K szimbólumból képezett pszeudovéletlen sorozatok

BSc Szakdolgozat

Deák Attila

Alkalmazott matematikus szak

Témavezető:

Sárközy András, Professzor Emeritus és Gyarmati Katalin, adjunktus

Algebra és Számelmélet Tanszék
Eötvös Loránd Tudományegyetem, Természettudományi Kar

Eötvös Loránd Tudományegyetem
Természettudományi Kar
2014

Tartalomjegyzék

1. fejezet

Bevezetés

„A véletlen sorozat bizonytalan fogalmán olyan sorozatot értünk, amelynek későbbi elemeit az avatatlan személy nem tudja megjósolni; továbbá jól vizsgázik néhány szokásos statisztikai próbán; ezeknek a próbáknak a megválasztása némileg attól is függ, mire akarjuk a sorozatot használni." (D.H.Lehmer)

A kriptográfiában rendkívül fontos szerepet játszanak a valamilyen értelemben véletlen bit sorozatok. Ilyen sorozatok felhasználására épül az úgynevezett „Vernam cipher" titkosítási rendszer, amely Gilbert Sandford Vernam (1890-1960) amerikai matematikusról kapta a nevét.

A módszer ismertetéséhez vegyünk egy $A_M = \{a_1, ..., a_M\} \in \{0,1\}^M$ bitsorozatot (titkosítandó információ), majd tekintsünk egy $E_M = \{e_1, ..., e_M\} \in \{0,1\}^M$ véletlen vagy pszeudovéletlen bitsorozatot (a „one time pad"[1] a Vernam cipher speciális esete, amikoris E_M véletlen). Az A_M titkosításához adjuk össze a_i, e_i $(i = 1, ..., M)$ elemeket modulo 2, így kapjuk a titkosított $F_M = \{f_1, ..., f_M\}$ szöveget, azaz $f_i = a_i \bigoplus e_i$ $(i = 1, ..., M)$, ahol a $\bigoplus$ művelet a bitenkénti összeadás modulo 2. Az E_M kulcs tudása nélkül F_M-ből nem nyerhető vissza A_M, de ha rendelkezünk vele, akkor könnyedén az $f_i \bigoplus e_i = a_i$ műveletet elvégezve visszanyerjük az eredeti információt.

Az eljárás hátránya, hogy az E_M sorozatnak ugyanolyan hosszúnak kell lennie, mint az A_M sorozatnak, az előnye a feltörhetetlenség, amely nagyban függ a kulcs véletlenségétől. Ehhez vehetünk egy véletlen bit generátort.

[1] másnéven egyszer használatos kulcs

DEFINÍCIÓ. *A véletlen bit generátor egy olyan algoritmus (készülék), amely statisztikusan független és torzítatlan biteket állít elő.*

A véletlen bit generátorokat napjainkban felváltotta a pszeudovéletlen bit generátorok használata.

DEFINÍCIÓ. *Egy pszeudovéletlen bit generátor ez egy olyan algoritmus, amely egy valóban véletlen k hosszú bináris sorozatot (mag) megadva, abból egy l hosszú ($l > k$) „véletlenszerűnek tűnő" bináris sorozatot (pszeudovéletlen bináris sorozat) készít.*

A kriptográfiai alkalmazásokban két fontos tulajdonságot keresünk a pszeudovéletlen bináris kulcsok esetében, az egyik az egyenletes 0-1 eloszlás, a másik a megjósolhatatlanság, ami alatt azt értjük, hogy ha adott a sorozatunkban k bit, akkor a következő (k+1)-edik bitet legfeljebb 1/2 valószínűséggel találhassuk ki.

DEFINÍCIÓ. *A pszeudovéletlen bit generátor kielégíti a „következő bit tesztet", ha nem létezik olyan polinomiális algoritmus, amelyre az első k jegy ismeretében a (k+1)-edik jegy 1/2-nél lényegesen nagyobb valószínűséggel megjósolható.*

A definíciónak több hibája is van. Az egyik, hogy a nem létezés bizonyítása legtöbbször lehetetlen feladat, másrészről pszeudovéletlen generátorokat minősít és nem pszeudovéletlen sorozatokat, így ez nem használható a gyakorlatban. Emiatt C. Maudit és A. Sárközy 1997-ben kifejlesztett egy új elméletet bináris sorozatok pszeudovéletlenségére [1].

Jelen szakdolgozatom célja ennek az elméletnek a bemutatása, illetve általánosítása $k-$szimbólumok, azaz k elemű halmazból vett sorozatok esetére. Az 2. fejezetben bináris sorozatokkal foglalkozom, majd a 3. fejezettől térek ki a $k-$szimbólumok részletezésére, és a legvégén egy alkalmazott matematikai feladat leprogramozásával zárom le a témát.

A szakdolgozatban technikai okokból a 0-1 sorozatok helyett a ± 1 sorozatokat vizsgálom (az ilyen sorozatok között egy-egy értelmű megfeleltetés létesíthető).

Az. 6. fejezetben szereplő feladatok kiszámítására a MAPLE programot használtam.

2. fejezet

A pszeudovéletlen bináris sorozatok[1]

2.1. A pszeudovéletlen bináris sorozatok mértékei

Mielőtt definiálnánk bináris sorozatok pszeudovéletlenségének C. Mauduit és A. Sárközy által 1997-ben [1] bevezetett különböző kvantitatív mértékeit, megadjuk, hogy mik azok a véletlenségi tulajdonságok, amiket elvárunk majd ezektől, a később bemutatott mértékektől. Legelőször három tulajdonságot adunk meg, ezek a következőek :

1. *normalitás;*
2. *számtani sorozatok mentén egyenletes eloszlás;*
3. *kis rendű korreláció.*

Vegyünk egy végtelen $E = (e_1, e_2, ...)$ sorozatot, amelynek elemei a $\{-1, 1\}$ halmazból származnak. Legyen $k, M, b \in \mathbb{N}$, $X = (x_1, ..., x_k) \in \{-1, 1\}^k$, $a \in \mathbb{Z}$ és $D = (d_1, ..., d_k) \in \mathbb{N}^k$, $d_1 < ... < d_k$. Ekkor használjuk az alábbi jelöléseket :

- $T(E, M, X) = |\{n : 0 \leq n < M, (e_{n+1}, e_{n+2}, ..., e_{n+k}) = X\}|$ (2.1)
- $U(E, M, a, b) = \sum_{j=1}^{M} e_{a+jb}$ (2.2)
- $V(E, M, D) = \sum_{n=0}^{M-1} e_{n+d_1} ... e_{n+d_k}$ (2.3)

[1] A könnyebb szóhasználat érdekében, pontosabban erős pszeudovéletlen tulajdonságokkal rendelkező bináris sorozatok.

Az E normalitási tulajdonsága teljesül (Knuth [5] használta még a $\infty - eloszlású$ kifejezést is), ha $|T(E,M,X) - \frac{M}{2^k}| = o(M)$, fix k-ra, M-re, ahol $M \to \infty$; ezenkívül a másik két tulajdonságra is igaz, hogy $U(E,M,a,b) = o(M)$, $V(E,M,D) = o(M)$, fix a,b,D-re és $M \to \infty$. Ebből a normalitási tulajdonságából (E normalitása) következik Niven és Zuckermann [25] szerint, hogy E teljesíti a 2. fent említett tulajdonságot, azaz E-t $(m,k) - eloszlásúnak$ mondjuk $(k,m \in \mathbb{N})$, másszóval E normális, mint a számtani sorozatok m differenciával és k szóhosszal. Ebből azt is látjuk, hogy a végtelen bináris sorozatok esetében elegendő a normáltsági tulajdonság teljesítése.

Most térjünk rá a véges bináris sorozatok esetére. Knuth az alábbi módon definiálta véges bináris sorozat pszeudovéletlenségét [5].

2.1.1 Definíció. Adott $E_N = (e_1, e_2, ..., e_N) \in \{-1,1\}^N$ véges bináris sorozatot pszeudovéletlennek mondjuk, ha bármely $k \in \mathbb{N}$, $k \leq \frac{logN}{log2}$, és bármely $X \in \{-1,1\}^k$ sorozatra teljesül, hogy $\left|T(E_N, N+1-k, X) - \frac{N+1-k}{2^k}\right| \leq \frac{1}{\sqrt{N}}$.

Ez a defíníció arra enged minket következtetni, hogy egy sorozat vagy „jó" (azaz pszeudovéletlen) vagy „rossz" (azaz nem pszedovéletlen) lehet. Előfordulhat azonban olyan eset, hogy a 2.1.1 Definícióban szereplő egyenlőtlenség nem teljesül, de $\frac{2}{\sqrt{N}}$-re például az egyenlőség érvényessége megmarad, ilyenkor a sorozat nem feltétlenül elvetendő.

Ezokból kifolyólag szükségünk van további véletlenségi tulajdonságokra.

4. *A bináris sorozatok pszeudovéletlenségének kifejezhetőnek kell lennie egy valós értékű, az összes véges bináris sorozaton értelmezett függvény által.*

Egy újabb következmény legyen, hogy

5. *a 4.-ben említett függvénynek jól becsülhetőnek kell lennie, legalább bizonyos „szép" sorozatok esetében.*

És a legvégső követelményünk pedig

6. *ennek a pszeudovéletlenségi mértéknek legyenek különböző szintjei, és képesnek kell lenniük legalább az alacsony rendű mértékek becslésére.*

Most már bemutathatjuk az általunk később sokat használt pszeudovéletlenségi mértékeket. Legelőször is azokat adjuk meg, amelyek teljesítik a fent említett 1-3. véletlenségi tulajdonságokat.

Ehhez vegyünk egy véges bináris $E_N = (e_1, ..., e_N) \in \{-1, 1\}^N$ sorozatot.

2.1.2. Definíció. Az E_N k-rendű normális mértéke :

$$N_k(E_N) = \max_{X \in \{-1,1\}^k} \max_{0<M \leq N+1-k} |T(E_N, M, X) - \tfrac{M}{2^k}|. \tag{2.4}$$

2.1.3. Definíció. Az E_N normális mértéke :

$$N(E_N) = \max_{k \leq \frac{logN}{log2}} N_k(E_N). \tag{2.5}$$

2.1.4. Definíció. Az E_N eloszlási mértéke :

$$W(E_N) = \max_{a,b,t} |U(E_N, t, a, b)|, \text{ ahol } a \in \mathbb{Z}, b, t \in \mathbb{N} \text{ és } 1 \leq a + b \leq a + tb \leq N. \tag{2.6}$$

2.1.5. Definíció. Az E_N k-rendű korrelációs mértéke :

$$C_k(E_N) = \max_{M,D} |V(E_N, M, D)|, \text{ ahol } D = (d_1, ..., d_k) \text{ és } M + d_k \leq N. \tag{2.7}$$

2.1.6. Definíció. Az E_N korrelációs mértéke :

$$C(E_N) = \max_{k \leq \frac{logN}{log2}} C_k(E_N) \text{ vagy } C^*(E_N) = \sum_{k=1}^{\infty} \frac{C_k(E_N)}{2^k}. \tag{2.8}$$

2.1.7. Definíció. Az E_N k-rendű kombinált mértéke :

$$Q_k(E_N) = \max_{a,b,t,D} |Z(a, b, t, D)| \text{ , ahol } |Z(a, b, t, D)| = \sum_{j=0}^{t} e_{a+jb+d_1} ... e_{a+jb+d_k} \text{ és}$$
$$a \in \mathbb{Z}, b, t \in \mathbb{N}, D = (d_1, ..., d_k),\ a + jb + d_l \in \{1, ..., N\}. \tag{2.9}$$

2.1.8. Definíció. Az E_N kombinált mértéke :

$$Q(E_N) = \max_{k \leq \frac{logN}{log2}} Q_k(E_N) \text{ vagy } Q^*(E_N) = \sum_{k=1}^{\infty} Q_k(E_N)/2^k. \tag{2.10}$$

A (2.9) és a (2.10) mértékek a (2.6)-(2.7) és a (2.6)-(2.8) mértékek kombinációja révén keletkeztek.

Az alábbi állításban összehasonlítjuk a $t-$*rendű* korrelációs mértékét és a $k-$*rendű* normális mértékét egy adott véges $E_N \in \{-1,1\}^N$ sorozatnak. Emiatt a későbbiekben elég a korrelációs mértékkel (és az eloszlási mértékkel) foglalkoznunk.

2.1.9. Állítás. Bármely N, E_N és $k < N$ esetén $N_k(E_N) \leq \max\limits_{1\leq t\leq k}|C_t(E_N)|$.

Bizonyítás. Bármely $k, N \in \mathbb{N}$ és $X = (x_1, ..., x_k) \in \{-1,1\}^k$, $1 \leq M \leq N+1-k$ mellett igaz a (2.1) felhasználva, hogy

$$|T(E_N, M, X) - \tfrac{M}{2^k}| = \left||\{n : 0 \leq n < M, (e_{n+1}, ..., e_{n+k}) = X\}| - \tfrac{M}{2^k}\right| =$$

$$= \left|\sum_{n=0}^{M-1} \tfrac{x_1...x_k}{2^k} \prod_{j=1}^{k} (e_{n+j}+x_j) - \tfrac{M}{2^k}\right| = \left|\tfrac{x_1...x_k}{2^k} \sum_{1\leq d_1<...<d_t\leq k} \Big(\prod_{j\in\{1,...,k\}\setminus\{d_1,...,d_t\}} x_j\Big) \sum_{n=0}^{M-1} e_{n+d_1}...e_{n+d_t}\right| \leq$$

$$\leq \tfrac{1}{2^k} \sum_{\substack{D\neq\varnothing \\ D\subset\{1,2,...,k\}}} |V(E_N, M, D)| \leq \tfrac{1}{2^k} \sum_{t=1}^{k} \tbinom{k}{t} C_t(E_N) \leq \max_{1\leq t\leq k} |C_t(E_N)|.$$ Ahol felhasználtuk a (2.3) és (2.7) közti összefüggést. ■

Ezekután adjunk példát olyan esetre, hogy az E_N normális mértéke és az eloszlási mértéke is kicsi, de a korrelációs mértéke nagyon nagy.

2.1.10. Példa. Adott egy véges bináris sorozat, $E_N \in \{-1,1\}^N$, amelynek a normális mértéke és az eloszlási mértéke lehetőleg legyen kicsi. Majd megadunk egy másik véges bináris sorozatot, $E'_{2N} = (e'_1, ..., e'_{2N}) \in \{-1,1\}^{2N}$, ahol

$$e'_n = \begin{cases} e_n, & 1 \leq n \leq N \\ e_{n-N}, & N < n \leq 2N \end{cases}.$$

Ekkor mind a normális mértéke, mind az eloszlási mértéke E'_{2N}-nek kisebb egy konstans szorzóval, mint E_N esetében, viszont $C_2(E'_N) \geq |\sum\limits_{n=1}^{N} e'_n e'_{n+N}| = N$.

Következmény. Ahhoz, hogy egy véges bináris sorozatot pszeudovéletlennek nevezzünk abban az értelemben, hogy a fent említett 1-3. véletlenségi tulajdonságokat teljesíti elég, ha belátjuk, hogy az eloszlási mérték és a korrelációs mérték kicsi.

Vegyünk ismételten egy $E_N \in \{-1,1\}^N$ véletlen bináris sorozatot, ahol az egyes elemeket $1/2^N$ valószínűséggel választottuk, ekkor a 2.1.9. és 2.1.10. tételben megmutatjuk, hogy az eloszlási mérték és a $k-$rendű korrelációs mérték nagyjából $\sqrt{N}$ körül

ingadozik. Ezen tételek bizonyításából csak az i.) pontok bizonyítását közöljük, a ii.) pontok bizonyítása megtalálható a [8] cikkben.

2.1.11. Tétel. Bármely $\varepsilon > 0$ mellett létezik olyan $N_0 = N_0(\varepsilon)$ és $\delta = \delta(\varepsilon)$, hogy $N > N_0$ esetén

$$\text{i.)}\ P(W(E_N) > \delta N^{1/2}) > 1 - \varepsilon,$$

$$\text{ii.)}\ P(W(E_N) > 6(NlogN)^{1/2}) < \varepsilon.$$

Bizonyítás.

Mivel $W(E_N) \geq |U(E_N, N, 1, 1)| = \left|\sum_{j=1}^{N} e_j\right|$, ezért

$$P(W(E_N) > \delta N^{1/2}) \geq P(\left|\sum_{j=1}^{N} e_j\right| > \delta N^{1/2}).$$

Így elég belátni, hogy $P(\left|\sum_{j=1}^{N} e_j\right| > \delta N^{1/2}) > 1 - \varepsilon$.

Ha $h = |\{j : 1 \leq j \leq N, e_j = -1\}|$, akkor (2.11)

$$\sum_{j=1}^{N} e_j = |\{j : 1 \leq j \leq N, e_j = 1\}| - |\{j : 1 \leq j \leq N, e_j = -1\}| = N - 2h.$$

Mivel a (2.11) sorban szereplő egyenlőség $\frac{1}{2^N}\binom{N}{h}$ valószínűséggel teljesül,

$$P(\left|\sum_{j=1}^{N} e_j\right| > \delta N^{1/2}) = \frac{1}{2^N} \sum_{h:|N-2h|>\delta N^{1/2}} \binom{N}{h}. \tag{2.12}$$

Azonban a binomiális eloszlásról ismertek miatt, bármely $\varepsilon > 0$-hoz létezik egy $\eta = \eta(\varepsilon) > 0$, hogy

$$\sum_{h:|h-N/2|>\eta N^{1/2}} \binom{N}{h} > (1 - \varepsilon)2^N. \tag{2.13}$$

Ha $\delta = 2\eta(\varepsilon)$ használunk, akkor a (2.12) és (2.13) sorokból megkapjuk, amit szerettünk volna belátni. ■

2.1.12. Tétel. Minden $k \in \mathbb{N}, k \geq 2$ és bármely $\varepsilon > 0$ mellett létezik olyan $N_0 = N_0(\varepsilon, k)$ és $\delta = \delta(\varepsilon, k)$, hogy $N > N_0$ esetén

$$\text{i.)}\ P(C_k(E_N) > \delta N^{1/2}) > 1 - \varepsilon,$$

$$\text{ii.)}\ P(C_k(E_N) > 5(kNlogN)^{1/2}) < \varepsilon.$$

Bizonyítás.

i.) Triviálisan adódik (2.7) felhasználva, hogy

$$P(C_k(E_N) > \delta N^{1/2}) \geq P(\left|\sum_{n=1}^{[N/2]-k} e_n e_{n+1}...e_{n+[N/2]}\right| > \delta N^{1/2}). \tag{2.14}$$

Ezért elég belátni, hogy (2.14) jobb oldala nagyobb, mint $(1 - \varepsilon)$.

Bármely $u = (e_n, ..., e_{n+k-2})$ esetén írjunk $f_n = e_n...e_{n+k-2}$ és $f_n g_n = e_{n+[N/2]}$.

Emiatt

$$\left|\sum_{n=1}^{[N/2]-k} e_n e_{n+1}...e_{n+[N/2]}\right| = \sum_{n=1}^{[N/2]-k} g_n, \text{ ahol } g_n \in \{-1, 1\}.$$

Az $e_n, ..., e_{n+k-2}$ és így g_n elemeit $1/2$ valószínűséggel választjuk, ezért

$$P(\left|\sum_{n=1}^{[N/2]-k} g_n\right| > \delta N^{1/2}) > 1 - \varepsilon.$$

Írjunk ismét $|\{n : 1 \leq n \leq [N/2] - k, e_n = -1\}| = h$-t. Ekkor

$$\sum_{n=1}^{[N/2]-k} g_n = [N/2] - k - 2h \text{ és } P(\left|\sum_{n=1}^{[N/2]-k} g_n\right| > \delta N^{1/2}) =$$

$$= \sum_{h:|(1/2)([N/2]-k)-h|>(\delta/2)N^{1/2}} \frac{1}{2^{[N/2]-k}} \binom{[N/2]-k}{h}. \tag{2.15}$$

Fix k és elég kicsi $\delta = \delta(\varepsilon)$ és $N > N_0(\varepsilon, k)$ mellett (2.15) választás valóban nagyobb, mint $1 - \varepsilon$. Felhasználva, hogy (2.14) alsó becslése egyértelmű bármely $e_1, ..., e_{[N/2]}$ választás esetén, a bizonyítást befejeztük. ■

Alakítsuk most át a 2.1.10. Példát olyan értelemben, hogy a véges bináris E_N sorozat tagjaira

$$e_n^{'} = \begin{cases} e_n, & 1 \leq n \leq N \\ e_{2N-n}, & N \leq n \leq 2N \end{cases}$$

elemeket vegyük. Megtartva a 2.1.10. Példa feltételeit ekkor azt tapasztaljuk, hogy $E_{2N}^{'}$ korrelációs mértéke és eloszlási mértéke kisebb egy konstans szorzóval, mint E_N-nek. Így $E_{2N}^{'}$-et pszeudovéletlen sorozatnak kellene tekintenünk, viszont ez ellentmond $E_{2N}^{'}$ szimmetriájának. Ebből adódóan, ha egy véges sorozat tartalmaz egy viszonylag nagy szimmetrikus részsorozatot, akkor nem lehet tipikus véletlen sorozat.

Következmény. Ezek a meggondolások azt is mutatják, hogy a mértékek közt nincsen egy univerzálisan jó, hanem az egyes mértékek az alkalmazások jellegétől függően kaphatnak nagyobb hangsúlyt.

Végül bevezetjük az utolsó bináris sorozatoknál használt mértéket, amelyet az előzőekben leírt szimmetria probléma inspirált. A (2.16) mértékét csak megemlítjük érdekesség gyanánt, a későbbiekben nem használjuk.

2.1.13. Definíció. Az E_N szimmetria mértéke :

$$S(E_N) = \max_{a<b} |H(E_N, a, b| = \max_{a<b} \left| \sum_{j=0}^{[(b-a)/2]-1} e_{a+j} e_{b-j} \right|, \text{ ahol } 1 \leq a < b \leq N. \tag{2.16}$$

Megjegyzés. A [9] cikkben a K. Gyarmati megmutatta, hogy egy véletlen E_N sorozat szimmetria mértéke $\sqrt{N}$ körüli.

2.2 A Legendre szimbólum pszeudovéletlensége

Ebben a részben alkalmazzuk a 2.1.6. Definícióban bevezetett korrelációs mértéket; egy Legendre szimbólumok felhasználásával konstruált sorozat vizsgálatára fogjuk alkalmazni, mint ezt az alábbi tétel mutatja.

2.2.1. Tétel. Adott p_0 olyan, hogy ha $p > p_0$ prímszám, $k \in \mathbb{N}, k < p$, és ha $E_{p-1} = ((\frac{1}{p}), (\frac{2}{p}), ..., (\frac{p-1}{p}))$ Legendre szimbólumok sorozata, akkor

$$Q_k(E_{p-1}) \leq 9kp^{1/2}logp.$$

Azaz $N = p - 1$ helyettesítés esetén

$$Q(E_N) = \max_{k \leq \frac{logN}{log2}} Q_k(E_N) \leq 27N^{1/2}(logN)^2 \text{ és } Q^\star(E_N) = \sum_{k=1}^{\infty} \frac{Q_k(E_N)}{2^k} \leq 33N^{1/2}logN.$$

Az 2.2.1.Tétel bizonyítása során a következő tételt használjuk majd fel, amelyet csak kimondunk, nem bizonyítunk. A bizonyítás (amely A. Weil egy mély tételére épül) megtalálható a [1] cikkben.

2.2.2. Tétel. Legyen p prímszám, χ egy $d-rendű$ nem főkarakter modulo p (azaz $d|p-1$), $f(x) \in F_p[x]$ egy $k-fokú$ polinom és $f(x) = b(x-x_1)^{d_1}...(x-x_s)^{d_s}$ $\overline{F_p} - ben$, ahol $x_i \neq x_j (i \neq j)$ és $(d, d_1, ..., d_s) = 1$. Emellett vegyünk X, Y valós számokat $(0 < Y \leq p)$. Ekkor $\left| \sum_{X<n\leq X+Y} \chi(f(n)) \right| < 9kp^{1/2}logp.$

2.2.3. Következmény. Ha p,$f(x)$, mint 2.2.2. Tételben, de nem $f(x) \in b(g(x))^2$ alakú ($b \in F_p$, $g(x) \in F_p[x]$). Emellett X, Y valós számok $(0 < Y \leq p)$, ekkor

$$\chi_p^\star = \begin{cases} (n/p), & (n,p) = 1 \\ 0 & p|n \end{cases} \text{ esetén } \left| \sum_{X<n\leq X+Y} \chi_p^\star(f(n)) \right| < 9kp^{1/2}logp.$$

Bizonyítás(2.2.2. Tétel). A bizonyításhoz szükségünk lesz még két lemmára, amelyeket csak felhasználunk, nem bizonyítunk. A bizonyítások megtalálhatóak a [10] és [11] cikkekben.

2.2.4. Lemma. Ha $p, \chi, d, f(x), k$ mint a 2.2.2.Tétel szerint és $a \in \mathbb{Z}$, akkor

$$\left| \sum_{x \in F_p} \chi(f(x)) e(\tfrac{ax}{p}) \right| \leq kp^{1/2}.$$

2.2.5. Lemma. Ha $m \in \mathbb{N}$,$g(x) : \mathbb{Z} \to \mathbb{C}$ m periódusú függvény és X, Y valós számok (Y>0), akkor

$$\left|\sum_{X<n\leq X+Y} g(n)\right| \leq \frac{Y+1}{m}\left|\sum_{n=1}^{m} g(n)\right| + \sum_{1\leq|h|\leq\frac{m}{2}} |h|^{-1}\left|\sum_{n=1}^{m} g(n)e(\tfrac{hn}{m})\right|.$$

Visszatérve a tétel bizonyításához, használjuk először a 2.2.5. Lemma állítását $p, \chi(f(n))$ helyett $m, g(n)$ jelöléssel, majd alkalmazzuk a 2.2.4. Lemma egyenlőtlenségét a következőképpen :

$$|\sum_{X<n\leq X+Y} \chi(f(n))| \leq \frac{Y+1}{p}|\sum_{n=1}^{p}\chi(f(n))| + \sum_{1\leq|h|\leq\frac{p}{2}} |h|^{-1}|\sum_{n=1}^{p}\chi(f(n))e(\tfrac{hn}{p})| <$$

$$< 2kp^{1/2} + 2\sum_{1\leq h\leq p/2} h^{-1}kp^{1/2} < 2kp^{1/2}(1+(1+log(\tfrac{p}{2}))) < 2kp^{1/2}(2+logp) \leq$$

$$\leq 2kp^{1/2}(2\frac{logp}{log2} + logp) < 9kp^{1/2}logp. \blacksquare$$

Végül rátérhetünk a Legendre szimbólumok korrelációs mértékéről szóló tételünk bizonyításához.

Bizonyítás(2.2.1. Tétel). Felhasznáva a 2.1.9. Definíciót kapjuk, hogy

$$|Z(a,b,t,D)| = |\sum_{n=0}^{t}(\tfrac{a+nb+d_1}{p})...(\tfrac{a+nb+d_k}{p})|,$$

bármely a, b, t esetén, $D = (d_1, ..., d_k)$ és $a + nb + d_l \in \{1, ..., p-1\}$ $(n = 0, ..., t;$ $l = 1, ..., k)$ mellett.

Ezután feltehetjük, hogy b és p relatív prímek és legyen $\overline{b}$ olyan egész szám, hogy $b\overline{b} \equiv 1$ $(mod$ p). Ezenkívül h_j $(j = 1, ..., k)$ jelölje azokat az egészeket, amelyekre $h_j \equiv (a + d_j)\overline{b}$ (mod p).

Ekkor h_i más maradékot ad p-vel osztva, mint h_j, ahol $1 \leq i < j \leq k$.

Így

$$|Z(a,b,t,D)| = |\sum_{n=0}^{t}(\tfrac{a\overline{b}+n+d_1\overline{b}}{p})...(\tfrac{a\overline{b}+n+d_k\overline{b}}{p})| = |\sum_{n=0}^{t}(\tfrac{n+h_1}{p})...(\tfrac{n+h_k}{p})| = |\sum_{n=0}^{t}(\tfrac{f(n)}{p})|,$$

ahol $f(n) := (n + h_1)...(n + h_k)$.

Felhasználva a 2.2.3.Következményt, $X = -1, Y = t+1$ $(0 < Y \leq t+1 \leq N+1 = p)$ mellett

$$|Z(a,b,t,D)| < 9kp^{1/2}logp,$$

így a 2.2.1. Tétel első részét bebizonyítottuk, a másik két rész ebből következik. ■

Megjegyzés. A 2.2.1.Tétel segítségével megmutattuk, hogy a Legendre szimbólumok „jó" pszeudovéletlen sorozatot alkotnak, azaz $N = p-1$, $e_n = (\frac{n}{p})$, $E_N = (e_1, ..., e_N)$ jelölés esetén $W(E_N) \ll p^{1/2}logp \ll N^{1/2}logN$ és $C_k(E_N) \ll kp^{1/2}logp \ll kN^{1/2}logN$.

Mivel a legtöbb alkalmazásban, pl. kriptográfiában „jó" pszeudovéletlen sorozatok nagy családjára van szükség, L. Goubin, C. Mauduit, A. Sárközy kiterjesztette a 2.2.1. Tételben szereplő konstrukciót [2].

Adjunk meg most ezt a második konstrukciót, legyen $e_n = (\frac{f(n)}{p})$, ahol $f(n)$ egy F_p feletti polinom. Ebben a konstrukcióban szeretnénk megbecsülni $W(E_p)$ és $C_l(E_p)$ értékeit. Ehhez legelőször is szükségünk van a megengedhetőség definíciójára.

2.2.6. Definíció. Ha $M \in \mathbb{N}$, $A, B \in \mathbb{Z}_m$ és az $A+B$ összeg $\mathbb{Z}_m$ összes elemét páros multiplicitással állítja elő, azaz bármely $c \in \mathbb{Z}_m$ esetén az $a + b = c$ $(a \in A, b \in B$) egyenletnek páros számú megoldása van (beleszámítva a triviális megoldást is), akkor az $A + B$ összeget $P - tulajdonságúnak$ nevezzük.

2.2.7. Definíció. Ha $k, l, m \in \mathbb{N}$ és $k, l \leq m$, akkor a (k, l, m) hármast megengedhetőnek hívjuk, ha $\nexists A, B \in \mathbb{Z}_m$, hogy $|A| = k$, $|B| = l$ és $A + B$ összeg $P - tulajdonságú$.

2.2.8. Tétel. Legyen p prímszám, $f(x) \in F_p[x]$ $k-fokú$ $(k > 0)$ polinom, amelynek nincs többszörös gyöke $\overline{F}_p - ben$ és $E_p = (e_1, ..., e_p)$ olyan bináris sorozat, amelynek elemeire teljesül, hogy $e_n = \begin{cases} (f(n)/p), & (f(n), p) = 1 \\ 1 & p|f(n) \end{cases}$. Ekkor

$$\text{i.) } W(E_p) < 10kp^{1/2}logp;$$

ii.) ha $l \in \mathbb{N}$ olyan, hogy (r, l, p) megengedhető hármas bármely $r \leq k$-ra, akkor
$$C_l(E_p) < 10klp^{1/2}logp.$$

Bizonyítás. A bizonyítás során szükségünk lesz két lemmára, amelyeket csak kimondunk, a bizonyítások megtalálhatóak a [2] cikkben.

2.2.9. LEMMA. Legyen p prímszám, χ $d-rendű$ nem főkarakter modulo p (azaz $d|p-1$), $f(x) \in F_p[x]$ egy $k-fokú$ polinom és $f(x) = b(x-x_1)^{d_1}...(x-x_s)^{d_s}$, ahol $x_i \neq x_j (i \neq j)$ $\overline{F}_p - ben$ és $(d, d_1, ..., d_s) = 1$. Legyen továbbá X, Y valós számok $(0 < Y \leq p)$, ekkor $\left| \sum_{X<n\leq X+Y} \chi(f(n)) \right| < 9kp^{1/2}logp$.

i.) Vegyünk $a \in \mathbb{Z}, b, t \in \mathbb{N}, 1 \leq a \leq a+(t-1)b \leq p$ és $g(x) = f(a+bx)$, $g(x) \in F_p[x]$. Ebből következik, hogy $g(x) \equiv 0 \pmod{p}$ egyenletnek legfeljebb k megoldása van, ezért definiálva $(\frac{a}{p})$ értékét 0-nak, ha $p|a$, kapjuk, hogy

$$\left|u(E_p, t, a, b)\right| = \left|\sum_{j=0}^{t-1} e_{a+jb}\right| \leq \left|\sum_{j=0}^{t-1} (\tfrac{f(a+jb)}{p})\right| + k = \left|\sum_{j=0}^{t-1} (\tfrac{g(j)}{p})\right| + k.$$

Természetesen adódik, hogy f és g foka megegyezik, ezenkívül ha

$$f(x) = c(x-x_1)...(x-x_k), \text{ ahol } x_i \neq x_j (i \neq j), \text{ akkor}$$

$$g(x) = f(a+bx) = cb^k(x-b^{-1}(x_1-a))...(x-b^{-1}(x_k-a)), \text{ amiből azonban kapjuk, hogy } g(x)\text{-nek nincs többszörös gyöke.}$$

Használjuk most fel a 2.2.9. Lemma állítását $(\frac{n}{p}), 2$ és $g(n)$ helyett $\chi(n), d$ és $f(n)$ felhasználásával. Ekkor

$$\left|u(E_p, t, a, b)\right| = \left|\sum_{j=0}^{t-1} (\tfrac{g(j)}{p})\right| + k < 9kp^{1/2}logp + k < 10kp^{1/2}logp.$$

Ezzel a 2.2.8. Tétel első részét bebizonyítottuk.

ii.) Legyen $f(x) = bf_1(x)$, $b \in \mathbb{Z}_p$, $f_1(x)$ egység polinom.

Ekkor $0 < d_1 < ... < d_l$, $M + d_l \leq p$, ahol $d_1, ..., d_l$ egész számok, $M \in \mathbb{N}$ és $f(n+d_i) \equiv 0 \pmod{p}$ $(1 \leq n \leq M,\ 1 \leq i \leq l)$ kongruenciának legfeljebb kl megoldása van. Írjunk $(\frac{0}{p}) = 0$-t, ekkor igaz, hogy

$$V(E_p, M, D) = \left|\sum_{n=1}^{M} e_{n+d_1}...e_{n+d_l}\right| \leq \left|\sum_{n=1}^{M} (\tfrac{f(n+d_1)}{p})...(\tfrac{f(n+d_l)}{p})\right| + kl =$$

$$= \left|(\tfrac{b^l}{p}) \sum_{n=1}^{M} (\tfrac{f_1(n+d_1)...f_1(n+d_l)}{p})\right| + kl.$$

Ezután az egyszerűség kedvéért használjuk a következő jelölést :

$$h(n) := f_1(n+d_1)...f_1(n+d_l).$$

Ekkor elég belátni a következő lemmát.

2.2.10. LEMMA. A $h(x)$-nek van legalább egy gyöke $\overline{F}_p - ben$, amelynek páratlan a multiplicitása.

A 2.2.10. Lemma és a 2.2.9. Lemma $(\frac{n}{p}), 2$ és $h(x)$ helyett χ, d és $f(x)$ felhasználásával kapjuk, hogy $\left|V(E_p,t,a,b)\right| \leq \left|\sum_{n=1}^{M}(\frac{h(n)}{p})\right| + kl < 9klp^{1/2}logp + kl < 10klp^{1/2}logp$, ahol felhasználtuk még, hogy $h(x)$ foka kl, és ezzel a 2.2.8. Tétel második részét is bebizonyítottuk. ■

Megjegyzés. A 2.2.8. Tételből következik, hogy a második konstrukció sorozata is „jó" pszeudovéletlen tulajdonságokkal rendelkezik.

A [2] cikkben a L. Goubin, C. Maudit, A. Sárközy megadtak egy algoritmust, amellyel konstruálni lehet adott p (prím) hosszú pszeudovéletlen bináris sorozatokat. Ez az algoritmus a 2.2.8. Tétel és az alábbi 2.3.1. Tétel kombinációjára épül.

2.3. Megengedhetőségi feltételek

Ahhoz, hogy a 2.2.8. Tételt könnyedén használhassuk, szükségünk van a (k,l,p) hármas megengedhetőségére. A következőekben erre adunk elégséges feltételeket.

2.3.1. Tétel.

i.) Bármely p prímszámra, $k \in \mathbb{N}, k < p$ esetén a $(k,2,p)$ hármas megengedhető;

ii.) Ha p prímszám, $k,l \in \mathbb{N}$ és $(4l)^k < p$, akkor a (k,l,p) hármas megengedhető;

iii.) Ha p prímszám és 2 primitív gyök modulo p, akkor bármely $k,l \in \mathbb{N}$ pár esetén $(k < p, l < p)$ a (k,l,p) hármas megengedhető.

Bizonyítás. ([2])

Megjegyzés. Miután sajnos nem tudjuk, hogy az iii.) pontban szereplő feltételek végtelen sok prímszámra teljesülnek-e, ezért a következőkben megadunk „jó" prímeket, amelyekre biztosan teljesülnek ezek a feltételek. Ehhez először definiálnunk kell, hogy mit értünk „jó" szám alatt.

2.3.2. Definíció. Egy poztív m egész számot jónak nevezünk, ha bármely $k, l \in \mathbb{N}$ $(k < m, l < m)$ párra a (k, l, m) hármas megengedhető.

2.3.3. Tétel. Egy páratlan p prímszámot jónak nevezünk, akkor és csak akkor, ha 2 primitív gyök modulo p.

Bizonyítás.

Bármely $C \in \mathbb{Z}_p$ esetén vegyük a $P_C(x) \in F_2[x]$ polinomot és $P_C(x) = \sum_{c \in C} x^{s(c)}$ legyen, ahol $s(c)$ jelölje a legkisebb negatív elemét a c maradékosztálynak modulo P. Megjegyezzük, hogy bármely $u \in \mathbb{Z}_p$ esetén a $P_{u+C}(x)$ polinom megegyezik $x^u P_C(x)$ maradékával modulo $(1 + x^p)$ az $F_2[x]$-ben. Ebből adódik, hogy bármely $A, B \subset \mathbb{Z}_p$ mellett az $A + B$ összeg $P - tulajdonságú$ akkor és csak akkor, ha $1 + x^p$ osztja $P_A(x)P_B(x)$-et $F_2[x]$-ben.

Ha $1 + x + ... + x^{p-1}$ felbontható $F_2[x]$-ben, írjunk $1 + x + ... + x^{p-1} = P_1(x)P_2(x)$, $2 \leq degP_i \leq p - 3$ $(i \in \{1, 2\})$.

Ha $P_1(x) = \sum_{a \in A} x^{s(a)}$ és $(1 + x)P_2(x) = \sum_{b \in B} x^{s(b)}$, akkor látható, hogy $A + B$ összeg $P - tulajdonságú$, így p nem jó prím.

Megfordítva, ha $1+x+...+x^{p-1}$ felbonthatatlan $F_2[x]$ felett, akkor $A, B \subset \mathbb{Z}_p$ esetén ($A+B$ összeg $P-tulajdonságú$) az $1+x+...+x^{p-1}$ polinomnak osztania kell vagy $P_A(x)$-et vagy $P_B(x)$-et az $F_2[x]$ felett, amiből $A = \mathbb{Z}_p$ vagy $B = \mathbb{Z}_p$, így p jó prím. Ezzel beláttuk, hogy p prím jó akkor és csak akkor, ha az $1 + x + ... + x^{p-1}$ polinom felbonthatatlan $F_2[x]$ felett.

A bizonyítás során felhasználtuk, amit a ciklikus polinomokról tudunk, mégpedig, hogy az $1+x+...+x^{p-1}$ polinom szétesik $\frac{p-1}{d}$ különböző felbonthatatlan polinomra, mindegyik d fokú $F_2[x]$ felett, ahol d a legkisebb olyan pozitív egész, hogy $2^d \equiv 1$ $(mod\ p)$. Így megkaptuk, hogy $1 + x + ... + x^{p-1}$ felbonthatatlan $F_2[x]$ felett, akkor és csak akkor, ha 2 primitív gyök modulo p, amivel a bizonyítást befejeztük. ■

Megjegyzés. Az m egész jó, akkor és csak akkor, ha $m = 4, p^k$ vagy $2p^k$ alakú, ahol p egy páratlan prím, $k \geq 0$ és 2 primitív gyök modulo m.

A következőkben megmutatunk néhány olyan példát, amiből látszik, hogy ha p egy nem jó prím, akkor az előző módszer miatt olyan példa van $A, B \subset \mathbb{Z}_p$ esetén, hogy az $A + B$ összeg $P - tulajdonságú$, azaz $k, l \in \mathbb{N}$ pár esetén a (k, l, p) hármas nem megengedhető.

2.3.4. Példa. Legyen $p = 17$. Ekkor $1 + x^{17} = (1 + x + x^3 + x^6 + x^8 + x^9)(1 + x + x^2 + x^4 + x^6 + x^7 + x^8)$ az $F_2[x]$ felett. Ebből kapjuk, hogy $A = \{0, 1, 3, 6, 8, 9\}$ és $B = \{0, 1, 2, 4, 6, 7, 8\}$ esetén az $A+B$ összeg $P-tulajdonságú$ és $(6, 7, 17), (7, 6, 17)$ hármasok nem megengedhetőek.

2.3.5. Példa. Legyen $p = 31$. Ekkor $1 + x^{31} = (1 + x^2 + x^5)(1 + x^2 + x^4 + x^5 + x^6 + x^8 + x^9 + x^{13} + x^{14} + x^{15} + x^{16} + x^{17} + x^{20} + x^{21} + x^{23} + x^{26})$ az $F_2[x]$ felett. Ebből kapjuk, hogy $A = \{0, 2, 5\}$ és $B = \{0, 2, 4, 5, 6, 8, 9, 13, 14, 15, 16, 17, 20, 21, 23, 26\}$ esetén az $A + B$ összeg $P - tulajdonságú$ és $(3, 16, 31), (16, 3, 31)$ hármasok nem megengedhetőek.

3. fejezet

A k szimbólumból képezett pszeudovéletlen sorozatok [1]

3.1. Bevezetés

A 2. fejezetben a véges bináris sorozatokat vizsgáltuk, ekkor E_N elemeit a $\{-1, 1\}$ halmazból választottuk. Definiáltunk különböző pszeudovéletlenségi mértékeket ezen az E_N sorozaton, mindvégig megfelelve a 1-6. pontokban feltett elvárásoknak. Beláttuk, hogy a $k-$rendű korrelációs mérték és az eloszlási mérték nagyjából $\sqrt{N}$ körül ingadozik, emellett speciálisan két konstrukciót vizsgálva megbizonyosodtunk arról, hogy mindkét esetben „jó" pszeudovéletlen sorozatot kapunk.

Azonban az alkalmazások tekintetében szükségessé vált, hogy C. Mauduit és A. Sárközy a [1] cikkében felépített elméletet a bináris sorozatokról kiterjesszék és általánosítsák egy tágabb, k szimbólumokból álló sorozatok elméletére [13]. A véletlenségi mértékek bevezetésekor (k szimbólum esetén) elsődlegesen azt tartották szem előtt, hogy a új definíciók összeegyeztethetőek legyenek a 2. fejezetben bemutatott mértékekkel, amikor is $k = 2$ szerepelt. A fent említett 1-6. pontot az alábbival bővítették ki:

7. *Az új mértékeknek (a bináris sorozatokra vonatkoztatva) nagyjából ekvivalensnek kellene lennie a régi mértékekkel abban az értelemben, hogy a hányadosuknak két pozitív konstans között kell lennie.*

Ebben a fejezetben a [13] cikkben bevezetett elméletnek a bemutatására törekszünk.

[1] A könnyebb szóhasználat érdekében, pontosabban: erős pszeudovéletlen tulajdonságokkal rendelkező k szimbólumból képezett sorozatok

3.2. Az $f-$mértékek

Legyen $k \in \mathbb{N}, k \geq 2$ és $A = \{a_1, ..., a_k\}$ k-szimbólumból („betűk") álló véges halmaz („abc"). Vegyük E_N elemeit ebből a véges halmazból, azaz $E_N = (e_1, ..., e_N) \in A^N$. Ekkor az alábbi jelöléseket használjuk :

- $x(E_N, a, M, u, v) = |\{j : 0 \leq j \leq M-1, e_{u+jv} = a\}|$ (3.1)
- $g(E_N, W, M, D) = |\{n : 1 \leq n \leq M, (e_{n+d_1}, ..., e_{n+d_l}) = W\}|$, ahol $W = (a_{i_1}, ..., a_{i_l}) \in A^l$ és $D = (d_1, ..., d_l)$, $d_1 < ... < d_l$ nem-negatív egészek. (3.2)

A pszeudovéletlenségi mértékek definiálásához vegyünk egy fent említett típusú$E_N \in A^N$ véges sorozatot.

3.2.1. Definíció. Az $f-$eloszlási mértéke E_N-nek:

$$\delta(E_N) = \max_{a,M,u,v} |x(E_N, a, M, u, v) - \tfrac{M}{k}|, \text{ ahol } a \in A,\ u + (M-1)v \leq N. \tag{3.3}$$

3.2.2. Definíció. Az $l-$rendű $f-$korrelációs mértéke E_N-nek :

$$\gamma_l(E_N) = \max_{W,M,D} |g(E_N, W, M, D) - \tfrac{M}{k^l}|, \text{ ahol } W \in A^l \text{ és } M + d_l \leq N. \tag{3.4}$$

Vegyünk újból egy bináris $E_N \in \{-1, 1\}^N$ sorozatot és legyen a $\varphi(E_N)$ olyan $[N/r]$ hosszú sorozat, amelyre $\varphi(E_N) = \Big((e_1, ..., e_r), (e_{r+1}, ..., e_{2r}), ..., (e_{([N/r]-1)r+1}, ..., e_{[N/r]r})\Big)$.

3.2.3. Tétel.

$$\text{i.)}\ \ \delta(\varphi(E_N)) \leq \tfrac{1}{2^r} \sum_{s=1}^{r} \binom{r}{s} Q_s(E_N),$$

$$\text{ii.)}\ \ \gamma_l(\varphi(E_N)) \leq \tfrac{1}{2^{rl}} \sum_{s=1}^{r} \sum_{q=1}^{l} \binom{r}{s} \binom{l}{q} Q_{qs}(E_N), \text{ bármely } l \in \mathbb{N} \text{ esetén.}$$

Következmény. A 3.2.3. Tételből adódik, hogy ha E_N „jó" pszeudovéletlen bináris sorozat, akkor $\varphi(E_N)$ is „jó" pszeudovéletlen sorozat.

Bizonyítás.(3.2.3. Tételé)

i.) Ha M, u, v adottak és $a = (\varepsilon_1, ..., \varepsilon_r) \in \{-1, 1\}^r$, akkor

$$x(\varphi(E_N),a,M,u,v)=$$

$$=|\{j:0\le j\le M-1,(e_{(u+jv-1)r+1},...,e_{(u+jv)r})=(\varepsilon_1,...,\varepsilon_r)\}|=\sum_{j=0}^{M-1}\prod_{i=1}^{r}\frac{e_{(u+jv-1)r+i}\varepsilon_i+1}{2}=$$

$$=\frac{M}{2^r}+\frac{1}{2^r}\sum_{s=1}^{r}\sum_{1\le i_1<...<i_s\le r}\varepsilon_{i_1}...\varepsilon_{i_s}\sum_{j=0}^{M-1}e_{(u+jv-1)r+i_1}...e_{(u+jv-1)r+i_s}. \tag{3.5}$$

Felhasználva (3.1)-et, illetve az 2.1.9. Definíciót

$$|x(\varphi(E_N),a,M,u,v)-\frac{M}{k}|=|x(\varphi(E_N),a,M,u,v)-\frac{M}{2^r}|\le$$

$$\le\frac{1}{2^r}\sum_{s=1}^{r}\sum_{1\le i_1<...<i_s\le r}|\sum_{j=0}^{M-1}e_{(u-1)r+jvr+i_1}...e_{(u-1)r+jvr+i_s}|=$$

$$=\frac{1}{2^r}\sum_{s=1}^{r}\sum_{1\le i_1<...<i_s\le r}|Z((u-1)r,vr,M-1,(i_1,...,i_s))|\le\frac{1}{2^r}\sum_{s=1}^{r}\sum_{1\le i_1<...<i_s\le r}Q_s(E_N)=$$

$$=\frac{1}{2^r}\sum_{s=1}^{r}\binom{r}{s}Q_s(E_N).$$

ii.) Legyen $A=\{-1,1\}^r$,$w=(a_{i_1},...,a_{i_l})\in A^l$,$a_{i_j}=(\varepsilon_1^{(j)},...,\varepsilon_r^{(j)})$ és $D=(d_1,...,d_l)$.

Ekkor az i.) rész bizonyításának menetéhez hasonlóan

$$g(\varphi(E_N),W,M,D)=$$

$$=|\{n:1\le n\le M,\ ((e_{(n+d_1-1)r+1},...,e_{(n+d_1)r}),...,(e_{(n+d_l-1)r+1},...,e_{(n+d_l)r}))=((\varepsilon_1^{(1)},...,\varepsilon_r^{(1)}),...,(\varepsilon_1^{(l)},...,\varepsilon_r^{(l)}))\}|=$$

$$=\sum_{n=1}^{M}\prod_{i=1}^{r}\prod_{j=1}^{l}\frac{e_{(n+d_j-1)+i}\varepsilon_i^{(j)}+1}{2}=\frac{M}{2^{rl}}+\frac{1}{2^{rl}}\sum_{s=1}^{r}\sum_{q=1}^{l}\sum_{\substack{1\le i_1<...<i_s\le r\\1\le j_1<...<j_q\le l}}(\prod_{\mu=1}^{s}\prod_{\nu=1}^{q}\varepsilon_{i_\mu}^{(j_\nu)})(\sum_{n=1}^{M}\prod_{\mu=1}^{s}\prod_{\nu=1}^{q}e_{(n+d_{j_\nu}-1)r+i_\mu}).$$

Így felhasználva ismét a 2.1.9. Definíciót kapjuk, hogy

$$|g(\varphi(E_N),W,M,D)-\frac{M}{2^{rl}}|=|g(\varphi(E_N),W,M,D)-\frac{M}{k^l}|\le$$

$$\le\frac{1}{2^{rl}}\sum_{s=1}^{r}\sum_{q=1}^{l}\sum_{\substack{1\le i_1<...<i_s\le r\\1\le j_1<...<j_q\le l}}|Z(0,r,M-1,(d_{j_1}r+i_1,...,d_{j_q}r+i_s))|\le$$

$$\le\frac{1}{2^{rl}}\sum_{s=1}^{r}\sum_{q=1}^{l}\sum_{\substack{1\le i_1<...<i_s\le\\1\le j_1<...<j_q\le l}}Q_{qs}(E_N)=\frac{1}{2^{rl}}\sum_{s=1}^{r}\sum_{q=1}^{l}\binom{r}{s}\binom{l}{q}Q_{qs}(E_N).$$

Ezzel beláttuk a 3.2.3. Tétel mindkét részét.■

3.3. A $k-$adrendű multiplikatív karakterek pszeudovéletlensége

Az alábbiakban k-adrendű multiplikatív karakterek egymás utáni értékei által alkotott sorozat egy erős pszeudovéletlen tulajdonságát fogjuk vizsgálni. A 3.3.5. Tételben bemutatott harmadik konstrukció általánosítása lesz a 2.2.8. Tételben szereplőnek. Ehhez azonban mindezek előtt szükségünk lesz a $k-$megengedhetőség fogalmára.

3.3.1. Definíció. Egy multihalmazt $k-$halmaznak hívunk, ha minden elem előfordulásának multiplicitása legfeljebb k.

Ezután definiáljuk, mit is értünk P_k-tulajdonság alatt, amely általánosítása a 2.2.6. Definícióban szereplő $P-$tulajdonságnak.

3.3.2. Definíció. Ha $k, m \in \mathbb{N}$, $k \geq 2$, A,B $\mathbb{Z}_m$-beli multihalmazok és $A+B$ előállítja $\mathbb{Z}_m$ minden elemét k-val osztható multiplicitással; azaz ha bármely $c \in \mathbb{Z}_m$ esetén az $a+b=c$ $(a \in A, b \in B)$ egyenlet megoldásának száma osztható k-val (tartalmazva azt is, ha nincs megoldás), akkor az $A+B$ összeget P_k-tulajdonságúnak nevezzük.

3.3.3. Definíció. Ha $k, h, l, m \in \mathbb{N}$, $k \geq 2$ és $h, l \leq m$, akkor a (h, l, m) hármast $k-$megengedhetőnek hívjuk, ha nincs olyan $2-$halmaz A és olyan $k-$halmaz B ($\mathbb{Z}_m$-beli elemmel), hogy $|A| = h$, $|B| = l$ és $A+B$ összeg P_k-tulajdonságú.

3.3.4. Definíció. Ha $k, h, l, m \in \mathbb{N}$, $k \geq 2$ és $h, l \leq m$, akkor a (h, l, m) hármast $(k, k)-$megengedhetőnek hívjuk, ha nincs olyan $k-$halmaz A és B ($\mathbb{Z}_m$-beli elemmel), hogy $|A| = h$, $|B| = l$ és $A+B$ összeg P_k-tulajdonságú.

Megjegyzés. A 3.3.4. Definícióban szereplő $(k, k)-$megengedhetőség általánosítása a 2.2.7. Definícióban szereplő $k = 2$-nek megfelelő megengedhetőségnek.

3.3.5. Tétel. Tegyük fel, hogy $k \in \mathbb{N}$, $k \geq 2$, p prímszám, χ egy $k-$rendű multiplikatív karakter modulo p (azaz $k|p-1$), $f(x) \in F_p[x]$ $h-$fokú $(h > 0)$ polinom, amelynek nincs többszörös gyöke $\overline{F}_p-$ben. Ezenkívűl vegyük az $E_p = (e_1, ..., e_p)$ k-adik (komplex) egységgyökök k betűs abc-jének sorozatát, ahol

$$e_n = \begin{cases} \chi(f(n)), & (f(n), p) = 1 \\ 1, & p|f(n) \end{cases}.$$ Ekkor

i.) $\delta(E_p) < 11hp^{1/2}\log p$;

ii.) ha $l \in \mathbb{N}$, (r,t,p) $k-$megengedhető hármas $(1 \le r \le h, 1 \le t \le l(k-1))$, akkor $\gamma_l(E_p) < 10lhkp^{1/2}\log p$.

Bizonyítás. A 3.3.5. Tétel bizonyítása során az alábbi két lemmára lesz szükségünk, bizonyításaik megtalálhatóak a [3] cikkben, ahol az első lemma bizonyítása Weil tételére [24] épül.

3.3.6. LEMMA. Legyen p prím, χ k-rendű nem főkarakter modulo p, Ezenkívűl legyen $f(x) \in F_p[x]$ egy h-fokú polinom és $f(x) = b(x-x_1)^{r_1}...(x-x_s)^{r_s}$, ahol $x_i \neq x_j$, ha $i \neq j$ $\overline{F}_p-$ben és $(k, r_1, ..., r_s) = 1$. Legyen ezenkívűl X, Y valós, $0 < Y \le p$. Ekkor $\left| \sum_{X<n\le X+Y} \chi(f(n)) \right| < 9sp^{1/2}\log p \le 9hp^{1/2}\log p$.

A 3.3.6. Lemmának a gyengébbik alakjára is szükségünk lesz.

3.3.7. LEMMA. A 3.3.6. Lemma igaz $(k, r_1, ..., r_s) < k$ mellett is.

Ezután folytathatjuk a 3.3.5. Tétel bizonyítását.

i.) Ha a egy k-adik egységgyök, akkor

$$S(a,m) = \frac{1}{k}\sum_{t=1}^{k}(\overline{a}\chi(m))^t, \text{ ahol} \tag{3.6}$$

$$S(a,m) = \begin{cases} 1, ha & \chi(m) = a \\ 0, ha & \chi(m) \neq a. \end{cases} \tag{3.7}$$

Emellett $u, v, M \in \mathbb{N}$ jelöléssel, ha $1 \le u \le u + (M-1)v \le p$, akkor

$$x(E_p, a, M, u, v) = \sum_{\substack{0\le j\le M-1 \\ e_{u+jv}=a}} 1, \text{ ahol} \tag{3.8}$$

$$\left| \sum_{\substack{0\le j\le M-1 \\ e_{u+jv}=a}} 1 - \sum_{\substack{0\le j\le M-1 \\ \chi(f(u+jv))=a}} 1 \right| \le \sum_{\substack{0\le j\le M-1 \\ p|f(u+jv)}} 1. \tag{3.9}$$

Felhasználva az (3.6),(3.7) pontokat kapjuk, hogy

$$\sum_{\substack{0\le j\le M-1\\ \chi(f(u+jv))=a}} 1 = \sum_{j=0}^{M-1} S(a, f(u+jv)) = \sum_{j=0}^{M-1} \tfrac{1}{k}\sum_{t=1}^{k} (\overline{a}\chi(f(u+jv)))^t =$$

$$= \tfrac{1}{k} \sum_{\substack{0\le j\le M-1\\ (f(u+jv),p)=1}} 1 + \tfrac{1}{k}\sum_{t=1}^{k-1}\overline{a}^t \sum_{j=0}^{M-1}\chi^t(f(u+jv)) = \tfrac{M}{k} - \tfrac{1}{k}\sum_{\substack{0\le j\le M-1\\ p|f(u+jv)}} 1 + \tfrac{1}{k}\sum_{t=1}^{k-1}\overline{a}^t \sum_{j=0}^{M-1}\chi^t(f(u+jv)).$$

Átrendezve adódik :

$$\left| \sum_{\substack{0\le j\le M-1\\ \chi(f(u+jv))=a}} 1 - \tfrac{M}{k} \right| \le \tfrac{1}{k}\sum_{t=1}^{k-1}\left|\sum_{j=0}^{M-1}\chi^t(f(u+jv))\right| + \tfrac{1}{k}\sum_{\substack{0\le j\le M-1\\ p|f(u+jv)}} 1. \tag{3.10}$$

Írjunk $g(x) = f(u+xv)$, ekkor a (3.8),(3.9),(3.10) pontokat felhasználva

$$\left| x(E_p, a, M, u, v) - \tfrac{M}{k} \right| \le \tfrac{1}{k}\sum_{t=1}^{k-1}\left|\sum_{j=0}^{M-1}\chi^t(g(j))\right| + 2\sum_{\substack{0\le j\le M-1\\ p|g(j)}} 1. \tag{3.11}$$

Az $M = 1$ eset triviális, ezért feltesszük, hogy $M > 1$. Mivel $1 \le r < p, (r,p) = 1$, ezért $f(x), g(x) \in F_p[x]$ ugyanolyan fokú, és mivel $f(x)-$nek nincs többszörös gyöke, így $g(x)-$nek sincs. Ezenfelül $\chi_1 = \chi^t$ is karakter modulo p és különbözik a χ_0 főkaraktertől $(1 \le t \le k-1)$. Ezért felhasználva a 3.3.6. Lemmát

$$\left|\sum_{j=0}^{M-1}\chi^t(g(j))\right| = \left|\sum_{j=0}^{M-1}\chi_1(g(j))\right| < 9hp^{1/2}\log p. \tag{3.12}$$

Mivel f, g foka megegyezik, kapjuk, hogy

$$\sum_{\substack{0\le j\le M-1\\ p|g(j)}} 1 \le \sum_{\substack{0\le j<p\\ p|g(j)}} 1 \le h. \tag{3.13}$$

Összevetve az (3.11),(3.12),(3.13) eredményeit

$$\left| x(E_p, a, M, u, v) - \tfrac{M}{k} \right| \le \tfrac{k-1}{k} 9hp^{1/2}\log p + 2h < 11hp^{1/2}\log p.$$

Ezzel a tétel egyik felét bebizonyítottuk.

ii.)

Legyen $l \in \mathbb{N}$, $l \leq N$, $b_1, ..., b_l$ a k-adik egységgyökök, $w = (b_1, ..., b_l)$, $D = (d_1, ..., d_l)$, $0 \leq d_1 < ... < d_l$, $M \in \mathbb{N}$ és $M + d_l \leq N$. Ekkor

$$g(E_N, w, M, D) = |\{n : 1 \leq n \leq M, (e_{n+d_1}, ..., e_{n+d_l}) = w\}|, \text{ ahol} \tag{3.14}$$

$$e_{n+d_i} = \chi(f(n + d_i)) \text{ és } f(n + d_i) \equiv 0 \ (mod\ p),\ i = 1, ..., l. \tag{3.15}$$

Fix $i-$re az (3.15) kongruenciának legfeljebb h megoldása lehet, és i felvehet legfeljebb l értéket, így a (3.15) megoldásszáma legfeljebb hl. Ha egy n nem megoldása ennek a kongruenciának, akkor

$$\prod_{i=1}^{l} S(b_i, f(n + d_i)) = \begin{cases} 1, ha & e_{n+d_1} = b_1, ..., e_{n+d_l} = b_l \\ 0, & k\ddot{u}l\ddot{o}nben \end{cases}. \tag{3.16}$$

Emiatt összevetve a (3.14), (3.16) pontokat

$$\left| g(E_N, w, M, D) - \sum_{n=1}^{M} \prod_{i=1}^{l} S(b_i, f(n + d_i)) \right| \leq hl, \text{ ahol} \tag{3.17}$$

$$\sum_{n=1}^{M} \prod_{i=1}^{l} S(b_i.f(n + d_i)) = \sum_{n=1}^{M} \prod_{i=1}^{l} \frac{1}{k} \sum_{t_i=1}^{k} (\bar{b}_i \chi(f + n + d_i))^{t_i} = \tag{3.18}$$

$$= \frac{1}{k^l} \sum_{t_1=1}^{k} ... \sum_{t_l=1}^{k} \overline{b_1^{t_1} ... b_l^{t_l}} \sum_{n=1}^{M} \chi((f(n + d_1)^{t_1} ... (f(n + d_l))^{t_l}) =$$

$$= \frac{M}{k^l} + \frac{1}{k^l} \sum_{\substack{0 \leq t_1, ..., t_l \leq k-1 \\ (t_1, ..., t_l) \neq (0, ..., 0)}} \overline{b_1^{t_1} ... b_l^{t_l}} \sum_{n=1}^{M} \chi((f(n + d_1)^{t_1} ... (f(n + d_l))^{t_l}).$$

Ekkor következik a (3.17),(3.18) pontokból, hogy

$$\left| g(E_N, w, M, D) - \frac{M}{k^l} \right| \leq \frac{1}{k^l} \sum_{\substack{0 \leq t_1, ..., t_l \leq k-1 \\ (t_1, ..., t_l) \neq (0, ..., 0)}} \left| \sum_{n=1}^{M} \chi((f(n + d_1)^{t_1} ... (f(n + d_l))^{t_l}) \right| + hl. \tag{3.19}$$

Vizsgáljuk meg az (3.19) sor jobb oldalán álló kifejezés belső összeget. Használjuk a következő jelöléseket : $f(x) := Bf_1(x), G(x) := f_1(x+d_1)^{t_1}...f_1(x+d_l)^{t_l}$,ahol $B \in \mathbb{Z}_p, f_1(x) \in \mathbb{Z}_p[x]$ egységpolinom.

$$\left|\sum_{n=1}^{M}\chi((f(n+d_1))^{t_1}...(f(n+d_l))^{t_l})\right| = \left|\chi(B^{t_1+...+t_l})\right|\left|\sum_{n=1}^{M}\chi(G(n))\right| \leq \left|\sum_{n=1}^{M}\chi(G(n))\right|.$$

A bizonyítás befejezéséhez elég a következő lemmát felhasználni, a bizonyítás megtalálható a [3] cikkben.

3.3.8. LEMMA. Ha megtartjuk a 3.3.5. Tétel jelöléseit, akkor a $G(x)$-nek van legalább egy gyöke $\overline{F}_p-$ben, amelynek multiplicitása osztható $k-$val.

A 3.3.8. Lemma helyességét elfogadva könnyen látszik, hogy $G(x)$ foka

$$\sum_{i=1}^{l} ht_i \leq lh(k-1) < lhk.$$

Felhasználva a 3.3.7. Lemmát kapjuk, hogy

$$\left|\sum_{n=1}^{M}\chi(G(n))\right| < 9lhkp^{1/2}\log p.$$

Ebből következik az (3.19) pontottal, hogy

$$\left|g(E_N, w, M, D) - \tfrac{M}{k^l}\right| \leq \tfrac{1}{k^l} \sum_{\substack{0\leq t_1,...,t_l\leq k-1 \\ (t_1,...,t_l)\neq(0,...,0)}} 9lhkp^{1/2}\log p + hl < 10lhkp^{1/2}\log p.$$

Ezzel a tétel második részét is bebizonyítottuk. ■

Megjegyzés. A 3.3.5. Tételből következik, hogy a harmadik konstrukció sorozata is „jó" pszeudovéletlen tulajdonságokkal rendelkezik.

3.4. A $k-$megengedhetőségi feltételek

A 3.3.5. Tétel ii.) pontjában bizonyos $k-$megengedhetőséget használtunk fel. R. Ahlswede, C. Mauduit, A. Sárközy a [3] cikkben megmutatták, hogy ez a feltétel nem kerülhető ki, emellett adtak egy negatív példát ennek igazolására. Vettek egy

A egyszerű halmazt és egy B $k-$halmazt. Az $A+B$ összeg P_k tulajdonsága adott egy 3.3.5. Tételben szereplő konstrukciót, de ii.) következmény sem teljesült, azaz bizonyos korreláció nagy volt.

A fentiek miatt a következőkben a 3.3.5 Tételnél felhasznált (r,t,p) hármasra elégséges $k-$megengedhetőségi feltételeket fogunk vizsgálni. Megjegyezzük, hogy az ezt bebizonyító 3.4.1. Tétel általánosítása a 2. fejezetben szereplő 2.3.1. Tételnek.

3.4.1. Tétel.

i.) Ha $k,r,t \in \mathbb{N}, 1 \leq t \leq k, p$ prím és $r < p$, akkor (r,t,p) hármas $k-$megengedhető

ii.) Ha $k,r,t \in \mathbb{N}, p$ prímszám és $(4t)^r < p$, akkor (r,t,p) hármas $k-$megengedhető

iii.) Ha $k \in \mathbb{N}, k \geq 2, k = q_1^{\alpha_1}...q_s^{\alpha_s}$ és p olyan prímszám, hogy minden egyes $q_i (i \in \{1,...,s\})$ primitív gyök modulo p. Ekkor minden $r,t \in \mathbb{N}$ és $r,t < p$ esetén az (r,t,p) hármas $k-$megengedhető.

Bizonyítás.

i.) Indirekt tegyük fel, hogy van olyan $k,r,t \in \mathbb{N}$, p prím, hogy$1 \leq t \leq k$,$r < p$ és az (r,t,p) hármas nem $k-$megengedhető. Azaz létezik olyan $A \subset \mathbb{Z}_p$, $k-$halmaz B, amelynek elemei $\mathbb{Z}_p-$beliek, hogy $|A| = r$, $|B| = t$ és az

$$a + b = c \ (a \in A, b \in B) \tag{3.20}$$

megoldásának száma oszható $k-$val, bármely $c \in \mathbb{Z}$ esetén.

Vegyünk tetszőleges $c \in A+B$. Mivel erre a $c-re$ a (3.20) egyenletnek van legalább egy megoldása és a megoldásának száma mindig osztható $k-$val ezért az egyenletnek legalább k megoldása van. Másfelöl nyilván legfeljebb $|B| = l$ megoldása van, azaz $|B| = t \geq k$. De ekkor$1 \leq t \leq k$,$r < p$ miatt $|B| = t = k$.

Mivel B egy $k-$halmaz minden elem multiplicitása legfeljebb $k-1$. $|B| = t = k$ miatt, B-nek van legalább két különböző eleme $(b_0, b_0 + d \in B, d \neq 0)$. Az $A + b_0$ minden elemének van legalább k előállítása a (3.20) egyenletben, ahol$|B| = t = k$ miatt van előállításuk az $(a+b_0+d)$-ben is $(a \in A, A+b_0 = A+b_0+rd, r \in \mathbb{N})$. Ezért $A + b_0 = A + b_0 + s, s \in \mathbb{Z}_p, s \in A + b_0$. Mivel azonban $A + b_0$ additív részcsoportja $\mathbb{Z}_p$-nek, $A = A + b_0 = \mathbb{Z}_p$, amely ellentmond annak, hogy $|A| = r$. Ezzel a tétel első részét bebizonyítottuk.

ii.) A bizonyítás nagyon hasonló a 2.3.1 Tétel bizonyításához, amely megtalálható a [2] cikkben. Emiatt elég, ha a legfontosabb részeket nézzük meg.

Tegyük fel, hogy létezik r, t, p, amely eleget tesz a 3.4.1. Tétel ii.) egyenlőtlenségének, $A \subset \mathbb{Z}_p$, B $k-$halmaz amelynek elemei $\mathbb{Z}_p$-beliek. Ezenkívül $|A| = r, |B| = t$. Elég megmutatni, hogy létezik olyan $c \in \mathbb{Z}_p$, amelyre a (3.20) egyenlet ($a \in A, b \in B$) megoldásának száma nagyobb mint 0, és kisebb mint k. Emiatt elég bebizonyítani, hogy létezik olyan $m \in \mathbb{N}, c' \in \mathbb{Z}_p$, amelyre $(m, p) = 1$ és az

$$ma + mb = mc' \tag{3.21}$$

megoldásának száma nagyobb 0-nál, és kisebb, mint k. Ehhez vegyünk $m, b_i, b_j, r_1, r_k, a_n, a_v$, hogy

$$mb_i + r_k = mb_j + ma_v \text{ és } mb_j + r_1 = mb_j + ma_u \tag{3.22}$$

számok esetén nincs más előállítása (3.21)-nek. Mivel B egy $k-$halmaz b_i, b_j multiplicitása kisebb k-nál. Ezért a (3.22)-ben említett számoknak legalább 0, legfeljebb k előállítása van (3.21) alakban, amellyel beláttuk, amit szerettünk volna.

Megjegyzés. Az iii.) pont részletes bizonyítása a 3.3.3. Tételen alapszik, ami megtalálható a [4] cikkben. A szerzők az igazoláshoz felhasználták a 2.3.2. Definíció általánosításaként szereplő „$k-$jó" szám elnevezést:

3.4.2. Definíció. Egy m természetes számot $k-$jónak hívunk, ha r, t természetes számok esetén $(r, t < m)$, az (r, t, m) $k-$megengedhető hármas. Ha ez a hármas $(k, k)-$megengedhető akkor $m-$et $(k, k)-$jónak nevezzük.

3.4.3. Tétel. Ha $k \geq 2$ olyan természetes szám, aminek prímtényezős felbontása $k = q_1^{\alpha_1} ... q_s^{\alpha_s}$ és $q_1, ..., q_s$ primitív gyök modulo p (páratlan prím), ekkor p $k-$jó.

Az 2. fejezet 2.3.3. Tételében kimondtuk, hogy egy p prímet $(2-)$jónak nevezünk akkor és csak akkor, ha 2 primitív gyök modulo p. Ez egy speciális esete volt a 3.4.3. Tételnek a $k = 2$ esetben. Ezenkívül megadtunk ott néhány példát, ahol p nem jó prím volt és az $A + B$ összeg rendelkezett a P_2-tulajdonsággal vagyis nem megengedhető hármasok keletkeztek. Az alábbiakban ehhez hasonló példát mutatunk, ahol $k = 6$.

3.4.4. Példa. Legyen $p = 31$, $A = \{0, 2, 4, 5, 6, 8, 9, 13, 14, 15, 16, 17, 20, 21, 23, 26\}$ és $B = \{0, 0, 0, 2, 2, 2, 5, 5, 5\}$. Ekkor az $A+B$ összeg P_6-tulajdonságú, azaz $(16, 9, 31)$ nem 6-megengedhető.

3.5. Három új konstrukció

Az alábbiakban megadunk néhány konstrukciót a k-szimbólumot tartalmazó pszeudovéletlen sorozatokon. Ezek a Lehmer probléma, multiplikatív inverz és az additív karakterek felhasználásával keletkeztek.

Számos matematikus foglalkozott a Lehmer probléma (bővebben ld.: [18]) megoldásával, általánosításával. Liu és Yang a [19] cikkben felhasználva ezt a problémát, megadtak egy konstrukciót a pszeudovéletlen bináris sorozatokra, ezenkívül belátták, hogy az általuk definiált E_N sorozat jó pszeudovéletlen tulajdonságokkal rendelkezik. A 3.5.1. Tételben szereplő konstrukció a Liu és Yang konstrukciónak az általánosítása. A tételeket csak kimondjuk, a bizonyítások megtalálhatóak Kit-Ho Mak [16] cikkében.

3.5.1. Tétel. Legyen p egy nagy prím, $r(x) = \frac{g(x)}{f(x)}$ racionális törtfüggvény, melynek foka $0 < d < p$, $f, g \in F_p[x]$ relatív prím polinomok. Tegyük fel, hogy $r(x)$ nem lineáris. Legyen $A = \{0, 1, ..., k-1\}$ egy $k-$elemű halmaz, N egész, $1 \leq N \leq p$.

Definiáljuk az $E_N^{(1)} := E_N^{(1)}(r) = (e_1^{(1)}, ..., e_N^{(1)}) \in A^N$ sorozatot, ahol

$$e_n^{(1)} = \begin{cases} i, ha & p \nmid f(n), R_p(r(n)) \equiv i(k) \\ 0, ha & p | f(n) \end{cases}.$$

Ekkor

$$\delta(E_N^{(1)}) \leq (8d-5)k\sqrt{p}log^2 p$$

és ha teljesül, hogy vagy

1. $deg(f) > 0$ és $(4deg(f))^l < p$, vagy
2. $deg(f) = 0$ és $2 \leq l < d$,

akkor

$$\gamma_l(E_N^{(1)}) \leq 2^l(4dl-2)\sqrt{p}log^{l+1}p.$$

Megjegyzés. A 3.5.1 Tételben szereplő $R_p(x)$ jelöli azon $0 \leq r \leq p-1$, hogy $x \equiv r(p)$.

C. Maudit, J. Rivat, A. Sárközy a [20] cikkükben additív karaktereket felhasználva konstruáltak pszeudovéletlen tulajdonsággal rendelkező bináris sorozatokat. A következő tétel ennek az általánosításáról szól, ehhez vegyünk egy $[0, p)$ intervallumot és osszuk fel k egyenlő részre.

3.5.2. Tétel. Legyen p egy nagy prím, $r(x) = \frac{g(x)}{f(x)}$ racionális törtfüggvény, melynek foka $0 < d < p$, $f, g \in F_p[x]$ relatív prím polinomok. Tegyük fel, hogy $r(x)$ nem lineáris. Legyen $A = \{0, 1, ..., k-1\}$ egy $k-$elemű halmaz.

Definiáljuk az $E_N^{(2)} := E_N^{(2)}(r) = (e_1^{(2)}, ..., e_N^{(2)}) \in A^N$ sorozatot, ahol

$$e_n^{(2)} = \begin{cases} i, ha & p \nmid f(n), \frac{i}{k}p \leq R_p(r(n)) < \frac{i+1}{k}p \\ 0, ha & p|f(n) \end{cases}.$$

Ekkor

$$\delta(E_N^{(2)}) \leq (8d-5)\sqrt{p}log^2 p$$

és ha teljesül, hogy vagy

1. $deg(f) > 0$ és $(4deg(f))^l < p$, vagy
2. $deg(f) = 0$ és $2 \leq l < d$,

akkor

$$\gamma_l(E_N^{(2)}) \leq 2^l(4dl-2)\sqrt{p}log^{l+1}p.$$

Végezetül a 3.5.1. és 3.5.2. Tételek kombinálásából keletkezett konstrukcióról megmutatjuk, hogy jó pszeudovéletlen tulajdonsággal rendelkező sorozat állít elő. Ehhez vegyük a $k = k_1k_2 \geq 2$, és készítsük el a $A = A_{k_1} \times A_{k_2}$ halmazt.

3.5.3. Tétel. Legyen p egy nagy prím, $r(x) = \frac{g(x)}{f(x)}$ racionális törtfüggvény, melynek foka $0 < d < p$, $f, g \in F_p[x]$ relatív prím polinomok. Tegyük fel, hogy $r(x)$ nem lineáris. Legyen $A = \{0, 1, ..., k-1\}$ egy $k-$elemű halmaz.

Definiáljuk az $E_N^{(3)} := E_N^{(3)}(r) = (e_1^{(3)}, ..., e_N^{(3)}) \in A^N$ sorozatot, ahol

$$e_n^{(3)} = \begin{cases} (i_1, i_2), ha & p \nmid f(n), R_p(f(n)) \equiv i_1(k_1), \frac{i_2}{k_2}p \leq R_p(r(n)) < \frac{i_2+1}{k_2}p \\ 0, ha & p|f(n) \end{cases}.$$

Ekkor

$$\delta(E_N^{(3)}) \leq (8d-5)k\sqrt{p}log^2 p$$

és ha teljesül, hogy vagy

1. $deg(f) > 0$ és $(4deg(f))^l < p$, vagy
2. $deg(f) = 0$ és $2 \leq l < d$,

akkor

$$\gamma_l(E_N^{(3)}) \leq 2^l(4dl-2)\sqrt{p}log^{l+1}p.$$

4. fejezet

Más típusú mértékek

4.1. Az $\varepsilon-$mértékek

A 3. fejezetben elkezdtük az erős pszeudovéletlen tulajdonságokkal rendelkező k szimbólumból képezett sorozatok vizsgálatát. Bevezettük ezen sorozatok $f-$mértékeit és beláttuk, hogy a $k-$adrendű multiplikatív karakterek sorozata erős pszeudovéletlen tulajdonságokkal rendelkezik. Azonban a bevezetésben kimondtuk, hogy a 7. követelménynek szeretnénk eleget tenni, miszerint az „új" mértékeknek összeegyeztethetőnek kell lennie a 2. fejezetben bevezett véletlenségi mértékekhez, amikor is $k = 2$ speciális eset szerepelt.

Ezért C. Mauduit és A. Sárközy a [13] cikkben új véletlenségi mértékeket definiáltak, amelyek szorosabb kapcsoltban állnak a 2. fejezetben bevezett mértékekkel. Ebben a fejezetben ennek az elméletnek a bemutatására törekszünk. Az új mértékek bevezetése után bebizonyítjuk, hogy ezek nagyjából egy konstans szorzóval térnek el a régi mértékektől, majd általánosítjuk a 2.2.1. Legendre szimbólumos konstrukciót $k \geq 2$ esetre. Megmutatjuk, hogy az ekkor kapott sorozat is jó pszeudovéletlen tulajdonságokkal rendelkezik. A fejezet legvégén felhasználva G. Bérczi [15] cikkét alsó és felső becslést adunk bizonyos az E_N véges sorozat a következőkben bevezetett mértékeire.

Legyen $k \in \mathbb{N}, k \geq 2$ és $E_N \in A^N = \{a_1, ..., a_k\}^N$. Ezenkívül vegyük a $k-$adik egységgyökök $\varepsilon = \{\varepsilon_1, ..., \varepsilon_k\}$ sorozatát és legyen F a $\varphi : A \leftrightarrow \varepsilon$ bijekciók halmaza ($|F| = k!$).

Használjuk a következő jelöléseket :

- $x(E_N, \varphi, M, u, v) = \sum_{j=0}^{M-1} \varphi(e_{u+jv})$ (4.1)

- $G(E_N, \phi, M, D) = \sum_{n=1}^{M} \varphi_1(e_{n+d_1}) ... \varphi_l(e_{n+d_l})$, (4.2)

ahol $\phi = (\varphi_1, ..., \varphi_l) \in F^l$, és $D = (d_1, ..., d_l)$, $d_1 < ... < d_l$.

4.1.1. Definíció. Az E_N sorozat $\varepsilon - \textit{eloszlási}$ mértéke:

$$\Delta(E_N) = \max_{\varphi, M, u, v} |x(E_N, \varphi, M, u, v)|, \text{ ahol } \varphi \in F \text{ és } u + (M-1)v \leq N. \tag{4.3}$$

4.1.2. Definíció. Az E_N sorozat $l - \textit{rendű}$ $\varepsilon - \textit{korrelációs}$ mértéke:

$$\Gamma_l(E_N) = \max_{\phi, M, D} |G(E_N, \phi, M, D)|, \text{ ahol } \phi \in F^l, \text{ és } D = (d_1, ..., d_l),\ M + d_l \leq N. \tag{4.4}$$

Az alábbiakban megmutatjuk, milyen kapcsolat áll fenn a (4.3), (4.4) és a bináris esetben definiált (2.6), (2.7) véletlenségi mértékek között.

Ehhez fixáljunk le egy $E_N \in \{a_1, a_2\}^N$véges sorozatot és legyen $\varepsilon = \{1, -1\}$.

Ezenkívül

$$\varphi_i(a_j) = \begin{cases} 1, & i = j, \\ -1, & i \neq j \end{cases} \text{ és } i, j \in \{1, 2\}.$$

Ekkor definiálhatunk egy E'_N sorozatot, amelynek elemeire $e'_n = \varphi_1(e_n) = -\varphi_2(e_n)$, $n = 1, 2, ..., N$.

4.1.3. Állítás. Ha $k = 2$, akkor $\Delta(E_N) = W(E'_N)$ és minden $l \in \mathbb{N}$ esetén $\Gamma_l(E_N) = C_l(E'_N)$.

Bizonyítás. Bármelyφ, M, u, v mellett

$$x(E_N, \varphi, M, u, v) = \sum_{j=0}^{M-1} \varphi(e_{u+jv}) = \pm \sum_{j=0}^{M-1} e'_{u+jv} = \pm U(E'_N, M, u, v). \tag{4.5}$$

Felhasználva (4.5),(4.3),(2.6) kapjuk, hogy

$$\Delta(E_N) = \max_{\varphi,M,u,v} |x(E_N, \varphi, M, u, v)| = W(E'_N).$$

Hasonlóan, bármely ϕ, M, D esetén

$$G(E_N, \phi, M, D) = \sum_{n=1}^{M} \varphi_{i_1}(e_n + d_1)...\varphi_{i_l}(e_n + d_l) = \pm V(E'_N, M, D). \tag{4.6}$$

Felhasználva (4.6),(4.4),(2.7) kapjuk, hogy

$$\Gamma_l(E_N) = \max_{\phi,M,D} |G(E_N, \phi, M, D)| = \max_{M,D} |V(E'_N, M, D)| = C_l(E'_N). \blacksquare$$

Következmény. A (4.3),(4.4) mértékek eleget tesznek a 3. fejezetben feltett 7. elvárásnak.

4.2. Az $f-$mértékek és az $\varepsilon-$mértékek közötti kapcsolat

A következőekben megmutatjuk, hogy az $f-$mértékek és az $\varepsilon-$mértékek között milyen szoros kapcsolat áll fent. Igazolható, hogy $E_N \in A^N$ sorozat esetén a (2.6), (2.7) és a (4.3), (4.4) mértékek legfeljebb egy konstans szorzóval térnek el egymástól, pontosabban:

4.2.1. Tétel. Bármely $k \in \mathbb{N}, k \geq 2, N \in \mathbb{N}, A = \{a_1, ..., a_k\}$ és $E_N \in A^N$ esetén

$$\tfrac{k}{k-1}\delta(E_N) \leq \Delta(E_N) \leq k\delta(E_N).$$

Megjegyzés. A bináris esetben $\Delta(E_N) = 2\delta(E_N)$.

Bizonyítás(4.2.1. Tétel). Bármely $\varphi \in F, M, u, v$ esetén

$$|x(E_N, \varphi, M, u, v)| =$$

$$= |\sum_{j=0}^{M-1} \varphi(e_{u+jv})| = \left| \sum_{a \in A} |\{j : j \leq M-1, e_{u+jv} = a\}| \varphi(a) \right| =$$

$$= \left|\sum_{a\in A} x(E_N,a,M,u,v)\varphi(a)\right| = \left|\sum_{a\in A}\left(x(E_N,a,M,u,v) - \tfrac{M}{k}\right)\varphi(a) + \tfrac{M}{k}\sum_{a\in A}\varphi(a)\right| =$$

$$= \left|\sum_{a\in A}\left(x(E_N,a,M,u,v) - \tfrac{M}{k}\right)\varphi(a)\right| \le \sum_{a\in A}\left|x(E_N,a,M,u,v) - \tfrac{M}{k}\right| \le$$

$$\le \sum_{a\in A}\delta(E_N) = k\delta(E_N).$$

Így megkaptuk a felső becslés igazolását. Az alsó becsléshez vegyünk olyan

$$F_i = \{\varphi : \varphi \in F, \varphi(a_i) = 1\}, \text{ hogy } |F_i| = (k-1)!.$$

Ekkor

$$\sum_{\varphi\in F_i}\varphi(a_i) = \sum_{\varphi\in F_i} 1 = |F_i| = (k-1)! \text{ és}$$

$$\sum_{\varphi\in F_i}\varphi(a_j) = \sum_{\substack{\epsilon\neq 1\\ \epsilon\in\varepsilon}} |\{\varphi : \varphi\in F_i, \varphi(a_j) = \epsilon\}|\epsilon = \sum_{\substack{\epsilon\neq 1\\ \epsilon\in\varepsilon}} (k-2)!\epsilon = -(k-2)!, \text{ ha } i \neq j.$$

Ebből adódik viszont, hogy

$$\sum_{\varphi\in F_i} x(E_N,\varphi,M,u,v) = \sum_{\varphi\in F_i}\sum_{j=0}^{M-1}\varphi(e_{u+jv}) =$$

$$= \sum_{\substack{0\le j<M\\ e_{u+jv}=a_j}} (k-1)! + \sum_{\substack{0\le j<M\\ e_{u+jv}\neq a_j}} (-(k-2)!) = k(k-2)!x(E_N,a_i,M,u,v) - M(k-2)!, \text{ ahol}$$

$$\left|x(E_N,a_i,M,u,v) - \tfrac{M}{k}\right| = \tfrac{1}{k}(k-2)!\left|\sum_{\varphi\in F_i} x(E_N,\varphi,M,u,v)\right| \le \tfrac{k-1}{k}\Delta(E_N). \blacksquare$$

4.2.2. Tétel. Bármely $k,l \in \mathbb{N}, k,l \ge 2, N \in \mathbb{N}, A = \{a_1,...,a_k\}$ és $E_N \in A^N$ esetén

$$\tfrac{1}{k^l}\Gamma_l(E_N) \le \gamma_l(E_N) \le \sum_{t=1}^{l}\binom{l}{t}(k-1)^t\Gamma_t(E_N).$$

Bizonyítás. ([13])

4.3. A $\Delta(E_N)$ és $\Gamma_l(E_N)$ becslése

A következőkben megmutatjuk, hogy egy véletlen $E_N \in A^N$ véletlen sorozatok (4.3) és (4.4) pontokban bemutatott $\varepsilon - eloszlási$ és $\varepsilon - korrelációs$ mértéke $\sqrt{N}$ körül van.

4.3.1. Tétel. Bármely $\varepsilon > 0 - hoz$ létezik olyan $N_0 = N_0(\varepsilon)$, hogy $N > N_0$ esetén $P(\Delta(E_N) > (16k^4 N log N)^{1/2}) < \varepsilon$.

Bizonyítás.

Minden $L > 0$ esetén

$$P(\Delta(E_N) > L) = P(\max_{\varphi,M,u,v} |X(E_N, \varphi, M, u, v)| > L) \leq$$

$$\leq \sum_{u,v,M} P(\max_{\varphi} |X(E_N, \varphi, M, u, v)| > L) \leq N^3 \max_{u,v,M} P(\max_{\varphi} |X(E_N, \varphi, M, u, v)| > L).$$

Megmutatjuk, hogy

$$P(\max_{\varphi} |X(E_N, \varphi, M, u, v)| > L) < \tfrac{2}{M^8},$$

minden lehetséges M, u, v esetén és

$$L = \sqrt{16k^4 M log M}.$$

Feltehetjük, hogy az e_{u+jv}, $(j = 0, ..., M-1)$ szimbólumok között $a_1 - ből$ n_1, $a_2 - ből$ $n_2, ...,$ $a_k - ból$ n_k, hogy $n_1 \geq ... \geq n_k$.

Jelöljük $\varphi_0 \in F$ a következő bijekciót :

$$\varphi_0(a_1) = 1 = \varepsilon^0, \varphi_0(a_2) = \varepsilon, ..., \varphi_0(a_k) = \varepsilon^{k-1}, \text{ ahol } \varepsilon = e^{\frac{2\pi i}{k}}.$$

A bizonyítás további lépéseihez szükségünk lesz az alábbi lemmára.

4.3.2. Lemma. Bármely $\varphi \in F$ esetén

$$\left| \sum_{j=0}^{M-1} \varphi(e_{u+jv}) \right| \leq [(n_1 - n_k) + ... + (n_{k-1} - n_k)] \leq k(n_1 - n_k).$$

Az előbb definiált φ_0 bijekció miatt

$$\tfrac{n_1-n_k}{2k} \leq \left|\sum_{j=0}^{M-1}\varphi(e_{u+jv})\right|.$$

Ebből adódik, hogy

$$\tfrac{n_1-n_k}{2k} \leq \max_{\varphi}|X(E_N,\varphi,M,u,v)| \leq k(n_1-n_k).$$

Bizonyítás(4.3.2. Lemma). Tetszőleges φ esetén

$$\left|\sum_{j=0}^{M-1}\varphi(e_{u+jv})\right| = |n_1\varphi(a_1)+...+n_k\varphi(a_k)| =$$

$$=|n_k(1+\varepsilon+\varepsilon^2+...+\varepsilon^{k-1})+\sum_{i=1}^{k-1}(n_i-n_k)\varphi(a_i)| \leq \sum_{i=1}^{k-1}(n_i-n_k).$$

Ezenkívűl a $\left\{z\in\mathbb{C}|arg(z)=-\frac{2\pi}{2k}\right\}$ egyenest választva látható, hogy a $\sum_{j=0}^{M-1}\varphi_0(e_{u+jv})$ komponens hossza, ami merőleges erre az egyenesre

$$(n_1-n_k)sin(\tfrac{\pi}{k})+(n_2-n_{k-1})sin(\tfrac{3\pi}{k})+...+(n_{k/2}-n_{k/2+1})sin(\tfrac{(k-1)\pi}{k})\geq$$

$$\geq \tfrac{1}{2k}[(n_1-n_k)+...+(n_{k/2}-n_{k/2+1})] \geq \tfrac{n_1-n_k}{2k}, \text{ ha } k \text{ páros.}$$

És

$$(n_1-n_k)sin(\tfrac{\pi}{k})+...+(n_{(k-1)/2}-n_{(k+3)/2})sin(\tfrac{(k-2)\pi}{k}) \geq$$

$$\geq \tfrac{1}{2k}[(n_1-n_k)+...+(n_{k/2}-n_{k/2+1})] \geq \tfrac{n_1-n_k}{2k}, \text{ha } k \text{ páratlan. } \blacksquare$$

Folytatva a 4.3.1. Tétel bizonyítását, felhasználva a 4.1.4. Lemma állítását kapjuk, hogy

$$P\left(\max_{\varphi}\left|\sum_{j=0}^{M-1}\varphi(e_{u+jv})\right|>L\right) \leq P(k(n_1-n_k)>L) = \tfrac{1}{k^M}\sum_{\substack{n_1+...+n_k=M\\ k(maxn_i-minn_i)>L}}\tfrac{M!}{n_1!...n_k!}.$$

Feltehető, hogy M osztható k-val, így

$$\tfrac{M!}{n_1!...n_k!} = \tfrac{M!}{(\frac{M}{k}-i_1)!(\frac{M}{k}-i_2)!...(\frac{M}{k}-i_j)!(\frac{M}{k}+i_{J+1})!...(\frac{M}{k}+i_k)!} = \tfrac{M!}{[(\frac{M}{k})!]^k}\cdot\tfrac{[\frac{M}{k}(\frac{M}{k}-1)...(\frac{M}{k}-i_1+1)]...[\frac{M}{k}(\frac{M}{k}-1)...(\frac{M}{k}-i_j+1)]}{[(\frac{M}{k}+1)...(\frac{M}{k}+i_{j+1})]...[(\frac{M}{k}+1)...(\frac{M}{k}+i_k)]},$$

ahol

$$\sum_{n=1}^{j} i_n = \sum_{m=j+1}^{k} i_m > \frac{L}{2k}.$$

Legyen most $i+j = o(a+j)$, ekkor

$$\log(\tfrac{a-i}{a+j}) = \log(1-\tfrac{i+j}{a+j}) = -\tfrac{i+j}{a+j} + \mathrm{O}((\tfrac{i+j}{a+j})^2).$$

Így

$$\log\tfrac{[\frac{M}{k}(\frac{M}{k}-1)\ldots(\frac{M}{k}-i_1+1)]\ldots[\frac{M}{k}(\frac{M}{k}-1)\ldots(\frac{M}{k}-i_j+1)]}{[(\frac{M}{k}+1)\ldots(\frac{M}{k}+i_{j+1})]\ldots[(\frac{M}{k}+1)\ldots(\frac{M}{k}+i_k)]} = \sum_{i,j}\log\tfrac{\frac{M}{k}-i}{\frac{M}{k}+j} < -\sum_{i,j}\tfrac{i+j}{M} + \sum_{i,j}\mathrm{O}\left(\tfrac{(i+j)^2}{(\frac{M}{k})^2}\right).$$

Itt

$$-\sum_{i,j}\tfrac{i+j}{M} = -\tfrac{(1+2+\ldots+i_1)+\ldots+(1+2+\ldots+i_k)}{M} + \tfrac{i_1+\ldots+i_j}{M} \leq -\tfrac{i_1^2+\ldots+i_k^2}{2M} \leq -\tfrac{\frac{(\sum i_s)^2}{k}}{2M} < -\tfrac{\frac{L^2}{k^3}}{2M} < -\tfrac{L^2}{2k^3M}.$$

Ha $i_1+i_2+\ldots+i_k = \mathrm{o}(\frac{M^{2/3}}{\sqrt{k}})$, akkor mivel minden (i,j) párra $i+j < i_1+i_2+\ldots+i_k$,

$$\sum_{i,j}\mathrm{O}\left(\tfrac{(i+j)^2}{(\frac{M}{k})^2}\right) \leq \sum_{i,j}\mathrm{o}\left(\tfrac{\frac{M^{4/3}}{k}}{(\frac{M}{k})^2}\right) = \sum_{\mathrm{i,j}}\mathrm{o}\left(\tfrac{kM^{4/3}}{M^2}\right) = \mathrm{o}\left(\tfrac{M^{2/3}kM^{4/3}}{\sqrt{k}M^2}\right) = \mathrm{o}(1).$$

Ekkor mivel $i_1+i_2+\ldots+i_k = \mathrm{o}(\frac{M^{2/3}}{\sqrt{k}})$ kapjuk, hogy

$$\tfrac{M!}{n_1!\ldots n_k!} < \tfrac{M!}{[(\frac{M}{k})!]^k}\exp\left(-\tfrac{L^2}{2Mk^3} + \mathrm{o}(1)\right),$$

majd felhasználjuk, hogy

$$\tfrac{M!}{n_1!\ldots n_k!} < \tfrac{M!}{n_1^\star!\ldots n_k^\star!}, \text{ ha } i_1+\ldots+i_k > i_1^\star+\ldots+i_k^\star \text{ és } n_1-n_k \leq i_1+\ldots+i_k.$$

Ebből már adódik, hogy

$$P\left(\max_{\varphi}\left|\sum_{j=0}^{M-1}\varphi(e_{u+jv})\right| > L\right) < \tfrac{1}{k^M}\sum_{i_1+\ldots+i_k>\frac{L}{k}}\tfrac{M!}{n_1!\ldots n_k!} <$$

$$< \tfrac{1}{k^M}\tfrac{M!}{[(\frac{M}{k})!]^k}M^k\exp\left(-\tfrac{L^2}{2Mk^3} + o(1)\right).$$

Fixáljuk most $L-$et, legyen $L = \sqrt{16Mk^4\log M}$. Mivel $\frac{1}{k^M}\frac{M!}{[(\frac{M}{k})!]^k} < 1$ kapjuk, hogy

$$\frac{1}{k^M}\frac{M!}{[(\frac{M}{k})!]^k}M^k\exp\left(-\frac{L^2}{2Mk^3}+\mathrm{o}(1)\right) < M^k\exp\left(-\sqrt{16Mk^4\log M}^2\frac{1}{2Mk^3}+\mathrm{o}(1)\right) =$$

$$= M^k\exp\left(-8k\log M+\mathrm{o}(1)\right) = \frac{M^k}{M^{8k}}(1+\mathrm{o}(1)) < \frac{2}{M^8}.$$

Ha $M < \sqrt{16Nk^4\log N}$, akkor

$$P(\max_{\varphi}|X(E_N,\varphi,M,u,v)| > \sqrt{16Nk^4\log N}) = 0.$$

Feltehetjük ezután, hogy $M > \sqrt{16Nk^4\log N}$, ekkor viszont

$$\max_{u,v,M} P\left(\max_{\varphi}|X(E_N,\varphi,M,u,v)| > \sqrt{16Nk^4\log N}\right) =$$

$$= \max_{\substack{M>\sqrt{16Nk^4\log N}\\ u,v,M}} P\left(\max_{\varphi}|X(E_N,\varphi,M,u,v)| > \sqrt{16Nk^4\log N}\right) \leq$$

$$\leq \max_{\substack{M>\sqrt{16Nk^4\log N}\\ u,v,M}} P\left(\max_{\varphi}|X(E_N,\varphi,M,u,v)| > \sqrt{16Mk^4\log M}\right) \leq$$

$$\leq \max_{\substack{M>\sqrt{16Nk^4\log N}\\ u,v,M}} \frac{2}{M^8} < \frac{2}{(16k^4N\log N)^4} < \frac{1}{N^4}. \blacksquare$$

4.3.3. Tétel. Bármely $\varepsilon > 0$ - hoz léteznek olyan $N_0 = N_0(\varepsilon)$ és $\delta = \delta(\varepsilon)$, hogy $N > N_0$ esetén $P\left(\Delta(E_N) > \delta\frac{\sqrt{N}}{k\sqrt{k}}\right) > 1-\varepsilon$.

Bizonyítás. ([15])

4.3.4. Tétel. Bármely $k \in \mathbb{N}, k \geq 2$ és $\varepsilon > 0$ esetén létezik olyan $N_0 = N_0(\varepsilon)$ és $\delta = \delta(\varepsilon)$, hogy $P\left(\Gamma_l(E_N) > \delta\frac{\sqrt{N}}{k\sqrt{k}}\right) > 1-\varepsilon$.

Bizonyítás. Ha $N > 2l$, akkor

$$\Gamma_l(E_N) \geq \max_{\phi}|G(E_N,\phi,\lfloor\tfrac{N}{2}\rfloor - l,(0,1,...,l-2,\lfloor\tfrac{N}{2}\rfloor))| =$$

$$= \max_{\phi} \left| \sum_{n=1}^{\left\lfloor \frac{N}{2} \right\rfloor - l} \varphi_1(e_n)....\varphi_l(e_{n+\left\lfloor N/2 \right\rfloor}) \right|.$$

Emiatt

$$P\left(\Gamma_l(E_N) > \delta\tfrac{\sqrt{N}}{k\sqrt{k}}\right) \geq P\left(\max_{\phi} \left| \sum_{n=1}^{\left\lfloor \frac{N}{2} \right\rfloor - l} \varphi_1(e_n)...\varphi_l(e_{n+\left\lfloor N/2 \right\rfloor} \right| > \delta\tfrac{\sqrt{N}}{k\sqrt{k}}\right). \tag{4.7}$$

Elég belátni tehát, hogy (4.7) egyenlőtlenség jobboldala $> 1-\varepsilon$-nál ($\star$).

Legyen $u = (e_n, ..., e_{n+l-2})$ és $f_n = \overline{\varphi_1(e_n)...\varphi_{l-1}(e_{n+l-2})}$, ezenkívűl igaz, hogy $\varphi_l(e_{n+\left\lfloor N/2 \right\rfloor}) = f_n g_n$.

Mivel g_n k-adik egységgyök, így

$$g_n = \varphi_l(b_n),$$

ahol $b_n \in \{a_1, ..., a_k\}$, hiszen $\varphi_l(e_{n+\left\lfloor N/2 \right\rfloor})$ felvesz $1, \varepsilon, ..., \varepsilon^{k-1}$ értékeket függetlenül, $1/k$ valószínűséggel.

Másfelől azonban

$$\varphi_1(e_n)...\varphi_l(e_{n+\left\lfloor N/2 \right\rfloor}) = \overline{f}_n f_n g_n = g_n.$$

Tehát ($\star$) ekvivalens az alábbival :

$$P\left(\max_{\varphi_l} \left| \sum_{n=1}^{\left\lfloor N/2 \right\rfloor - l} \varphi_l(b_n) \right| > \delta\tfrac{\sqrt{N}}{k\sqrt{k}}\right) > 1-\varepsilon,$$

ahol $b_1, ..., b_{\left\lfloor N/2 \right\rfloor - l}$ felveszi a k szimbólumot függetlenül, $1/k$ valószínűséggel. De ez már szerepelt a 4.3.3. Tétel bizonyításában. ■

4.3.5. Tétel. Legyen $\varepsilon > 0$ és $l \in \mathbb{N}$. Ekkor bármely páros $k \in \mathbb{N}$ mellett van olyan $N_0 = N_0(\varepsilon, k, l)$ szám, hogy $N > N_0$ esetén $P(\Gamma_l(E_N) > 10(klN\log N)^{1/2}) < \varepsilon$.

Bizonyítás. ([15])

4.4. Egy konstrukció

Általánosítsuk a 2. fejezetben szereplő Legendre szimbólumokon használt konstrukciót $k \geq 2$ esetére. Ehhez vegyünk egy p prímet, amelyre $p \equiv 1 \ (mod\ k)$ és $N = p-1$. Legyen $A = \left\{ e(\frac{j}{k}) : j = 0, 1, ..., k-1 \right\}$, g primitív gyök modulo p és $\chi_1(g) = e(\frac{1}{k})$, ezenkívül ha $1 \leq n \leq N = p-1$, akkor $\chi_1(n) \in A$.

Definiáljuk $E_N = (e_1, ..., e_N)$ sorozatot az alábbi módon : $e_n = \chi_1(n)$ $(n \in \{1, 2, ..., N\})$. Célunk megmutatni, hogy az így definiált E_N sorozat jó pszeudovéletlen tulajdonságokkal rendelkezik. Ennek belátását, az alábbi tétel segíti.

4.4.1. Tétel. A fent szereplő E_N sorozat esetén igaz, hogy

$$\text{i.)}\ \delta(E_N) < 2N^{1/2}\log N;$$

$$\text{ii.)}\ \text{minden } l \in \mathbb{N}, l \leq N \text{ esetén } \gamma_l(E_N) < 27klN^{1/2}\log N.$$

A 4.4.1. Tétel bizonyításához az alábbi lemmákra lesz szükségünk, bizonyításaik megtalálhatóak C. Mauduit és A. Sárközy [13] cikkében és H. Davenport [7] könyvében.

4.4.2. Lemma. Ha p prím, χ karakter modulo p, de különbözik a χ_0 főkaraktertől modulo p. Legyen X, Y valós számok, $X < Y$, ekkor $\left| \sum_{X<n<Y} \chi(n) \right| < p^{1/2}\log p$.

4.4.3. Lemma. Tegyük fel, hogy p prím, χ egy $d - rendű$ nem főkarakter modulo p, $f(x) \in F_p[x]$ $h - fokú$ polinom és $f(x) = b(x-x_1)^{d_1}...(x-x_s)^{d_s}$ $\overline{F}_p$–ben, ahol $x_i \neq x_j$ $(i \neq j)$ és $(d, d_1, ..., d_s) = 1$. Legyen ezenkívül X, Y valósak, $0 < Y \leq p$. Ekkor $\left| \sum_{X<n\leq X+Y} \chi(f(n)) \right| < 9hp^{1/2}\log p$.

4.4.4. Lemma. A 4.4.3. Lemma igaz marad, ha $(d, d_1, ..., d_s) < d$.

Bizonyítás.

i.)

Írjunk

$$S(a, m) = \frac{1}{k}\sum_{t=0}^{k-1} (\overline{a}\chi_1(m))^t,$$

bármely $a \in A, (m,p) = 1$ mellett.

Nyílván

$$S(a,m) = \begin{cases} 1, ha & \chi_1(m) = a \\ 0, ha & \chi_1(m) \neq a \end{cases}.$$

Ezért bármely $a \in A, u + (M-1)v \leq N$ esetén

$$x(E_N, a, M, u, v) =$$

$$= \sum_{\substack{0 \leq j \leq M-1 \\ e_{u+jv}=a}} 1 = \sum_{\substack{0 \leq j \leq M-1 \\ \chi_1(u+jv)=a}} 1 = \sum_{j=0}^{M-1} S(a, u+jv) = \tfrac{1}{k}M + \tfrac{1}{k}\sum_{t=1}^{k-1}\overline{a}^t \sum_{j=0}^{M-1}\chi_1^t(u+jv).$$

Ezt felhasználva

$$\left| x(E_N, a, M, u, v) - \tfrac{M}{k} \right| \leq \tfrac{1}{k}\sum_{t=1}^{k-1}\left| \sum_{j=0}^{M-1}\chi_1^t(u+jv) \right|. \tag{4.8}$$

Írjunk most $\chi_2 = \chi_1^t$, ahol $1 \leq t \leq k-1$ és χ_2 is karakter modulo p, de $\chi_2 \neq \chi_0$. Ekkor azonban

$$\left| \sum_{j=0}^{M-1}\chi_2(u+jv) \right| = \left| \overline{\chi}_2(v) \sum_{j=0}^{M-1}\chi_2(u+jv) \right| = \left| \sum_{j=0}^{M-1}\chi_2(uv^{-1}+j) \right| < p^{1/2} logp. \tag{4.9}$$

A (4.8) és (4.9) pontok alapján ekkor viszont

$$\left| x(E_N, a, M, u, v) - \tfrac{M}{k} \right| \leq \tfrac{1}{k}(k-1)p^{1/2}logp < p^{1/2}logp < 2N^{1/2}logN. \blacksquare$$

ii.) A bizonyításhoz felhasználjuk a 4.4.3. és 4.4.4. Lemmát.

Legyen $l, M \in N$, $l \leq N$, $w = (b_1, ..., b_l) \in A^l$, $D = (d_1, ..., d_l)$, $0 \leq d_1 < ... < d_l$ és $M + d_l \leq N$.

Ekkor azonban a bizonyítás i.) részében szereplő $S(a,m)$ definíciója miatt

$$g(E_N, w, M, D) =$$

$$= |\{n : 1 \leq n \leq M, (e_{n+d_1}, ..., e_{n+d_l}) = w\}| = \sum_{n=1}^{M} \prod_{j=1}^{l} S(b_j, n + d_j) =$$

$$= \sum_{n=1}^{M} \prod_{j=1}^{l} \left(\frac{1}{k} \sum_{t=0}^{k-1} (\bar{b}_j \chi_1(n + d_j))^t \right) = \frac{1}{k^l} \sum_{0 \leq t_1, ..., t_l \leq k-1} \bar{b}_1^{t_1} ... \bar{b}_l^{t_l} \sum_{n=1}^{M} \chi((n + d_1)^{t_1} ... (n + d_l)^{t_l}). \quad (4.10)$$

Mivel a $t_1 = ... = t_l = 0$ tagok eredménye $\frac{M}{k^l}$, így

$$\left| g(E_N, w, M, D) - \frac{M}{k^l} \right| =$$

$$= \frac{1}{k^l} \left| \sum_{\substack{0 \leq t_1, .., t_l \leq k-1 \\ (t_1, ..., t_l) \neq (0, ..., 0)}} \bar{b}_1^{t_1} ... \bar{b}_l^{t_l} \sum_{n=1}^{M} \chi_1((n + d_1)^{t_1} ... (n + d_l)^{t_l}) \right| \leq$$

$$\leq \max_{\substack{0 \leq t_1, ..., t_l \leq k-1 \\ (t_1, ..., t_l) \neq (0, ..., 0)}} \left| \sum_{n=1}^{M} \chi_1((n + d_1)^{t_1} ... (n + d_l)^{t_l}) \right|.$$

Mivel $0 \leq t_1, ..., t_l \leq k - 1$, $(t_1, ..., t_l) \neq (0, ..., 0)$ és $f(n) = (n + d_1)^{t_1} ... (n + d_l)^{t_l}$. Ezért létezik legalább egy olyan t_i, hogy $(k, t_1, ..., t_l) < k$.

Használjuk fel a 4.4.4. lemmát a (4.10) becslésére, ekkor

$$\left| \sum_{n=1}^{M} \chi_1((n + d_1)^{t_1} ... (n + d_l)^{t_l}) \right| <$$

$$< 9(t_1 + ... + t_l) p^{1/2} log p < 9klp^{1/2} log p < 27klN^{1/2} log N. \blacksquare$$

4.5. A $k = 4$ eset

Az 2. fejezetben bináris sorozatokkal foglalkoztunk, majd ezt követően kitértünk a k szimbólumot tartalmazó sorozatok vizsgálatára. Most tekintsük a $k = 4$ speciális esetet és nézzük meg a kapcsolatot ezen sorozatok és a bináris sorozatok között.

Legyen $E_N, F_N \in \{-1, 1\}^N$ két N hosszúságú bináris sorozat. Készítsük el a $G_N \in \{1, -1, i, -i\}^N = \varepsilon^N$ sorozatot, melynek elemeire teljesül, hogy

$$g_n = \frac{(1+i)e_n+(1-i)f_n}{2},\ n = 1, 2, ..., N \text{ (ez az ún. Gray mapping).} \tag{4.11}$$

Megfordítva, vegyük a negyedik egységgyökök ε halmazát és legyen $G_N \in \varepsilon^N$ egy 4 elemből képezett sorozat. Ekkor definiálhatunk két bináris sorozatot, $E_N, F_N \in \{-1, 1\}^N$ az alábbi módon

$$e_n = \frac{(1-i)g_n+(1+i)\overline{g}_n}{2} \text{ és } f_n = \frac{(1+i)g_n+(1-i)\overline{g}_n}{2}, \text{ ahol } n = 1, 2, ..., N. \tag{4.12}$$

Megjegyzés. A (4.12) pontban $\overline{x}$ jelöli x komplex konjugáltját.

Legyen $G_N \in \{1, -1, i, -i\}^N$ és $E_N, F_N \in \{1, -1\}^N$ két sorozat. Készítsük el az $E_N F_N$ szorzat bináris sorozatot. A következő tételekben ([17] nyomán) megmutatjuk, hogy milyen kapcsolat van $E_N, F_N, E_N F_N$ sorozatok véletlenségi mértékei és a G_N sorozat mértékei között.

4.5.1. Tétel. Legyen G_N sorozat, E_N, F_N két bináris sorozat (ld. (4.12)). Ekkor

$$\max\{W(E_N), W(F_N)\} \leq \sqrt{2}\Delta(G_N) \text{ és } W(E_N F_N) \leq 3\Delta(G_N)\ .$$

Megfordítva, legyen E_N, F_N két bináris sorozat és G_N a fenti sorozat (ld. (4.11)). Ekkor

$$\Delta(G_N) \leq \sqrt{2}\max\{W(E_N), W(F_N), W(E_N F_N)\}.$$

Bizonyítás.

Felhasználva (4.12)-t kapjuk, hogy

$$\left|\sum_{j=0}^{M-1} e_{u+jv}\right| \leq \frac{|1-i|}{2}\left|\sum_{j=0}^{M-1} g_{u+jv}\right| + \frac{|1+i|}{2}\left|\sum_{j=0}^{M-1}\overline{g_{u+jv}}\right| \leq \sqrt{2}\Delta(G_N),$$

$$\left|\sum_{j=0}^{M-1} f_{u+jv}\right| \leq \frac{|1+i|}{2}\left|\sum_{j=0}^{M-1} g_{u+jv}\right| + \frac{|1-i|}{2}\left|\sum_{j=0}^{M-1}\overline{g_{u+jv}}\right| \leq \sqrt{2}\Delta(G_N).$$

Készítsük el az $E_N F_N$ szorzatot. Nyílvánvalóan

$$e_n f_n = i(g_n - \phi_1(g_n) - \phi_2(g_n)),$$

ahol ϕ_1, ϕ_2 jelöli az $1 \leftrightarrow i, -1 \leftrightarrow i$ cserét. Ekkor

$$\left|\sum_{j=0}^{M-1} e_{u+jv} f_{u+jv}\right| \leq \left|\sum_{j=0}^{M-1} g_{u+jv}\right| + \left|\sum_{j=0}^{M-1} \phi_1(g_{u+jv})\right| + \left|\sum_{j=0}^{M-1} \phi_2(g_{u+jv})\right| \leq 3\Delta(G_N).$$

Eddig beláttuk az első és a második részét a tételnek. A harmadik részhez használjuk fel a (4.11) pontot, így kapjuk, hogy

$$\phi_1(g_n) = \tfrac{(i+1)e_n + (i-1)e_n f_n}{2} \text{ és } \phi_2(g_n) = \tfrac{(1-i)f_n + (i+1)e_n f_n}{2}, \text{ ezért}$$

$$\left|\sum_{j=0}^{M-1} g_{u+jv}\right| \leq \tfrac{1}{\sqrt{2}}(W(E_N) + W(F_N)),$$

$$\left|\sum_{j=0}^{M-1} \phi_1(g_{u+jv})\right| \leq \tfrac{1}{\sqrt{2}}(W(E_N) + W(E_N F_N)) \text{ és}$$

$$\left|\sum_{j=0}^{M-1} \phi_2(g_{u+jv})\right| \leq \tfrac{1}{\sqrt{2}}(W(F_N) + W(E_N F_N)). \blacksquare$$

A következő tételünk miatt szükségünk lesz bináris sorozatok kereszt-korrelációs mértékére. Legyen $H_1 \in \{-1,1\}^N$, $H_2 \in \{-1,1\}^N$,..., $H_k \in \{-1,1\}^N$ ilyen sorozat.

4.5.2. Definíció. A $H_1, ..., H_k$ sorozatok kereszt-korrelációs mértéke:

$$C_k(H_1, ..., H_k) = \max_{M,D} \left|\sum_{n=1}^{M} h_{n+d_1,1} h_{n+d_2,2} ... h_{n+d_k,k}\right|, \tag{4.13}$$

ahol $D = (d_1, ..., d_k)$ és $0 \leq d_1 < ... < d_k \leq N - M$.

4.5.3. Tétel. Legyen $G_N \in \varepsilon^N$ sorozat és E_N, F_N két bináris sorozat (ld. (4.12)). Ekkor

$$\max\{C_k(E_N), C_k(F_N)\} \leq 2^{k/2}\Gamma_k(G_N) \text{ és } \max C_k(H_1, ..., H_k) \leq 3^k \Gamma_k(G_N),$$

ahol $(H_1, ..., H_k) \in \{E_N, F_N, E_N F_N\}^k$.

Megfordítva, legyen E_N, F_N két bináris sorozat és G_N egy fenti sorozat (ld. (4.11)). Ekkor

$$\Gamma_k(G_N) \leq 2^{k/2} \max C_k(H_1, ..., H_k),$$

ahol $(H_1, ..., H_k) \in \{E_N, F_N, E_N F_N\}^k$.

Bizonyítás. ([17])

5. fejezet

A k szimbólumból képezett pszeudovéletlen rácsok

5.1. Bevezetés

Az alkalmazásokban, például a több dimenziós képek,térképek titkosításában szükségesség vált a pszeudovéletlen rácsok használata. Emiatt P. Hubert, C. Mauduit és A. Sárközy 2006-ban a [14] cikkükben kiterjesztették a pszeudovéletlen bináris sorozatok fogalmát több dimenzióra. Ebben az alszakaszban néhány lépésben összefoglaljuk az előbb említett szerzők fontosabb eredményeit a pszeudovéletlen bináris rácsokra vonatkozóan, majd az 5.2. alszakaszban kitérünk részletesebben a $k-$szimbólumok esetére.

Legyen az $n-$dimenziós I_N^n vektorok halmaza a következő:

$$I_N^n = \{\mathbf{x} = (x_1, ..., x_n) : x_1, ..., x_n \in \{0, 1, ..., N-1\}\}. \tag{5.1}$$

Az I_N^n halmazt $N-$rácsnak nevezzük. Ekkor bináris rácsnak hívjuk a

$$\eta : I_N^n \to \{-1, 1\} \tag{5.2}$$

függvényt. A szemléltetés miatt gondolhatunk erre a függvényre úgy, mint egy $N-$rács, amelyben a rácspontokat a $\pm$ előjelekkel helyettesítjük.

Hasonlóan az egydimenziós esethez ($n = 1$) definiálhatunk mértékeket, ehhez vegyük az $\mathbf{u}_i$ $(i = 1, ..., n)$ lineárisan független vektorokat, amelyeknek az i-edik $(i = 1, ..., n)$ koordinátája egy pozitív egész szám, míg a többi 0. Legyen továbbá $t_1, ..., t_n$ olyan egész, ahol $0 \leq t_1, ..., t_n < N$. Ekkor a

$$B_N^n = \{\mathbf{x} = x_1\mathbf{u}_1 + ... + x_n\mathbf{u}_n : 0 \leq x_i|\mathbf{u}_i| \leq t_i(< N), i = 1, ..., n\} \tag{5.3}$$

halmazt $N-$téglarácsnak nevezzük.

5.1.1. Definíció. Az $l-$rendű pszeudovéletlen mértéke $\eta-$nak :

$$Q_l(\eta) = \max_{B,\mathbf{d_1},...,\mathbf{d_l}} \left| \sum_{\mathbf{x}\in B} \eta(x + \mathbf{d}_1)...\eta(x + \mathbf{d}_l) \right|, \tag{5.4}$$

ahol $B + \mathbf{d}_1, ..., B + \mathbf{d}_l \subseteq I_N^n$ és $\mathbf{d_1}, ..., \mathbf{d_l} \in I_N^n$.

A [14] cikkben a szerzők vizsgálták az (5.4) mértékeket a valódi véletlen esetben, (azaz amikor $P(\eta(\mathbf{x}_i) = \pm 1) = \frac{1}{2}$, $i = 1, ..., n$) és bebizonyították, hogy $N^{n/2} \ll Q_l(\eta) \ll N^{n/2}(\log N^n)^{1/2}$ teljesül $(1 - \varepsilon)$-nál nagyobb valószínűséggel, fix l mellett.

5.2. A k szimbólum esete

Hasonlóan a bináris esethez, kiterjeszthetjük a k-szimbólumok sorozatát a k-szimbólumok rácsaira, mégpedig a $\eta : I_N^n \to A$ által. A $k-$szimbólumból képezett rácsok pszeudovéletlenségi mértékét definiáljuk az alábbi módon :

5.2.1. Definíció. Legyen

$$\Omega_l(\eta) = \max_{\mathbf{B},\mathbf{D},\mathbf{T},\Phi} \left|\omega_l(\eta, \mathbf{B}, \mathbf{D}, \mathbf{T}, \Phi)\right| \text{ és}$$

$$\omega_l(\eta, \mathbf{B}, \mathbf{D}, \mathbf{T}, \Phi) = \sum_{j_1=0}^{t_1} ... \sum_{j_n=0}^{t_n} \varphi_1(\eta(j_1b_1\mathbf{u}_1 + ... + j_nb_n\mathbf{u}_n + \mathbf{d}_1))...$$

$$...\varphi_l(\eta(j_1b_1\mathbf{u}_1 + ... + j_nb_n\mathbf{u}_n + \mathbf{d}_l)), \tag{5.5}$$

ahol $\mathbf{B} = (b_1, ..., b_n), \mathbf{T} = (t_1, ..., t_n), \mathbf{D} = (\mathbf{d}_1, ..., \mathbf{d}_l)$,$t_i (i = 1, ..., n)$ nem negatív egészek,$b_i (i = 1, ..., n)$ nem nulla,$d_i (i = 1, ..., l)$ különbözőek, $\sum_{k=1}^{n} j_k b_k \mathbf{u}_k + \mathbf{d}_i \in I_N^n$ és $\Phi \in F^l$.

Megjegyzés. Az 5.2.1. Definícióban bemutatott mérték megegyezik az 5.1.1. Definícióban szereplő $\varepsilon-$korrelációs mértékkel. A $\eta-$t „jó" pszeudovéletlen rácsnak fogjuk nevezni, ha a (5.5) mértéke „kicsi", azaz $\Omega_l(\eta) = o(N^n)$, ha $N \to \infty$ és l „kicsi".

Legyen a következőkben $N, n \in \mathbb{N}$, $Z = |I_N^n| = N^n$. Ezenkívűl jelöljük I_N^n elemeit $\mathbf{x}_1, ..., \mathbf{x}_Z$ és A-val a k-szimbólumok halmazát. Megmutatjuk, hogy az $\Omega_l(\eta)$ mérték valódi véletlen esetben, azaz amikor $P(\eta(\mathbf{x}) = a) = \frac{1}{k}$, ahol $a \in A$ nagyjából $N^{n/2}$ körül ingadozik. A tétel csak kimondjuk, a részletes bizonyítás megtalálható Mérai László [21] cikkében.

5.2.2. Tétel. Ha $k, l \in \mathbb{N}, \varepsilon > 0$, akkor létezik olyan $N_0 = N_0(k, l, \varepsilon)$ és $\delta = \delta(k, l, \varepsilon)$, hogy $N > N_0$ esetén teljesül

$$\text{i.)}\ P\left(\Omega_l(\eta) > \delta \frac{N^{n/2}}{k\sqrt{k}}\right) \geq 1 - \varepsilon \text{ és}$$

$$\text{ii.)}\ P\left(\Omega_l(\eta) > 84k^2(lN^n \log N^n)^{1/2}\right) < \varepsilon.$$

Következmény. Közel hasonló becslést adtunk így a $k-$szimbólumos esetre, mint amelyet P. Hubert, C. Mauduit, A. Sárközy adott a [14] cikkükben bináris esetben.

5.3. Egy konstrukció

Legyen p $(k|p-1)$ prím, $A = \left\{e\left(\frac{j}{k}\right) : j = 0, ..., k-1\right\}$ halmaz. Vegyünk egy $\mathbf{v}_1, ..., \mathbf{v}_n \in F_q$ bázist F_p felett, ahol $q = p^n$. Ezenkívűl legyen $\mathbf{g} \in F_q$ mellett $\chi_1(\mathbf{g}) = e\left(\frac{1}{k}\right)$. Definiáljuk a rácsot az alábbi módon bármely $x_1, ..., x_n \in F_p$ esetén

$$\eta(\mathbf{x}) = \begin{cases} \chi_1(x_1\mathbf{v}_1 + ... + x_n\mathbf{v}_n), & ha \quad x_1\mathbf{v}_1 + ... + x_n\mathbf{v}_n \neq 0, \\ 1, & különben. \end{cases} \tag{5.6}$$

5.3.1. Tétel. Ha p prím, $k, l, n \in \mathbb{N}$, akkor a (5.6) pontban definiált rácsra igaz, hogy $\Omega_l(\eta) < klq^{1/2}(1 + \log p)^n$.

Bizonyítás.

Legyen

$$B = \left\{ \sum_{i=1}^{n} j_i b_i \mathbf{v}_i : 0 \leq j_i \leq t_i \right\}.$$

Ekkor

$$|\omega_l(\eta, B, D, T, \Phi)| = \left| \sum_{x \in B} \varphi_1(\chi_1(\mathbf{x} + \mathbf{d}_1)) ... \varphi_l(\chi_1(\mathbf{x} + \mathbf{d}_l)) \right| =$$

$$= \left| \sum_{(a_1,...,a_l) \in A^l} |\{\mathbf{x} \in B : \varphi_j(\chi_1(\mathbf{x} + \mathbf{d}_j)) = a_j, j = 1, ..., l\}| \cdot \varphi_1(a_1) ... \varphi_l(a_l) \right| \leq$$

$$\leq \sum_{(a_1,...,a_l) \in A^l} \left| |\{\mathbf{x} \in B : \chi_1(\mathbf{x} + \mathbf{d}_j) = a_j, j = 1, ..., l\}| - \tfrac{M}{k^l} \right| + \tfrac{M}{k^l} \left| \sum_{(a_1,...,a_l) \in A^l} a_1 ... a_l \right|.$$

Használjuk fel, hogy

$$\tfrac{1}{k} \sum_{r=0}^{k-1} \mathbf{z}^r = \begin{cases} 1, ha & \mathbf{z} = 1 \\ 0 & különben \end{cases} \quad \text{és} \quad \sum_{(a_1,...,a_l) \in A^l} a_1 ... a_l = 0.$$

Ekkor azonban

$$|\{x \in B : (\chi_1(\mathbf{x} + \mathbf{d}_1), ..., \chi_1(\mathbf{x} + \mathbf{d}_l)) = (a_1, ..., a_l)\}| =$$

$$= \tfrac{1}{k^l} \sum_{0 \leq r_1,...,r_l < k} \overline{a}_1^{r_1} ... \overline{a}_l^{r_l} \sum_{\mathbf{x} \in B} \chi_1(\mathbf{x} + \mathbf{d}_1)^{r_1} ... \chi_1(\mathbf{x} + \mathbf{d}_l)^{r_l} \leq$$

$$\leq \tfrac{1}{k^l} \sum_{0 \leq r_1,...,r_l < k} \left| \sum_{\mathbf{x} \in B} \chi_1((\mathbf{x} + \mathbf{d}_1)^{r_1} ... (\mathbf{x} + \mathbf{d}_l)^{r_l}) \right|.$$

Mivel az $r_1 = ... = r_l = 0$ tagok adaléka $\frac{M}{k^l}$, így

$$\left|\sum_{\mathbf{x}\in B}\varphi_1(\chi_1(\mathbf{x}+\mathbf{d}_1))...\varphi_l(\chi_l(\mathbf{x}+\mathbf{d}_l))\right| \leq \max_{(r_1,...,r_l)\neq(0,...,0)}\left|\sum_{\mathbf{x}\in B}\chi_1((\mathbf{x}+\mathbf{d}_1)^{r_1}...(\mathbf{x}+\mathbf{d}_l)^{r_l})\right|.$$

A folytatáshoz szükségünk lesz az alábbi lemmára, melynek bizonyítása megtalálható Winterhof [22] cikkében.

5.3.2. LEMMA. Ha p, q, n, $v_1, ..., v_n$ olyan mint fent, χ egy $d-$rendű multiplikatív F_q-beli karakter, $f \in F_q[x]$ nem konstans polinom, amely nem d-edik hatvány és amelynek m különböző gyöke van az osztási mezején F_q felett. Ezenkívűl $t_1, ..., t_n$ pozitív egészek, $t_1, ..., t_n \leq p$. Ekkor $B = \left\{\sum_{i=1}^{n} j_i\mathbf{v}_i : 0 \leq j_i < t_i\right\}$ jelölést használva

$$\left|\sum_{\mathbf{x}\in B}\chi(f(z))\right| < mq^{1/2}(1+\log p)^n.$$

Visszatérve a bizonyításhoz legyen

$$(r_1, ..., r_l) \neq (0, ..., 0),\ 0 \leq r_1, ..., r_l \leq k-1 \text{ és } f(\mathbf{x}) = (\mathbf{x}+\mathbf{d}_1)^{r_1}...(\mathbf{x}+\mathbf{d}_l)^{r_l}.$$

Ekkor felhasználva a 5.3.2. Lemmát kapjuk, hogy

$$\left|\sum_{\mathbf{x}\in B} f(\mathbf{x})\right| < (r_1 + ... + r_l)q^{1/2}(1+\log p)^n < klq^{1/2}(1+\log p)^n. \blacksquare$$

Következmény. A (5.6) pontban definiált rács jó pszeudovéletlen tulajdonságokkal rendelkezik.

6. fejezet

Alkalmazás

Jelen fejezetben a célom, hogy bizonyos k-szimbólumot (k=4 és k=8) tartalmazó sorozatok esetén kiszámoljam ezen sorozatok (4. fejezetben definiált) $\varepsilon-$mértékét, Γ_1-,illetve Γ_2-mértékét. A korábbi meggondolások alapján az elvárás az, hogy ezek az értékek nagyjából a vizsgált sorozat hosszának a gyöke körül ingadozzanak. Az időigény miatt csak rövidebb sorozatokra tesztelek, ugyanis kicsivel nagyobb sorozat esetén a futásidő akár megtöbbszörösödhet. Ezenkívül csak a fontosabb eredményeket közlöm a példák során, a teljes algoritmusok a mellékelt CD-n helyezkednek el, ezeket később jelzem is.

6.1. $\Delta, \Gamma_1, \Gamma_2$ mértékek

6.1.1. Példa 1.

Vegyük a következő függvényt és prímet (ügyelve arra, hogy $4|p-1$) :

- $f_1(x) := 12x^5 + 13x^4 - 14x^3 + 15x^2 - 16x + 17$
- $p := 101$

Definiáljuk az $E_{101} = (e_1, ..., e_{101})$ negyedik (komplex) egységgyökök (k=4) sorozatát a következőképpen (ld. 3.3.5. Tétel) :

$$e_n = \begin{cases} \chi_{(4)}(f_1(n)), & (f_1(n), p) = 1 \\ 1, & p|f_1(n). \end{cases}$$

Megjegyzés. Az így legyártott E_{101} elemeinek véletlenszerűen tartalmazza a negyedik egységgyököket.

A szemléltetés kedvéért a következőkben kiszámolom az eloszlási mérték néhány értékét bizonyos paraméter választások esetén, ezeket az alábbi táblázatban foglalom össze :

	$M-1$	u	v	Δ		$M-1$	u	v	Δ		$M-1$	u	v	Δ
1.	20	1	1	1	*13.*	40	2	1	$\sqrt{5}$	*25.*	60	3	1	2
2.	20	1	2	$\sqrt{13}$	*14.*	40	2	2	$\sqrt{29}$	*26.*	60	3	2	$4\sqrt{2}$
3.	20	1	3	$\sqrt{37}$	*15.*	40	2	3	$\sqrt{61}$	*27.*	60	3	3	4
4.	20	2	1	$\sqrt{5}$	*16.*	40	3	1	$\sqrt{13}$	*28.*	80	1	1	$\sqrt{5}$
5.	20	2	2	$\sqrt{5}$	*17.*	40	3	2	5	*29.*	80	1	2	5
6.	20	2	3	$\sqrt{29}$	*18.*	40	3	3	$\sqrt{17}$	*30.*	80	1	3	$\sqrt{29}$
7.	20	3	1	$\sqrt{13}$	*19.*	60	1	1	2	*31.*	80	2	1	$\sqrt{5}$
8.	20	3	2	5	*20.*	60	1	2	$\sqrt{34}$	*32.*	80	2	2	$\sqrt{5}$
9.	20	3	3	1	*21.*	60	1	3	$\sqrt{26}$	*33.*	80	2	3	$\sqrt{41}$
10.	40	1	1	$\sqrt{5}$	*22.*	60	2	1	$\sqrt{2}$	*34.*	80	3	1	3
11.	40	1	2	$\sqrt{17}$	*23.*	60	2	2	$3\sqrt{2}$	*35.*	80	3	2	5
12.	40	1	3	$\sqrt{17}$	*24.*	60	2	3	$5\sqrt{2}$	*36.*	80	3	3	7

Ahogyan a mellékletben található program (program1.mw) is mutatja, a fent definiált E_{101} sorozat esetén azt kapjuk, hogy :

- $\Delta(E_{101}) \approx 8,54$
- $\Gamma_1(E_{101}) \approx 8,54$
- $\Gamma_2(E_{101}) \approx 19,24$

Következmény. Az előbb kiszámolt mértékek $\sqrt{101} \approx 10$ körül helyezkednek el.

6.1.2. Példa 2.

Vegyük a következő függvényt és prímet (ügyelve arra, hogy $4|p-1$) :

- $f_2(x) := x^6 + x$
- $p := 101$

Definiáljuk az $F_{101} = (f_1, ..., f_{101})$ negyedik (komplex) egységgyökök sorozatát a következőképpen (ld. 3.3.5. Tétel) :

$$f_n = \begin{cases} \chi_{(4)}(f_2(n)), & (f_2(n), p) = 1 \\ 1, & p | f_2(n). \end{cases}$$

Hasonlóan a előző példához, kiszámolok néhány értéket :

	$M-1$	u	v	Δ		$M-1$	u	v	Δ		$M-1$	u	v	Δ
1.	15	1	1	$\sqrt{5}$	13.	20	2	1	$\sqrt{29}$	25.	25	3	1	$2\sqrt{17}$
2.	15	1	2	$\sqrt{37}$	14.	20	2	2	$\sqrt{5}$	26.	25	3	2	$5\sqrt{2}$
3.	15	1	3	$\sqrt{5}$	15.	20	2	3	$\sqrt{37}$	27.	25	3	3	4
4.	15	2	1	$\sqrt{5}$	16.	20	3	1	$\sqrt{53}$	28.	30	1	1	$\sqrt{65}$
5.	15	2	2	1	17.	20	3	2	$\sqrt{29}$	29.	30	1	2	$\sqrt{65}$
6.	15	2	3	$\sqrt{17}$	18.	20	3	3	$\sqrt{17}$	30.	30	1	3	3
7.	15	3	1	$\sqrt{17}$	19.	25	1	1	$\sqrt{58}$	31.	30	2	1	7
8.	15	3	2	$\sqrt{37}$	20.	25	1	2	$5\sqrt{2}$	32.	30	2	2	$\sqrt{17}$
9.	15	3	3	$\sqrt{13}$	21.	25	1	3	$\sqrt{2}$	33.	30	2	3	$\sqrt{61}$
10.	20	1	1	$\sqrt{53}$	22.	25	2	1	$2\sqrt{10}$	34.	30	3	1	7
11.	20	1	2	$\sqrt{53}$	23.	25	2	2	$2\sqrt{2}$	35.	30	3	2	7
12.	20	1	3	$\sqrt{5}$	24.	25	2	3	$\sqrt{34}$	36.	30	3	3	5

Ahogyan a mellékletben található program (program2.mw) is mutatja, a fent definiált F_{101} sorozat esetén azt kapjuk, hogy :

- $\Delta(F_{101}) \approx 15,56$
- $\Gamma_1(F_{101}) \approx 15,56$
- $\Gamma_2(F_{101}) \approx 19,92$

Következmény. A kiszámított mértékekről elmondható, hogy kicsivel rosszabbak, mint az 1. példa esetében.

6.1.3. Példa 3.

Vegyük a következő függvényt és prímet (ügyelve arra, hogy $4|p-1$) :

- $f_3(x) := -20x^{10} + 18x^9 - 16x^8 + 14x^7 - 12x^6 + 10x^5 - 8x^4 + 6x^3 - 4x^2 + 2x - 1$
- $p := 101$

Definiáljuk az $G_{101} = (g_1, ..., g_{101})$ negyedik (komplex) egységgyökök sorozatát a következőképpen (ld. 3.3.5. Tétel) :

$$g_n = \begin{cases} \chi_{(4)}(f_3(n)), & (f_3(n), p) = 1 \\ 1, & p | f_3(n). \end{cases}$$

Hasonlóan a előző példához, kiszámolok néhány értéket :

	$M-1$	u	v	Δ		$M-1$	u	v	Δ		$M-1$	u	v	Δ
1.	15	1	1		13.	20	2	1		25.	25	3	1	
2.	15	1	2		14.	20	2	2		26.	25	3	2	
3.	15	1	3		15.	20	2	3		27.	25	3	3	
4.	15	2	1		16.	20	3	1		28.	30	1	1	
5.	15	2	2		17.	20	3	2		29.	30	1	2	
6.	15	2	3		18.	20	3	3		30.	30	1	3	
7.	15	3	1		19.	25	1	1		31.	30	2	1	
8.	15	3	2		20.	25	1	2		32.	30	2	2	
9.	15	3	3		21.	25	1	3		33.	30	2	3	
10.	20	1	1		22.	25	2	1		34.	30	3	1	
11.	20	1	2		23.	25	2	2		35.	30	3	2	
12.	20	1	3		24.	25	2	3		36.	30	3	3	

Ahogyan a mellékletben található program (progam3.mw) is mutatja, a fent definiált G_{101} sorozat esetén azt kapjuk, hogy :

- $\Delta(E_{101}) \approx 10,2$
- $\Gamma_1(E_{101}) \approx 11,2$
- $\Gamma_2(G_{101}) \approx 17,5$

Következmény. A kiszámított mértékekről elmondható, hogy legjobban közelítik a 10 értéket a három példa közül.

Az alábbi táblázatban összefoglalom az eddigi példákban szereplő eredményéket.

Példa sorszáma	f	p	Δ	Γ_1	Γ_2	$\sqrt{p}$
1.	f_1	101	$\approx 8,54$	$\approx 8,54$	$\approx 19,24$	10
2.	f_2	101	$\approx 15,56$	$\approx 15,56$	$\approx 19,92$	10
3.	f_3	101	$\approx 10,2$	$\approx 11,2$	$\approx 17,5$	10

6.1.4. Példa 4. (Gray mapping)

A feladatunk, hogy vegyünk két tetszőleges hosszú bináris (k=2) sorozatot, amiből a Gray mapping segítségével legyártunk egy k=4 szimbólumot tartalmazó sorozatot, majd ezen 3 sorozat, illetve a két bináris szorzat sorozatának eloszlási mértéke közötti kapcsolatra adunk példát. Az egyszerűség kedvéért vegyünk az 1. példában és 2. példában szereplő $f_1(x), f_2(x)$ függvényeket, legyen $p := 101$ és az előzökhez hasonlóan legyártunk két bináris E_{bin}, F_{bin} sorozatot, amelynek elemeire igaz, hogy

$$e_n = \begin{cases} \chi_{(2)}(f_1(n)), & (f_1(n), p) = 1 \\ 1, & p | f_1(n) \end{cases}$$

és

$$f_n = \begin{cases} \chi_{(2)}(f_2(n)), & (f_2(n), p) = 1 \\ 1, & p | f_2(n). \end{cases}$$

Ezután definiáljuk a G_{kvad} sorozatot az alábbi módon

$$g_n = \frac{(1+i)e_n + (1-i)f_n}{2}, n = 1, .., p.$$

Szükségünk van még az $E_{bin}F_{bin} =: H_{bin}$ sorozatra is, amely a két sorozat megfelelő elemeinek szorzásával keletkezik.

Ahogyan a mellékletben található program (program4.mw) is mutatja, az alábbiakat kapjuk :

- $W(E_{bin}) = 8$
- $W(F_{bin}) = 9$
- $W(H_{bin}) = 16$
- $\Delta(G_{kvad}) = 7,3$

Megjegyzés. Mivel a 4. fejezetben a Δ mértéket úgy definiáltuk, hogy a k=2 speciális esetben is alkalmazható legyen (ekkor W jelölést szerepelt rá) , így használhatjuk ugyanazt az algoritmust az előbbi 4 mérték kiszámításához.

Megjegyzés. A 4.5.1. Tételben szereplő $\Delta(G_{kvad}) \leq \sqrt{2}\max\{W(E_{bin}), W(F_{bin}), W(H_{bin})\}$ egyenlőtlenség teljesül.

6.2. A k=8 eset

Ebben a szakaszban érdekesség miatt a 8-adrendű komplex egységgyökök által alkotott sorozatokat fogom az előző 1-3. példához hasonló módon vizsgálni. Ehhez vegyük az alábbiakat :

- $f := 13x^7 - 3x^4 + 5x$
- $p := 113$ $(112 \equiv 0(8))$

A mellékletben szereplő program (program5.mw) szerint az alábbiakat kapjuk :

- $\Delta(K) \approx 9,84$
- $\Gamma_1(K) \approx 11,2$
- $\Gamma_2(K) \approx 20,9$

Megjegyzés. Több (jelen esetben 8) szimbólumból felépített sorozatunk esetében, a kiszámolt mértékek közelebb vannak a $\sqrt{p} \approx 10,6$ értékhez (kivéve esetleg a másodrendű korrelációs mértéket).

Irodalomjegyzék

[1] C. Maudit, A. Sárközy: *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arithmetica 82 (1997), 365-377.

[2] L. Goubin, C. Maudit, A. Sárközy: *Construction of large families of pseudorandom binary sequences*, J. Number Theory 106 (2004), no. 1, 56-69.

[3] R. Ahlswede, C. Maudit, A. Sárközy: *Large families of pseudorandom sequences of k symbols and their complexity - Part I.*, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, vol. 4123, Springer-Verlag, Berlin, 2006, 293-307.

[4] R. Ahlswede, C. Maudit, A. Sárközy: *Large families of pseudorandom sequences of k symbols and their complexity - Part II.*, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, vol. 4123, Springer-Verlag, Berlin, 2006, 308-325.

[5] D. E. Knuth: *A Számítógépprogramozás művészete*, 2. kötet, 2. kiadás, Műszaki Könyvkiadó, Budapest 1994.

[6] Mérai László: *Pszeudovéletlen sorozatok és rácsok*, Doktori (Ph.D.) értekezés, Eötvös Loránd Tudományegyetem, Természettudományi Kar, Matematikai Intézet, Budapest 2010.

[7] H. Davenport, *Multiplicative number theory*, 2nd ed., Springer-Verlag, New York (1980).

[8] J. Cassaigne, C. Maudit, A. Sárközy: *On finite pseudorandom binary sequences VII: The measures of pseudorandomness*, Acta Arithmetica 103.2 (2002), 97-118.

[9] K. Gyarmati: *On a pseudorandom property of binary sequences*, Ramanujan J. 8 (2004), 289-302.

[10] W. Schmidt: *Equations over finite fields. An elementary approach,* Lecture Notes in Math. 536, Springer, New York, 1976.

[11] H. Iwaniec: *Fourier coefficients of modular forms of half-integral weight*, Invent. Math. 87 (1987), 385-401.

[12] K. Gyarmati, A. Sárközy: *Pszeudovéletlenség*, online jegyzet, Eötvös Loránd Tudományegyetem, 2012. http://www.cs.elte.hu/~gykati/diak/13-14elsofelev/diaka.html

[13] C. Maudit, A. Sárközy: *On finite pseudorandom sequences of k symbols*, Indag. Math. 13, 89-101, 2002.

[14] P. Hubert, C. Maudit, A. Sárközy: *On pseudorandom binary lattices*, Acta Arith. 125 (2006), 51-62.

[15] G. Bérczi, *On finite pseudorandom sequences of k symbols*, Period. Math. Hungar. 47 (1,2) (2003) 29-44.

[16] Kit-Ho Mak, *More constructions of pseudorandom sequences of k symbols*, Finite fields and their applications, Volume 25, Elsevier, 222-233, 2014.

[17] R. Marzouk, A. Winterhof, *On the pseudorandomness of binary and quaternary sequences linked by the Gray mapping*, Periodica Mathematica Hungarica Vol. 60 (1), 13-23, 2010.

[18] R. Guy, *Unsolved problems in number theory*, second ed., Problem Books in Mathematics, Springer-Verlag, New York, 1994, Unsolved Problems in Intuitive Mathematics, I.

[19] H. Liu, C. Yang, *On a problem of D. H. Lehmer and pseudorandom binary sequences*, Bull. Braz. Math. Soc. (N.S.) 39 (2008), no. 3, 387-399.

[20] C. Maudit, J. Rivat, A. Sárközy, *Construction of pseudorandom binary sequences using additive characters*, Monatsh. Math. 141 (2004), no. 3, 197-208.

[21] L. Mérai, *On finite pseudorandom lattices of k symbols*, Monatsh. Math. 161 (2010), no. 2, 173-191.

[22] A. Winterhof, *Some estimate for character sums and applications*, Des. Codes Crytogr. 22 (2001), 123-131.

[23] A. Winterhof, Z. Chen, *Linear complexity profile of m-ary pseudorandom sequences with small correlation measure*, Indag. Mathem., N.S., 20 (4), 2009, 631-640.

[24] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Hermann, Paris, 1948.

[25] I. Niven, H. S. Zuckerman, *On the definition of normal numbers*, Pacific J. Math. 1 (1951), 103-109.