	$0.x^2 + 1.x + 0$	0 1 0	α^1
3	$0.x^2 + 1.x + 1$	0 1 1	α^5
4	$1.x^2 + 0.x + 0$	1 0 0	α^2
5	$1.x^2 + 0.x + 1$	1 0 1	α^3
6	$1.x^2 + 1.x + 0$	1 1 0	α^6
7	$1.x^2 + 1.x + 1$	1 1 1	α^4

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:

$$
\begin{aligned}
&P(x)=(x-\alpha).(x-\alpha^2).(x-\alpha^3).(x-\alpha^4)= \\
&=(x^2-\alpha x-\alpha^2 x+\alpha^3).(x^2-\alpha^3 x-\alpha^4 x+\alpha^7)= \\
&=\left[x^2-(\alpha^1+\alpha^2)x+\alpha^3\right].\left[x^2-(\alpha^3+\alpha^4)x+\alpha^7\right]=(x^2-\alpha^6 x+\alpha^3).(x^2-\alpha^1 x+1)= \\
&=x^4-\alpha^1 x^3+x^2-\alpha^6 x^3+\underbrace{\alpha^7}_{\alpha^0}x^2-\alpha^6 x+\alpha^3 x^2-\alpha^4 x+\alpha^3= \\
&=x^4-(\alpha^1+\alpha^6)x^3+\underbrace{\alpha^0 x^2+\alpha^0 x^2}_{0}+\alpha^3 x^2-(\alpha^6+\alpha^4)x+\alpha^3= \\
&=x^4+\alpha^2 x^3+\alpha^3 x^2+x+\alpha^3.
\end{aligned}
\tag{4}
$$

При пресмятането е използвано, че операцията изваждане е еквивалентна на операцията събиране в полето на Галоа $GF(2^3)$ с основа 2.

Алгоритъмът за кодиране и декодиране при кодовете на Рийд-Соломон ще бъде пояснен като се използва дадения пример. За удобство първо се привеждат таблиците за сумиране и умножение в полето $GF(2^3)$.

Таблица 2. Сумиране в поле $GF(2^3)$, породено от $f(x) = x^3 + x^2 + 1$

	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^0	0	α^5	α^3	α^2	α^6	α^1	α^4
α^1	α^5	0	α^6	α^4	α^3	α^0	α^2
α^2	α^3	α^6	0	α^0	α^5	α^4	α^1
α^3	α^2	α^4	α^0	0	α^1	α^6	α^5
α^4	α^6	α^3	α^5	α^1	0	α^2	α^0
α^5	α^1	α^0	α^4	α^6	α^2	0	α^3
α^6	α^4	α^2	α^1	α^5	α^0	α^3	0

Таблица 3. Умножение в поле $GF(2^3)$, породено от $f(x) = x^3 + x^2 + 1$

	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^0	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^1	α^1	α^2	α^3	α^4	α^5	α^6	α^0
α^2	α^2	α^3	α^4	α^5	α^6	α^0	α^1
α^3	α^3	α^4	α^5	α^6	α^0	α^1	α^2
α^4	α^4	α^5	α^6	α^0	α^1	α^2	α^3
α^5	α^5	α^6	α^0	α^1	α^2	α^3	α^4
α^6	α^6	α^0	α^1	α^2	α^3	α^4	α^5

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 $n=7$, броят на информационните символи е $k=3$, като всеки от тях преставлява трибитов вектор-стълб, който се разглежда като елемент на $GF(2^3)$. 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 9 информационни бита 101 001 111. Тези 9 бита се групират в три трибитови символа 101, 001 и 111. Като се използва таблица 1 се установява, че на посочените трибитови символи съответстват следните елементи от $GF(2^3)$:

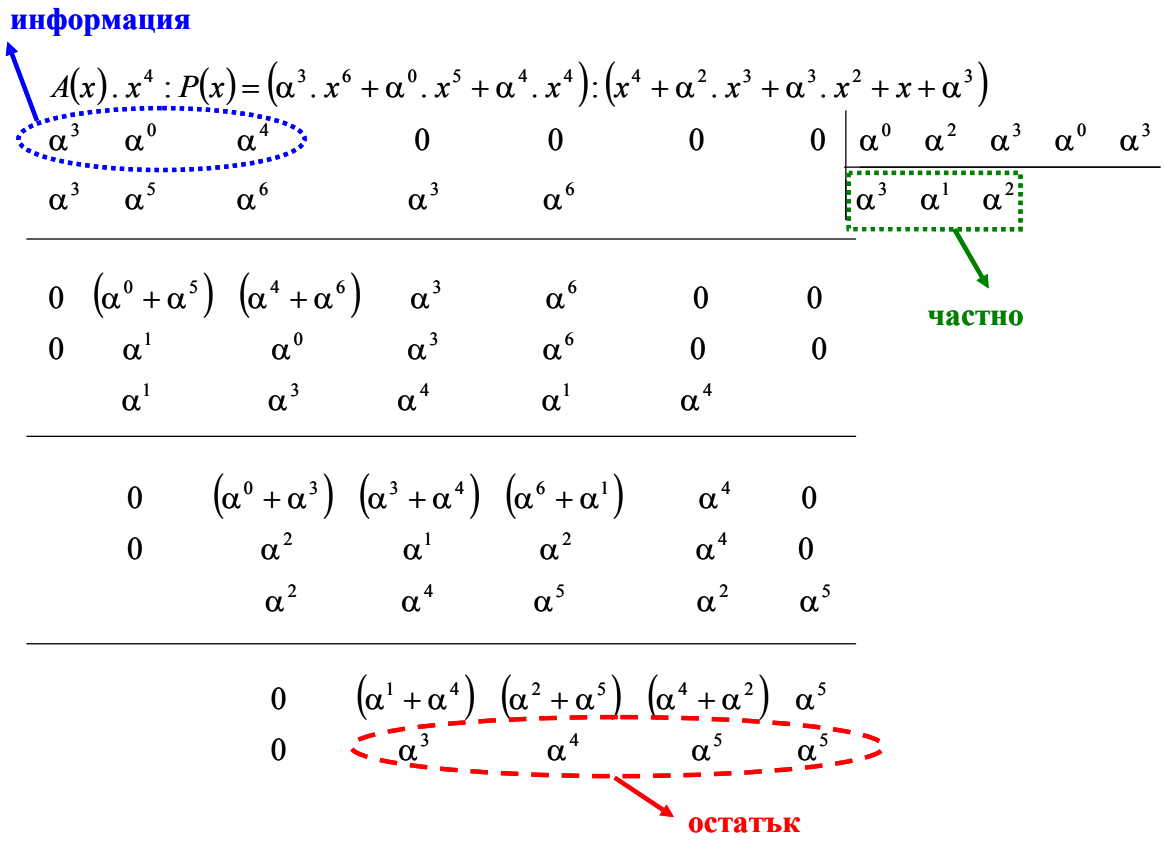
(5) $$\begin{bmatrix}1\\0\\1\end{bmatrix}=\alpha^3,\quad \begin{bmatrix}1\\0\\0\end{bmatrix}=\alpha^0,\quad \begin{bmatrix}1\\1\\1\end{bmatrix}=\alpha^4.$$

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

Стъпка 3. На информационната дума 101 001 111 съответства полиномът:

(6) $$A(x)=\alpha^3.x^2+\alpha^0.x+\alpha^4.$$

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 поставят 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 „чистата информационна" дума $A(x)$ се умножава с x^4, така че информационните символи ще заемат трите най-старши 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 таблица 3 (в изчисленията по-долу се използва, че в полето на Галоа $GF(2^3)$ 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 $R(x)=\alpha^3.x^3+\alpha^4.x^2+\alpha^5.x+\alpha^5$.

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 $GF(2^3)$ операциите изваждане и събиране се изпълняват по модул 2 и по тази причина са еквивалентни) и резултатът е:

$$C(x)=A(x).x^4+R(x)=\alpha^3.x^6+\alpha^0.x^5+\alpha^4.x^4+\alpha^3.x^3+\alpha^4.x^2+\alpha^5.x+\alpha^5=$$

$$(7)\qquad =\begin{bmatrix}1\\0\\1\end{bmatrix}.x^6+\begin{bmatrix}1\\0\\0\end{bmatrix}.x^5+\begin{bmatrix}1\\1\\1\end{bmatrix}.x^4+\begin{bmatrix}1\\0\\1\end{bmatrix}.x^3+\begin{bmatrix}1\\1\\1\end{bmatrix}.x^2+\begin{bmatrix}1\\1\\0\end{bmatrix}.x+\begin{bmatrix}1\\1\\0\end{bmatrix}.$$

Следователно, „чистата информационна" дума 101 001 111 се допълва с още 12 бита, представляващи 4 трибитови контролни символа и в комуникационния канал се излъчва кодовата дума 101 001 111 101 111 011 011, т.е. относителната скорост на предаване на информацията за разглеждания код е $3/7$.

Нека при предаване на кодовата дума два символа са повредени от шумовете и са приети с грешка. Това количество грешки съответства на максималната възможност на кода да коригира грешки.

При използване на 7-символна кодова дума, моделът на грешката може да се представи във вида $E(x)=\sum_{k=0}^{6}e_k.x^k$.

За определеност нека двусимволната грешка се представя с полинома:

$$(8)\qquad E(x)=\begin{bmatrix}1\\0\\0\end{bmatrix}.x^6+\begin{bmatrix}0\\0\\0\end{bmatrix}.x^5+\begin{bmatrix}0\\0\\0\end{bmatrix}.x^4+\begin{bmatrix}0\\0\\0\end{bmatrix}.x^3+\begin{bmatrix}1\\1\\1\end{bmatrix}.x^2+\begin{bmatrix}0\\0\\0\end{bmatrix}.x+\begin{bmatrix}0\\0\\0\end{bmatrix}=$$

$$=\alpha^0.x^6+0.x^5+0.x^4+0.x^3+\alpha^4.x^2+0.x+0.$$

С други думи, най-младшият бит на първия информационен символ е сгрешен (представен като α^0) и трите бита на втория контролен символ на съобщението са сгрешени (представено като α^4). Следователно, полиномът на грешно приетата кодова дума е:

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

$$(9)\qquad =\begin{bmatrix}0\\0\\1\end{bmatrix}.x^6+\begin{bmatrix}1\\0\\0\end{bmatrix}.x^5+\begin{bmatrix}1\\1\\1\end{bmatrix}.x^4+\begin{bmatrix}1\\0\\1\end{bmatrix}.x^3+\begin{bmatrix}0\\0\\0\end{bmatrix}.x^2+\begin{bmatrix}1\\1\\0\end{bmatrix}.x+\begin{bmatrix}1\\1\\0\end{bmatrix}=$$

$$=\alpha^2.x^6+\alpha^0.x^5+\alpha^4.x^4+\alpha^3.x^3+0.x^2+\alpha^5.x+\alpha^5.$$

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:

$$(10)\qquad S_1=r(\alpha)=B(\alpha)=\alpha^2.\alpha^6+\alpha^0.\alpha^5+\alpha^4.\alpha^4+\alpha^3.\alpha^3+0.\alpha^2+\alpha^5.\alpha^1+\alpha^5=$$

$$=\alpha^8+\alpha^5+\alpha^8+\alpha^6+0+\alpha^6+\alpha^5=\alpha^1+\alpha^5+\alpha^1+\alpha^6+0+\alpha^6+\alpha^5=0;$$

$$S_2 = r(\alpha^2) = B(\alpha^2) = \alpha^2.\alpha^{12} + \alpha^0.\alpha^{10} + \alpha^4.\alpha^8 + \alpha^3.\alpha^6 + 0.\alpha^4 + \alpha^5.\alpha^2 + \alpha^5 =$$

(11) $$= \alpha^{14} + \alpha^{10} + \alpha^{12} + \alpha^9 + 0 + \alpha^7 + \alpha^5 = \alpha^0 + \alpha^3 + \alpha^5 + \alpha^2 + 0 + \alpha^0 + \alpha^5 =$$

$$= \alpha^3 + \alpha^2 = \alpha^0 \neq 0;$$

$$S_3 = r(\alpha^3) = B(\alpha^3) = \alpha^2.\alpha^{18} + \alpha^0.\alpha^{15} + \alpha^4.\alpha^{12} + \alpha^3.\alpha^9 + 0.\alpha^6 + \alpha^5.\alpha^3 + \alpha^5 =$$

(12) $$= \alpha^{20} + \alpha^{15} + \alpha^{16} + \alpha^{12} + 0 + \alpha^8 + \alpha^5 = \alpha^6 + \alpha^1 + \alpha^2 + \alpha^5 + 0 + \alpha^1 + \alpha^5 =$$

$$= \alpha^6 + \alpha^2 = \alpha^1 \neq 0;$$

$$S_4 = r(\alpha^4) = B(\alpha^4) =$$

(13) $$= \alpha^2.\alpha^{24} + \alpha^0.\alpha^{20} + \alpha^4.\alpha^{16} + \alpha^3.\alpha^{12} + 0.\alpha^8 + \alpha^5.\alpha^4 + \alpha^5 =$$

$$= \alpha^{26} + \alpha^{20} + \alpha^{20} + \alpha^{15} + 0 + \alpha^9 + \alpha^5 = \alpha^5 + \alpha^6 + \alpha^6 + \alpha^1 + 0 + \alpha^2 + \alpha^5 =$$

$$= \alpha^1 + \alpha^2 = \alpha^6 \neq 0.$$

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

$$r(\alpha) = e_1.X_1 + e_2.X_2 + ... + e_i.X_i + ... + e_t.X_t,$$

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

(14) $$r(\alpha^3) = e_1.X_1^3 + e_2.X_2^3 + ... + e_i.X_i^3 + ... + e_t.X_t^3,$$

.....

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

като в разглеждания случай $t = 2$. Това е доста 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 количеството на неизвестните. Изход от тази сложна ситуация са намерили известните теоретиците Берлекемп и Меси, които са въвели т.нар. полином на локатора на грешката [5, 6]:

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

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:

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

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

(17) $$\begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} . \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} S_3 \\ S_4 \end{bmatrix}, \text{ т.е. } \begin{bmatrix} 0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix} . \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^1 \\ \alpha^6 \end{bmatrix}.$$

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:

$$(18)\qquad \boldsymbol{A}^{-1} = \frac{1}{\det \boldsymbol{A}} \begin{bmatrix} A_{11} & A_{21} & \ldots & A_{t1} \\ A_{12} & A_{22} & \ldots & A_{t2} \\ \ldots & \ldots & \ldots & \ldots \\ A_{1t} & A_{2t} & \ldots & A_{tt} \end{bmatrix}.$$

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:

$$(19)\qquad \det \boldsymbol{A} = \det \begin{bmatrix} 0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix} = 0.\alpha^1 - \alpha^0.\alpha^0 = 0 - \alpha^0 = -\alpha^0 = \alpha^0,$$

$$(20)\qquad \begin{aligned} &A_{11} = (-1)^{1+1}.\alpha^1 = \alpha^1, A_{12} = (-1)^{1+2}.\alpha^0 = -\alpha^0 = \alpha^0, \\ &A_{21} = (-1)^{2+1}.\alpha^0 = -\alpha^0 = \alpha^0, A_{22} = (-1)^{2+2}.0 = 0. \end{aligned}$$

Следователно, за обратната матрица се получава:

$$(21)\qquad \boldsymbol{A}^{-1} = \frac{1}{\alpha^0} \begin{bmatrix} \alpha^1 & \alpha^0 \\ \alpha^0 & 0 \end{bmatrix} = \begin{bmatrix} \alpha^1 & \alpha^0 \\ \alpha^0 & 0 \end{bmatrix}.$$

Верността на получения резултат се проверява от равенството:

$$(22)\qquad \boldsymbol{A}.\boldsymbol{A}^{-1} = \begin{bmatrix} 0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix} . \begin{bmatrix} \alpha^1 & \alpha^0 \\ \alpha^0 & 0 \end{bmatrix} = \begin{bmatrix} \alpha^0 & 0 \\ \alpha^1 + \alpha^1 & \alpha^0 \end{bmatrix} = \begin{bmatrix} \alpha^0 & 0 \\ 0 & \alpha^0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \boldsymbol{E}_2.$$

Следователно:

$$(23)\qquad \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^1 & \alpha^0 \\ \alpha^0 & 0 \end{bmatrix} . \begin{bmatrix} \alpha^1 \\ \alpha^6 \end{bmatrix} = \begin{bmatrix} \alpha^2 + \alpha^6 \\ \alpha^1 \end{bmatrix} = \begin{bmatrix} \alpha^1 \\ \alpha^1 \end{bmatrix},$$

откъдето следва:

$$(24)\qquad \sigma(x) = 1 + \sigma_1.x + \sigma_2.x^2 = \alpha^0 + \alpha^1.x + \alpha^1.x^2.$$

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 8 проверки с всички елементи на полето $GF(2^m)$. Резултатите за $\sigma(\alpha^i)$, които се получават, са:

$$(25)\qquad \sigma(\alpha^0) = \alpha^0 + \alpha^1.\alpha^0 + \alpha^1.\alpha^0 = \alpha^0 + \alpha^1 + \alpha^1 = \alpha^0 \neq 0,$$

$$(26)\qquad \sigma(\alpha^1) = \alpha^0 + \alpha^1.\alpha^1 + \alpha^1.\alpha^2 = \alpha^0 + \alpha^2 + \alpha^3 = \alpha^3 + \alpha^3 = 0 \Rightarrow \text{грешка},$$

$$(27)\qquad \sigma(\alpha^2) = \alpha^0 + \alpha^1.\alpha^2 + \alpha^1.\alpha^4 = \alpha^0 + \alpha^3 + \alpha^5 = \alpha^2 + \alpha^5 = \alpha^4 \neq 0,$$

$$(28)\qquad \sigma(\alpha^3) = \alpha^0 + \alpha^1.\alpha^3 + \alpha^1.\alpha^6 = \alpha^0 + \alpha^4 + \alpha^7 = \alpha^6 + \alpha^0 = \alpha^4 \neq 0,$$

$$(29)\qquad \sigma(\alpha^4) = \alpha^0 + \alpha^1.\alpha^4 + \alpha^1.\alpha^8 = \alpha^0 + \alpha^5 + \alpha^9 = \alpha^1 + \alpha^2 = \alpha^6 \neq 0,$$

$$(30)\qquad \sigma(\alpha^5) = \alpha^0 + \alpha^1.\alpha^5 + \alpha^1.\alpha^{10} = \alpha^0 + \alpha^6 + \alpha^{11} = \alpha^4 + \alpha^4 = 0 \Rightarrow \text{грешка},$$

$$(31)\qquad \sigma(\alpha^6) = \alpha^0 + \alpha^1.\alpha^6 + \alpha^1.\alpha^{12} = \alpha^0 + \alpha^7 + \alpha^{13} = \alpha^0 + \alpha^0 + \alpha^6 = \alpha^6 \neq 0.$$

Както се вижда, $\sigma(\alpha^1)=\sigma(\alpha^5)=0$, т.е. нулите на полинома на локатора на грешката са α^1 и α^5, а за X_1 и X_2 се получава:

(32) $$X_1=\frac{1}{\alpha^1}=\frac{\alpha^7}{\alpha^1}=\alpha^6, X_2=\frac{1}{\alpha^5}=\frac{\alpha^7}{\alpha^5}=\alpha^2.$$

Оттук следва, че сгрешените символи в приетата кодова дума са коефициентите пред x^6 и x^2 в израза за $B(x)$.

И така, в разгледания пример бяха открити две грешки в символите, които са коефициентите пред x^6 и x^2 в израза за $B(x)$. Сега трябва да се открият стойностите на грешките e_1 и e_2, свързани с позициите x^6 и x^2. За разглеждания случай системата уравнения за $r(\alpha^i)$ се опростява до:

(33) $$\begin{aligned} r(\alpha)&=e_1.X_1+e_2.X_2\\ r(\alpha^2)&=e_1.X_1^2+e_2.X_2^2 \end{aligned}$$

Тъй като $r(\alpha)=S_1=0,\quad r(\alpha^2)=S_2=\alpha^0,\quad X_1=\alpha^6,\quad X_2=\alpha^2$, то системата се записва във вида:

(34) $$\begin{bmatrix} X_1 & X_2\\ X_1^2 & X_2^2 \end{bmatrix}.\begin{bmatrix} e_1\\ e_2 \end{bmatrix}=\begin{bmatrix} S_1\\ S_2 \end{bmatrix}, \text{ т.е. } \begin{bmatrix} \alpha^6 & \alpha^2\\ \alpha^{12} & \alpha^4 \end{bmatrix}.\begin{bmatrix} e_1\\ e_2 \end{bmatrix}=\begin{bmatrix} 0\\ \alpha^0 \end{bmatrix}.$$

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:

(35) $$\begin{aligned} B^{-1}&=\begin{bmatrix} \alpha^6 & \alpha^2\\ \alpha^{12} & \alpha^4 \end{bmatrix}^{-1}=\begin{bmatrix} \alpha^6 & \alpha^2\\ \alpha^5 & \alpha^4 \end{bmatrix}^{-1}=\frac{\begin{bmatrix} \alpha^4 & \alpha^2\\ \alpha^5 & \alpha^6 \end{bmatrix}}{\alpha^6.\alpha^4-\alpha^2.\alpha^5}=\frac{\begin{bmatrix} \alpha^4 & \alpha^2\\ \alpha^5 & \alpha^6 \end{bmatrix}}{\alpha^{10}-\alpha^7}=\\ &=\frac{\begin{bmatrix} \alpha^4 & \alpha^2\\ \alpha^5 & \alpha^6 \end{bmatrix}}{\alpha^3+\alpha^0}=\frac{\begin{bmatrix} \alpha^4 & \alpha^2\\ \alpha^5 & \alpha^6 \end{bmatrix}}{\alpha^2}=\begin{bmatrix} \alpha^2 & \alpha^0\\ \alpha^3 & \alpha^4 \end{bmatrix}. \end{aligned}$$

Следователно за стойностите на грешките се получават:

(36) $$\begin{bmatrix} e_1\\ e_2 \end{bmatrix}=\begin{bmatrix} \alpha^2 & \alpha^0\\ \alpha^3 & \alpha^4 \end{bmatrix}.\begin{bmatrix} 0\\ \alpha^0 \end{bmatrix}=\begin{bmatrix} 0+\alpha^0\\ 0+\alpha^4 \end{bmatrix}=\begin{bmatrix} \alpha^0\\ \alpha^4 \end{bmatrix}.$$

Следователно, полиномът на грешката е:

(37) $$E(x)=\alpha^0.x^6+0.x^5+0.x^4+0.x^3+\alpha^4.x^2+0.x+0,$$

което съответства на полинома на приетата двусимволната грешка. Тъй като в полето на Галоа $GF(2^3)$ 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.:

(38) $$\begin{aligned} C(x)&=B(x)+E(x)=\\ &=\alpha^2.x^6+\alpha^0.x^5+\alpha^4.x^4+\alpha^3.x^3+0.x^2+\alpha^5.x+\alpha^5+\\ &+\alpha^0.x^6+0.x^5+0.x^4+0.x^3+\alpha^4.x^2+0.x+0=\\ &=\alpha^3.x^6+\alpha^0.x^5+\alpha^4.x^4+\alpha^3.x^3+\alpha^4.x^2+\alpha^5.x+\alpha^5. \end{aligned}$$

Тъй като символите на съобщението се съдържат в първите $k=3$ символа, декодерът ще изведе следното съобщение:

(39) $\alpha^3\ \alpha^0\ \alpha^4 = \begin{bmatrix}1\\0\\1\end{bmatrix}\begin{bmatrix}1\\0\\0\end{bmatrix}\begin{bmatrix}1\\1\\1\end{bmatrix} \Rightarrow 101\ \ 001\ \ 111.$

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

ПРИЛОЖЕНИЕ В УЧЕБНИЯ ПРОЦЕС

Така представеният материал се използва в учебния процес по дисциплината „Кодиране в телекомуникационните системи", включена като избираема в учебния план на специалност „Телекомуникационни системи" за студентите от IV курс, образователно-квалификационна степен „Бакалавър". С цел по-добре възприемане и усвояване на преподавания материал се прилагат активни методи на обучение, при които на всеки студент се задава индивидуално задание, което той трябва да реши по време на практическото упражнение и да представи в края на часа на преподавателя.

В таблица 4 са представени резултатите от 10 варианта, които се прилагат в учебния процес – за кодиране на 9-битови информационни думи чрез код на Рийд-Соломон, като са посочени коефициентите на полинома $A(x)$ на информационната дума (колона 3), коефициентите на остатъка $R(x)$ (колона 4), които съвместно с тези на $A(x)$, формират коефициентите на кодовата дума $C(x) = A(x).x^4 + R(x)$ (фиг. 1), както и коефициентите на частното (колона 5) (фиг. 1).

Таблица 4. Кодиране на 9-те информационни бита чрез код на Рийд-Соломон

№	Информация	Коефициенти на:			Кодова дума
		$A(x)$	Остатък	частно	
1	100 010 011	$\alpha^2\ \alpha^1\ \alpha^5$	$\alpha^5\ \alpha^2\ \alpha^3\ \alpha^1$	$\alpha^2\ \alpha^3\ \alpha^5$	100 010 011 011 100 101 010
2	111 011 010	$\alpha^4\ \alpha^5\ \alpha^1$	$\alpha^0\ \alpha^2\ \alpha^6\ 0$	$\alpha^4\ \alpha^3\ 0$	111 011 010 001 100 110 000
3	101 110 111	$\alpha^3\ \alpha^6\ \alpha^4$	$\alpha^6\ \alpha^2\ \alpha^2\ \alpha^4$	$\alpha^3\ \alpha^3\ \alpha^1$	101 110 111 110 100 100 111
4	010 111 101	$\alpha^1\ \alpha^4\ \alpha^3$	$\alpha^5\ \alpha^2\ 0\ \alpha^0$	$\alpha^1\ \alpha^1\ \alpha^4$	010 111 101 011 100 000 001
5	011 101 001	$\alpha^5\ \alpha^3\ \alpha^0$	$\alpha^4\ \alpha^3\ \alpha^4\ \alpha^5$	$\alpha^5\ \alpha^2\ \alpha^2$	011 101 001 111 101 111 011
6	001 100 110	$\alpha^0\ \alpha^2\ \alpha^6$	$0\ \alpha^4\ \alpha^5\ \alpha^1$	$\alpha^0\ 0\ \alpha^5$	001 100 110 000 111 011 010
7	100 111 010	$\alpha^2\ \alpha^4\ \alpha^1$	$0\ \alpha^6\ \alpha^0\ \alpha^3$	$\alpha^2\ 0\ \alpha^0$	100 111 010 000 110 001 101
8	110 001 100	$\alpha^6\ \alpha^0\ \alpha^2$	$0\ \alpha^1\ \alpha^5\ \alpha^3$	$\alpha^6\ \alpha^5\ \alpha^0$	110 001 100 000 010 011 101
9	111 101 011	$\alpha^4\ \alpha^3\ \alpha^5$	$\alpha^2\ 0\ \alpha^0\ \alpha^1$	$\alpha^4\ \alpha^5\ \alpha^5$	111 101 011 100 000 001 010
10	011 001 110	$\alpha^5\ \alpha^0\ \alpha^6$	$\alpha^2\ \alpha^0\ \alpha^2\ \alpha^5$	$\alpha^5\ 0\ \alpha^2$	011 001 110 100 001 100 011

В таблица 5 са представени резултатите от коригиране на грешки в 21-битовите прието кодови думи, като сгрешените битове са изписани на тъмен фон, и самото декодиране чрез използване на разглеждания код на Рийд-Соломон. Междинните резултати на изчислявани величини в хода на представения алгоритъм за декодиране са представени в таблица 6.

Вижда се, че при въвеждане на грешки в два от символите (таблица 5) са използвани най-различни варианти:

1) двата най-младши бита на първи информационен символ и трите бита на трети контролен символ;

2) най-старшият и най-младшият бит на втори информационен символ и двата най-старши бита на първи контролен символ;

Таблица 5. Декодиране на 9-те информационни бита чрез код на Рийд-Соломон

№	Приета кодова дума (грешните битове са на тъмен фон)	Информация
1	111 010 011 011 100 010 010	100 010 011
2	111 110 010 111 100 110 000	111 011 010
3	101 110 001 110 111 100 111	101 110 111
4	101 111 101 011 100 000 100	010 111 101
5	011 101 001 100 011 111 011	011 101 001
6	001 100 001 111 111 011 010	001 100 110
7	101 101 010 000 110 001 101	100 111 010
8	110 111 100 000 010 011 010	110 001 100
9	010 101 011 001 000 001 010	111 101 011
10	011 001 110 011 110 100 011	011 001 110

Таблица 6. Междинни резултати при декодирането чрез код на Рийд-Соломон

№	Коефициенти на $B(x)$							S_1	S_2	S_3	S_4	σ_1	σ_2
	$\sigma(\alpha^i),\ i=0\div 6$							X_1	X_2	X_1^2	X_2^2	e_1	e_2
1	α^4	α^1	α^5	α^5	α^2	α^1	α^1	α^2	α^5	α^3	0	α^2	α^0
	α^2	0	α^0	α^2	α^3	α^3	0	α^6	α^1	α^5	α^2	α^5	α^4
2	α^4	α^6	α^1	α^4	α^2	α^6	0	α^6	α^3	α^3	α^5	α^6	α^1
	α^3	α^3	0	α^2	0	α^0	α^2	α^5	α^3	α^3	α^6	α^3	α^6
3	α^3	α^6	α^0	α^6	α^4	α^2	α^4	α^2	α^3	0	α^2	α^5	α^6
	α^2	α^3	α^3	0	α^2	0	α^0	α^4	α^2	α^1	α^4	α^6	α^5
4	α^3	α^4	α^3	α^5	α^2	0	α^2	0	α^0	α^4	α^2	α^4	α^6
	0	0	α^1	α^5	α^1	α^0	α^5	α^0	α^6	α^0	α^5	α^3	α^4
5	α^5	α^3	α^0	α^4	α^3	α^4	α^5	0	α^1	α^1	α^2	α^0	α^5
	α^5	α^1	α^0	α^5	0	0	α^1	α^3	α^2	α^6	α^4	α^5	α^6
6	α^0	α^2	α^0	α^4	α^4	α^5	α^1	α^5	α^6	α^1	α^1	α^1	α^0
	α^1	α^0	α^5	0	0	α^1	α^5	α^4	α^3	α^1	α^6	α^4	α^4
7	α^3	α^3	α^1	0	α^6	α^0	α^3	0	α^2	α^5	α^2	α^3	α^4
	α^5	0	0	α^1	α^5	α^1	α^0	α^6	α^5	α^5	α^3	α^0	α^1
8	α^6	α^4	α^2	0	α^1	α^5	α^1	0	α^5	α^6	α^2	α^1	α^5
	0	α^2	0	α^0	α^2	α^3	α^3	α^0	α^5	α^0	α^3	α^4	α^6
9	α^1	α^3	α^5	α^0	0	α^0	α^1	α^1	α^6	α^1	α^2	α^5	α^2
	α^6	0	α^6	α^0	0	α^4	α^4	α^6	α^3	α^5	α^6	α^3	α^3
10	α^5	α^0	α^6	α^5	α^6	α^2	α^5	α^4	α^4	α^5	α^4	α^0	α^5
	α^5	α^1	α^0	α^5	0	0	α^1	α^3	α^2	α^6	α^4	α^4	α^4

3) двата най-старши бита на трети информационен символ и двата най-младши бита на втори контролен символ;

4) трите бита на първи информационен символ и най-старшият и най-младшият бит на четвърти контролен символ;

5) двата най-младши бита на първи контролен символ и двата най-старши бита на втори контролен символ;

6) трите бита на трети информационен символ и трите бита на първи контролен символ;

7) най-младшият бит на първи информационен символ и средният бит на втори информационен символ;

8) двата най-старши бита на втори информационен символ и трите бита на четвърти контролен символ;

9) най-старшият и най-младшият бит на първи информационен символ и най-старшият и най-младшият бит на първи контролен символ;

10) трите бита на първи контролен символ и трите бита на втори контролен символ.

ЗАКЛЮЧЕНИЕ

В публикацията е представена методика за построяване на код на Рийд-Соломон с дължина $n = 7$, коригиращ двусимволна грешка, който е базиран на полето на Галоа $GF\left(2^3\right)$, породено от примитивния неразложим полином $f(x) = x^3 + x^2 + 1$, като са изведени таблиците за събиране и умножение 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. Приложени са подробни резултати от кодиране и декодиране с код на Рийд-Соломон за 10 варианта, при различни случаи на възникнала грешка в кодовата дума. Материалът намира приложение в учебния процес по дисциплината „Кодиране в телекомуникационните системи”, включена като избираема в учебния план на специалността „Телекомуникационни системи”, за студентите от 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] Proakis, J.G. Digital Communications. McGraw-Hill, 1989.

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

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

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

ENCODING AND DECODING USING (7,3) REED-SOLOMON CODES, BASED ON GALOIS FIELD $GF(2^3)$, 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 (7,3) Reed-Solomon code, based on Galois field GF(2^3), generated by a primitive irreducible polynomial $f(x) = x^3 + x^2 + 1$. 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 6 consecutive bits. The process of encoding a 9-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.*