TÓTH ÁRPÁD
Orion Rádió és Villamossági Vállalat

# Maximális hosszúságú bináris álvéletlen jelsorozat előállításának kritériumai

ETO 681.325.86

Az elektronikus alapáramkörök fejlődésével a berendezésekkel szemben támasztott minőségi igények is egyre nőnek. Ez maga után vonja új vizsgálati módszerek kidolgozását.

A fejlődés során kialakult napjaink egyik legexaktabb megfigyelése: a sztochasztikus módszer. Az elektronikus rendszerek ilyen vizsgálatánál véletlenjel generátorokat használunk és attól függően, hogy analóg vagy digitális-e a rendszer, analóg, ill. bináris véletlen jelsorozatot alkalmazunk. Az analóg jel eloszlása az alkalmazástól függően változik, de az esetek legtöbbjében döntő fontosságú szerepük van a Gauss-amplitúdóeloszlású forrásjeleknek [1, 2].

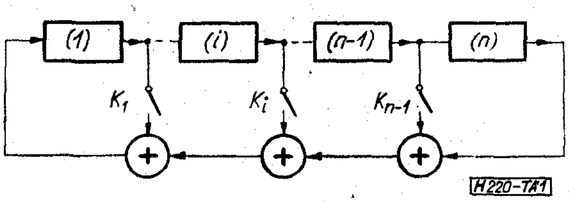
A mérések és számítások során adódó problémák leegyszerűsítése végett előnyösnek bizonyult az álvéletlen Gauss- és bináris jelsorozatok alkalmazása [3].

Digitális automatikai és hírátvivő rendszerek statisztikus vizsgálataihoz szinte általános módszer álvéletlen bináris jelgenerátorok alkalmazása.

## Maximális hosszúságú bináris álvéletlen jelsorozat előállítása

### *Lineáris rekurrens reláció, lineáris rekurrens sorozatok*

A léptető regiszter generátor általános tömbvázlata az 1. ábrán látható. A $K_i$ kapcsolók azt jelképezik, hogy van-e visszacsatolás az $i$-edik tároló kimenetéről, vagy nincs. A mod 2 összeadók a visszacsatoló áramkörök. Jelöljük $a_k$-val a léptető regiszter generátor által előállított jelsorozat $k$-adik elemét, $c_i$ a visszacsatolási koefficiens, amely 1, ha az $i$-edik fokozatról visszacsatolunk, és 0, ha nem.




*1. ábra.* Álvéletlen bináris sorozatot előállító visszacsatolt léptető regiszter generátor általános tömbvázlata

n=4 esetén például a 2*a* ábrának megfelelően alakul a léptető regiszter generátor.

E fogalmak és jelölések bevezetése után a következők mondhatók:

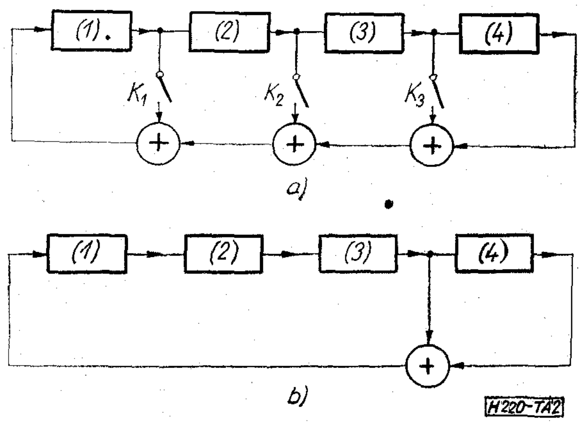
$a_k$ kielégíti a következő egyenletet:

$$a_k = c_1 a_{k-1} + c_2 a_{k-2} + \dots + c_n a_{k-n} = \sum_{i=1}^{n} c_i a_{k-i} \qquad (1)$$

ahol

$$0 < k \leqq 2^n - 1 \text{ egy cikluson belül.}$$

Az egyenletben szereplő összeadás mod 2 műveletet jelöl. Az (1) összefüggést lineáris rekurrens relációnak és bármelyik $\{a_k\}$ sorozatot, amely ezt kielégíti, lineáris rekurrens sorozatnak nevezzük.




*2. ábra*
*a)* Visszacsatolt léptető regiszter generátor 4 tárolóval, ahol $K_1$ vagy $K_3$ rövidzár
*b)* Egyszerűsített visszacsatolt léptető regiszter generátor 4 tárolóval

Visszatérve példánkra, a 2*a* ábra alapján a következő írható:

$$a_k = 0 \cdot a_{k-1} + 0 \cdot a_{k-2} + 1 \cdot a_{k-3} + 1 \cdot a_{k-4},$$

$$a_k = a_{k-3} + a_{k-4}.$$

Tehát az (1) összefüggés alapján a jelsorozat $k$-adik eleme meghatározható, ha ismert az ezt megelőző 3. és 4. elem.

Például, ha $k=9$, $a_k = a_9$, $a_9 = a_6 + a_5$.

Az 1. táblázat első oszlopának értékei alapján:

$$a_9 = 1,\ a_6 = 0,\ a_5 = 1,\ a_5 + a_6 = 0 + 1 = 1.$$

Nem szabad elfelejteni, hogy itt és a későbbiekben is az összeadás művelete alatt mod 2 műveletet értünk.

*1. táblázat*

| |
|---|
| 1000 |
| 0100 |
| 0010 |
| 1001 |
| 1100 |
| 0110 |
| 1011 |
| 0101 |
| 1010 |
| 1101 |
| 1110 |
| 1111 |
| 0111 |
| 0011 |
| 0001 |

Ahol visszacsatolás nincs, mod 2 összeadó nem is szükséges (2*b* ábra).

Vizsgáljuk ebben az esetben valamelyik tároló kimenetén megjelenő jelsorozatot. Tegyük fel, hogy ismerjük az egy perióduson belüli állapotokat, ezek rendre:

$$a_1, a_2, \ldots, a_k, \ldots, a_{2^n-1}.$$

Példánkban, ha feltételezzük, hogy a regiszter kezdeti állapota 1000, akkor egy ciklus az 1. táblázatnak megfelelően alakul. A táblázat alapján pl. az 1. tároló kimeneti jele:

$$\ldots . 100110101111000 \ldots .$$

Ha $K_i$ zárt, akkor $c_i=1$, ha $K_i$ nyitott, akkor $c_i=0$, továbbá $c_n=1$, mivel az n fokozatú léptető regiszter n-edik kimenetéről mindig történik visszacsatolás ahhoz, hogy $N=2^n-1$ maximális hosszúságú bináris álvéletlen sorozatot kapjunk (ld. 1. ábra), így a $K_n$ kapcsolót rövidzár helyettesíti.

## Generátorfüggvény, karakterisztikus polinom

A rekurrens sorozatok vizsgálatának két módszere van:

generátorfüggvények módszere,
mátrix módszer.

Ha a léptető regiszter egyetlen tárolójának kimeneti jelét vizsgáljuk csak, akkor a generátorfüggvények módszerét alkalmazzuk. Ha a teljes léptető regisztert vizsgáljuk, amelynek kimeneti jelsorozata kielégíti a rekurrens relációt, akkor a mátrix módszert alkalmazzuk.

### *Generátorfüggvények módszere*

Legyen adott az

$$\{a_k\}_{k=0}^{\infty}$$

sorozat, amely például a léptető regiszter 1. tárolójának kimeneti jelsorozata, akkor a generátorfüggvény a következőképpen definiálható:

$$G(x)=\sum_{k=0}^{\infty} a_k x^k,$$

ahol $x$ a generátorfüggvény változója, amely 1 és 0 lehet.

A léptető regiszter kezdeti állapotának tekinthetjük az

$$a_{-1}, a_{-2}, a_{-3}, \ldots\ldots\ldots, a_{-n}$$

sorozatot.

Ha $\{a_k\}$ kielégíti a rekurrens relációt:

$$a_k=\sum_{i=1}^{n} c_i a_{k-i},$$

akkor

$$G(x)=\sum_{k=0}^{\infty}\sum_{i=1}^{n} c_i a_{k-i} x^k=\sum_{i=1}^{n} c_i x^i \sum_{k=0}^{\infty} a_{k-i} x^{k-i}=$$

$$=\sum_{i=1}^{n} c_i x^i [a_{-i}x^{-i}+\ldots+a_{-1}x^{-1}+\sum_{k=0}^{\infty} a_k x^k],$$

így

$$G(x)=\sum_{i=1}^{n} c_i x^i [a_{-i}x^{-i}+\ldots+a_{-1}x^{-1}+G(x)],$$

és

$$G(x)=\sum_{i=1}^{n} c_i x^i G(x)+\sum_{i=1}^{n} c_i x^i [a_{-i}x^{-i}+\ldots+a_{-1}x^{-1}].$$

$G(x)$-re rendezve:

$$G(x)=\frac{\sum_{i=1}^{n} c_i x^i [a_{-i}x^{-i}+\ldots+a_{-1}x^{-1}]}{1-\sum_{i=1}^{n} c_i x^i}. \qquad (2)$$

Láthatjuk, hogy a generátorfüggvény a léptető regiszter kezdeti állapotával: $a_{-1}, a_{-2}, \ldots, a_{-n}$-nel és a visszacsatoló koefficiensekkel: $c_1, c_2, \ldots, c_n$-nel van kifejezve. (2) nevezője független a kezdeti állapottól.

Ha kiindulásként feltételezzük, hogy

$$a_{-1}=a_{-2}=\ldots=a_{1-n}=0 \text{ és } a_{-n}=1,$$

akkor (2) a következőképpen redukálódik:

$$G(x)=\frac{c_n}{1-\sum_{i=1}^{n} c_i x^i}.$$

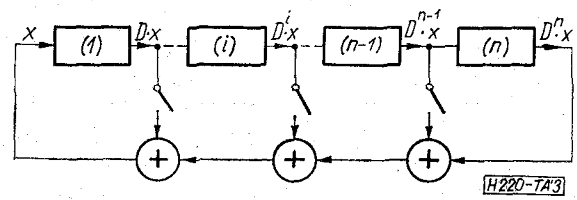
A generátorfüggvény nevezőjének n-ed fokú polinomját a léptető regiszter által előállított $\{a_k\}$ sorozat karakterisztikus polinomjának nevezzük:

$$f(x)=1-\sum_{i=1}^{n}{}' c_i x^i. \qquad (3)$$

A karakterisztikus polinomnak számunkra értékes további alakjaihoz juthatunk el, ha a következő megfontolásokat tesszük [4, 5].

A léptető regiszter felfogható tulajdonképpen mint késleltető vonal, hiszen a bemenetére adott $x$ jel óraimpulzusonként lép egy fokozattal tovább. Tehát például az $i$-edik tároló kimenetén az $i \cdot \Delta T$ idővel korábban a bemenetre adott jel van.

Így a visszacsatolt léptető regiszter generátorunk mod 2 összeadóinak bemenetein is a bemeneti jel késleltetettjei vannak.




*3. ábra.* Magyarázó ábra a **D** késleltetési operátorhoz

A 3. ábrán látható áramkörre felírható a következő egyenlőség:

$$x=c_1\mathbf{D}x+c_2\mathbf{D}^2x+\ldots+c_i\mathbf{D}^i x+\ldots+c_n\mathbf{D}^n x, \quad (4)$$

ahol a $\mathbf{D}^i$ szimbólum algebrai operátor, neve késleltetési operátor. Azt az időt reprezentálja, ami ahhoz kell, hogy az $i$-edik tárolóba a bemeneti jel beíródjon. Ez az idő az ütemidő egész számú többszöröse.

Adjunk (4) mindkét oldalához $x$-et, ekkor kapjuk:

$$0=x+c_1\mathbf{D}x+c_2\mathbf{D}^2x+\dots+c_i\mathbf{D}^ix+\dots+c_n\mathbf{D}^nx, \tag{5}$$

és vezessük be a következő operátort:

$$\mathbf{I}=\mathbf{D}^0.$$

Emeljük ki $x$-et (5) jobb oldalából:

$$0=x[1+c_1\mathbf{D}+c_2\mathbf{D}^2+\dots+c_n\mathbf{D}^n],$$

$$0=x[1+\sum_{i=1}^{n}c_i\mathbf{D}^i].$$

Ennek az egyenletnek a jobb oldalát nevezzük karakterisztikus polinomnak.

Mivel $c_i$ értéke 0 vagy 1 lehet, az összegzésen belül csak azok a tagok szerepelnek, amelyeknek visszacsatolási koefficiensei 1-gyel egyenlők.

Tehát

$$f(x)=x[1+\sum_j \mathbf{D}^j],$$

ahol $j$ azon léptető regiszter-tárolókat jelöli, amelyekről a visszacsatolás történik.

Tekintsük a korábbiakban említett példát (n=4 a fokozatok száma, a léptető regiszter 3. és 4. tárolójáról történik visszacsatolás). Ekkor:

$$x=c_1\mathbf{D}x+c_2\mathbf{D}^2x+c_3\mathbf{D}^3x+c_4\mathbf{D}^4x,$$

$$c_1=c_2=0,$$

$$c_3=c_4=1,$$

$$x=\mathbf{D}^3x+\mathbf{D}^4x.$$

Mindkét oldalhoz $x$-et adva:

$$0=x+\mathbf{D}^3x+\mathbf{D}^4x,$$

tehát:

$$f(x)=x[\mathbf{I}+\mathbf{D}^3+\mathbf{D}^4],$$

$$G(x)=\frac{c_n}{f(x)}.$$

Minthogy $c_n=1$,

$$G(x)=\frac{\mathbf{I}}{\mathbf{I}+\mathbf{D}^3+\mathbf{D}^4}x=$$

$$=x[\mathbf{I}+\mathbf{D}^3+\mathbf{D}^4+\mathbf{D}^6+\mathbf{D}^8+\mathbf{D}^9+\mathbf{D}^{10}+\mathbf{D}^{11}+\mathbf{D}^{15}+\dots].$$

A zárójelen belüli kifejezés az álvéletlen sorozatot írja le. Ugyanis, ha minden tagot kiírunk $N=2^4-1=15$-ig:

$$1\cdot\mathbf{D}^0,\ 0\cdot\mathbf{D}^4,\ 0\cdot\mathbf{D}^2,\ 1\cdot\mathbf{D}^3,\ 1\cdot\mathbf{D}^1,\ 0\cdot\mathbf{D}^5,\ 1\cdot\mathbf{D}^6,\ 0\cdot\mathbf{D}^7,\ 1\cdot\mathbf{D}^8;$$

$$1\cdot\mathbf{D}^9,\ 1\cdot\mathbf{D}^{10},\ 1\cdot\mathbf{D}^{11},\ 0\cdot\mathbf{D}^{12},\ 0\cdot\mathbf{D}^{13},\ 0\cdot\mathbf{D}^{14},\ 1\cdot\mathbf{D}^{15},\ \dots$$

Ami pontosan ugyanaz, mint ami az 1. táblázat első oszlopában található:

1001101011110001 . . .

### *A periódus meghatározása*

Az előzőekben láttuk, hogy a visszacsatolt léptető regiszter által előállított bináris álvéletlen jel periodikus és a periódus felső határa $N=2^n-1$.

Vizsgáljuk meg, hogy ha egy n állapotú visszacsatolt léptető regiszter sorozata $A=\{a_k\}$, és kezdeti állapota $a_{-1}=a_{-2}=a_{1-n}=0$, $a_{-n}=1$, akkor $A$ periódusa az a legkisebb pozitív $N$ egész szám amelyre igaz, hogy $1-x^N$ osztható $f(x)$-szel.

Bizonyítás:

$$G(x)=\frac{1}{f(x)}=\sum_{k=0}^{\infty}a_kx^k=a_0x^0+a_1x+\dots+$$

$$+a_Nx^N+a_{N+1}x^{N+1}+\dots$$

Ha $A$ periódusa $N$, akkor

$$G(x)=[a_0+a_1x+\dots+a_{N-1}x^{N-1}]+$$

$$+x^N[a_0+a_1x+\dots+a_{N-1}x^{N-1}]+$$

$$+x^{2N}[a_0+a_1x+\dots+a_{N-1}x^{N-1}]+\dots=$$

$$=[a_0+a_1x+\dots+a_{N-1}x^{N-1}]\cdot$$

$$\cdot[1+x^N+x^{2N}+\dots]=$$

$$=\frac{a_0+a_1x+\dots+a_{N-1}x^{N-1}}{1-x^N},$$

ugyanis

$$1+x^N+x^{2N}+\dots=\frac{1}{1-x^N}\ \text{(lásd [6])}.$$

Így

$$f(x)=\frac{1-x^N}{a_0+a_1x+\dots+a_{N-1}x^{N-1}}.$$

Tehát $1-x^N$ osztható $f(x)$-szel, ha $A$ periódusa $N$. Viszont, ha $1-x^N$ osztható $f(x)$-szel, legyen a hányados:

$$\alpha_0+\alpha_1x+\dots+\alpha_{N-1}x^{N-1},$$

akkor $\{\alpha_k\}=\{a_k\}$.

$$\frac{1}{f(x)}=\frac{\alpha_0+\alpha_1x+\dots\alpha_{N-1}x^{N-1}}{1-x^N}=$$

$$=[\alpha_0+\alpha_1x+\dots+\alpha_{N-1}x^{N-1}]\cdot[1+x^N+x^{2N}+\dots]=$$

$$=[\alpha_0+\alpha_1x+\dots+\alpha_{N-1}x^{N-1}]+$$

$$+x^N[\alpha_0+\alpha_1x+\dots+\alpha_{N-1}x^{N-1}]+$$

$$+\dots=G(x)=\sum_{k=0}^{\infty}a_kx^k,$$

és $x$ hatványsorának koefficiense:

$$\{a_k\}=\{\alpha_k\}.$$

Tehát $A$-nak valóban $N$ a periódusa.

Következtetések:

(2) alapján

$$G(x)=\frac{g(x)}{f(x)},$$

ahol a számláló, $g(x)$ kisebb fokszámú, mint a nevező $f(x)$. Ha a léptető regiszter n fokozatú, akkor $f(x)$ n-ed fokú. Ha $N$ az a legkisebb egész szám, hogy $1-x^N$ osztható $f(x)$-szel, $N$-et $f(x)$ exponensének nevezzük.

### *A maximális hosszúságú sorozat szükséges feltétele*

Ha az $A$ sorozat maximális hosszúságú, akkor karakterisztikus polinomja irreducibilis $GF(2)$ felett.

Bizonyítás:

Tegyük fel, hogy $f(x)$ felbontható két tényező szorzatára:

$$f(x)=s(x)\cdot t(x).$$

Akkor

$$\frac{1}{f(x)}=\frac{\alpha(x)}{s(x)}+\frac{\beta(x)}{t(x)}.$$

Tegyük fel, hogy $s(x)$ és $t(x)$ fokszáma $n_1>0$ és $n_2>0$, $n_1+n_2=n$. $\frac{\alpha(x)}{s(x)}$ tehát egy hatványsor, amelynek koefficiensei ismétlődnek $2^{n_1}-1$ után és $\frac{\beta(x)}{t(x)}$ is egy hatványsor, amelynek koefficiensei $2^{n_2}-1$ után ismétlődnek.

Akkor az

$$\frac{1}{f(x)}=\frac{\alpha(x)}{s(x)}+\frac{\beta(x)}{t(x)}$$

összeg hatványsor koefficienseinek periódusa legfeljebb az egyes periódusok legkisebb közös többszöröse, amely nem lehet nagyobb a periódusok szorzatánál. Így tehát a tétel alapján írható:

$$2^n-1\leq(2^{n_1}-1)\cdot(2^{n_2}-1)=2^{n_1+n_2}-2^{n_1}-2^{n_2}+1,$$

$$2^{n_1+n_2}=2^n, \quad \text{és}$$

$$2^n-2^{n_1}-2^{n_2}+1=2^n-1-[2^{n_1}+2^{n_2}-2],$$

ami mindenképp kisebb, mint $2^n-1$, tehát ellentmondáshoz jutottunk, ami tételünket igazolja.

A tétel akkor is igaz, ha $s(x)=t(x)$, azaz

$$f(x)=s^2(x).$$

Ekkor $f(x)$ periódusa $s(x)$ periódusának kétszerese, ami

$$2[2^{n/2}-1],$$

viszont

$$2[2^{n/2}-1]<2^n-1.$$

A tétel megfordítottja nem állítható — tehát az, hogy ha az $f(x)$ karakterisztikus polinom irreducibilis, akkor a hozzá tartozó $A$ sorozat maximális hosszúságú.

Például az

$$f(x)=1+x+x^2+x^3+x^4$$

karakterisztikus polinomról egyszerű osztással belátható, hogy $1-x^5$ osztható $f(x)$-szel, ami a korábbiak alapján azt jelenti, hogy $f(x)$ periódusa $N=5$, nem pedig $2^4-1=15$.

*A maximális hosszúságú sorozat szükséges és elégséges feltétele*

Ha a visszacsatolt léptető regiszter generátor karakterisztikus polinomja primitív, akkor a hozzá tartozó $A$ sorozat maximális hosszúságú.

A második követelmény, hogy a karakterisztikus polinom primitív is, már egy szorosabb megkötés. Primitívnek nevezzük az irreducibilis polinomot, ha $N=2^n-1$-re van olyan $f'(x)$ polinom, hogy

$$\frac{1-x^N}{f(x)}=f'(x),$$

és semmilyen $N'<N$ számra nem létezik az egyenletet kielégítő $f'(x)$.

Tehát a feladat, megkeresni az irreducibilis polinomok közül a primitíveket, ezek megadják a maximális hosszúságú sorozatokat előállító visszacsatolt léptető regiszter generátor karakterisztikus polinomjait.

A primitív és irreducibilis polinomokra táblázatot a [6] irodalomban találunk. Ha megvan a karakterisztikus polinom, a legnagyobb hatványkitevő a léptető regiszter tárolóinak számát és az egyik visszacsatolást, a többi hatványkitevő pedig a többi visszacsatolási helyet adja meg. Szemléltessük fenti állításainkat a következő példákkal:

*a*) Legyen adva a következő irreducibilis karakterisztikus polinom:

$$f(x)=1+x+x^2+x^3+x^4.$$

Korábban már említettük, hogy $1-x^5$ osztható a fenti $f(x)$-szel, így eredményül $N=5$ hosszúságú sorozatot kaptunk $2^4-1=15$ helyett. Tehát ez az irreducibilis polinom nem primitív.

*b*) Legyen adott az

$$f(x)=1+x^3+x^4 \tag{6}$$

irreducibilis karakterisztikus polinom.

Bizonyítható, hogy $1-x^{15}$ osztható $f(x)$-szel,

$$f'(x)=\frac{1-x^{15}}{1+x^3+x^4}=1-x^3-x^4+x^6+x^8-x^9-x^{10}-x^{11},$$

$$\text{és } 1-x^{N'} \text{ nem osztható } f(x)\text{-szel, ha } N'<15. \tag{7}$$

Mivel antivalencia képzés szempontjából mínusz és plusz között nincs különbség, (7) jobb oldala így is írható:

$$f'(x)=1+x^3+x^4+x^6+x^8+x^9+x^{10}+x^{11}.$$

Tehát a (6)-tal definiált karakterisztikus polinom irreducibilis és primitív.

## Összefoglalás

Összefoglalva az előbbieket:

- álvéletlen bináris hullámformák előállítása mod 2 összeadókkal visszacsatolt léptető regiszter segítségével történik;
- az előállított sorozatok periodikusak $2^n-1$ periódushosszal, ahol n a léptető regiszter tárolóinak száma;
- minden $\{a_k\}$ léptető regiszter sorozat kielégíti a lineáris rekurrens relációt:

$$a_k=\sum_{i=1}^{n}c_i a_{k-i},$$

ahol $c_i$ visszacsatolási koefficiens $-1$ vagy 0 értéket vehet fel —, a tárolók visszacsatolására jellemző;
- a léptető regiszter generátor-függvénye

$$G(x)=\sum_{k=0}^{\infty}a_k x^k=\frac{g(x)}{f(x)}$$

alakban írható, ahol a számláló legfeljebb (n – 1)-ed fokú polinom, a nevező:

$$f(x) = 1 - \sum_{i=1}^{n} c_i x^i$$

a karakterisztikus polinom;

— a léptető regiszter sorozatának periódusa az a legkisebb pozitív $N$ egész szám, amellyel képzett $1 - x^N$ osztható $f(x)$-szel;

— $f(x)$-nek primitívnek kell lennie ahhoz, hogy a hozzá tartozó visszacsatolt léptető regiszter maximális hosszúságú jelsorozatot állítson elő.

## IRODALOM


[1] Dr. *Gordos G.—Sallai Gy.*: Híranyagok természetes és összetett jeleinek statisztikai tulajdonságai. Híradástechnika, XXIII. évf. 9. szám, 257—269. old. (1972. szept.).

[2] Dr. *Ambrózy A.*: Elektronikus zajok. Műszaki Könyvkiadó, Budapest, 1972.

[3] *Tóth Á.*: Bináris és Gauss-amplitúdóeloszlású álvéletlen zajgenerátorok, előnyeik és alkalmazásuk. Híradástechnika, XXIII. évf. 2. szám, 46—49. old. (1972. febr.).

[4] *Curry, R. C.*: A method of obtaining arbitrary phases of an M-sequence. The University of Rochester, Department of Electrical Engineering, Rochester, New York, 1960. nov.

[5] *Davies, W. D. T.*: Generation and properties of maximum length sequences. Control, 1966. jún. p. 302—304; 1966. júl. p. 364—365; 1966. aug. p. 431—433.

[6] *Peterson, W. W.*: Error Correcting Codes. John Wiley and Sons, Inc. New York, 1961.

[7] *Soloman, W. G.*: Shift register sequences. Holden—Day Inc. San Francisco, 1967.