Katona Gyula - Nemetz Tibor:

Néhány megjegyzés a shift-regiszter generátorokról

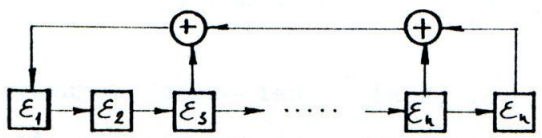
1. Bevezetés.

Jelen dolgozat F.H.Young, a shift-regiszter generátorokkal foglalkozó dolgozatához kapcsolódik. Young az általa tekintett kérdésre vonatkozóan ismertet egy algebrai segédeszközt, mellyel konkrét esetekben sikeresen lehet számolni, azonban általános válasz megadása ezideig más szerzőknek sem sikerült. Utalunk Peterson [2] könyvére, mely e témáról alapos ismertetést ad, s bővebb irodalomjegyzéket tartalmaz.

Dolgozatunkban a Young által bevezetett függvényleirás mellett megadjuk a probléma mátrixleirását, rámutatva arra, hogy ez a lényegében ekvivalens leirás az összefüggések kimutatásánál milyen előnyökkel járhat. Az [1] dolgozat eredményein kivül ezen az uton általánosabb eredményeket is bizonyitunk. Vizsgáljuk továbbá a gépi uton nyerhető eredmények egyszerü, de hatásos ellenőrzési lehetőségeit.

2. Definiciók, fogalmak

Egy shift-regiszter (a továbbiakban S-R) müködését a következőképpen irhatjuk le (lásd 1. ábra). Az S-R tartalmát egy n-dimenziós $\mathcal{E} = (\mathcal{E}_1, \dots, \mathcal{E}_n)$ vektorral szemléltethetjük, ahol $\mathcal{E}_i$ értéke a 0 vagy 1 szám lehet.



1.sz. ábra

MAGYAR TUDOMÁNYOS AKADÉMIA
SZÁMÍTÁSTECHNIKAI KÖZPONTJA

KÖZLEMÉNYEK 5.

Budapest, 1969. június

Egy adott pillanatban az i-edik tároló tartalma átvivődik az (i+1)-edik tárolóba, i=1,2,...,n-1 ill. az n-edik tároló tartalma az első tárolóba. Mig az előző átvitelek változtatás nélkül történnek, addig az utolsó információ-bit az átvitel során oly módon transzformálódik, hogy az $i_1,i_2,\ldots,i_r$ tárolókon levő bitek moduló 2 hozzáadódnak. Hangsulyozni kell, hogy a fenti átvitelek a matematikai modell számára egyidejüleg következnek be. Az átvitel hatására a S-R tartalma megváltozik, uj tartalmát az $\underline{\varepsilon}' = T\underline{\varepsilon}$

$$/2.1/ \qquad \varepsilon'_i = \begin{cases} \varepsilon_{i-1}, & \text{ha } i=2,3,\ldots,n \\ \varepsilon_n \oplus \varepsilon_{i_1} \oplus \ldots \oplus \varepsilon_{i_r}, & \text{ha } i=1 \end{cases}$$

vektor írja le, ahol $\oplus$ a moduló 2 vett összeadást jelöli.

Az $\varepsilon^{(2)}$ vektort az $\varepsilon^{(1)}$ vektorból elérhetőnek nevezzük, ha létezik olyan m szám, melyre $\varepsilon^{(2)} = T^m \varepsilon^{(1)}$, azaz ha az $\varepsilon^{(1)}$ tartalmu SR-t lépésenként müködtetve elérhetjük, hogy tartalma $\varepsilon^{(2)}$ legyen. Látni fogjuk, hogy az elérhetőség ekvivalencia reláció. A keletkező ekvivalencia-osztályokat ciklusoknak, elemszámukat ciklushossznak (jele c_ε), mig a legnagyobb ciklushosszat periodusnak (jele p) nevezzük. A legkisebb c_ε érték nyilvánvalóan egy, ami az $\underline{\varepsilon} \equiv \underline{0}$ zérusvektornak felel meg. (Ezenkivül $c_\varepsilon = 1$ akkor és csak akkor, ha r páros és $\varepsilon_i \equiv 1$, i=1,...,n). Ennek megfelelően $p = \max c_\varepsilon \leq 2^n-1$

Young azt a speciális esetet tekintette, amikor r=1, azaz ha

$$\varepsilon'_1 = \varepsilon_n \oplus \varepsilon_k, \qquad 1 \leq k \leq n-1$$

Feladat a ciklushosszak $\{ c_\varepsilon (k,n) \}$ halmazának meghatározása, de érdekes lenne már a p=p(k,n) periódus explicit megadása k és n függvényeként. Bár e feladatot megoldani nem sikerült, de részeredmények elérésére, illetve konkrét esetekben hasznos a probléma következő két átfogalmazása véges testek feletti függvények, illetve mátrixok terminológiájában.

3. Függvényleirás

Először speciálisan $r=1$, $i=i_1$ esetén tekintsük moduló $x^n + x^i + 1$ az x változó polinomjait a mod2 vett egészek teste felett.

Definiáljuk az $\underline{\varepsilon}$ vektor segitségével a következő függvényt:

$$/3.1/ \quad F(x) = \varepsilon_n x^{i-1} + \varepsilon_{n-1} x^{i-2} + \ldots + \varepsilon_{n-i+1} + \varepsilon_{n-i} x^{n-1} + \ldots + \varepsilon_1 x^i$$

Felhasználva, hogy

$$x^n \equiv x^i + 1 \pmod{x^n + x^i + 2},$$

nyerjük:

$$x F(x) = \varepsilon_{n-1} x^{i-1} + \varepsilon_{n-2} x^{i-2} + \ldots + \varepsilon_{n-i} + \varepsilon_{n-i-1} x^{n-1} + \ldots + (\varepsilon_n \oplus \varepsilon_{n-i}) x^i$$

Ha tehát a SR tartalma rendre megegyezik a fenti módon rendezett $F_\varepsilon(x)$ együtthatóival, akkor egy átvitel-lépés után a SR tartalma az $x.F_\varepsilon(x)$ polinom együtthatóival egyezik meg. A 2. pontban bevezetett definició értelmében c_ε az a legkisebb pozitiv egész szám, melyre

$$x^{c_\varepsilon} F_\varepsilon(x) \equiv F_\varepsilon(x) \pmod{x^n + x^i + 1}$$

azaz

$$/3.2/$$

$$(x^{c_\varepsilon} + 1) F_\varepsilon(x) \equiv 0 \pmod{x^n + x^i + 1}$$

Speciálisan, ha $F_\varepsilon(x) \equiv 1$, akkor $c_1 = c_\varepsilon$ az a legkisebb szám, melyre $x^{c_1} + 1$ osztható az $x^n + x^i + 1$ polinommal. Nyilvánvaló, hogy tetszőleges ε mellett fennáll ekkor az

$$(x^{c_1} + 1)\, F_\varepsilon(x) \equiv 0 \pmod{x^n + x^i + 1}$$

reláció, tehát egyrészt $c_1 = p$, másrészt p osztható c_ε -nal ε minden értékére. Ez azt jelenti, hogy tetszőleges ε esetén p lépés után a SR. tartalma ismét az eredeti lesz, tehát ebben az értelemben jogos volt p-t periódusnak nevezni.

Speciálisan, ha $x^n + x^i + 1$ irreducibilis polinom, akkor tetszőleges legfeljebb n-1-edfoku $F_\varepsilon(x) \not\equiv 0$ mellett a /3.2/ összefüggés akkor és csak akkor teljesül, ha a

$$/3.3/ \qquad x^{c_1} + 1 \equiv 0 \pmod{x^n + x^i + 1}$$

összefüggés is teljesül. Ez azt jelenti, hogy ebben az esetben c_ε nem függ ε -tól, ha $\varepsilon \not\equiv 0$, azaz minden egynél nagyobb ciklushossz egyenlő. Másrészt könnyü látni, hogy ez csak akkor van igy, ha $x^n + x^i + 1$ irreducubilis polinom.

Az általános eset tárgyalása az un. lineáris rekurziók keretén belül végezhető el legcélszerübben.

Legyenek adottak a $h_o = 1, h_1, \ldots, h_{n-1}, h_n = 1$ számok, ahol a h_i, $1 \leq i \leq n-1$ számok mindegyike 0 vagy 1, továbbá egy $\underline{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_n)$ vektor, melynek koordinátái szintén csak a 0 és 1 számok lehetnek. Ezek segitségével definiáljuk az ε_{n+1}, majd rekurzive az $\varepsilon_{n+2}, \ldots$ számokat az

$$\varepsilon_{n+1} = \sum_{j=o}^{n-1} h_j\, \varepsilon_{1+j}$$

illetve általában az

$$/3.4/ \qquad \varepsilon_{n+i} = \sum_{j=o}^{n-1} h_j\, \varepsilon_{i+j}$$

rekurzió segitségével, ahol a $\sum$ jel mod 2 vett összeadást jelöl. Az ily módon nyerhető számsor periódusára vonatkozik a következő tétel, melyet a fentiek jól szemléltetnek:

1. Tétel: Tekintsük a $h(x) = \sum_{j=o}^{n} h_j x^j$ polinomot, s legyen p az a legkisebb pozitiv egész szám, melyre $x^p + 1$ osztható h(x)-szel. Akkor az $\varepsilon_1, \varepsilon_2, \ldots,$ sorozat periódikus p szerint.

A tétel bizonyitására nem térünk ki, csak utalunk arra, hogy ez megtalálható Peterson [2] könyvében (118. old.).

Megjegyezzük, hogy az idézett gondolatmenetből következik az

1. Lemma: Minden részperiódus osztója p-nek.

Térjünk vissza ezután egy kis időre a /3.2/ összefüggéshez. Nyilván létezik olyan $(c_\varepsilon - 1)$-ed foku g(x) polinpm, melyre

$$(x^{c_\varepsilon} + 1)\, F_\varepsilon(x) = (x^n + x^i + 1)\, g(x)$$

x helyébe $\frac{1}{x}$ -t irva és x^{c_ε} -nal végigszorozva nyerjük:

/3.5/ $$(x^{c_\varepsilon} + 1)\, F_{\varepsilon^*}(x) = (x^n + x^{n-i} + 1)\, g^*(x)$$

ahol

$$g^*(x) = x^{c_\varepsilon - 1} g\left(\frac{1}{x}\right),$$

és /3.1/ alapján könnyen látható, hogy

$$\varepsilon^* = (\varepsilon_n, \varepsilon_{n-1}, \ldots, \varepsilon_1),$$

azaz

$$\varepsilon_i^* = \varepsilon_{n-i}$$

Ez azt jelenti, hogy az r=1 esetben az $i_1 = i$ és az $i_1 = n-i$ visszacsatolások mellett létezik egyértelmü megfeleltetés az ekvivalencia osz-

tályok között, tehát speciálisan a ciklushosszak és igy a periodusok is egyenlőek. Eredményünket tétel formájában is megfogalmazhatjuk:

2. Tétel: Ha $\{c_\varepsilon(i,n)\}$ jelöli $r=1$, $i_1 = i$ esetben a ciklushosszak halmazát, akkor a $\{c_\varepsilon(i,n)\}$ és a $\{c_\varepsilon(n-i,n)\}$ halmazok permutáció tól eltekintve megegyeznek.

Megjegyezzük, hogy ez a tétel Young [1] dolgozatában más bizonyitással szerepel, azonban mi bizonyitásunk az általános esetre is minden nehézség nélkül átvihető.

Vizsgáljuk meg most, milyen esetben lesz a periódus maximális, tehát 2^n-1 hosszuságu. Mivel tetszőleges $\varepsilon \neq 0$ esetén $c_\varepsilon = 2^n-1$ ekkor, s igy a ciklushossz nem függ ε-tól, tehát a megelőzőek szerint ebben az esetben szükséges, hogy az $x^n + x^i + 1$ polinom (vagy általános esetben a $h(x)$) irreducibilis legyen. Ez a feltétel azonban nem elégséges, mint azt $n=6$ esetén az irreducibilis $x^6 + x^3 + 1$ polinom mellett láthatjuk.

Érvényes ugyanis az

$$x^9 + 1 = (x^6 + x^3 + 1)(x^3 + 1)$$

reláció, másrészt 9 az a legkisebb p pozitiv egész, melyre

$$x^p + 1 = 0 \pmod{x^6 + x^3 + 1}$$

tehát a periódus $p=9 \neq 2^6-1 = 63$. Ez azt jelenti, hogy ekkor 7 különböző 9 hosszusá. . ciklus létezik, amiről direkt számolás segitségével is könynyen meg lehet győződni.

Abban az esetben, ha a legkisebb olyan p egész, melyre az irreducibilis $h(x)$ n-edfoku polinom esetén

/3.6/ $$x^p + 1 = 0 \pmod{h(x)}$$

teljesül, $p = 2^n-1$, akkor az irreducibilis $h(x)$ polinomot primitiv

polinomnak nevezzük. Megjegyezzük, hogy ez a definició eltér a fogalomnak a matematikai irodalomban szokásos bevezetésétől, azonban azzal ekvivalens. Az irreducibilis és primitiv polinomokról n nem tul nagy értéke mellett több részleges vagy teljes táblázat létezik, pl. Marsh [3], Peterson [2]. Ezek a táblázatok jól felhasználhatók arra, hogy maximális periódusu SR-t készitsünk, de nyilván nem adnak választ arra, hogy milyen ciklushosszuságok lépnek fel adott, nem primitiv polinomok esetén. Megjegyezzük még, hogy tetszőleges n mellett létezik n-edfoku primitiv polinom, azonban, ha csak olyan h(x) polinomokra szoritkozunk, melyeknél $h_i = 1$ csak egyetlen $1 \leq i \leq n-1$ esetén teljesül, ez már nem lesz igaz. A legkisebb n érték, melyre ezt láthatjuk, n = 8 (lásd 1. táblázat).

4. Mátrixleirás

A /2.1/ összefüggéssel definiált T transzformációt mátrixszorzás segitségével is leirhatjuk. Tekintsük az

$$A = (a_{jik}) \quad \begin{matrix} k = \overline{1,n} \\ j = \overline{1,n} \end{matrix}$$

mátrixot, ahol

$$/4.1/ \qquad a_{j,k} = \begin{cases} 1, & \text{ha } j = 1,\ k = i_u,\ u=1,2,\ldots,r, \text{ vagy } k = n \\ 1, & \text{ha } j = k+1,\ k = 1,2,\ldots,n-1 \\ 0 & \text{különben} \end{cases}$$

Igy pl. a 3. pontban leirt $x^6 + x^3 + 1$ függvény esetén

$$A_{6,3} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Az $\underline{\varepsilon}$ vektort oszlopvektorként felfogva a /2.1/ összefüggés az

/4.2/ $$\underline{\varepsilon}' = \underline{\underline{A}}\ \underline{\varepsilon}$$

alakot ölti, ahol az összeadások modulo kettő történnek. Továbbá, ha $\underline{\varepsilon}^{(n)}$ jelöli az $\underline{\varepsilon} = \underline{\varepsilon}^{(o)}$ vektorból a T transzformáció ismételt alkalmazásával nyert n-edik vektort, akkor

$$\underline{\varepsilon}^{(n)} = A^n \cdot \underline{\varepsilon}^{(o)}$$

ahol A^n jelöli az A mátrix mod 2 vett n-edik hatványát.

Legyen $\underline{\varepsilon}^{(o)} = (1,0,0,\ldots,0)$, azaz legyen

$$\varepsilon_i^{(o)} = \begin{cases} 1, & \text{ha } i = 1 \\ 0, & \text{ha } 1 < i \leq n \end{cases}$$

Ekkor a

$$B = \begin{bmatrix} \underline{\varepsilon}^{(o)} \\ \underline{\varepsilon}^{(1)} \\ \vdots \\ \underline{\varepsilon}^{(n-1)} \end{bmatrix}$$

mátrixról könnyü látni, hogy un. háromszögmátrix, s igy a determinánsa det(B) = 1. Ez azt jelenti, hogy az egy ciklusba tartozó vektorok lineárisan függetlenek. Ezért ezen ciklus hossza megegyezik a p periodussal, hiszen bármely $\underline{\varepsilon}$ vektor előállitható a fentiek lineáris kombinációjaként.

Jelöljük az összes n-edrendü, egy determinánsu 0 és 1 elemü A mátrixok halmazát $\mathcal{A}$ -val. Nyilván $\mathcal{A}$ csoportot alkot a modulo 2 vett szorzásra nézve. Ebből következik, hogy tetszőleges $A \in \mathcal{A}$ esetén létezik olyan e érték, melyre $A^e = E$, ahol E az egységmátrixot jelöli. Mivel a /4.1/ alatt leirt A mátrixok beletartozmak $\mathcal{A}$ -ba, igy a c_ε

számok feltétlen léteznek, továbbá a 2. pontban definiált elérhetőség valóban ekvivalencia reláció.

Határozzuk meg $\mathcal{A}$ elemszámát, azaz a csoport rendjét. E célból nézzük meg, hogy az A mátrix egyes sorait rendre hányféleképpen lehet kitölteni oly módon, hogy az egyes sorok mint n dimenziós vektorok lineárisan függetlenek legyenek, továbbá az azonosan 0 vektort egyik sornak se válasszuk. Nyilvánvalóan az első sort $2^n - 1$, a második sort pedig $2^n - 2$ féleképpen lehet megválasztani. Tegyük föl, hogy az első s sort kitöltöttük a kívánt módon. Ekkor az s lineárisan függetlenül kitöltött sor által meghatározott altérbe 2^s vektor tartozik, így ezek egyikét sem választhatjuk (s+1)-edik sorként, viszont bármelyik más vektort igen. Ez azt jelenti, hogy az (s+1)-edik sort $2^n - 2^s$ különböző módon választhatjuk meg. Az $\mathcal{A}$ csoport rendjét nyilván az egyes sorok kitöltési lehetőségeinek a szorzata adja meg, vagyis a

$$/4.3/ \qquad \prod_{s=0}^{n-1} (2^n - 2^s) = 2^{\binom{n}{2}} \prod_{s=1}^{n} (2^s - 1)$$

szám.

Figyelembe véve, hogy véges csoportok esetén az elem rendje osztója a csoport rendjének, nyerjük a következő tételt:

<u>3. Tétel.</u> Tetszőleges shift-regiszter esetén a p periódus osztója a

$$2^{\binom{n}{2}} \cdot \prod_{s=1}^{n} (2^s - 1)$$

szorzatnak.

Megjegyezzük, hogy a /4.3/ számnak viszonylag kevés primfaktora van. Így pl. n = 34 esetén a páratlan primosztók száma 38. A $2^s - 1$ számok törzstényezős alakját s 34 -ig a 2. sz. táblázat tartalmazza.

5. A p(k.n)-re vonatkozó tételek

A következő 4. és 5. tétel Youngtól származik:

4. Tétel:

/4.4/ $$p(1,2^s) = 2^{2s} - 1$$

Bizonyitás: Mivel

$$x^{2^s} = x + 1 \pmod{x^{2^s} + x + 1},$$

igy

$$x^{2^{2s}} = (x + 1)^{2^s} = x^{2^s} + 1 = x$$

és

$$x^{2^{2s}} - 1 + 1 = 0 \pmod{x^{2^s} + x + 1}$$

másrészt könnyü látni, hogy a /4.4/ a lehető legkisebb ilyen szám.

5. Tétel:

/4.5/ $$p(1,2^s+1) = 2^{2s} + 2^s + 1$$

Bizonyitás: Mivel

$$x^{2^s} + 1 = x + 1 \pmod{x^{2^s+1} + x + 1},$$

igy

$$x^{2^{2s+2^s+1}} = x\,(x + 1)^{2^s} = x^{2^s} + x = 1 \pmod{x^{2^s+1} + x + 1}$$

tehát a /3.6/ reláció érvényes a fenti p mellett. Könnyü látni, hogy ez a p érték a lehető legkisebb, igy a tételt bizonyitottuk.

Legyen az n és k számok legnagyobb közös osztója $[n,k] = d$. Ekkor érvényes a következő:

6. Tétel:

$$p(k,n) = d.p\left(\frac{k}{d}, \frac{n}{d}\right)$$

Bizonyitás: Könnyen látható, hogy a transzformáció /4.1/ mátrixának hat-

ványozásakor a sorok d diszjunkt osztályba sorolhatók oly módon, hogy az A^s mátrix első sora s minden értéke mellett az A mátrix moduló d kongruens soraival végzett különböző müveletekkel keletkezik, s kialakitásában más sorok nem vesznek részt. Tekintsük az A mátrix azon részmátrixát, mely az (ud, vd) indexü elemeiből áll, s jelöljük ezt D-vel. Ugyancsak egyszerüen igazolható, hogy az

$$A^e = E$$

feltétel teljesüléséhez szükséges az

$$D^{\left[\frac{e}{d}\right]} = E$$

feltétel teljesülése. Mivel D megegyezik az $r = 1$, $i = \frac{k}{d}$, $n^* = \frac{n}{d}$ értékekhez tartozó SR mátrixával, igy nyertük a következő szükséges feltételt:

/4.6/ $$\left[\frac{p(k,n)}{d}\right] = p\left(\frac{k}{d}, \frac{n}{d}\right)$$

(az $[\alpha]$ jel az α szám egész értékét jelöli).

A /4.6/ relációt átirva kapjuk, hogy

$$p(k,n) \geq d.p\left(\frac{k}{d}, \frac{n}{d}\right)$$

Az ellenkező irányu egyenlőtlenség is egyszerüen adódik mátrixterminológiában is, de még egyszerübben látható, ha az

$$x^{p\left(\frac{k}{d}, \frac{n}{d}\right)} = 1 \pmod{x^{\frac{n}{d}} + x^{\frac{K}{d}} + 1}$$

összefüggésben x helyébe x^d -t helyettesitünk.

Megjegyezzük, hogy a 6. tétel alkalmazásával speciális eredményként adódnak Young 3.2, 3.4, 3.5, 3.6, 3.7. tételei. Valóban, pl. a 3.7 tétel állitása a jelen dolgozat terminológiájában

/4.7/ $$p(j, j(2^k + 1)) = j^{\cdot}(2^{2k}+2^k+1),$$

s mivel a 6. tétel szerint

$$p(j,j^{\bullet}(2^k+1)) = j^{\bullet}p(1,2^k+1)$$

és a /4.5/ alatti $p(1, 2^k+1)$ értéket ide behelyettesitve valóban /4.7/ adódik.

6. A ciklushosszak gépi meghatározásáról

Gyakorlati szempontokból elsőrendü feladat lehet a SR. periódusának meghatározása. Mint láttuk, az $\underline{\varepsilon}^{(o)} = (1,0,\ldots,0)$ vektorhoz tartozó ciklushossz megegyezik a SR periódusával, igy kézenfekvő az a gondolat, hogy a SR müködésének szimulálásával az $\underline{\varepsilon}^{(o)}$ kezdővektorból kiindulva határozzuk meg a periódust oly módon, hogy figyeljük, melyik az a legkisebb p érték, melyre $\underline{\varepsilon}^{(o)} = \underline{\varepsilon}^{(p)}$. Egy ilyen szimulációs program már a kisteljesitményü számológépeken is igen egyszerü és gyors, igy célszerünek látszik ezt az utat követni. Azonban a gépi uton nyert periódust a végzendő müveletek nagy száma miatt valamilyen módon ellenőrizni szükséges.

Egy egyszerü, de hatékony ellenőrzési lehetőséget kinál a 3. tétel. Valóban, elkészitve a gépi uton nyert periódus primtényezős felbontását, a fellépő primosztók csak a /4.3/ szám primosztói közül kerülhetnek ki. Előnye ennek az eljárásnak, hogy rendkivül gyorsan végrehajtható, mig hátránya, hogy sok esetben jónak fogadunk el hibás eredményt is. Ilyen hibás döntések valószinüségének meghatározása rendkivül bonyolult, igy arra jelen dolgozat keretei között nem térhetünk ki.

Gyakorlatilag teljesen biztonságos ellenőrzés hajtható végre a /3.3/ összefüggés alapján. Az alkalmazások során célszerü használni a következő egyszerü tényt:

7. Tétel: Legyenek $a_1,a_2,\ldots,a_r$ tetszőleges számok, p tetszőleges primszám. Akkor érvényes az

/6.1/ $(a_1+a_2+\ldots+a_r)^{p^k} = a_1^{p^k} + a_2^{p^k} + \ldots + a_r^{p^k} \pmod p$

összefüggés.

Bizonyitás: $k = 1$, $r = 2$ esetén

$$(a_1+a_2)^p = \sum_{i=0}^{p} \binom{p}{i} a_1^i \cdot a_2^{p-i} = a_1^p + a_2^p + b \cdot p$$

tehát az állitás igaz. Ezután $k = 1$ esetén r-re vonatkozó teljes indukcióval adódik

$$(a_1 + a_2 + \ldots + a_r)^p = a_1^p + a_2^p + \ldots + a_r^p$$

s ennek felhasználásával k-ra vonatkozó teljes indukcióval nyerjük a tétel állitását.

A tétel egy fontos speciális esetét külön is megfogalmazzuk, melyet fel fogunk használni:

2. Lemma:

/6.2/ $$(a + 1)^{2^k} = a^{2^k} + 1 \pmod 2$$

A lemma alkalmazásával a következőképpen járhatunk el: Legyen $m > n$, s jelölje $\sum_{\ell=0}^{\infty} \delta_\ell \cdot 2^\ell$ az $\left[\frac{m}{n}\right]$ szám diadikus felbontását. Ekkor

$$x^m = x^{m-\left[\frac{m}{n}\right]} \prod_{\ell=0}^{\infty} (x^{n})^{\delta_\ell \cdot 2^\ell}$$

s mivel

$$x^n = x^i + 1 \pmod{x^n + x^i + 1}$$

igy

$$x^m = x^{m-\left[\frac{m}{n}\right]} \cdot \prod_{\ell : \delta_\ell = 1} (x^i+1)^{2^\ell} \equiv x^{m-\left[\frac{m}{n}\right]} \prod_{\ell : \delta_\ell = 1} (x^{i \cdot 2^\ell}+1)$$

Mivel $p(i,n) = p(n-i,n)$, igy az általánosság megszoritása nélkül feltehetjük, hogy $i \leq \frac{n}{2}$. Ez azt jelenti, hogy x^m helyett x olyan hatványait kell tovább vizsgálnunk, melyeknek kitevője $\frac{m}{2}$ -nél nem nagyobb. A gépi uton nyert p periódusnak megfelelő x^p hatványra a fentieket alkalmazva viszonylag gyorsan megállapithatjuk azt a legfeljebb n-1-edfoku g(x) polinomot, melyre

$$x^p \equiv g(x) \pmod{x^n + x^i + 1}$$

/3.3/ szerint p csak akkor lehet periódus, ha $g(x) \equiv 1$. Megforditva, ha $g(x) \equiv 1$, akkor p a valódi periódus többszöröse lehet csak, s igy gyakorlatilag teljes biztonsággal végezhető az ellenőrzés.

Nézzünk két példát erre a második ellenőrzési eljárásra!

<u>1. Példa:</u> $p(1,10) = 889$

$$x^{889} = x^9 (x^{10})^{64} (x^{10})^{16} (x^{10})^8 =$$

$$= x^9 (x^{64}+1) (x^{16} + 1) (x^8 + 1) \qquad (\text{mod } x^{10}+x+1)$$

$$x^{64} = x^4 (x^4 + 1) (x^2 + 1)$$

$$x^9 (x^{64}+1) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$$

$$(x^{16} + 1) (x^8 + 1) = x^8 + x^7 + x^4 + 1$$

igy

$$x^{889} = x^{16} + x^{12} + x^{11} + x^7 + x^6 + x^3 + x + 1 = 1$$

azaz a $p = 889$ értéket elfogadhatjuk periódusnak.

2. Példa: $p(1,12) = 3255$

$$x^{3264} = (x^{12})^{256}\,(x^{12})^{16} = (x^{256} + 1)\,(x^{16} + 1) =$$

$$= x^{272} + x^{256} + x^{16} + 1$$

Továbbá

$$x^{272} = x^8\,(x^{16} + 1)\,(x^4 + 1)\,(x^2 + 1) = x^{10} + x^3 + x^2 + x$$

$$x^{256} = x^4\,(x^{16} + 1)\,(x^4 + 1)\,(x + 1) =$$

$$= x^{10} + x^9 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$x^{16} = x^5 + x^4$$

Igy

$$x^{3264} = x^9 \pmod{x^{12} + x + 1}$$

tehát

$$x^{3255} = 1 \pmod{x^{12} + x + 1}$$

azaz a $p(1,12) = 3255$ értéket elfogadhatjuk.

A ciklushosszak megállapitására Young a következő triviális módszert ajánlja: Induljunk ki tetszőleges $\underline{\varepsilon}^{(o)}$ kezdővektorból, s állapitsuk meg a $c_{\varepsilon}(o)$ -t. Jelöljön ε^1 olyan vektort, mely nem szerepelt az előző ciklusban, s ehhez is állapitsuk meg a c_{ε^1} -t, majd folytassuk ezt az eljárást, amig nem teljesül a $\sum_i c_{\varepsilon^i} = 2^n$ összefüggés. Ez az eljárás meglehetősen hosszadalmas, sőt $n > 20$ esetén a gépi végrehajtása is jelentős bonyodalmakat okoz. E helyett célszerü gyakran a következő eljárást követni: Határozzuk meg az $\varepsilon^\circ = (1,0,0,\ldots,0)$ kezdővektorból kiindulva a p periódust, s jelölje $p_1, p_2, \ldots, p_s$ ennek primosztóit. (Nyilván a p_i szám osztója (4.3)-nak, $i = 1,2,\ldots,s$). Nyilvánvaló, hogy a $\{c_\varepsilon\}$ halmaz elemeinek osztói csak azon p_i számok lehetnek, melyekre a

/6.3/ $$2^n - p - 1 = \sum_{i=1}^{s} p_i x_i , \qquad x_i \geq 0$$

diofantikus egyenlet megoldásában $x_i > 0$.

Megjegyezzük, hogy abban az esetben, ha a /6.3/ egyenletnek nincs megoldása, akkor a számolt p érték nyilvánvalóan helytelen, igy a /6.3/ egyenlet megoldása egy harmadik ellenőrzési lehetőséget jelent.

Nézzünk egy példát a ciklushosszak meghatározására:

3. Példa: A fenti módon számolt p (1,13) = 8001.
A kivánt törzstényezős felbontás:

$$8001 = 3^2 \cdot 7 \cdot 127$$

lássuk be, hogy $c_\varepsilon \neq 3$ semmilyen $\underline{\varepsilon}$-ra. Könnyebb a számolást végrehajtani, ha i = 1 helyett i = 12 -vel számolunk. Tegyük föl, hogy ilyen $\underline{\varepsilon}$ létezik. Akkor érvényes a

$$/6.4/ \quad \begin{cases} \varepsilon_{10} \oplus \varepsilon_{11} = \varepsilon_1 = \varepsilon_4 = \varepsilon_7 = \varepsilon_{10} = \varepsilon_{13} \\ \varepsilon_{11} \oplus \varepsilon_{12} = \varepsilon_2 = \varepsilon_5 = \varepsilon_8 = \varepsilon_{11} \\ \varepsilon_{12} \oplus \varepsilon_{13} = \varepsilon_3 = \varepsilon_6 = \varepsilon_9 = \varepsilon_{12} \end{cases}$$

egyenletrendszer. Könnyen látható, hogy ennek egyetlen megoldása $\varepsilon_i = 0$, i = 1,2,...,13, s ez ellentmond feltevésünknek.

Hasonlóan ellentmondásra jutunk a $c_\varepsilon = 7$ feltételből. Ekkor a

$$/6.5/ \quad \begin{cases} \varepsilon_6 \oplus \varepsilon_7 = \varepsilon_1 = \varepsilon_8 \\ \varepsilon_7 \oplus \varepsilon_1 = \varepsilon_2 = \varepsilon_9 \\ \varepsilon_1 \oplus \varepsilon_2 = \varepsilon_3 = \varepsilon_{10} \\ \varepsilon_2 \oplus \varepsilon_3 = \varepsilon_4 = \varepsilon_{11} \\ \varepsilon_3 \oplus \varepsilon_4 = \varepsilon_5 = \varepsilon_{12} \\ \varepsilon_4 \oplus \varepsilon_5 = \varepsilon_6 = \varepsilon_{13} \\ \varepsilon_5 \oplus \varepsilon_6 = \varepsilon_7 \end{cases}$$

Könnyen nyerhető az egymásutáni egyenletpárok összeadásával, hogy $\varepsilon_1 = \varepsilon_2 = \ldots = \varepsilon_7$ továbbá az összes egyenlet összeadásával $\sum \varepsilon_i = 7 \cdot \varepsilon_1 = 0$, ami ellentmondást jelent. Ezután az

$$2^{13} - 8001 - 1 = 9x + 127y \,, \quad x \geq 0, \quad y \geq 0$$

egyenletet oldjuk meg.

Az általános megoldás:

$$x = 7 + 127t$$
$$y = 1 - 9t$$

Ha $t < 0$, akkor $x < 0$, míg ha $t > 0$, akkor $y < 0$, tehát az egyetlen megoldás: $x = 7$ és $y = 1$.

Ez azt jelenti, hogy egy 127 hosszuságu ciklus van, továbbá vagy 7 db 9 hosszuságu, vagy egy darab 63 hosszuságu. A fentiekhez teljesen hasonlóan ellentmondásra jutunk akkor is, ha feltesszük, hogy létezik olyan $\underline{\varepsilon}$, melyre $c_{\varepsilon} = 9$. Ez azt jelenti, hogy a különböző ciklusokhoz tartozó ciklushosszak halmaza a következő:

$$\{1, 8001, 127, 63\}$$

1. sz. táblázat: p(k,n)

2	3							
3	7	7						
4	15	6	15					
5	21	31	31	21				
6	63	14	9	14	63			
7	127	93	127	127	93	127		
8	63	30	217	12	217	30	63	
9	73	465	21			21	465	
10	889	42	1023	62	15	62	1023	
11		2047				18		
12	3255	126	45	28				
13	8001				254	21	254	
14		254	186		35	93	32767	
15	32767	4599	63	32767				
16	255	126	57337	60	16383	434	63457	
17	273	114681	131071	1023	131071	131071	4599	
18	253921	146	189	930	32767	42	262143	
19	413385	129921	491505	91749				
20	767163	1778	1048575	84	75	2046	779907	
21	5461	2097151	381	406317	5461	279	49	
22	4194303	3066	3670009	4094	2752491	3906	4063201	
23	2088705	7864305	32767	2088705	8388607	458645	2094081	
24	2097151	6510	189	252	16766977	90	1048575	
25	10961685	25165821	33554431	2158065	105			
26	298935	15810	2094081	3570	67074050	16002	13797	
27	125829105	458745	219	5592405	8877935	1395	44564396	
28			268435455	508			105	
29		536870911						
30		65534	2667	9198	315	186		
31			2147483647					

2. sz. táblázat: $2^n - 1$ primfelbontása

3	7
4	3x5
5	31
6	3x3x7
7	127
8	3x5x17
9	7x73
10	3x11x31
11	23x89
12	3x3x5x7x13
13	8191
14	3x43x127
15	7x31x151
16	3x5x17x257
17	131071
18	3^3x7x19x73
19	524287
20	3x5^2x11x31x41
21	7^2x127x337
22	3x23x89x683
23	47x178481
24	3^2x5x7x13x17x241
25	31x601x1801
26	3x2731x8191
27	7x73262657
28	3x5x29x43x113x127
29	233x1103x2089
30	3^2x7x11x31x151x331
31	2147483647
32	3x5x17x257x65537
33	7x23x89x599479
34	3x43691x131071

Irodalom:

[1] Young,F.H. Analysis of Shift Register Counters, Journ. A.C.M. 5, (1958) 385-388 old.

[2] Peterson,W.W. Error Correcting Codes, Wiley, New-York, 1962.

[3] Marsh,R.W. Table of Irreducible Polynomials Over GF/2/, Through Degree 19, NSA, Washington, D.C. (1957)

Summary

Notes on the shift-register generators

This paper is connected with the results of F.H.Young [1] , concerning to the cycles and periods of the shiftregister generators. The paper contains well known theorems, and obtains new results too. The authors show that these theoretical results are practically not or only hardly applicable. So they deal with the determination of the cycles and periods of given shift-registers on the electronic computers, and the problems regarding this matter.