AUTOMATE LINIARE

S.l. dr. Ing. Vlad-Cristian Miclea

Universitatea Tehnica din Cluj-Napoca
Departamentul Calculatoare

CUPRINS

PLAN CURS

- Partea 1 – VHDL
  1. Limbajul VHDL – 1
  2. Limbajul VHDL – 2
  3. Limbajul VHDL – 3
- Partea 2 – Implementarea sistemelor numerice
  4. Microprogramare
  5. Partea 1 - Unitate de comanda – exemplu cuptor
  5. Partea 2 - Unitate de executie – exemplu cuptor
- Partea 3 – Automate
  6. Automate finite
  7. Stari
  8. Automate sincrone
  9. Automate asincrone
  10. Identificarea automatelor
  11. Automate fara pierderi
  12. **Automate liniare**
- Partea 4 – Probleme si discutii

CONTEXT

Cursurile trecute

- Automate finite
  - Abstractizarea circuitelor secventiale
- Stari ale automatelor
- Automate sincrone
- Automate asincrone
- Identificarea automatelor
- Automate fara pierderi
  - Identificarea pierderilor
  - Reconstituirea secventei de intrare

INTRODUCERE

Definiţie

- Automatele – foarte utile in comunicatii
- De multe ori mesajele trimise trebuie criptate/ascunse
- Un mesaj criptat, depinde de *cheie*
- Exemplu “simplist”
  - Transmit mesajul “15”
  - Cum stiu care e defapt valoarea transmisa?
  - Poate fi 15, daca numarul e in baza 10;
  - Poate fi 21, daca numarul e in baza 16
- Automate liniare – genereaza mesajul + folosim o metoda artimetica pt a stabili “regulile numerelor”

INTRODUCERE

Definiţie

- Automatul liniar este o reţea cu un număr finit de intrări şi ieşiri, compusă din interconectarea a 3 componente de bază, fiecare componentă fiind liniară, adică răspunsul la o combinaţie liniară a intrărilor respectă factorul scalar şi principiul superpoziţiei
- Intrările sunt elemente ale câmpului finit Galois GF(p) = {0,1, …, p-1} şi operaţiile efectuate de componentele de bază asupra intrărilor satisfac regulile câmpului
- **Aplicaţii**: comunicaţii; comprimarea datelor

INTRODUCERE

Inel

- Un set I este inel dacă posedă două operaţii, **adunarea şi înmulţirea**, care sunt definite pentru orice perechi de elemente din R ($\forall$ a,b $\in$ R, **a+b** şi **a x b** $\in$ R) şi care satisfac următoarele proprietăţi:
  - R conţine un element unic 0
  - fiecare “a” are un element invers
  - asociativitate
  - distributivitate
  - comutativitate a+b = b+a
  - dacă şi a x b = b x a inelul este comutativ

INTRODUCERE

Exemplu

- Inel modulo 4
  - Adunarea modulo 4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

  - Înmulţirea modulo 4

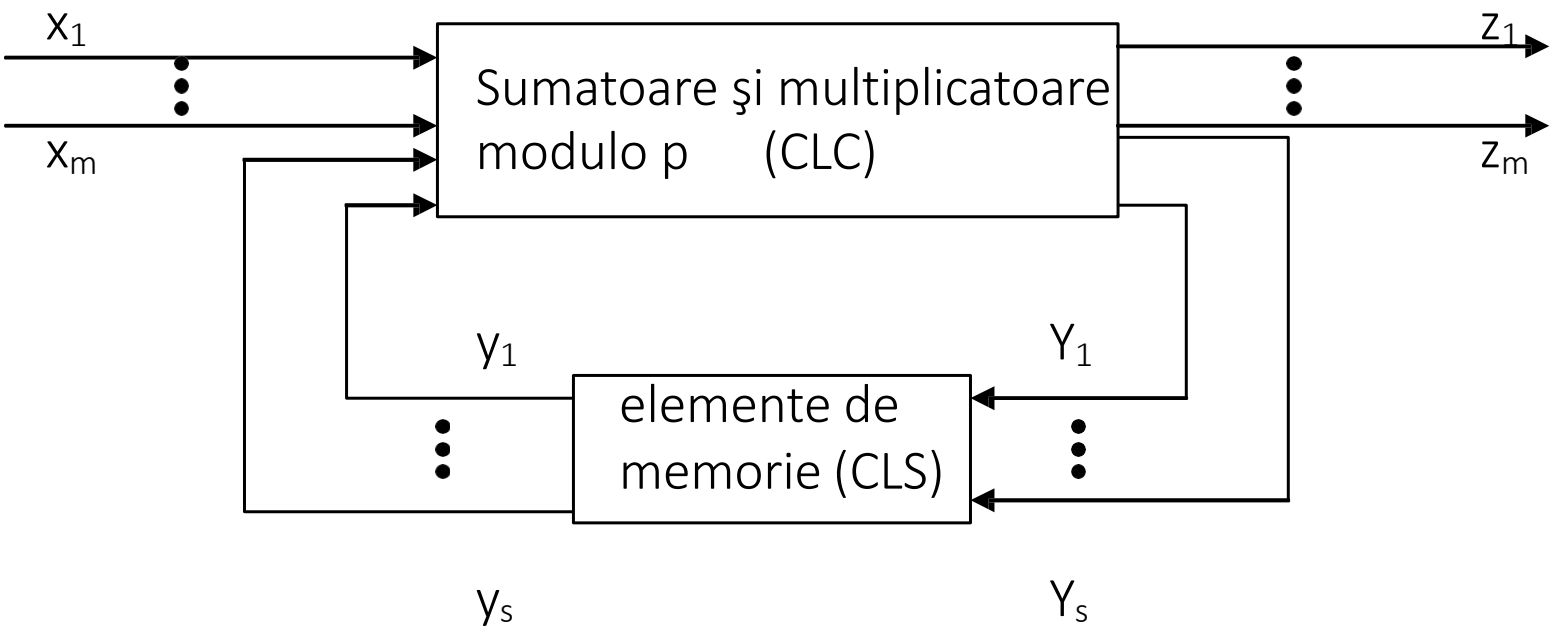
x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

INTRODUCERE

Câmp

- Un set C este **câmp** dacă este inel comutativ şi mai satisface următoarele proprietăţi:
  - există un element neutru, 1, diferit de zero, astfel încât **a x 1 = 1 x a = a**
  - pentru $\forall$ a $\neq$ 0 există un element invers $\mathbf{a^{-1}}$ sau **1/a** astfel încât $\mathbf{a \times a^{-1} = 1}$
- **Câmp finit** – are un număr finit de elemente
  - Observaţie: Inelul modulo 4 definit anterior nu este câmp fiindcă nu are element invers la înmulţire (elementul 2 nu are invers pentru ca a x 2 = 1; de asemenea, 2 x a = 2 are două valori posibile pentru a, a=1 şi a=3)
- Dacă "p" este prim, inelul întregilor "mod p" formează un câmp finit şi se numeşte câmp Galois GF(p) (Exemplu: GF(3) = {0,1,2})

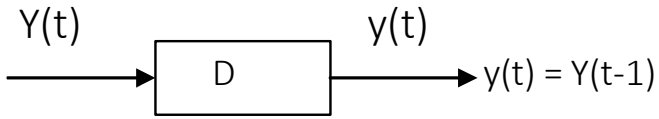
SCHEMA BLOC


x_1
x_m
Sumatoare şi multiplicatoare modulo p (CLC)
z_1
z_m
y_1
Y_1
elemente de memorie (CLS)
y_s
Y_s

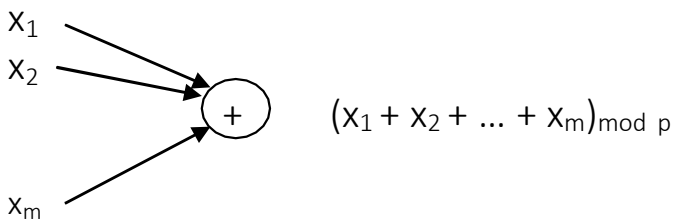
COMPONENTE

Componente de bază

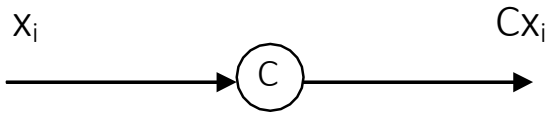
- 1. Element de memorie



- 2. Sumator mod p



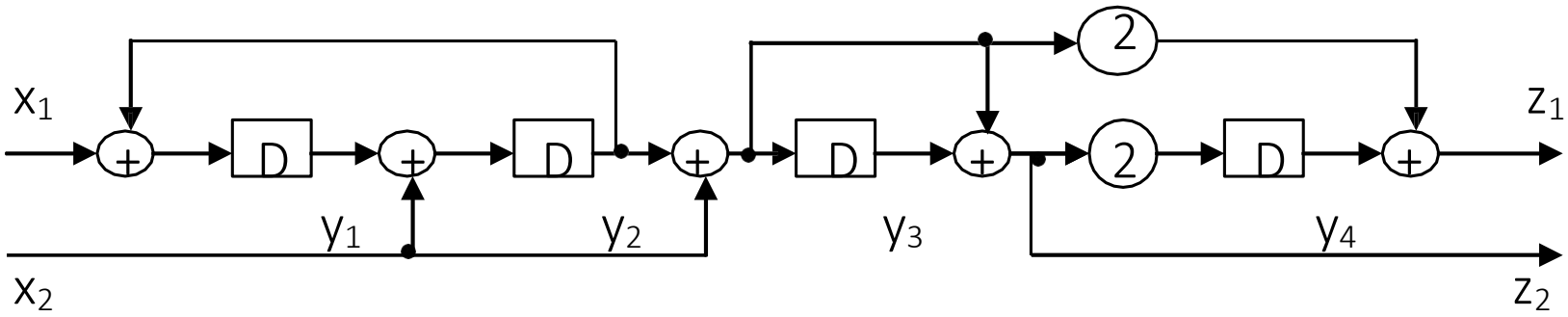
- 3. Multiplicator scalar mod p



  - C este un scalar care aparţine GF(p)

COMPONENTE

- Fiecare componentă de bază este liniară
- Un automat liniar are în fiecare buclă de reacţie cel puţin un element de memorie (care produce o întârziere egală cu intervalul de timp dintre două impulsuri de ceas)
- Numărul de elemente de memorie prezente determină dimensiunea **k** a automatului
- **Exemplu**: automat liniar mod 3, dimensiunea k=4

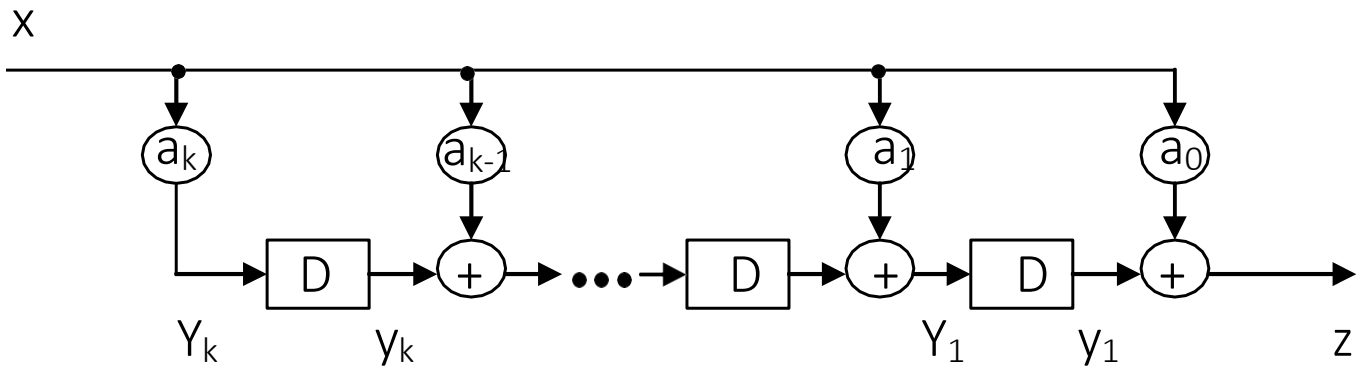


AUTOMATE LINIARE INERTE

- În starea inițială au în elementele de memorie valoarea 0
- Se folosesc la:
  - codificarea şi decodificarea informaţiei
  - în aplicaţii care necesită transformări de secvenţă

REGISTRE DE DEPLASARE CU LEGĂTURI DIRECTE

Schema bloc



- Dimensiunea = k
- Ieşirea z este descrisă ca un polinom în D:

  $z = a_0x + a_1Dx + a_2D^2x + \ldots + a_kD^kx$
- D^i este un operator de întârziere – face operaţia de întârziere i
- **Exemplu**: $z = D^2x$
  - pt. $\forall\ t \geq 2$ avem $z(t) = x(t-2)$.

REGISTRE DE DEPLASARE CU LEGĂTURI DIRECTE

Schema bloc

- $D^0 = 1$ operaţia de identitate
- D^1 produce o întârziere cu un impuls de ceas
- D^k produce o întârziere cu k impulsuri de ceas
- Ecuaţia pentru **z** este valabilă numai pentru automate inerte, când:
  - $y1(0) = y2(0) = \ldots = yk(0) = 0$
- Ieşirea se poate scrie:

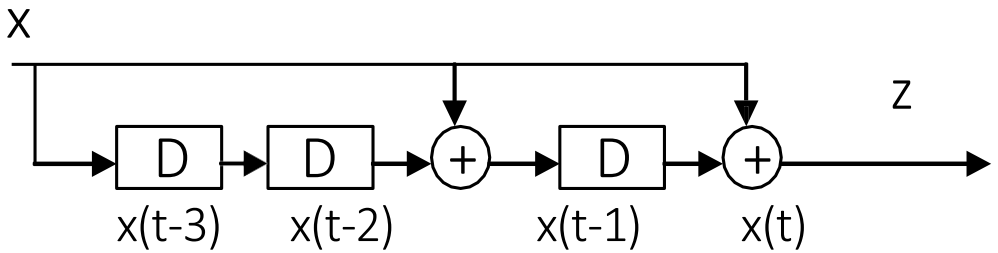
$$z = (a_0 + a_1 D + a_2 D^2 + \ldots + a_k D^k)x$$

- Funcţia de transfer a automatului este:

$$T(D) = z/x = a_0 + a_1 D + a_2 D^2 + \ldots + a_k D^k$$

REGISTRE DE DEPLASARE CU LEGĂTURI DIRECTE

Exemplu

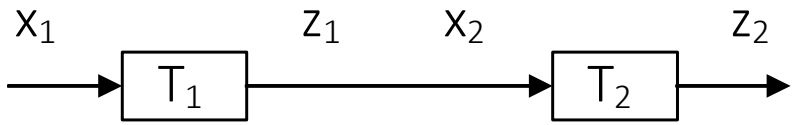


- Câmpul pe care este definit automatul: GF(2)
- Dimensiunea: k = 3
- Scalarul folosit la multiplicare este 1 sau 0 după cum există sau nu există legătură la sumatoarele automatului
- Ieşirea: $z(t) = x(t) + x(t-1) + x(t-3)$
- Polinomul corespunzător: $z = x + Dx + D^3x$
- Funcţia de transfer: $T = z/x = 1 + D + D^3$

REGISTRE DE DEPLASARE CU LEGĂTURI DIRECTE

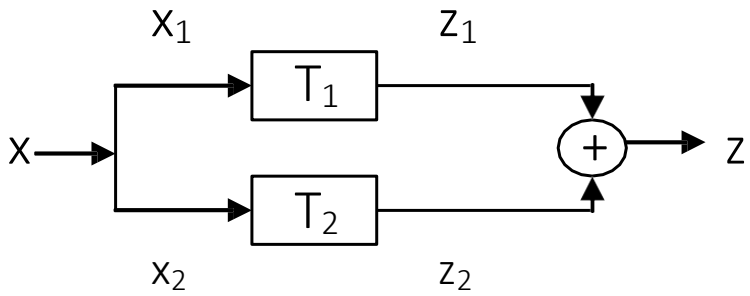
Tipuri de legături

- 1. Conectare serie



$T = z_2/x_1 = z_1/x_1 \,.\, z_2/x_2 = T_1T_2$
$(z_1 = x_2)$

- 2. Conectare paralelă



$T = z/x = (z_1 + z_2)/x = T_1 + T_2$

- Conectarea automatelor poate reduce numărul elementelor de memorie

REGISTRE DE DEPLASARE CU LEGĂTURI DIRECTE

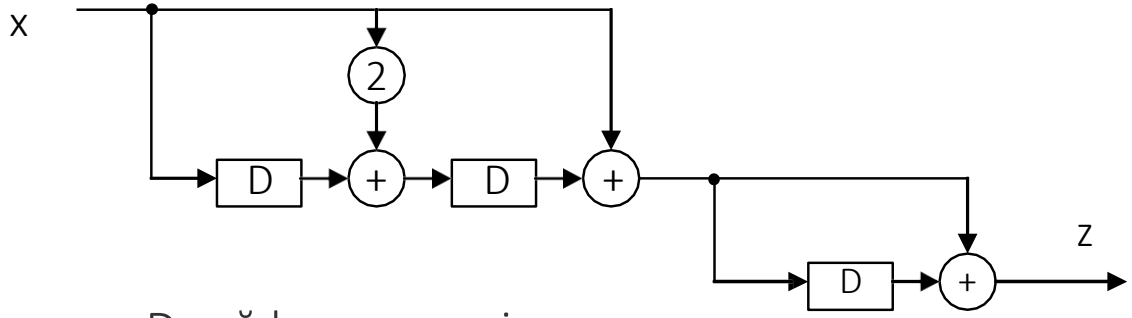
Tipuri de legături

- Exemplu
  - $T_1 = D^2 + 2D + 1$ funcţie de transfer pe GF(3) ={0,1,2}
  - $T_2 = D + 1$ funcţie de transfer pe GF(2) = {0,1}
  - Funcţiile de transfer pentru legarea serie şi paralel:
    - $Ts = T_1T_2 = (D^2 + 2D + 1)(D + 1) = D^3 + 2D^2 + D + D^2 + 2D + 1 =$
      $= D^3 + 3D^2 + 3D + 1 = D^3 + 1$
      - Observaţie: în GF(3) nu există factorul scalar 3!
    - $Tp = T_1 + T_2 = D^2 + 2D + 1 + D + 1 = D^2 + 3D + 2 = D^2 + 2$
    - funcţiile de transfer sunt pe GF(3) → în urma conectării se poate ajunge la un rezultat care poate fi interpretat pe alt GF - în cazul nostru GF(2)

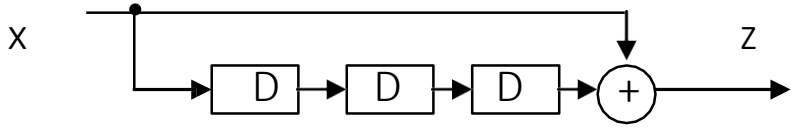
REGISTRE DE DEPLASARE CU LEGĂTURI DIRECTE

Tipuri de legături

- Exemplu
  - $T_1 = D^2 + 2D + 1$ funcţie de transfer pe GF(3) ={0,1,2}
  - $T_2 = D + 1$ funcţie de transfer pe GF(2) = {0,1}
  - Schemele pentru legarea serie
    - Iniţial



    - După legarea serie



REGISTRE DE DEPLASARE CU LEGĂTURI DIRECTE

Răspunsul la impuls

- Definiţie: Răspunsul la impuls h al unui automat liniar inert este răspunsul la o secvenţă de intrare de tipul 100.....0
- Exemplu 1: Răspunsul la impuls a unui **registru cu legături directe** (înainte): $a_0a_1a_2...a_k00...0$
  - După cel mult k+1 unităţi de timp ieşirea registrului k dimensional va fi o secvenţă de 0
- Exemplu 2: Automat inert cu $T = 1 + D + D^3$
  - Răspuns la impuls 110100...0
  - Răspuns la o secvenţă de intrare: 1001 – suprapunerea efectelor

```
1101000000...
 000000000...
  00000000...
   1101000...
-------------------------------
1100101000...0      Secvenţa de ieşire
```

REGISTRE DE DEPLASARE CU LEGĂTURI DIRECTE

Secvenţa nulă

- Starea iniţială a unui automat inert este 00000…0
- Dacă se aplică o secvenţă de intrare 000…0 se obţine ieşirea 000… 0
- Există posibilitatea să se găsească o secvenţă de intrare diferită de 0 care să producă o secvenţă de ieşire 0. O astfel de secvenţă de intrare se numeşte **secvenţă nulă** şi se notează X_0.
- $z = TX_0 = 000…0$
- Orice combinaţie de secvenţe nule este o secvenţă nulă

REGISTRE DE DEPLASARE CU LEGĂTURI DIRECTE

Secvenţa nulă

- Exemplu 1: Se dă automatul inert cu funcţia de transfer: $T = 1 + D + D^3$ pe GF(2)
- Relaţia pe baza căreia se obţine secvenţa nulă se determină astfel:
  - $0 = (1 + D + D^3)X_0 = X_0 + DX_0 + D^3X_0$ $\quad | + X_0$ în mod 2
  - $X_0 = X_0 + X_0 + DX_0 + D^3X_0$ deci $\mathbf{X_0 = DX_0 + D^3X_0}$
  - Pe baza ecuaţiei obţinute, elementul prezent al lui X_0 este găsit prin suma modulo 2 (SAU EXCLUSIV) între primul şi al treilea simbol al lui X_0
- Secvenţa nulă X_0 este determinată prin alegerea unei secvenţe arbitrare de lungime k (dimensiunea automatului)

REGISTRE DE DEPLASARE CU LEGĂTURI DIRECTE

Secvenţa nulă

- Exemplu 1
  - Luăm secvenţa iniţială arbitrară 001 (numărul elementelor de memorie k = 3)
  - Pe baza relaţiei se obţine $X_0 = (001)1101001$
  - După 7 biţi secvenţa nulă se repetă
- Numărul de elemente după care secvenţa nulă se repetă este dat de $p^k - 1$ (p provine de la GF(p), k este dimensiunea automatului)
  - În exemplu avem $2^3 - 1 = 7$, unde p = 2 provine de la GF(2), iar k = 3 este dimensiunea automatului, adică numărul elementelor de memorie

REGISTRE DE DEPLASARE CU LEGĂTURI DIRECTE

Secvenţa nulă

- Exemplu 2: Se dă automatul inert cu funcţia de transfer: $T = 1 + 2D^2 + D^3$ peGF(3)
- Relaţia pe baza căreia se obţine secvenţa nulă se determină astfel:
  - $0 = X_0 + 2D^2X_0 + D^3X_0$ $\quad | + 2X_0$ în mod 3
  - $2X_0 = 2D^2X_0 + D^3X_0$ $\quad | \cdot 2$ în mod 3
  - $\mathbf{X_0 = D^2X_0 + 2D^3X_0}$
- Alegem secvenţa iniţială arbitrară 111 şi obţinem X_0 = (111)00202122102220010121120111
- Repetiţia are loc după $3^3 - 1 = 26$ pentru că suntem pe GF(3) şi dimensiunea automatului este 3

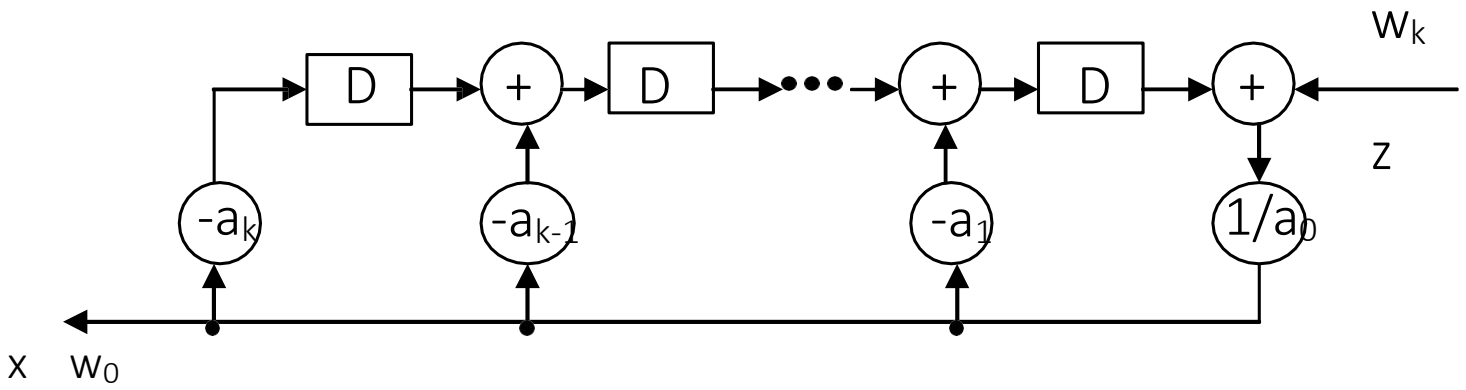
AUTOMATE INVERSE

Consideraţii generale

- Registrele de deplasare cu legături înainte se folosesc de obicei pentru codificarea informaţiei
- Determinarea unui automat invers, folosit ca şi decodor → dacă există, să se construiască!
- Un polinom T(D) care satisface ecuaţia z = Tx are un polinom invers 1/T(D) dacă există o reţea care să realizeze funcţia $z = (1/T)x = T^{-1}x$
- Considerăm acele automate inverse care realizează operaţia de decodare fără nici o întârziere (simultan)

AUTOMATE INVERSE

Schema automatului invers

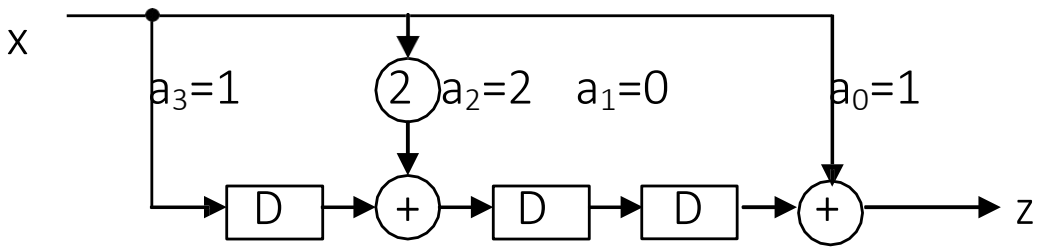


- Dacă aplicăm automatului invers răspunsul la impuls al registrului direct ($a_0a_1...a_k00...0$) se obţine la ieşire 100...00
- Dacă automatul invers este liniar şi inert el decodifică orice mesaj sosit de la automatul original: scalarii negativi sunt întregi pozitivi deoarece (-a)mod p = (p-a)mod p
- Un automat liniar inert descris de un polinom T are un automat invers descris de T^{-1}, care decodifică fără întârziere, dacă şi numai dacă T conţine un termen constant diferit de 0, care e prim faţă de mod p (automatul invers este realizabil numai dacă a_0 este diferit de 0)

AUTOMATE INVERSE

Exemplu

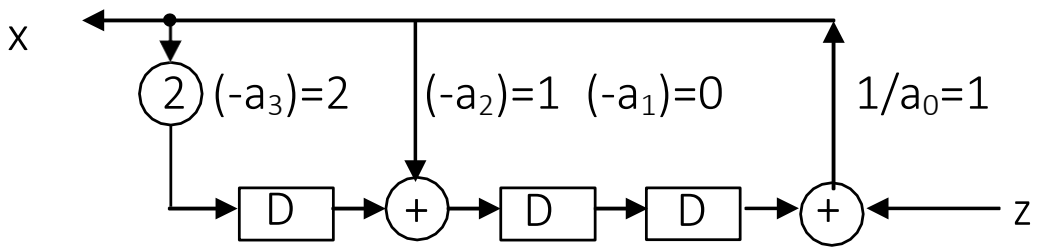
- Avem automatul direct cu funcţia de transfer:
  - $T = 1 + 2D^2 + D^3$ peGF(3)
  - Operaţiile sunt modulo 3
  - Coeficienţii sunt: $a_0 = 1$; $a_1 = 0$; $a_2 = 2$ şi $a_3 = 1$
- Schema automatului direct este:



AUTOMATE INVERSE

Exemplu

- Automatul invers are funcţia de transfer 1/T
  - $T^{-1} = \quad 1/(1 + 2D^2 + D^3)$
- Calculul coeficienţilor pentru automatul invers:
  - $1/a_0 = 1$; $(-a_1) = 3-0 = 0$; $(-a_2) = 3-2 = 1$; $(-a_3) = 3-1 = 2$
- Schema automatului invers este:



AUTOMATE NON-INERTE

Generalităţi

- Automatele liniare non-inerte au elementele de memorie cu condiţiile iniţiale diferite de 0
- Inversul unui automat liniar inert poate să nu fie inert, adică răspunsul la o secvenţă de intrări 0 nu duce necesar la secvenţe de ieşiri 0
- Poate exista o secvenţă nulă X_0 ai cărei biţi de start sunt determinaţi de starea iniţială a automatului invers. Atunci funcţia de transfer a automatului invers este $T^{-1} = x/z$ sau $z = Tx = 0$, pentru că intrarea z a automatului invers trebuie să fie o secvenţă de 0. În mod evident soluţia ecuaţiei este secvenţa nulă X_0.

AUTOMATE NON-INERTE

Generalităţi

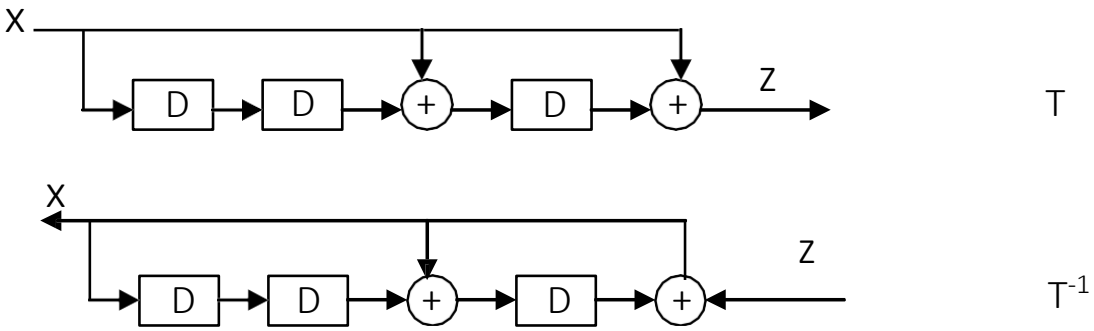
- Considerăm automatele liniare direct şi invers, primul cu funcţia de transfer T şi al doilea cu funcţia de transfer T^{-1}
  - Presupunem că se aplică intrări de 0 şi la T şi la T^{-1}
  - Dacă cele două automate sunt inerte, ieşirile vor fi 0
  - Dacă automatele nu sunt inerte, ieşirile respective nu vor fi 0, dar depind de starea iniţială a automatelor
  - Dacă automatul direct conţine reacţii directe, răspunsul la secvenţe de intrare 0 poate să nu fie iniţial 0, în funcţie de starea iniţială
  - În general, pentru automatul direct k dimensional, la secvenţe de intrare 0, după k+1 perioade de timp, ieşirea va fi 0
  - În cazul în care registrul nu este inert şi conţine căi inverse T^{-1}, răspunsul la secvenţe de intrare 0 nu e necesar să fie 0

AUTOMATE NON-INERTE

Comportarea autonomă

- Comportarea unui automat liniar non-inert a cărui secvenţă de intrare este 0 este o comportare autonomă şi poate fi descrisă cu ajutorul unei diagrame de stări a automatului respectiv
- Exemplu
  - Avem automatele direct şi invers cu funcţiile de transfer:

$T = 1 + D + D^3$ şi $T^{-1} = 1/(1 + D + D^3)$ pe GF(2)

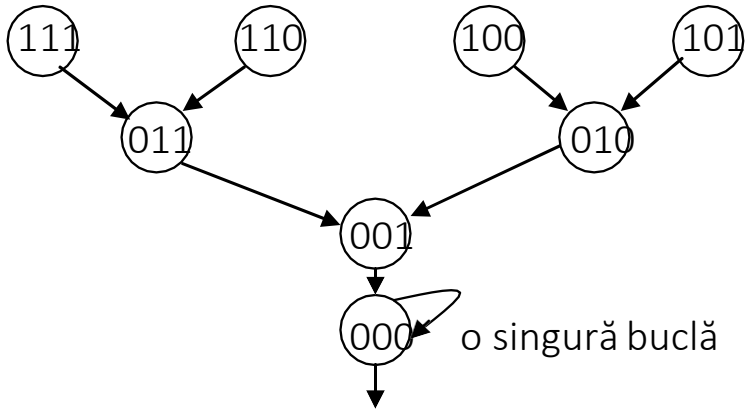


AUTOMATE NON-INERTE

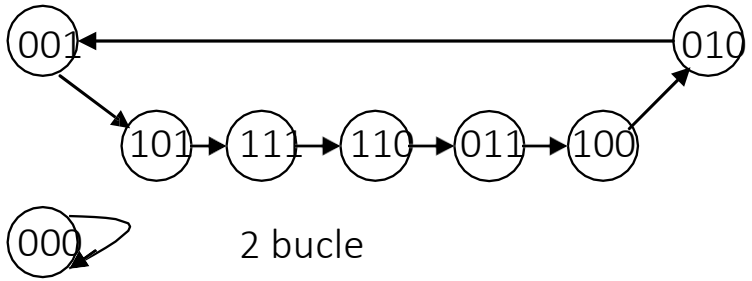
Comportarea autonomă

- Exemplu
  - Avem automatele direct şi invers cu funcţiile de transfer:

$T = 1 + D + D^3$ şi $T^{-1} = 1/(1 + D + D^3)$ pe GF(2)



T



T^{-1}

AUTOMATE NON-INERTE

Comportarea autonomă

- Exemplu
  - Evoluţia se face pe impulsul de ceas şi se presupune că automatul este determinist, adică este permisă o singură tranziţie în fiecare stare

Stare actuală T	Stare următoare T	Stare actuală T^{-1}	Stare următoare T^{-1}	x
000	000	000	000	0
001	000	001	101	1
010	001	010	001	0
011	001	011	100	1
100	010	100	010	0
101	010	101	111	1
110	011	110	011	0
111	011	111	110	1

(reg. de deplasare)

AUTOMATE LINIARE INERTE ŞI FUNCŢII DE TRANSFER RAŢIONALE

Funcţia de transfer raţională

- La automatele liniare avem ieşirea ca funcţie de valorile de intrare prezente sau trecute
- Studiem situaţia în care ieşirea depinde şi de un număr finit de ieşiri trecute → se defineşte o funcţie de transfer polinomială care este raţională: T = P(D)/Q(D)

AUTOMATE LINIARE INERTE ŞI FUNCŢII DE TRANSFER RAŢIONALE

Funcţia de transfer raţională pe GF(2)

- Funcţia de transfer raţională pe GF(2) în cazul general:
- $T = P(D) / Q(D) = z/x =$

  $= (a_0 + a_1D + \ldots + a_kD^k) / (1 + b_1D + \ldots + b_kD^k)$ pe GF(2)
- **Observaţie**: Q(D) trebuie să conţină 1 pentru a fi realizabilă!
- **Exemplu:**
  - Considerăm un automat liniar inert a cărui ieşire z este suma modulo 2 a intrării prezente şi a intrărilor anterioare prima, a doua şi a patra, precum şi a ieşirilor anterioare prima şi a treia
  - $z = x + Dx + D^2x + D^4x + Dz + D^3z$ pe GF(2)
  - Funcţia de transfer a unui astfel de automat va fi:
  - $z(1 + D + D^3) = x(1 + D + D^2 + D^4)$
  - $T = z/x = (1 + D + D^2 + D^4) / (1 + D + D^3)$

AUTOMATE LINIARE INERTE ŞI FUNCŢII DE TRANSFER RAŢIONALE

Funcţia de transfer raţională

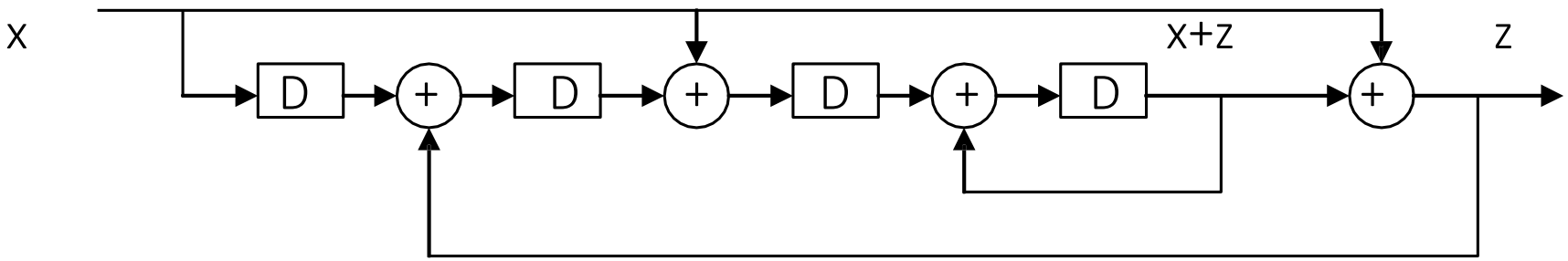
- **Exemplu:**
  - Construim automatul pe baza funcţiei sale de transfer
  - Automatul ar trebui să aibă 7 elemente de întârziere
  - Minimizăm la un automat cu maximum (grad P, grad Q) celule de memorie D şi obţinem 4 celule de tip D
  - Rescriem ecuaţia:
  - $z + x = x + Dx + D^2x + D^4x + Dz + D^3z + x$

    $= Dx + D^2x + D^4x + Dz + D^3z$
  - **$z + x = D\{(x + z) + D[x + D(z + Dx)]\}$**

AUTOMATE LINIARE INERTE ŞI FUNCŢII DE TRANSFER RAŢIONALE

Funcţia de transfer raţională

- **Exemplu:**
  - Realizarea este următoarea (desenăm de la sfârşit spre început):



  - cu ieşirea z = (x + z) + x

AUTOMATE LINIARE INERTE ŞI FUNCŢII DE TRANSFER RAŢIONALE

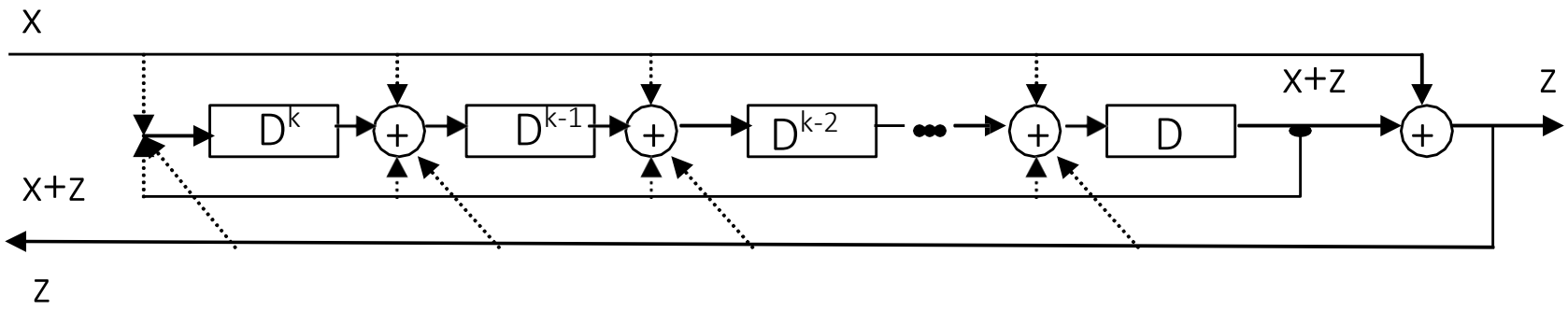
Funcţia de transfer raţională

- **Exemplu:**
- Pentru $T^{-1} = x/z = (1 + D + D^3) / (1 + D + D^2 + D^4)$ se obţine schema schimbând sensul intrărilor şi ieşirilor
- Observaţie: Pentru funcţia de transfer pe GF(2), în cazul general se poate determina o expresie pentru $x + z$
- $x + z = D[(a_1x + b_1z) + D[... + D(a_kx + b_kz)]$ care se poate realiza alternând elementele de întârziere cu sumatoare mod 2

AUTOMATE LINIARE INERTE ŞI FUNCŢII DE TRANSFER RAŢIONALE

Funcţia de transfer raţională

- **Exemplu – cazul general:**



- Există k elemente de întârziere şi cel mult k sumatoare mod 2
- Una dintre intrările în sumatoarele mod 2 este ieşirea elementului de întârziere anterior
- Cealaltă intrare este x sau z sau x + z, în funcţie de prezenţa coeficienţilor a_i şi b_i la numărător, numitor sau şi la numărător şi la numitor
- Dacă pentru un sumator nu există ca a doua intrare coeficienţi a_i şi b_i, sumatorul dispare
- Pentru sumatorul cel mai din dreapta, a doua intrare este întotdeauna x
- D_{i-1} lipseşte dacă $a_i = b_i = 0$ şi neexistând o intrare,

sumatorul i poate fi şters

CONCLUZII

Automate liniare

- Aritmetica in campuri finite
- Automate Interte
  - Automate Directe
  - Automate Inverse
- Automate non-inerte
- Functii de transfer rationale