Kreiranje kodova na osnovu prostih polinoma

Korišćenje matričnog zapisa u kreiranju kodova nam daje određenu slobodu, ali ima i znatne nedostatke. Naime, danas korišćeni kodovi imaju često dužinu od $n = 100$ pa i do $n = 1000$ bita, što znači da su memorijski zahtjevi za kontrolnu i generišuću matricu znatni. Takođe, ni matrično množenje nije jednostavna operacija.

Zbog toga se razvila posebna grupa kodova, podklasa linearnih kodova, koja predstavlja kodne riječi kao polinome. Takvi kodovi se zovu **ciklični kodovi**. Ovi kodovi se koriste kako samo za otkrivanje tako i za ispravljanje greške. Oni imaju jednostavniju hardversku realizaciju, a posebno u slučajevima otkrivanja i ispravljanja jednostrukih grešaka.

Primjer:

Sekvenca **10110** se može zapisati kao polinom:

$$P_1(X) = 1 \cdot X^4 + 0 \cdot X^3 + 1 \cdot X^2 + 1 \cdot X^1 + 0 \cdot X^0 = X^4 + X^2 + X$$

Sekvenca **01101** se može zapisati kao polinom:

$$P_2(X) = 0 \cdot X^4 + 1 \cdot X^3 + 1 \cdot X^2 + 0 \cdot X^1 + 1 \cdot X^0 = X^3 + X^2 + 1$$

Ovi polinomi se sabiraju po modulu 2 (sabiraju se koeficijenti uz odgovarajuće stepene po modulu 2, odnosno po ekskluzivnoj ili operaciji)

$$P_1(X) + P_2(X) = X^4 + X^2 + X + X^3 + X^2 + 1 = X^4 + X^3 + X + 1$$

Situacija sa množenjem polinoma je znatno komplikovanija, jer se često vrši po modulu najvećeg stepena u dva polinoma. Na primjer, ako je najveći dozvoljeni stepen u sistemu g, odnosno član X^g, i ako se prilikom množenja pojavi član X^r, gdje je $r > g$ uzima se $X^{r \bmod g}$.

Primjer:

$$P_1(X) = X + 1 \qquad P_2(X) = X^3 + X + 1$$

$$P_1(X) \cdot P_2(X) = (X+1) \cdot (X^3 + X + 1) = X^4 + X^2 + X + X^3 + X + 1 = X^4 + X^3 + X^2 + 1$$

Primjer:

$P_2(X) : P_1(X)$ (dijeljenje polinoma)

$$(X^3 + X + 1) : (X + 1) = X^2 + X$$

$$\begin{array}{r} -X^3 + X^2 \\ \hline X^2 + X + 1 \\ -X^2 + X \\ \hline 1 \end{array}$$

Ovdje je "+" i "-" ista operacija

$$P_2(X) = P_1(X) \cdot (X^2 + X) + 1$$

Definicija:

Prost polinom je onaj polinom koji je bez ostatka djeljiv sa samim sobom i sa jedinicom. Ili: prost polinom se ne može prikazati kao proizvod dva polinoma.

Primjer:

$$\left.\begin{array}{c} P(X)=1 \\ P(X)=X \\ P(X)=X+1 \\ P(X)=X^2+X+1 \end{array}\right\} \text{su prosti polinomi}$$

$$\left.\begin{array}{c} X^2=X\cdot X \\ X^2+1=(X+1)\cdot(X+1) \\ X^2+X=X\cdot(X+1) \end{array}\right\} \text{nijesu prosti polinomi}$$

$$(X+1)^2=X^2+1=(X+1)(X+1)$$

Kako se može dokazati da je neki polinom prost?

To se postiže dijeljenjem toga polinoma sa prostim polinomima nižeg reda (bez $P(X)=1$) i ako se dobija dijeljenje sa ostatkom u pitanju je prost polinom.

Prosti polinomi III stepena

$P(X)=X^3+X+1$ binarni zapis **1011** (ili obrnuto **1101**)

$P(X)=X^3+X^2+1$ binarni zapis **1101** (ili obrnuto **1011**)

Prosti polinomi IV stepena

$P(X)=X^4+X^3+1$ binarni zapis **11001** (ili obrnuto **10011**)

$P(X)=X^4+X+1$ binarni zapis **10011** (ili obrnuto **11001**)

Gore navedeni prosti polinomi se koriste kao **generatorski polinomi** za kreiranje cikličnih kodova.

Primjer:

Za kreiranje Hemingovog koda (7, 4) se koristi generatorski polinom III stepena, a za kreiranje Hemingovog koda (15, 11) generatorski polinom IV stepena.

n – dužina kodne riječi – polinom je reda n - 1

k – dužina informacione kodne riječi – polinom je reda k - 1

n - k – broj provjera na parnost, pa je stepen polinoma n - k

Ako želimo da kreiramo Hemingov kod (7, 4) koristeći generatorski prosti polinom $P(X) = X^3 + X + 1$, znamo da kodna riječ ima najveći stepen reda X^6. Sve kodne riječi se kreiraju po pravilu da su djeljive bez ostatka sa generatorskim polinomom. Da bi to bilo zadovoljeno kontrolna matrica koda mora da zadovoljava posebna pravila. Jedno od tih pravila je da u kolonama kontrolne matrice moraju da stoje stepeni nula polinoma:

$$X^3 + X + 1$$

Postavlja se pitanje što je nula polinoma $X^3 + X + 1$?

Očigledno da ni jedan od binarnih brojeva $X = 0$ i $X = 1$ ne zadovoljava ovu osobinu. Zbog toga se nule polinoma zapisuju u obliku vektora (broj elemenata je n - k)

$$P(a) = 0$$

Stepeni nule polinoma su:

$$1 = a^0 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \qquad a^1 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \qquad a^2 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

Ostale stepene nule polinoma dobijamo na sledeći način:

$P(a) = a^3 + a + 1$

$$a^3 = a + 1 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

$$a^4 = a^3 \cdot a = (a + 1) \cdot a = a^2 + a = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

$$a^5 = a \cdot a^4 = a(a^2 + a) = a^3 + a^2 = a^2 + a + 1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$$a^6 = a \cdot a^5 = a(a^2 + a + 1) = a^3 + a^2 + a = a^2 + 1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

$$a^7 = a \cdot a^6 = a(a^2 + 1) = a^3 + a = a + 1 + a = 1 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = a^0$$

Sada je kontrolna matrica ovog koda:

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}_{3\times 7}$$
$$a^6 \quad a^5 \quad a^4 \quad a^3 \quad a^2 \quad a^1 \quad a^0$$

Za vježbu dobiti matricu kada se koristi polinom $P(X) = X^3 + X^2 + 1$

Kodiranje

Pošto želimo da nam sindrom bude 0, 0, ..., 0, tj. da nema grešaka moramo zahtjevati da poslati polinom bude djeljiv sa polinomom $P(a) = a^3 + a + 1$.

Primjer:

Kodirati sekvencu **1001** Hemingovim kodom (7, 4) čiji je generatorski polinom $P(X) = X^3 + X + 1$ i neka se kontrolni biti dodaju na kraju kodne riječi.

Kodna riječ $C(X)$ mora biti djeljiva bez ostatka sa $P(X)$

1 0 0 1 C_2 C_1 C_0 – kodna riječ

$$C(X) = X^6 + X^3 + C_2X^2 + C_1X + C_0$$

$$C(X) : P(X) = X^6 + X^3 + C_2X^2 + C_1X + C_0 : X^3 + X + 1 = X^3 + X$$
$$\underline{X^6 + X^4 + X^3}$$
$$X^4 + C_2X^2 + C_1X + C_0$$
$$\underline{X^4 + X^2 + X}$$
$$(C_2 + 1)X^2 + (C_1 + 1)X + C_0$$

Da bi $C(X)$ bio djeljiv sa $P(X)$ bez ostatka:

$C_2 + 1 = 0 \Rightarrow C_2 = 1$
$C_1 + 1 = 0 \Rightarrow C_1 = 1$
$C_0 = 0 \Rightarrow C_0 = 0$

Kodna riječ je **1001110**

Dekodiranje

Pretopstavimo da je došlo do greške:

poslata kodna riječ: 1 0 0 1 1 1 0
primljena kodna riječ: 1 0 0 1 0 1 0

$C(X) = X^6 + X^3 + X$

$C(X) : P(X)$

$X^6 + X^3 + X : X^3 + X + 1 = X^3 + X$
$X^6 + X^4 + X^3$
$X^4 + X$
$X^4 + X^2 + X$
X^2 → ostatak

$X^2 = a^2 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ - greška je na ovoj poziciji