Pszeudovéletlen sorozatok

Habilitációs tézisfüzet

Mérai László
ELTE IK Komputeralgebra Tanszék

2017. április 20.

Tartalomjegyzék

1. Bevezetés

Dolgozatom célja a PhD fokozat megszerzését követően, részben társszerzőkkel elért néhány eredményem tömör bemutatása. Ezek az eredmények elsősorban kriptográfiai és kommunikációs alkalmazások által motivált számelméleti problémákkal foglalkoznak. A tézisfüzet az [M1–M7] publikációkból (illetve az [M8] dolgozatból) mutat be eredményeket. Nem tartalmazza az eredmények bizonyítását, ezeket az eredeti cikkekben megtalálhatóak. Azonban törekedtem arra, hogy a dolgozat önmagában is olvasható legyen.

A jelen dolgozat a sorozatok pszeudovéletlen tulajdonságainak vizsgálatával foglalkozik. A pszeudovéletlen sorozatok olyan determinisztikus algoritmus segítségével generált számsorozatok, melyek rendelkeznek valamilyen véletlenségi tulajdonsággal. A megkívánt tulajdonság elsősorban a felhasználási területtől függ. Például kriptográfiában olyan sorozatokra van szükség, melyek elemei megjósolhatatlanok a sorozat korábbi elemei segítségével. Numerikus módszereknél (mint a Monte Carlo módszer) olyan sorozatokra van szükség, melyeknek elemei egyenletes eloszlást követnek. Végül kommunikációs rendszerek esetében olyan sorozatokra van szükség, melyeknek elemei korrelálatlanok. A megkívánt tulajdonságok a pszeudovéletlenség különböző megközelítéseihez vezettek. Az 1.2. részben néhány – az irodalomban gyakran előforduló – pszeudovéletlenségi mértéket ismertetek.

A sorozatok pszeudovéletlen tulajdonságainak vizsgálata általában két részre osztható. Egyrészről vizsgálhatjuk adott sorozat-konstrukciók pszeudovéletlen tulajdonságait, másrészről tanulmányozhatjuk a pszeudovéletlenség különböző mértékeit. Először, a 2. részben konkrét sorozatok tulajdonságaival foglalkozom. Nevezetesen az elliptikus görbék segítségével definiált sorozatok pszeudovéletlenségét vizsgálom. Ezek után, a 3. és a 4. részekben a pszeudovéletlenség újonnan bevezetett mértékeinek vizsgálatával foglalkozom.

1.1. Jelölések

Egy adott m esetén $\mathbb{Z}_m$ a modulo m maradékosztályok gyűrűjét jelöli, melyet leggyakrabban az m-nél kisebb nemnegatív egészekkel reprezentálunk, míg adott q prímhatvány esetén, a q elemű véges testet $\mathbb{F}_q$ jelöli.

Adott $f(x), g(x)$ függvények esetén, $f(x) = O(g(x))$ illetve $f(x) \ll g(x)$, ha létezik olyan $C > 0$ érték, hogy $|f(x)| \leq C \cdot g(x)$ minden x esetén. Továbbá $f(x) = o(g(x))$, ha $f(x)/g(x) \to 0$, $x \to \infty$ esetén.

1.2. Pszeudovéletlen számgenerátorok jellemzése

Egy jó pszeudovéletlen sorozatnak számos követelményt ki kell elégítenie. A lényeges tulajdonságok alkalmazási területenként változnak. Sorozatok kriptográfiai használatánál a lényeges követelményeket például Menezes, Oorschot és Vanstone [23] és Shparlinski [31] foglalja össze. Sorozatok alkalmazását numerikus módszereknél Niederreiter [27] tárgyalja. Jelen dolgozatban elsősorban sorozatok eloszlásának vizsgálatára és lineáris komplexitására koncentrálok.

A pszeudovéletlenség egyik alapvető követelménye, hogy a sorozat elemei egy adott (általában egyenletes) eloszlást kövessenek. Az egyenletes eloszlás egy kvantitatív mértéke a *diszkrepancia.*

1. definíció Az $S_N = (s_1, \ldots, s_N) \in [0,1)^N$ sorozat *diszkrepanciája*

$$\Delta(S_N) = \sup_{0 \le \alpha < \beta < 0} \left| \frac{|\{n : \alpha \le s_n < \beta\}|}{N} - (\beta - \alpha) \right|.$$

Egy jó pszeudovéletlen sorozat szükségképpen kis diszkrepanciával rendelkezik. Nevezetesen, egy S_N sorozatot egyenletes eloszlásúnak tekinthetünk, ha diszkrepanciája kicsi N függvényében, $\Delta(S_N) = o(N)$.

Egy sorozat eloszlásának (diszkrepanciájának) vizsgálatának egyik alapvető eszköze a sorozatból képzett exponenciális (additív karakter) összegek becslése. A diszkrepancia és exponenciális összegek kapcsolatát az Erdős-Turán egyenlőtlenség írja le (lásd például [28, Theorem 4.1.13]).

2. lemma (Erdős-Turán egyenlőtlenség) *Adott $H > 1$ egész esetén az S_N sorozat diszkrepanciája a következő módon becsülhető*

$$\Delta(S_N) \ll \left(\frac{1}{H} + \frac{1}{N} \sum_{h=1}^{H} \frac{1}{h} \left| \sum_{n=1}^{N} \exp\left(2\pi i h s_n\right) \right| \right).$$

Míg a diszkrepancia a sorozatok pszeudovéletlen tulajdonságait elsősorban statisztikai szempontból vizsgálja, a lineáris komplexitás a pszeudovéletlenség egy algoritmikus megközelítése. A lineáris komplexitás sorozatok kriptográfiai alkalmazásánál játszik szerepet, azok kriptográfiai biztonságának egy mérőszáma. Egy sorozat lineáris komplexitása a legkisebb lineáris visszacsatolt shift regiszter (linear feedback shift regiszter, LFSR) mérete, mely a sorozatot előállítja. Az érdeklődő olvasónak Meidl és Winterhof összefoglaló munkáját ajánlom [22].

3. definíció Legyen $S = (s_n)$ egy $\mathcal{R}$ gyűrű elemeiből képzett sorozat. A sorozat *N-edik lineáris komplexitása* $L(S, N)$ egy legrövidebb lineáris rekurzió hossza, mely generálja a sorozatot, azaz a legkisebb olyan L érték, melyre léteznek olyan $c_0, c_0, \ldots, c_{L-1} \in \mathcal{R}$ elemek, hogy

$$s_{n+L} = c_{L-1} s_{n+L-1} + \cdots + c_0 s_n, \quad n = 0, 1, \ldots, N - L - 1.$$

Ha $s_0 = s_1 = \cdots = s_{L-1} = 0$, akkor az N-edik lineáris komplexitás értékét 0-nak definiáljuk, $L(S, N) = 0$, míg ha $s_0 = s_1 = \cdots = s_{N-2} = 0$, $s_{N-1} \neq 0$ akkor az N-edik lineáris komplexitás értékét N-nek definiáljuk, $L(S, N) = N$.

Egy sorozat *lineáris komplexitása* $L(S)$, az N-edik lineáris komplexitások szuprémuma

$$L(S) = \sup_{N \ge 1} L(S, N).$$

Az N-edik lineáris komplexitás N-ben korlátos, $0 \leq L(S,N) \leq N$, továbbá $L(S,N) \leq L(S,N+1)$. Véletlen (tipikus) sorozatok N-edik lineáris komplexitását Niederreiter vizsgálta [26]. Megmutatta, hogy véletlen bináris, $\mathbb{F}_2$ fölött értelmezett sorozatok esetében az N-edik lineáris komplexitás $N/2$ körül koncentrálódik,

$$L(S,N) = \frac{N}{2} + O(\log N), \quad N \geq 2. \tag{1}$$

Megjegyzem, hogy az N-edik lineáris komplexitás hatékonyan kiszámolható a Berlekamp-Massey algoritmus segítségével [20].

Könnyen látható, hogy egy sorozat lineáris komplexitása pontosan akkor véges, ha a sorozat egy küszöbindextől kezdve periodikus. Ilyen sorozatok esetében elsősorban a sorozat lineáris komplexitását, ellenkező esetben az N-edik lineáris komplexitások sorozatát (linear complexity profile) vizsgáljuk.

Niederreiter [26] eredménye alapján azt mondhatjuk, hogy a pszeudovéletlenség egyik szükséges feltétele a nagy N-edik lineáris komplexitás. Azonban könnyen látható, hogy ez nem elégséges feltétel. A 3. részben a lineáris komplexitás egy finomítását mutatom be, mellyel sorozatok pszeudovéletlen tulajdonságai érzékenyebben vizsgálhatóak.

2. Pszeudovéletlen pontsorozatok elliptikus görbéken

Ebben a fejezetben különböző, elliptikus görbék segítségével definiált sorozatok pszeudovéletlen tulajdonságait vizsgálom. Az elliptikus görbék részletes tárgyalása Silverman [33] könyvében található.

Legyen E egy nem szinguláris elliptikus görbe $\mathbb{F}_q$ felett, melyet az

$$E: \; y^2 + (a_1 x + a_3) y = x^3 + a_2 x^2 + a_4 x + a_6, \quad a_1, \ldots, a_6 \in \mathbb{F}_q$$

egyenlet definiál.

A görbe pontjai Abel csoportot alkotnak a $\oplus$ műveletre nézve, ahol a nullelem a görbe ideális egyenesen levő pontja, melyre a ∞ jelölést használom. Az $\mathbb{F}_q$-racionális $E(\mathbb{F}_q)$ pontok számát a Hasse-Weil tétel becsüli

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2q^{1/2}.$$

Legyen $\mathbb{F}_q(E)$ az E függvényteste $\mathbb{F}_q$ fölött. Legyenek $x, y \in \mathbb{F}_q(E)$ a koordinátafüggvények, speciálisan adott $P \in E$, $P \neq \infty$ esetén $P = (x(P), y(P))$. A görbe divizorai a görbe pontjaiból képzett véges formális összegek, egy divizor foka a divizor együtthatóinak összege

$$\deg\left(\sum_{P \in E(\overline{\mathbb{F}_q})} n_P [P]\right) = \sum_{P \in E(\overline{\mathbb{F}_q})} n_P \in \mathbb{Z}.$$

Egy $f \in \mathbb{F}_q(E)$ függvény divizorára az (f) jelölést használjuk,

$$(f) = \sum_{P \in E(\overline{\mathbb{F}_q})} \mathrm{ord}_P(f)[P],$$

ahol $\mathrm{ord}_P(f)$ az f rendje a P pontban. (Speciálisan $\mathrm{ord}_P(f) > 0$, ha P gyöke, míg $\mathrm{ord}_P(f) < 0$, ha P pólusa f-nek.) Az $f \in \mathbb{F}_q(E)$ függvény $(f)_\infty$ pólus- és $(f)_0$ gyök-divizora az

$$(f)_\infty = \sum_{\substack{P \in E(\overline{\mathbb{F}_q}) \\ \mathrm{ord}_P(f) < 0}} (-\mathrm{ord}_P(f))[P] \qquad (f)_0 = \sum_{\substack{P \in E(\overline{\mathbb{F}_q}) \\ \mathrm{ord}_P(f) > 0}} \mathrm{ord}_P(f)[P],$$

speciálisan $(f) = (f)_0 - (f)_\infty$. Legyen végül $\deg f$ az f pólus-divizorának foka. Például $\deg(x) = 2$ és $\deg(y) = 3$.

Elliptikus görbék használatát jó pszeudovéletlen tulajdonságokkal rendelkező sorozatok generálásához először Hallgren javasolta [12]. Munkája nyomán több, elliptikus görbék segítségével definiált sorozatot vizsgáltak. A témában Shparlinski [32] és Lange, Lubicz és Weigl [7, Chapter 30] írt összefoglaló munkát.

Az egyik tipikus és praktikus módja pontsorozatok generálásához görbéken, ha a sorozatot rekurzív módon definiáljuk. Azaz egy kezdeti $P_0 \in E(\mathbb{F}_q)$ pont és egy $\rho : E(\mathbb{F}_q) \to E(\mathbb{F}_q)$ leképzés esetén definiáljuk a (P_n) sorozatot a

$$P_n = \rho(P_{n-1}), \quad n \geq 1 \tag{2}$$

rekurzióval. Mivel a ρ leképzés egy véges halmazon hat, a (P_n) sorozat egy adott küszöbindextől kezdve periodikus.

A ρ leképzés különböző választásával ismert sorozat-konstrukciókat kapunk. Például, ha a ρ leképzés egy $G \in E$ ponttal való eltolás, $\rho(P) = P \oplus G$, a (2) rekurzió a *lineáris kongruencia generátort* definiálja elliptikus görbéken. Ezen generátor pszeudovéletlen tulajdonságait a 2.1. részben tárgyalom. Ha ρ egy skalárral való szorzás, $\rho(P) = eP$ egy adott e egésszel, a (2) rekurzió a *hatványgenerátort* definiálja elliptikus görbéken. Ezen generátorral kapcsolatos eredményeimet a 2.2. részben tárgyalom.

Megjegyzem, hogy a (2) konstrukció olyan általánosságban is vizsgálható, mikor ρ egy tetszőleges *morfizmus*, azaz egy olyan $\rho : E \to E$ leképezés, mely racionális törtfüggvényekkel reprezentálható. Megmutatható [33, Example 4.7], hogy ekkor ρ egy affin leképzés, azaz létezik olyan $\vartheta : E \to E$ endomorfizmus és olyan G pont, hogy $\rho(P) = \vartheta(P) \oplus G$. A (2) konstrukció ilyen általánosságban is vizsgáltam, lásd például [25].

A (P_n) sorozat pszeudovéletlen tulajdonságainak vizsgálatának egy természetes módja, hogy a sorozat pontjainak komponenseit vizsgáljuk, azaz például az $(x(P_n))$, $\mathbb{F}_q$ fölötti sorozatot. Ennek a megközelítésnek a hátránya, hogy az így elért eredmények érzékenyek a koordinátatranszformációkra. Ez abból a szempontból nem szerencsés, hogy gyakorlati alkalmazásoknál gyakran nem a Weierstrasse koordinátákat használják, hanem más, jóval hatékonyabb reprezentációt, például Montgomery vagy Edwards koordinátákat, lásd [7,

Chapter 13] és [35, Section 2.6]. Ennek érdekében realisztikusabb az $(f(P_n))$ sorozatok vizsgálata tetszőleges $f \in \mathbb{F}_q(E)$ függvény esetén. Ennek a megközelítésnek a másik előnye, hogy nem egy konkrét sorozat pszeudovéletlen tulajdonságait tudjuk vizsgálni, hanem sorozatok egy nagy családjáét.

A fejezetben a $(f(P_n))$ sorozatok eloszlását és lineáris komplexitását fogom vizsgálni.

2.1. Lineáris kongruencia generátor elliptikus görbéken

Legyen E egy elliptikus görbe és definiáljuk a (P_n) pontsorozatot a (2) rekurzió segítségével, ahol $\rho(P) = P \oplus Q$ adott $Q \in E$ ponttal. Ekkor a rekurzió a *linear kongruencia generátort* definiálja elliptikus görbéken. Ebben az esetben a pont-sorozat elemeire a

$$P_n = nG \oplus P_0, \quad n = 0, 1, \ldots \tag{3}$$

explicit képlet adható. A generátort először Hallgren [12] javasolta. Pszeudovéletlen tulajdonságait többen vizsgálták, lásd például [1, 5, 6, 9, 13, 15, 19, 24]. Világos, hogy a (3) sorozat periodikus, ahol a periódus ℓ hossza a G elem rendje.

Kohel és Shparlinski [15], illetve Beelen és Doumen [1] megmutatta, hogy

$$\sum_{P \in \mathcal{H}} \psi(f(nP)) \ll \deg f q^{1/2}, \tag{4}$$

ahol $\mathcal{H}$ egy tetszőleges részcsoportja $E(\mathbb{F}_q)$-nak, ψ az $\mathbb{F}_q$ egy (nem-triviális) additív karaktere, $f \in \mathbb{F}_q(E)$ pedig egy tetszőleges függvény, melyre $f \neq z^p - z$ $(z \in \overline{\mathbb{F}_q(E)})$.

A (4) becslés segítségével az $f(nG \oplus P_0)$ sorozat diszkrepanciája is becsülhető. Alkalmazva a korlátot az $\bar{f}_{P_0}(P) = f(P \oplus P_0)$ függvényre, a 2. lemma felhasználásával közvetlenül adódik, hogy $(f(nG \oplus P_0))$ sorozat diszkrepanciája kicsi, ha G rendje elég nagy és $f \neq z^p - z$ $(z \in \overline{\mathbb{F}_q(E)})$.

A (3) sorozat N-edik lineáris komplexitását Hess és Shparlinski [13] vizsgálta először bizonyos típusú f függvények esetében.

Legyen H egy olyan d-ed fokú divizora a görbének, mely megfelel egy $H_0 \in E(\overline{\mathbb{F}_q})$ pont Galois-orbitjának. Legyen $f \in \mathbb{F}_q(E)$ egy olyan függvény, melynek $(f)_\infty$ pólus-divizora

$$(f)_\infty = (1 + \delta)H \tag{5}$$

ahol

$$\delta = \begin{cases} 1, & \text{ha } d = 1, \\ 0, & \text{ha } d \geq 2. \end{cases}$$

Ekkor megmutatták, hogy

$$L(f(nG), N) \geq \min \left\{ \frac{N}{(1+\delta)d + 2}, \frac{\ell}{(1+\delta)d + 1} \right\}, \quad N \geq 1,$$

ahol ℓ a G rendje.

Tipikus példa függvényre, mely teljesíti a (5) feltételt az x koordinátafüggvény ($H = [\infty]$ és $d = 1$ választással). Ugyanakkor a (5) feltétel nagyon megszorító. Például az y koordinátafüggvény nem elégíti ki ($(y)_\infty = 3[\infty]$).

Winterhoffal közösen [M2] egy olyan megközelítést dolgoztunk ki, mely az f függvények egy jóval nagyobb osztálya esetén ad becslést az $(f(nG))$ sorozat N-edik lineáris komplexitására. A módszer lényege, hogy az elliptikus görbéket nem Weierstrasse hanem Edwards koordináták segítségével reprezentáljuk.

Elliptikus görbék Edwards koordinátáit Edwards vezette be 2007-ben, majd később Brenstein és Lange [4] dolgozta ki. Előnyük a Weierstrasse koordinátákkal szemben, hogy egységes módon lehet a csoportműveletet definiálni (azaz nincs külön formula összegzésre és pont-kétszerezésre) és a görbepontok jóval gyorsabb számolását engedi meg. Ezen tulajdonságok népszerűvé teszik kriptográfiai alkalmazásokban.

Legyen $\mathbb{F}_q$ egy páratlan karakterisztikájú test. A C Edwards görbét az

$$u^2 + v^2 = c^2(1 + du^2v^2)$$

egyenlet definiálja, ahol $c, d \in \mathbb{F}_q$, $d \neq 0, 1$, $c \neq 0$. Ha d nem négyzet $\mathbb{F}_q$-ban, akkor pontok összegét a

$$(u_1, v_1) \oplus (u_2, v_2) = \left(\frac{u_1v_2 + u_2v_1}{c(1 + du_1u_2v_1v_2)}, \frac{v_1v_2 - u_1u_2}{c(1 - du_1u_2v_1v_2)} \right)$$

képlettel definiálhatjuk. A görbe pontja a fenti összeadással Abel csoportot alkotnak, ahol a $(0, c)$ a nullelem.

Minden Edwards görbe izomorf egy elliptikus görbével. Másrészről, ha $E(\mathbb{F}_q)$-nak pontosan két negyed és egy másod rendű pontja van, akkor E izomorf egy Edwards görbével $c = 1$ választással. Nevezetesen, ha $c = 1$, akkor C izomorf az

$$E : y^2 = x^3 + 2(1 + d)x^2 + (1 - d)^2x \tag{6}$$

elliptikus görbével, az

$$\begin{array}{rccl} \psi: & E(\mathbb{F}_q) \setminus \{\infty, (0,0)\} & \to & C \setminus \{(0,1), (0,-1)\} \\ & (x, y) & \mapsto & \left\{ \begin{array}{l} u = 2\frac{x}{y} \\ v = \frac{x-1+d}{x+1-d}. \end{array} \right. \end{array} \tag{7}$$

$\psi(\infty) = (0, 1)$, $\psi((0, 0)) = (0, -1)$ izomorfizmussal.

Ha d nem négyzet $\mathbb{F}_q$-ban, akkor az Edwards görbe minden $\mathbb{F}_q$-racionális pontja affin. A görbe két ideális pontja, Ω_1 és Ω_2, a test kvadratikus bővítése felett van definiálva.

2.1. tétel (vö. [M2, Theorem 1]) *Legyen $\mathbb{F}_q$ egy páratlan karakterisztikájú véges test, legyen $d \in \mathbb{F}_q$ egy nem négyzet elem és legyen C a (6) egyenlettel definiált Edwards görbe. Legyen $f \in \mathbb{F}_q(C)$ egy olyan függvény, hogy Ω_1 vagy Ω_2 pólusa f-nek és legyen $G \in C$ egy ℓ-ed rendű pont. Ekkor*

$$L(f(nG), N) \geq \min \left\{ \frac{N - \deg f}{4 \deg f + 1}, \frac{\ell - \deg f}{4 \deg f} \right\}, \quad N \geq \deg f.$$

1. példa Tekintsük az $f(u,v) = (2-2d)\frac{1+v}{u(1-v)} \in \mathbb{F}_q(C)$ függvényt. Ennek pólus-divizora

$$(f)_\infty = (1+v)_\infty + (u)_0 + (1-v)_0. \tag{8}$$

Megmutatható, hogy Ω_1 és Ω_2 gyökei u-nak, de se nem gyökei se nem pólusai az $1 \pm v$ függvényeknek. Így a 2.1. tétel alkalmazható. A (8) alapján $\deg f = 6$, így

$$L(f(nG), N) \geq \min\left\{\frac{N-6}{25}, \frac{\ell-6}{24}\right\}, \quad N \geq 6.$$

Megjegyzem, hogy a (7) izomorfizmus alapján $f(P) = y(\psi^{-1}(P))$, azaz ily módon a lineáris kongruencia generátor y-koordinátájának N-edik lineáris komplexitása szintén becsülhető.

A lineáris kongruencia generátor erős pszeudovéletlen tulajdonságokkal rendelkezik mind az eloszlás (diszkrepancia), mind a lineáris komplexitás szempontjából. Mindazonáltal biztonsági vizsgálatok az mutatják, hogy kriptográfiai alkalmazásai kerülendők. Az [M4] dolgozatban megmutattam, hogy a (3) lineáris kongruencia generátor koordinátái polinomiális időben kiszámolhatóak egy viszonylag rövid kezdeti sorozat ismeretében.

Legyen az E görbe az $\mathbb{F}_p$ prímtest felett definiálva ($p > 3$) és legyen (x_n) a (3) sorozat x koordinátáiból alkotott sorozat,

$$x_n = x(nG \oplus P_0) \quad n = 0, 1 \ldots. \tag{9}$$

Tegyük fel, hogy az (x_n) sorozat néhány kezdeti $x_1, \ldots, x_s$ eleme ismert (mint nemnegatív egészek). Ekkor kérdezhetjük, hogy kiszámolhatóak-e a lineáris kongruencia generátor valamely paraméterei (úgy mint a p prímszám, a görbe egyenlete, a G illetve a P_0 pontok).

A feladat ilyen általánosságban nem mindig oldható meg. Például, ha a görbe a racionális számtest felett van definiálva, ahol az $x(nG \oplus P_0)$ $(n = 1, \ldots, s)$ koordináták mind egészek, akkor a p prímek egy végtelen sorozatát lehet adni, hogy a megfelelő, $\mathbb{F}_p$ fölött definiált, sorozat megegyezzen az eredeti sorozattal. Ezért célunk nem egy adott prímszám, hanem a lehetséges prímek egy listájának megkeresése. Ebben az esetben megmutattam, hogy 7 elem segítségével a sorozat minden paramétere kiszámolható ($\log p$-ben) polinomiális időben.

A tétel könnyebb kimondásához azonosítsuk $\mathbb{Z}_0$-t a racionális számtesttel, $\mathbb{Z}_0 = \mathbb{Q}$.

2.2. tétel (vö. [M4, Theorem 1]) *Létezik egy algoritmus mely a következő feltételeket elégíti ki. Legyenek $x_1, \ldots, x_7 \in \mathbb{F}_p$ a (9) képlettel definiált elemek és tegyük fel, hogy $iG \oplus P_0 \neq \infty$ $(i = 0, 1, \ldots, 7)$. Ekkor az algoritmus kiszámol egy olyan $m \geq 0$ egészt és egy olyan $\widetilde{x}_n \in \mathbb{Z}_m$ elemet, hogy $p \mid m$ és $\widetilde{x}_n \equiv x_n \mod p$ ha $nG \oplus P_0 \neq \infty$. Az algoritmus $\log p$ -ben polinomiális, n-ben lineáris.*

A tételben szereplő algoritmus pszeudokódját az 1. algoritmus írja le (lásd Függelék). Ez olyan m és $\widetilde{x}, \widetilde{(y^2)}, \widetilde{A}, \widetilde{B} \in \mathbb{Z}_m$ értékeket számol ki, melyekre

$$\widetilde{x}_n = 2\frac{\widetilde{x}_{n-1}^3 + \widetilde{A}\widetilde{x}_{n-1} + \widetilde{B} + \widetilde{(y_G^2)}}{(\widetilde{x}_{n-1} - \widetilde{x_G})^2} - 2(\widetilde{x}_{n-1} + \widetilde{x_G}) - \widetilde{x}_{n-2}, \quad n = 2, 3, \ldots, \tag{10}$$

és $\widetilde{x}_n \equiv x_n \mod p$.

Az ismert értékek számának növelésével az algoritmus hatékonysága növelhető oly módon, hogy p értékét közelítő m egész értékére kisebb pozitív számot ad meg. Véletlen minták tesztelése során az algoritmus 7 sorozatelemből az esetek 95,2%-ban számolta ki a helyes p értéket (a maradék esetben egy összetett m számot adott, melyre $p \mid m$), míg 8 sorozatelemből az esetek 100%-ban számolta ki a helyes p értéket.

2.2. Hatványgenerátor elliptikus görbéken

A 2.2. tétel szerint a lineáris kongruencia generátor nem megfelelő választás kriptográfiai alkalmazásokhoz, annak ellenére, hogy erős pszeudovéletlen tulajdonságokkal rendelkezik. Kriptográfiai alkalmazásokhoz egy alkalmas jelölt az úgynevezett hatványgenerátor, melyet a (2) definiál a $\rho(P) = eP$ ($e \in \mathbb{Z}$) választással, azaz ahol a pontsorozatot a

$$P_n = eP_{n-1} = e^n P, \quad n = 1, 2, \ldots \tag{11}$$

definiálja adott $P_0 = P$ ponttal.

A hatványgenerátorokat eredetileg maradékosztálygyűrűkben definiálták. Nevezetesen, legyenek ϑ, m, e olyan egészek, hogy $\mathrm{lnko}(\vartheta, m) = 1$. Ekkor definiáljuk az (u_n) sorozatot a

$$u_n \equiv u_{n-1}^e \mod m, \quad 0 \leq u_n < m, \quad n = 1, 2, \ldots$$

rekurzióval és az $u_0 = \vartheta$ kezdőértékkel.

Az általános konstrukció két speciális esete (mindkét esetben az m egy úgynevezett RSA modulus, azaz $m = p \cdot q$ különböző p, q prímekkel) az RSA generátor, ahol $\mathrm{lnko}(e, \varphi(m)) = 1$, illetve a Blum-Blum-Shub generátor, ahol $e = 2$ (lásd [23]).

A generátor elliptikus görbés változatát Lange és Shparlinski definiálta [16]. Vizsgálták a (11) sorozat koordinátáinak eloszlását és lineáris komplexitását. Legyen ℓ a P elem rendje és legyen e olyan egész, melyre $\mathrm{lnko}(e, \ell) = 1$. Ekkor a (11) sorozat periodikus, és a periódus T hossza az e multiplikatív rendje modulo ℓ.

Legyen E egy nem szuperszinguláris elliptikus görbe $\mathbb{F}_p$ fölött. Ekkor Lange és Shparlinski [16] megmutatta például, hogy

$$\sum_{n=1}^{T} \exp\left(\frac{x\left(e^n P\right)}{p}\right) \ll T^{1/6} \ell^{2/3} p^{1/12}. \tag{12}$$

Az eredmény az Erdős-Turán tétel segítségével (2. lemma) megmutatja, hogy az $(x(e^n P)/p)$ sorozat koordinátáinak diszkrepanciája kicsi.

$$\Delta\left(\frac{x(e^n P)}{p}\right) \ll T^{1/6} \ell^{2/3} p^{1/12} \log p.$$

Lange és Shparlinski [16] vizsgálta továbbá az $(x(e^n P))$ sorozat lineáris komplexitását. Megmutatták, hogy

$$L(x(e^n P)) \gg T \ell^{-2/3}.$$

Az [M1, M2] dolgozatokban vizsgáltam (részben társszerzőkkel) a fenti problémákat az $(f(e^nP))$ sorozatok esetében, ahol $f \in \mathbb{F}_q(E)$. Először megmutattam, hogy a sorozatból képzett karakterösszeg kicsi.

2.3. tétel (vö. [M1, Theorem 4]) *Legyen E egy $\mathbb{F}_p$ felett definiált nem szuperszinguláris elliptikus görbe, $P \in E$ egy ℓ-ed rendű pont. Legyen $f \in \mathbb{F}_p(E)$ egy nem konstans függvény és ψ az $\mathbb{F}_p$ egy nem-triviális additív karaktere. Ekkor minden $1 \le N \le T$ egészre és adott $\varepsilon > 0$ esetén*

$$\sum_{n=1}^{N} \psi\left(f\left(e^nP\right)\right) \ll \deg f N^{1/3} \ell^{5/9} p^{1/18+\varepsilon}.$$

Megjegyzem, hogy a tétel eredménye a (12) becslésnél kissé gyengébb. Ennek oka, hogy a tétel nem teljes karakterösszegre ad becslést míg a (12) csak teljes karakterösszegre vonatkozik.

Az eredmény az Erdős-Turán tétel segítségével (2. lemma) korlátot ad az $(f(e^nP)/p)$ sorozat diszkrepanciájára.

4. következmény (vö. [M1, Corollary 6]) *A 2.3. tétel feltételeivel*

$$\Delta\left(\frac{f(e^nP)}{p}\right) \ll \deg f N^{1/3} \ell^{5/9} p^{1/18+\varepsilon} \log p.$$

Winterhoffal közösen vizsgáltuk az $(f(e^nP))$ sorozat lineáris komplexitását.

2.4. tétel (vö. [M2, Theorem 2]) *Legyen E egy $\mathbb{F}_q$ felett definiált nem szuperszinguláris elliptikus görbe, $P \in E$ egy ℓ-ed rendű pont. Legyen $f \in \mathbb{F}_p(E)$ egy nem konstans függvény melyre* $\deg f < \ell^\delta$ *valamely $\delta < 1$ számra. Ha az e multiplikatív rendje T modulo ℓ, akkor*

$$L(f(e^nP)) \gg \frac{T}{\ell^{2/3}(\deg f)^{1/3}}.$$

2.3. Frobenius generátor

Az eddig tárgyalt generátorok mind a (10) generátor speciális esetei voltak, mindegyik egy klasszikus, maradékosztályokon definiált generátor elliptikus görbés változata. Ebben a részben egy olyan generátort tárgyalok melyet egy merőben más típusú konstrukció definiál, és kihasználja az elliptikus görbék, maradékosztályokhoz képest vett extra struktúráját.

Egy adott k egész esetén legyen $\mathcal{M}_k$ az olyan 0, ± 1 vektorok halmaza, mely nem tartalmaz két nem-nulla szomszédos koordinátát

$$\mathcal{M}_k = \{(\mu_0, \dots, \mu_{k-1}) \in \{0, \pm 1\}^k \mid \mu_j \mu_{j+1} = 0\}.$$

Ismert, lásd [2], hogy

$$\#\mathcal{M}_k = \frac{4}{3} 2^k + O(1).$$

Továbbá nem nehéz megmutatni, hogy minden n egész felírható

$$n = \sum_{j=0}^{k-1} \mu_j 2^j, \quad (\mu_0, \ldots, \mu_{k-1}) \in \mathcal{M}_k \tag{13}$$

alakban valamely $k = \log n + O(1)$ esetén. Egészeknek ezen reprezentációjának előnye, hogy elliptikus görbék pontjainak skalárral való szorzását meggyorsítja a hagyományos bináris ábrázoláshoz képest.

Legyen E_a az

$$y^2 + xy = x^3 + ax^2 + 1 \quad a \in \mathbb{F}_2 \tag{14}$$

$\mathbb{F}_2$ fölött definiált Kobiltz görbe [14], és legyen σ az E_a görbe *Frobenius automorfizmusa*, mely adott $P \in E_a$, $P \neq \infty$ pont esetén

$$P = (x, y) \overset{\sigma}{\mapsto} (x^2, y^2),$$

illetve $\sigma(\infty) = \infty$.

Legyen $r \geq k$ egész és rögzítsünk egy $P \in E_a(\mathbb{F}_{2^r})$ pontot. Ekkor a *Frobenius generátor* egy olyan $(P_{\mathbf{n}})$ pontsorozatot definiál, ahol az $\mathbf{n} \in \mathcal{M}_k$ vektorok *lexikografikusan* vannak rendezve, és

$$P_{\mathbf{n}} = \sum_{j=0}^{k-1} \mu_j \sigma^j(P), \quad \mathbf{n} = (\mu_0, \ldots, \mu_{k-1}) \in \mathcal{M}_k \tag{15}$$

(ahol a szummajel az elliptikus görbén definiált pontösszeadásra utal).

Megjegyzem, hogy ha a σ automorfizmust a kettővel való szorzásra cseréljük, $\delta(P) = 2P$, akkor a (15) összefüggés lényegében a lineáris kongruencia generátort definiálja, $P_{\mathbf{n}} = nP$, ahol $\mathbf{n}$ az n (13) reprezentációja. A (15) konstrukció előnye, hogy jóval hatékonyabb a lineáris kongruencia generátornál: a $P_{\mathbf{n}}$ pont kiszámolásához nem kell pontok kétszeresét kiszámolni, csak a Frobenius automorfizmust kell végrehajtani, illetve pontok ellentettjét kell kiszámolni, mely műveletek az alaptestben hatékonyan végrehajthatók.

A sorozatot Lange és Shparlinski vezette be [17], akik vizsgálták az ütközések számát a $(P_{\mathbf{n}})$ sorozatban. Később [18] korlátot adtak a

$$\sum_{\mathbf{n} \in \mathcal{M}_k} \psi(x(P_{\mathbf{n}}))$$

karakterösszegre adott ψ nem-triviális additív karakter esetén.

Mind a [17] mind a [18] dolgozat a $(P_{\mathbf{n}})$ pontjait mint *pontrendszer* vizsgálja, azaz nem veszi figyelembe a pontok rendezését. Az [M7] dolgozatban a $(P_{\mathbf{n}})$ *sorozat* pszeudovéletlen tulajdonságait vizsgáltam. Először vizsgáltam az egymást követő pontok *együttes* eloszlását.

Legyen $s \geq 2$ egy adott egész. Tekintsük a lexikografikus rendezést az $\mathcal{M}_k$ halmazon, és legyen $\mathcal{M}_k^*$ az $\mathcal{M}_k$ azon (legbővebb) részhalmaza, mely nem tartalmazza $\mathcal{M}_k$ utolsó

$s-1$ elemét. Legyen továbbá τ az a függvény, mely adott $\mathbf{n} \in \mathcal{M}_k^*$ vektorhoz, a vektort lexikografikusan követő elemet rendeli. Ekkor szeretnénk vizsgálni a

$$(P_{\mathbf{n}}, P_{\tau(\mathbf{n})}, \dots, P_{\tau^{s-1}(\mathbf{n})}) \in E(\mathbb{F}_{2^r})^s \tag{16}$$

s-es eloszlását.

2.5. tétel (vö. [M7, Theorem 2]) *Legyen E_a a (14) által definiált görbe, legyen $P \in E_a(\mathbb{F}_{2^r})$ egy ℓ-ed rendű pont és ψ az $\mathbb{F}_{2^r}$ egy nem-triviális additív karaktere. Ekkor tetszőleges $k \geq 1$ és $s \geq 2$ egészekre és bármely $(a_0, \dots, a_{s-1}) \neq (0, \dots, 0)$ vektorra*

$$\sum_{\mathbf{n} \in \mathcal{M}_k^*} \chi\left(\sum_{i=0}^{s-1} a_i x\left(P_{\sigma,\tau^i(\mathbf{n})}\right)\right) \ll \#\mathcal{M}_k \, s \left(q^{1/4\nu} \ell^{-1/2\nu} + 2^{-k/2\nu} q^{(\nu+1)/4\nu^2}\right)$$

teljesül bármely

$$\nu > \frac{r \log 2}{\min\{2k, 2(\log \ell - 3)\}}$$

egészre.

A fenti eredmény lényegében az mutatja, hogy a sorozat szomszédos pontjainak x komponensei lényegében statisztikailag függetlenek.

Legyen $\beta_1, \dots, \beta_r$ az $\mathbb{F}_{2^r}$ egy bázisa $\mathbb{F}_2$ fölött és adott $u \in \mathbb{F}_{2^r}$ elemet ábrázoljunk az $u = u_1\beta_1 + \dots + u_r\beta_r$ alakban. Adott $J \subset \{1, \dots, r\}$ részhalmaz és $c_{i,j} \in \mathbb{F}_2$, $i \in \{0, 1, \dots, s-1\}$, $j \in J$ elemek esetén legyen

$$N\big(J, (c_{i,j})\big) = \left|\left\{\mathbf{n} \in \mathcal{M}_k : \; x\left(P_{\sigma,\tau^i(\mathbf{n})}\right)_j = c_{i,j}, i \in \{0, 1 \dots, s-1\}, j \in J\right\}\right|.$$

Ekkor, a 2.5. tétel alapján becsülhető $N\big(J, (c_{i,j})\big)$ diszkrepanciája.

5. következmény (vö. [M7, Corollary 1]) *A 2.5. tétel feltételei mellett*

$$\max_{J, (c_{i,j})} \left|N\big(J, (c_{i,j})\big) - \frac{\#\mathcal{M}_k}{p^{\#J \cdot s}}\right| \ll \#\mathcal{M}_k \, s \left(q^{1/4\nu} \ell^{-1/2\nu} + 2^{-k/2\nu} q^{(\nu+1)/4\nu^2}\right)$$

teljesül bármely

$$\nu > \frac{r \log 2}{\min\{2k, 2(\log \ell - 3)\}}$$

egészre

Az $\ell = q^{1+o(1)}$ és $k = \lfloor \log q \rfloor$ esetén a $\nu = 2$ választással a következmény szerint a (16) komponensei egyenletes eloszlást követnek minden $|\mathcal{J}| \leq \alpha n$ koordinátában.

A szomszédos pontok együttes eloszlása mellett vizsgáltam a sorozat lineáris komplexitását.

2.6. tétel (vö. [M7, Theorem 1]) *Legyen E_a a (14) által definiált görbe, legyen $P \in E_a(\mathbb{F}_{2^r})$ egy ℓ prímrendű pont. Ekkor*

$$L(x\left(P_{\sigma,\mathbf{n}}\right)) \gg \min\left\{\#\mathcal{M}_{\lceil k/2 \rceil}, \ell\right\}.$$

Megjegyzem, hogy a fenti eredmény megválaszolja Shparlinski egy kérdését [32, Question 31.].

3. Sorozatok algebrai komplexitása

A lineáris komplexitás sorozatok kriptográfiai alkalmazhatóságának egy mérőszáma. Ha egy sorozatnak kicsi a lineáris komplexitása, akkor a sorozatelemek könnyen kiszámolhatóak egy aránylag rövid kezdőszeletből, így kriptográfiai alkalmazásuk kerülendő. Természetesen sorozatok optimális lineáris komplexitása csak szükséges, de nem elégséges feltétele a kriptográfiai biztonságnak. Diem [8] 2012-ben bevezette a pszeudovéletlenség egy új mérőszámát (algebrai komplexitás, expansion complexity), mely a lineáris komplexitásnál erősebb mérték. Ebben a részben ezen új mértékkel kapcsolatos eredményeimet foglalom össze.

Xing és Lam [34] 1999-ben olyan végtelen (nem periodikus) sorozatokat vezettek be, melyek optimális lineáris komplexitással rendelkeznek, a sorozat N-edik lineáris komplexitása az $N/2$ ideális értéktől (lásd (1)) csak korlátos mértékben tér el. Legyen $h(x,y) \in \mathbb{F}_q[x,y]$ egy irreducibilis polinom. Ennek segítségével hatékonyan kiszámolható egy olyan $S = (s_n)_{n=0}^{\infty}$ sorozat, melyre $L(S,N) = N/2 + O(1)$ (ahol a konstans függ a $h(x,y)$ polinomtól). A sorozat elemei lényegében az $y \in \mathbb{F}_q[x,y]/(h(x,y))$ elem formális hatványsorának eggyüthatói,

$$h(x, G(x)) = 0, \quad \text{ahol } G(x) = \sum_{i=0}^{\infty} s_i x^i. \tag{17}$$

Annak ellenére, hogy a sorozat N-edik lineáris komplexitásai nagyok, a sorozat elemei egy aránylag kis kezdőszeletből hatékonyan kiszámolható. Diem [8] megmutatta, hogy $(\deg h(x,y))^2$ kezdeti elem ismeretéből egyértelműen kiszámolható a $h(x,y)$ polinom, és így maga az S sorozat is.

A támadás alapján Diem a pszeudovéletlenség következő mértékét vezette be:

6. definíció Legyen $S = (s_n)_{n=0}^{\infty}$ egy $\mathbb{F}_q$-beli sorozat. A

$$G(x) = \sum_{i=0}^{\infty} s_i x^i$$

formális hatványsort az S sorozat generátorfüggvényének hívjuk. Adott pozitív N esetén az N-edik $E(S,N)$ algebrai komplexitás értéke 0, ha $s_0 = \cdots = s_{N-1} = 0$, egyébként értéke a legkisseb olyan d, melyre létezik d-ed fokú $h(x,y) \in \mathbb{F}_q[x,y]$ polinom, melyre

$$h(x, G(x)) \equiv 0 \mod x^N.$$

Legyen továbbá $E(S) = \sup_{N \geq 1} E(S,N)$ az S sorozat algebrai komplexitása.

Niederreiterrel és Winterhoffal [M3] illetve Gomez-Perezzel és Niederreiterrel [M8] vizsgáltuk az újjonan bevezetett mérték tulajdonságait.

A definícióból azonnal adódik a

$$0 \leq E(S,N) < N$$

triviális korlát. Megmutattuk, hogy ez lényegesen javítható.

3.7. tétel (vö. [M8, Theorem 1]) *Adott S sorozat és N pozitív egész esetén*

$$\binom{E(S,N)+1}{2} \leq N.$$

A tétel alapján kapjuk az $E(S,N) \leq \sqrt{2N}$ erősebb korlátot.

Az algebrai komplexitás tekinthető a lineáris komplexitás erősítésének. Ha a 6. definícióban csak olyan $h(x,y)$ polinomokat tekintünk, melyek legfeljebb elsőfokúak az y változóban, a lineáris komplexitás fogalmát kapjuk vissza. Az [M3] dolgozatban vizsgáltuk a sorozatok lineáris és algebrai komplexitásának kapcsolatát.

A mértékek kapcsolatát először olyan sorozatok esetében vizsgáltuk melyek periodikusak egy küszöbindextől kezdve.

3.8. tétel (vö. [M3, Theorem 1]) *Legyen $S = (s_n)_{n=0}^{\infty}$ egy olyan nem-nulla sorozat, mely a t küszöbindextől kezdve periodikus. Ekkor*

$$E(S,N) \geq \begin{cases} L(S) - t + 1 & \text{ha } N > (L(S)-t)(L - \min\{1, t-1\}), \\ \lceil N/(L(S) - \min\{1,t-1\}) \rceil & \text{egyébként,} \end{cases}$$

továbbá

$$E(S,N) \leq L(S) + \max\{-1, -t+1\}.$$

Az eredmény azt mutatja, hogy periodikus sorozatok esetén az algebrai és lineáris komplexitás közel van egymáshoz.

Vizsgáltuk a tétel lokális változatát is, azaz amikor az $L(S)$ lineáris komplexitás nem véges.

3.9. tétel (vö. [M3, Theorem 3]) *Legyen S egy $\mathbb{F}_q$ fölötti sorozat és $N \geq 2$ egy adott egész. Tegyük fel hogy S generátorfüggvényére*

$$G(x) \not\equiv 0 \mod x^N$$

továbbá legyen

$$\sum_{\ell=t_N}^{L(S,N)-1} c_\ell s_{i+\ell} = s_{i+L(S,N)}, \quad 0 \leq i < N - L(S,N)$$

egy legrövidebb lineáris rekurzió az első N elemre, ahol $c_{t_N} \neq 0$. Ekkor

$$E(S,N) \geq \begin{cases} L(S,N) - t_N + 1 & \text{ha } N > (L(S,N)-t_N)(L(S,N) - \min\{1, t_N - 1\}), \\ \lceil \frac{N}{(L(S,N) - \min\{1,t_N-1\})} \rceil & \text{egyébként,} \end{cases}$$

továbbá

$$E(S,N) \leq L(S,N) + \max\{-1, -t_N + 1\}.$$

Mind a 3.7. tétel, mind a 3.8. és a 3.9. tételek azt sugallják, hogy egy S sorozat akkor optimális az algebrai komplexitás szempontjából, ha $E(S,N)$ értéke közel $\sqrt{2N}$. Az [M8] dolgozatban ilyen sorozatra mutattunk példát.

3.10. tétel (vö. [M8, Theorem 4]) *Legyen p egy prímszám, és definiáljuk a $B = (b_n)_{n=0}^{\infty}$ p szerinti periodikus sorozatot a*

$$b_n \equiv n^{p-2} \mod p, \quad 0 \leq b_n < p$$

összefüggéssel. Ekkor $2 \leq N < p$ esetén

$$E(B, N) = d \quad \textit{mikor} \binom{d+1}{2} \leq N < \binom{d+2}{2}.$$

Ezzel az új komplexitás fogalommal hatékonyan azonosíthatóak kriptográfiailag gyenge sorozatok. Azonban Diem definiciója nem túl szerencsés, az nem modellezi hatékonyan a támadást a (17) sorozat ellen. A támadáshoz ugyanis szükséges feltétel, hogy a 6. definícióban szereplő $h(x, y)$ polinom *irreducibilis* legyen. Gomez-Perezzel és Niederreiterrel [M8] vizsgáltuk az algebrai komplexitás ezen változatát.

7. definíció Legyen $S = (s_n)_{n=0}^{\infty}$ egy $\mathbb{F}_q$-beli sorozat. Adott pozitív N esetén legyen $E^*(S, N) = 0$ ha $s_0 = \cdots = s_{N-1} = 0$, egyébként értéke a legkisebb olyan d, melyre létezik d-ed fokú irreducibilis $h(x, y) \in \mathbb{F}_q[x, y]$ polinom, melyre

$$h(x, G(x)) \equiv 0 \mod x^N.$$

Legyen továbbá $E^*(S) = \sup_{N \geq 1} E^*(S, N)$.

A definícióból azonnal következik az

$$E(S, N) \leq E^*(S, N) \leq \max\{1, N - 1\}$$

egyenlőtlenség. Azonban a 3.7. tétellel ellentétben, $E^*(S, N)$ értéke lehet nagy. Ha S egy olyan sorozat, melynek $G(x)$ generátorfüggvényére $G(x) \equiv x^{N-1} \mod x^N$, megmutatható, hogy $E^*(S, N) = N - 1$. Ennél azonban több is mondható. Megmutattuk, hogy a 3.7. tétel korlátja tipikusan nem teljesül ebben az esetben. Ehhez legyen μ az egyenletes valószínűségi mérték $\mathbb{F}_q$-n. Legyen $\mathbb{F}_q^{\infty}$ az $\mathbb{F}_q$ fölötti végtelen sorozatok halmaza és legyen μ^{∞} a μ által definiált teljes szorzat mérték az $\mathbb{F}_q^{\infty}$ halmazon.

3.11. tétel (vö. [M8, Theorem 2]) *μ^{∞}-majdnem mindenütt teljesül a*

$$\liminf_{N \to \infty} \frac{E^*(S, N)}{\sqrt{2N}} \geq 1$$

egyenlőtlenség.

A tétel alsó korlátot ad az $E^*(S, N)$ tipikus értékeire. Azonban sejtésünk, hogy ez felső korlát is (esetleg konstans szorzotól eltekintve).

Ahogy korábban megjegyezetem, $E^*(S, N)$ egy szigorúan erősebb mérték mint $E(S, N)$. Azonban olyan sorozatok esetében, melyek N-edik algebrai komplexitása optimális, azaz közel $\sqrt{2N}$, az $E^*(S, N)$ értéke szintén közel van az általunk sejtett tipikus $\sqrt{2N}$ értékhez.

3.12. tétel (vö. [M8, Theorem 3]) *Adott S sorozat és minden $d \geq 1$ esetén ha*

$$E(B,N) = d \quad \textit{mikor} \binom{d+1}{2} \leq N < \binom{d+2}{2},$$

akkor

$$E^*(B,N) = d' \quad \textit{mikor} \binom{d'+1}{2} + 2 \leq N < \binom{d'+2}{2}.$$

Megjegyzem, hogy a 3.10. és a 3.12. tételek alapján a $B = (b_n)_{n=0}^{\infty}$ sorozat $E^*(B,N)$ komplexitása a 3.11. tétel által sejtetett értékkel aszimptotikusan megegyezik.

4. Bináris sorozatcsaládok kereszt-korrelációja

Véges bináris sorozatok pszeudovéletlen tulajdonságainak vizsgálatára Mauduit és Sárközy [21] egy újfajta megközelítést dolgozott ki. Bevezettek több a pszeudovéletlenség különböző szükséges feltételeit vizsgáló mértéket. Megközelítésük előnye, hogy mértékei erősek, azaz ha egy sorozat jó pszeudovéletlen tulajdonságokkal rendelkezik a mértékek szempontjából, további klasszikus pszeudovéletlenségi teszteket is kielégít [3, 29]. A különböző pszeudovéletlen mértékekről Gyarmati [10] írt összefoglaló munkát.

Bináris sorozatok mellett sorozat *családok* pszeudovéletlen tulajdonságainak vizsgálatára is több lehetséges mértéket vezettek be az irodalomban, lásd Sárközy [30] összefoglaló munkáját. Például Gyarmati, Mauduit és Sárközy [11] bevezette az úgynevezett kereszt-korrelációs (cross-correlation) mértéket.

8. definíció Legyen $\mathcal{F}$ az N hosszú bináris sorozatok egy családja,

$$\mathcal{F} = (E_N^{(1)}, \ldots, E_N^{(|\mathcal{F}|)}): \quad E_N^{(i)} = (e_1^{(i)}, \ldots, e_N^{(i)}) \in \mathbb{F}_2^N, \quad 1 \leq i \leq |\mathcal{F}|. \tag{18}$$

Ekkor az $\mathcal{F}$ család *k-ad rendű kereszt-korrelációs mértékét* a

$$\Phi_k(\mathcal{F}) = \max \left| \sum_{n=1}^{M} (-1)^{e_{n+d_1}^{(i_1)} + \cdots + e_{n+d_k}^{(i_k)}} \right|$$

képlettel definiáljuk, ahol a maximum olyan M, $0 \leq d_1 \leq \ldots \leq d_k \leq N - M$ és $1 \leq i_1 \leq \cdots \leq i_k \leq |\mathcal{F}|$ egészeken fut melyekre $d_r \neq d_s$ ha $i_r = i_s$.

Az egyelemű $\mathcal{F} = (E_N)$ családra a mérték megegyezik az úgynevezett korrelációs mértékkel. Nagyobb családok esetén a mérték azt vizsgálja, hogy a család elemeinek különböző eltoltjai között mekkora korreláció mérhető. Nagy, optimális kereszt-korrelációval rendelkező sorozatok a kriptográfia mellett a vezeték nélküli kommunikációban játszanak szerepet (például a Code division muliple access - CDMA technológiában). Az [M5, M6] dolgozatokban a Φ_k mértéket vizsgáltam.

Akkor mondható egy sorozat-családról, hogy erős pszeudovéletlen tulajdonságokkal rendelkezik a kereszt-korreláció szempontjából, ha mértéke közel van a véletlen családok mértékéhez, legalábbis kis k esetén. Az [M5] dolgozatban vizsgáltam a Φ_k mértéket véletlen családok esetén. Ehhez legyen $\mathcal{F}$ egy véletlen család, azaz adott $|\mathcal{F}|$ méret esetén legyen $\mathcal{F}$ a (18) által definiált család ahol az $e_n^{(i)}$ $(1 \le n \le N,\ 1 \le i \le |\mathcal{F}|)$ független egyenletes eloszlású $0-1$ valószínűségi változók. A $\Phi_k(\mathcal{F})$ mérték nagyban függ a család méretétől. Ha $|\mathcal{F}| = 2^N$ (azaz a család tartalmazza az összes N hosszú sorozatot), nem lehet nemtriviális eredményt bizonyítani. Hasonló az eset, ha az $\mathcal{F}$ család túl nagy: ha $|\mathcal{F}| > 2^{cN}$ valamely $0 < c < 1/2$ esetén, akkor $\Phi_k(\mathcal{F}) \gg N$ (c választható $c = 0,18$-nak, lásd [11]). Megmutattam azonban, hogy ha $|\mathcal{F}| < 2^{c'N}$, $c' = 1/12 = 0,0833\ldots$, a kereszt-korrelációs mérték uralható.

4.13. tétel (vö. [M5, Theorem 2]) *Adott $\varepsilon > 0$ esetén létezik olyan N_0, hogy $N > N_0$ és $1 \le \log_2 |\mathcal{F}| < N/12$ esetén*

$$\frac{2}{5}\sqrt{N\left(\log\binom{N}{k} + k\log|\mathcal{F}|\right)} < \Phi_k(\mathcal{F}) < \frac{5}{2}\sqrt{N\left(\log\binom{N}{k} + k\log|\mathcal{F}|\right)}$$

teljesül legalább $1-\varepsilon$ valószínűséggel minden $2 \le k \le N/(6\log_2|\mathcal{F}|)$ esetén.

A 4.13. tétel értelmében egy $\mathcal{F}$ család jó pszeudovéletlen tulajdonságokkal rendelkezik, ha $\Phi_k(\mathcal{F}) \ll \sqrt{N\log|\mathcal{F}|}\,(\log N)^{O(1)}$, legalábbis kis k esetén. Ilyen családra Gyarmati, Mauduit és Sárközy mutatott példát [11] a Legendre szimbólum segítségével. Adott páratlan p prím esetén az $\left(\frac{a}{p}\right)$ Legendre szimbólum értéke $+1$, ha a kvadratikus maradék, -1, ha a kvadratikus nemmaradék.

2. példa Legyen p egy páratlan prím, $d < p$ egy egész és tekintsük az

$$f(x) = x^d + a_2x^{d-2} + a_3x^{d-3} + \cdots + a_d \in \mathbb{F}_p[x]$$

(azaz az x^{d-1} együtthatója 0) irreducibilis polinomok F halmazát. Legyen $\mathcal{F} = (E_p(f) : f \in F)$, ahol

$$e_n^{(f)} = \begin{cases} 1, & \text{ha } \left(\frac{f(n)}{p}\right) = 1, \\ 0 & \text{ha } \left(\frac{f(n)}{p}\right) = -1. \end{cases}$$

Ekkor

$$\Phi_k(\mathcal{F}) \ll kdp^{1/2}\log p$$

minden $1 < k < p$ esetén, továbbá ha $d < p^{1/2}/(20\log p)$, akkor

$$|\mathcal{F}| \ge p^{\lfloor d/3\rfloor - 1}.$$

A 4.13. tétel szerint a Φ_k mérték véletlen családokra egy érték körül koncentrálódik. Ha a mérték rendje nem túl nagy, ez a megfigyelés explicitté tehető.

4.14. tétel (vö. [M6, Theorem 2]) *Adott $\varepsilon > 0$ és $k(N)$ egész értékű függvény esetén, ha $2 \le k \le (\log N + \log|\mathcal{F}|)/\log\log N$, akkor létezik olyan $N_0 \le \log_2|\mathcal{F}|$ küszöbindex, hogy $N \ge N_0$ esetén*

$$1 - \varepsilon < \frac{\Phi_k(\mathcal{F})}{\mathbb{E}[\Phi_k(\mathcal{F})]} < 1 + \varepsilon$$

teljesül legalább $1 - \varepsilon$ valószínűséggel.

Végül, ha mind a mérték k rendje, mind a család $|\mathcal{F}|$ mérete fix, megmutatható, hogy $\Phi_k(\mathcal{F})$ rendelkezik határeloszlással. Megjegyzem, hogy a 4.14. tétel értelmében ez a határeloszlás csak elfajult eloszlás lehet.

4.15. tétel (vö. [M6, Theorem 4]) *Legyen $\mathcal{F}$ az N hosszú sorozatok egy fix méretű véletlen családja. Ekkor*

$$\frac{\Phi_k(\mathcal{F})}{\sqrt{2N\log\binom{N}{k-1}}} \to 1 \quad \textit{majdnem mindenütt,}$$

ha $N \to \infty$.

A 4.13. tétel értelmében egy $\mathcal{F}$ család jó pszeudovéletlen tulajdonságokkal rendelkezik, ha mértéke $\Phi_k(\mathcal{F})$ kicsi. Azonban a tétel tipikus családok mértékére nem csak felső, hanem alsó korlátot is ad. Felmerül a kérdés, hogy az alsó korlát mennyire megszorító, azaz milyen kicsi lehet a Φ_k mérték.

Az [M6] dolgozatban megmutattam, hogy ha a mérték rendje páros, a tipikus és minimum értéke a mértéknek közel azonos.

4.16. tétel (vö. [M6, Theorem 6]) *Minden N és k pozitív egész és minden $\mathcal{F}$ család esetén ha $2kN \le |\mathcal{F}|$, akkor*

$$\Phi_{2k}(\mathcal{F}) \ge \sqrt{\frac{1}{50}N\log\lfloor|\mathcal{F}|/k\rfloor \Big/ \log\frac{50N}{\log\lfloor|\mathcal{F}|/k\rfloor}}$$

míg $2kN > |\mathcal{F}|$ esetén

$$\Phi_{2k}(\mathcal{F}) \ge \sqrt{\frac{N}{2\lceil k/|\mathcal{F}|\rceil + 1}}.$$

Ha a mérték rendje páratlan, akkor a mérték értéke lehet triviális. Például az egyetlen $E_N = (0,1,0,1,\dots)$ sorozatot tartalmazó család mértéke $\Phi_{2k+1}(E_N) = 1$. Megmutattam, hogy nagyobb családok esetén a mérték minimum értéke logaritmikus a család méretében.

4.17. tétel (vö. [M6, Theorem 5]) *Minden N és k pozitív egész esetén*

$$\lfloor\log_2|\mathcal{F}| - \log_2(2k+1)\rfloor \le \min\{\Phi_{2k+1}(\mathcal{F})\} \le \lceil\log_2|\mathcal{F}|\rceil,$$

ahol a minimum az $|\mathcal{F}|$ méretű családokon fut.

Megjegyzem, hogy a tétel megoldja Gyarmati, Mauduit és Sárközy egy problémáját [11, Problem 1].

5. Függelék

1. algoritmus A 2.2. tételben szereplő algoritmus pszeudokódja.

Bemenet: $x_1, \dots, x_7$ a (9) által generált nemnegativ egészek

Kimenet: $\left(\widetilde{x}, \widetilde{(y^2)}, \widetilde{A}, \widetilde{B}, m\right)$ hogy $p \mid m$, és ha $\widetilde{x}_n$ $(n = 2, 3, \dots)$ kielégíti (9), akkor $\widetilde{x}_n \equiv x_n \mod p$ feltéve $P_n \neq \infty$.

legyenek $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4, \mathbf{u} \in \mathbb{Q}^5$ a következő vektorok

$$(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4) = \begin{pmatrix} 2x_2^2 + 2x_2(x_1+x_3) & 2x_2 - (x_1+x_3) & 2x_2 & 2 \\ 2x_3^2 + 2x_3(x_2+x_4) & 2x_3 - (x_2+x_4) & 2x_3 & 2 \\ 2x_4^2 + 2x_4(x_3+x_5) & 2x_4 - (x_3+x_5) & 2x_4 & 2 \\ 2x_5^2 + 2x_5(x_4+x_6) & 2x_5 - (x_4+x_6) & 2x_5 & 2 \\ 2x_6^2 + 2x_6(x_5+x_7) & 2x_6 - (x_5+x_7) & 2x_6 & 2 \end{pmatrix}$$

és

$$\mathbf{u} = ((x_1+x_3)x_2^2, (x_2+x_4)x_3^2, (x_3+x_5)x_4^2, (x_4+x_6)x_5^2, (x_5+x_7)x_6^2)^T$$

$m \leftarrow \det(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4, \mathbf{u})$.
ha $m = 0$
    legyen $\lambda_1\mathbf{c}_1 + \lambda_2\mathbf{c}_2 + \lambda_3\mathbf{c}_3 + \lambda_4\mathbf{c}_4 = \mu\mathbf{u}$ ahol $\lambda_1, \dots, \lambda_4, \mu \in \mathbb{Z}$, $\mu > 0$
    $m \leftarrow (\lambda_1^2 - \lambda_2\mu)/\gcd(\lambda_1^2, \mu)$
    ha $m = 0$
        $\widetilde{x} \leftarrow \frac{\lambda_1}{\mu}$, $\widetilde{(y^2)} \leftarrow \left(\frac{\lambda_1}{\mu}\right)^3 + \frac{\lambda_4}{2\mu} + \frac{\lambda_1\lambda_3}{2\mu^2}$,$\widetilde{A} \leftarrow \frac{\lambda_3}{\mu}$, $\widetilde{B} \leftarrow \frac{\lambda_4}{2\mu} - \frac{\lambda_1\lambda_3}{2\mu^2}$
    elágazás vége
elágazás vége
ha $m \neq 0$
    amíg $\mathbf{c}_1$, $\mathbf{c}_2$, $\mathbf{c}_3$, $\mathbf{c}_4$ lineárisan összefüggőek modulo m
        legyen $\lambda_1\mathbf{c}_1 + \lambda_2\mathbf{c}_2 + \lambda_3\mathbf{c}_3 + \lambda_4\mathbf{c}_4 \equiv 0 \mod m$ ahol $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) \neq (0,0,0,0)$,
        $m \leftarrow \gcd(m, \lambda_1, \lambda_2, \lambda_4, \lambda_5)$
    ciklus vége
    legyen $\lambda_1\mathbf{c}_1 + \lambda_2\mathbf{c}_2 + \lambda_3\mathbf{c}_3 + \lambda_4\mathbf{c}_4 \equiv \mu\mathbf{u} \mod m$ ahol $\mu > 0$
    ha $\gcd(m, \mu) > 0$
        $m \leftarrow m/\gcd(m, \mu)$
    elágazás vége
    legyen $\lambda_1\mathbf{c}_1 + \lambda_2\mathbf{c}_2 + \lambda_3\mathbf{c}_3 + \lambda_4\mathbf{c}_4 \equiv \mathbf{u} \mod m$
    ha $\lambda_1^2 \not\equiv \lambda_2 \mod m$
        $m \leftarrow \gcd(m, \lambda_1^2 - \lambda_2)$
    elágazás vége
    $\widetilde{x} \leftarrow \lambda_1 \bmod m$, $\widetilde{(y^2)} \leftarrow \lambda_1^3 + \frac{\lambda_4 + \lambda_1\lambda_3}{2} \bmod m$, $\widetilde{A} \leftarrow \lambda_3 \bmod m$,
    $\widetilde{B} \leftarrow \frac{\lambda_4 - \lambda_1\lambda_3}{2} \bmod m$
elágazás vége
visszatérési érték $\left(\widetilde{x}, \widetilde{(y^2)}, \widetilde{A}, \widetilde{B}, m\right)$

Az értekezés alapját képező publikációk

[M1] L. Mérai, On the elliptic curve power generator, Unif. Distrib. Theory, 9 (2014), no. 2, 59–65.

[M2] L. Mérai, A. Winterhof, On the linear complexity profile of some sequences derived from elliptic curves, Des. Codes Cryptogr., (2015) doi: 10.1007/s10623-015-0140-0

[M3] L. Mérai, H. Niederreiter, A. Winterhof, Expansion complexity and linear complexity of sequences over finite fields, Cryptogr. Commun. (2016) doi: 10.1007/s12095-016-0189-2

[M4] L. Mérai, Predicting the elliptic curve congruential generator, Appl. Algebra Eng. Commun. Comput. (2016) doi: 10.1007/s00200-016-0303-x

[M5] L. Mérai, On the typical values of the cross-correlation measure, Monatsh. Math. 180 (2016) no. 1, 83-99 doi: 10.1007/s00605-016-0886-0

[M6] L. Mérai, The cross-correlation measure of families of finite binary sequences: limiting distributions and minimal values, Discrete Appl. Math. (2016) doi: 10.1016/j.dam.2016.06.024

[M7] L. Mérai, On pseudorandom properties of certain sequences of points on elliptic curve, Lecture Notes in Comput. Sci., 10064, Springer, Berlin, 2017, 54–63 , doi: 10.1007/978-3-319-55227-9_4

[M8] D. Gómez-Pérez, L. Mérai, H. Niederreiter, On the expansion complexity of sequences over finite fields, elbírálás alatt, arXiv: 1702.05329.

Hivatkozások

[1] P. H. T. Beelen, J. M. Doumen, Pseudorandom sequences from elliptic curves, Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), 37–52, Springer, Berlin, 2002.

[2] W. Bosma, Signed bits and fast exponentiation. 21st Journées Arithmétiques (Rome, 2001). J. Théor. Nombres Bordeaux 13 no. 1, 27–41 (2001)

[3] N. Brandstätter, A. Winterhof, Linear complexity profile of binary sequences with small correlation measure. Period. Math. Hungar. 52 (2006), no. 2, 1–8.

[4] D. J. Bernstein, T. Lange, Faster addition and doubling on elliptic curves. Advances in Cryptology–ASIACRYPT 2007, 29–50, Lecture Notes in Comput. Sci. **4833**, Springer, Berlin, 2007.

[5] Z. Chen, Elliptic curve analogue of Legendre sequences, Monatsh. Math. 154 (2008), 1–10.

[6] Z. Chen, D. Gomez-Perez, G Pirsic, On lattice profile of the elliptic curve linear congruential generators. Period. Math. Hungar. 68 (2014), no. 1, 1–12.

[7] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren, Handbook of elliptic and hyperelliptic curve cryptography, Chapman & Hall/CRC, Boca Raton, FL, 2006.

[8] C. Diem, On the use of expansion series for stream ciphers, LMS J. Comput. Math. 15 (2012) 326–340.

[9] E. El Mahassni, I. Shparlinski, On the uniformity of distribution of congruential generators over elliptic curves. Sequences and their applications (Bergen, 2001), 257–264, Discrete Math. Theor. Comput. Sci. (Lond.), Springer, London, 2002.

[10] K. Gyarmati, Measures of pseudorandomness, P. Charpin, A. Pott, A. Winterhof (eds.), Radon Series in Computational and Applied Mathematics, de Gruyter 2013, 43-64.

[11] K. Gyarmati, C. Mauduit, A. Sárközy, The cross-correlation measure for families of binary sequences, Applied algebra and number theory, 126–143, Cambridge Univ. Press, Cambridge, 2014.

[12] S. Hallgren, Linear congruential generators over elliptic curves, Preprint CS-94-143 , Dept. of Comp. Sci., Cornegie Mellon Univ., 1994, 1–10.

[13] F. Hess, I. E. Shparlinski, On the linear complexity and multidimensional distribution of congruential generators over elliptic curves. Des. Codes Cryptogr. 35 (2005), 111–117.

[14] N. Koblitz, CM-curves with good cryptographic properties. In: Advances in cryptology–CRYPTO '91 (Santa Barbara, CA, 1991), 279–287, LNCS, vol 576, Springer, Berlin (1992)

[15] D. Kohel, I. E. Shparlinski, Exponential sums and group generators for elliptic curves over finite fields, Proc. Algorithmic Number Theory Symposium, Leiden, 2000, LNCS 1838, Berlin: Springer-Verlag, 395–404.

[16] T. Lange, I. E. Shparlinski, Certain exponential sums and random walks on elliptic curves. Canad. J. Math. 57 (2005), 338–350.

[17] T. Lange, I. E. Shparlinski, Collisions in fast generation of ideal classes and points on hyperelliptic and elliptic curves. Appl. Algebra in Engin., Commun. and Computing 15, 329–337 (2005)

[18] T. Lange, I. E. Shparlinski, Distribution of some sequences of points on elliptic curves. J. Math. Cryptol. 1 no. 1, 1–11 (2007)

[19] H. Liu, A family of elliptic curve pseudorandom binary sequences. Des. Codes Cryptogr. 73 (2014), no. 1, 251–265.

[20] J. L. Massey, Shift-register synthesis and BCH decoding. IEEE Trans. Information Theory IT-15 1969 122–127.

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

[22] W. Meidl, A. Winterhof, Linear complexity of sequences and multisequences, in: G. Mullen, D. Panario (eds.), Handbook of Finite Fields: Chapman & Hall, (2013) 324–336.

[23] A. J. Menezes, P. C. Oorschot, S. A. Vanstone, Handbook of applied cryptography, CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997

[24] L. Mérai, Construction of pseudorandom binary sequences over elliptic curves using multiplicative characters. Publ. Math. Debrecen 80 (2012), no. 1-2, 199–213.

[25] L. Mérai, On the elliptic curve endomorphism generator, elbírálás alatt.

[26] H. Niederreiter, The probabilistic theory of linear complexity. Advances in cryptology–EUROCRYPT '88 (Davos, 1988), 191–209, Lecture Notes in Comput. Sci., 330, Springer, Berlin, 1988.

[27] H. Niederreiter, Random number generation and quasi-Monte Carlo methods. CBMS-NSF Regional Conference Series in Applied Mathematics, 63. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992.

[28] H. Niederreiter, A. Winterhof, Applied number theory. Springer, Cham, 2015.

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

[30] A. Sárközy, On pseudorandomness of families of binary sequences, Discrete Appl. Math., 216 (2017) no. 3, 670–676.

[31] I. E. Shparlinski, Cryptographic applications of analytic number theory, Birkhauser, 2003.

[32] I. E. Shparlinski, Pseudorandom number generators from elliptic curves, Recent trends in cryptography, 121–141, Contemp. Math., 477, Amer. Math. Soc., Providence, RI, 2009.

[33] J. H. Silverman, The arithmetic of elliptic curves, Springer-Verlag, Berlin, 1995.

[34] C. P. Xing, K.Y. Lam, Sequences with almost perfect linear complexity profiles and curves over finite fields, IEEE Trans. Inform. Theory 45 (1999), no. 4, 1267–1270.

[35] L. C. Washington, Elliptic Curves: Number Theory and Cryptography, 2nd edition. Chapman & Hall/CRC Press, 2008.