SAT-2G.302-2-CSNT-02

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

Adriana Borodzhieva

Откриване и коригиране на трисимволна грешка при декодиране с код на Рийд-Соломон (15,9), базиран на полето на Галоа GF(2^4)

Адриана Бороджиева

Abstract: *The paper describes the process of decoding using (15,9) Reed-Solomon code, based on Galois field GF(2^4), generated by a primitive irreducible polynomial f(x) = $x^4 + x + 1$. This code will detect and correct errors occurring in three symbols of the codeword, as these symbols may be consecutive, i.e. in a series of 12 consecutive bits. After introducing errors in three 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.*

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

ВЪВЕДЕНИЕ

Кодовете на Рийд-Соломон са създадени и описани през 1960 г., от Irving Reed и Gustave Solomon, в тяхната публикация „Полиномиални кодове над някои крайни полета". По това време все още не е бил известен 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) [3, 4].

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 е в сила $0 < k < n < 2^m + 2$, 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, 2, 3, 4]. За кодовете на Рийд-Соломон е изпълнено $(n,k) = (2^m - 1, 2^m - 1 - 2.t)$, където *t* е броят на грешките, които кодът може да коригира; $r = n - k = 2t$ е броят на контролните символи [1, 2, 3, 4].

ДЕКОДИРАНЕ С ИЗПОЛЗВАНЕ НА КОД НА РИЙД-СОЛОМОН

Въз основа на описания в [3, 4] 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 [5] 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 $f(x) = x^4 + x + 1$. В [5] е илюстриран процесът на кодиране на зададена информационна дума при използване на разглеждания код на Рийд-Соломон, а в настоящата публикация е илюстриран процесът на декодиране, при въвеждане на грешка в три символа. 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 [5]. Операциите в полето се извършват по модул $f(x) = x^4 + x + 1$. Алгоритъмът за декодиране при код 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 $r = 2t = 6$.

Нека при предаване на кодовата дума три 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 $E(x) = \sum_{k=0}^{14} e_k . x^k$.

При пресмятанията по-долу 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 правилата, представени в [5, таблица 2], а умножението се извършва съгласно правилото $\alpha^x . \alpha^y = \alpha^{(x+y) \bmod 15}$.

Нека са сгрешени първият (най-старшият) и третият бит на седми информационен символ (представено като α^9), четирите бита на девети информационен символ (представено като α^{12}) и четирите бита на първи контролен символ на съобщението (представено като α^{12}), т.е. моделът на грешката включва поредица от 8 последователни бита.

В този случай трисимволната грешка ще се представя с полинома от израз (1), а полиномът на грешно приетата кодова дума – с израз (2).

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

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

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

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

$$=\alpha^3.x^{14}+\alpha^4.x^{13}+\alpha^2.x^{12}+\alpha^{11}.x^{11}+\alpha^0.x^{10}+\alpha^6.x^9+\alpha^4.x^8+$$

$$+\alpha^{14}.x^7+\alpha^{13}.x^6+\alpha^1.x^5+\alpha^9.x^4+\alpha^2.x^3+\alpha^2.x^2+\alpha^{13}.x+\alpha^0.$$

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 6 символа, които се изразяват чрез изрази (3)...(8).

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

$$+\alpha^{14}.\alpha^7+\alpha^{13}.\alpha^6+\alpha^1.\alpha^5+\alpha^9.\alpha^4+\alpha^2.\alpha^3+\alpha^2.\alpha^2+\alpha^{13}.\alpha+\alpha^0=$$

$$=\alpha^{17}+\alpha^{17}+\alpha^{14}+\alpha^{22}+\alpha^{10}+\alpha^{15}+\alpha^{12}+\alpha^{21}+\alpha^{19}+\alpha^6+\alpha^{13}+\alpha^5+\alpha^4+\alpha^{14}+\alpha^0= \quad (3)$$

$$=\alpha^2+\alpha^2+\alpha^{14}+\alpha^7+\alpha^{10}+\alpha^0+\alpha^{12}+\alpha^6+\alpha^4+\alpha^6+\alpha^{13}+\alpha^5+\alpha^4+\alpha^{14}+\alpha^0=$$

$$=\alpha^7+\alpha^{10}+\alpha^{12}+\alpha^{13}+\alpha^5=\alpha^6+\alpha^1+\alpha^5=\alpha^{11}+\alpha^5=\alpha^3\neq 0;$$

$$S_2=r(\alpha^2)=B(\alpha^2)=\alpha^3.\alpha^{28}+\alpha^4.\alpha^{26}+\alpha^2.\alpha^{24}+\alpha^{11}.\alpha^{22}+\alpha^0.\alpha^{20}+\alpha^6.\alpha^{18}+\alpha^4.\alpha^{16}+$$

$$+\alpha^{14}.\alpha^{14}+\alpha^{13}.\alpha^{12}+\alpha^1.\alpha^{10}+\alpha^9.\alpha^8+\alpha^2.\alpha^6+\alpha^2.\alpha^4+\alpha^{13}.\alpha^2+\alpha^0=$$

$$=\alpha^{31}+\alpha^{30}+\alpha^{26}+\alpha^{33}+\alpha^{20}+\alpha^{24}+\alpha^{20}+\alpha^{28}+\alpha^{25}+\alpha^{11}+\alpha^{17}+\alpha^8+\alpha^6+\alpha^{15}+\alpha^0= \quad (4)$$

$$=\alpha^1+\alpha^0+\alpha^{11}+\alpha^3+\alpha^5+\alpha^9+\alpha^5+\alpha^{13}+\alpha^{10}+\alpha^{11}+\alpha^2+\alpha^8+\alpha^6+\alpha^0+\alpha^0=$$

$$=\alpha^9+\alpha^{10}+\alpha^4+\alpha^{14}+\alpha^0=\alpha^{13}+\alpha^9+\alpha^0=\alpha^{10}+\alpha^0=\alpha^5\neq 0;$$

$$S_3=r(\alpha^3)=B(\alpha^3)=\alpha^3.\alpha^{42}+\alpha^4.\alpha^{39}+\alpha^2.\alpha^{36}+\alpha^{11}.\alpha^{33}+\alpha^0.\alpha^{30}+\alpha^6.\alpha^{27}+\alpha^4.\alpha^{24}+$$

$$+\alpha^{14}.\alpha^{21}+\alpha^{13}.\alpha^{18}+\alpha^1.\alpha^{15}+\alpha^9.\alpha^{12}+\alpha^2.\alpha^9+\alpha^2.\alpha^6+\alpha^{13}.\alpha^3+\alpha^0=$$

$$=\alpha^{45}+\alpha^{43}+\alpha^{38}+\alpha^{44}+\alpha^{30}+\alpha^{33}+\alpha^{28}+\alpha^{35}+\alpha^{31}+\alpha^{16}+\alpha^{21}+\alpha^{11}+\alpha^8+\alpha^{16}+\alpha^0= \quad (5)$$

$$=\alpha^0+\alpha^{13}+\alpha^8+\alpha^{14}+\alpha^0+\alpha^3+\alpha^{13}+\alpha^5+\alpha^1+\alpha^1+\alpha^6+\alpha^{11}+\alpha^8+\alpha^1+\alpha^0=$$

$$=\alpha^{14}+\alpha^3+\alpha^5+\alpha^6+\alpha^{11}+\alpha^1+\alpha^0=\alpha^0+\alpha^9+\alpha^6+\alpha^0=\alpha^5\neq 0;$$

$$S_4=r(\alpha^4)=B(\alpha^4)=\alpha^3.\alpha^{56}+\alpha^4.\alpha^{52}+\alpha^2.\alpha^{48}+\alpha^{11}.\alpha^{44}+\alpha^0.\alpha^{40}+\alpha^6.\alpha^{36}+\alpha^4.\alpha^{32}+$$

$$+\alpha^{14}.\alpha^{28}+\alpha^{13}.\alpha^{24}+\alpha^1.\alpha^{20}+\alpha^9.\alpha^{16}+\alpha^2.\alpha^{12}+\alpha^2.\alpha^8+\alpha^{13}.\alpha^4+\alpha^0=$$

$$=\alpha^{59}+\alpha^{56}+\alpha^{50}+\alpha^{55}+\alpha^{40}+\alpha^{42}+\alpha^{36}+\alpha^{42}+\alpha^{37}+\alpha^{21}+\alpha^{25}+\alpha^{14}+\alpha^{10}+\alpha^{17}+\alpha^0= \quad (6)$$

$$=\alpha^{14}+\alpha^{11}+\alpha^5+\alpha^{10}+\alpha^{10}+\alpha^{12}+\alpha^6+\alpha^{12}+\alpha^7+\alpha^6+\alpha^{10}+\alpha^{14}+\alpha^{10}+\alpha^2+\alpha^0=$$

$$=\alpha^{11}+\alpha^5+\alpha^7+\alpha^2+\alpha^0=\alpha^3+\alpha^{12}+\alpha^0=\alpha^{10}+\alpha^0=\alpha^5\neq 0;$$

$$S_5 = r(\alpha^5) = B(\alpha^5) = \alpha^3.\alpha^{70} + \alpha^4.\alpha^{65} + \alpha^2.\alpha^{60} + \alpha^{11}.\alpha^{55} + \alpha^0.\alpha^{50} + \alpha^6.\alpha^{45} + \alpha^4.\alpha^{40} +$$
$$+ \alpha^{14}.\alpha^{35} + \alpha^{13}.\alpha^{30} + \alpha^1.\alpha^{25} + \alpha^9.\alpha^{20} + \alpha^2.\alpha^{15} + \alpha^2.\alpha^{10} + \alpha^{13}.\alpha^5 + \alpha^0 =$$
$$= \alpha^{73} + \alpha^{69} + \alpha^{62} + \alpha^{66} + \alpha^{50} + \alpha^{51} + \alpha^{44} + \alpha^{49} + \alpha^{43} + \alpha^{26} + \alpha^{29} + \alpha^{17} + \alpha^{12} + \alpha^{18} + \alpha^0 =$$
$$= \alpha^{13} + \alpha^9 + \alpha^2 + \alpha^6 + \alpha^5 + \alpha^6 + \alpha^{14} + \alpha^4 + \alpha^{13} + \alpha^{11} + \alpha^{14} + \alpha^2 + \alpha^{12} + \alpha^3 + \alpha^0 = \quad (7)$$
$$= \alpha^9 + \alpha^5 + \alpha^4 + \alpha^{11} + \alpha^{12} + \alpha^3 + \alpha^0 = \alpha^6 + \alpha^{13} + \alpha^{10} + \alpha^0 = \alpha^0 + \alpha^5 = \alpha^{10} \neq 0;$$

$$S_6 = r(\alpha^6) = B(\alpha^6) = \alpha^3.\alpha^{84} + \alpha^4.\alpha^{78} + \alpha^2.\alpha^{72} + \alpha^{11}.\alpha^{66} + \alpha^0.\alpha^{60} + \alpha^6.\alpha^{54} + \alpha^4.\alpha^{48} +$$
$$+ \alpha^{14}.\alpha^{42} + \alpha^{13}.\alpha^{36} + \alpha^1.\alpha^{30} + \alpha^9.\alpha^{24} + \alpha^2.\alpha^{18} + \alpha^2.\alpha^{12} + \alpha^{13}.\alpha^6 + \alpha^0 =$$
$$= \alpha^{87} + \alpha^{82} + \alpha^{74} + \alpha^{77} + \alpha^{60} + \alpha^{60} + \alpha^{52} + \alpha^{56} + \alpha^{49} + \alpha^{31} + \alpha^{33} + \alpha^{20} + \alpha^{14} + \alpha^{19} + \alpha^0 =$$
$$= \alpha^{12} + \alpha^7 + \alpha^{14} + \alpha^2 + \alpha^0 + \alpha^0 + \alpha^7 + \alpha^{11} + \alpha^4 + \alpha^1 + \alpha^3 + \alpha^5 + \alpha^{14} + \alpha^4 + \alpha^0 = \quad (8)$$
$$= \alpha^{12} + \alpha^2 + \alpha^{11} + \alpha^1 + \alpha^3 + \alpha^5 + \alpha^0 = \alpha^7 + \alpha^6 + \alpha^{11} + \alpha^0 = \alpha^{10} + \alpha^{12} = \alpha^3 \neq 0;$$

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

$$\begin{aligned} r(\alpha) &= e_1.X_1 + e_2.X_2 + ... + e_i.X_i + ... + e_t.X_t, \\ r(\alpha^2) &= e_1.X_1^2 + e_2.X_2^2 + ... + e_i.X_i^2 + ... + e_t.X_t^2, \\ r(\alpha^3) &= e_1.X_1^3 + e_2.X_2^3 + ... + e_i.X_i^3 + ... + e_t.X_t^3, \\ &..... \\ r(\alpha^{2t}) &= e_1.X_1^{2t} + e_2.X_2^{2t} + ... + e_i.X_i^{2t} + ... + e_t.X_t^{2t}, \end{aligned} \quad (9)$$

като в разглеждания случай $t = 3$. 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 броят на неизвестните. Изход от тази сложна ситуация са намерили известните теоретици Берлекемп и Меси, които са въвели т.нар. полином на локатора на грешката [3, 4]:

$$\sigma(x) = (1 - X_1.x).(1 - X_2.x)...(1 - X_{2t}.x) = 1 + \sigma_1.x + \sigma_2.x^2 + ... + \sigma_{2t}.x^{2t}. \quad (10)$$

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. Нулите на полинома $\sigma(x)$ са реципрочните стойности $X_1^{-1}, X_2^{-1}, ..., X_{2t}^{-1}$ на елементите $X_1, X_2, ..., X_{2t}$, 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:

$$\begin{bmatrix} S_1 & S_2 & S_3 & ... & S_{t-1} & S_t \\ S_2 & S_3 & S_4 & ... & S_t & S_{t+1} \\ ... & .... & .... & .... & .... & .... \\ S_{t-1} & S_t & S_{t+1} & ... & S_{2t-3} & S_{2t-2} \\ S_t & S_{t+1} & S_{t+2} & ... & S_{2t-2} & S_{2t-1} \end{bmatrix} . \begin{bmatrix} \sigma_t \\ \sigma_{t-1} \\ ... \\ \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} -S_{t+1} \\ -S_{t+2} \\ ... \\ -S_{2t-1} \\ -S_{2t} \end{bmatrix} \quad (11)$$

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

$$\begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} . \begin{bmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} S_4 \\ S_5 \\ S_6 \end{bmatrix}, \text{ т.е. } \begin{bmatrix} \alpha^3 & \alpha^5 & \alpha^5 \\ \alpha^5 & \alpha^5 & \alpha^5 \\ \alpha^5 & \alpha^5 & \alpha^{10} \end{bmatrix} . \begin{bmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^5 \\ \alpha^{10} \\ \alpha^3 \end{bmatrix}. \quad (12)$$

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:

$$\boldsymbol{A}^{-1} = \frac{1}{\det \boldsymbol{A}} \begin{bmatrix} A_{11} & A_{21} & \ldots & A_{t1} \\ A_{12} & A_{22} & \ldots & A_{t2} \\ \ldots & \ldots & \ldots & \ldots \\ A_{1t} & A_{2t} & \ldots & A_{tt} \end{bmatrix} \tag{13}$$

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 $\boldsymbol{A}$ последователно се определят детерминантата (израз 14), адюнгираните количества (израз 15) и обратната матрица (израз 16):

$$\det \boldsymbol{A} = \det \begin{bmatrix} \alpha^3 & \alpha^5 & \alpha^5 \\ \alpha^5 & \alpha^5 & \alpha^5 \\ \alpha^5 & \alpha^5 & \alpha^{10} \end{bmatrix} =$$

$$= \alpha^3.\alpha^5.\alpha^{10} + \alpha^5.\alpha^5.\alpha^5 + \alpha^5.\alpha^5.\alpha^5 - \alpha^5.\alpha^5.\alpha^5 - \alpha^3.\alpha^5.\alpha^5 - \alpha^5.\alpha^5.\alpha^{10} =$$
$$= \alpha^{18} + \alpha^{15} + \alpha^{15} - \alpha^{15} - \alpha^{13} - \alpha^{20} = \alpha^3 + \alpha^0 + \alpha^0 + \alpha^0 + \alpha^{13} + \alpha^5 = \alpha^{14} + \alpha^7 = \alpha^1 \neq 0 \tag{14}$$

$$A_{11} = (-1)^{1+1}.\begin{vmatrix} \alpha^5 & \alpha^5 \\ \alpha^5 & \alpha^{10} \end{vmatrix} = +\left(\alpha^5.\alpha^{10} - \alpha^5.\alpha^5\right) = \alpha^{15} + \alpha^{10} = \alpha^0 + \alpha^{10} = \alpha^5,$$

$$A_{12} = (-1)^{1+2}.\begin{vmatrix} \alpha^5 & \alpha^5 \\ \alpha^5 & \alpha^{10} \end{vmatrix} = -\left(\alpha^5.\alpha^{10} - \alpha^5.\alpha^5\right) = \alpha^{15} + \alpha^{10} = \alpha^0 + \alpha^{10} = \alpha^5,$$

$$A_{13} = (-1)^{1+3}.\begin{vmatrix} \alpha^5 & \alpha^5 \\ \alpha^5 & \alpha^5 \end{vmatrix} = +\left(\alpha^5.\alpha^5 - \alpha^5.\alpha^5\right) = \alpha^{10} + \alpha^{10} = 0,$$

$$A_{21} = (-1)^{2+1}.\begin{vmatrix} \alpha^5 & \alpha^5 \\ \alpha^5 & \alpha^{10} \end{vmatrix} = -\left(\alpha^5.\alpha^{10} - \alpha^5.\alpha^5\right) = \alpha^{15} + \alpha^{10} = \alpha^0 + \alpha^{10} = \alpha^5,$$

$$A_{22} = (-1)^{2+2}.\begin{vmatrix} \alpha^3 & \alpha^5 \\ \alpha^5 & \alpha^{10} \end{vmatrix} = +\left(\alpha^3.\alpha^{10} - \alpha^5.\alpha^5\right) = \alpha^{13} + \alpha^{10} = \alpha^9,$$

$$A_{23} = (-1)^{2+3}.\begin{vmatrix} \alpha^3 & \alpha^5 \\ \alpha^5 & \alpha^5 \end{vmatrix} = -\left(\alpha^3.\alpha^5 - \alpha^5.\alpha^5\right) = \alpha^8 + \alpha^{10} = \alpha^1,$$

$$A_{31} = (-1)^{3+1}.\begin{vmatrix} \alpha^5 & \alpha^5 \\ \alpha^5 & \alpha^5 \end{vmatrix} = +\left(\alpha^5.\alpha^5 - \alpha^5.\alpha^5\right) = \alpha^{10} + \alpha^{10} = 0,$$

$$A_{32} = (-1)^{3+2}.\begin{vmatrix} \alpha^3 & \alpha^5 \\ \alpha^5 & \alpha^5 \end{vmatrix} = -\left(\alpha^3.\alpha^5 - \alpha^5.\alpha^5\right) = \alpha^8 + \alpha^{10} = \alpha^1, \tag{15}$$

$$A_{33} = (-1)^{3+3}.\begin{vmatrix} \alpha^3 & \alpha^5 \\ \alpha^5 & \alpha^5 \end{vmatrix} = +\left(\alpha^3.\alpha^5 - \alpha^5.\alpha^5\right) = \alpha^8 + \alpha^{10} = \alpha^1.$$

$$\boldsymbol{A}^{-1} = \frac{1}{\alpha^1} \begin{bmatrix} \alpha^5 & \alpha^5 & 0 \\ \alpha^5 & \alpha^9 & \alpha^1 \\ 0 & \alpha^1 & \alpha^1 \end{bmatrix} = \begin{bmatrix} \alpha^4 & \alpha^4 & 0 \\ \alpha^4 & \alpha^8 & \alpha^0 \\ 0 & \alpha^0 & \alpha^0 \end{bmatrix} \tag{16}$$

Верността на получения резултат се проверява от равенството:

$$\boldsymbol{A}\,.\,\boldsymbol{A}^{-1}=\begin{bmatrix}\alpha^3 & \alpha^5 & \alpha^5\\ \alpha^5 & \alpha^5 & \alpha^5\\ \alpha^5 & \alpha^5 & \alpha^{10}\end{bmatrix}.\begin{bmatrix}\alpha^4 & \alpha^4 & 0\\ \alpha^4 & \alpha^8 & \alpha^0\\ 0 & \alpha^0 & \alpha^0\end{bmatrix}=$$

$$=\begin{bmatrix}\alpha^7+\alpha^9+0 & \alpha^7+\alpha^{13}+\alpha^5 & 0+\alpha^5+\alpha^5\\ \alpha^9+\alpha^9+0 & \alpha^9+\alpha^{13}+\alpha^5 & 0+\alpha^5+\alpha^5\\ \alpha^9+\alpha^9+0 & \alpha^9+\alpha^{13}+\alpha^{10} & 0+\alpha^5+\alpha^{10}\end{bmatrix}=\begin{bmatrix}\alpha^0 & \alpha^7+\alpha^{13}+\alpha^5 & 0\\ 0 & \alpha^9+\alpha^{13}+\alpha^5 & 0\\ 0 & \alpha^9+\alpha^{13}+\alpha^{10} & \alpha^0\end{bmatrix}= \quad (17)$$

$$=\begin{bmatrix}\alpha^0 & \alpha^5+\alpha^5 & 0\\ 0 & \alpha^{10}+\alpha^5 & 0\\ 0 & \alpha^{10}+\alpha^{10} & \alpha^0\end{bmatrix}=\begin{bmatrix}\alpha^0 & 0 & 0\\ 0 & \alpha^0 & 0\\ 0 & 0 & \alpha^0\end{bmatrix}=\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}=\boldsymbol{E}_3.$$

Следователно, оттук следва:

$$\begin{bmatrix}\sigma_3\\ \sigma_2\\ \sigma_1\end{bmatrix}=\begin{bmatrix}\alpha^4 & \alpha^4 & 0\\ \alpha^4 & \alpha^8 & \alpha^0\\ 0 & \alpha^0 & \alpha^0\end{bmatrix}.\begin{bmatrix}\alpha^5\\ \alpha^{10}\\ \alpha^3\end{bmatrix}=\begin{bmatrix}\alpha^9+\alpha^{14}+0\\ \alpha^9+\alpha^{18}+\alpha^3\\ 0+\alpha^{10}+\alpha^3\end{bmatrix}=\begin{bmatrix}\alpha^4\\ \alpha^9+\alpha^3+\alpha^3\\ \alpha^{12}\end{bmatrix}=\begin{bmatrix}\alpha^4\\ \alpha^9\\ \alpha^{12}\end{bmatrix}, \text{ т.е.} \quad (18)$$

$$\sigma(x)=1+\sigma_1.\,x+\sigma_2.\,x^2=\alpha^0+\alpha^{12}.\,x+\alpha^9.\,x^2+\alpha^4.\,x^3. \quad (19)$$

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 в сравнение с необходимите 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 $GF(2^m)$. Получените резултати за $\sigma(\alpha^i)$ са:

$$\sigma(\alpha^0)=\alpha^0+\alpha^{12}.\,\alpha^0+\alpha^9.\,\alpha^0+\alpha^4.\,\alpha^0=\alpha^0+\alpha^{12}+\alpha^9+\alpha^4=\alpha^{11}+\alpha^{14}=\alpha^{10}\neq 0, \quad (20)$$

$$\sigma(\alpha^1)=\alpha^0+\alpha^{12}.\,\alpha^1+\alpha^9.\,\alpha^2+\alpha^4.\,\alpha^3=\alpha^0+\alpha^{13}+\alpha^{11}+\alpha^7=\alpha^6+\alpha^8=\alpha^{14}\neq 0, \quad (21)$$

$$\sigma(\alpha^2)=\alpha^0+\alpha^{12}.\,\alpha^2+\alpha^9.\,\alpha^4+\alpha^4.\,\alpha^6=\alpha^0+\alpha^{14}+\alpha^{13}+\alpha^{10}=\alpha^3+\alpha^9=\alpha^1\neq 0, \quad (22)$$

$$\sigma(\alpha^3)=\alpha^0+\alpha^{12}.\,\alpha^3+\alpha^9.\,\alpha^6+\alpha^4.\,\alpha^9=\alpha^0+\alpha^{15}+\alpha^{15}+\alpha^{13}=$$
$$=\alpha^0+\alpha^0+\alpha^0+\alpha^{13}=\alpha^0+\alpha^{13}=\alpha^6\neq 0, \quad (23)$$

$$\sigma(\alpha^4)=\alpha^0+\alpha^{12}.\,\alpha^4+\alpha^9.\,\alpha^8+\alpha^4.\,\alpha^{12}=\alpha^0+\alpha^{16}+\alpha^{17}+\alpha^{16}=$$
$$=\alpha^0+\alpha^1+\alpha^2+\alpha^1=\alpha^0+\alpha^2=\alpha^8\neq 0, \quad (24)$$

$$\sigma(\alpha^5)=\alpha^0+\alpha^{12}.\,\alpha^5+\alpha^9.\,\alpha^{10}+\alpha^4.\,\alpha^{15}=\alpha^0+\alpha^{17}+\alpha^{19}+\alpha^{19}=$$
$$=\alpha^0+\alpha^2+\alpha^4+\alpha^4=\alpha^0+\alpha^2=\alpha^8\neq 0, \quad (25)$$

$$\sigma(\alpha^6)=\alpha^0+\alpha^{12}.\,\alpha^6+\alpha^9.\,\alpha^{12}+\alpha^4.\,\alpha^{18}=\alpha^0+\alpha^{18}+\alpha^{21}+\alpha^{22}=$$
$$=\alpha^0+\alpha^3+\alpha^6+\alpha^7=\alpha^{14}+\alpha^{10}=\alpha^{11}\neq 0, \quad (26)$$

$$\sigma(\alpha^7)=\alpha^0+\alpha^{12}.\,\alpha^7+\alpha^9.\,\alpha^{14}+\alpha^4.\,\alpha^{21}=\alpha^0+\alpha^{19}+\alpha^{23}+\alpha^{25}=$$
$$=\alpha^0+\alpha^4+\alpha^8+\alpha^{10}=\alpha^1+\alpha^1=0\Rightarrow \text{грешка}, \quad (27)$$

$$\sigma(\alpha^8)=\alpha^0+\alpha^{12}.\,\alpha^8+\alpha^9.\,\alpha^{16}+\alpha^4.\,\alpha^{24}=\alpha^0+\alpha^{20}+\alpha^{25}+\alpha^{28}=$$
$$=\alpha^0+\alpha^5+\alpha^{10}+\alpha^{13}=\alpha^{10}+\alpha^9=\alpha^{13}\neq 0, \quad (28)$$

$$\sigma(\alpha^9) = \alpha^0 + \alpha^{12}.\alpha^9 + \alpha^9.\alpha^{18} + \alpha^4.\alpha^{27} = \alpha^0 + \alpha^{21} + \alpha^{27} + \alpha^{31} =$$
$$= \alpha^0 + \alpha^6 + \alpha^{12} + \alpha^1 = \alpha^{13} + \alpha^{13} = 0 \Rightarrow \text{грешка}, \quad (29)$$

$$\sigma(\alpha^{10}) = \alpha^0 + \alpha^{12}.\alpha^{10} + \alpha^9.\alpha^{20} + \alpha^4.\alpha^{30} = \alpha^0 + \alpha^{22} + \alpha^{29} + \alpha^{34} =$$
$$= \alpha^0 + \alpha^7 + \alpha^{14} + \alpha^4 = \alpha^9 + \alpha^9 = 0 \Rightarrow \text{грешка}, \quad (30)$$

$$\sigma(\alpha^{11}) = \alpha^0 + \alpha^{12}.\alpha^{11} + \alpha^9.\alpha^{22} + \alpha^4.\alpha^{33} = \alpha^0 + \alpha^{23} + \alpha^{31} + \alpha^{37} =$$
$$= \alpha^0 + \alpha^8 + \alpha^1 + \alpha^7 = \alpha^2 + \alpha^{14} = \alpha^{13} \neq 0, \quad (31)$$

$$\sigma(\alpha^{12}) = \alpha^0 + \alpha^{12}.\alpha^{12} + \alpha^9.\alpha^{24} + \alpha^4.\alpha^{36} = \alpha^0 + \alpha^{24} + \alpha^{33} + \alpha^{40} =$$
$$= \alpha^0 + \alpha^9 + \alpha^3 + \alpha^{10} = \alpha^7 + \alpha^{12} = \alpha^2 \neq 0, \quad (32)$$

$$\sigma(\alpha^{13}) = \alpha^0 + \alpha^{12}.\alpha^{13} + \alpha^9.\alpha^{26} + \alpha^4.\alpha^{39} = \alpha^0 + \alpha^{25} + \alpha^{35} + \alpha^{43} =$$
$$= \alpha^0 + \alpha^{10} + \alpha^5 + \alpha^{13} = \alpha^5 + \alpha^7 = \alpha^{13} \neq 0, \quad (33)$$

$$\sigma(\alpha^{14}) = \alpha^0 + \alpha^{12}.\alpha^{14} + \alpha^9.\alpha^{28} + \alpha^4.\alpha^{42} = \alpha^0 + \alpha^{26} + \alpha^{37} + \alpha^{46} =$$
$$= \alpha^0 + \alpha^{11} + \alpha^7 + \alpha^1 = \alpha^{12} + \alpha^{14} = \alpha^5 \neq 0. \quad (34)$$

Както се вижда, $\sigma(\alpha^7) = \sigma(\alpha^9) = \sigma(\alpha^{10}) = 0$, т.е. нулите на полинома на локатора на грешката са α^7, α^9 и α^{10}, а за X_1, X_2 и X_3 се получава:

$$X_1 = \frac{1}{\alpha^7} = \frac{\alpha^{15}}{\alpha^7} = \alpha^8, X_2 = \frac{1}{\alpha^9} = \frac{\alpha^{15}}{\alpha^9} = \alpha^6, X_3 = \frac{1}{\alpha^{10}} = \frac{\alpha^{15}}{\alpha^{10}} = \alpha^5. \quad (35)$$

Оттук следва, че сгрешените символи в приетата кодова дума са коефициентите пред x^8, x^6 и x^5 в израза за $B(x)$.

И така, в разгледания пример бяха открити две грешки в символите, които са коефициентите пред x^8, x^6 и x^5 в израза за $B(x)$. Следва да се открият стойностите на грешките e_1, e_2 и e_3, свързани с позициите x^8, x^6 и x^5. За разглеждания случай системата уравнения за $r(\alpha^i)$ се опростява до:

$$\begin{aligned} r(\alpha) &= e_1.X_1 + e_2.X_2 + e_3.X_3 \\ r(\alpha^2) &= e_1.X_1^2 + e_2.X_2^2 + e_3.X_3^2 . \\ r(\alpha^3) &= e_1.X_1^3 + e_2.X_2^3 + e_3.X_3^3 \end{aligned} \quad (36)$$

Тъй като $r(\alpha) = S_1 = \alpha^3$, $r(\alpha^2) = S_2 = \alpha^5$, $r(\alpha^3) = S_3 = \alpha^5$, $X_1 = \alpha^8$, $X_2 = \alpha^6$, $X_3 = \alpha^5$, то системата се записва във вида:

$$\begin{bmatrix} X_1 & X_2 & X_3 \\ X_1^2 & X_2^2 & X_3^2 \\ X_1^3 & X_2^3 & X_3^3 \end{bmatrix} . \begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix} = \begin{bmatrix} S_1 \\ S_2 \\ S_3 \end{bmatrix}, \text{ т.е. } \begin{bmatrix} \alpha^8 & \alpha^6 & \alpha^5 \\ \alpha^{16} & \alpha^{12} & \alpha^{10} \\ \alpha^{24} & \alpha^{18} & \alpha^{15} \end{bmatrix} . \begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix} = \begin{bmatrix} \alpha^3 \\ \alpha^5 \\ \alpha^5 \end{bmatrix}. \quad (37)$$

За да се намерят стойностите на грешките e_1, e_2 и e_3 е необходимо да се изчисли обратната матрица на матрицата на коефициентите в последното матрично уравнение. Следователно:

$$\det \boldsymbol{B} = \det \begin{bmatrix} \alpha^8 & \alpha^6 & \alpha^5 \\ \alpha^{16} & \alpha^{12} & \alpha^{10} \\ \alpha^{24} & \alpha^{18} & \alpha^{15} \end{bmatrix} = \det \begin{bmatrix} \alpha^8 & \alpha^6 & \alpha^5 \\ \alpha^1 & \alpha^{12} & \alpha^{10} \\ \alpha^9 & \alpha^3 & \alpha^0 \end{bmatrix} =$$
$$= \alpha^8.\alpha^{12}.\alpha^0 + \alpha^6.\alpha^{10}.\alpha^9 + \alpha^5.\alpha^1.\alpha^3 - \alpha^5.\alpha^{12}.\alpha^9 - \alpha^8.\alpha^{10}.\alpha^3 - \alpha^6.\alpha^1.\alpha^0 = \quad (38)$$
$$= \alpha^{20} + \alpha^{25} + \alpha^9 - \alpha^{26} - \alpha^{21} - \alpha^7 = \alpha^5 + \alpha^{10} + \alpha^9 + \alpha^{11} + \alpha^6 + \alpha^7 =$$
$$= \alpha^0 + \alpha^2 + \alpha^{10} = \alpha^8 + \alpha^{10} = \alpha^1 \neq 0$$

$$A_{11}=(-1)^{1+1}.\begin{vmatrix}\alpha^{12} & \alpha^{10}\\ \alpha^{3} & \alpha^{0}\end{vmatrix}=+\left(\alpha^{12}.\,\alpha^{0}-\alpha^{10}.\,\alpha^{3}\right)=\alpha^{12}+\alpha^{13}=\alpha^{1},$$

$$A_{12}=(-1)^{1+2}.\begin{vmatrix}\alpha^{1} & \alpha^{10}\\ \alpha^{9} & \alpha^{0}\end{vmatrix}=-\left(\alpha^{1}.\,\alpha^{0}-\alpha^{10}.\,\alpha^{9}\right)=\alpha^{1}+\alpha^{19}=\alpha^{1}+\alpha^{4}=\alpha^{0},$$

$$A_{13}=(-1)^{1+3}.\begin{vmatrix}\alpha^{1} & \alpha^{12}\\ \alpha^{9} & \alpha^{3}\end{vmatrix}=+\left(\alpha^{1}.\,\alpha^{3}-\alpha^{12}.\,\alpha^{9}\right)=\alpha^{4}+\alpha^{21}=\alpha^{4}+\alpha^{6}=\alpha^{12},$$

$$A_{21}=(-1)^{2+1}.\begin{vmatrix}\alpha^{6} & \alpha^{5}\\ \alpha^{3} & \alpha^{0}\end{vmatrix}=-\left(\alpha^{6}.\,\alpha^{0}-\alpha^{5}.\,\alpha^{3}\right)=\alpha^{6}+\alpha^{8}=\alpha^{14},$$

$$A_{22}=(-1)^{2+2}.\begin{vmatrix}\alpha^{8} & \alpha^{5}\\ \alpha^{9} & \alpha^{0}\end{vmatrix}=+\left(\alpha^{8}.\,\alpha^{0}-\alpha^{5}.\,\alpha^{9}\right)=\alpha^{8}+\alpha^{14}=\alpha^{6},$$

$$A_{23}=(-1)^{2+3}.\begin{vmatrix}\alpha^{8} & \alpha^{6}\\ \alpha^{9} & \alpha^{3}\end{vmatrix}=-\left(\alpha^{8}.\,\alpha^{3}-\alpha^{6}.\,\alpha^{9}\right)=\alpha^{11}+\alpha^{15}=\alpha^{11}+\alpha^{0}=\alpha^{12},$$

$$A_{31}=(-1)^{3+1}.\begin{vmatrix}\alpha^{6} & \alpha^{5}\\ \alpha^{12} & \alpha^{10}\end{vmatrix}=+\left(\alpha^{6}.\,\alpha^{10}-\alpha^{5}.\,\alpha^{12}\right)=\alpha^{16}+\alpha^{17}=\alpha^{1}+\alpha^{2}=\alpha^{5},$$

$$A_{32}=(-1)^{3+2}.\begin{vmatrix}\alpha^{8} & \alpha^{5}\\ \alpha^{1} & \alpha^{10}\end{vmatrix}=-\left(\alpha^{8}.\,\alpha^{10}-\alpha^{5}.\,\alpha^{1}\right)=\alpha^{18}+\alpha^{6}=\alpha^{3}+\alpha^{6}=\alpha^{2},\qquad(39б)$$

$$A_{33}=(-1)^{3+3}.\begin{vmatrix}\alpha^{8} & \alpha^{6}\\ \alpha^{1} & \alpha^{12}\end{vmatrix}=+\left(\alpha^{8}.\,\alpha^{12}-\alpha^{6}.\,\alpha^{1}\right)=\alpha^{20}+\alpha^{7}=\alpha^{5}+\alpha^{7}=\alpha^{13}.$$

$$\boldsymbol{B}^{-1}=\frac{1}{\alpha^{1}}\begin{bmatrix}\alpha^{1} & \alpha^{14} & \alpha^{5}\\ \alpha^{0} & \alpha^{6} & \alpha^{2}\\ \alpha^{12} & \alpha^{12} & \alpha^{13}\end{bmatrix}=\begin{bmatrix}\alpha^{0} & \alpha^{13} & \alpha^{4}\\ \alpha^{14} & \alpha^{5} & \alpha^{1}\\ \alpha^{11} & \alpha^{11} & \alpha^{12}\end{bmatrix}.\qquad(40)$$

Следователно за стойностите на грешките се получават:

$$\begin{bmatrix}e_1\\ e_2\\ e_3\end{bmatrix}=\begin{bmatrix}\alpha^{0} & \alpha^{13} & \alpha^{4}\\ \alpha^{14} & \alpha^{5} & \alpha^{1}\\ \alpha^{11} & \alpha^{11} & \alpha^{12}\end{bmatrix}.\begin{bmatrix}\alpha^{3}\\ \alpha^{5}\\ \alpha^{5}\end{bmatrix}=\begin{bmatrix}\alpha^{3}+\alpha^{18}+\alpha^{9}\\ \alpha^{17}+\alpha^{10}+\alpha^{6}\\ \alpha^{14}+\alpha^{16}+\alpha^{17}\end{bmatrix}=\begin{bmatrix}\alpha^{3}+\alpha^{3}+\alpha^{9}\\ \alpha^{2}+\alpha^{10}+\alpha^{6}\\ \alpha^{14}+\alpha^{1}+\alpha^{2}\end{bmatrix}=$$

$$=\begin{bmatrix}\alpha^{9}\\ \alpha^{4}+\alpha^{6}\\ \alpha^{7}+\alpha^{2}\end{bmatrix}=\begin{bmatrix}\alpha^{9}\\ \alpha^{12}\\ \alpha^{12}\end{bmatrix}.\qquad(41)$$

Следователно, полиномът на грешката е:

$$E(x)=0.\,x^{14}+0.\,x^{13}+0.\,x^{12}+0.\,x^{11}+0.\,x^{10}+0.\,x^{9}+\alpha^{9}.\,x^{8}+$$
$$+0.\,x^{7}+\alpha^{12}.\,x^{6}+\alpha^{12}.\,x^{5}+0.\,x^{4}+0.\,x^{3}+0.\,x^{2}+0.\,x+0,\qquad(42)$$

което съответства на полинома на приетата трисимволна 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.:

$$
\begin{aligned}
&C(x)=B(x)+E(x)= \\
&=\alpha^3.x^{14}+\alpha^4.x^{13}+\alpha^2.x^{12}+\alpha^{11}.x^{11}+\alpha^0.x^{10}+\alpha^6.x^9+\alpha^4.x^8+ \\
&+\alpha^{14}.x^7+\alpha^{13}.x^6+\alpha^1.x^5+\alpha^9.x^4+\alpha^2.x^3+\alpha^2.x^2+\alpha^{13}.x+\alpha^0+ \\
&+0.x^{14}+0.x^{13}+0.x^{12}+0.x^{11}+0.x^{10}+0.x^9+\alpha^9.x^8+ \\
&+0.x^7+\alpha^{12}.x^6+\alpha^{12}.x^5+0.x^4+0.x^3+0.x^2+0.x+0= \\
&=\alpha^3.x^{14}+\alpha^4.x^{13}+\alpha^2.x^{12}+\alpha^{11}.x^{11}+\alpha^0.x^{10}+\alpha^6.x^9+\alpha^{14}.x^8+ \\
&+\alpha^{14}.x^7+\alpha^1.x^6+\alpha^{13}.x^5+\alpha^9.x^4+\alpha^2.x^3+\alpha^2.x^2+\alpha^{13}.x+\alpha^0.
\end{aligned}
\tag{43}
$$

Тъй като символите на съобщението се съдържат в първите $k=9$ символа, декодерът ще изведе следното съобщение:

$$
\begin{matrix}
\alpha^3 & \alpha^4 & \alpha^2 & \alpha^{11} & \alpha^0 & \alpha^6 & \alpha^{14} & \alpha^{14} & \alpha^1 & \Rightarrow \\
\begin{bmatrix}0\\0\\0\\1\end{bmatrix} & \begin{bmatrix}1\\1\\0\\0\end{bmatrix} & \begin{bmatrix}0\\0\\1\\0\end{bmatrix} & \begin{bmatrix}0\\1\\1\\1\end{bmatrix} & \begin{bmatrix}1\\0\\0\\0\end{bmatrix} & \begin{bmatrix}0\\0\\1\\1\end{bmatrix} & \begin{bmatrix}1\\0\\0\\1\end{bmatrix} & \begin{bmatrix}1\\0\\0\\1\end{bmatrix} & \begin{bmatrix}0\\1\\0\\0\end{bmatrix} & \Rightarrow
\end{matrix}
\tag{44}
$$

1000 0011 0100 1110 0001 1100 1001 1001 0010.

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

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 зададена 21-битова кодова дума. 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].

На любознателните студенти се дава възможност и за допълнителна самостоятелна работа – декодиране с използване 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, процесът на декодиране за разглеждания код на Рийд-Соломон е доста времеотнемащ и най-често продължителността на упражнението от 90 минути е твърде недостатъчна за цялостно 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 вече е по силите на отличните студенти.

ЗАКЛЮЧЕНИЕ

В публикацията е представена методика за декодиране чрез синтезиран 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 $f(x)=x^4+x+1$. Илюстрирани са процесите на откриване и коригиране на

трисимволна грешка при декодиране с 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

[5] Бороджиева, А. Кодиране с код на Рийд-Соломон (15,9), базиран на полето на Галоа GF(2^4), коригиращ трисимволна грешка. Научна конференция на РУ & СУ '16, Русе, 28 – 29.10.2016 г. (под печат).

За контакти:

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