dc_603_12

Véges bináris sorozatok és rácsok pszeudovéletlensége

Doktori értekezés tézisei

Gyarmati Katalin

Eötvös Loránd Tudományegyetem

Budapest

2013

1. Bevezetés

Az elmúlt száz évben a kriptográfia egyre nagyobb szerepet kapott a matematikai és informatikai kutatásokban. A területnek számos fontos gyakorlati alkalmazása van, így például a digitális aláírás, a vezeték nélküli mikrohullámú kommunikáció (WLAN) vagy különböző titkosítási algoritmusok. Ezek az alkalmazások különböző objektumok pszeudovéletlenségének tanulmányozását inspirálták. Kezdetben a véletlen vagy pszeudovéletlen objektumokat fizikai módszerekkel generálták (pl. diódával), azonban a fizikai módszereknek számos hátránya van: költségesek, lassúak, nehézkes megoldani az adatok biztonságos tárolását, a generált sorozatok véletlenszerűsége nem bizonyítható matematikailag. Manapság pszeudovéletlen objektumokat inkább matematikai algoritmusok és számítógépek segítségével konstruálnak. Ezek az objektumok ugyan nem tekinthetők „véletlennek", de reményeink szerint még számítógépek segítségével sem különböztethetőek meg a fizikai módszerekkel generált véletlen objektumoktól, ezért a továbbiakban a pszeudovéletlen elnevezést használjuk rájuk vonatkozóan.

A pszeudovéletlenségnek számos megközelitése és definíciója van. Menezes, Oorschot és Vanstone [52] kitűnő monográfiát írt ezekről a megközelítésekről. A pszeudovéletlenség leggyakoribb értelmezése bonyolultságelméleti úton történik; erről Goldwasser [16] írt összefoglaló cikket. A bonyolultságelméleti megközelítést egyre szélesebb körben kritizálják: általában csak végtelen hosszú sorozatokat minősít, míg a gyakorlati alkalmazások során mindig csak véges hosszú sorozatok kerülnek felhasználásra. A legtöbb bonyolultságelméleti eredmény bizonyos bizonyítatlan hipotéziseken alapul (ilyen például az, hogy az egész számok körében nem lehet gyorsan faktorizálni). Véges hosszú $[0,1)$ sorozatok pszeudovéletlenségét Niederreiter vizsgálta.

Az 1990-es évek második felében Mauduit és Sárközy [51] bevezette a pszeudovéletlenségnek egy új, konstruktív és kvantitatív megközelítését, amelyben *véges bináris sorozatok* pszeudovéletlenségét definiálták, karakte-

rizálták. A következő kvantitatív pszeudovéletlen mértékeket vezették be:

1.1. Definíció. (Mauduit, Sárközy) *Legyen* $E_N = (e_1, e_2, \dots, e_N) \in \{-1, +1\}^N$ *egy* N *hosszú* ± 1 *sorozat. Jelölje* $U(E_N, t, a, b)$ *az*

$$U(E_N, t, a, b) \stackrel{\text{def}}{=} \sum_{j=0}^{t-1} e_{a+jb}.$$

összeget. Ekkor E_N*-nek az* **eloszlás mérték***ét*

$$W(E_N) \stackrel{\text{def}}{=} \max_{a,b,t} |U(E_N, t, a, b)| = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|,$$

képlettel definiáljuk, ahol a maximumot az összes olyan a, b, t*-n vesszük, ahol* $a, b, t \in \mathbb{N}$ *és* $1 \le a \le a + (t-1)b \le N$.

Az eloszlás mérték számtani sorozatokban tanulmányozza azt, hogy a $+1$-ek és -1-ek száma mennyire közel van. Gyakran azonban szükség van arra is, hogy a sorozatban több elem egymáshoz való viszonyát is vizsgáljuk. Ehhez:

1.2. Definíció. (Mauduit, Sárközy) *Legyen* $E_N = (e_1, e_2, \dots, e_N) \in \{-1, +1\}^N$ *egy* N *hosszú* ± 1 *sorozat. Legyen továbbá* $D = (d_1, \dots, d_\ell)$ *természetes számokból álló sorozat, ahol* $d_1 < \dots < d_\ell$*, jelölje* $V(E_N, M, D)$ *a*

$$V(E_N, M, D) \stackrel{\text{def}}{=} \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell}$$

összeget. Ekkor E_N*-nek az* ℓ**-edrendű korreláció mérték***ét*

$$C_\ell(E_N) \stackrel{\text{def}}{=} \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2}, \dots e_{n+d_\ell} \right|$$

képlettel definiáljuk, ahol a maximumot az összes olyan $D = (d_1, d_2, \dots, d_\ell)$ *sorozaton és* M *egész számon vesszük, ahol* $0 \le d_1 < d_2 < \dots < d_\ell < M + d_\ell \le N$.

1.3. Definíció. (Mauduit, Sárközy) *Legyen* $E_N = (e_1, e_2, \ldots, e_N) \in \{-1,+1\}^N$ *egy* N *hosszú* ± 1 *sorozat. Legyen továbbá* $X = (x_1, \ldots, x_\ell) \in \{-1,+1\}^\ell$, *jelölje* $T(E_N, M, X)$ *a következő egész számot:*

$$T(E_N, M, X) = \left|\{n : 0 \le n < M,\ (e_{n+1}, e_{n+2}, \ldots, e_{n+\ell}) = X\}\right|.$$

Ekkor E_N*-nek az* ℓ**-edrendű normalitás mértéké**t

$$N_\ell(E_N) = \max_{M,X} \left|T(E_N, M, X) - M/2^\ell\right|$$

képlettel definiáljuk, ahol a maximumot az összes olyan $X = (x_1, \ldots, x_\ell) \in \{-1,+1\}^\ell$ *sorozaton és* M *egész számon vesszük, ahol* $0 < M \le N - \ell + 1$.

A kombinált mérték a korreláció és az eloszlás mérték közös általánosítása:

1.4. Definíció. (Mauduit, Sárközy) *Legyen* $E_N = (e_1, e_2, \ldots, e_N) \in \{-1,+1\}^N$ *egy* N *hosszú* ± 1 *sorozat. Ekkor* E_N*-nek az* ℓ**-edrendű kombinált (eloszlás-korreláció) mértéké**t *a következőképpen definiáljuk:*

$$Q_\ell(E_N) \stackrel{\text{def}}{=} \max_{a,b,t,D} |Z(a,b,t,D)| = \max_{a,b,t,D} \left|\sum_{j=0}^{t-1} e_{a+jb+d_1} e_{a+jb+d_2} \ldots e_{a+jb+d_\ell}\right|,$$

ahol a maximumot az összes olyan a, b, t *egész számokon és* $D = (d_1, d_2, \ldots, d_\ell)$ *különböző egész számokból álló sorozaton vesszük, ahol az összes szummában előforduló* $a + jb + d_i$ *index eleme az* $\{1, \ldots, N\}$ *halmaznak.*

A gyorsan fejlődő területen azóta nagyon sok szerző dolgozott, számos konstrukció, rengeteg eredmény és különböző általánosítás született.

[10]-ben Cassaigne, Ferenczi, Mauduit, Rivat és Sárközy a következő elvet fogalmazta meg: Az E_N sorozat erős pszeudovéletlen tulajdonságokkal rendelkezik, amennyiben a $W(E_N)$ és $C_\ell(E_N)$ mértékek (legalább „kis” ℓ-ekre) „kicsik”. Ezt az elvet később [11]-ben Cassaigne, Mauduit és Sárközy igazolta, bebizonyítva, hogy majdnem minden N hosszú sorozatra ezeknek a mértékeknek az értéke alig lehet nagyobb $N^{1/2}$-nél.

Disszertációmban összefoglalom a területen elért legfontosabb eredményeimet. Néhány cikkemet (a [20], [22], [26], [30], [41], [42]) részletesen ismertetem a disszertáció 2.-7. fejezetében, míg más munkáimat (a [19], [21], [23], [24], [25], [27], [28], [29] [31], [32], [33], [34], [35], [36], [37], [38], [39] és [40] cikkeket) csak röviden összefoglalom a disszertáció 8. fejezetében.

2. Hatványgenerátor

L. Blum, M. Blum és M. Shub [7] megalkotta a máig egyik legismertebb és leggyakrabban tanulmányozott pszeudovéletlen generátort, mely a nevét feltalálóiról kapta. Azóta a Blum-Blum-Shub generátornak számtalan tulajdonságát vizsgálták, azonban a legtöbb eredmény bizonyos bizonyítatlan hipotéziseken alapul (például az egész számok körében a faktorizálás nehézségén).

Disszertációm 2. fejezetében (mely [20]-as cikkem tartalmát ismerteti) olyan eredményeket bizonyítok, amelyek kvantitatívak. Az általam bizonyított tételek feltétel nélküliek, nem alapszanak bizonyítatlan hipotézisek igazságán.

A *hatványgenerátort* (amely a Blum-Blum-Shub generátor általánosítása) szerzői [7] a következőképpen definiálták:

Legyenek $k \geq 2, m \geq 1$ és ϑ egészek, amelyre $1 \leq \vartheta \leq m-1$, $(\vartheta, m) = 1$. Az $\{u_n\}$ sorozatot a következő rekurzióval definiáljuk

$$\begin{aligned} &u_0 = \vartheta, \\ &u_n \equiv u_{n-1}^k \pmod{m}, \quad 0 \leq u_n \leq m-1, \quad n = 1, 2, \ldots . \end{aligned} \tag{2.1}$$

Ezután az $\{u_n\}$ sorozatot u_n utolsó bitje szerint bináris sorozattá konvertáljuk:

2.1. Konstrukció. (Blum, Blum, Shub) *Definiáljuk az* $E_\infty = (e_1, e_2 \ldots)$ *sorozat n-edik elemét a következő képlettel*

$$e_n = \begin{cases} +1 & \text{ha } u_n \text{ páros,} \\ -1 & \text{ha } u_n \text{ páratlan.} \end{cases}$$

A (2.1) rekurzióból adódóan az E_∞ sorozat periodikus, jelölje T e sorozat periódushosszát. Disszertációm 2. fejezetében az $(e_1, e_2, \ldots, e_T)$ véges hosszú sorozat pszeudovéletlen tulajdonságait vizsgálom. A következőket bizonyítottam:

2.1. Tétel. *Legyen m prím, és jelölje T a 2.1. Konstrukcióban definiált E_∞ periodikus végtelen sorozat periódushosszát. Jelölje $E_T = (e_1, e_2, \ldots, e_T)$ az E_∞ sorozat első T eleméből álló részsorozatot. Ekkor:*

$$W(E_T) \ll m^{7/8} \log m,$$
$$N_\ell(E_T) \ll m^{7/8} \log m.$$

Ha T a modulus m függvényében elég nagy, ezek a becslések nem triviális felső becslések. A korreláció becslése Bourgain 2005-ös exponenciális összegekre vonatkozó eredményéig [8] elérhetetlen volt, azonban Bourgain tétele segítségével a következőt tudtam igazolni:

2.2. Tétel. *Legyen m prím, $\delta > 0$, ekkor létezik ε csak ℓ-től és δ-tól függő pozitív konstans, hogy ha N $(< T)$ kielégít bizonyos feltételeket (lásd 2.3. Tétel a disszertációm 2. fejezetében), akkor E_∞ első N eleme által alkotott $E_N = (e_1, e_2, \ldots, e_N)$ sorozatra*

$$C_\ell(E_N) < m^{1-\varepsilon}.$$

Disszertációm 2. fejezetében (Sophie-German prímeket használva) olyan eseteket mutatok, amikor N $(< T)$ értéke $m/4$ körül van.

Megjegyzem, [20]-ban és disszertációm 2. fejezetében a fenti tételeket csak abban az esetben igazolom, ha az m modulus prím. Valószínűleg összetett modulus esetén a magasabb rendű korreláció naggyá válhat. (Ez a szituáció bizonyos további konstrukciók esetén valóban fennáll, lásd például Rivat és Sárközy cikkét [57] vagy Liu, Zhan és Wang cikkét [48].)

3. Bináris sorozatok korrelációja

[11]-ben Cassaigne, Mauduit és Sárközy igazolta, hogy majdnem minden N hosszú $E_N \in \{-1,+1\}^N$ bináris sorozatra $W(E_N)$ és $C_\ell(E_N)$ értéke $N^{1/2}$ körül van. Ezt az eredmény később Alon, Kohayakawa, Mauduit, Moreira és Rödl [3] tovább élesítette.

Egy erős pszeudovéletlen tulajdonságokkal rendelkező sorozattól azt várjuk, hogy a pszeudovéletlen mértékeik bizonyos felső korlát alatt vannak, azonban hasonló alsó korlát kikötése nem szükséges, az alábbiak alapján:

Jelölje $m(N)$ és $M_\ell(N)$ a következő értékeket:

$$m(N) = \min_{E_N \in \{-1,+1\}^N} W(E_N), \qquad M_\ell(N) = \min_{E_N \in \{-1,+1\}^N} C_\ell(E_N).$$

$m(N)$ becslése klasszikus probléma: 1964-ben Roth [58] bebizonyította, hogy $m(N) \gg N^{1/4}$. Sárközy [14] majd Beck [5] adott felső becslést $m(N)$-re. Végül Matoušek és Spencer [49] bebizonyította, hogy $m(N) \ll N^{1/4}$.

$M_\ell(N)$ nagyságrendje ℓ paritásától függ. Cassaigne, Mauduit és Sárközy [11] bebizonyította, hogy $M_\ell(E_N) \ll (\ell N \log N)^{1/2}$. Alon, Kohayakawa, Mauduit, Moreira és Rödl [2]-ben és [46]-ban alsó becslést adott, bebizonyítva:

3.A. Tétel (Alon, Kohayakawa, Mauduit, Moreira, Rödl) *Ha ℓ páros, akkor*

$$M_\ell(N) \geq \sqrt{\frac{1}{2}\left[\frac{N}{\ell+1}\right]}.$$

Cassaigne, Mauduit és Sárközy [11] észrevette, hogy a páratlan rendű korrelációk minimuma nagyon kicsi, nevezetesen az $E_N = (-1,+1,-1,+1,\dots) \in \{-1,+1\}^N$ sorozatra $C_\ell(E_N) = 1$, és így $M_\ell(N) = 1$, ha ℓ páratlan. Cassaigne, Mauduit és Sárközy [11] cikkükben megjegyezték, hogy habár az $E_N = (-1,+1,-1,+1,\dots)$ sorozatra $C_3(E_N) = 1$, ekkor a másodrendű korreláció nagy: $C_2(E_N) = N-1$. Cassaigne, Mauduit és Sárközy [11] valamint Mauduit [50] problémáit megoldva [18]-ban igazoltam,

hogy ha $C_2(E_N) \ll N^{2/3}$, akkor $C_3(E_N) \gg N^{1/2}$. Ebből adódóan a

$$C_2(E_N)C_3(E_N) \gg N^{2/3} \tag{3.1}$$

összefüggés mindig fennáll. Sőt, [18]-ban egy a fentieknél általánosabb egyenlőtlenséget igazoltam, amelyben egy páratlan rendű C_{2k+1} és egy páros rendű $C_{2\ell}$ korrelációt vetettem össze, abban az esetben, ha $2k+1 > 2\ell$. Később Anantharam [4] élesítette (3.1)-et. A korábbi eredményeket általánosítva, [30]-ban Mauduit-val C_{2k+1} és $C_{2\ell}$-t vetettük össze (abban az esetben is, amikor $2k+1 < 2\ell$). Főeredményünk a következő volt:

3.1. Tétel. (Gyarmati, Mauduit) *Létezik olyan $c_{k,\ell}$ csak k-tól és ℓ-től függő konstans, amelyre ha*

$$C_{2k+1}(E_N) < c_{k,\ell}N^{1/2},$$

akkor

$$C_{2k+1}(E_N)^{2\ell}C_{2\ell}(E_N)^{2k+1} \gg N^{2k+1},$$

ahol az alkalmazott konstans szorzó csak k-tól és ℓ-től függ.

Ennek a tételnek a következő következményei vannak:

3.1. Következmény. (Gyarmati, Mauduit) *Ha $C_{2k+1}(E_N) = O(1)$, akkor $C_{2\ell}(E_N) \gg N$, ahol az alkalmazott konstans szorzó csak k-tól és ℓ-től függ.*

3.2. Következmény. (Gyarmati, Mauduit)

$$C_{2k+1}(E_N)C_{2\ell}(E_N) \gg N^{c(k,\ell)}$$

ahol az alkalmazott konstans szorzó csak k-tól és ℓ-től függ, és

$$c(k,\ell) = \begin{cases} 1 & \text{ha } k \geq \ell, \\ \frac{1}{2} + \frac{2k+1}{4\ell} & \text{ha } k < \ell. \end{cases}$$

Disszertációm 3. fejezetében a 3.1. Tételt és következményeit igazolom.

4. A Legendre szimbólumot használó család f-bonyolultsága

Goubin, Mauduit és Sárközy [17]-ben pszeudovéletlen sorozatoknak egy nagy családját konstruálták.

4.1. Konstrukció. (Goubin, Mauduit, Sárközy) *Legyen $K > 0$ rögzített egész. Tekintsük az összes olyan $f(x) \in \mathbb{F}_p[x]$ k-adfokú polinomot, ahol $k \le K$, és amelynek nincs többszörös gyöke $\overline{\mathbb{F}}_p$-ben. Minden ilyen polinomhoz hozzárendelünk egy $E_p = (e_1, e_2, \dots, e_p) \in \{-1, +1\}^p$, p hosszú bináris sorozatot úgy, hogy a sorozat n-edik eleme*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right) & \text{ha } (f(n), p) = 1, \\ +1 & \text{ha } p \mid f(n). \end{cases} \tag{4.1}$$

Hoffstein és Lieman [43] olyan $f(x)$ polinom használatát javasolták (4.1)-ben, melyeknek nincs többszörös gyöke, se nem páros, se nem páratlan. Azonban a kapcsolódó $E_p = (e_1, e_2, \dots, e_p)$ sorozat pszeudovéletlen tulajdonságairól semmit sem bizonyítottak. Később Goubin, Mauduit és Sárközy [17] igazolta, hogy ha néhány nem túlságosan megszorító feltevést kikötünk a konstrukcióban szereplő $f(x)$ polinomra, úgy az E_p sorozatnak erős pszeudovéletlen tulajdonságai vannak.

Néhány alkalmazásban nem elég tudni, hogy a család sok pszeudovéletlen sorozatot tartalmaz, az is fontos, hogy a családban sok „független" sorozat van. Ennek vizsgálatára vezette be Ahlswede, Khachatrian, Mauduit és Sárközy [1] az *f-bonyolultság* fogalmát:

4.1. Definíció. (Ahlswede, Khachatrian, Mauduit, Sárközy) *Legyen $\mathcal{F}$ N hosszú $E_N \in \{-1, +1\}^N$ pszeudovéletlen sorozatoknak egy nagy családja. Jelöljük $C(\mathcal{F})$-fel az $\mathcal{F}$ család f-bonyolultságát, amelyet azzal a legnagyobb j egész számmal definiálunk, amelyre a következő teljesül: minden $1 \le i_1 < i_2 < \cdots < i_j \le N$ j-esre és $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_j \in \{-1, +1\}$*

számokra legalább egy $E_N = (e_1, \dots, e_N) \in \mathcal{F}$ *sorozat létezik, amelyre*

$$e_{i_1} = \varepsilon_1,\ e_{i_2} = \varepsilon_2, \dots, e_{i_j} = \varepsilon_j.$$

Ahlswede, Khachatrian, Mauduit és Sárközy [1] a következő általános felső becslést adta bináris sorozatok tetszőleges $\mathcal{F}$ nagy családjára:

4.1. Propozíció. (Ahlswede, Khachatrian, Mauduit, Sárközy)

$$C(\mathcal{F}) \le \frac{\log |\mathcal{F}|}{\log 2}.$$

Ahlswede, Khachatrian, Mauduit és Sárközy [1] bebizonyította, hogy ha kicsit módosítjuk a 2.1. Konstrukciót, akkor olyan pszeudovéletlen generátort kapunk, amelynek nagy az f-bonyolultsága.

4.A. Tétel (Ahlswede, Khachatrian, Mauduit, Sárközy) *Legyen* p *prím. Tekintsük az összes olyan* $f(x)$ *polinomot, amelyre*

$$0 < \deg f(x) \le K$$

(itt $\deg f(x)$ *jelöli* $f(x)$ *fokát) és* $f(x)$*-nek nincs többszörös gyöke* $\overline{\mathbb{F}}_p$*-ben. Minden ilyen* $f(x)$ *polinomra, tekintsük azt a bináris* $E_p = E_p(f) = (e_1, e_2, \dots, e_p) \in \{-1, +1\}^p$ *sorozatot, amelyet* (4.1)*-gyel definiálunk, és jelölje* $\mathcal{F}_1$ *az ily módon kapott bináris sorozatok családját. Ekkor*

$$C(\mathcal{F}_1) \ge K.$$

A 4.1. Propozícióból azonnal következik, hogy

$$|C(\mathcal{F}_1)| \le \frac{\log |\mathcal{F}_1|}{\log 2} \le \frac{K+1}{\log 2} \log p.$$

Így alsó becslésként K-t, felső becslésként $\frac{K+1}{\log 2} \log p$-t tudunk mondani $C(\mathcal{F}_1)$-re. Érdekes kérdés, hogy vajon melyik becslés áll közelebb az igazsághoz? [22]-ben megjavítottam az alsó becslést, és a következőt bizonyítottam:

4.1. Tétel.

$$C(\mathcal{F}_1) \geq \frac{K-1}{2\log 2}\log p - O(K\log(K\log p)).$$

Vagyis az alsó és a felső becslés most már csak egy konstans szorzóval tér el egymástól. Az alsó becslés bizonyítása karakterösszegekre, Weil tételére [59] és egy átlagolásos ötlet újszerű alkalmazására épül. Disszertációm 4. fejezetében igazolom a 4.1. Tételt.

5. Rövid részsorozatok korrelációja

Néhány kriptográfiai alkalmazásban rendkívül fontos, hogy ne csak az egész sorozat, hanem annak rövidebb részsorozatai is erős pszeudovéletlen tulajdonságokkal rendelkezzenek. Nyilvánvalóan

$$\max_{E_N\in\{-1,+1\}^N} |U(E_N,t,a,b)| = t,$$
$$\max_{E_N\in\{-1,+1\}^N} |V(E_N,M,D)| = M.$$

Amennyiben $|U(E_N,t,a,b)|$ nagy t-hez képest vagy $|V(E_N,M,D)|$ nagy M-hez képest, úgy az E_N sorozatnak van egy „része", amely gyenge pszeudovéletlen tulajdonságokkal rendelkezik. A legjobb egydimenziós konstrukciókban

$$|U(E_N,t,a,b)| \ll N^{1/2}(\log N)^{c_1}, \quad |V(E_N,M,D)| \ll N^{1/2}(\log N)^{c_\ell}$$

bizonyított. Ha t vagy $M < N^{1/2}$, ezek a becslések triviálisak. Az alkalmazásokban azonban előfordulhat, hogy olyan szöveget szeretnénk titkosítani, amelynek hossza $< N^{1/2}$. Ez esetben kulcsként nem az egész pszeudovéletlen sorozat, hanem annak csak egy rövidebb része (mondjuk $N^{1/2-\varepsilon}$ hosszúságú) kerül tényleges felhasználásra. Ezért fontos, hogy a rövid részsorozatok pszeudovéletlen mértékeit is kontrolláljuk. A disszertációm 5. fejezetének rövid részsorozatokra vonatkozó eredménye:

5.1. Tétel. *Minden N egész számra létezik egy olyan $E_N \in \{-1,+1\}^N$ sorozat, hogy ha $D = (d_1, d_2, \dots, d_\ell)$ és $M \le N^{1/2}$-re $0 \le d_1 < d_2 < \cdots < d_\ell < M + d_\ell \le N$ teljesül, akkor*

$$|V(E_N, M, D)| \ll \ell^2 N^{1/4} \log N. \tag{5.1}$$

Továbbá

$$C_\ell(E_N) \ll \ell^2 N^{1/2} (\log N)^2$$

és

$$W(E_N) \ll N^{3/4} \log N$$

is fennáll.

(5.1)*-ból következően* $1 \le M \le N$*-re*

$$|V(E_N, M, D)| \ll \ell^2 \left\lceil \frac{M}{N^{1/2}} \right\rceil N^{1/4} \log N$$

teljesül.

Az 5.1. Tételt először [26]-ban publikáltam. Az eredmény abban az esetben ad a rövid részsorozatok korrelációjára éles becslést, ha azoknak hossza $c_1 N^{1/4} \log N$-nél hosszabb. Mivel várhatóan a teljes sorozatban létezik olyan $c_2 \log N$ hosszú részsorozat, amely csupa egyesből áll, ezért nem remélhetjük, hogy egy erős pszeudovéletlen sorozat összes részsorozata erős pszeudovéletlen tulajdonságokkal rendelkezzék. Nyitott kérdés, hogy vajon becsülhető-e azon részsorozatok korrelációja, amelyek hosszúsága $c_2 \log N$ és $c_1 N^{1/4} \log N$ közé esik. E probléma nehézségét mutatja, hogy egy ehhez kapcsolódó probléma, a legkisebb kvadratikus nemmaradék $\pmod p$ becslése esetén is nagyon nagy hézag van Burgess [9] felső becslése $O\left(p^{\frac{1}{4\sqrt{e}}}\right)$ és a megoldatlan sejtés ($O(\log p \log\log p)$) között.

Az 5.1. Tétel bizonyítása konstruktív, és a pszeudovéletlenség többdimenziós elméletét is használja.

6. A Legendre szimbólum rács

Ebben a fejezetben disszertációm 6. és 7. fejezetét foglalom össze.

A pszeudovéletlenség többdimenziós kiterjesztése Hubert, Mauduit és Sárközy [44] nevéhez kötődik. Ők vezették be a következő definíciókat:

Jelölje I_N^n azon n-dimenziós vektorok halmazát, amelynek koordinátái 0 és $N-1$ közötti egész számok:

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

Ezt a halmazt *n-dimenziós N-rácsnak* vagy röviden *N-rácsnak* nevezzük. Ez a definíció általánosabb rácsokra is kiterjeszthető: Legyen $\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_n}$ n darab lineárisan független vektor, ahol $\mathbf{u_i}$-nek az i-edik koordinátája pozitív egész, a többi koordináta viszont 0, azaz $\mathbf{u_i} = (0, \ldots, 0, z_i, 0, \ldots, 0)$ alakú, ahol $z_i \in \mathbb{Z}^+$. Legyen $t_1, t_2, \ldots, t_n$ olyan egészek, amelyekre $0 \leq t_1, t_2, \ldots, t_n < N$. Ekkor a

$$B_N^n = \{\mathbf{x} = x_1\mathbf{u_1} + \cdots + x_n\mathbf{u_n} : \ 0 \leq x_i \, |\mathbf{u_i}| \leq t_i (< N) \ i = 1, \ldots, n \text{ esetén}\}$$

halmazt *n-dimenziós N-téglarácsnak* vagy röviden *N-téglarácsnak* nevezzük.

Hubert, Mauduit és Sárközy [44]-ben kiterjesztette a bináris sorozatok definícióját több dimenzióra: Legyen

$$e_{\mathbf{x}} = \eta(\mathbf{x}) : \ I_N^n \to \{-1, +1\}$$

egy függvény. Az egyszerűség kedvéért, ha $\mathbf{x} = (x_1, \ldots, x_n)$ és így $\eta(\mathbf{x}) = \eta((x_1, \ldots, x_n))$, akkor a jövőben azt írjuk, hogy $\eta(\mathbf{x}) = \eta(x_1, \ldots, x_n)$.

Az ilyen függvényeket *bináris N-rácsoknak* vagy rövidebben *bináris rácsoknak* nevezzük. Szemléltetésük egyszerű: egy N-rács, amelyben a rácspontokat a $+$ és $-$ előjelek valamelyikével helyettesítjük. A bináris 2 vagy 3 dimenziós pszeudovéletlen rácsok használatosak digitális képek, térképek titkosításához, valamint az orvosi diagnosztikában.

[44]-ben Hubert, Mauduit és Sárközy a következő pszeudovéletlen mértékeket vezette be bináris rácsok pszeudovéletlen tulajdonságainak vizsgálatára:

6.1. Definíció. *Legyen*

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

egy bináris rács. Definiáljuk az ℓ**-edrendű pszeudovéletlen mérték**$\acute{e}t$ η*-nak a következő képlettel:*

$$Q_\ell(\eta) = \max_{B,\mathbf{d_1},\ldots,\mathbf{d_k}} \left| \sum_{\mathbf{x}\in B} \eta(\mathbf{x}+\mathbf{d_1}) \cdots \eta(\mathbf{x}+\mathbf{d}_\ell) \right|,$$

ahol a maximumot az összes olyan különböző $\mathbf{d_1}, \ldots, \mathbf{d}_\ell \in I_N^n$ *vektoron és* N*-téglarács* B*-n vesszük, ahol* $B + \mathbf{d_1}, \ldots, B + \mathbf{d}_\ell \subseteq I_N^n$.

Ebben a fejezetben egy természetes - Legendre szimbólumon alapuló - konstrukciót ismertetek, melyet társszerzőimmel, Sárközy Andrással és Cameron L. Stewarttal közösen [41]-ben és [42]-ben publikáltunk. A korábbi cikkekben megadott konstrukciók kissé mesterkéltek. Ráadásul ezeknek a korábbi konstrukcióknak az implementálása meglehetősen bonyolult. Így [41]-ben olyan „természetes" konstrukciót definiáltunk, ahol a pszeudovéletlen mértékekre adott becslések gyengébbek ugyan, mint a korábbi konstrukciók esetében, de még mindig erős, nem triviális becslések. Ez az új konstrukció az egy dimenzióban a legjobb és a legtöbbet vizsgált bináris sorozatok, a Legendre szimbólumon alapuló 4.1. Konstrukcióban megadott bináris sorozatok két dimenziós kiterjesztése:

6.1. Konstrukció. (Gyarmati, Sárközy, Stewart) *Legyen* p *egy páratlan prím,* $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ *pedig kétváltozós polinom. Definiáljuk* $\eta : I_p^2 \to \{-1, +1\}$ *rácsot*

$$\eta(x_1, x_2) = \begin{cases} \left(\frac{f(x_1,x_2)}{p}\right) & \text{ha } (f(x_1, x_2), p) = 1, \\ +1 & \text{ha } p \mid f(x_1, x_2) \end{cases} \tag{6.1}$$

képlettel.

Megjegyezzük, hogy több olyan kétváltozós $f(x_1, x_2)$ polinom létezik, amelyre az η rács gyenge pszeudovéletlen tulajdonságokkal rendelkezik.

Disszertációm 6. fejezetében példákat adok ilyen polinomokra. Az összes megadott példa speciális esete volt a következőnek:

6.1. Példa. (Gyarmati, Sárközy, Stewart) Legyen r nem negatív egész és legyen α_j, $\beta_j \in \mathbb{F}_p$ $j = 1, \dots, r$ esetén. Legyen

$$f(x_1, x_2) = \left(\prod_{j=1}^{r} f_j(\alpha_j x_1 + \beta_j x_2) \right) g(x_1, x_2)^2 \tag{6.2}$$

alakú polinom, ahol $f_j(x) \in \mathbb{F}_p[x]$ és $g(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$.

Az olyan $f \in \mathbb{F}_p[x_1, x_2]$ polinomokat, amelyek felírhatóak (6.2) alakban degenerált polinomnak hívjuk, és amelyek nem írhatóak fel ilyen alakban, azok a nem-degenerált polinomok.

Abban az esetben, amikor az f polinom nem-degenerált [41]-ben a következőt tudtuk bizonyítani:

6.1. Tétel. (Gyarmati, Sárközy, Stewart) *Legyen $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ k-adfokú polinom. Tegyük fel, hogy $f(x_1, x_2)$ nem írható fel* (6.2) *alakban, és a következő 5 feltétel közül egy fennáll:*
a) $f(x_1, x_2)$ irreducibilis $\mathbb{F}_p[x_1, x_2]$-ben,
b) $\ell = 2$,
c) 2 primitív gyök modulo p,
d) $4^{k+\ell} < p$,
e) ℓ és az $f(x_1, x_2)$ polinom foka x_1-ben (esetleg x_2-ben) páratlan.
Ekkor a (6.1)*-gyel definiált η bináris rács esetén*

$$Q_\ell(\eta) < 11k\ell p^{3/2} \log p.$$

Amennyiben f degenerált, akkor a (6.1)-gyel definiált bináris rács akár gyenge pszeudovéletlen tulajdonságokkal is rendelkezhet. Ezt a szituációt [41] folytatásában, [42]-ben analizáltuk. A degenerált esetre vonatkozó eredményeket disszertációm 7. fejezetében ismertetem. A legfontosabb tételek a következők:

Degenerált polinomok esetében a rangot azzal a legkisebb r pozitív egésszel definiáljuk, melyre $f(x_1, x_2)$ felírható (6.2) alakban.

6.2. Tétel. (Gyarmati, Sárközy, Stewart) *Legyen $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ egy kétváltozós, legalább elsőfokú, r rangú, k-adfokú polinom. Tegyük fel, hogy ℓ a korreláció rangja kisebb vagy egyenlő mint r, és a 6.1. Tételben megadott a), b), c), d) és e) feltételek közül legalább egy fennáll. Ekkor a* (6.1)*-gyel definiált η bináris rács esetén*

$$Q_\ell(\eta) < 11k\ell p^{3/2} \log p.$$

Azt is bizonyítottuk, hogy létezik olyan magasrendű korreláció, amely nagy.

6.3. Tétel. (Gyarmati, Sárközy, Stewart) *Legyen $f \in \mathbb{F}_p[x_1, x_2]$ degenerált polinom, amelynek fokát k-val, rangját r-rel jelöljük. Ekkor létezik $\ell \le 2^r$ pozitív egész, amelyre*

$$Q_\ell(\eta) \ge p^2 - 4rp^{3/2} - 4\ell kp.$$

Megoldatlan kérdés, hogy r rangú, degenerált polinom esetén hogyan becsülhető azon további pszeudovéletlen mértékek értéke, amelyek rendje $r+1$ és 2^r közé esik.

Erős pszeudovéletlen tulajdonságokkal rendelkező bináris sorozatok és rácsok konstruálása igen fontos terület a kriptográfiában. [27]-ben egy összefoglaló cikkemben számos új konstrukciót említettem, ezek közül különösen figyelemreméltóak az elliptikus görbéket is használó konstrukciók, lásd pl. Mérai [53], [54], [55], [56], Chen [12], Chen, Li és Xiao [13] és Liu, Zhan és Wang [47] eredményeit.

7. További eredmények

Disszertációm utolsó fejezetében rövid összefoglalót adok a PhD-m óta (részben egyedül, részben társszerzőkkel közösen) írt pszeudovéletlenséggel

kapcsolatos 18 cikkem eredményeiről (ld. [19], [21], [23], [24], [25], [27], [28], [29], [31], [32], [33], [34], [35], [36], [37], [38], [39] és [40] cikkek).

Hivatkozások

[1] R. Ahlswede, L.H. Khachatrian, C. Mauduit and A. Sárközy, *A complexity measure for families of binary sequences*, Periodica Math. Hungar. 46 (2003), 107-118.

[2] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite sequences: minimal values*, Combin., Probab. Comput. 15 (2005), 1-29.

[3] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite sequences: typical values*, Proc. London Math. Soc. 95 (2007), 778-812.

[4] V. Anantharam, *A technique to study the correlation measures of binary sequences*, Discrete Math. 308, (24) (2008), 6203 -6209.

[5] J. Beck, *Roth's estimate on the discrepancy of integer sequences is nearly sharp*, Combinatorica 1 (1981), 319-325.

[6] A. Bérczes, J. Ködmön and A. Pethő, *A one-way function based on norm form equations*, Periodica Math. Hungar. 49 (2004), 1-13.

[7] L. Blum, M. Blum and M. Shub, *A simple unpredictable pseudorandom number generator*, SIAM J. Comp. 15 (1986), 364-383.

[8] J. Bourgain, *Mordell's exponential sum estimate revisited*, J. Amer. Math. Soc. 18 (2005), 477–499.

[9] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika 4 (1957) 106-112.

[10] J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat and A. Sárközy, *On finite pseudorandom binary sequences III: The Liouville function, I*, Acta Arith. 87 (1999), 367-384.

[11] J. Cassaigne, C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences VII: The measures of pseudorandomness*, Acta Arith. 103 (2002), 97-118.

[12] Z. Chen, *Elliptic curve analogue of Legendre sequences*, Monatshefte für Mathematik, 154 (2008), 1-10.

[13] Z. Chen, S. Li and G. Xiao, *Construction of pseudo-random binary sequences from elliptic curves by using discrete logarithm*, in: Sequences and their applications - SETA 2006, Lecture Notes in Computer Science 4086, Berlin ; Heidelberg: Springer Verlag, 2006, 285-294.

[14] P. Erdős and A. Sárközy, *Some solved and unsolved problems in combinatorial number theory*, Math. Slovaca 28 (1978), 407-421 (page 415).

[15] H. Feistel, W. A. Notz, J. L. Smith, *Some cryptographic techniques for machine-to-machine data communications*, Proceedings of the IEEE 63 (1975), 1545-1554.

[16] S. Goldwasser, *Mathematical Foundations of Modern Cryptography: Computational Complexity Perspective*, ICM 2002, vol., I, 245-272.

[17] L. Goubin, C. Mauduit and A. Sárközy, *Construction of large families of pseudorandom binary sequences*, J. Number Theory 106 (2004), 56-69.

[18] K. Gyarmati, *On the correlation of binary sequences*, Studia Sci. Math. Hungar. 42 (2005), 59-75.

[19] K. Gyarmati, *A note to the paper „On a fast version of a pseudorandom generator"*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 49 (2006), 87-93.

[20] K. Gyarmati, *Pseudorandom sequences constructed by the power generator*, Period. Math. Hungar. 52 (2), (2006) 9-26.

[21] K. Gyarmati, *Concatenation of pseudorandom binary sequences*, Period. Math. Hung. 58 (1), (2009), 99-120.

[22] K. Gyarmati, *On the complexity of a family related to the Legendre symbol*, Period. Math. Hung. 58 (2), (2009), 209-215.

[23] K. Gyarmati, *Concatenation of Legendre symbol sequences*, Studia Sci. Math. Hungarica 48 (2), (2011), 193-204.

[24] K. Gyarmati, *On new measures of pseudorandomness of binary lattices*, Acta Math. Hung. 131 (4), (2011), 346-359.

[25] K. Gyarmati, *Elliptic curve analogues of a pseudorandom generator*, Period. Math. Hungar. 64 (2), (2012), 119-130.

[26] K. Gyarmati, *On the correlation of subsequences*, Unif. Distrib. Theory 7 (2012), 169–195.

[27] K. Gyarmati, *Measures of pseudorandomness*, Finite fields and applications: character sums and polynomials, P. Charpin, A. Pott, A. Winterhof (eds.), Radon Series in Computational and Applied Mathematics, de Gruyter, to appear.

[28] K. Gyarmati, P. Hubert and A. Sárközy, *Pseudorandom binary functions on almost uniform trees*, J. Combin. Number Theory 2, (2010), 1-24.

[29] K. Gyarmati, P. Hubert and A. Sárközy, *Pseudorandom binary functions on rooted plane trees*, J. Combin. Number Theory 4, (2012), Article 1.

[30] K. Gyarmati and C. Mauduit, *On the correlation of binary sequences, II*, Discrete Math. 312 (2012), 811-818.

[31] K. Gyarmati, C. Mauduit and A. Sárközy, *Pseudorandom binary sequences and lattices*, Acta Arith. 135 (2008), 181-197.

[32] K. Gyarmati, C. Mauduit and A. Sárközy, *Constructions of pseudorandom binary lattices*, Uniform Distribution Theory 4, (2009), 59-80.

[33] K. Gyarmati, C. Mauduit and A. Sárközy, *Measures of pseudorandomness of binary lattices, I. (The measures Q_k, normality.)*, Acta Arith. 144 (2010), 295-313.

[34] K. Gyarmati, C. Mauduit and A. Sárközy, *Measures of pseudorandomness of binary lattices, III. (Q_k, correlation, normality, minimal values.)*, Unif. Distrib. Theory 5 (2010), 183-207.

[35] K. Gyarmati, C. Mauduit and A. Sárközy, *Measures of pseudorandomness of finite binary lattices, II (The symmetry measures.)*, Ramanujan J. 25 (2), (2011), 155-178.

[36] K. Gyarmati, C. Mauduit and A. Sárközy, *Measures of pseudorandomness of families of binary lattices, I (Definitions, a construction using quadratic characters.)*, Publi. Math. Debrecen 79 (3), (2011), 445-460.

[37] K. Gyarmati, C. Mauduit and A. Sárközy, *Measures of pseudorandomness of families of binary lattices, II (A further construction.)*, Publi. Math. Debrecen 80 (3), (2012), 479-502.

[38] K. Gyarmati, C. Maduit and A. Sárközy, *On linear complexity of binary lattices*, Ramanujan J., to appear.

[39] K. Gyarmati, C. Maduit and A. Sárközy, *On linear complexity of binary lattices, II*, submitted.

[40] K. Gyarmati, A. Pethő and A. Sárközy, *On linear recursion and pseudorandomness*, Acta Arith. 118 (4), (2005), 359-374.

[41] K. Gyarmati, A. Sárközy and C. L. Stewart, *On Legendre symbol lattices*, Unif. Distrib. Theory 4 (2009), 81-95.

[42] K. Gyarmati, A. Sárközy and C. L. Stewart, *On Legendre symbol lattices, II*, Unif. Distrib. Theory, to appear.

[43] J. Hoffstein and D. Lieman, *The distribution of the quadratic symbol in function fields and a faster mathematical stream cipher*, Progress in Computer Science and Applied Logic, Vol. 20, Birkhäuser, Verlag, Basel, 2001; pp. 59-68.

[44] P. Hubert, C. Mauduit and A. Sárközy, *On pseudorandom binary lattices*, Acta Arith. 125 (2006), 51-62.

[45] J. Kam and G. Davida, *Structured design of subtitution-permutation encryption networks*, IEEE Transactions on Computers 28 (1979), 747-753.

[46] Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite sequences: minimum and typical values*, Proceedings of WORDS'03, TUCS Gen. Publ. 27, Turku Cent. Comput. Sci., Turku, 2003, 159-169.

[47] H. Liu, T. Zhan and X. Wang, *Large families of elliptic curve pseudorandom binary sequences*, Acta Arith. 140 (2009), 135-144.

[48] H. Liu, T. Zhan and X. Wang, *On the correlation of pseudorandom binary sequences with composite moduli*, Publ. Math. Debrecen 74 (2009), 195–214.

[49] J. Matoušek and J. Spencer, *Discrepancy in arithmetic progressions*, J. Amer. Math. Soc. 9 (1996), 195-204.

[50] C. Mauduit, *Construction of pseudorandom finite sequences*, unpublished lecture notes to the conference, Information Theory and Some Friendly Neighbours- ein Wunschkonzert, Bielefeld, 2003.

[51] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences I: Measures of pseudorandomness, the Legendre symbol*, Acta Arith. 82 (1997), 365-377.

[52] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1997.

[53] L. Mérai, *Pszeudovéletlen sorozatok és rácsok*, PhD értekezés, 2010.

[54] L. Mérai, *Construction of pseudorandom binary lattices using elliptic curves*, Proc. Amer. Math. Soc. 139 (2011), no. 2, 407-420.

[55] L. Mérai, *Construction of pseudorandom binary sequences over elliptic curves using multiplicative characters*, Publ. Math. Debrecen, 80 (2012), 199-213.

[56] L. Mérai, *Remarks on pseudorandom binary sequences over elliptic curves*, Fund. Inform. 114 (2012), 301-308.

[57] J. Rivat and A. Sárközy, *Modular constructions of pseudorandom binary sequences with composite moduli*, Period. Math. Hungar. 51 75–107.

[58] K. F. Roth, *Remark concerning integer sequences*, Acta Arith. 9 (1964), 257-260.

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