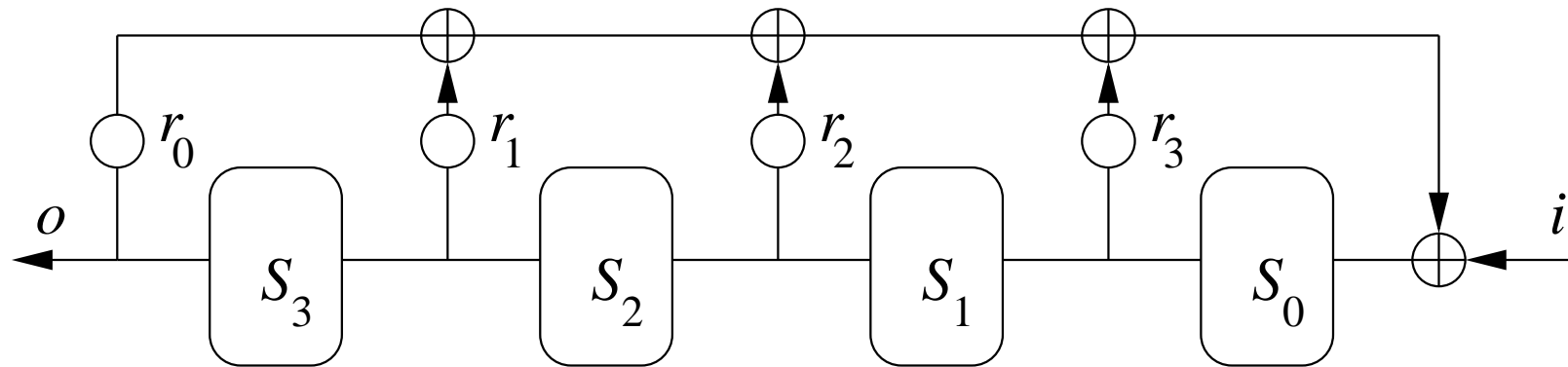


Lineaarsed nihkeregistrid

Ahto Buldas

Lineaarne Nihkeregister (LNR)



LNR on *Moore'i automaat*: paar $\mathcal{A} = (\delta, \lambda)$, kus:

- δ on *olekufunktsioon*: seab olekule $S \in \mathcal{S}$ ja sisendile i vastavusse uue oleku $S' = \delta(S, i)$,
- λ on *väljundfunktsioon*: seab olekule S vastavusse väljundi $o = \lambda(S)$.

Registri olek: $S = S_3S_2S_1S_0$, kus $S_j \in \{0, 1\}$. Sisend/väljundtähestik: $\{0, 1\}$.

Lineaarset nihkeregistrit kirjeldavad võrrandid

$$\begin{aligned} S'_0 &= (r_3 S_0 + r_2 S_1 + r_1 S_2 + r_0 S_3 + i) \pmod{2} \\ S'_1 &= S_0, \quad S'_2 = S_1, \quad S'_3 = S_2, \quad o = S_3, \end{aligned}$$

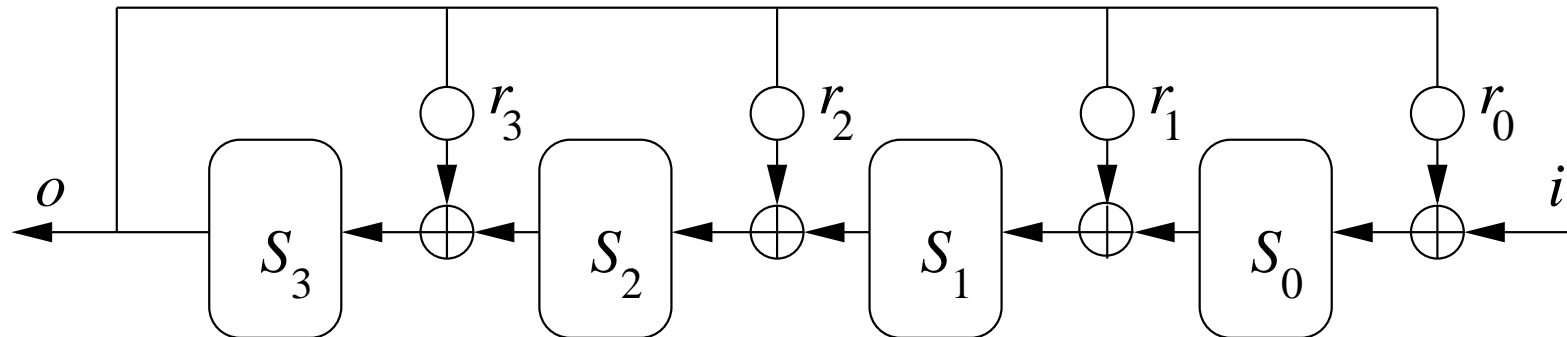
kus S'_j tähistavad olekumuutujate uusi väärtusi peale sisendile i reageerimist. Neid võrrandeid võib üles tähendada ka maatrikskujul järgmiselt:

$$\begin{aligned} S' &= A \cdot S + \mathcal{I} \cdot i \\ o &= \mathcal{O} \cdot S, \end{aligned} \tag{1}$$

kus $\mathcal{O} = \begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix}$,

$$S' = \begin{bmatrix} S'_0 \\ S'_1 \\ S'_2 \\ S'_3 \end{bmatrix}, \quad A = \begin{bmatrix} r_3 & r_2 & r_1 & r_0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad S = \begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix} \text{ ja } \mathcal{I} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Teist liiki nihkeregister



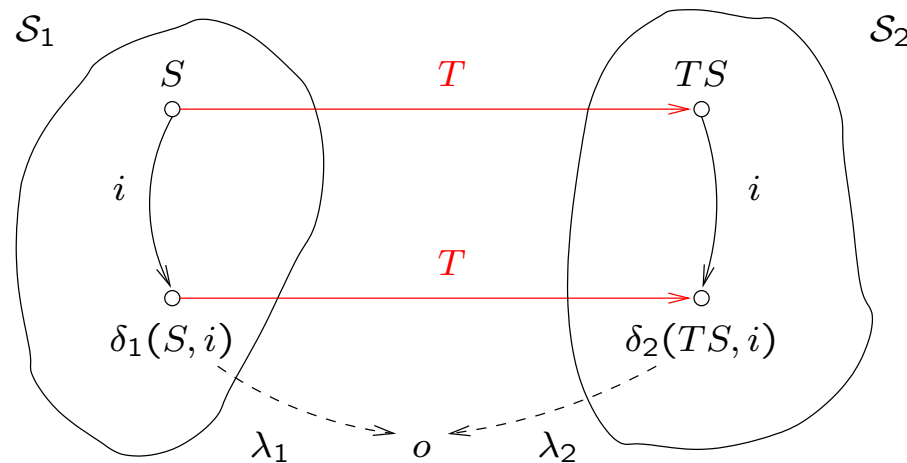
$$\begin{aligned} S'_* &= A_* \cdot S_* + \mathcal{I} \cdot i \\ o &= \mathcal{O} \cdot S_*, \end{aligned} \quad (2)$$

kus \mathcal{I} ja \mathcal{O} on samad, mis võrrandis (1), ja

$$A_* = \begin{bmatrix} 0 & 0 & 0 & r_0 \\ 1 & 0 & 0 & r_1 \\ 0 & 1 & 0 & r_2 \\ 0 & 0 & 1 & r_3 \end{bmatrix}.$$

Automaatide ekvivalentsus (bisimilaarsus)

Automaate $\mathcal{A}_1 = (\delta_1, \lambda_1)$ olekute hulgaga \mathcal{S}_1 ja $\mathcal{A}_2 = (\delta_2, \lambda_2)$ olekute hulgaga \mathcal{S}_2 nimetame **ekvivalentseteks** (ka **bisimilaarseteks**), kui leidub kujutus $T: \mathcal{S}_1 \rightarrow \mathcal{S}_2$, nii et $T\delta_1(S, i) = \delta_2(TS, i)$ ja $\lambda_1(S) = \lambda_2(TS)$ mis tahes oleku $S \in \mathcal{S}_1$ ja sisendi i korral.



Järeldus. Teatud algolekutest annavad automaadid samadele sisendjadadele samad väljundjadad: **automaadid on sisendi/väljundi põhjal eristamatud.**

Tavalise ja teist järku nihkeregistrite ekvivalentsus

Automaatide ekvivalentsus tuleneb asjaolust, et leidub regulaarmatriks T , nii et $TA = A_*T$, $T\mathcal{I} = \mathcal{I}$ ja $\mathcal{O}T = \mathcal{O}$. Tõepoolest, selliseks matriksiks sobib

$$T = \begin{bmatrix} 1 & r_3 & r_2 & r_1 \\ 0 & 1 & r_3 & r_2 \\ 0 & 0 & 1 & r_3 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

sest võttes $S_* = TS$, saame võrrandit (1) teisendades, et

$$\begin{aligned} S'_* &= TS' = TA \cdot S + T\mathcal{I} \cdot i = A_* \cdot TS + \mathcal{I} \cdot i = A_* \cdot S_* + \mathcal{I} \cdot i \\ o &= \mathcal{O} \cdot S = \mathcal{O}T \cdot S = \mathcal{O} \cdot TS = \mathcal{O} \cdot S_*, \end{aligned}$$

mis ühtib võrrandiga (2) ja automaadid on seega ekvivalentsed.

Nihkeregistri karakteristlik polünoom

Vaatleme polünoome üle arvuvalla \mathbb{Z}_2 , st kehtib $x + x \equiv 0$.

Maatriksite A ja A_* karakteristlikku polünoomi

$$\det(A + xI) = \det(A_* + xI) = f(x) = x^4 + r_3x^3 + r_2x^2 + r_1x + r_0$$

nimetatakse *nihkeregistri karakteristlikuks polünoomiks*.

NB! Maatriksite A ja A_ sarnasuse tõttu on nende karakteristlikud polünoomid võrdsed.*

Polünoomide jagamine

Teoreem. Olgu $f(x)$ ja $g(x)$ polünoomid ja $\deg f(x) \leq \deg g(x)$. Leiduvad üheselt määratud polünoomid $d(x)$ ja $s(x)$, kus $\deg s(x) < \deg f(x)$, nii et

$$g(x) = d(x)f(x) + s(x) .$$

Polünoomi $d(x)$ võib täisarvude jagamise eeskujul nimetada polünoomide jagatise $g(x)/f(x)$ **täisosaks** ja polünoomi $s(x)$ vastavalt **jäägiks**.

Polünoomi $g(x)$ polünoomiga $f(x)$ jagamisel tekkiva jäägi leidmist tähistatakse $s(x) \equiv g(x) \pmod{f(x)}$.

Sisend- ja väljundjadad

Olgu $S^0 = S_0S_1S_2S_3$ mingi algolek ja olgu $i_1i_2 \dots i_n$ mingi sisendjada ja $o_1o_2 \dots o_n$ sellele jadale vastav väljundjada ja $S^0S^1S^2 \dots S^n$ olgu vastav olekute jada, st

$$\begin{aligned} S^0 &= A_* \cdot S + \mathcal{I} \cdot i_0, & o_0 &= \mathcal{O} \cdot S^0 \\ S^1 &= A_* \cdot S^0 + \mathcal{I} \cdot i_1, & o_1 &= \mathcal{O} \cdot S^1 \\ &\dots \end{aligned}$$

Olgu $S^k = S_0^k S_1^k S_2^k S_3^k$, kus $k = 0, \dots, n$. Võtame kasutusele järgmised polünoomid

$$\begin{aligned} i^0(x) &= 0 = o^0(x) \\ i^k(x) &= i_1x^{k-1} + i_2x^{k-2} + \dots + i_{k-1}x + i_k, & k &= 1, \dots, n \\ o^k(x) &= o_1x^{k-1} + o_2x^{k-2} + \dots + o_{k-1}x + o_k, & k &= 1, \dots, n \\ s^k(x) &= S_3^kx^3 + S_2^kx^2 + S_1^kx + S_0^k, & k &= 0, \dots, n. \end{aligned}$$

Seos sisend-, väljund- ja olekupolünoomi vahel

$$s^n(x) = x^n \cdot s^0(x) + o^n(x) \cdot f(x) + i^n(x). \quad (3)$$

On lihtne veenduda, et võrrand (3) peab paika $k = 0$ korral. Oletame, et võrrand kehtib ka mingi $n = k > 0$ korral. Induktsioonisammu tõestamiseks märgime esmalt, et $i^{k+1}(x) = x \cdot i^k(x) + i_{k+1}$ ja samuti $o^{k+1}(x) = x \cdot o^k(x) + o_{k+1}$. Kasutades teist liiki nihkeregistri kirjeldust, saame et

$$\begin{aligned} s^{k+1}(x) &= S_3^{k+1}x^3 + S_2^{k+1}x^2 + S_1^{k+1}x + S_0^{k+1} \\ &= (S_2^k + r_3 \cdot S_3^k)x^3 + (S_1^k + r_2 \cdot S_3^k)x^2 + (S_0^k + r_1 \cdot S_3^k)x^1 \\ &\quad + r_0 \cdot S_3^k + i_{k+1} \\ &= x \cdot (S_2^kx^2 + S_1^kx + S_0^k) + S_3^k(r_3x^3 + r_2x^2 + r_1x + r_0) + i_{k+1} \\ &= x(S_3^kx^3 + S_2^kx^2 + S_1^kx + S_0^k) + \\ &\quad + S_3^k(x^4 + r_3x^3 + r_2x^2 + r_1x + r_0) + i_{k+1} \\ &= x \cdot s^k(x) + o_{k+1} \cdot f(x) + i_{k+1} \end{aligned}$$

Teist liiki nihkeregister jagab polünoome!

Võrrandi (3) kehtivusest $n = k$ korral tuleneb

$$\begin{aligned} s^{k+1}(x) &= x \cdot [i^k(x) + x^k \cdot s^0(x) + o^k(x) \cdot f(x)] + o_{k+1} \cdot f(x) + i_{k+1} \\ &= x^{k+1} \cdot s^0(x) + [x \cdot o^k(x) + o_{k+1}] \cdot f(x) + x \cdot i^k(x) + i_{k+1} \\ &= x^{k+1} \cdot s^0(x) + o^{k+1} \cdot f(x) + i^{k+1}(x). \end{aligned}$$

Järeldus: Seos (3) kehtib iga $n > 0$ korral. Kui algolek $s^0(x) = 0$, siis **teist liiki nihkeregister teostab polünoomi $i^n(x)$ jagamist polünoomiga $f(x)$** , kusjuures:

- jagatise täisosa esitab polünoom $o^n(x)$ ja
- jääki polünoom $s^n(x)$.

Maksimaalse perioodi probleem

Oleme taandanud lineaarse nihkeregistri uurimise täielikult algebraliseks probleemiks: Tuleb uurida polünoome kordajatega hulgast \mathbb{Z}_2 .

Kui ka sisendsignaal puudub, st kui $i^n(x) = 0$, siis registri (nö. tühikäigul) tööd (algolekust $s^0(x)$) iseloomustab kongruents

$$s^n(x) \equiv x^n \cdot s^0(x) \pmod{f(x)}. \quad (4)$$

Küsimus: Millise $f(x)$ korral annab register maksimaalse perioodiga väljundjada?

Vastust otsides jõuame üldalgebra küsimusteni!

Polünoomi juured arvuvaldades

Arvuvald = hulk, mille elemente saab liita ja korrutada ja kus kehtivad tavalistele (reaal-)arvudele iseloomulikud algebralised omadused. Tavaliselt eeldame, et arvuvald on *korpus*.

Def. Polünoomi f *juureks* arvuvallas R nimetatakse suurust $\vartheta \in R$, mille korral $f(\vartheta) = 0$.

Näiteks arv 1 on polünoomi $f(x) = x^2 - 1$ juureks täisarvude hulgas \mathbb{Z} , sest $1^2 - 1 = 0$. Samuti võib öelda, et 1 on polünoomi $f(x) = x^2 + 1$ juureks arvuvallas \mathbb{Z}_2 , sest $1^2 + 1 = 1 + 1 = 2 \equiv 0 \pmod{2}$.

Polünoomil $x^2 + 1$ juurt reaalarvude vallas \mathbb{R} .

Arvuvalla (korpuse) laiendamine

Saab näidata, et kui polünoomil $f(x)$ puudub arvuvallas R juur, saab alati arvuvalla laiendada, nii et uus arvuvald juba sisaldab vähemalt ühte juurt.

Selleks defineerime ϑ kui uue suuruse, mille korral $f(\vartheta) = 0$ ja "lisame" selle arvuvalla R .

Selleks, et uus arvuvald oleks kinnine liitmise ja korrutamise suhtes, tuleb uude arvuvalla (mida tähistame $R[\vartheta]$) võtta kõik avaldised kujul

$$a_0 + a_1 \cdot \vartheta + a_2 \cdot \vartheta^2 + \dots + a_m \cdot \vartheta^m.$$

Teoreem minimaalpolünoomist

Teoreem. Olgu λ element arvuvalla R mingis laienduses ja $0 \neq m(x) \in R[x]$ olgu minimaalse astmega polünoom, mille korral $m(\lambda) = 0$. Sellist polünoomi nimetame (elemendi λ) *minimaalpolünoomiks*. Siis polünoom $g(x)$ jagub polünoomiga $m(x)$.

Tõestus. Et $\deg(m) \leq \deg(g)$, siis leiduvad polünoomid $g'(x), r(x) \in R[x]$ ($\deg r < \deg m$), nii et *

$$g(x) = g'(x) \cdot m(x) + r(x).$$

Järelikult $0 = g(\lambda) = g'(\lambda) \cdot m(\lambda) + r(\lambda) = r(\lambda)$, st $r(\lambda) = 0$, millest minimaalpolünoomi definitsiooni tõttu järeldub, et r on konstantne polünoom, mis võrdub samaselt nulliga. Järelikult $g(x) = g'(x) \cdot m(x)$. \square

*Siin on oluline eeldus, et R on korpus, st igal mittenullisel elemendil on pöördement. Näiteks, ei leidu polünoome $g'(x), r(x) \in \mathbb{Z}[x]$, nii et $x^2 + 1 = g'(x) \cdot (2x + 1) + r(x)$.

Järeldus: Bézout' teoreem

Lihtne on näha, et kui $\lambda \in R$, siis on λ minimaalpolünoomiks lineaarpolünoom $m(x) = x - \lambda$. Siit aga tuleneb järgmine teoreem:

Teoreem (Bézout'). Kui polünoomil $g(x) \in R[x]$ on juur $\lambda \in R$, siis $g(x) = g'(x) \cdot (x - \lambda)$ mingi polünoomi $g'(x) \in R[x]$ korral.

Taandumatus ja ühene esitus laiendis

Teoreem. Seosega $f(\vartheta) = 0$ defineeritud laiendi $R[\vartheta]$ iga elementi $\alpha \in R[\vartheta]$ saab esitada polünoomina $\alpha = r(\vartheta)$, kus $\deg r < \deg f$. Kui f on taandumatu, siis esitus $\alpha = r(\vartheta)$ on ühene.

Tõestus. Olgu $\alpha = a_0 + a_1\vartheta + \dots + a_m\vartheta^m$ ja $a(x) = a_0 + a_1x + \dots + a_nx^m$. Siis leiduvad polünoomid $a'(x), r(x) \in R[x]$ ($\deg r < \deg f$), nii et

$$a(x) = a'(x) \cdot f(x) + r(x).$$

Seega $\alpha = a(\vartheta) = a'(\vartheta) \cdot f(\vartheta) + r(\vartheta) = r(\vartheta)$. Sellega on esituse olemasolu tõestatud. Jääb üle tõestada esituse ühesus ...

Esituse ühesuse tõestus

Näitame, et r on ühene, juhul kui f on taandumatu.

Oletame, et leidub kaks polünoomi $r_1(x), r_2(x) \in R[x]$, nii et

$$\deg r_1, \deg r_2 < \deg f \quad \text{ja} \quad r_1(\vartheta) = \alpha = r_2(\vartheta) .$$

Siis $g(x) = r_1(x) - r_2(x) \in R[x]$ rahuldab seost $g(\vartheta) = 0$. Olgu $m(x) \neq 0$ minimaalse astmega polünoom, mille korral $m(\vartheta) = 0$.

Kui $g(x) \neq 0$, siis oleks $\deg m < \deg f$, mistõttu $f(x) = f'(x) \cdot m(x)$ ja $f(x)$ taandumatuse tõttu saame, et $m(x)$ on konstantne.

Seosest $m(\vartheta) = 0$ järeldub siis, et $m(x) = 0$, mis on vastuolu. Järelikult $r_1(x) = r_2(x)$. \square

Näide laiendusest

Näiteks reaalarvude valla laiendamisel polünoomi $x^2 + 1$ juurega ϑ , saame arvuvalla, mille elemendid on lineaaravaldised $z = a + b\vartheta$, kusjuures näiteks elementide $z_1 = a_1 + b_1\vartheta$ ja $z_2 = a_2 + b_2\vartheta$ korrutamisreegel

$$\begin{aligned} z_1 z_2 &= (a_1 + b_1\vartheta)(a_2 + b_2\vartheta) \\ &= a_1 a_2 + b_1 b_2 \vartheta^2 + (a_1 b_2 + a_2 b_1) \vartheta \\ &= a_1 a_2 + b_1 b_2 \underbrace{[\vartheta^2 + 1 - 1]}_0 + (a_1 b_2 + a_2 b_1) \vartheta \\ &= (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) \vartheta \end{aligned}$$

langeb kokku **kompleksarvude** korrutamise reegluga. Saabki näidata, et reaalarvude korpuse \mathbb{R} laiendamise tulemusena saame kompleksarvude korpuse \mathbb{C} .

Laiendi olemasolu

Oluline on tähele panna, et laiendi $R(\vartheta)$ struktuur (arvutusreeglid) on üheselt määratud polünoomiga $f(x)$, eeldusel et f on taandumatu. Seetõttu ei ole laiendi defineerimisel muud omadused olulised.

Üheks võimalikuks laiendiks on alati *jäägiklassiring* mooduli $f(x)$ järgi, kusjuures jääk x käitub nagu polünoomi f juur selles arvuvallas. See tuleneb triviaalsest seosest $f(x) \equiv 0 \pmod{f(x)}$.

Teoreem. Kui $f(x) \in R[x]$ on taandumatu polünoom, siis seosega $f(\vartheta) = 0$ defineeritud laiend $R[\vartheta]$ on isomorfne polünoomide jäägiklassiringiga mooduli $f(x)$ järgi, kusjuures suurusele $\vartheta \in R[\vartheta]$ vastab jääk x .

Tõestus

Et iga elementi $\alpha \in R[\vartheta]$ saab ühesel viisil esitada polünoomiaalse avaldisena $\alpha = r(\vartheta)$, kus $r(x) \in R[x]$ ja $\deg r < \deg f$, siis saab sobiliku isomorfismi φ defineerida seosega $\varphi[r(x)] = r(\vartheta)$. Seos on bijektiivne ja säilitab tehted, sest

$$\begin{aligned}\varphi[r_1(x) + r_2(x)] &= \varphi[(r_1 + r_2)(x)] = (r_1 + r_2)(\vartheta) = r_1(\vartheta) + r_2(\vartheta) \\ &= \varphi[r_1(x)] + \varphi[r_2(x)], \text{ ja}\end{aligned}$$

$$\begin{aligned}\varphi[r_1(x) \cdot r_2(x)] &= \varphi[(r_1 \cdot r_2)(x)] = (r_1 \cdot r_2)(\vartheta) = r_1(\vartheta) \cdot r_2(\vartheta) \\ &= \varphi[r_1(x)] \cdot \varphi[r_2(x)]\end{aligned}$$

□

Primitiivsed elemendid arvuvallas

Elementi $\lambda \in R$ nimetatakse lõpliku arvuvalla R ($|R| = M + 1$) **primitiivseks elemendiks** kui iga element $0 \neq r \in R$ on elemendi λ mingi M -st väiksem (või võrdne) aste, st kui $R \setminus \{0\} = \{\lambda, \lambda^2, \lambda^3, \dots, \lambda^M\}$.

Oluline on tähele panna, et kui arvuvallas R on ühikelement 1, siis peab kehtima seos $\lambda^M = 1$, sest vastasel korral oleks hulgas $\{\lambda, \lambda^2, \lambda^3, \dots\}$ vähem kui M erinevat elementi.

Tõepoolest, et $1 = \lambda^k$ mingi $k \in \{1, \dots, M\}$ korral, siis juhul kui $k < M$, oleks võimalik taandamine $\lambda^{m+k} = \lambda^m$ ja erinevaid elemente ei oleks rohkem kui k .

Järeldus. Seega võib öelda, et element $0 \neq \lambda \in R$ on primitiivne parajasti siis, kui seosest $\lambda^p = 1$ järeldub võrratus $p \geq M$.

Primitiivsed polünoomid

Taandumatut polünoomi $f \in R[x]$ nimetatakse *primitiivseks polünoomiks*, kui vähemalt üks tema juurtest ϑ on laiendi $R[\vartheta]$ primitiivne element.

Eelmisest teoreemist järeldeb, et polünoom $f(x)$ on primitiivne parajasti siis, kui polünoom x on jäägiklassiringi $R[x]/f(x)$ primitiivne element.

Et ringis $R[\vartheta]$ on parajasti $2^{\deg f}$ elementi, siis võib öelda, et polünoom $f(x)$ on primitiivne parajasti siis, kui seosest $x^p \equiv 1 \pmod{f(x)}$ järeldeb võrratus $p \geq 2^{\deg f} - 1$.

Perioodi maksimaalsuse tingimus

Teoreem. Lineaarse nihkeregistri väljundjada periood on maksimaalne parajasti siis, kui karakteristlik polünoom $f(x) \in \mathbb{Z}_2[x]$ on primitiivne.

Tõestus. Olgu $f(x)$ primitiivne polünoom ja oletame, et p on registri periood, st $x^p \cdot s(x) \equiv s(x) \pmod{f(x)}$ iga $s(x) \in \mathbb{Z}_2[x]/f(x)$ korral. Järelikult kehtib seos ka $s(x) = 1$ korral, st $x^p \equiv 1 \pmod{f(x)}$, millest primitiivsuse tõttu järeljub $p \geq 2^{\deg f} - 1$, st periood on maksimaalne.

Oletame, et registri periood on maksimaalne, st kui p on mingi arv, nii et iga $s(x)$ korral $x^p s(x) \equiv s(x) \pmod{f(x)}$, siis $p \geq 2^{\deg f} - 1$. Olgu $x^p \equiv 1 \pmod{f(x)}$. Kuid siis kehtib iga $s(x)$ korral seos

$$x^p s(x) \equiv s(x) \pmod{f(x)},$$

millest perioodi maksimaalsuse tõttu järeljub, et $p \geq 2^{\deg f} - 1$. Seega, f on primitiivne polünoom. \square