Vježbe 8

1. (a) Dokazati da je binarni polinom $x^3 + x^2 + 1$ prost.
   (b) Upotrijebiti ovaj polinom za dobijanje odgovarajućeg Hamming-ovog koda (napisati kontrolnu matricu).
   (c) Kreirati odgovarajuću hardversku strukturu (pravilo za funkcionisanje pomjeračkih registara) ovog koda.
   (d) Kodirati poruku 1001 kreiranim Hamming-ovim kodom.
   (e) Generisana je greška na poziciji x^2. Provjeriti rad kreiranog Hamming-ovog koda u ovom slučaju.
   (f) Predstaviti kontrolnu matricu Hamming-ovog koda sa 15 bita, ako je generatorski polinom $x^4 + x + 1$.

Rješenje:

(a) Binarni polinom se, u opštem slučaju smatra prostim, ukoliko nije djeljiv sa polinomima nižeg reda, tj. ako u procesu dijeljenja sa njima dobijamo ostatak.
Podijelimo $x^3 + x^2 + 1$ redom sa $x^2 + x + 1$, $x + 1$ i x.

$$\begin{array}{l}(x^3 + x^2 + 1) : (x^2 + x + 1) = x \\ \underline{x^3 + x^2 + x} \\ \qquad x + 1\end{array} \qquad\qquad \begin{array}{l}(x^3 + x^2 + 1) : (x + 1) = x^2 \\ \underline{x^3 + x^2} \\ \qquad 1\end{array}$$

$$\begin{array}{l}(x^3 + x^2 + 1) : x = x^2 + x \\ \underline{x^3} \\ \quad x^2 + 1 \\ \quad \underline{x^2} \\ \quad 1\end{array}$$

Očigledno, dobijamo ostatak prilikom svakog dijeljenja, što znači da je posmatrani binarni polinom prost.

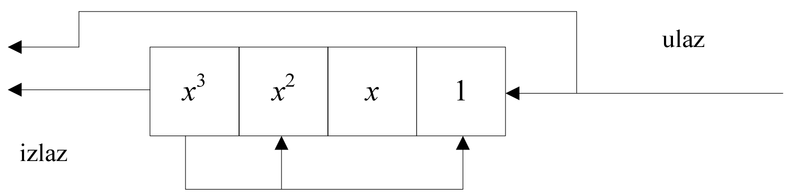
(b) Označimo sa a korjene posmatranog polinoma. Dalje možemo pisati:
$a^3 + a^2 + 1 = 0$, odnosno
$a^3 = a^2 + 1$
$a^4 = aa^3 = a(a^2 + 1) = a^3 + a = a^2 + a + 1$
$a^5 = aa^4 = a(a^2 + a + 1) = a^3 + a^2 + a = a^2 + 1 + a^2 + a = a + 1$
$a^6 = aa^5 = a(a + 1) = a^2 + a$
$a^7 = aa^6 = a(a^2 + a) = a^3 + a^2 = a^2 + 1 + a^2 = 1$
Zapišimo dobijene rezultate u binarnom obliku:

$$a^0 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \quad a^1 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \quad a^2 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \quad a^3 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \quad a^4 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \quad a^5 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \quad a^6 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

Kontrolna matrica H je tada:

$$\begin{array}{cc} & \begin{array}{ccccccc} a^6 & a^5 & a^4 & a^3 & a^2 & a & 1 \end{array} \\ H = & \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

(c) Hardverska struktura je oblika:



(d) Poruka koju treba kodirati je 1001, odnosno:

$$1\ 0\ 0\ 1\ \_\ \_\ \_$$

U cilju dobijanja nedostajućih kontrolnih bita podijelimo poznati dio poruke sa datim binarnim polinomom:

$$(x^6 + x^3) : (x^3 + x^2 + 1) = x^3 + x^2 + x + 1$$
$$\underline{x^6 + x^5 + x^3}$$
$$x^5$$
$$\underline{x^5 + x^4 + x^2}$$
$$x^4 + x^2$$
$$\underline{x^4 + x^3 + x}$$
$$x^3 + x^2 + x$$
$$\underline{x^3 + x^2 + 1}$$
$$x + 1$$

Imajući u vidu dobijeni ostatak, zaključujemo da su kontrolni biti 011, odnosno da je kodirana poruka oblika:

$$\begin{array}{ccccccc} a^6 & a^5 & a^4 & a^3 & a^2 & a & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}$$

(e) Pošto je greška na poziciji a^2, to je dobijena poruka:

$$\begin{array}{ccccccc} a^6 & a^5 & a^4 & a^3 & a^2 & a & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}$$

Dekodiranje obavljamo dijeljenjem polinoma dobijene poruke i generišućeg polinoma:

$$
\begin{array}{l}
(x^6+x^3+x^2+x+1):(x^3+x^2+1)=x^3+x^2+x+1\\
\underline{x^6+x^5+x^3}\\
\qquad\quad x^5+x^2+x+1\\
\qquad\quad \underline{x^5+x^4+x^2}\\
\qquad\qquad x^4+x+1\\
\qquad\qquad \underline{x^4+x^3+x}\\
\qquad\qquad\quad x^3+1\\
\qquad\qquad\quad \underline{x^3+x^2+1}\\
\qquad\qquad\qquad\quad x^2
\end{array}
$$

Odavde nedvosmisleno zaključujemo da je greška detektovana na poziciji a^2.

(f) Označimo sa a korjene posmatranog polinoma. Dalje možemo pisati:

$a^4+a+1=0$, odnosno

$a^4=a+1$

$a^5=aa^4=a(a+1)=a^2+a$

$a^6=aa^5=a(a^2+a)=a^3+a^2$

$a^7=aa^6=a(a^3+a^2)=a^4+a^3=a^3+a+1$

$a^8=aa^7=a(a^3+a+1)=a^4+a^2+a=a+1+a^2+a=a^2+1$

$a^9=aa^8=a(a^2+1)=a^3+a$

$a^{10}=aa^9=a(a^3+a)=a^4+a^2=a^2+a+1$

$a^{11}=aa^{10}=a(a^2+a+1)=a^3+a^2+a$

$a^{12}=aa^{11}=a(a^3+a^2+a)=a^4+a^3+a^2=a^3+a^2+a+1$

$a^{13}=aa^{12}=a(a^3+a^2+a+1)=a^4+a^3+a^2+a=a+1+a^3+a^2+a=a^3+a^2+1$

$a^{14}=aa^{13}=a(a^3+a^2+1)=a^4+a^3+a=a+1+a^3+a=a^3+1$

$a^{15}=aa^{14}=a(a^3+1)=a^4+a=a+1+a=1$

Stoga, kontrolna matrica je oblika:

$$
H=\begin{bmatrix}
1&1&1&1&0&1&0&1&1&0&0&1&0&0&0\\
0&1&1&1&1&0&1&0&1&1&0&0&1&0&0\\
0&0&1&1&1&1&0&1&0&1&1&0&0&1&0\\
1&1&1&0&1&0&1&1&0&0&1&0&0&0&1
\end{bmatrix}.
$$