Vježbe 11

1. Na prethodnom času je generisan BCH kod (15, 3) i kodirana je poruka 10111, tako da glasi: $c(x)$=100100011110101. Generisati 3 greške u ovoj poruci, pa je potom dekodirati.

Rješenje:

Neka se greške nalaze na pozicijama 7, 8 i 9. Primljena poruka je:

$$\begin{array}{c} r=[\begin{array}{ccccccccccccccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}] \\ \begin{array}{ccccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \end{array} \end{array}$$

Zapišimo opšti oblik sindroma, $S_j = \sum_{i=0}^{n-1} r_i \alpha_i^{-j},\ j = 1, 2, ..., 2w$ za posmatranu primljenu poruku:

$S_j = 1 + \alpha^{3j} + \alpha^{10j} + \alpha^{12j} + \alpha^{14j}$.

Pojedini sindromi su (sjetite se da smo ranije dokazali da je $\alpha^{15} = 1$):

$S_1 = 1 + \alpha^3 + \alpha^{10} + \alpha^{12} + \alpha^{14}$,

$S_2 = 1 + \alpha^6 + \alpha^{20} + \alpha^{24} + \alpha^{28} = 1 + \alpha^6 + \alpha^5 + \alpha^9 + \alpha^{13}$,

$S_3 = 1 + \alpha^9 + \alpha^{30} + \alpha^{36} + \alpha^{42} = 1 + \alpha^9 + 1 + \alpha^6 + \alpha^{12} = \alpha^6 + \alpha^9 + \alpha^{12}$,

$S_4 = 1 + \alpha^{12} + \alpha^{40} + \alpha^{48} + \alpha^{56} = 1 + \alpha^{12} + \alpha^{10} + \alpha^3 + \alpha^{11}$,

$S_5 = 1 + \alpha^{15} + \alpha^{50} + \alpha^{60} + \alpha^{70} = 1 + 1 + \alpha^5 + 1 + \alpha^{10} = 1 + \alpha^5 + \alpha^{10}$,

$S_6 = 1 + \alpha^{18} + \alpha^{60} + \alpha^{72} + \alpha^{84} = 1 + \alpha^3 + 1 + \alpha^{12} + \alpha^9 = \alpha^3 + \alpha^{12} + \alpha^9$.

Iskoristimo stepene primitivnog korjena prostog polinoma na kome je baziran dati kod (tabela kreirana na prethodnom času):

α^0	0001
α^1	0010
α^2	0100
α^3	1000
α^4	1001
α^5	1011
α^6	1111
α^7	0111
α^8	1110
α^9	0101
α^{10}	1010
α^{11}	1101
α^{12}	0011
α^{13}	0110
α^{14}	1100

Za S_1:

α^0	0001
α^3	1000
α^{10}	1010
α^{12}	0011
α^{14}	1100
$S_1=$	1100=α^{14}

Za S_2:

α^0	0001
α^5	1011
α^6	1111
α^9	0101
α^{13}	0110
$S_2=$	0110=α^{13}

Za S_3:

α^6	1111
α^9	0101
α^{12}	0011
$S_3=$	1001=α^4

Za S_4:

α^0	0001
α^3	1000
α^{10}	1010
α^{11}	1101
α^{12}	0011
$S_4=$	1101=α^{11}

Za S_5:

α^0	0001
α^5	1011
α^{10}	1010
$S_5=$	0000=0

Za S_6:

α^3	1000
α^9	0101
α^{12}	0011
$S_6=$	1110=α^8

Sada sindrom možemo pisati:

$S(x) = S_1 + S_2 x + S_3 x^2 + ... + S_{2w} x^{2w-1}$,

$S(x) = \alpha^{14} + \alpha^{13}x + \alpha^{4}x^{2} + \alpha^{11}x^{3} + 0x^{4} + \alpha^{8}x^{5}$.

U cilju dekodiranja primljene poruke, primjenimo dalje Euklidski algoritam na polinome $x^{2w} = x^{6}$ i dobijeni sindrom:

i	*V*	*R*	*Q*
-1	0	[0, *, *, *, *, *]	...
0	1	[8, *, 11, 4, 13, 14]	...
1	[7, *]	[3, 11, 5, 6, *]	[7, *]
2	[12, 5, 0]	[1, 14, 5, 16]	[5, 13]
3	[14, 12, 4, 5]	[14, *, 4]	[2, 5]

Podsjećanja radi, osnovne relacije u Euklidskom algoritmu (koje koristimo za popunjavanje gornje tabele) su:

$r_{-1} = prvi\ polinom$, $r_{0} = drugi\ polinom$, $v_{-1} = 0$, $v_{0} = 1$

$g_{k+1} = r_{k-1} / r_{k}$, $v_{k+1} = v_{k-1} - q_{k+1}v_{k}$.

Tako smo u prvoj iteraciji, za k=1, u cilju dobijanja q_1 i r_1 podijelili r_{-1} i r_0 (q_1 će biti rezultat dijeljenja, a r_1 ostatak dijeljenja):

$$x^{6} : (\alpha^{8}x^{5} + \alpha^{11}x^{3} + \alpha^{4}x^{2} + \alpha^{13}x + \alpha^{14}) = x\alpha^{-8} = x\alpha^{7}$$

$$\underline{x^{6} + \alpha^{3}x^{4} + \alpha^{-4}x^{3} + \alpha^{5}x^{2} + \alpha^{6}x}$$

$$\alpha^{3}x^{4} + \alpha^{11}x^{3} + \alpha^{5}x^{2} + \alpha^{6}x$$

pa odatle q_1=[7, *] (upisujemo eksponente, a sa * označavamo nepostojanje određenog stepena) i r_1= [3, 11, 5, 6, *]. Takođe, primjenom relacije za v_{k+1}:

$$v_1 = v_{-1} - q_1\, v_0 = [7, *].$$

U drugoj iteraciji, za k=2, dijelimo $(\alpha^{8}x^{5} + \alpha^{11}x^{3} + \alpha^{4}x^{2} + \alpha^{13}x + \alpha^{14})$ i $(\alpha^{3}x^{4} + \alpha^{11}x^{3} + \alpha^{5}x^{2} + \alpha^{6}x)$, i dobijamo q_2 i r_2.

Ovaj postupak primjenjujemo zaključno sa k=3 (odnosno do kada stepen polinoma r padne ispod w).

Sada za $v_{3}(x) = (\alpha^{14}x^{3} + \alpha^{12}x^{2} + \alpha^{4}x + \alpha^{5})$ tražimo vrijednosti x za koje će dati polinom biti jednak nuli. Ispostavlja se da će $v_{3}(\alpha^{6})$, $v_{3}(\alpha^{7})$ i $v_{3}(\alpha^{8})$ biti nule ovoga polinoma, pa zaključujemo da su greške nastale na pozicijama: 15–6=9, 15–7=8 i 15–8=7:

$$\begin{aligned} v_{3}(\alpha^{6}) &= \alpha^{14}(\alpha^{6})^{3} + \alpha^{12}(\alpha^{6})^{2} + \alpha^{4}(\alpha^{6}) + \alpha^{5} = \\ &= \alpha^{14}\alpha^{18} + \alpha^{12}\alpha^{12} + \alpha^{4}\alpha^{6} + \alpha^{5} = \\ &= \alpha^{2} + \alpha^{9} + \alpha^{10} + \alpha^{5} \end{aligned}$$

α^{2}	0100
α^{5}	1011
α^{9}	0101
α^{10}	1010
	0000

Isto se jednostavno pokazuje za $v_{3}(\alpha^{7})$ i $v_{3}(\alpha^{8})$.