Seminarski rad iz predmeta
Teorija kodiranja

Primjena Furijeove transformacije u teoriji kodiranja

Student: Penjić Safet

PMF, Sarajevo, Decembar 2010.

Sadržaj

Napomena

- Ono što čini Diskretnu Furijeovu transformaciju korisnom u kodiranju je njezina veza sa linearnom kompleksnošću niza
- Ova vezu čemo iskoristiti za dekodiranje Reed-Solomonovog koda
- Čitav seminarski rad prati program napisan u C++ za kodiranje i enkodiranje Reed-Solomonovog koda
- Kako budem izlagao teoriju to ću pokazivati i kod programa koji to koristi
- Seminarski rad je kucan u LaTeX-u. Prezentacije je napravljene u PowerPointu. Moj mail je *infoarrt@gmail.com*

Prsten polinoma

- Konačno polje može se dobiti iz prstena plinoma

Definicija 1

Za svaki monik polinom *p(x)* nenula stepena nad poljem **F**, prsten polinoma modulo *p(x)* je skup svih polinoma sa stepenom manjim od *p(x)*, zajedno sa polinomijalnim sabiranjem i polinomijalnim množenjem modulo p(x). Ovaj prsten konvencionalno označavamo sa $F[x]/\langle p(x)\rangle$.

Teorema 2

$F[x]/\langle p(x)\rangle$ je prsten.

Prsten polinoma - Primjer 1

- U prstenu polinoma nad poljem *GF(2)*, izaberimo $p(x) = x^3 + 1$. Tada prsten polinoma modulo $p(x)$ je $GF(2)[x]/\langle x^3+1\rangle$. Ovaj prsten sadrži skup {0, 1, x, x + 1, x^2, x^2 + 1, x^2+x, x^2+x+1}. Navedimo primjer množenja u ovom prstenu:

$$(x^2+1)\cdot(x^2) = R_{x^3+1}[(x^2+1)\cdot(x^2)] = R_{x^3+1}[x(x^3+1)+x^2+x] =$$
$$= x^2+x$$

- Koristili smo redukciju $x^4 = x(x^3+1)+x.$

Konačno polje nad prstenom polinoma

Teorema 3

Prsten polinoma modulo monik polinom *p(x)* je polje ako i samo ako je *p(x)* prost polinom.

- Dokaz teoreme je u Seminarskom radu na strani 4. (dokažimo teorem)
- Koristeći ovu teoremu možemo zaključiti da kadgod možemo naći prost polinom stepena *m* nad *GF(q)*, tada možemo konstruisati konačno polje sa q^m elemenata u polju. Zašto? U ovoj konstrukciji, elementi su predstavljeni pomoću polinoma nad poljem *GF(q)* stepena manjeg od *m*. Postoji q^m takvih polinoma, pa prema tome q^m elemenata u polju.

Konačno polje - Primjer 1

- Konstruišimo *GF(4)* iz *GF(2)*, korištenjem primitivnog polinoma $p(x) = x^2 + x + 1$.
- Nesvodljivost ovog polinoma nije teško provjeriti testirajući sve moguce faktorizacije.
- Elementi polja su predstavljeni skupom polinoma *{0, 1, x, x + 1}.* Tabela aritmetike:

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

·	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

Problem za pisanje programa?

- Nije teško napisati program za sabiranje elemenata nekog konačnog polja **F** dobijenog iz prstena polinoma (svodi se na pisanje program za sabiranje polinoma čiji su koeficijenti iz nekog konačnog polja).
- Problem predstavlja kako definisati množenje elemenata nekog konačnog polja **F** dobijenog iz prstena polinoma?
- Rezultat proizvoda dva elementa iz konačnog polja **F**, gdje je polje **F** dobijeno iz prstena polinoma modulo monik polinom *p(x)*, je treći element iz polja **F** kojem odgovara polinom dobijen kao ostatak pri djeljenju proizvoda dva polinoma sa *p(x)* (vidjeti primjer sa 5 slajda).

Neke osobine konačnog polja

- Nenula elementi **F** bilo kojeg polja **F** formiraju Abelovu grupu.
- U slučaju konačnog polja *GF(q)*, multiplikativna grupa *GF(q)* ima red *q-1*.
- Iz činjenice da svaki element konačne grupe ima konačan red i generise cikličku grupu sa ovim redom i iz činjenice da red podgrupe od konačne grupe dijeli red ove grupe (Lagrangeov teorem) (za dokaz ove dvije teoreme pogledati Seminarski rad), slijedi da svaki element iz *GF(q)* je korijen polinomijalne jednačine $x^{q-1} = 1$, ili, što je ekvivalentno, svi nenula elementi od *GF(q)* kojih ukupno ima *q-1*, su nule polinoma $x^{q-1} - 1$.

Neke osobine konačnog polja

- Primjetimo da polinom stepena *d* (gdje je $d \geq 0$) sa koeficijentima iz polja **F** može imati najviše *d* nula u **F** ili u proširenom polju **E** od **F**.
- Prema tome, β je nula polinoma $x^{q-1}-1$ (ili, ekvivalentno, $x-\beta$ je djelilac od $x^{q-1}-1$) ako i samo ako je β nenula element iz GF(q).
- Time smo dokazali sljedeću teoremu

Faktorizacija od $x^{q-1}-1$ i primitivni element

Teorema 4 (Faktorizacija od $x^{q-1}-1$)

Polinom $x^{q-1}-1$ (gdje su koecijenti 1 i -1elementi polja GF(q)) se može potpuno faktorisati u linearne faktore na sljedeći način:

$$x^{q-1} - 1 = \prod_{\beta \in GF(q)^*} (x - \beta)$$

Definicija 5 (Primitivni element)

Primitivni element polja *GF(q)* je element β takav da se svi elementi polja osim nule mogu izraziti kao stepen od β.

Ciklička grupa iz GF(q)

- Pokažimo još da **grupa nenula elemenata iz *GF(q)* pod operacijom množenja tvori cikličku grupu reda q-1.**
- Prisjetimo se, grupa koja sadrži sve stepene jednog svog elementa zovemo ciklička grupa.
- Neka je *n* najveći (multiplikativni) red elementa iz GF(q).
- Kako red svakog elementa dijeli red elementa maksimalnog reda kad god je ovaj red konačan (Algebra), slijed da (multiplikativni) red svakog elementa iz *GF(q)* djeli *n*.
- Prema tome, svi elementi iz *GF(q)*, kojih ukupno ima *q-1* su nule polinoma x^n-1.

Ciklička grupa iz GF(q)

- Kako *n* dijeli *q-1* tada je sigurno $n \leq q-1$.
- Sa druge pak strane, x^n-1 ima najmanje *q-1* različitih nula pa je $n \geq q-1$.
- Prema tome možemo zaključiti da je $n = q-1$.
- Prema tome *GF(q)* sadrži element reda *q-1* pa je prema tome ciklička grupa reda *q-1*.

Multiplikativna grupa iz *GF(q)* - Primjer 1

- Posmatrajmo prsten svih polinoma nad poljem *GF(2).*
- Razmotrimo konstrukciju *GF(8)* koristeći prosti polinom $h(x) = x^3 + x + 1$. Znamo da je $GF(2)[x]/\langle x^3 + x + 1 \rangle$ polje. Primitivni element je x, koji ćemo označiti sa β, *pa* računajući $x^i \ mod \ h(x)$ dobićemo:

binarni zapis riječi	polinomijalni zapis $(x^i \ mod \ h(x))$	eksponencijalni zapis
000	0	-
001	1	β^0
010	x	β^1
100	x^2	β^2
011	$x+1$	β^3
110	x^2+x	β^4
111	x^2+x+1	β^5
101	x^2+1	β^6

Multiplikativna grupa iz *GF(q)* - Primjer 2

- Posmatrajmo konstrukciju polja *GF(16)* koristeći prosti polinom $p(x) = x^4 + x + 1$.

binarni zapis riječi	polinomijalni zapis $(x^i \bmod p(x))$	eksponencijalni zapis
0000	0	-
0001	1	γ^0
0010	x	γ^1
0100	x^2	γ^2
1000	x^3	γ^3
0011	$x+1$	γ^4
0110	x^2+x	γ^5
1100	x^3+x^2	γ^6
1011	x^3+x+1	γ^7
0101	x^2+1	γ^8
1010	x^3+x	γ^9
0111	x^2+x+1	γ^{10}
1110	x^3+x^2+x	γ^{11}
1111	x^3+x^2+x+1	γ^{12}
1101	x^3+x^2+1	γ^{13}
1001	x^3+1	γ^{14}

Multiplikativna grupa iz *GF(q)* - Primjer 2

- Npr. Ako podjelimo x^{10} sa $x^4 + x + 1$ iz dolje napisane računice vidimo da je ostatak djeljenja $x^2 + x + 1$.

$$
\begin{array}{rl}
x^{10} : (x^4 + x + 1) = x^6 + x^3 + x^2 + 1 & \\
\underline{+\ x^{10} + x^7 + x^6} & \\
x^7 + x^6 & \\
\underline{+\ x^7 + x^4 + x^3} & \\
x^6 + x^4 + x^3 & \\
\underline{+\ x^6 + x^3 + x^2} & \\
x^4 + x^2 & \\
\underline{+\ x^4 + x + 1} & \\
x^2 + x + 1 &
\end{array}
$$

$$
\begin{array}{rl}
x^{15} : (x^4 + x + 1) = x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1 & \\
\underline{+\ x^{15} + x^{12} + x^{11}} & \\
x^{12} + x^{11} & \\
\underline{+\ x^{12} + x^9 + x^8} & \\
x^{11} + x^9 + x^8 & \\
\underline{+\ x^{11} + x^8 + x^7} & \\
x^9 + x^7 & \\
\underline{+\ x^9 + x^6 + x^5} & \\
x^7 + x^6 + x^5 & \\
\underline{+\ x^7 + x^4 + x^3} & \\
x^6 + x^5 + x^4 + x^3 & \\
\underline{+\ x^6 + x^3 + x^2} & \\
x^5 + x^4 + x^2 & \\
\underline{+\ x^5 + x^2 + x} & \\
x^4 + x & \\
\underline{+\ x^4 + x + 1} & \\
1 &
\end{array}
$$

Konstrukcija Reed-Solomonovih kodova

- Razmotrit ćemo konstrukciju najvažnijih linearnih kodova, najvažnijih i teoriski i praktično koji su do sad pronađeni.
- Neka je dato bilo koje konačno polje *GF(q)* sa q≥3 elemenata i neka je *N* djelilac od *q - 1* koji je N ≥ 2.
- Neka je *α* element (multiplikativnog) reda *N* u *GF(q)*
  (Takvo *α* uvijek postoji. Zašto?)
- Neka je m_0 bilo koji cijeli broj koji zadovoljava $0 \leq m_0 < N$;
  (m_0 u praksi često ima vrijednost 0 ili 1)
- Neka je *d* cijeli koji je 2 ≤ d ≤ N.
- Na osnovu ovih parametara možemo definisati RS kodove

Reed-Solomonovi kodovi

Definicija 6 (Reed-Solomonovih kodova)

Reed-Solomonov kod *RS(q, N, α, m_0, d)* je *q*-arni linearni kod dužine bloka *N* za koji je

$$H = \begin{bmatrix} (\alpha^{m_0})^{N-1} & (\alpha^{m_0})^{N-2} & \dots & \alpha^{m_0} & 1 \\ (\alpha^{m_0+1})^{N-1} & (\alpha^{m_0+1})^{N-2} & \dots & \alpha^{m_0+1} & 1 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ (\alpha^{m_0+d-2})^{N-1} & (\alpha^{m_0+d-2})^{N-2} & \dots & \alpha^{m_0+d-2} & 1 \end{bmatrix}$$

matrica provjere parnosti.

Reed-Solomonovi kodovi - Primjer 1

- Razmotrimo kako bi izgledala matrica za provjeru parnosti Reed-Solomonovog koda u slučaju kada je $m_0=0$ i $m_0=1$.

$$H = \begin{bmatrix} 1 & 1 & \dots & 1 & 1 \\ \alpha^{N-1} & \alpha^{N-2} & \dots & \alpha & 1 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ (\alpha^{d-2})^{N-1} & (\alpha^{d-2})^{N-2} & \dots & \alpha^{d-2} & 1 \end{bmatrix}$$

$$H = \begin{bmatrix} \alpha^{N-1} & \alpha^{N-2} & \dots & \alpha & 1 \\ (\alpha^{2})^{N-1} & (\alpha^{2})^{N-2} & \dots & \alpha^{2} & 1 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ (\alpha^{d-1})^{N-1} & (\alpha^{d-1})^{N-2} & \dots & \alpha^{d-1} & 1 \end{bmatrix}$$

Reed-Solomonovi kodovi - Primjer 2

- Posmatrajmo polje *GF(8)* koje smo formirali u Primjeru 1 lekcije *Multiplikativna grupa iz GF(q)*, slajd 14
- Matrica provjere parnosti *RS(8, 7, α, 1, 3)* koda izgleda ovako:

$$H = \begin{bmatrix} \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha & 1 \\ \alpha^{12} & \alpha^{10} & \alpha^8 & \alpha^6 & \alpha^4 & \alpha^2 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha & 1 \\ \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^4 & \alpha^2 & 1 \end{bmatrix}$$

Vandermondova matrica

Problem

Vandermond matrica je kvadratna $m \times m$ matrica oblika:

$$V_m = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_m \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_m^2 \\ \alpha_1^3 & \alpha_2^3 & \dots & \alpha_m^3 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{m-1} & \alpha_2^{m-1} & \dots & \alpha_m^{m-1} \end{bmatrix}$$

gdje su α_1, α_2, ..., α_m elementi polja **F** (koje ne mora biti konačno). Dokazati da je

$$det(V_m) = \prod_{j=1}^{m-1} \prod_{i=j+1}^{m} (\alpha_i - \alpha_j)$$

pa prema tome V_m je nesingularna matrica ako i samo ako su α_1, α_2, ..., α_m različiti.

(rješenje problema se nalazi u Seminarskom radu na str. 10)

Dimenzija i minimalna udaljenost RS koda

- Odredimo dimenziju *K* i minimalnu udaljenost d_{min}

RS(q, N, α, m_0, d) koda. Primjetimo da *H* ima *d-1* redova

$$H = \begin{bmatrix} (\alpha^{m_0})^{N-1} & (\alpha^{m_0})^{N-2} & \dots & \alpha^{m_0} & 1 \\ (\alpha^{m_0+1})^{N-1} & (\alpha^{m_0+1})^{N-2} & \dots & \alpha^{m_0+1} & 1 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ (\alpha^{m_0+d-2})^{N-1} & (\alpha^{m_0+d-2})^{N-2} & \dots & \alpha^{m_0+d-2} & 1 \end{bmatrix}$$

- Posmatrajmo kvadratnu podmatricu formiranu biranjem kolona $i_1=N-k_1$, $i_2=N-k_2$, ..., $i_{d-1}=N-k_{d-1}$ iz *H*

(gdje je $N \geq k_1 > k_2 > \dots > k_{d-1} > 0$)

Dimenzija i minimalna udaljenost RS koda

- Ova podmatrica ima oblik

$$\tilde{H} = \begin{bmatrix} (\alpha^{m_0})^{i_1} & (\alpha^{m_0})^{i_2} & \dots & (\alpha^{m_0})^{i_{d-1}} \\ (\alpha^{m_0+1})^{i_1} & (\alpha^{m_0+1})^{i_2} & \dots & (\alpha^{m_0+1})^{i_{d-1}} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ (\alpha^{m_0+d-2})^{i_1} & (\alpha^{m_0+d-2})^{i_2} & \dots & (\alpha^{m_0+d-2})^{i_{d-1}} \end{bmatrix}$$

- Pokažimo da je ova matrica nesingularna, tj. da ima linearne nezavisne redove (ili sto je ekvivalentno, linearno nezavisne kolone).
- Svaku kolonu ove podmatrice možemo podijeliti sa $(\alpha^{m_0})^{i_j} \ (\neq 0),$ bez uticana na linearnu zavisnost ili nezavisnost kolona.
- Radeći tako, dobijamo novu podmatricu

Dimenzija i minimalna udaljenost RS koda

$$\hat{H} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{d-1}} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ (\alpha^{i_1})^{d-2} & (\alpha^{i_2})^{d-2} & \dots & (\alpha^{i_{d-1}})^{d-2} \end{bmatrix}$$

- Koju možemo prepoznati kao Vandermonde matrica reda *d-1*. Kako, *α* ima multiplikativni red *N* i kako imamo

  $0 < i_{d-1} < \dots < i_2 < i_1 \leq N$, slijedi da su elementi $i_1, i_1, \dots, i_{d-1}$ različiti pa je i ova Vandermonde matrica nesingularna (vidjeti prethodno problem)
- Prema tome *d-1* proizvolojnih kololna iz H su uvijek linearno nezavisne.

Dimenzija i minimalna udaljenost RS koda

- Primjerimo da *d* kolona izabranih iz *H* moraju biti linearno zavisne, s obzirom da ove kolone imaju samo *d-1* komponentu.
- Napisani argumenti povlače i to da su redovi od H linearno nezavisni. Slijedi da je minimalna udaljenost $d_{min}=d$ za RS kod (iz teorije kodiranja).
- Iz osobina linearnih kodova znamo da je $dim(H)+dim(G)=N$
- Prema tome dimenzija *K* našeg *RS* koda zadovoljava $N-K=d-1$ ili što je ekvivalentno, $d_{min} = N-K+1$, a linearni kodovi sa ovom osobinom se nazivaju MDS (maximum-distance-separable) kodovi.

Generator matrica RS koda

- Sad želimo da pronađemo generator matricu RS koda i ekasan algoritam za dekodiranje RS koda.
- Za ovu svrhu, predstavit ćemo diskretnu Furijeovu transformaciju (DFT), koja će nam pomoći da detaljnije shvatimo strukturu RS koda.

Diskretna Furijer-ova transformacija (DFT)

- Za prvi susret sa DFT tretiraćemo je kao aproksimaciju
- Definicija Furijeova transformacija funkcije f ϵ $L^1(\mathbf{R})$ gdje je

$$L_1(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{C} \mid \int_R |f(x)|dx < \infty\}$$

- je

$$\widehat{f}(\omega) = \int_{-\infty}^{\infty} f(t)e^{-i\omega t}\,dt$$

- Kada se gornji integral ne može izračunati u zatvorenom obliku, za dovoljno velike *a<0* i *b>0*, integral $\int_a^b f(t)e^{-i\omega t}\,dt$ je dobra aproksimacija za $\widehat{f}(\omega)$.

Diskretna Furijer-ova transformacija (DFT)

- Aproksimirajmo sad integral

$$\int_a^b f(t)e^{-i\omega t}\,dt$$

- Uzmimo uzorak na konačnom broju jednako vremenski razdvojenih tački

$$t_0 = a < t_1 < \ldots < t_N = b,\ a < 0,\ b > 0.$$

- Neka je $\Delta t = \frac{b-a}{N}$ i $t_k = a + k\Delta t,\ k = 0, 1, 2, \ldots, N.$

- Tada aproksimacija ϕ je data sa

Diskretna Furijer-ova transformacija (DFT)

$$\phi(\omega) = \sum_{k=0}^{N-1} f(t_k) e^{-i\omega t_k} \Delta t = \sum_{k=0}^{N-1} f(t_k) e^{-i\omega(a+k\Delta t)} \Delta t = \sum_{k=0}^{N-1} f(t_k) e^{-i\omega a} e^{-i\omega k \Delta t} \Delta t$$

$$= e^{-i\omega a} \sum_{k=0}^{N-1} f(t_k) e^{-i\omega k \frac{(b-a)}{N}} \Delta t.$$

- Izvadimo vremensko trajanje *[a, b]* iz prikaza, fokusirajući se samo na tačke (frekvenciju)

$$\omega_n = \frac{2\pi n}{b-a}$$

gdje je *n* cio broj. U ovim tačkama imamo

Diskretna Furijer-ova transformacija (DFT)

$$\phi(\omega_n) = e^{-i\omega_n a}\sum_{k=0}^{N-1} f(t_k)e^{-i\omega_n k\frac{(b-a)}{N}}\Delta t = e^{-i\omega_n a}\sum_{k=0}^{N-1} f(t_k)e^{-i\frac{2\pi n}{b-a}k\frac{(b-a)}{N}}\Delta t$$

$$= e^{-i\omega_n a}\sum_{k=0}^{N-1} f(t_k)e^{-i\frac{2\pi nk}{N}}\Delta t$$

- Ako zanemarimo multiplikativnu konstantu $e^{-i\omega_n a}\Delta t$

i fokusiramo pažnju samo na *N*-periodičnu funkciju $Df : \mathbb{Z} \to \mathbb{C}$, dobićemo

$$Df(n) = \sum_{k=0}^{N-1} f(t_k)e^{-i\frac{2\pi nk}{N}}, \quad n \in \mathbb{Z},$$

Diskretna Furijer-ova transformacija (DFT)

- Ili drugačije napisano

$$Df(n) = \sum_{k=0}^{N-1} f(t_k)\omega^{-nk}, \ gdje\ je\ \omega = e^{i\frac{2\pi}{N}}, \quad n \in \mathbb{Z}.$$

- Pogledajmo sad na ove stvari sa "diskretne" perspektive. Zaboravimo da je funkcija *f* denisana na **R**. Kako radimo samo sa vrijednostima funkcije *f* u konačnom broju tački, pretpostavimo da je *f* denisana na skupu *{0, 1, ..., N-1}*. Drugim riječima posmatrajmo funkciju f kao *n*-torku kompleksnih brojeva:

$$f = (f(0), f(1), ..., f(N-1)) \in \mathbb{C}^N.$$

Diskretna Furijer-ova transformacija (DFT)

Definicija 7 (Diskretna Furijeova transformacija)

- Pretpostavimo da je konačan skup $\mathbf{Z}_N$ opremljen sa diskretnom mjerom (svi podskupovi su mjerljivi i mjera svakog podskupa je broj elemenata u njemu). Kako je $\mathbf{Z}_N$ konačan skup, svaka funkcija denisana na njemu je integrabilna.

Diskretna Furijeova transformacija (DFT) funkcije $f : \mathbb{Z}_N \to \mathbb{C}$ je

$$Df(n) = \sum_{k=0}^{N-1} f(k) e^{-i\frac{2k\pi n}{N}} = \sum_{k=0}^{N-1} f(k)\omega^{-kn},\ n \in \mathbb{Z}_N,\ \omega = e^{i\frac{2\pi}{N}}$$

DFT u konačnom polju

- Bilo koji vektor $\mathbf{b} = [b_1 \;\; b_2 \;\; \ldots \;\; b_N] \in \mathbb{F}^N$ možemo identicirati kao polinom

$$\begin{aligned} b(X) &= b_1 X^{N-1} + b_2 X^{N-2} + \ldots + b_{N-1} X + b_N \\ &= \sum_{n=1}^{N} b_n X^{N-n} \end{aligned} \qquad (1)$$

reda manjeg od N sa koeficijentima iz polja **F** i možemo pričati naizmjenično o vektoru **b** ili o polinomu *b(X)*.

- Pretpostavimo da postoji element *α* (multiplikativnog) reda *N* u polju **F**.

DFT u konačnom polju

- Tada **Diskretna Furijeova transformacija** (DFT) vektora iz "vremenskog-domena" **b** je vektor iz "frekvenciskog-domena" $\mathbf{B} = [B_1 \ B_2 \ \ldots \ B_N] \in \mathbb{F}^N$ definisan sa

$$B_i = b(\alpha^i), \ i = 1, 2, ..., N. \qquad (2)$$

- Koristeći (1), (2) možemo napisati eksplicitno pomoću komponenti od **b** kao

$$B_i = \sum_{n=1}^{N} b_n \cdot (\alpha^i)^{N-n}$$

što, zbog činjenice da je $\alpha^{iN} = 1,$ možemo napisati u obliku

DFT u konačnom polju

$$B_i = \sum_{n=1}^{N} b_n \alpha^{-in}, \quad i = 1, 2, ..., N$$

što nam je već poznato iz Definicije 7.

- Pokažimo da ne postoje dva vektora sa istom DFT
- Pretpostavimo da su **b** i **b'** vektori sa istom DFT, tj. da je **B** = **B'**. Iz (2) slijedi da je α^i nula polinoma $b(X)-b'(X)$ za $i = 1, 2, ..., N$. Dalje, polinom $b(X) - b'(X)$ je reda manjeg od N, i nule $\alpha^1, \alpha^2, ..., \alpha^N$ ovog polinoma su sve različite.
- Možemo zaključiti da je $b(X)-b'(X)$ nula polinom, tj. $b(X) = b'(X)$, ili ekvivalentno, da je **b=b'**.

Teorema inverzije

Teorema 8 (Teorema inverzije)

Za funkciju $f : \mathbb{Z}_N \to \mathbb{F}$ sa DFT defisanom sa

$$Df(i) = B_i = \sum_{n=1}^{N} f(n)\alpha^{-in} = \sum_{n=1}^{N} b_n\alpha^{-in}, \;\; i = 1, 2, ..., N$$

$$(Df : \mathbb{Z}_N \to \mathbb{F})$$

gdje je *α* element iz F (multiplikativnog) reda N imamo

$$f(i) = b_i = \frac{1}{((N))} \sum_{i=1}^{N} Df(i)\alpha^{+ni} = \frac{1}{((N))} \sum_{i=1}^{N} B_i\alpha^{+ni}$$

gdje je *((N))* suma *N* jedinica iz polja **F**.

Teorema inverzije

- Dokaz teoreme se nalazi u Seminarskom radu na str. 16. (dokažimo teorem)
- Smisao ove lekcije je da se DFT može koristiti u bilo kojem polju. Preciznije, ako možemo naći element (multiplikativnog) reda *N* u polju **F**, tada možemo definisati i DFT dužine *N* za to polje.
- Iz diskusije o Multipllikativnoj grupi iz *GF(q)* slijedi da možemo podesiti DFT dužine *N* za konačno polje *GF(q)* ako i samo ako je *N* djelilac od *q-1*.
- Sljedeću teoremu ćemo iskoristiti u lekciji DFT i Reed-Solomonov kod

Još jedna korisna teorema

Teorema 9

Neka je $\boldsymbol{B}=(B_1, B_2, \ldots, B_N)$ DFT koja odgovara vektoru $\boldsymbol{b}=(b_1, b_2, \ldots, b_N)$.

Tada:

a) DFT koja odgovara komponenti $b_{((n-1))}$ je $\alpha^n B_n$;

b) DFT koja odgovara komponenti $\alpha^n b_n$ je $B_{((n-1))}$.

- Dokaz teoreme se nalazi u Seminrskom radu na str. 17 (dokažimo teoremu)

Reed-Solomonov kod i DFT

- Iz matrice provjere parnosti H, definisanoj u Definiciji 6, koju smo koristili za definisanje *RS(q, N, α, m_0, d)* koda, vidimo da $$bH^T = [b(\alpha^{m_0}) \quad b(\alpha^{m_0+1}) \quad \dots \quad b(\alpha^{m_0+d-2})]$$
- gdje je $$b(X) = b_1 X^{N-1} + b_2 X^{N-2} + \dots + b_{N-1} X + b_N.$$
- Iz (2) slijedi da $$bH^T = [B_{m_0} \quad B_{m_0+1} \quad \dots \quad B_{m_0+d-2}].$$
- Prema tome, alternativna definicija *RS(q, N, α, m_0, d)* koda je kao skup vektora **b** iz vremenskog domena *GF(q)^N* čija DFT nestaje u granicama frekvencije od m_0 do *m_0+d-2* uključivo.

Generator polinom RS koda i DFT

- Pokažimo da je RS kod ciklički kod.
- Neka je **d** kodna riječ iz RS koda. Prema Teoremi 9 (tvrdnja pod a)) ako je kodna riječ $\mathbf{d}= [d_1\ d_2\ \ldots\ d_N]$ ciklički pomjerena za jedno mjesto, npr. poslije pomjeranja dobijena riječ je $\mathbf{e}=[e_1\ e_2\ \ldots\ e_N] = [d_N\ d_1\ \ldots\ d_{N-1}]$, tada njezine komponente u frekventnom domenu D_j su pomnozene sa α^{-j}.
- Drugim riječima $\mathbf{E}= [\alpha^{-1}D_1\ \alpha^{-2}D_2\ \ldots\ \alpha^{-N}D_N\ ]$.
- Kako je $\alpha^{-j}D_j$ nula kadgod je D_j nula, cikličko pomjeranje od **d** je također kodna riječ. Prema tome RS kod je ciklički kod.

Generator polinom RS koda i DFT

- Jedinstven nenula monik polinom najmanjeg stepena iz linearnog koda *C* zovemo generator polinom koda C i označavamo ga sa *g(x)*.
- Prost polinom *f(x)* najmanjeg stepena nad poljem *GF(q)* sa osobinom *f(β)=0* se zove minimalni polinom od *β* nad *GF(q)* (*β* može biti i element iz proširenog polja *GF(q)*).

Teorema 10 *Ciklički kod sadrži sve množitelje generator polinom g(x) sa polinomima stepena k-1 i manje.*

Teorema 11 *Postoji ciklički kod blokdužine N sa generator polinomom g(x) ako i samo ako g(x) djeli x^N-1.*

Generator polinom RS koda i DFT

- Kako je RS kod ciklički kod, postoji generator polinom, *g(x)*, koji se može izračunati. Minimalni polinom nad *GF(q)* elementa *β* u istom polju je $f_\beta = x - \beta$. Primjetimo da su svi minimalni polinomi prvog stepena.
- Prema alternativnoj deniciji RS koda, **b** je kodna riječ ako i samo ako vrijedi $b(\alpha^{m_0}) = b(\alpha^{m_0+1}) = \ldots = b(\alpha^{m_0+d-1}) = 0.$
- Primjetimo da elementi $\{\alpha^{m_0}, \alpha^{m_0+1}, \ldots, \alpha^{m_0+d-1}\}$ potpuno definišu nenula monik polinom

$$g(x) = (x - \alpha^{m_0})(x - \alpha^{m_0+1})\ldots(x - \alpha^{m_0+d-1})$$

koji je najmanjeg stepena u RS kodu (Zašto?). Drugim riječima polinom *g(x)* je generator polinom za RS kod.

Generator matrica RS koda

- Posljedica Teorema 10 i 11 je

Posljedica 12

Neka polinom *g(x)* ima red *N-k*. Ako *g(x)* generiše linearan ciklički kod *C* nad $GF(2^r)$ dužine $N = 2r-1$, i dimenzije *k* tada

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix}$$

je generator matrica za C, i broj kodnih riječi u C je $(2^r)^k$.

Generator matrica RS koda - Primjer 1

- Konstruišimo GF(8) korištenjem prostog polinoma $h(x) = x^3 + x + 1$ (vidjeti Primjer 1, Multiplikativna grupa iz GF(q)) sa β kao primitivnim elementom. Neka je

$$g(x) = (x+\beta)(x+\beta^2) = x^2 + (\beta+\beta^2)x + \beta^3 = x^2 + \beta^4 x + \beta^3.$$

- Tada g(x) generiše linearni ciklički kod C nad GF(8) dužine 7. Generator matrica za C je

$$G = \begin{bmatrix} 1 & \beta^4 & \beta^3 & 0 & 0 & 0 & 0 \\ 0 & 1 & \beta^4 & \beta^3 & 0 & 0 & 0 \\ 0 & 0 & 1 & \beta^4 & \beta^3 & 0 & 0 \\ 0 & 0 & 0 & 1 & \beta^4 & \beta^3 & 0 \\ 0 & 0 & 0 & 0 & 1 & \beta^4 & \beta^3 \end{bmatrix}.$$

Generator matrica RS koda - Primjer 1

- C ima 8^5 kodnih riječi. Kodna riječ koja odgovara polinomu

$$m(x) = \beta^3 x^4 + \beta x + 1 \leftrightarrow \beta^3 00 \beta 1 = m,$$

na primjer je $m(x)g(x) \leftrightarrow mG = \beta^3 1 \beta^6 \beta \beta^4 0 \beta^3.$

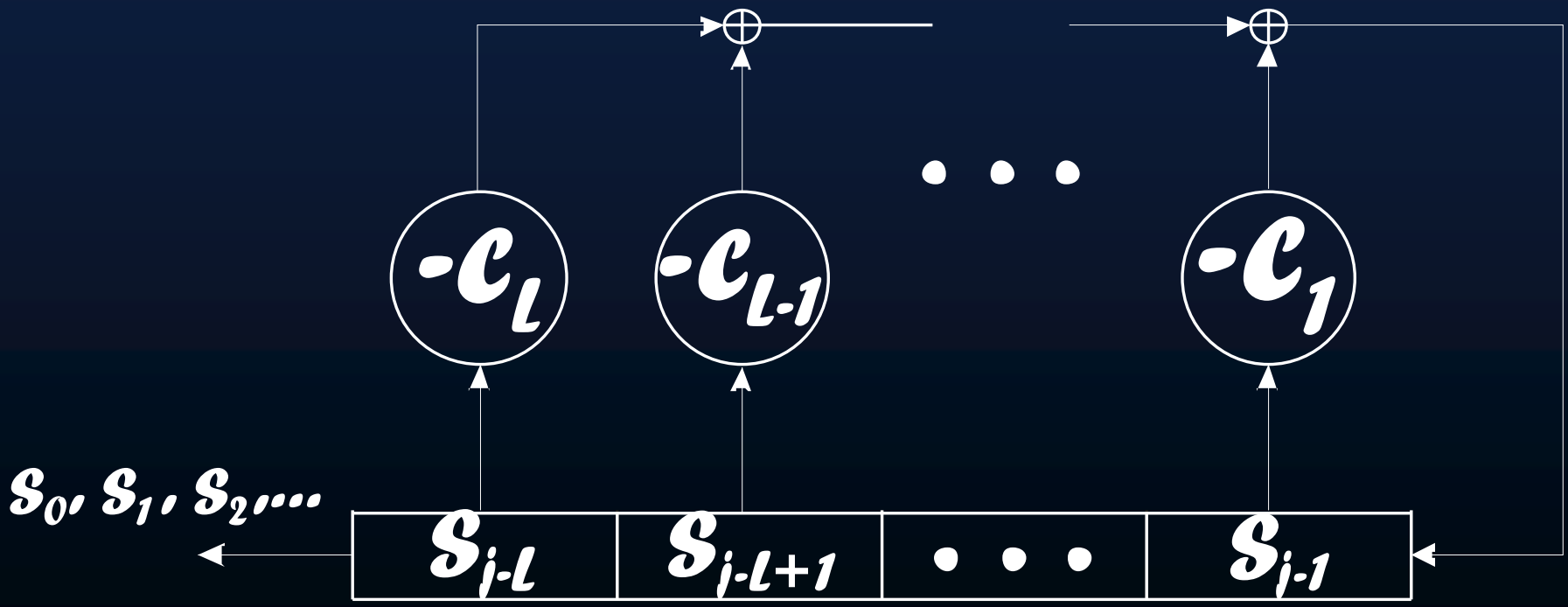
- Elementarnim transformacijama matrica G se može svesti na sljedeći oblik:

$$G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \beta^4 & \beta \\ 0 & 1 & 0 & 0 & 0 & \beta^5 & \beta \\ 0 & 0 & 1 & 0 & 0 & \beta^5 & \beta^3 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & \beta^4 & \beta^3 \end{bmatrix}.$$

- Zašto smo matricu G sveli na ovaj oblik?

Linear Feedback Shift Registar (LFSR)

- Linear Feedback Shift Registar je uređaj prikazan na slici (čelije sabiranja, množitelji sa konstantom, adrese)



Linear Feedback Shift Registar (LFSR)

- U LFSR inicijalno su učitani brojevi $s_0, s_1, \ldots, s_{L-1}$

(L je dužina LFSR)

- $s_0, s_1, \ldots, s_{L-1}$ su elementi nekog polja **F**
- $c_0, c_1, \ldots, c_{L-1}$ su elementi istog polja **F**
- LFSR počinje u vremenu 0, proizvodeći jednostrano beskonačan niz

$$\underset{\sim}{s} = (s_0, s_1, \ldots, s_N, \ldots)$$

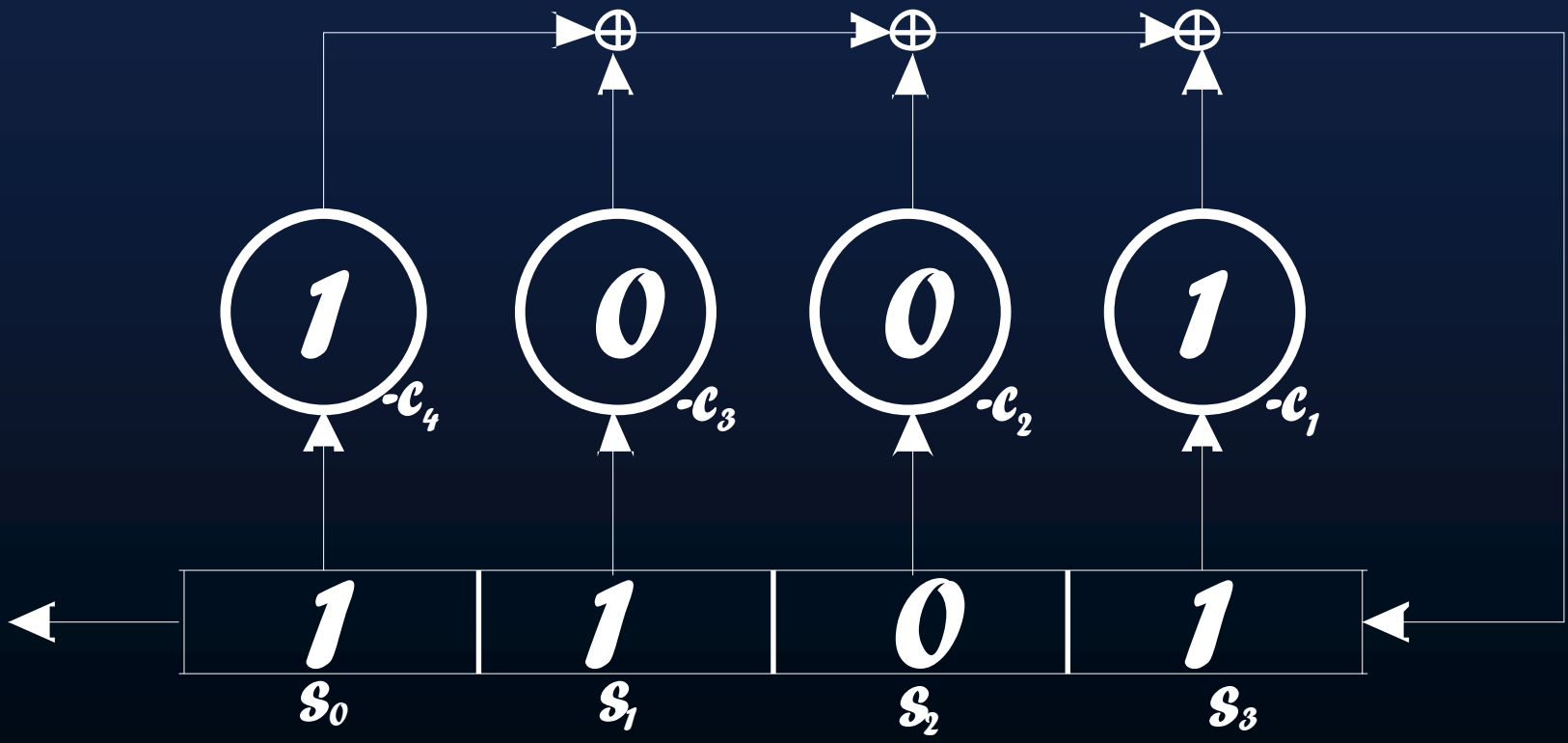
elemenata polja F po pravilu rekurzije

$$s_j = -c_1 s_{j-1} - c_2 s_{j-2} - \ldots - c_L s_{j-L},\ j = L, L+1 \ldots$$

ili drugačije napisano: $s_j + c_1 s_{j-1} + c_2 s_{j-2} + \ldots + c_L s_{j-L} = 0,$

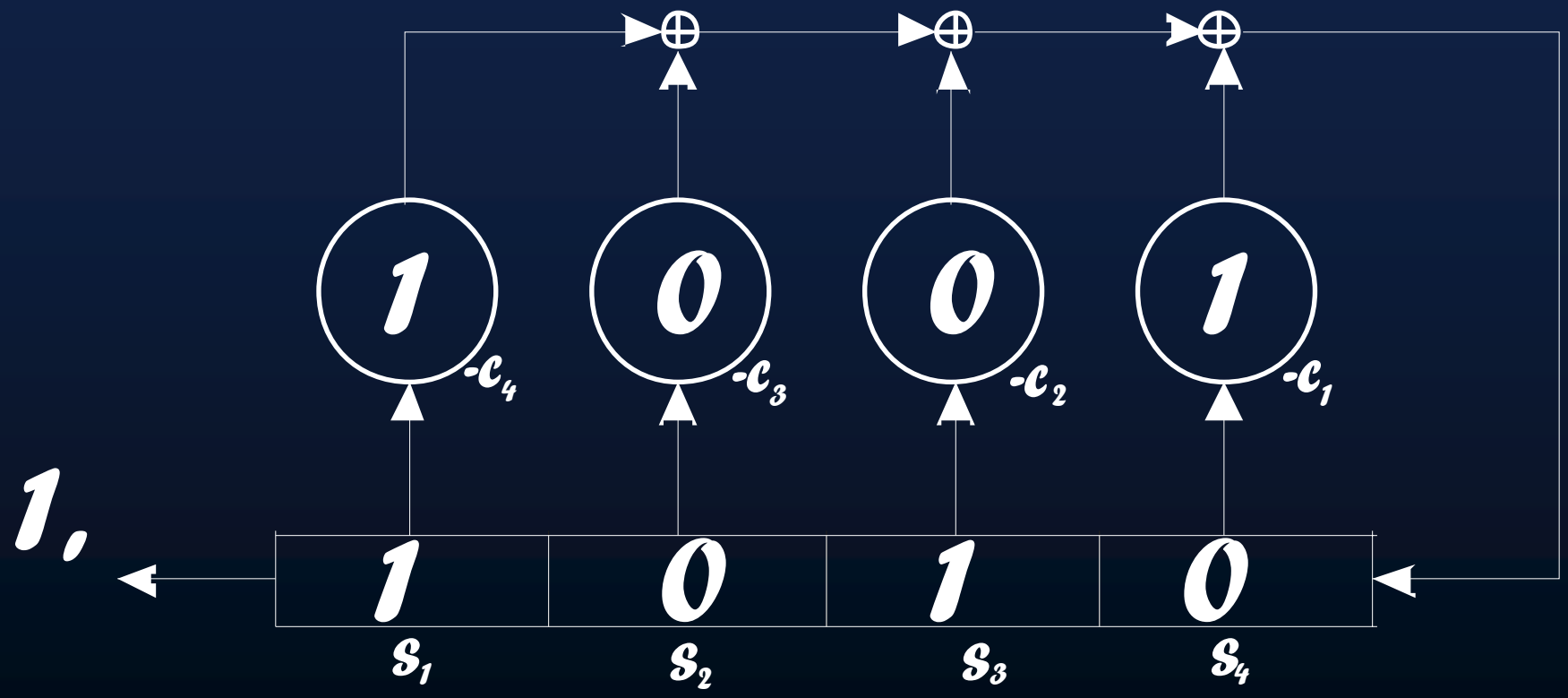
LFSR - Primjer 1

- Usvojimo binarnu aritmetiku i posmatrajmo



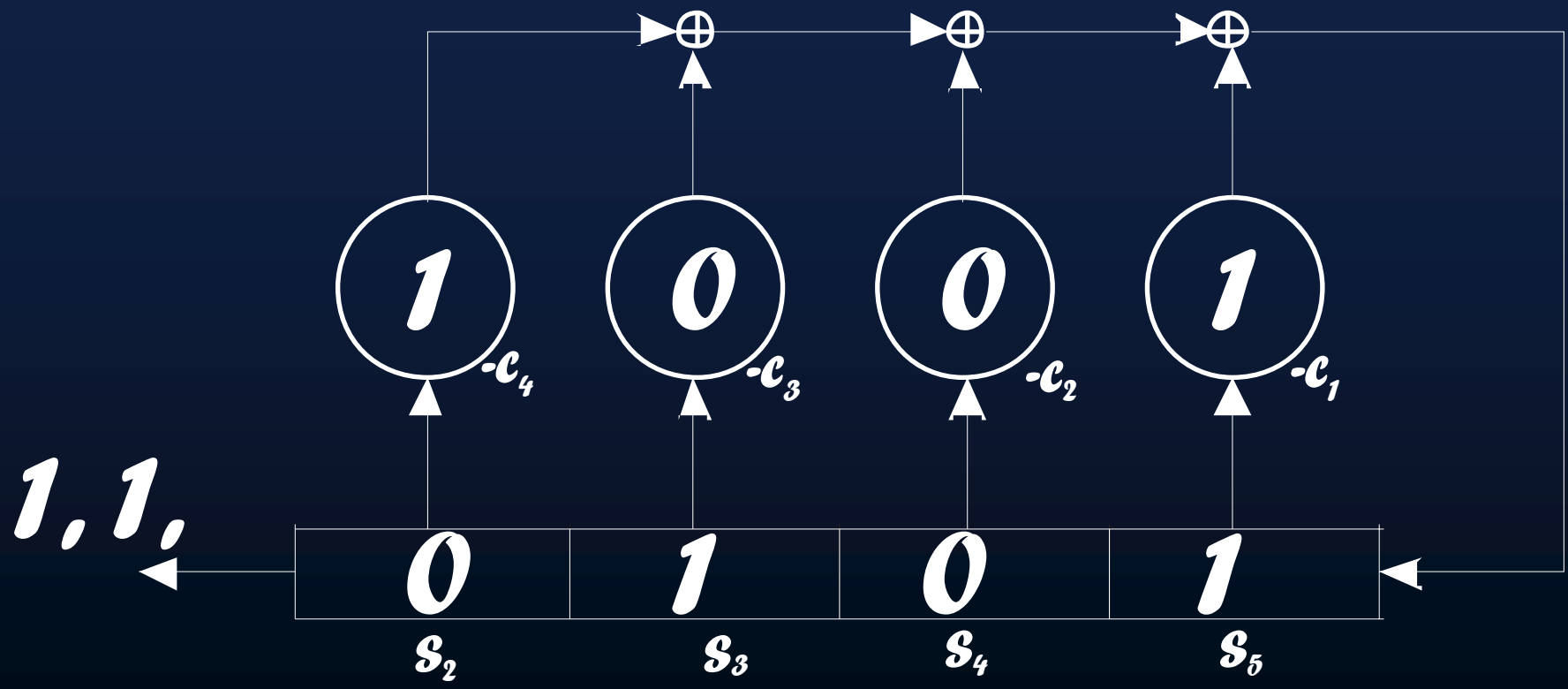
$$s_4=(-c_1)s_3+(-c_2)s_2+(-c_3)s_3-(c_4)s_0=1\bullet1+0\bullet0+0\bullet1+1\bullet1=0$$

LFSR - Primjer 1



$$s_5=(-c_1)s_4+(-c_2)s_3+(-c_3)s_2-(c_4)s_1=1\bullet0+0\bullet1+0\bullet0+1\bullet1=1$$

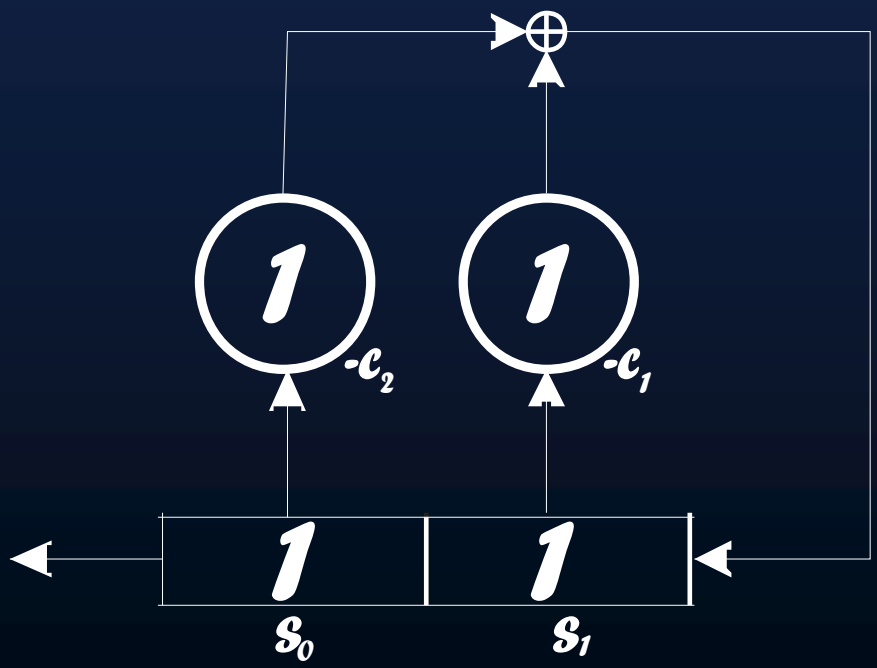
LFSR - Primjer 1

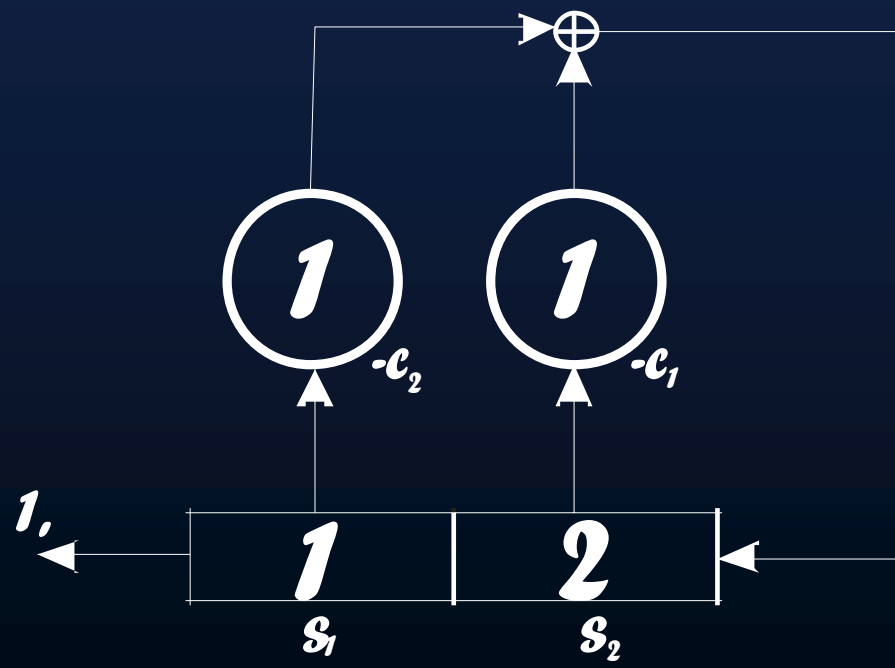


$$s_6=(-c_1)s_5+(-c_2)s_4+(-c_3)s_3-(c_4)s_2=1\cdot1+0\cdot0+0\cdot1+1\cdot0=1$$

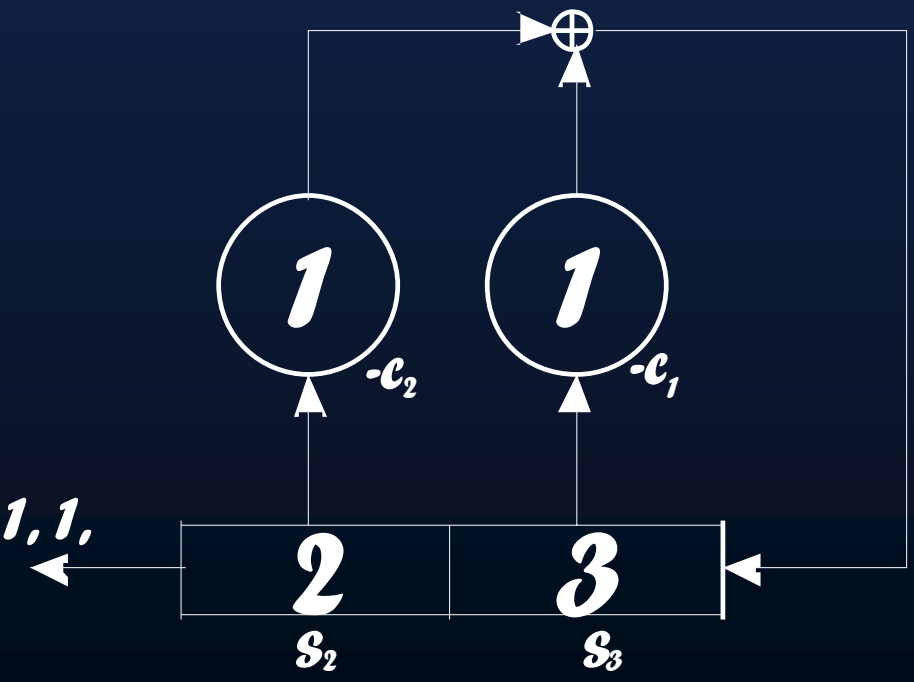
LFSR - Primjer 2 (Fibonačijev niz)

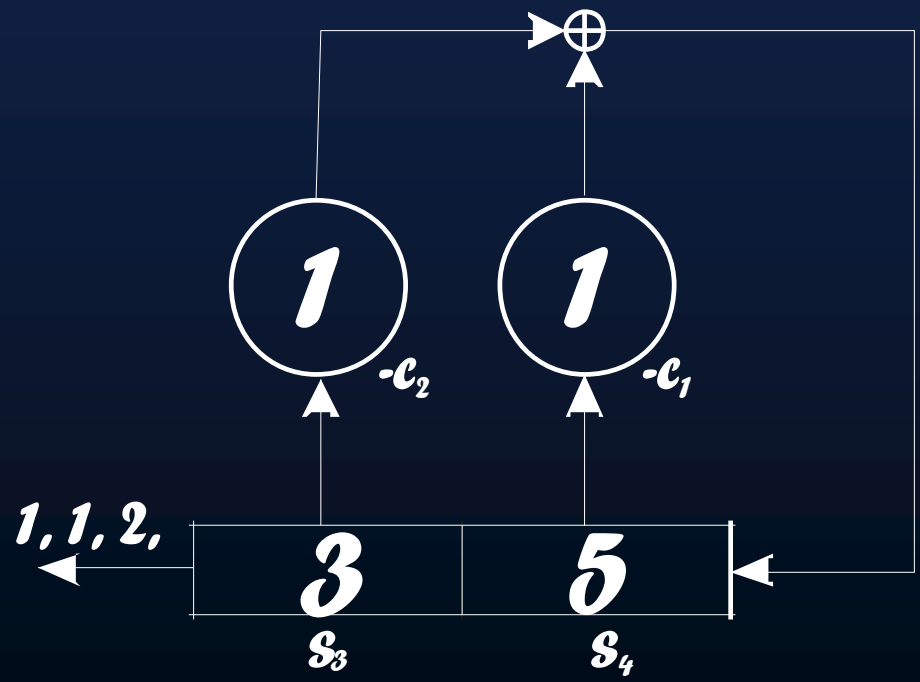
- Ako imamo prirodne brojeve i posmatramo





LFSR - Primjer 2 (Fibonačijev niz)





LFSR - Algebarski opis

- Želimo algebarski opisati izlazni niz $\underset{\sim}{s} = (s_0, s_1, ..., s_N, ...)$
- Niz $\underset{\sim}{s} = (s_0, s_1, ..., s_N, ...)$ poistovjetimo sa stepenim redom $S(D)=s_0 +s_1D+s_2D^2+...s_jD^j+s_{j+1}D^{j+1}+...$
- Polinom veze ćemo definisati sa

$$C(D)=1+c_1D+c_2D^2+...+c_LD^L$$

- Pišemo $\langle C(D),L \rangle$ za oznaku LFSR sa polinomom veze $C(D)$ i dužinom L
- $C(D)$ sam nije dovoljan da opiše LFSR
- Sad primjetimo rekurziju $s_j +c_1 s_{j-1} +c_2 s_{j-2} +...+ c_L s_{j-L}=0$.
- Šta možemo reći za proizvod $C(D)S(D)$?

LFSR - Algebarski opis

$$C(D)S(D) = (1 + c_1 D + c_2 D^2 + ... + c_L D^L)(s_0 + s_1 D + s_2 D^2 + ... s_L D^L + ...) =$$

$$= s_0 + (c_1 s_0 + s_1) D + (c_2 s_0 + c_1 s_1 + s_2) D^2 + ... + (c_{L-1} s_0 + c_{L-2} s_1 + ... + s_{L-1}) D^{L-1} +$$

$$\underbrace{(c_L s_0 + c_{L-1} s_1 + ... + s_L)}_{=0} D^L + \underbrace{(c_{L+1} s_1 + c_L s_2 + ... + s_{L+1})}_{=0} D^{L+1} + ...$$

- **P(D)** nema nenula članova stepena L ili većeg (Zašto?)
- **P(D)** je polinom stepena strogo manjeg od L i možemo napisati

$$\mathbf{P(D)=p_0+p_1D+p_2D^2+...+p_{L-1}D^{L-1}}$$

- Ako izjednačimo članove stepena *i*, *i*<*L*, sa obe strane jednakosti **C(D)S(D)= P(D)** dobićemo sljedeću matričnu jednakost:

LFSR - Algebarski opis

$$\begin{bmatrix} p_0 \\ p_1 \\ . \\ . \\ . \\ p_{L-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \dots & \dots & 0 \\ c_1 & 1 & \dots & 0 & 0 \\ . & . & \dots & & . \\ . & \dots & . & & . \\ c_{L-2} & & \dots & . & 0 \\ c_{L-1} & c_{L-2} & \dots & c_1 & 1 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ . \\ . \\ . \\ s_{L-1} \end{bmatrix}$$

- Možemo zaključiti da za svaki izbor od **P(D)** (za svaki niz od **L** brojeva), postoji LFSR čiji su množitelji koeficijeniti iz **C(D),** i postoji jedinstveno odgovarajuće inicijalno stanje $s_0, s_1, s_2, \dots, s_L$ od LFSR, takvo da konstruisani LFSR može proizvesti beskonačan niz $\underset{\sim}{s} = (s_0, s_1, \dots, s_N, \dots)$

LFSR - Algebarski opis

- Time smo dokazali sljedeću teoremu

Teorema 1

- LFSR $\langle \mathbf{C(D),L} \rangle$ može proizvesti jednostrano-beskonačan izlazni niz $\underset{\sim}{\mathbf{s}}$ ako i samo ako se stepeni red **S(D)** može napisati u obliku

$$S(D) = \frac{P(D)}{C(D)}$$

gdje je **P(D)** polinom stepena strogo manjeg od L.

LFSR - Primjer 3

- Neka je dato polje $\mathbf{F_3[x]}$ (skup svih polinom nad poljem GF(3))
- Neka je **f(x)=1** i $\mathbf{g(x)=2x^4+x+1}$ (iz prethodne teoreme **P(D)=f(x)** i **C(D)=g(x)**)
- **g(x)** u ovom slučaju je polinom veze
- Tada možemo konstruisati LFSR koji će proizvesti jednostrano-beskonačan niz
- Članovi tog niza neka su koeficijenti polinoma h(x)

$$h(x) = \frac{f(x)}{g(x)} = 1 + 2 \cdot x + x^2 + 2 \cdot x^3 + 2 \cdot x^4 + x^6 + x^7 + x^8 + \ldots$$

(Kako smo dobili 1+2x+...?)

LFSR - Primjer 3

- Kako naći inicijalno stanje ovog LFSR?
- Primjetimo da je $\mathbf{h(x)=h_0+h_1x+h_2x^2+...+h_Lx^L+h_{L+1}x^{L+1}+...}$
- Kad iskoristimo formulu rekurzije dobijemo da je

$$h_j + g_1 h_{j-1} + g_2 h_{j-2} + g_3 h_{j-3} + g_4 h_{j-4} = 0, \quad j = 4, 5, \ldots$$

- Ako sa p(x) označimo

$$\mathbf{p(x)= h_0+h_1x+h_2x^2+h_3x^3}$$

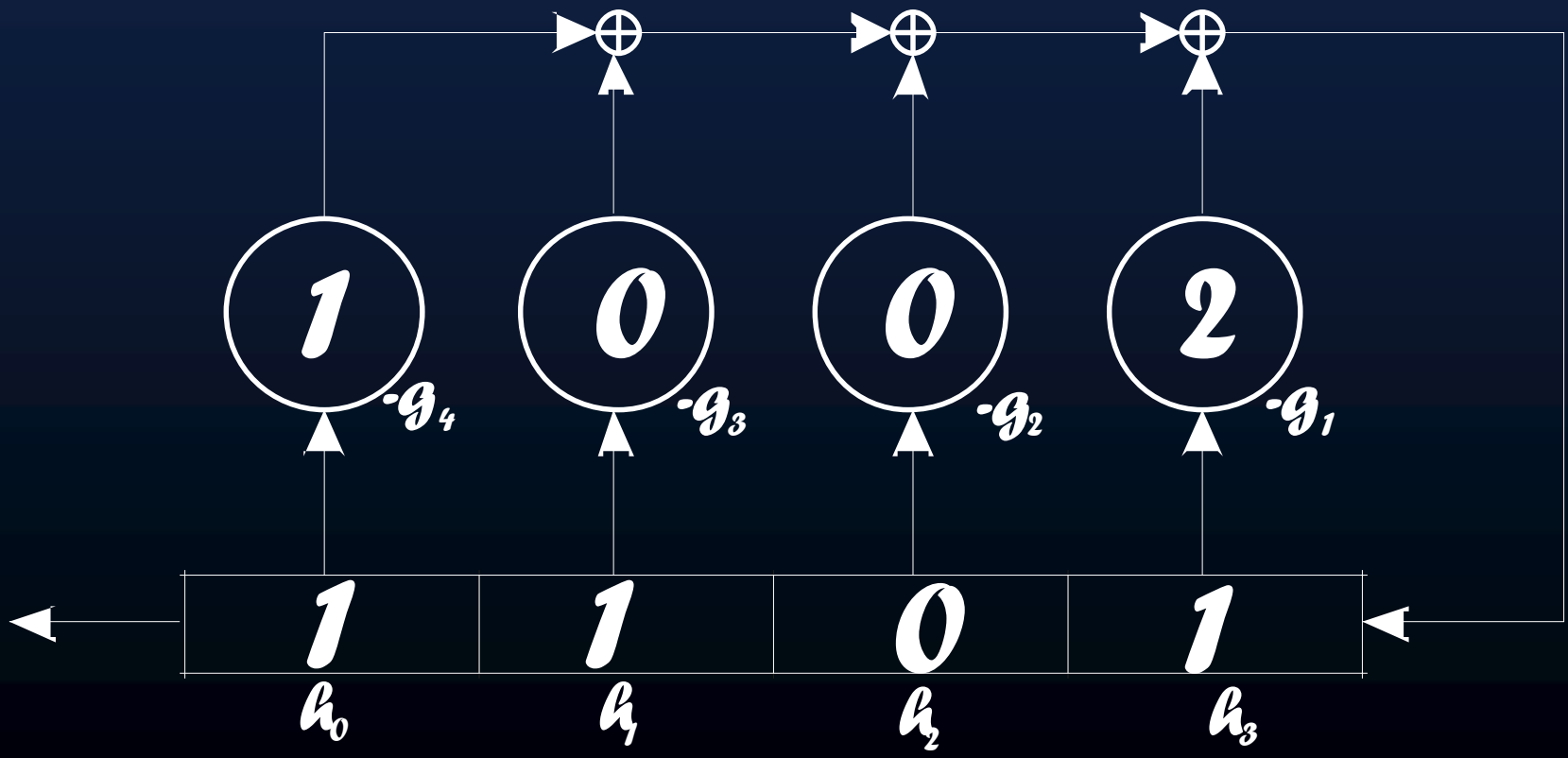
primjetimo da je

$$h(x)g(x) = p(x)g(x) = 1$$

a odavde dobijemo da su $\mathbf{h_0=1, h_1=2, h_2=2}$

LFSR - Primjer 3

- Početno stanje LFSR koji proizvodi koeficijente 2, 1, 2, 2, 0, 1, 1, 1, 2, 2, 2, 2, 0, 2, 0, 2, 1, 1, 2, 0, 1, ... izgleda



Linearna kompleksnost niza

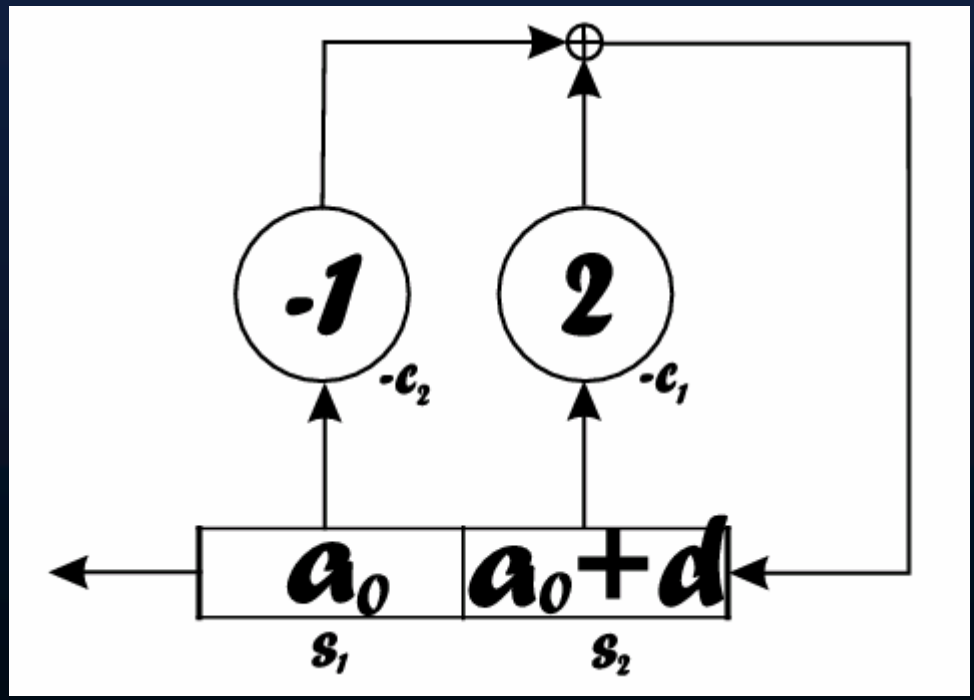
- Linearna kompleksnost jednostranog-beskonačnog niza $\underset{\sim}{\mathbf{s}}$ je najmanji broj **L** takav da se niz $\underset{\sim}{\mathbf{s}}$ može proizvesti pomoću LFSR dužine **L**, i on je beskonačan ako takav LFSR ne postoji
- Linearnu kompleksnost ćemo označavati sa $\mathbf{L}(\underset{\sim}{\mathbf{s}})$
- Nula niz $\underset{\sim}{\mathbf{0}}=(0, 0, 0,...)$ ima linearnu kompleksnost 0
- Linearna kompleksnost konačnog niza

$$\underset{\sim}{\mathbf{s}}^{(n)}=(s_1, s_2, \ldots, s_n)$$

se definiše kao najmanja linearna kompleksnost od svih jednostrano-beskonačnih nizova koji imaju $\underset{\sim}{\mathbf{s}}^{(n)}$ kao prefiks.

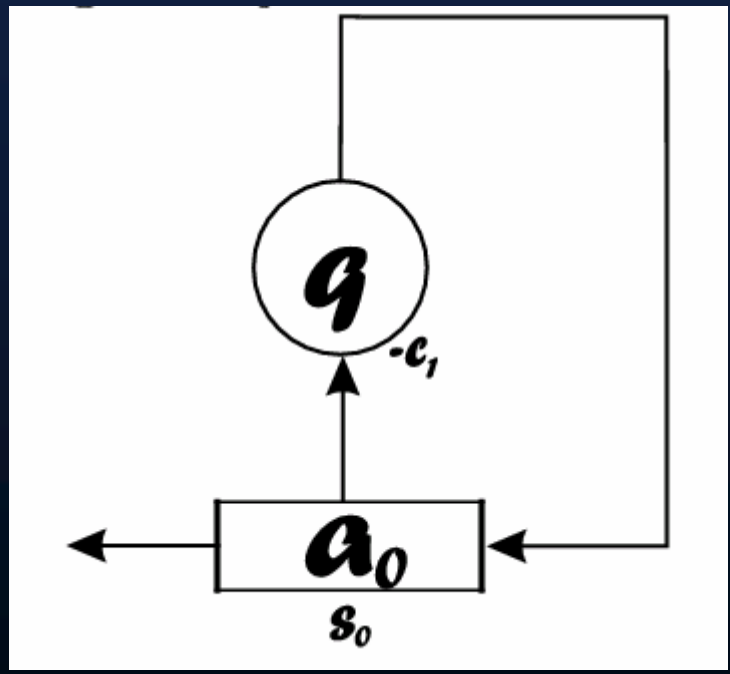
Linearna kompleksnost aritmetičkog niza

- Linearna kompleksnost aritmetičkog niza je 2.



Linearna kompleksnost geometriskog niza

- Linearna kompleksnost geometriskog niza je 1.



Zanimljiva pitanja

- Kolika je linearna kompleksnost niza $a_n=n/(n+1)$?

1/2, 2/3, 3/4, 4/5, 5/6, 6/7, ...

- Kolika je linearna kompleksnost niza $b_n=2n/(n^2+3)$?

1/2, 4/7, 1/2, 8/19, 5/16, 4/13, ...

- Da li se niz brojeva koji dolazi iz broja $\sqrt{2}$ može uhvatiti pomoću LFSR?

1, 4, 1, 4, 2, 1, 3, 5, 6, 2, 3, 7, 3, 0, 9, 5, 0, 4, 8, 8, ...

- Može li neki LFSR biti korišten kao brojač?
- Može li LFSR biti korišten kao generator pseudo-slučajnog niza koji se onda možda može koristiti u kriptografiji?

Dvije korisne teoreme za kompleksnost niza

Teorema 2 (Linearna kompleksnost jednostrano besonačnog niza)

Ako se stepeni red *S(D)* jednostranog-beskonačnog niza $\underset{\sim}{s}$ može napisati u obliku

$$S(D) = \frac{P(D)}{C(D)}$$

gdje su *P(D)* i *C(D)* relativno prosti polinomi (tj. nemaju zajedničkog faktora stepena 1 ili većeg) i *C(D)=1*, tada imamo

$$L(\underset{\sim}{\mathbf{s}}) = max\{stepen(C(D)), 1 + stepen(P(D))\}$$

Štaviše, *C(D)* je polinom veze jedinstvenog LFSR dužine *L=L(**s**)* koji može proizvesti $\underset{\sim}{\mathbf{s}}$.

Dvije korisne teoreme za kompleksnost niza

Teorema 3 (Linearna kompleksnost konačnog niza)

Ako je $\mathbf{L}(\underset{\sim}{\mathbf{s}})=L>0$ i ako $\underset{\sim}{\mathbf{s}}^{(n)}$ označav prvih n brojeva od $\underset{\sim}{\mathbf{s}}$ tada

$$L(\underset{\sim}{\mathbf{s}}^{(n)}) = L, \;\; za\, sve\, n \geq 2L$$

Štaviše, jedinstvenost od LFSR dužine L koji može proizvesti $\underset{\sim}{\mathbf{s}}$ je također jedinstveni LFSR dužine L koji može proizvesti $\underset{\sim}{\mathbf{s}}^{(n)}$ za svaki $n \geq 2L$.

- Dokaz ove teorem se nalazi u Seminarskom radu na str. 25.

Zanimljiv problem

- Neka je dat neki niz $s_0, s_1, \ldots, s_{N-1}$ dužine N.
- Postoji li i ako postoji, kako pronaći efikasan algoritam za pronalaženje (jednog od) najkraćih LFSR koji proizvode dati niz $\mathbf{s}^{(n)}$ dužine N?
- Odgovor na ovo pitanje je pozitivan i zvove se LFSR sinteza algoritam (ili Barlekamp-Massey algoritam, kako se često zove).
- Dijagram ovog algoritma je dat na sljedećoj slici, a dokaz da algoritam zaista pronalazi jedan od najkraćih LFSR koji proizvode $\mathbf{s}^{(n)}$ se može naći u [4]

Zanimljiv problem

- Neka je dat neki niz $s_0, s_1, \ldots, s_{N-1}$ dužine N.
- Postoji li i ako postoji, kako pronaći efikasan algoritam za pronalaženje (jednog od) najkraćih LFSR koji proizvode dati niz $\underset{\sim}{\mathbf{s}}^{(n)}$ dužine N?
- Odgovor na ovo pitanje je pozitivan i zvove se LFSR sinteza algoritam (ili Barlekamp-Massey algoritam, kako se često zove).
- Dijagram ovog algoritma je dat na sljedećoj slici, a dokaz da algoritam zaista pronalazi jedan od najkraćih LFSR koji proizvode $\mathbf{s}^{(n)}$ se može naći u [4]

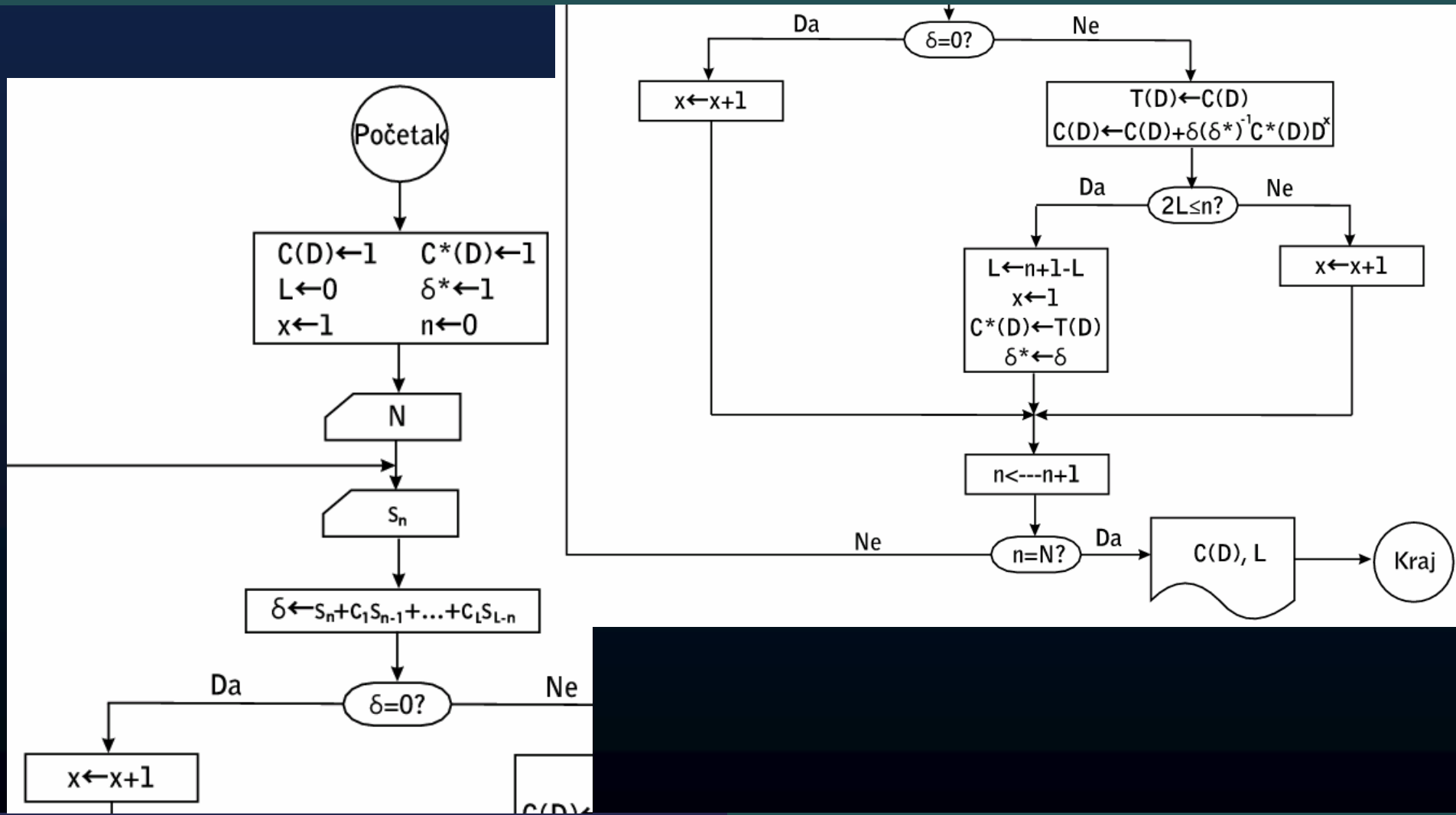
Zanimljiv problem

- Neka je dat neki niz $s_0, s_1, \ldots, s_{N-1}$ dužine N.
- Postoji li i ako postoji, kako pronaći efikasan algoritam za pronalaženje (jednog od) najkraćih LFSR koji proizvode dati niz $\underset{\sim}{\mathbf{s}}^{(n)}$ dužine N?
- Odgovor na ovo pitanje je pozitivan i zvove se LFSR sinteza algoritam (ili Barlekamp-Massey algoritam, kako se često zove).
- Dijagram ovog algoritma je dat na sljedećoj slici, a dokaz da algoritam zaista pronalazi jedan od najkraćih LFSR koji proizvode $\mathbf{s}^{(n)}$ se može naći u [4]

Zanimljiv problem

- Neka je dat neki niz $s_0, s_1, \ldots, s_{N-1}$ dužine N.
- Postoji li i ako postoji, kako pronaći efikasan algoritam za pronalaženje (jednog od) najkraćih LFSR koji proizvode dati niz $\underset{\sim}{\mathbf{s}}^{(n)}$ dužine N?
- Odgovor na ovo pitanje je pozitivan i zvove se LFSR sinteza algoritam (ili Barlekamp-Massey algoritam, kako se često zove).
- Dijagram ovog algoritma je dat na sljedećoj slici, a dokaz da algoritam zaista pronalazi jedan od najkraćih LFSR koji proizvode $\underset{\sim}{\mathbf{s}}^{(n)}$ se može naći u [4]

Zanimljiv problem



Linearna kompleksnost i DFT

- Da li postoji veza između linearne kompleksnosti i diskretne Furijeove transformacije?
- Pokazaćemo da je Haming težina konačnog niza u jednom domenu jednaka linearnoj kompleksnosti tog niza u drugom

Blahut-ova teorema

Teorema 4 (Blahut-ova teorema)

Ako je $\mathbf{B} \in \mathbf{F}^N$ DFT od vektora $\mathbf{b} \in \mathbf{F}^N$, i ako su $\underset{\sim}{\mathbf{b}}$ i $\underset{\sim}{\mathbf{B}}$ jednostrano beskonačni nizovi $\underset{\sim}{\mathbf{b}}=(b_0, b_1, b_2, \ldots)$, $\underset{\sim}{\mathbf{B}}=(B_0, B_1, B_2, \ldots)$ koji su definisani iz $\mathbf{b}$ i $\mathbf{B}$ relacijom $b_n=b_{n+N}$ i $B_i=B_{i+N}$ za svakok $n>0$ i $i>0$ (ili drugačije napisano $\underset{\sim}{\mathbf{B}}=(\mathbf{B}, \mathbf{B}, \mathbf{B},\ldots)$, $\underset{\sim}{\mathbf{b}}=(\mathbf{b}, \mathbf{b}, \mathbf{b},\ldots)$) tada

$$L(\underset{\sim}{\mathbf{B}}) = w(\mathbf{b})$$

i

$$w(\mathbf{B}) = L(\underset{\sim}{\mathbf{b}}).$$

Blahut-ova teorema - dokaz

Dokaz:

- Ako bi bilo **b=0** tvrdnja je trivijalna, pa pretpostavimo da je **b≠0**.
- Kako je **b≠0** to je i **B≠0**.
- Koristeći definiciju DFT

$$B_i = \sum_{n=1}^{N} b_n \alpha^{-in}, \quad i = 1, 2, ..., N$$

stepeni red $\underset{\sim}{B}$ možemo napisati kao

$$B(D) = \sum_{i=0}^{\infty} B_i D^i = \sum_{i=0}^{\infty} \left(\sum_{n=1}^{N} b_n \alpha^{-in} \right) D^i$$

$$= \sum_{n=1}^{N} b_n \sum_{i=0}^{\infty} (\alpha^{-n} D)^i$$

Blahut-ova teorema - dokaz

- ili

$$B(D) = \sum_{n=1}^{N} b_n \frac{1}{1 - \alpha^{-n} D} =$$

$$= \frac{b_1}{1 - \alpha^{-1} D} + \frac{b_2}{1 - \alpha^{-2} D} + \ldots + \frac{b_N}{1 - \alpha^{-N} D}$$

- α ima multiplikativni red **N** pa su α^{-1}, α^{-2}, ..., α^{-N} različiti
- Kad saberemo, desna strana zadnje jednakosti je parcijalni razlomak sa *w(b)* članova, pa možemo pisati

$$B(D) = \frac{P(D)}{C(D)}$$

Blahut-ova teorema - dokaz

- *P(D)* i *C(D)* su relativno prosti polinomi i imamo

  stepen(P(D))<stepena(C(D))=w(b)

- i

$$C(D) = \prod_{n=1 \, i \, b_n \neq 0}^{N} (1 - \alpha^{-n} D).$$

- Iz ove jednakosti slijedi da je *C(0)=1*, pa prema Teoremi 1

$$\langle C(D), L = w(\mathbf{b}) \rangle$$

je jedinstveni najkraći LFSR koji proizvodi $\underset{\sim}{\mathbf{B}}$. U stvari pokazali smo da je $\mathrm{L}(\underset{\sim}{\mathrm{B}}) = w(\mathbf{b})$ q.e.d.

Dekodiranje Reed-Solomonovog koda

- Sad kad znamo definiciju matrice provjere parnosti RS koda, vezu između te matrice i DFT, pojam linearne kompleksnosti niza i vezu između linearne kompleksnosti i DFT nije teško formulirati algoritam za dekodiranje RS koda koji će ispraviti uzorke od *t* ili manje greški gdje je $2t<d=d_{min}$.
- Neka je **b** tranzmitovana riječ i neka je **e** napravljeni uzorak greške, tako da je $\mathbf{r} = \mathbf{b} + \mathbf{e}$ primljena riječ ($r=[r_0 \quad r_1 \quad r_2 \quad \ldots \quad r_{N-1}]$).
- Uzimajući DFT dobijemo $R_i = B_i + E_i, \ za\ sve\ i.$

Dekodiranje Reed-Solomonovog koda

- Ali kako je $B_i=0$ za $i=m_0, m_0+1, \ldots, m_0+d-2$ imamo

$$R_i = E_i, \quad m_o \leq i \leq m_0 + d - 2.$$

- Sad primjetimo da znamo *d-1* članova jednostrano-beskonačnog niza

$$\underset{\sim}{\mathbf{E}}' = [E_{m_0} \quad E_{m_0+1} \quad \ldots \quad E_{m_0+d-2} \quad E_{m_0+d-1} \quad E_{m_0+d} \quad \ldots]$$

gdje "prim" na $\underset{\sim}{\mathbf{E}}'$ nas podsjeća da ovaj niz nije isti kao $\underset{\sim}{\mathbf{E}}$ čiji je prvi član E_0.

- $\underset{\sim}{\mathbf{E}}$ je perodičan niz pa je $\mathbf{L(\underset{\sim}{E}')=L(\underset{\sim}{E})}$ (svaki od ovih nizova sadrži drugi kao podniz)

Dekodiranje Reed-Solomonovog koda

- Blahut-ova teorema nam govori da je $L(\underset{\sim}{\mathbf{E}}) = w(\mathbf{e})$

iz čega možemo zaključiti da je

$$L(\underset{\sim}{\mathbf{E}}') = w(\mathbf{e}).$$

- Iz naših rezultata o Linearnoj kompleksnosti konačnih nizova, slijedi da ako je $2w(\mathbf{e}) \leq d - 1$

tada možemo pronaći najkraći LFSR koji proizvodi $\underset{\sim}{\mathbf{E}}'$ primjenjujući LFSR sinteza algoritam na prvih *d-1* poznatih članova od $\underset{\sim}{\mathbf{E}}'$.

Dekodiranje Reed-Solomonovog koda

- Poslije toga možemo koristiti ovaj LFSR zajedno sa poznatim članovima od $\tilde{\mathbf{E}}'$ da bi proizveli *N*-torku $\tilde{\mathbf{E}}'$ koja je samo cikličko pomjeranje od $\tilde{\mathbf{E}}$.
- Poznavajući **E**, možemo pronaći **e** pomoću inverzne DFT i tad povratiti kodnu riječ **b** kao **r-e**.
- S druge pak strane, ako dobijemo da je $2w(\mathbf{e}) \geq d$

ovaj algoritam će dati netačan rezultat.

- Dekodirana riječ će garantovano biti tačna samo kad stvarna greška ima Hamming težinu koja zadovoljava

$$2w(\boldsymbol{e}) < d = d_{min}.$$

Dekodiranje Reed-Solomonovog koda

- Sumirajmo ovaj efikasni algoritam dekodiranja

1. korak: Izračunati E_i za $m_0 \leq i \leq m_0 + d - 2$ tako što ćemo izračunati DFT primljene riječi $\mathbf{r}$ nad ovom granicom frekvencije.

2. korak: Koristeći LFSR sinteza algoritam pronaći (jedan od) najkraćih LFSR-a $\langle C(D), L \rangle$ koji će proizvesti konačan niz E_{m_0}, E_{m_0+1}, ..., E_{m_0+d-2}. Ako dobijemo da je $2L \geq d$, stani i emitiraj **?**, tj. objavi da je pronađen uzorak greške.

Dekodiranje Reed-Solomonovog koda

3. korak: Učitaj LFSR $\langle C(D), L\rangle$ sa zadnjih L brojeva niza $E_{m_0}, E_{m_0+1}, \ldots, E_{m_0+d-2}$ i pokreni LFSR $N-(d-1)$ put da bi proizveli $\hat{\mathbf{E}}' = [E_{m_0} \;\; E_{m_0+1} \;\; \ldots \;\; E_{m_0+d-2} \;\; \hat{E}_{m_0+d-1} \;\; \hat{E}_{m_0+N-1}]$.

4. korak: Ciklički, odgovarajuće, pomjerimo $\hat{\mathbf{E}}'$ (u zavisnosti od vrijednosti m_0) da bi dobili $\hat{\mathbf{E}} = [\hat{E}_1 \;\; \hat{E}_2 \;\; \ldots \;\; \hat{E}_N]$.

5. korak: Izračunati inverznu DFT $\hat{\mathbf{e}}$ od $\hat{\mathbf{E}}$.

6. korak: Oduzmimo $\hat{\mathbf{e}}$ od $\mathbf{r}$ da bi dobili dekodirajuću odluku $\hat{\mathbf{b}}$ za tranzmitovanu riječ.

Dvije zanimljivosti - 1. zanimljivost

- Diskretna Furijeova transformacija se može definisati nad komutativnim prstenom. Tačnije vrijedi sljedeća teorema. (dokaz vidjeti u [2]).

Teorema

Ako je α primitivni N-ti korijen jedinice u komutativnom prstenu **R**, tada

$$B_i = \sum_{n=1}^{N} b_n \alpha^{-in}, \quad i = 1, 2, ..., N$$

definiše inverzibilno prslikavanje sa $\mathbf{R}^N$ u $\mathbf{R}^N$ čija inverzija je data sa

$$b_n = \frac{1}{((N))} \sum_{i=1}^{N} B_i \alpha^{+ni}, \quad n = 1, 2, ..., N$$

ako i samo ako $\alpha^k - 1$ je jedinica u **R** za *k=1, 2, ..., N*.

Dvije zanimljivosti - 2. zanimljivost

- Blahut-ova teorema vrijedi nad komutativnim prstenom (dokaz vidjeti u [2]).

Teorema (Blahutova teorema za komutativni prsten)

Ako β generiše DFT dužine N u komutativnom prstenu R i **B**=DFT_{β}(**b**), tada linearna kompleksnost periodično ponavljanog niza **B**, **B**, **B**,... je jednak w_H(**b**), Haming težini od **b**.

Literatura

- [1] J. L. Massey, "**Applied Digital Information Theory II**", Lecture notes hold by author from 1981 until 1997 at the ETH Zurich, str. 49-60.
- [2] J. L. Massey, "**Discrete Fourier Transform in Coding and Cryptography**", In Proc. IEEE Information Theory Workshop, San Diego, CA, 8-11, str. 1-2, Feb. 1998.
- [3] R. E. Blahut, "**Algebraic Codes for Data Transmission**", Cambridge University Press, str. 67-163, 2003.
- [4] J. L. Massey, "**Shift-Register Synthesis and BCH Decoding**", IEEE Trans. on Info. Th., Vol. IT-15, str. 122-127, Jan. 1969.

Literatura

- [5] J. L. Massey i T. Schaub, "**Linear Complexity in Coding Theory**", Coding theory and Applications (Eds G. Cohen and Ph. Godlewski), Lecture notes in Computer Science, No. 311. Heidelberg and New York: Springer, str. 19-32, 1998.
- [6] G. Bachman, L. Narici i E. Beckenstein, "**Fourier and Wavelet Analysis**", Springer-Verlag New York, str. 383-406, 2000.
- [7] D.G. Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger i J.R. Wall, "**Coding Theory - The Essentials**", Marcel Dekker, str. 97-164, 1991.