Vježbe 10

1. (a) Odrediti generatorski polinom za BCH kodove (15,2) i (15,3), koristivši prosti polinom $x^4 + x^3 + 1$.

   (b) Data je poruka 10111. Kodirati je BCH kodom (15,3), definisanim pod (a).

Rješenje:

(a) Označimo sa α korjene posmatranog prostog polinoma $p(x) = x^4 + x^3 + 1$. Dalje možemo pisati:

$\alpha^4 + \alpha^3 + 1 = 0$, odnosno $\alpha^4 = \alpha^3 + 1$.

Prikažimo sada svaki stepen α^i pomoću izvedene jednakosti:

$\alpha^5 = \alpha\alpha^4 = \alpha(\alpha^3 + 1) = \alpha^4 + \alpha = \alpha^3 + \alpha + 1$,

$\alpha^6 = \alpha\alpha^5 = \alpha(\alpha^3 + \alpha + 1) = \alpha^4 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$,

$\alpha^7 = \alpha\alpha^6 = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^2 + \alpha + 1$,

$\alpha^8 = \alpha\alpha^7 = \alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha$,

$\alpha^9 = \alpha\alpha^8 = \alpha(\alpha^3 + \alpha^2 + \alpha) = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^2 + 1$,

$\alpha^{10} = \alpha\alpha^9 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha$,

$\alpha^{11} = \alpha\alpha^{10} = \alpha(\alpha^3 + \alpha) = \alpha^4 + \alpha^2 = \alpha^3 + \alpha^2 + 1$,

$\alpha^{12} = \alpha\alpha^{11} = \alpha(\alpha^3 + \alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha = \alpha + 1$,

$\alpha^{13} = \alpha\alpha^{12} = \alpha(\alpha + 1) = \alpha^2 + \alpha$,

$\alpha^{14} = \alpha\alpha^{13} = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2$,

$\alpha^{15} = \alpha\alpha^{14} = \alpha(\alpha^3 + \alpha^2) = \alpha^4 + \alpha^3 = \alpha^3 + 1 + \alpha^3 = 1$.

Predstavimo dobijene rezultate tabelarno, radi preglednosti:

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

Konjugati su stepeni reda 2^n stepena korjena prostog polinoma, koji se koriste u konstrukciji koda. Pošto konstruišemo kodove koji maksimalno mogu ispraviti tri greške, w=3, u našem slučaju to su stepeni:

α^{2w-1} za w=1,2,3, odnosno $[\alpha, \alpha^3, \alpha^5]$.

Odgovarajući konjugati za ove stepene su:

$\alpha : \alpha, \alpha^2, \alpha^4, \alpha^8$;

$\alpha^3 : \alpha^3, \alpha^6, \alpha^9, \alpha^{12}$;

$\alpha^5 : \alpha^5, \alpha^{10}$.

Obratite pažnju na to da se konjugati se ne ponavljaju, odnosno da se uzima samo broj različitih vrijednosti konjugata!

Npr. kada tražimo konjugate za stepen α:

α^{2^n} za n=0 dobijamo α,
za n=1 dobijamo α^2,
za n=2 dobijamo α^4,
za n=3 dobijamo α^8,
za n=4 dobijamo $\alpha^{16} = \alpha\alpha^{15} = \alpha$ (sjetite se da smo dokazali da je $\alpha^{15} = 1$!), a α već imamo!

Pošto smo sa α označili korjene posmatranog prostog polinoma, definišimo i preostala dva polinoma (za stepene α^3 i α^5). Označimo ih sa $g^3(x)$ i $g^5(x)$.

Pri tome važi $g_3(\alpha^3)$=0 i $g_5(\alpha^5)$=0 (isto tako važi za naš prosti polinom $p(\alpha)$=0).

$$g_3(x) = g_{30} + g_{31}x + g_{32}x^2 + g_{33}x^3 + g_{34}x^4$$

$$g_{30}[0001] + g_{31}[1000] + g_{32}[1111] + g_{33}[0101] + g_{34}[0011] = [0000]$$

$$\alpha^3 \qquad \alpha^6 \qquad \alpha^9 \qquad \alpha^{12}$$

Napišimo sada odgovarajući sistem jednačina, u cilju dobijanja koeficijenata ovog polinoma:

$$g_{31} + g_{32} = 0$$

$$g_{32} + g_{33} = 0$$

$$g_{32} + g_{34} = 0$$

$$g_{30} + g_{32} + g_{33} + g_{34} = 0$$

Netrivijalno rješenje je: $g_{30} = g_{31} = g_{32} = g_{33} = g_{34} = 1$, pa je:

$g_3(x) = x^4 + x^3 + x^2 + x + 1$.

Na sličan način odredimo i polinom $g_5(x)$:

$$g_5(x) = g_{50} + g_{51}x + g_{52}x^2$$

$$g_{50}[0001] + g_{51}[1011] + g_{52}[1010] = [0000]$$

$$\alpha^5 \qquad \alpha^{10}$$

Odgovarajući sistem jednačina je:

$$g_{51} + g_{52} = 0$$

$$g_{51} + g_{52} = 0$$

$$g_{50} + g_{51} = 0$$

Netrivijalno rješenje je: $g_{50} = g_{51} = g_{52} = 1$, pa je:

$g_5(x) = x^2 + x + 1$.

Napišimo sada generatorski polinom za BCH kod (15,2):

$g(x) = p(x)g_3(x) = (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^4 + x^2 + x + 1$.

Slično, generatorski polinom za BCH kod (15,3):

$g(x) = p(x)g_3(x)g_5(x) = (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$.

(b) Kodiranu poruku dobijamo množenjem informacionih simbola i generatorskog polinoma:

$c(x) = i(x)g(x)$.

Riječ koju treba da kodiramo je 10111, pa je njen odgovarajući polinom u opštem obliku:

$i(x) = i_0 + i_1 x + i_2 x^2 + i_3 x^3 + i_4 x^4$.

Odredimo sada odgovarajuću kodiranu riječ:

$$\begin{aligned}c(x) &= (i_0 + i_1 x + i_2 x^2 + i_3 x^3 + i_4 x^4)(x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1) = \\ &= i_0 + i_1 x + (i_0 + i_2)x^2 + (i_1 + i_3)x^3 + (i_2 + i_4)x^4 + \\ &+ (i_0 + i_3)x^5 + (i_0 + i_1 + i_4)x^6 + (i_1 + i_2)x^7 + (i_0 + i_2 + i_3)x^8 + (i_0 + i_1 + i_3 + i_4)x^9 + \\ &+ (i_0 + i_1 + i_2 + i_4)x^{10} + (i_1 + i_2 + i_4)x^{11} + (i_2 + i_3 + i_4)x^{12} + (i_3 + i_4)x^{13} + i_4 x^{14}\end{aligned}$$

$c_0 = i_0$	$c_8 = i_0 + i_2 + i_3$
$c_1 = i_1$	$c_9 = i_0 + i_1 + i_3 + i_4$
$c_2 = i_0 + i_2$	$c_{10} = i_0 + i_1 + i_2 + i_4$
$c_4 = i_1 + i_3$	$c_{11} = i_1 + i_2 + i_4$
$c_5 = i_0 + i_3$	$c_{12} = i_2 + i_3 + i_4$
$c_6 = i_0 + i_1 + i_4$	$c_{13} = i_3 + i_4$
$c_7 = i_1 + i_2$	$c_{14} = i_4$

Kodirana riječ je:

$c(x) =$	1	0	0	1	0	0	0	1	1	1	1	0	1	0	1
	c_0	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}