

Katona Gyula - Nemetz Tibor:

Néhány megjegyzés a shift-regiszter generátorokról

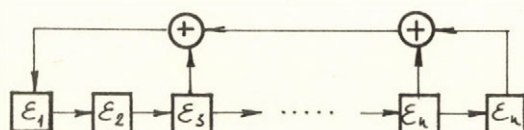
1. Bevezetés.

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 függvényleírás mellett megadjuk a probléma mátrixleírását, rámutatva arra, hogy ez a lényegében ekvivalens leírás az összefüggések kimutatásánál milyen előnyökkel járhat. Az [1] dolgozat eredményein kívül ezen az uton általánosabb eredményeket is bizonyítunk. Vizsgáljuk továbbá a gépi uton nyerhető eredmények egyszerű, de hatásos ellenőrzési lehetőségeit.

2. Definíciók, fogalmak

Egy shift-regiszter (a továbbiakban S-R) működését a következőképpen írhatjuk 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.



⊕ moduló 2 vett összeadó

□ információ-tároló

1.sz. ábra

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

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

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 működtetve elérhetjük, hogy tartalma  $\varepsilon^{(2)}$  legyen. Látni fogjuk, hogy az elérhetőség ekvivalencia reláció. A keletkező ekvivalencia-osztályokat ciklusoknak, elemszámukat ciklushossznak (jele  $c_\varepsilon$ ), míg a legnagyobb ciklushosszat periodusnak (jele  $p$ ) nevezzük. A legkisebb  $c_\varepsilon$  érték nyilvánvalóan egy, ami az  $\underline{\varepsilon} \equiv \underline{0}$  zérusvektornak felel meg. (Ezenkívül  $c_\varepsilon = 1$  akkor és csak akkor, ha  $r$  páros és  $\varepsilon_i \equiv 1, i=1,\dots,n$ ). Ennek megfelelően  $p = \max c_\varepsilon \leq 2^n - 1$

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

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

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. Függvényleírás

Először speciálisan  $r=1$ ,  $i=i_1$  esetén tekintsük moduló  $x^n + x^i + 1$  az  $x$  változó polinomjait a mod 2 vett egészek teste felett.

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

$$\begin{aligned} /3.1/ \quad F(x) &= \varepsilon_n x^{i-1} + \varepsilon_{n-1} x^{i-2} + \dots + \varepsilon_{n-i+1} + \\ &+ \varepsilon_{n-i} x^{n-1} + \dots + \varepsilon_1 x^i \end{aligned}$$

Felhasználva, hogy

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

nyerjük:

$$\begin{aligned} x F(x) &= \varepsilon_{n-1} x^{i-1} + \varepsilon_{n-2} x^{i-2} + \dots + \varepsilon_{n-i} + \varepsilon_{n-i-1} x^{n-1} + \\ &+ \dots + (\varepsilon_n \oplus \varepsilon_{n-i}) x^i \end{aligned}$$

Ha tehát a SR tartalma rendre megegyezik a fenti módon rendezett  $F_{\underline{\varepsilon}}(x)$  együtthatóival, akkor egy átvitel-lépés után a SR tartalma az  $x \cdot F_{\underline{\varepsilon}}(x)$  polinom együtthatóival egyezik meg. A 2. pontban bevezetett definíció értelmében  $c_{\underline{\varepsilon}}$  az a legkisebb pozitív egész szám, melyre

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

azaz

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

/3.2/

Speciálisan, ha  $F_{\underline{\varepsilon}}(x) \equiv 1$ , akkor  $c_1 = c_{\underline{\varepsilon}}$  az a legkisebb szám, melyre  $x^{c_1} + 1$  osztható az  $x^n + x^i + 1$  polinommal. Nyilvánvaló, hogy tetszőleges  $\underline{\varepsilon}$  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  $c_{\varepsilon}$ -nal  $\varepsilon$  minden értékére. Ez azt jelenti, hogy tetszőleges  $\varepsilon$  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  $F_{\varepsilon}(x) \neq 0$  mellett a /3.2/ összefüggés akkor és csak akkor teljesül, ha a

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

összefüggés is teljesül. Ez azt jelenti, hogy ebben az esetben  $c_{\varepsilon}$  nem függ  $\varepsilon$ -tól, ha  $\varepsilon \neq 0$ , azaz minden egynél nagyobb ciklushossz egyenlő. Másrészt könnyű látni, hogy ez csak akkor van így, ha  $x^n + x^i + 1$  irreducibilis polinom.

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

Legyenek adottak a  $h_0 = 1, h_1, \dots, h_{n-1}, h_n = 1$  számok, ahol a  $h_i, 1 \leq i \leq n-1$  számok mindegyike 0 vagy 1, továbbá egy  $\underline{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_n)$  vektor, melynek koordinátái szintén csak a 0 és 1 számok lehetnek. Ezek segítségével definiáljuk az  $\varepsilon_{n+1}$ , majd rekurzive az  $\varepsilon_{n+2}, \dots$  számokat az

$$\varepsilon_{n+1} = \sum_{j=0}^{n-1} h_j \varepsilon_{1+j}$$

illetve általában az

$$/3.4/ \quad \varepsilon_{n+i} = \sum_{j=0}^{n-1} h_j \varepsilon_{i+j}$$

rekurzió segítségével, 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  $h(x) = \sum_{j=0}^n h_j x^j$  polinomot, s legyen  $p$  az a legkisebb pozitív egész szám, melyre  $x^p + 1$  osztható  $h(x)$ -szel. Akkor az  $\varepsilon_1, \varepsilon_2, \dots$ , sorozat periódikus  $p$  szerint.

A tétel bizonyítására 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 fokú  $g(x)$  polinpm, melyre

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

$x$  helyébe  $\frac{1}{x}$ -t írva és  $x^{c_\varepsilon}$ -nal végigszorozva nyerjük:

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

ahol

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

és /3.1/ alapján könnyen látható, hogy

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

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 egyértelmű megfeleltetés az ekvivalencia osz-

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

2. Tétel: Ha  $\{c_\varepsilon(i, n)\}$  jelöli  $r=1, i_1 = 1$  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 bizonyítással szerepel, azonban<sup>a</sup>mi bizonyításunk az általános esetre is minden nehézség nélkül átvihető.

Vizsgáljuk meg most, milyen esetben lesz a periódus maximális, tehát  $2^n-1$  hosszúságú. Mivel tetszőleges  $\varepsilon \neq 0$  esetén  $c_\varepsilon = 2^n-1$  ekkor, s így a ciklushossz nem függ  $\varepsilon$ -től, tehát a megelőzők 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  $p$  pozitív 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 hosszúságú ciklus létezik, amiről direkt számolás segítségével is könnyen 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 primitív

polinomnak nevezzük. Megjegyezzük, hogy ez a definíció eltér a fogalomnak a matematikai irodalomban szokásos bevezetésétől, azonban azzal ekvivalens. Az irreducibilis és primitív polinomokról  $n$  nem túl 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 készítsünk, de nyilván nem adnak választ arra, hogy milyen ciklushosszuságok lépnek fel adott, nem primitív polinomok esetén. Megjegyezzük még, hogy tetszőleges  $n$  mellett létezik  $n$ -edfoku primitív polinom, azonban, ha csak olyan  $h(x)$  polinomokra szorítkozunk, 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. Mátrixleírás

A /2.1/ összefüggéssel definiált  $T$  transzformációt mátrixszorzás segítségével is leírhatjuk. Tekintsük az

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

mátrixot, ahol

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

Igy pl. a 3. pontban leírt  $x^6 + x^3 + 1$  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  $\underline{\xi}$  vektort oszlopvektorként felfogva a /2.1/ összefüggés az

$$/4.2/ \quad \underline{\xi}' = \underline{A} \underline{\xi}$$

alakot ölti, ahol az összeadások modulo kettő történnék. Továbbá, ha  $\underline{\xi}^{(n)}$  jelöli az  $\underline{\xi} = \underline{\xi}^{(0)}$  vektorból a T transzformáció ismételt alkalmazásával nyert n-edik vektort, akkor

$$\underline{\xi}^{(n)} = A^n \cdot \underline{\xi}^{(0)}$$

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

Legyen  $\underline{\xi}^{(0)} = (1, 0, 0, \dots, 0)$ , azaz legyen

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

Ekkor a

$$B = \begin{bmatrix} \underline{\xi}^{(0)} \\ \underline{\xi}^{(1)} \\ \vdots \\ \underline{\xi}^{(n-1)} \end{bmatrix}$$

mátrixról könnyű látni, hogy un. háromszögmátrix, s így 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  $\underline{\xi}$  vektor előállítható a fentiek lineáris kombinációjaként.

Jelöljük az összes n-edrendű, egy determinánsu 0 és 1 elemű 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 leírt A mátrixok beletartoznak  $\mathcal{A}$ -ba, így a  $c_e$



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

Határozzuk meg  $A$  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 választjuk. 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  $A$  csoport rendjét nyilván az egyes sorok kitöltési lehetőségeinek a szorzata adja meg, vagyis a

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

szám.

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

3. Tétel. 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/ 
$$p(1,2^s) = 2^{2^s} - 1$$

Bizonyítás: Mivel

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

így

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

és

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

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

5. Tétel:

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

Bizonyítás: Mivel

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

így

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

tehát a /3.6/ reláció érvényes a fenti  $p$  mellett. Könnyű látni, hogy ez a  $p$  érték a lehető legkisebb, így a tételt bizonyítottuk.

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

6. Tétel:

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

Bizonyítás: Könnyen látható, hogy a transzformáció /4.1/ mátrixának het-

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 műveletekkel keletkezik,  $s$  kialakításában más sorok nem vesznek részt. Tekintsük az  $A$  mátrix azon részmatrixát, mely az  $(ud, vd)$  indexü elemeiből áll,  $s$  jelöljük ezt  $D$ -vel. Ugyancsak egyszerűen igazolható, hogy az

$$A^e = E$$

feltétel teljesüléséhez szükséges az

$$D \begin{bmatrix} e \\ d \end{bmatrix} = E$$

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

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

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

A /4.6/ relációt átírva kapjuk, hogy

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

Az ellenkező irányú egyenlőtlenség is egyszerűen adódik mátrixterminológiában is, de még egyszerűbben 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 helyettesítünk.

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 állítása a jelen dolgozat terminológiájában

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

s mivel a 6. tétel szerint

$$p(j, j \cdot (2^k + 1)) = j \cdot p(1, 2^k + 1)$$

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

#### 6. A ciklushosszak gépi meghatározásáról

Gyakorlati szempontokból elsőrendű feladat lehet a SR. periódusának meghatározása. Mint láttuk, az  $\underline{\xi}^{(0)} = (1, 0, \dots, 0)$  vektorhoz tartozó ciklushossz megegyezik a SR periódusával, így kézenfekvő az a gondolat, hogy a SR működésének szimulálásával az  $\underline{\xi}^{(0)}$  kezdővektorból kiindulva határozzuk meg a periódust oly módon, hogy figyeljük, melyik az a legkisebb  $p$  érték, melyre  $\underline{\xi}^{(0)} = \underline{\xi}^{(p)}$ . Egy ilyen szimulációs program már a kisteljesítményű számológépeken is igen egyszerű és gyors, így célszerűnek látszik ezt az utat követni. Azonban a gépi uton nyert periódust a végzendő műveletek nagy száma miatt valamilyen módon ellenőrizni szükséges.

Egy egyszerű, de hatékony ellenőrzési lehetőséget kínál a 3. tétel. Valóban, elkészítve a gépi uton nyert periódus primtényezős felbontását, a fellépő primosztók csak a /4.3/ szám primosztói közül kerülhetnek ki. Előnye ennek az eljárásnak, hogy rendkívül gyorsan végrehajtható, míg hátránya, hogy sok esetben jónak fogadunk el hibás eredményt is. Ilyen hibás döntések valószínűségének meghatározása rendkívül bonyolult, így arra jelen dolgozat keretei között nem térhetünk ki.

Gyakorlatilag teljesen biztonságos ellenőrzés hajtható végre a /3.3/ összefüggés alapján. Az alkalmazások során célszerű használni a következő egyszerű ténnyt:

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

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

összefüggés.

Bizonyítás:  $k = 1, r = 2$  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 állítás igaz. Ezután  $k = 1$  esetén  $r$ -re vonatkozó teljes indukcióval adódik

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

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

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

2. Lemma:

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

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

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

így

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

Mivel  $p(i, n) = p(n-i, n)$ , így az általánosság megszorítása 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 megállapíthatjuk 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  $g(x) \equiv 1$ . Megfordítva, ha  $g(x) \equiv 1$ , akkor  $p$  a valódi periódus többszöröse lehet csak, s így gyakorlatilag teljes biztonsággal végezhető az ellenőrzés.

Nézzünk két példát erre a második ellenőrzési eljárásra!

1. Példa:  $p(1, 10) = 889$

$$\begin{aligned} x^{889} &= x^9 (x^{10})^{64} (x^{10})^{16} (x^{10})^8 = \\ &= x^9 (x^{64} + 1) (x^{16} + 1) (x^8 + 1) \pmod{x^{10} + x + 1} \end{aligned}$$

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

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

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

így

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

azaz a  $p = 889$  értéket elfogadhatjuk periódusnak.

2. Példa:  $p(1,12) = 3255$

$$\begin{aligned}x^{3264} &= (x^{12})^{256} (x^{12})^{16} = (x^{256} + 1) (x^{16} + 1) = \\ &= x^{272} + x^{256} + x^{16} + 1\end{aligned}$$

Továbbá

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

$$\begin{aligned}x^{256} &= x^4 (x^{16} + 1) (x^4 + 1) (x + 1) = \\ &= x^{10} + x^9 + x^5 + x^4 + x^3 + x^2 + x + 1\end{aligned}$$

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

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 megállapítására Young a következő triviális módszert ajánlja: Induljunk ki tetszőleges  $\underline{\varepsilon}^{(0)}$  kezdővektorból, s állapítsuk meg a  $c_{\varepsilon}^{(0)}$ -t. Jelöljön  $\varepsilon^1$  olyan vektort, mely nem szerepelt az előző ciklusban, s ehhez is állapítsuk meg a  $c_{\varepsilon^1}$ -t, majd folytassuk ezt az eljárást, amíg 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 célszerű gyakran a következő eljárást követni: Határozzuk meg az  $\varepsilon^0 = (1, 0, 0, \dots, 0)$  kezdővektorból kiindulva a  $p$  periódust, s jelölje  $p_1, p_2, \dots, p_s$  ennek primosztóit. (Nyilván a  $p_i$  szám osztója (4.3)-nak,  $i = 1, 2, \dots, s$ ). Nyilvánvaló, hogy a  $\{c_{\varepsilon}\}$  halmaz elemeinek osztói csak azon  $p_i$  számok lehetnek, melyekre a

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

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, így 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 kívánt törzstényező 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

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

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

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

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



Könnyen nyerhető az egymásutáni egyenletpárok összeadásával, hogy

$$\varepsilon_1 = \varepsilon_2 = \dots = \varepsilon_7 \text{ továbbá az összes egyenlet összeadásával}$$

$$\sum \varepsilon_i = 7 \cdot \varepsilon_1 = 0, \text{ ami ellentmondást jelent. Ezután az}$$

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

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 hosszúságu ciklus van, továbbá vagy 7 db 9 hosszúságu, vagy egy darab 63 hosszúságu. 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							
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						
12	3255	126		45	28		18	
13	8001							
14		254		186		254	21	254
15	32767	4599		63	32767	35	93	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	$3 \times 5$
5	31
6	$3 \times 3 \times 7$
7	127
8	$3 \times 5 \times 17$
9	$7 \times 73$
10	$3 \times 11 \times 31$
11	$23 \times 89$
12	$3 \times 3 \times 5 \times 7 \times 13$
13	8191
14	$3 \times 43 \times 127$
15	$7 \times 31 \times 151$
16	$3 \times 5 \times 17 \times 257$
17	131071
18	$3^3 \times 7 \times 19 \times 73$
19	524287
20	$3 \times 5^2 \times 11 \times 31 \times 41$
21	$7^2 \times 127 \times 337$
22	$3 \times 23 \times 89 \times 683$
23	$47 \times 178481$
24	$3^2 \times 5 \times 7 \times 13 \times 17 \times 241$
25	$31 \times 601 \times 1801$
26	$3 \times 2731 \times 8191$
27	$7 \times 73 \times 262657$
28	$3 \times 5 \times 29 \times 43 \times 113 \times 127$
29	$233 \times 1103 \times 2089$
30	$3^2 \times 7 \times 11 \times 31 \times 151 \times 331$
31	2147483647
32	$3 \times 5 \times 17 \times 257 \times 65537$
33	$7 \times 23 \times 89 \times 599479$
34	$3 \times 43691 \times 131071$

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)

S u m m a r y

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.

Резюме

Статья занимается достижениями Ф.Х. Бнга [1], относящимися к циклам и периодам генераторов двиговых регистров. Статья содержит хорошо известные теоремы и достигает новых результатов. Авторы показывают, что эти теоретические результаты в практике совсем неприменимы или почти неприменимы. И так они тактуют определение циклов и периодов данного двигающего регистра в электронных вычислительных машинах, и проблем, связанных с этой темой.