Pszeudovéletlen diszkrét struktúrákról

Habilitáció

Gyarmati Katalin

Eötvös Loránd Tudományegyetem

2012

1. Bevezetés

A számítógépek korában a véletlengenerálás fontos szerepet játszik életünkben. Azonban a véletlengenerálás kapcsán felmerül néhány nehéz kérdés: Mi is az a véletlen generálás? Az általunk használt módszerek valóban véletlen objektumokat állítanak-e elő? Manapság nagyon sokféle véletlen struktúrákat vizsgálnak, de az alkalmazásokban a legtöbbször a pszeudovéletlen $[0, 1)$ sorozatok (ld. pl. Niederreiter [60]) és a pszeudovéletlen bitsorozatok szerepelnek. Jelen dolgozatban pszeudovéletlen sorozatokat és azok többdimenziós kiterjesztéseit tanulmányozzuk.

Valódi véletlen sorozatokat többnyire fizikai módszerekkel generálnak, de vajon ezek a fizikai módszerek tényleg megfelelőek-e? E kérdések és problémák kapcsán idéznék Lovász László [53] ismeretterjesztő cikkéből:

„Ugyanakkor a véletlen igen nehéz fogalom is. Véletlen-e az, hogy egy földobott pénz fejre vagy írásra esik? A pénzfeldobás eredménye a véletlen esemény iskolapéldája, de ha jól meggondoljuk, miért is ne tudná egy igazán éles szemű és gyors eszű ember az alatt, amíg a pénz fölfelé száll, megfigyelni a pályáját, perdületét és amit csak még kell, és ebből kiszámítani, hogy melyik oldalára fog esni? Hogyan lehet megkülönböztetni az "igazi" véletlen jelenségeket az olyan jelenségektől, melyeknek a kimenetelét csak azért nem tudjuk megjósolni, mert nem áll rendelkezésünkre elegendő adat, vagy elegendő idő ahhoz, hogy kiszámítsuk?”

A valódi véletlengenerálásnak a gyakorlatban sok hátránya van: Valódi véletlengenerálással nyert sorozatok között elő kell fordulnia - mégha nagyon ritkán is - nagyon speciális szerkezetű sorozatoknak is, melyek speciális szerkezete az alkalmazás(ok)ban hibás eredményekre vezethet. Éppen ezért, ha valóban véletlen (pl. fizikai módszerre épülő) generátort használunk, akkor a kapott sorozatot utólag tesztelnünk kell, hogy valóban rendelkezik-e bizonyos véletlen szerkezettel. Továbbá, ha a kapott sorozatot például a kriptográfi-

A tudományos kutatást részben az Országos Tudományos Kutatási Alap K67676 és PD72264, részben a Bolyai János Kutatási Ösztöndíj támogatta.

ában akarjuk felhasználni, akkor a teljes sorozatot el kell juttatnunk levelezőpartnerünknek. Általában tehát az ilyen típusú sorozatok alkalmazása hosszadalmas és nehézkes. Ezért a gyakorlatban ma már csak nem kizárólag valamilyen matematikai algoritmussal előállított, a véletlent csupán imitáló un. *pszeudovéletlen* sorozatokat használunk.

2. Előzmények

Az elmúlt 70 évben rengeteg cikk született a pszeudovéletlenség témaköréből. Ezekben a cikkekben különböző célok, megközelítések, matematikai módszerek széles skálája szerepel. Magát a pszeudovéletlenség fogalmát is többféleképpen definiálják. Menezes, Oorschot és Vanstone [57] egy kitűnő kriptográfiai könyvet írt 2001-ben, melyben - többek között - a pszeudovéletlenség fogalmát is analizálják. Korábban a pszeudovéletlenség fogalmát általában bonyolultságelméleti úton definiálták. Goldwasser [17] egy kitűnő áttekintő cikket írt erről a nézőpontról. Azonban mostanában a bonyolultságelméleti megközelítést egyre szélesebb körben kritizálják. Fontos probléma például az, hogy ez a megközelítés csak generátorokat minősít, de az egyes sorozatok aposzteriori tesztelését nem teszi elkerülhetővé. A bonyolultságelméleti megközelítés egyik standard definíciója az úgynevezett „következő bit teszt", amely azonban csak bizonyítatlan hipotéziseken alapuló tesztelést tesz lehetővé. Továbbá a bonyolultságelméleti megközelítés általában végtelen hosszú számsorozatok esetén használatos csak, míg a gyakorlati alkalmazások során mindig csak véges hosszú sorozatot használunk.

A pszeudovéletlen bináris sorozatoknak rengeteg alkalmazása van. Ezek közül a legfontosabbak a híres Vernam féle titkosító eljáráshoz kapcsolódnak (mely abból áll, hogy a bitsorozat formájában adott továbbítandó információt úgy titkosítja, hogy ahhoz modulo 2 hozzáad egy véletlen vagy pszeudovéletlen bitsorozatként megadott kulcsot).

Több mint 15 évvel ezelőtt Mauduit és Sárközy [55] bevezetett egy új, konstruktív megközelítést. Azóta ez a terület folyamatosan fejlődik, rengeteg cikk született a témában. Sárközy [62]-ben egy kitűnő összefoglalást ad a legfontosabb eredményekről.

Egy adott sorozat pszeudovéletlen tulajdonságainak jellemzésére Mauduit és Sárközy [55] a következő kvantitatív mértékeket vezették be (bitsorozat helyett nyilván vizsgálhatunk +1-ekből és -1-ekből álló sorozatokat):

2.1. Definíció. *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:

2.2. Definíció. *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* $V(E_N, M, D)$ *az*

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

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* $0 \le d_1 < d_2 < \dots < d_\ell < M + d_\ell \le N$.

Cassaigne, Mauduit és Sárközy [9] bebizonyította, hogy majdnem minden $E_N \in \{-1,+1\}^N$ sorozatra $W(E_N)$ és $C_\ell(E_N) \ll \sqrt{N}(\log N)^c$. Így egy E_N sorozatot „jó” pszeudovéletlen sorozatnak tekintünk, ha mind $W(E_N)$ mind $C_\ell(E_N)$ (legalább kicsi ℓ-re) kicsi (legfeljebb $o(N)$) N függvényében.

[61]-ben Mauduit és Rivat a legalapvetőbb statisztikus tesztek eredményét jól becsülte W és C_ℓ segítségével. (Ezeknek a statisztikus teszteknek a pontos definícióját például [57]-ben találhatjuk meg.) Brandstätter, Winterhof [7] és Andics [3] a lineáris komplexitást becsülte a korreláció segítségével. Ezek az eredmények azt mutatják, hogy W és C_ℓ alapvető mértékek, segítségükkel több pszeudovéletlen tulajdonság jól kontrollálható. Természetesen számtalan további W-hez és C_ℓ-hez hasonló pszeudovéletlen mérték lenne bevezethető, azonban valahol határt kell szabnunk az újabb és újabb mértékek bevezetésének. Ezt a problémát Knuth [50] könyvében részletesen tárgyalja a Kolmogorov komplexitás nézőpontjából. A fent említett - statisztikus tesztekre és a lineáris komplexitásra vonatkozó - eredmények miatt a legtöbb cikk a W és C_ℓ mértékekre szorítkozik, melyek tekinthetők a pszeudovéletlenség legalapvetőbb mértékeinek. Jelen dolgozatban az eloszlás és korreláció mérték mellett, időnként még a következő mértékeket fogjuk használni:

2.3. Definíció. *Legyen $E_N = (e_1, e_2, \dots, e_N) \in \{-1,+1\}^N$ egy N hosszú ± 1 sorozat. $\ell \in \mathbb{N},\ M \in \mathbb{N},\ X = (x_1, \dots, x_\ell) \in \{-1,+1\}^\ell$ esetén legyen*

$$T(E_N, M, X) \stackrel{\text{def}}{=} |\{n:\ 0 \le n < M,\ (e_{n+1}, e_{n+2}, \dots, e_{n+\ell}) = X\}|.$$

*Ekkor az ℓ-**ed rendű normalitás mérték**e E_N-nek*

$$N_\ell(E_N) \stackrel{\text{def}}{=} \max_{X \in \{-1,+1\}^\ell} \max_{0 < M \le N+1-\ell} \left| T(E_N, M, X) - M/2^\ell \right|.$$

Megjegyzem, hogy Mauduit és Sárközy [55] eredménye szerint

2.1. Tétel.

$$N_\ell(E_N) \le \max_{1 \le t \le \ell} C_t(E_N).$$

Vagyis a korreláció segítségével a normalitás mérték jól becsülhető. (Ezért a legtöbb cikkben nem kezelik külön a normalitás mértéket.)

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

2.4. Definíció. *Legyen* $E_N = (e_1, e_2, \dots, e_N) \in \{-1, +1\}^N$ *egy* N *hosszú* ± 1 *sorozat. Ekkor* E_N*-nek az* **ℓ-ed rendű kombinált (eloszlás-korreláció) mérték***ét a következőképpen definiáljuk:*

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

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

Mauduit és Sárközy [55] először a Legendre szimbólum segítségével konstruált erős pszeudovéletlen tulajdonságokkal rendelkező sorozatot.

2.2. Tétel. *Létezik egy* p_0 *szám, hogy ha* $p > p_0$ *prím, akkor ha az* $E_{p-1} = (e_1, ..., e_{p-1})$ *sorozat* n*-edik elemét*

$$e_n = \left(\frac{n}{p}\right) \qquad (n = 1, 2, ..., p-1 \text{ esetén})$$

képlettel definiáljuk, akkor

$$W(E_{p-1}) \leq 9p^{1/2} \log p$$

és

$$C_\ell(E_{p-1}) \leq 9\ell p^{1/2} \log p.$$

A bizonyítás Weil tételének [68] egy következményén alapul, melyet Sárközy és Mauduit [55] Vinogradov egy egyenlőtlenségét [66] használva bizonyított:

2.3. Tétel. *Ha p prím és χ egy d-ed rendű karakter, amely azonban nem főkarakter modulo p, $f(x) \in F_p[x]$ k-adfokú polinom, melynek faktorizációja $f(x) = b(x - x_1)^{d_1} \dots (x - x_s)^{d_s}$ $(x_i \neq x_j$ ha $i \neq j)$ $\overline{\mathbb{F}}_p$ $(= \mathbb{F}_p$ algebrai lezártja) felett és ahol*

$$(d, d_1,\ d_2,\ \dots,\ d_s) = 1,$$

akkor az olyan X, Y valós számokra, ahol $0 < Y \leq p$, tudjuk, hogy

$$\left| \sum_{X < n \leq Y} \chi(f(n)) \right| < 9kp^{1/2}\ \log p.$$

Az utóbbi tíz évben számtalan pszeudovéletlen bináris sorozatot konstruáltak és teszteltek, a legjobb konstrukciókra $W(E_N) \ll N^{1/2}(\log N)^c$ és $C_\ell(E_N) \ll N^{1/2}(\log N)^{c_\ell}$ becslések is fennállnak, ahol $c, c_2, c_3, \dots$ pozitív konstansok. Eleinte ezek a konstrukciók rögzített N-re csak „kevés" N hosszúságú sorozatot adtak. Néhány kriptográfiai alkalmazásban azonban nagyon „sok" sorozatra van egyszerre szükség. (Gyakran szükséges például, hogy az alkalmazott sorozat minél több azonos hosszúságú sorozatból legyen kiválasztva, abból a célból, hogy ésszerű időn belül ne lehessen - például az összes lehetséges sorozatot végigpróbálva - megtalálni az alkalmazott sorozatot.) Először Goubin, Mauduit és Sárközy [18] igazolta, hogy pszeudovéletlen sorozatoknak - egy általuk bevezetett nagy családjában - a sorozatok erős pszeudovéletlen tulajdonságokkal rendelkeznek.

2.1. Konstrukció. *Legyen $K > 0$ rögzített egész. Tekintsük az összes olyan $f(x) \in \mathbb{F}_p[x]$ k-adfokú polinomot, ahol $k \leq K$, 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*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right) & \text{ha } (f(n), p) = 1, \\ +1 & \text{ha } p \mid f(n). \end{cases} \tag{2.1}$$

Hoffstein és Lieman [47] olyan $f(x)$ polinom használatát javasolták (2.1)-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 [18] igazolta, hogy ha néhány nem túlságosan megszorító feltevést kikötünk a konstrukcióban szereplő $f(x)$ polinomról, úgy az E_N sorozatnak erős pszeudovéletlen tulajdonságai vannak:

2.4. Tétel. *Ha p prím és $f(x)$ polinomra teljesülnek a 2.1. Konstrukció kikötései, akkor a (2.1)-gyel definiált E_p sorozatra*

$$W(E_p) < 10kp^{1/2} \log p.$$

Tegyük fel továbbá, hogy $\ell \in \mathbb{N}$ és legalább egy teljesül a következő 3 feltétel közül:
(i) $\ell = 2$;
(ii) $\ell < p$ és 2 primitív gyök modulo p;
(iii) $(4k)^\ell < p$.
Ekkor

$$C_\ell(E_p) < 10k\ell p^{1/2} \log p.$$

Később Mauduit és Sárközy [56] az élesebb

$$4^{k+\ell} < p$$

feltétellel helyettesítette az (iii) feltételt a 2.4. Tételben.

Valószínűleg az (i)-(iii) feltételek mindegyike élesíthető (dolgozatom 6. fejezetében kísérletet is teszek erre), de példák mutatják, hogy ilyen vagy hasonló típusú feltételekre szükség van.

A 2.1. Konstrukcióban szereplő sorozatokat aposzteriori tesztelte Rivat, Sárközy [61]-ben. Az Amerikai Szabványhivatal (National Institute of Standards and Technology) sts-1.4. csomagjában megjelölt néhány olyan statisztikus tesztet, amelyek alapvető fontosságúak, és amelyeknek egy erős pszeudovéletlen tulajdonságokkal rendelkező sorozatoknak feltétlen eleget kell tennie. Rivat és Sárközy számítógép segítségével tesztelt néhány 2.1. Konstrukcióban előállított sorozatot. Minden esetben azt találták, hogy ezek a sorozatok messze eleget tesznek a NIST által megjelölt statisztikus tesztek mindegyik kritériumának. Ezentúl is vannak számítógépes evidenciák a 2.1. Konstrukció erős pszeudovéletlen tulajdonságainak az igazolására. Pl. Andics [3] a lineáris komplexitást vizsgálta számitógép segítségével, s azt találta, hogy annak értéke is - minden vizsgált esetben - optimális.

Bizonyos alkalmazásokban a pszeudovéletlenség többdimenziós analogonjára van szükségünk. Ahhoz például, hogy egy képet a Vernam-féle titkosító eljárással titkosítsunk pszeudovéletlen bináris sorozatok helyett „pszeudovéletlen bináris rácsokra" van szükségünk. Ezért a közelmúltban Hubert, Mauduit és Sárközy [48] bevezette a pszeudovéletlenség többdimenziós elméletét.

Egy dimenzióban tehát sok erős pszeudovéletlen sorozatot konstruáltak. A legerősebb konstrukciókat tipikusan $\mathbb{F}_p$-ben generálták, additív vagy multiplikatív karaktereket és polinomokat használva. A pszeudovéletlen mértékek becslése során használt legkomolyabb eszköz Weil tétele [68] volt. Sajnos, a legtöbb egydimenziós konstrukció több dimenzióra való kiterjesztése során gondok merülnek fel. Ugyanis a Weil tétel többdimenziós kiterjesztését, a Deligne tételt kellene alkalmaznunk. Bár mostanában Fouvry és Katz [14] egyszerűsítette a Delinge tétel alkalmazhatóságához szükséges feltételeket, de azért bizonyos nem szingularitási feltételre még mindig szükség van, és ez gondokat okoz a tétel alkalmazása során. A nehézségek ellenére, [36], [44], [45] [48], [52], [54], [56] [58], [59]-ben erős n-dimenziós konstrukciókat adtak meg.

A következő 8 fejezetben részben egyedül, részben társszerzőkkel írt [21], [22], [27] [29], [31] [32], [44], [45] cikkeimből ismertetek eredményeket. Végül az utolsó fejezetben röviden említem a [20], [23], [33], [34], [35], [36], [37], [38], [39],[40], [41], [42], [43] cikkekben szereplő kutatási témáimat.

3. A hatványgenerátorral konstruált pszeudovéletlen sorozatok

Ebben a fejezetben a hatványgenerátor pszeudovéletlen tulajdonságait tanulmányozzuk. (A hatványgenerátor speciális esetként tartalmazza az RSA generátort és a Blum-Blum-Shub generátort.)

A *hatványgenerátort* a következőképpen definiáljuk:

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

$$\begin{aligned} &u_0 = \vartheta \\ &u_n \equiv u_{n-1}^k \pmod m, \quad 0 \leq u_n \leq m-1, \quad n = 1, 2, \dots . \end{aligned} \tag{3.1}$$

A hatványgenerátornak számos alkalmazása van a kriptográfiában, ld. [5], [11], [51], [63]. A hatványgenerátort a $(k, \varphi(m)) = 1$ (ahol $\varphi(m)$ az Euler függvény) speciális esetben *RSA generátornak*, a $k = 2$ speciális esetben *Blum-Blum-Shub generátornak* hívjuk.

Habár a hatványgenerátornak számtalan különböző tulajdonságát tanulmányozták (pl. [5], [8], [10], [11], [13], [16] [19], [46], [51], [57], [63]), de nagyon kevés feltétel nélküli eredmény ismert; a legtöbb eredmény azon a feltételezésen alapul, hogy nem lehet polinomiális időben faktorizálni. A [32]-ben közölt eredményeim feltétel nélküliek. Ezekről adnék itt egy rövid összefoglalót:

3.1. Jelölés. *Legyen p prím, $\vartheta \in \mathbb{F}_p^*$. Definiáljuk az u_n sorozatot* (3.1)*-gyel, ahol p prím modulust vesszük m helyén (ekkor u_n a $[0, p-1]$ intervallumban van). Nyilvánvalóan $u_n \equiv \vartheta^{k^n} \pmod p$ multiplikatív rendje monoton csökkenő (nem szigorúan!), ahogy $n \to \infty$. Jelölje n_0 a legkisebb pozitív egészet, amelyre $n \geq n_0$ esetén*

$$u_n \equiv \vartheta^{k^n} \pmod p$$

multiplikatív rendje ugyanaz a t szám. Ekkor

$$(k, t) = 1.$$

Jelölje T k multiplikatív rendjét modulo t.

Ebben a fejezetben $p, \vartheta, t, k, T, n_0$ számokat és $\{u_n\}$ sorozatot végig a fent definiált módon értelmezzük. Világos, hogy az

$$u_{n_0}, u_{n_0+1}, u_{n_0+2}, \dots$$

sorozat tisztán periodikus T periódussal.

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

3.1. Konstrukció. *Definiáljuk az $E_T = (e_1, \dots, e_T)$ sorozatot a következő képlettel*

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

Ebben a fejezetben az E_T sorozat pszeudovéletlen tulajdonságait becsüljük. Először az eloszlás mértéket és a normalitás mértéket becsüljük.

3.1. Tétel.

$$W(E_T) \ll p^{7/8} (\log p)^2.$$

A normalitás mértékre a következő becslésünk van:

3.2. Tétel. *Minden $\varepsilon > 1/4$ esetén*

$$N_\ell(E_T) \ll k^{\varepsilon(\ell-1)} p^{7/8} (\log p)^{\ell+1},$$

ahol az alkalmazott konstans szorzó csak ε-tól függ.

A 3.1. és 3.2. Tétel bizonyítása Friedlander, Hansen és Shparlinski [15] tételeinek általánosításait használja.

Egészen mostanáig csak a „rövidtávolságú" (shortrange) korrelációt ($\sum_n e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell}$ kis d_i-kre) tudtuk becsülni. Bourgain új, gyönyörű tételét [6] használva azonban a „hosszútávolságú" (longrange) korreláció is jól becsülhető. Így [32]-ben mindhárom (eloszlás, normalitás, korreláció) mértékre nem triviális felső becslést adtam, ezzel bebizonyítva, hogy a hatványgenerátor a Mauduit és Sárközy által bevezetett értelemben is erős pszeudovéletlen tulajdonságokkal rendelkezik.

4. A Legendre szimbólumot használó család f-bonyolultsága

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. *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 $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_j \in \{-1,+1\}$-re, legalább egy $E_N = (e_1, \ldots, e_N) \in \mathcal{F}$ sorozat létezik, amelyre*

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

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.

4.1. Tétel. *Legyen p prím. Tekintsük az összes olyan $f(x)$ polinomot, amelyre*

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

(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 $E_p = E_p(f) = (e_1, e_2, \ldots, e_p) \in \{-1,+1\}^p$ sorozatot, amelyet (2.1)-gyel definiálunk, és jelölje $\mathcal{F}_1$ az ily módon kapott bináris sorozatok családját. Ekkor

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

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

4.1. Propozíció.

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

A 3.1. Propozícióból azonnal következik, hogy

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

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? [29]-ben megjavítottam az alsó becslést, és a következőt kaptam:

4.2. Tétel.

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

Vagyis az alsó és a felső becslés most már csak egy konstans szorzóval tér el egymástól. Az alsó becslés bizonyítása során karakterösszegeket és Weil tételt [68] alkalmaztam.

5. Pszeudovéletlen bináris sorozatok konkatenációja

A pszeudovéletlen sorozatok használata közben előfordulhat, hogy az alkalmazott pszeudovéletlen sorozat nem elég hosszú. Ezen úgy próbálunk segíteni, hogy a családból több sorozatot rakunk egymás mögé. Persze kérdéses, hogy ekkor a kapott hosszabb sorozatnak mikor lesznek erős pszeudovéletlen tulajdonságai? Tulajdonképpen azt szeretnénk, hogy bárhogy veszünk a családból sorozatokat, azokat egymás mögé írva („konkatenálva”), még mindig erős pszeudovéletlen tulajdonságokkal rendelkezzen a kapott, hosszabb sorozat. Anantharam [2] definícióját általánosítva [22]-ben bevezettem az f-korreláció fogalmát.

5.1. Definíció. *Legyen $\mathcal{F} \subseteq \{-1,+1\}^N$ pszeudovéletlen sorozatoknak egy nagy családja. $\mathcal{F}$-nek ℓ-edrendű f-korrelációját a következőképpen definiáljuk:*

$$C_\ell(\mathcal{F}) \stackrel{\text{def}}{=} \max_{1 \le k \le \ell,\ E_N^{(1)}, E_N^{(2)}, \ldots, E_N^{(k)} \in \mathcal{F}} C_\ell((E_N^{(1)}, E_N^{(2)}, \ldots, E_N^{(k)})),$$

ahol a maximumot az összes $1 \le k \le \ell$ egészen és különböző $E_N^{(1)}, E_N^{(2)}, \ldots, E_N^{(k)} \in \mathcal{F}$ sorozatokon vesszük, és ahol $(E_N^{(1)}, E_N^{(2)}, \ldots, E_N^{(k)}) \in \{-1,+1\}^{kN}$ kN hosszú bináris sorozat, amelyet úgy kapunk, hogy rendre az $E_N^{(1)}, E_N^{(2)}, \ldots, E_N^{(k)}$ sorozatok elemeit egymás után írjuk (azaz az $(E_N^{(1)}, E_N^{(2)}, \ldots, E_N^{(k)})$ sorozat az $E_N^{(1)}, E_N^{(2)}, \ldots, E_N^{(k)}$ sorozatok konkatenációja).

Korábban a 4.1. Definícióban bevezettük az f-bonyolultság fogalmát. Felmerül a kérdés, hogy valóban szükség van-e az f-korreláció bevezetésére? [22]-ben példákkal igazoltam az f-korreláció szükségességét.

Ezek után olyan nagy családot konstruáltam, amelynek a f-korrelációja kicsi. Kiindulási alapul a 2.1. Konstrukcióban ismertetett nagy családot vettem. Ebben az esetben $f(x)$-et írva (2.1)-ben egy $(e_1, e_2, \ldots, e_p)$ sorozatot kapunk, $f(x+1)$-et írva pedig ennek a sorozatnak egy „eltoltját”, az $(e_2, e_3, \ldots, e_p, e_1)$ sorozatot kapjuk. Ezen két sorozat nyilvánvalóan nem független, s valóban egymás mögé írva a két sorozatot egy olyan $2p$ hosszú sorozatot kapunk, amelynek a másodrendű korrelációja nagy. Szerencsére, a 2.1. Konstrukcióban szereplő családnak egy elég nagy részcsaládját véve ez a probléma elkerülhető:

5.1. Tétel. *Legyen p prím és $K \in \mathbb{N}$, $K < p$. Tekintsük az összes $f(x) \in \mathbb{F}_{|}[x]$ polinomot, amely irreducibilis és*

$$0 < k = \deg f(x) \le K,$$

továbbá $f(x)$ felírható

$$f(x) = x^k + a_{k-2}x^{k-2} + a_{k-3}x^{k-3} + \cdots + a_1 x + a_0$$

alakban, ahol $1 \le i \le k-2$ *esetén* $a_i \in \mathbb{F}_p$ *és* $x^{\deg f - 1} = x^{k-1}$ *együtthatója* $a_{k-1} = 0$. *Minden ilyen* $f(x)$ *polinomra, vegyük az* $E_p = E_p(f) = (e_1, e_2, \ldots, e_p) \in \{-1,+1\}^p$ (2.1)*-gyel definiált bináris sorozatot, és legyen* $\mathcal{F}_2$ *az így kapott bináris sorozatok nagy családja. Ekkor* $\ell \ge 2$ *esetén*

$$C_\ell(\mathcal{F}_2) \le 10K\ell^2 2^{\ell-1} p^{1/2} \log p.$$

E konstrukció némi szépséghibája, hogy irreducibilis polinomokból indul ki, de megjegyzem, hogy viszonylag egyszerű és gyors konstrukciók és algoritmusok ismeretesek irreducibilis polinomok készítésére. Az 5.1. Tételt [22]-ben igazoltam. [22]-ben bevezettem a gyenge korreláció fogalmát is, melyben csak bizonyos konkatenációkon vesszük a maximumot.

6. Legendre szimbólumon alapuló sorozatok konkatenációja

Az előző fejezetben láttuk, hogy az irreducibilis polinomokból való kiindulás miatt az 5.1. Tételben bevezetett $\mathcal{F}_2$ család alkalmazása nem ideális. Ebben a fejezetben egy másik családot adunk meg, úgy, hogy a családban szereplő sorozatok sokkal gyorsabban generálhatóak. Sajnos, ennek a családnak az f-korrelációja nagy lesz, de ez a probléma megkerülhető. Egyszerűen megmondjuk, hogy a családból milyen sorozatok írhatóak egymás után úgy, hogy a kapott hosszabb sorozatnak biztosan (és bizonyítottan) erős pszeudovéletlen tulajdonságai legyenek. A fejezetben szereplő eredményeket [21]-ben igazoltam.

A kiindulási alapunk továbbra is a 2.1. Konstrukcióban szereplő nagy család. Ennek vesszük egy részcsaládját, amely még mindig elegendően sok sorozatot tartalmaz. Ezt úgy tesszük meg, hogy a konstrukcióban szereplő $f(x)$ polinomok halmazát szűkítjük. A 2.4. Tételben láttuk, hogy ha $f(x)$ polinom foka és a korreláció rendje nem túl nagy, akkor a sorozatnak a korrelációja kicsi. A következőkben egy olyan $f(x)$-re vonatkozó feltételt ismertetek, amely szintén biztosítja a kicsi korrelációt, ráadásul az ilyen polinomok nagyon egyszerűen és gyorsan konstruálhatóak.

6.1. Tétel. *Legyen p egy páratlan prím, $R \in \mathbb{N}$, $f(x) \in \mathbb{F}_p[x]$ egy polinom, amely felírható*

$$f(x) = \left(x^2 - a_1\right)\left(x^2 - a_2\right)\cdots\left(x^2 - a_k\right)(x-1)$$

alakban, ahol $0 \leq \deg f(x) = 2k+1 \leq K$, az a_i-k különböző kvadratikus nem maradékok modulo p, azaz $\left(\frac{a_i}{p}\right) = -1$ ha $1 \leq i \leq k$. Minden ilyen f polinomra, tekintsük a (2.1)-gyel definiált $E_p = E_p(f)$ pszeudovéletlen bináris sorozatot. Legyen $\mathcal{F}_3$ az ily módon definiált bináris sorozatok családja. Ekkor minden $E_p(f) \in \mathcal{F}_3$ esetén

$$C_\ell(E_p(f)) \ll K\ell p^{1/2} \log p.$$

A 6.1. Tételben nem becsültük az eloszlás mértéket. De a 2.4. Tételt alkalmazva azonnal éles becslést kapunk az eloszlás mértékre:

$$W(E_p(f)) \ll K p^{1/2} \log p.$$

Természetesen adódik a kérdés, hogy a 6.1. Tételben miért nem a kicsit egyszerűbb $f(x) = (x^2 - a_1)(x^2 - a_2)\cdots(x^2 - a_k)$ alakú polinomokat használjuk? Ekkor ugyan az $E_p(f)$ sorozat korrelációja kicsi, de ez a sorozat szimmetrikus ($e_n = e_{p-n}$ ha $1 \leq n \leq p$), ami problémákat okoz az alkalmazásokban (ld. pl. [26]).

Habár az $\mathcal{F}_3$ család sok erős pszeudovéletlen tulajdonságokkal rendelkező sorozatot tartalmaz, előfordulhat, hogy a család bizonyos sorozatai nem függetlenek egymástól. Legyenek $E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \ldots, E_p^{(t)} \in \{-1,+1\}^p$ p hosszú bináris sorozatok. Jelölje $(E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \ldots, E_p^{(t)}) \in \{-1,+1\}^{tp}$ azt a tp hosszú sorozatot, amelyet úgy kapunk, hogy rendre az $E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \ldots, E_p^{(t)} \in \{-1,+1\}^p$ sorozat elemeit egymás után írjuk.

Kérdésünk a következő: adott egy fix $E_p^{(1)} \in \mathcal{F}_3$ sorozat, ekkor hogyan választhatunk további $E_p^{(2)}, E_p^{(3)}, \dots, E_p^{(t)} \in \mathcal{F}_3$ sorozatokat úgy, hogy a sorozatok „konkatenációjának”, azaz $(E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \dots, E_p^{(t)}) \in \{-1,+1\}^{tp}$ sorozatnak erős pszeudovéletlen tulajdonságai legyenek? Sajnos, az nem igaz, hogy bárhogyan választjuk az $E_p^{(1)}, E_p^{(2)}, \dots, E_p^{(t)} \in \mathcal{F}_3$ sorozatokat, akkor az $(E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \dots, E_p^{(t)}) \in \{-1,+1\}^{tp}$ sorozatnak mindig erős pszeudovéletlen tulajdonságai lesznek. Tekintsük a következő egyszerű ellenpéldát:

$$\begin{aligned}
E_p^{(1)} &= E_p\left((x-1)\right) \in \mathcal{F}_3,\\
E_p^{(2)} &= E_p\big((x^2-a_1)(x-1)\big) \in \mathcal{F}_3,\\
E_p^{(3)} &= E_p\big((x^2-a_2)(x-1)\big) \in \mathcal{F}_3,\\
E_p^{(4)} &= E_p\big((x^2-a_1)(x^2-a_2)(x-1)\big) \in \mathcal{F}_3,
\end{aligned}$$

Ekkor $E_{4p} = (E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, E_p^{(4)})$ sorozatnak a 4-edrendű korrelációja nagy. Valóban:

$$\begin{aligned}
C_4(E_{4p}) &\geq |V(E_{4p}, p, (0, p, 2p, 3p))|\\
&= 1 + \sum_{n=2}^{p} \left(\frac{n-1}{p}\right)\left(\frac{(n^2-a_1)(n-1)}{p}\right)\\
&\quad \left(\frac{(n^2-a_2)(n-1)}{p}\right)\left(\frac{(n^2-a_1)(n^2-a_2)(n-1)}{p}\right)\\
&= 1 + \sum_{n=2}^{p} \left(\frac{(n^2-a_1)^2(n^2-a_2)^2(n-1)^4}{p}\right) = p.
\end{aligned}$$

A következőkben elégséges feltételt adunk arra, hogy az $(E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \dots, E_p^{(t)}) \in \{-1,+1\}^{tp}$ sorozatnak erős pszeudovéletlen tulajdonságai legyenek.

6.2. Tétel. *Legyen*

$$\begin{aligned} f_1(x) &= (x^2 - a_{11})(x^2 - a_{12}) \dots (x^2 - a_{1r_1})(x-1), \\ f_2(x) &= (x^2 - a_{21})(x^2 - a_{22}) \dots (x^2 - a_{2r_2})(x-1), \\ &\vdots \\ f_t(x) &= (x^2 - a_{t1})(x^2 - a_{t2}) \dots (x^2 - a_{tr_t})(x-1), \end{aligned} \tag{6.1}$$

ahol $a_{i1}, a_{i2}, \dots, a_{ir_i}$ *különböző kvadratikus nem maradékok modulo* p *ha* $1 \leq i \leq t$. *Tegyük fel továbbá, hogy* $a_{i1} = a_{vs}$ *akkor és csak akkor fordulhat elő* $i = v$ *és* $1 = s$. *Legyen*

$$K = 2 \max_{1 \leq i \leq t} r_i + 1 = \max_{1 \leq i \leq t} \deg f_i(x).$$

Definiáljuk $E_p^{(i)} \in \mathcal{F}_3$*-t* $E_p(f_i)$*-vel úgy, hogy* (2.1)*-ben* f_i*-t írunk* f *helyébe* $1 \leq i \leq t$ *esetén. Ekkor* $E_{tp} = (E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \dots, E_p^{(t)}) \in \{-1, +1\}^{tp}$ *sorozatnak erős pszeudovéletlen tulajdonságai vannak:*

$$\begin{aligned} W(E_{tp}) &\ll tKp^{1/2} \log p, \\ C_\ell(E_{tp}) &\ll K\ell t 2^{\ell-1} p^{1/2} \log p. \end{aligned}$$

7. A Legendre szimbólum rács

A pszeudovéletlenség többdimenziós kiterjesztése Hubert, Mauduit és Sárközy [48] 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:

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

Ezt a halmazt *n-dimenziós N-rácsnak* vagy röviden *N-rácsnak* nevezzük. Ezt a definíciót általánosabb rácsokra is kiterjeszthetjük. Legyen $\mathbf{u_1}, \mathbf{u_2}, \dots, \mathbf{u_n}$ n darab lineárisan független vektor, ahol $\mathbf{u_i}$-nek az i-edik koordinátája pozitív egész, a többi koordináta viszont 0, azaz $\mathbf{u_i} =$

$(0, \dots, 0, z_i, 0, \dots, 0)$ alakú, ahol $z_i \in \mathbb{Z}^+$. Legyen $t_1, t_2, \dots, t_n$ olyan egészek, ahol $0 \le t_1, t_2, \dots, t_n < N$. Ekkor a

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

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

Hubert, Mauduit és Sárközy [48]-ban 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 $\mathbf{x} = (x_1, \dots, x_n)$ és így $\eta(\mathbf{x}) = \eta((x_1, \dots, x_n))$, akkor a jövőben azt írjuk, hogy $\eta(\mathbf{x}) = \eta(x_1, \dots, x_n)$.

Egy ilyen függvény úgy szemléltethető, mint egy N-rács, amelyben a rácspontokat a + és − előjelek valamelyikével helyettesítjük. Az ilyen függvényeket *bináris N-rácsoknak* vagy rövidebben *bináris rácsoknak* nevezzük. A bináris 2 vagy 3 dimenziós pszeudovéletlen rácsok használatosak digitális képek, térképek titkosításához.

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

7.1. Definíció. *Legyen*

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

egy bináris rács. Definiáljuk **az ℓ-edrendű pszeudovéletlen mértékét** *η-nak a következő képlettel*

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

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

Ma már jónéhány többdimenziós konstrukció ismert erős pszeudovéletlen tulajdonságokkal rendelkező rácsokra ld. pl. [36], [44], [45] [48], [52], [54],

[56] [58], [59]. Ebben a fejezetben egy természetes - Legendre szimbólumon alapuló - konstrukciót ismertetek, melyet [44]-ben és [45]-ben publikáltunk. A korábbi cikkekben megadott konstrukciók kissé mesterkéltek. Ráadásul ezeknek a mesterkélt konstrukcióknak az implementálása meglehetősen bonyolult. Így [44]-ben - Sárközy Andrással és Cameron L. Stewarttal közösen - olyan „természetes” konstrukciót definiáltunk, ahol a pszeudovéletlen mértékekre adott becslések gyengébbek ugyan, mint az előbb említett cikkekben, de még mindig erős, nem triviális becslések. Ez a következő volt: Egy dimenzióban a legjobb és a legtöbbet vizsgált bináris sorozat a 2.1. Konstrukcióban definiált bináris sorozat. Ennek természetes két dimenziós kiterjesztése a következő:

7.1. Konstrukció. *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*

$$\eta(x_1, x_2) = \begin{cases} \left(\frac{f(x_1,x_2)}{p}\right) & \text{ha } (f(x_1, x_2), p) = 1, \\ +1 & \text{ha } p \mid f(x_1, x_2) \end{cases} \tag{7.1}$$

képlettel.

Megjegyezzük, hogy több olyan kétváltozós $f(x_1, x_2)$ polinom létezik, amelyre az η rácsnak gyenge pszeudovéletlen tulajdonságai vannak. Nézzünk néhány ilyen példát:

7.1. Példa. Legyen

$$f(x_1, x_2) = c\,(g(x_1, x_2))^2\,,$$

ahol $c \in \mathbb{F}_p$, $g(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$. Ekkor a (7.1)-gyel definiált rács majdnem minden eleme $\left(\frac{c}{p}\right)$ kivéve $f(x_1, x_2)$ nullhelyeit. Ebből következően, ha $f(x_1, x_2)$ foka nem túl nagy, akkor $Q_1(\eta)$ nagy.

7.2. Példa. Legyen $f(x_1, x_2) = g(x_1)$, ahol $g(x) \in \mathbb{F}_p[x]$ egyváltozós polinom. Ekkor

$$\eta(x_1, x_2)\eta(x_1, x_2 + 1) = \left(\frac{g(x_1)}{p}\right)\left(\frac{g(x_1)}{p}\right) = +1$$

kivéve $g(x_1)$ gyökeire, amiből következően $Q_2(\eta)$ nagy.

7.3. Példa. Legyen $f(x_1, x_2) = g(x_1)h(x_2)$ ahol $g(x), h(x) \in \mathbb{F}_p[x]$ egyváltozós polinomok. Kis számolás után könnyen látható, hogy $Q_4(\eta)$ nagy.

Az összes fenti példa speciális esete a következőnek:

7.4. Példa. Legyen r nem negatív egész és legyen α_j, $\beta_j \in \mathbb{F}_p$ $j = 1, \dots, r$ esetén. Legyen

$$f(x_1, x_2) = \left(\prod_{j=1}^{r} f_j(\alpha_j x_1 + \beta_j x_2) \right) g(x_1, x_2)^2 \tag{7.2}$$

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 $f \in \mathbb{F}_p[x, y]$ polinomokat, amelyek felírhatóak (7.2) 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 [44]-ben a következőt tudtuk bizonyítani:

7.1. Tétel. *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* (7.2) *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 (7.1)*-gyel definiált η bináris rács esetén*

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

Az első három példa azt mutatja, hogy ha f degenerált, akkor az (7.1)-gyel definiált bináris rács akár gyenge pszeudovéletlen tulajdonságokkal is rendelkezhet. Ezt a szituációt [44] egy folytatásában [45]-ben analizáltuk. Bebizonyítottuk, hogy az f degenerált polinomhoz rendelt η bináris rács pszeudovéletlen mértékeinek értéke az f polinom (7.2) alakjában szereplő r nagyságától függ. Továbbá [45]-ben azt is igazoltuk, hogy a 7.1. Konstrukció bizonyos nagyon speciális esetekben megegyezik egy - Hubert, Mauduit és Sárközy által - [48]-ban bevezetett konstrukcióval. Így ekkor egyszerre vannak optimális becsléseink a pszeudovéletlen mértékekre, ugyanakkor a konstrukció rendkívül gyorsan és egyszerűen implementálható.

8. Konvex és egyenes mérték

Bináris rácsok pszeudovéletlenségének vizsgálata során - talán csak a [39], [40], [41] sorozatban bevezetett normalitás, korreláció és szimmetria mértékeken kívül - leginkább a 7.1. Definícióban megadott $Q_\ell(\eta)$ pszeudovéletlen mérték használatos. Azonban csak ezeket a mértékeket alkalmazva, nem kaphatunk teljes képet a bináris rács összes pszeudovéletlen tulajdonságáról. A $Q_\ell(\eta)$ definíciójában a maximumot nagyon speciális alakú B halmazokon (téglarácsokon) vesszük. Világos, hogy itt a maximumot nem vehetjük az *összes* $B \subseteq I_N^n$ halmazon, szükség van bizonyos megkötésekre. Ugyanakkor fontos, hogy ezek a megkötések ne legyenek nagyon specifikusak. [27]-ben olyan új pszeudovéletlen mértéket vezettem be, melyben a maximumot konvex politópokon vettük, és így egy természetesen adódó új mértéket nyertünk.

8.1. Definíció. *Legyen* $\eta : I_N^n \to \{-1,+1\}$ *bináris rács. Az* η *bináris rács* **ℓ-edrendű konvex mérték***ét az*

$$X_\ell(\eta) \overset{\text{def}}{=} \max_{K,\mathbf{d_1},\dots,\mathbf{d}_\ell} \left| \sum_{\mathbf{x}\in K\cap I_N^n} \eta(\mathbf{x}+\mathbf{d_1})\dots\eta(\mathbf{x}+\mathbf{d}_\ell) \right|, \qquad (8.1)$$

képlettel definiáljuk, ahol a maximumot az összes olyan $\mathbf{d_1},\mathbf{d_2},\dots,\mathbf{d}_\ell \in I_N^n$ *különböző vektoron és* $K \subseteq [0,N-1]^n$ *konvex politópon vesszük, ahol* $K+\mathbf{d_1},\dots,K+\mathbf{d}_\ell \subseteq [0,N-1]^n$.

Nagyon valószínű, hogy az $X_\ell(\eta)$ konvex és $Q_\ell(\eta)$ pszeudovéletlen mértékek egymástól függetlenek, de ennek bizonyítása reménytelenül nehéznek tűnik. Azonban [27]-ben bevezettem egy harmadik mértéket, melynek segítségével mind a konvex mind a pszeudovéletlen mérték jól kezelhető. Ehhez szükség van a következő definícióra:

8.2. Definíció. *$L \subseteq I_N^n$* szegmens *ha L a következő alakba írható*

$$L = \{\mathbf{x} = (x_1, \dots, x_n) : \ x_1 = a_1 t + b_1, \dots, x_n = a_n t + b_n, \ t \in \{0, 1, \dots, M-1\}\},$$

ahol $M \le N$, $a_i, b_i \in \mathbb{Z}$ ($i = 1, 2, \dots, n$-re) és $(a_1, \dots, a_n) \ne (0, \dots, 0)$.

Ezután [27]-ben definiáltam az un. egyenes mértéket:

8.3. Definíció. *Legyen $I_N^n \to \{-1, +1\}$ egy bináris rács. Az η rács ℓ-***edrendű egyenes mérték***ét a következő képlettel definiáljuk:*

$$\begin{aligned} L_\ell(\eta) &\overset{\text{def}}{=} \max_{L, \mathbf{d_1}, \mathbf{d_2}, \dots, \mathbf{d}_\ell} |V(\eta, L, D)| \\ &= \max_{L, \mathbf{d_1}, \mathbf{d_2}, \dots, \mathbf{d}_\ell} \left| \sum_{\mathbf{x} \in \mathbf{L}} \eta(\mathbf{x} + \mathbf{d_1}) \dots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|, \end{aligned}$$

ahol a maximumot az összes olyan különböző $\mathbf{d_1}, \dots, \mathbf{d}_\ell \in I_N^n$ vektoron és L szegmensen vesszük, ahol $L + \mathbf{d_1}, \dots, L + \mathbf{d}_\ell \subseteq I_N^n$.

[27]-ben bebizonyítottam, hogy az $X_\ell(\eta)$, $Q_\ell(\eta)$ mértékek felülről becsülhetőek $L_\ell(\eta)$-val.

8.1. Tétel. *Minden $\eta : \ I_N^n \to \{-1, +1\}$ bináris rácsra*

$$X_\ell(\eta) \le N^{n-1} L_\ell(\eta).$$

és

$$Q_\ell(\eta) \le N^{n-1} L_\ell(\eta).$$

[27]-ben egyszerűen konstruáltam olyan bináris rácsokat, amelyekre $X_\ell(\eta)$ illetve $Q_\ell(\eta)$ optimálisan kicsi, ugyanakkor az egyenes mérték $L(\eta)$ maximális. Ezek az eredmények azt mutatják, hogy az egyenes mérték segítségével

jól tudunk kontrollálni további pszeudovéletlen mértékeket. Így a jelenleg ismert mértékek közül ez a „legszigorúbb”.

[27]-ben igazoltam, hogy majdnem minden $\eta : I_N^n \to \{-1,+1\}$ bináris rácsra $L_\ell(\eta)$ értéke $c_1 N^{1/2}$ és $c_\ell N^{1/2}(\log N)^{1/2}$ között van. Végül megadtam egy konstrukciót, amelyre az egyenes mérték optimálisan kicsi. A 8.1. Tételből adódóan ennek a bináris rácsnak a konvex és pszeudovéletlen mértékeire is nem triviális felső becslés adható.

9. 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 $N^{1/2}$ hosszúságú) kerül tényleges felhasználásra. Ezért fontos, hogy a rövid részsorozatok pszeudovéletlen mértékeit is kontrolláljuk. [31]-ben $|V(E_N,M,D)|$-re adtam nem triviális becslést. A cikk főeredménye a következő:

9.1. 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 $0 \le d_1 < d_2 < \dots < d_\ell <$*

$M + d_\ell \leq N$ teljesül, akkor

$$|V(E_N, M, D)| \ll \ell^2 N^{1/4} \log N. \tag{9.1}$$

Továbbá

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

és

$$W(E_N) \ll N^{3/4} \log N \tag{9.2}$$

is fenn áll.

(9.1)*-ból következően* $1 \leq M \leq N$*-re*

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

teljesül.

A 9.1. Tétel bizonyítása konstruktív. A bizonyításban tekintjük a p^2 elemű test feletti kvadratikus karaktert használó - Mauduit és Sárközy [56] által bevezetett - $\eta: \ I_p^2 \to \{-1, +1\}$ bináris rácsot, amely erős pszeudovéletlen tulajdonságokkal rendelkezik. Ehhez a rácshoz hozzárendelünk egy p^2 hosszú sorozatot az

$$\begin{aligned} E_{p^2} = \{&\eta(0,0), \eta(1,0), \dots, \eta(p-1,0), \eta(0,1), \eta(1,1), \dots, \eta(p-1,1), \\ &\dots, \eta(0,p-1), \eta(1,p-1), \dots, \eta(p-1,p-1)\} \end{aligned} \tag{9.3}$$

képlettel. E_{p^2} sorozatnak az első N eleme által alkotott E_N részsorozata ($p^2/4 < N \leq p^2$ esetén) eleget tesz a tétel feltételeinek. Ekkor $|V(E_N, M, D)|$ becslése $\mathbb{F}_{p^2}$-beli karakterösszegek becslésére vezetődik vissza. Ez a becslés önmagában is érdekes:

9.1. Lemma. *Legyen p páratlan prím, és jelölje γ a kvadratikus karaktert $\mathbb{F}_{p^2}$-ben. (Megjegyezzük, ekkor $\mathbb{F}_p \subset \mathbb{F}_{p^2}$.) Legyen $I = [a, a+1, a+2, \dots, b] \subseteq \mathbb{F}_p$ és $f(x) \in \mathbb{F}_{p^2}[x]$ egy olyan polinom, amely nem áll elő $cg(x)h^2(x)$ alakban,* *ahol $c \in \mathbb{F}_{p^2}$, $g(x) \in \mathbb{F}_p[x]$ és $h(x) \in \mathbb{F}_{p^2}[x]$. Tegyük fel, hogy $f(x)$-nek m darab különböző gyöke van $\mathbb{F}_p$ algebrai lezártja felett. Ekkor*

$$a) \quad \left| \sum_{x \in \mathbb{F}_p} \gamma(f(x)) \right| \leq 2mp^{1/2}, \tag{9.4}$$

$$b) \quad \left| \sum_{x \in I} \gamma(f(x)) \right| \leq 2mp^{1/2}(1 + \log p). \tag{9.5}$$

A lemma a) része speciális esete Wan [67] nagyon általános tételének. A b) részt Weil tételét [68] és egy a γ kvadratikus karakter és a Legendre szimbólum között fennálló összefüggést alkalmazva igazoltam.

10. További eredmények

10.1. Bináris sorozatok

[24], [25]-ben és PhD disszertációmban [28] kezdtem el vizsgálni egy az indexen alapuló konstrukciót és annak „gyorsított" változatát. [20]-ban a PhD disszertáció megírása után tovább élesítettem ezeket az eredményeket. Később [23] ezt a konstrukciót tovább általánosítottam. Ez utóbbi konstrukció érdekes vonása, hogy speciális esetekben elliptikus görbéken alapuló pszeudovéletlen sorozatokat ad. Ilyenkor a sorozat n-edik tagja, egy elliptikus görbe adott pontjának y koordinátájától függ.

Szintén még a PhD-m alatt oldottam meg Mauduit egy híres sejtését miszerint ha $C_2(E_N)$ nagy, akkor $C_3(E_N)$ kicsi (ezt az eredményt [30]-ban publikáltam). Az állítást valójában magasabbrendű korrelációra is igazoltam abban az esetben, amikor a páratlanrendű korreláció rendje nagyobb mint a párosrendűjé: azaz ha $2k + 1 > 2\ell$ és $C_{2k+1}(E_N)$ nagy, akkor $C_{2\ell}(E_N)$ kicsi. Később, 2011-ben Mauduittal közösen [35]-ben vizsgáltuk a $2k + 1 < 2\ell$ esetet. A következő általános eredményt igazoltuk: Ha $C_{2k+1}(E_N) \ll N^{1/2}$, akkor $C_{2k+1}(E_N)^{2\ell} C_{2\ell}(E_N)^{2k+1} \gg N^{2k+1}$, ahol az alkalmazott konstansok csak k-tól és ℓ-től függenek.

10.2. Bináris rácsok

[43]-ban Christian Mauduittal és Sárközy Andrással közösen a bináris sorozatok illetve a bináris rácsok pszeudovéletlensége közötti kapcsolatot vizsgáltuk. Ugyanis minden többdimenziós rácshoz egyértelműen hozzárendelhető egy sorozat. Dolgozatunkban megmutattuk, hogy a többdimenziós rács pszeudovéletlen mértékei nem becsülhetők felülről a kapcsolódó sorozat pszeudovéletlen mértékeivel, azaz természetes módon nem vezethető vissza a többdimenziós eset az egydimenziósra.

[36]-ban társszerzőimmel közösen három - erős pszeudovéletlen tulajdonságokkal rendelkező - egydimenziós konstrukciót terjesztettünk ki a többdimenziós esetre. Az ily módon kapott rácsoknak becsültük a pszeudovéletlen tulajdonságait.

[39], [40], [41] sorozatban társszerzőimmel közösen kétdimenziós bináris rácsok esetén vizsgáltuk a kétdimenziós pszeudovéletlen mértékek tulajdonságait. Így [39]-ben összehasonlítottuk a különböző rendű mértékeket, valamint a normalitás mértéket a Q_ℓ mértékek maximumával becsültük. [40]-ben bináris rácsok szimmetria tulajdonságait vizsgáltuk. [41]-ben bevezettük a C_ℓ mértéket a többdimenziós esetben, majd a C_ℓ, Q_ℓ értékek minimumát vizsgáltuk.

[37] és [38]-ban Mauduittal és Sárközyvel folytattuk a közös kutatómunkát. Rácsok kriptográfiai alkalmazása során nem elég, ha a bináris rácsnak erős pszeudovéletlen tulajdonságai vannak, hanem fontos az is, hogy a rácsok egy megadott nagy családjában a sorozatok „lényegesen” különbözőek legyenek. Ezt tanulmányozza az ütközés és lavina hatás. Az egydimenziós esetben pl. [4], [12], [49], [57], [64] és [65] cikkekben tanulmányozták ezeket a fogalmakat. [37]-ben általánosítottuk az ütközés és lavina hatást többdimenzióra. [38]-ban megadtunk egy olyan konstrukciót, amelyben mind az ütközés és lavina hatás mind a család bonyolultság optimális.

[42]-ben társszerzőimmel közösen a lineáris komplexitást terjesztettük ki a többdimenziós esetre.

10.3. Egyéb pszeudovéletlen objektumok

[33], [34]-ben fákon definiáltunk pszeudovéletlen függvényeket, és tanulmányoztuk az így kapott függvények pszeudovéletlen tulajdonságait.

Hivatkozások

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

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

[3] Á. Andics, *On the linear complexity of binary sequences*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 48 (2005), 173-180.

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

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

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

[7] N. Brandstätter, A. Winterhof, *Linear complexity profile of binary sequences with small correlation measure*, Periodica Math. Hungar. 52 (2006), 1-8.

[8] J. J. Brennan, B. Geist, *Analysis of iterated modular exponentiation: The orbit of x^α mod N*, Designs, Codes and Cryptography 13 (1998), 229-245.

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

[10] T. W. Cusick, *Properties of the x^2 mod N pseudorandom number generator*, IEEE Trans. Inform. Theory 41 (1995), 1155-1159.

[11] T. W. Cusick, C. Ding, A. Renvall, *Stream Ciphers and Number Theory*, Elsevier, North-Holland Publishing Co., Amsterdam 1998.

[12] 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.

[13] R. Fischlin, C. P. Schnorr, *Stronger Security proofs for RSA and Rabin bits*, Lecture Notes in Comp. Sci. 1233, Springer-Verlag, Berlin 1997, 267-279.

[14] E. Fouvry, N. Katz, *A general stratification theorem for exponential sums, and applications*, J. Reine Angew. Math. 540 (2001), 115-166.

[15] J. B. Friedlander, J. Hansen, I. Shparlinski, *Character sums with exponential functions*, Mathematika, 47 (2000), 75-85.

[16] J. B. Friedlander, I. E. Shparlinski, *On the distribution of the power generator*, Math Comp. 70 (2001), no. 236, 1575-1589.

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

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

[19] F. Griffin, I. E. Shparlinski, *On the linear complexity profile of the power generator*, IEEE Trans. Inform. Theory 46 (2000), no. 6, 2159-2162.

[20] K. Gyarmati, *A note to the paper "On a fast version of a pseudorandom generator"*, Annales Univ. Sci. Budapest. 49 (2006), 143-149.

[21] K. Gyarmati, *Concatenation of Legendre symbol sequences*, Studia Sci. Math. Hungar. 131 (2011), 346-359.

[22] K. Gyarmati, *Concatenation of pseudorandom binary sequences*, Periodica Math. Hungar. 58 (2009), 99-120.

[23] K. Gyarmati, *Elliptic curve analogues of a pseudorandom generator*, Periodica Math. Hungar., megjelenés alatt.

[24] K. Gyarmati, *On a family of pseudorandom binary sequences*, Periodica Math. Hungar. 49 (2004), 45-63.

[25] K. Gyarmati, *On a fast version of a pseudorandom generator*, Lecture Notes in Computer Science 4123, General Theory of Information Transfer and Combinatorics, Springer, Berlin / Heidelberg 2006, 326-342.

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

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

[28] K. Gyarmati, *On pseudorandom binary sequences*, PhD értekezés, Budapest 2004.

[29] K. Gyarmati, *On the complexity of a family related to the Legendre symbol*, Periodica Math. Hungar. 58 (2009), 209-215.

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

[31] K. Gyarmati, *On the correlation of subsequences*, Unif. Distrib. Theory, közlésre leadva.

[32] K. Gyarmati, *Pseudorandom sequences constructed by the power generator*, Periodica Math. Hungar. 52 (2006) 1-18.

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

[34] K. Gyarmati, P. Hubert, A. Sárközy, *Pseudorandom binary functions on rooted plane trees*, J. Combin. Number Theory, megjelenés alatt.

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

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

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

[38] K. Gyarmati, C. Mauduit, A. Sárközy, *Measures of pseudorandomness of families of binary lattices, II (A further construction.)*, Publi. Math. Debrecen, megjelenés alatt.

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

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

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

[42] K. Gyarmati, C. Maduit, A. Sárközy, *On linear complexity of binary lattices*, Ramanujan J., közlésre leadva.

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

[44] K. Gyarmati, A. Sárközy, C. L. Stewart, *On Legendre symbol lattices*, Uniform Distribution Theory 4 (2009), 81-95.

[45] K. Gyarmati, A. Sárközy, C. L. Stewart, *On Legendre symbol lattices, II*, közlésre leadva.

[46] J. Håstad, M. Näslund, *The security of individual RSA bits*, Proc 39th IEEE Symp. on Foundations of Comp. Sci., 1998, 510-519.

[47] J. Hoffstein, 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, Birkhauser Verlag, Basel, Switzerland, 2001, 59-68.

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

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

[50] D. E. Knuth, *The Art of Computer Programming*, Vol. 2, 2nd ed., Addision-Wesley, Reading Mass., 1981.

[51] J. C. Lagarias, *Pseudorandom number generators in cryptography and number theory*, Proc. Symp. in Appl. Math., Amer. Math. Soc., Providence, RI, 42 (1990), 115-143.

[52] H. Liu, *A large family of pseudorandom binary lattices*, Proc. Amer. Math. Soc. 137 (2009), 793-803.

[53] Lovász László, *Véletlen és álvéletlen*, Természetvilága 2000 II. Informatika különszám, 5-8.

[54] C. Mauduit, A. Sárközy, *Construction of pseudorandom binary lattices by using the multiplicative inverse*, Monatsh. Math. 153 (2008), 217-231.

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

[56] C. Mauduit, A. Sárközy, *On large families of pseudorandom binary lattices*, J. Uniform Distribution Theory 2 (2007), 23-37.

[57] A. Menezes, P. van Oorshot, S. A. Vanstone, *Handbook of Applied Cryptography*, CRS Press, Boca Raton, 1997.

[58] L. Mérai, *Construction of pseudorandom binary lattices based on multiplicative characters*, Periodica Math. Hungar. 59 (2009), 43-51.

[59] L. Mérai, *Construction of pseudorandom binary lattices using elliptic curves*, Proc. Amer. Math. Soc. 139 (2011), 407-420.

[60] H. Niederreiter, *Quasi-Monte Carlo methods and pseudorandom numbers*, Bull. Amer. Math. Soc. 84 (1978), 957-1041.

[61] J. Rivat, A. Sárközy, *On pseudorandom sequences and their application*, Lecture Notes in Comput. Sci. 4123, General theory of information transfer and combinatorics, Springer, Berlin / Heidelberg, 2006, 343–361.

[62] A. Sárközy, *On finite pseudorandom binary sequences and their applications in Cryptography*, Tatra Mt. Math. Publ 37 (2007), 123-136.

[63] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Boca Raton, FL, 1995.

[64] V. Tóth, *Collision and avalanche effect in families of pseudorandom binary sequences*, Periodica Math. Hungar. 55 (2007), 185-196.

[65] V. Tóth, *The study of collision and avalanche effect in a family of pseudorandom binary sequences*, Periodica Math. Hungar. 59 (2009), 1-8.

[66] I. M. Vinogradov, *Elements of Number Theory*, Dover, 1954.

[67] D. Wan, *Generators and irreducible polynomials over finite fields*, Math. Comput. 66 (219) (1997), 1195-1212.

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