SZÉKFOGLALÓ ELŐADÁSOK A MAGYAR TUDOMÁNYOS AKADÉMIÁN

Sárközy András

VÉGES PSZEUDOVÉLETLEN BINÁRIS SOROZATOKRÓL

Tekintetes Nagy gy[...]

[...] szabályainak 32-ka így szól:
[...]fennálló szabályainak 32-ka így szól:
[...] újonnan választott tag, a külsők kivétele-
[...]ztályába tartozó dolgozat felolvasásával,
[...]emélyes megnem jelenhetés esetén beküldé-
[...]legfelebb egy év alatt székét foglal; különben meg-
[...]ztására megsem misítőén."

Lehetnek esetek, melyekben kiválóbb vidéken la-
[...]gátoltatnak a határidőt megtartani: de hallga-
[...]elnézni e szabály meg nem tartatását, annyi[...]
[...], mint összes szabályzatunkat erőtlennek tekinteni
[...]következményeire figyelmessé tenni a T. Akadem[...]
[...]szükségtelen.

Inditványba hozatik tehát, hogy egyelőre az
[...]61. 1862 választott s székfoglalás által meg nem erő-
[...]tett rendes tagok nevei a névkönyvből kitöröltessenek, az 1861-
[...]63-ig választottak a szabályokra emlékeztessenek, jö-
[...]vőre pedig a titoknoki hivatal oda utasíttassék, hogy
[...] evidentiában tartás végett az újdon választottakat,
[...] még széket nem foglaltak, a sorozatba fel ne vegye."

853/1865

[...], jan. 26. 1865.

B. Kemény Zsigmond
Kőrösi? László
[...] Mór
[...] János
[...] Szalay?
Hollán Ernő
Törökh? Lőrincz? r. tag
Toldy Ferencz r. tag
Gyulay? Arnold?

Sárközy András

VÉGES PSZEUDOVÉLETLEN BINÁRIS SOROZATOKRÓL

SZÉKFOGLALÓK
A MAGYAR TUDOMÁNYOS AKADÉMIÁN

A 2004. május 3-án megválasztott
akadémikusok székfoglalói

Sárközy András

VÉGES PSZEUDOVÉLETLEN BINÁRIS SOROZATOKRÓL

Magyar Tudományos Akadémia • 2014

Az előadás elhangzott 2004. szeptember 15-én

Sorozatszerkesztő: Bertók Krisztina

Olvasószerkesztő: Laczkó Krisztina

Borító és tipográfia: Auri Grafika

ISSN 1419-8959

ISBN 978-963-508-749-5

Kiadja a Magyar Tudományos Akadémia
Kiadásért felel: Lovász László, az MTA elnöke
Felelős szerkesztő: Kindert Judit
Nyomdai munkálatok: Kódex Könyvgyártó Kft.

Bevezetés

A véges pszeudovéletlen bináris sorozatoknak számos alkalmazása van. Legfontosabbak a kriptográfiai alkalmazások, amelyek főként az úgynevezett *Vernam titkosításhoz* („Vernam cipher") kapcsolódnak. Ennek leírása:

1. Először a titkosítandó szöveget konvertáljuk egy $A_N = (a_1, \ldots, a_N)$, $a_i \in \{0, 1\}$ bitsorozattá; ez az ún. *nyílt szöveg* („plaintext").

2. Tekintsünk egy $E_N = (e_1, \ldots, e_N)$, $e_i \in \{0, 1\}$ véletlen bináris sorozatot, amelyet *kulcsfolyamnak* („keystream") hívunk. Megjegyzendő, hogy a „folyam" szó a kulcsfolyam, *folyamtitkosírás* („streamchipher") összetételben arra utal, hogy a titkosírást folyamatosan, bitenként végezzük, ellentétben a *blokktitkosírásokkal* („blockchipher"), ahol a biteket nem egyenként, hanem blokkban összefogva konvertáljuk.

3. Alkalmazzuk azt a φ *titkosítási transzformációt*, amely a következőképpen van definiálva: az A_N nyílt szöveg képe a $\varphi(A_N) = F_N = (f_1, \ldots, f_N)$ *titkosított szöveg* („chipertext"), amelynek az i-edik bitjét az $f_i = a_i \bigoplus e_i$ operációval kapjuk. Itt $\bigoplus$ az úgynevezett XOR függvényt jelöli, amely modulo 2 összeadást jelent, tehát $f_i \equiv a_i + e_i \pmod 2$, $f_i \in \{0, 1\}$.

4. Az *elolvasási transzformáció* szintén φ, tehát az A_N nyílt szöveghez a φ transzformáció újabb alkalmazása révén tudunk eljutni: $A_N = \varphi(F_N) = \varphi(\varphi(A_N))$.

		nyílt szöveg:	$(0, 1, 1, 0, 0, \ldots, 1)$	titkosítás
	$\oplus$	kulcsfolyam:	$(1, 1, 0, 0, 1, \ldots, 1)$	
PÉLDA:		titkosított szöveg:	$(1, 0, 1, 0, 1, \ldots, 0)$	elolvasás
	$\oplus$	kulcsfolyam:	$(1, 1, 0, 0, 1, \ldots, 1)$	
		nyílt szöveg:	$(0, 1, 1, 0, 0, \ldots, 1)$	

Idézem (és a továbbiakban is ismételten fogom idézni) A. Menezes, P. van Oorshot és S. Vanstone „Handbook of Applied Cryptography" [49] című kitűnő könyvét: „Ha a kulcsfolyamot alkotó bitek függetlenül és véletlenül vannak generálva, akkor a Vernam titkosírást *egyszer használatos kódnak* („one time pad") hívjuk, és az minden *feltétel nélkül biztonságos* („unconditionally secure") minden, csak titkosított szöveget használó támadás ellenében." Következik Shannon elméletéből, hogy az egyszer használatos kód *feltétel nélkül* biztonságos a nyílt szöveg statisztikai eloszlásától függetlenül, és optimális abban az értelemben, hogy annak kulcsa a legrövidebb az összes olyan szimmetrikus kulcsú titkosítási rendszeré közül, amelyek rendelkeznek ezzel a tulajdonsággal.

Az egyszer használatos kódot széles körben használták a második világháborúban és a hidegháború idején. Az egyszer használatos kód kulcsát alkotó biteket rendszerint egy fizikára épülő készülékkel (például diódával) állítják elő, ennek a készüléknek két lehetséges kimenete van, amelyek (remélhetőleg) egyenlő valószínűséggel fordulnak elő, és (remélhetőleg) véletlen módon váltakoznak. Ám „[a] véletlenség természetes forrásaira épülő véletlen bit generátorokat külső tényezők is befolyásolhatják, és meg is hibásodhatnak. Ezért feltétlenül szükséges ezeknek az eszközöknek a rendszeres tesztelése a . . . §-ban felsorolt statisztikai tesztek [„(frequency test)", „(serial test)", „(poker test)", „(runs test)", „(autocorrelation test)"] révén". Az ilyen típusú tesztelést Knuth [35] *„a posteriori tesztelésnek"* hívja.

„Az egyszer használatos kódnak nyilvánvaló gyengéje, hogy a kulcsnak ugyanolyan hosszúnak kell lennie, mint a nyílt szövegnek; ez nehezíti a kulcselosztást és kulcskezelést. Ez a tény motiválja olyan folyamtitkosírások készítését, melyekben a kulcsfolyam

PSZEUDOVÉLETLEN

módon van generálva egy rövidebb titkos kulcsból, abban a reményben, hogy az így keletkezett kulcsfolyam véletlennek tűnik egy számítástechnikailag korlátozott ellenfél számára. Ilyen folyamtitkosírások nem biztosítanak feltétlen biztonságot [...], de azt reméljük, hogy számítástechnikailag biztonságosak."

Pontosabban:

1. DEFINÍCIÓ. „Egy pszeudovéletlen bitgenerátor (PVBG) egy olyan determinisztikus *algoritmus,* mely egy valóban véletlen k hosszúságú bináris sorozatból egy olyan $\ell \gg k$ [ℓ sokkal nagyobb, mint k] hosszúságú bináris sorozatot készít, mely véletlennek „látszik". A PVBG bemenő sorozatát *magnak* „(seed)" nevezzük (ezt például pénzfeldobással készítjük, és nyilvános kulcsú kriptográfiával továbbítjuk partnerünknek), míg a PVBG kimenő sorozatát *pszeudovéletlen* (röviden: PV) *bitsorozatnak* hívjuk."

Ilyen típusú titkosíráshoz tehát *„jó" PVBG-kre* van szükségünk. De mikor „jó" egy PVBG? Ezt a kérdést a

BONYOLULTSÁGELMÉLET

fogalmainak és eszközeinek a felhasználásával szokták megválaszolni, és így a válasz tükrözi a bonyolultságelmélet nehézségeit és korlá-

tait. (Ennek a bonyolultságelméleti megközelítésnek jó áttekintését adta S. Goldwasser a 2002. évi Nemzetközi Matematikus Kongresszuson elhangzott „Mathematical Foundations of Modern Cryptography: Computational Complexity Perspective" című előadásában [21].) Részletezve:

2. DEFINÍCIÓ. „Egy PVBG-ről akkor mondjuk, hogy az kielégíti a *következő bit tesztet*, ha nincs olyan polinomiális idejű algoritmus, mellyel egy s kimenő sorozat első ℓ bitjének ismeretében az $\ell + 1$-edik bit megjósolható $1/2$-nél lényegesen nagyobb valószínűséggel."

3. DEFINÍCIÓ. „Egy olyan PVBG-t, mely kielégíti a következő bit tesztet (esetleg valamely *plauzibilis, de bizonyítatlan matematikai feltevés* mellett, mint például annak feltételezése, hogy az egész számok faktorizálására nincs jó algoritmus) *kriptográfiailag biztonságos PVBG-nek* hívunk."

A legismertebb ilyen kriptográfiailag biztonságos PVBG-k (amelyek a faktorizálás, illetve a diszkrét logaritmus megkeresésének nehézségére épülnek) az RSA [5], Blum–Blum–Shub- [7] és Blum–Micali- [8] PVBG-k.

E definíciók több szempontból is problematikusak. A gyakorlatban általában adott N hosszúságú PV-sorozatot kell készítenünk, ugyanakkor e definíciók semmi megkötést nem tartalmaznak a „polinomiális idejű algoritmus" kifejezésben szereplő polinom fokáról és együtthatóiról N függvényében, tehát e definíciók csupán aszimptotikus természetűek. Az „$1/2$-nél lényegesen nagyobb valószínűség" fogalma szintén problematikus. Továbbá „polinomiális idejű" algoritmus nemlétezése nem bizonyítható, ezért nincs olyan PVBG, amelyről bizonyítatlan hipotézis feltételezése nélkül igazolták volna, hogy az kriptográfiailag biztonságos. A bizonyítatlan, ma még plauzibilisnek tűnő hipotézisekről pedig holnapra kiderülhet, hogy azok plau-

zibilitása vitatható, esetleg nem is igazak; így például a polinomiális idejű prímtesztelés létezésének a bebizonyítása óta sokan megkérdőjelezik a faktorizálás nehézségére vonatkozó hipotézis jogosultságát. Végül e definíciók csupán a PVBG-ket minősítik, de nem az általuk előállított egyes sorozatokat, azaz előfordulhat, hogy egy „jó" PVBG előállíthat például egy csupa 0 bitből álló sorozatot, amely a gyakorlatban nyilván használhatatlan. Éppen ezért még jónak minősített PVBG-k esetén is indokolt az előállított sorozatok „a posteriori" tesztelése a korábban leírt módon.

Ezek a problémák indokolják a pszeudovéletlenség fogalmának egy olyan új megközelítését, amely a bonyolultságelméletinél konstruktívabb, nem használ bizonyítatlan hipotéziseket, amely a generátorok pszeudovéletlenségének vizsgálata helyett az egyes sorozatokéból indul ki, és amely „a priori" típusú tesztelést is lehetővé tesz.

Egy új, konstruktív megközelítés

Végtelen bináris sorozatok pszeudovéletlen jellegének régóta használt és általánosan elfogadott mércéje a *normalitás* Borel által mintegy 100 évvel ezelőtt bevezetett fogalma [9]. A véges bináris sorozatok esete nehezebb, ebben az esetben nincs ilyen általánosan elfogadott mérce. Golomb [22], majd Knuth [35] tettek említésre érdemes – de nem nagyon sikeres – kísérletet véges bináris sorozatok pszeudovéletlenségének a definiálására. Kolmogorov [38] és Chaitin [13] vezették be az úgynevezett Turing–Kolmogorov–Chaitin-bonyolultság fogalmát, amely azonban csupán elméleti jelentőségű, hiszen nem ismerünk algoritmust a kiszámítására. Érdekesebb az úgynevezett *lineáris bonyolultság* fogalma. Ez ugyanis egyrészt egy fontos tulajdonságot vizsgál (generálható-e az adott sorozat viszonylag alacsony rendű lineáris rekurzióval?), másrészt konkrét sorozatok lineáris bonyolultsága jól számolható

az úgynevezett Berlekamp–Massey-algoritmus révén. Ugyanakkor egyszerű példák adhatók olyan sorozatokra, amelyek lineáris bonyolultsága ideálisan nagy, mégis a sorozat nyilvánvalóan nem véletlen jellegű. Másrészt általános sorozatok, sorozattípusok lineáris bonyolultsága általában nem számolható. A lineáris bonyolultság tehát a pszeudovéletlenségnek fontos, de távolról sem kielégítő mércéje.

1997-ben egy C. Mauduit-val közös cikkünkben a véges sorozatok pszeudovéletlenségének mérésére az alábbi PV-mértékek bevezetését javasoltuk [42]:

Legyen $E_N = (e_1, e_2, \ldots, e_N) \in \{-1, +1\}^N$ egy véges bináris sorozat (bitsorozatok helyett nyilván megengedhető ± 1 sorozatok vizsgálata, és az utóbbi esetben sok formula egyszerűbb). Ekkor az E_N sorozat *jóleloszlás-mértékének* az alábbi mennyiséget nevezzük:

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

ahol a maximum az olyan a, b, t hármasokra veendő, amelyekre $a, b, t \in \mathbb{N}$ és $a + (t-1)b \leq N$. A sorozat *k-ad rendű korrelációmértékének* definíciója pedig a következő:

$$C_k(E_N) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} \ldots e_{n+d_k} \right|,$$

ahol a maximumot az olyan $D = (d_1, \ldots, d_k)$ k-asokra ($d_1 < \cdots < d_k$ nemnegatív egészek) és $M \in \mathbb{N}$-ekre képezzük, amelyekre $M + d_k \leq N$.

Az E_N sorozatot akkor tekintjük „jó" pszeudovéletlen sorozatnak, ha mind $W(E_N)$, mind $C_k(E_N)$ (legalábbis „kis" k-ra) „kicsi". Ezt a terminológiát az a tény indokolja, hogy – mint később Cassaigne-nyel és Mauduit-

val közösen igazoltuk – ezek a mértékek egy igazán véletlen E_N sorozatra „kicsik”.

Az új PV-mértékek kipróbálására a legalkalmasabb jelölt a Legendre-szimbólum volt, amelynek véletlenszerű viselkedése régóta ismert, mint azt Jacobstahl [34], Davenport [17], [18], Bach [6], Peralta [52] és Damgård [16] cikkei, valamint [59] könyvem is mutatják. Valóban, még ugyanabban a Mauduit-val közös cikkben bizonyítottuk a következőt:

1. TÉTEL (Mauduit és Sárközy, 1997): *Létezik olyan p_0 szám, hogy ha p p_0-nál nagyobb prímszám, $k \in \mathbb{N}$, $k < p$, és az $E_{p-1} = (e_1, \dots, e_{p-1})$ sorozatot*

$$e_n = \left(\frac{n}{p}\right) \qquad (n = 1, 2, \dots, p-1) \tag{1}$$

-vel definiáljuk (ahol $\left(\frac{n}{p}\right)$ a Legendre-szimbólumot jelöli), akkor

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

és

$$C_k(E_{p-1}) \le 9kp^{1/2} \log p.$$

A bizonyítás az alábbi tételre épült, amelyet Weil [64] tételéből vezettünk le, felhasználva egy Vinogradovtól [63] származó egyenlőtlenséget:

2. TÉTEL (Mauduit és Sárközy, 1997): *Tegyük fel, hogy p prímszám, χ a főkaraktertől különböző (multiplikatív) karakter modulo p, amelynek rendje d (tehát $d \mid p-1$), $f(x) \in F_p[x]$ (ahol F_p a modulo p maradékosztályok teste), $f(x)$ k-adfokú és $f(x) = b(x-x_1)^{d_1} \dots (x-x_s)^{d_s}$ (ahol $i \ne j$ esetén $x_i \ne x_j$) alakban faktorizálható $\overline{F}_p$ (F_p algebrai lezártja) felett, és itt*

$$(d, d_1, \dots, d_s) = 1. \tag{2}$$

Legyenek X, Y valós számok és $0 < Y \leq p$. Ekkor

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

Később [56]-ban megmutattuk, hogy a (2) feltétel azzal helyettesíthető, hogy $f(x)$ nem $cg(x)^d$ alakú, ahol $c \in F_p$, $g(x) \in F_p[x]$ és $d \in \mathbb{N}$. Ez utóbbi formában a tétel Honkala és Tietäväinen [42]-nél egy évvel későbbi [32] cikkében is megtalálható. (Weil tételének különböző következményei a későbbiekben is meghatározó szerepet fognak játszani.)

E Mauduit-val közösen kezdeményezett irányban azóta mintegy 40 cikk született. Ezek a cikkek 5 kérdéskört vizsgálnak, ezek a következők

a) a pszeudovéletlenség mértékei;

b) pszeudovéletlen sorozatok egy nagy családja, f-bonyolultság és élesítése;

c) további jó konstrukciók;

d) számelméleti alkalmazások;

e) kiterjesztések, általánosítások.

Az alábbiakban ennek az öt területnek az irodalmát fogom áttekinteni, külön figyelmet fordítva természetesen az általam elért eredményekre.

A pszeudovéletlenség mértékei

Cassaigne-nyel és Mauduit-val közös [12] cikkünkben igazoltuk, hogy egy N hosszúságú $E_N \in \{-1, +1\}^N$ sorozatot véletlenül választva (pontosabban a 2^N számú ilyen E_N sorozat mindegykét $\frac{1}{2^N}$ valószínűséggel választva),

mind a sorozat jóleloszlás-mértéke, mind a k-adrendű korreláció mértéke nagy valószínűséggel $N^{1/2}$ körül van:

3. TÉTEL (Cassaigne, Mauduit és Sárközy, 2002):

a) *Tetszőleges $\varepsilon > 0$-hoz van olyan $\delta = \delta(\varepsilon) > 0$ és $N_0 = N_0(\varepsilon)$, hogy $N > N_0$ esetén*

$$P\big(\delta N^{1/2} < W(E_N) < 6(N\log N)^{1/2}\big) > 1-\varepsilon. \tag{3}$$

b) *Tetszőleges $\varepsilon > 0$-hoz és $k \in \mathbb{N}$-hez van olyan $\delta = \delta(\varepsilon, k) > 0$ és $N_0 = N_0(\varepsilon, k)$, hogy $N > N_0$ esetén*

$$P\big(\delta N^{1/2} < C_k(E_N) < 5(kN\log N)^{1/2}\big) > 1-\varepsilon. \tag{4}$$

Később Kohayakawa, Mauduit, Moreira és Rödl [37] élesítették ezt a tételt, és megmutatták, hogy (3) javítható

$$P\left(\delta N^{1/2} < W(E_N) < \frac{1}{\delta}N^{1/2}\right) > 1-\varepsilon$$

-ra, (4) pedig $2 \le k \le N/4$ esetén

$$P\left(\frac{2}{5}\left(N\log\binom{N}{k}\right)^{1/2} < C_k(E_N) < \frac{7}{4}\left(N\log\binom{N}{k}\right)^{1/2}\right) > 1-\varepsilon$$

-ra (k-ban egyenletesen).

Mauduit-val közös [47] cikkünkben a W és a C_2 mértékek közti kapcsolatot vizsgáltuk, és megállapítottuk, hogy e mértékek gyengén összefüggnek:

4. TÉTEL (Mauduit és Sárközy, 2003): *Bármely $N \in \mathbb{N}$-re és $E_N \in \{-1,+1\}^N$ sorozatra teljesül a*

$$W(E_N) \le 3(NC_2(E_N))^{1/2} \quad \textit{egyenlőtlenség.} \tag{5}$$

Továbbá igazoltuk, hogy ez az egyenlőtlenség az $N^{3/4}(\log N)^{1/4} \ll W(E_N) \leq N$ intervallumban egyenletesen a lehető legjobb (konstans szorzótól eltekintve):

5. TÉTEL (Mauduit és Sárközy, 2003): *Ha* $N \in \mathbb{N}$, $\ell \in \mathbb{N}$ *és* $N^{3/4}(\log N)^{1/4} \leq \ell \leq N$, *akkor van olyan* $E_N \in \{-1,+1\}^N$ *sorozat, amelyre*

$$\ell \leq W(E_N) \leq 3(NC_2(E_N))^{1/2} < 33\ell.$$

Gyarmati [27] kiterjesztette az (5) egyenlőtlenséget C_2-ről C_{2k}-ra, és később [28] az általánosított egyenlőtlenségben szereplő konstans faktor k-tól való függését is pontosan meghatározta.

Cassaigne-nyel és Mauduit-val közös [12] cikkünkben azt is vizsgáltuk, hogy van-e kapcsolat a különböző rendű korrelációk között? Megmutattuk, hogy $C_k(E_N)$ és $C_\ell(E_N)$ értéke szorosan összefügg akkor és csak akkor, ha k és ℓ közül az egyik osztója a másiknak. Pontosabban, igazoltuk, hogy ha k, ℓ rögzített természetes számok, $k \mid \ell$, $N \to \infty$ és $C_\ell(E_N)$ „kicsi" $(= o(N))$, akkor szükségképpen $C_k(E_N)$ is „kicsi"; ugyanakkor létezik olyan E_N sorozat, hogy $C_\ell(E_N)$ „nagy" akkor, ha ℓ többszöröse k-nak (beleértve $\ell = k$-t), viszont „kicsi" akkor, ha $k \nmid \ell$.

Ugyanebben a cikkben kezdeményeztük a PV-mértékek minimumának vizsgálatát is. Legyen

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

$m(N)$ becslése klasszikus probléma: következik Roth [57], illetve Matousek és Spencer [39] eredményeiből, hogy

$$c_1 N^{1/4} < m(N) < c_2 N^{1/4}.$$

Ugyanakkor $M_k(N)$ értékét mi vizsgáltuk elsőnek. Igazoltuk, hogy

6. TÉTEL (Cassaigne, Mauduit és Sárközy, 2002):

a) *$k, N \in \mathbb{N}$, $2 \le k \le N$ esetén*

$$M_k(N) < 27kN^{1/2} \log N.$$

b) *$k \in \mathbb{N}$, $k \ge 2$ esetén létezik egy olyan $N_0 = N_0(k)$ szám, hogy $N \in \mathbb{N}$, $N > N_0$ esetén*

$$M_k(N) \le 5(kN \log N)^{1/2}.$$

Ezek a felső korlátok páratlan k-ra érdektelenek, amennyiben azt is megmutattuk, hogy

$$M_{2k+1}(N) = 1 \qquad (\text{minden } k \in \mathbb{N}\text{-re}).$$

Viszont igazoltuk, hogy rögzített k-ra $M_{2k}(N) \to \infty$, ha $N \to \infty$:

$$M_{2k}(N) \ge \left(\frac{1}{\log 2} + o(1) \right) \log N.$$

Ebben a cikkben felvetettünk két megoldatlan problémát is, amelyek évekig nyitottak maradtak, és az egész témakör legérdekesebb problémáivá váltak:

1. PROBLÉMA: Van-e olyan $c > 0$, hogy $N \to \infty$ esetén

$$M_2(N) \gg N^c? \tag{6}$$

Azt sejtettük, hogy a válasz igenlő.

2. PROBLÉMA: $N \to \infty$ esetén léteznek-e olyan E_N sorozatok, amelyekre $C_2(E_N) = O(N^{1/2})$ és $C_3(E_N) = O(1)$ egyidejűleg teljesül? Itt azt sejtettük, hogy a válasz tagadó, sőt talán az is igaz, hogy létezik olyan $c > 1/2$ szám, hogy $N \to \infty$ esetén bármely $E_N \in \{-1, +1\}^N$-re

$$C_2(E_N)C_3(E_N) \gg N^c. \tag{7}$$

Az első problémát a közelmúltban Kohayakawa, Mauduit, Moreira és Rödl megoldották [37]. Igazolták, hogy (6) $c = 1/2$-del teljesül még $M_2(N)$ helyett $M_{2k}(N)$-nel is:

$$M_{2k}(N) > \left(\frac{N}{3(k+1)}\right)^{1/2} \quad \text{(minden } k, N \in \mathbb{N}, 1 \le k \le N/2\text{-re)}.$$

A szellemes bizonyítás a lineáris algebrára épül.

A 2. problémát pedig Gyarmati [25] oldotta meg, aki igazolta, hogy (7) teljesül $c = \frac{2}{3} - \varepsilon$-nal:

$$C_2(E_N)C_3(E_N) \gg N^{2/3}(\log N)^{-1/2}$$

(sőt, ennél lényegesen általánosabb tételt bizonyított szellemes elemi úton).

Ahlswedével és Cassaigne-nyel közös [1] cikkünkben adott α, k és $N \to \infty$ mellett becsültük azon $E_N \in \{-1, +1\}^N$ sorozatok számát, melyekre

$$C_k(E_N) > \alpha N.$$

Rivat-val közös [55] cikkünkben megmutattuk, hogy a jóleloszlás- és korrelációmértékekre adott felső korlátok függvényében a bevezetésben említett statisztikai tesztekben szereplő mennyiségek jól becsülhetők. Ezért ha

e korlátok elég élesek, akkor a kérdéses sorozat garantáltan sikerrel veszi e tesztek döntő részét, vagy pedig ha ezek a korlátok kicsit elmaradnak a teszt teljesítéséhez szükségestől, akkor ennek a kis pontatlanságnak nincs gyakorlati jelentősége. Így ha e PV-mértékeket elég jól tudjuk becsülni, akkor ez olyan *a priori tesztelésnek tekinthető*, amely az esetek nagy részében *feleslegessé teszi az a posteriori tesztelést*.

A legtöbb alkalmazásban a jóleloszlás- és korrelációmértékek használata elegendő. Természetesen, további PV-mértékek is bevezethetők, amelyek bizonyos alkalmazásokban hasznosak lehetnek. Így például már a Mauduittal közös [42] cikkünkben bevezettük a „normalitásmérték", valamint a „kombinált mérték" fogalmát, Gyarmati [24] pedig bevezette és tanulmányozta a „szimmetriamérték" fogalmát. Ezek közül a normalitásmérték rekurzív konstrukciók kapcsán lehet hasznos, míg a szimmetriamérték például a Legendre-szimbólumra épülő konstrukciókban játszik fontos szerepet.

PV-sorozatok egy nagy családja, f-bonyolultság

Az alkalmazások nagy részében (így például a kriptográfiában) nem elég „néhány" „jó" PV-sorozatot konstruálni, hanem ilyen sorozatok *nagy családjára* van szükség. Természetes ötlet az 1. tételben leírt konstrukciót úgy kiterjeszteni ebben az irányban, hogy ott $e_n = \left(\frac{n}{p}\right)$ helyett

$$e_n = \left(\frac{f(n)}{p}\right) \tag{8}$$

-t írunk, ahol $f(x) \in F_p[x]$. Itt $f(x)$ nem lehet akármilyen polinom, hiszen ha $f(x) = cg(x)^2$, ahol $c \in F_p$ és $g(x) \in F_p[x]$, akkor

$$e_n = \left(\frac{c}{p}\right) \quad \text{minden } n\text{-re, amelyre } p \nmid g(n),$$

tehát az $e_1, e_2, \dots$ sorozat lényegében állandó, és így biztosan nem tekinthető pszeudovéletlennek. Hoffstein és Lieman [31] javasolták (8)-ban olyan $f(x)$ polinom használatát, amely négyzetmentes és se nem páros, se nem páratlan, ám semmit sem bizonyítottak az így nyert sorozatok PV-tulajdonságaira vonatkozóan. Később [23]-ban ismertettünk olyan példákat, amelyek mutatják, hogy vannak más problematikus polinomok is. Először Mauduit-val közös [43] cikkünkben adtunk elégséges feltételt arra, hogy valamely $f(x)$ polinomra a (8) konstrukció „jó" ($W(E_N)$ és $C_k(E_N)$ kicsi legyen): megmutattuk, hogy a (8) konstrukció jó, ha $f(x)$ permutációpolinom F_p felett van. Ennek az eredménynek az a szépséghibája, hogy viszonylag keveset tudunk a permutációpolinomokról.

Goubinnel és Mauduit-val közös [23] cikkünkben lényegesen szélesítettük a „jó" $f(x)$ polinomok körét:

7. TÉTEL (Goubin, Mauduit és Sárközy, 2004): *Ha p prímszám, $f(x) \in F_p[x]$, $f(x)$ d-edfokú $(d > 0)$, és nincs többszörös gyöke $\overline{F}_p$-ben (F_p algebrai lezártjában), és az $E_p = (e_1, \dots, e_p)$ bináris sorozatot*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right), & \text{ha } (f(n), p) = 1 \\ +1, & \text{ha } p \mid f(n) \end{cases} \tag{9}$$

definiálja, akkor

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

Ha továbbá $k \in \mathbb{N}$, és feltesszük, hogy az alábbi 3 feltétel valamelyike teljesül:

a) $k = 2$; b) $k < p$ *és 2 primitív gyök modulo p;* c) $(4d)^k < p$,

akkor $C_k(E_p) < 10dkp^{1/2} \log p$ *is teljesül.*

Ellenpéldák mutatják, hogy az a), b) és c) feltételek ugyan esetleg valamelyest enyhíthetők, de teljesen nem engedhetők el. A bizonyításban a karakterösszegekre vonatkozó 2. tétel mellett egy új kombinatorikus számelméleti addíciós tétel is fontos szerepet játszik, és szükség van a véges testek elméletére is. A tételben leírt konstrukciót szeretnénk PVBG-nek tekinteni, amelyben a mag az $f(x)$ polinom együtthatóit alkotó bitekből áll. Ez így nem egészen pontos, mert az $f(x)$-re tett kikötések miatt e bitek nem választhatók szabadon. E kis nehézségen a konstrukció minimális módosításával (csak bizonyos speciális $f(x)$-ek megtartásával) könnyen lehet segíteni. Megjegyezzük, hogy a leírt E_p PV-sorozatok gyorsan elkészíthetők, hiszen a Legendre-szimbólum értéke gyorsan számolható (sőt, ha p nem túl nagy, akkor a Legendre-szimbólumok kiszámítása helyettesíthető igen gyorsan elkészíthető táblázat használatával).

Bár azóta más jó konstrukciók is születtek jó PV-tulajdonságokkal rendelkező sorozatok nagy családjaira, máig a 7. tételben leírt konstrukció és annak változatai a legjobbak.

Rivat-val közös [55] cikkünkben főleg kapcsolódó implementációs kérdésekkel és numerikus vizsgálatokkal foglalkoztunk.

A 7. tétel tehát „jó" PV-sorozatok *nagy* családját írja le. Bizonyos alkalmazásokban – így például a kriptográfiában – azonban nem elég, ha a család nagy; sokkal fontosabb, hogy a család *„gazdag", „bonyolult" szerkezetű* legyen. Ennek a tulajdonságnak a mérésére Ahlswedével, Khachatriannal és Mauduit-val közös [2] cikkünkben bevezettük az f*-bonyolultság* fogalmát:

Tekintsük bináris sorozatok egy $\mathcal{F} \subset \{-1,+1\}^N$ családját, legyen $k \in \mathbb{N}$, $k \le N$, $1 \le i_1 < i_2 < \dots i_k \le N$ és $(\varepsilon_1, \dots, \varepsilon_k) \in \{-1,+1\}^k$. Tekintsünk

olyan $E_N = (e_1, \dots, e_N) \in \mathcal{F}$ sorozatokat, amelyekre

$$e_{i_1} = \varepsilon_1,\ e_{i_2} = \varepsilon_2, \dots, e_{i_k} = \varepsilon_k; \tag{10}$$

(10)-et az E_N sorozat egy k *hosszúságú specifikációjának* mondjuk.

4. DEFINÍCIÓ. Bináris sorozatok egy $\mathcal{F} \subset \{-1, +1\}^N$ családjának $\Gamma(\mathcal{F})$-fel jelölt f*-bonyolultságán* (az „f" a „family" szóra utal) a legnagyobb olyan k természetes számot értjük, hogy bármely k hosszúságú specifikációhoz található legalább egy olyan $E_N \in \mathcal{F}$ sorozat, amely ezt kielégíti.

Ha PV-sorozatok egy $\mathcal{F}$ családját egy ℓ hosszúságú (véletlen) magból képezzük, akkor nyilván $|\mathcal{F}| = 2^\ell$, ebből következik, hogy

$$\Gamma(\mathcal{F}) \le \ell.$$

Így $\mathcal{F}$-et akkor tekinthetjük *magas bonyolultságúnak,* ha f-bonyolultsága nem sokkal (mondjuk legfeljebb egy $\log \ell$ hatvánnyal) kisebb az ℓ maghossznál. Ahlswedével, Khachatriannal és Mauduit-val közös cikkünkben igazoltuk, hogy a 7. tételben leírt konstrukció minimális módosításával elérhető, hogy pontosan ez legyen a helyzet.

Stewarttal közös [61] cikkünkben még egy lépéssel tovább mentünk: megmutattuk, hogy a 7. tételbeli konstrukció kis módosításával nemcsak az érhető el, hogy minden „hosszú" specifikáció előforduljon a konstruált $\mathcal{F}$ család legalább egy E_N elemében, hanem még az is, hogy minden ilyen specifikáció körülbelül azonos számú $E_N \in \mathcal{F}$ sorozatban forduljon elő.

8. TÉTEL (Stewart és Sárközy, sajtó alatt): *Legyen p prímszám, $\ell \in \mathbb{N}$, $\ell \le p$. $\mathcal{A} \subset \{1, 2 \dots, p\}$ esetén legyen*

$$f_{\mathcal{A}}(x) = \prod_{a \in \mathcal{A}} (x - a), \tag{11}$$

és definiáljuk az $E_{p,\ell}(f_{\mathcal{A}}) = (e_1, \dots, e_\ell)$ *sorozatot a következőképpen:* $1 \le n \le \ell$ *esetén legyen*

$$e_n = \begin{cases} \left(\frac{f_{\mathcal{A}}(n)}{p}\right) & \text{ha } n \notin \mathcal{A} \\ (-1)^i & \text{ha } n \in \mathcal{A} \text{ és } |\{1, \dots, n\} \cap \mathcal{A}| = i. \end{cases} \tag{12}$$

$d \in \mathbb{N}$, $d \le p$, $m \in \mathbb{N}$, $\ell + m \le p$ *esetén legyen*

$$\mathcal{F} = \mathcal{F}(p, \ell, m, d) = \left\{E_{p,\ell}(f_{\mathcal{A}}) : |\mathcal{A}| = d, \mathcal{A} \subset \{1, \dots, m\}\right\}.$$

Ekkor $E_{p,\ell}(f_{\mathcal{A}}) \in \mathcal{F}$ *esetén*

$$W(E_{p,\ell}(f_{\mathcal{A}})) < 10dp^{1/2} \log p, \tag{13}$$

és ha $k \in \mathbb{N}$ *és*

a) $k = 2$,

b) $k < p$ *és* 2 *primitív gyök modulo* p,

vagy

c) $(4d)^k < p$,

akkor

$$C_k(E_{p,\ell}(f_{\mathcal{A}})) < 10kdp^{1/2} \log p \tag{14}$$

is teljesül. Jelöljük azon $\mathcal{F}$*-beli sorozatok halmazát, amelyek egy adott* S *specifikációt kielégítenek,* $\mathcal{F}(S)$*-sel. Tegyük fel még azt is, hogy*

$$\min(\ell, m) > 20dp^{1/2} \log p,$$

$d < p^{1/2}$, $t \in \mathbb{N}$ és $t \leq \ell$. Ekkor bármely $\{1, 2, \ldots, \ell\}$-ből képezett t hosszúságú S specifikációra

$$\left| |\mathcal{F}(S)| - \frac{|\mathcal{F}|}{2^t} \right| \leq \frac{12tp^{1/2}\log p}{m}|\mathcal{F}|. \tag{15}$$

E tételben (13) és (14) lényegében a 7. tételből következnek, hiszen e_n 7. tételbeli (9) definíciója és a mostani (12) definíció közt alig van eltérés (a két definíció csupán $p \mid f(n)$ esetén tér el), és ez a minimális eltérés csupán kis hibát eredményez. A tétel lényeges új része a (15) egyenlőtlenség.

A 8. tétel bizonyítása azt is tartalmazza, hogy a tételben szereplő konstrukció *„ütközésellenálló"* („collision resistant"), ami annyit jelent, hogy különböző magokhoz ($\mathcal{A}$-khoz) különböző $E_{p,\ell}(f_{\mathcal{A}})$ sorozatok tartoznak (vagyis az $\{\mathcal{A} : |\mathcal{A}| = d, \mathcal{A} \subset \{1, \ldots, m\}\} \to \mathcal{F}$ leképezés invertálható).

Az is könnyen igazolható lenne, hogy az $\mathcal{F}$ család rendelkezik az *erős lavinatulajdonsággal* („strict avalanche effect") is, ami azt jelenti, hogy $\mathcal{A}$-nak csak egyetlen elemét is megváltoztatva, az $\mathcal{A}$-hoz rendelt $E_{p,\ell}(f_{\mathcal{A}})$ sorozatot alkotó bitek körülbelül fele megváltozik.

Megjegyzem, hogy a 7. és a 8. tételben leírt PVBG bonyolultságelméleti értelemben is kriptográfiailag biztonságosnak tekinthető, azon hipotézis mellett, hogy az $f(n)$ polinom rekonstrukciója az $\left(\frac{f(n)}{p}\right)$ értékekből nagy fokszám esetén nehéz feladat. Ezt a hipotézist alátámasztja az a tény, hogy ebben az irányban a legjobb becslés Russelltől és Shparlinskitől [58] származik, és még ez is igen gyenge: igazolták, hogy ha $\varepsilon > 0$, $d < p^{1/2}(\log p)^{-2}$, és adott egy orákulum, amely megmondja $\left(\frac{f(x)}{p}\right)$ értékét bármely $x \in F_p$-re, akkor bármely d-edfokú F_p feletti polinom meghatározható $O(d^2 p^{d+\varepsilon})$ bitoperáció révén.

Összegezve: a „jó” PV-tulajdonságokkal rendelkező sorozatok nagy családjára a 8. tételben adott konstrukció sok szempontból máig a legjobb konstrukció.

További jó konstrukciók

Vannak azonban további jó konstrukciók is, amelyek alig gyengébbek, és bizonyos körülmények közt versenyképesek.

Jelöljük n modulo p legkisebb nemnegatív maradékát $r_p(n)$-nel.

Mauduit-val közös [48] cikkünkben bizonyítottuk a következőt:

9. TÉTEL (Mauduit és Sárközy, sajtó alatt): *Tegyük fel, hogy p prím, $f(x) \in F_p[x]$, $f(x)$ d-edfokú, $0 < d < p$ és $f(x)$-nek nincs többszörös gyöke $\overline{F}_p$-ben. $(a,p) = 1$ esetén jelöljük a multiplikatív inverzét a^{-1}-gyel: $aa^{-1} \equiv 1 (\mathrm{mod}\, p)$. Definiáljuk az $E_p = (e_1, \dots, e_p) \in \{-1,+1\}^p$ sorozatot a következőképpen: $1 \le n \le p$ esetén*

$$e_n = \begin{cases} +1 & \text{ha } (f(n),p) = 1,\ r_p(f(n)^{-1}) < p/2 \\ -1 & \text{ha vagy } (f(n),p) = 1,\ r_p(f(n)^{-1}) > p/2 \text{ vagy } p \mid f(n). \end{cases}$$

Ekkor

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

Ha továbbá $k \in \mathbb{N}$, $2 \le k \le p$, és vagy

a) $k = 2$,

vagy

b) $(4d)^k < p$,

akkor

$$C_k(E_p) \ll kdp^{1/2}(\log p)^{k+1}. \tag{16}$$

([48]-ban azt is igazoltuk, hogy (11) típusú polinomokra e tételben a) és b) elhagyható, (16) ezek feltételezése nélkül is teljesül.)

Ennek a tételnek a bizonyítása ismét Weil tételének egy következményére épül.

Mauduit-val és Rivat-val közös [41] cikkünkben viszont a 2. tételnek az *additív* karakterekre vonatkozó analogonját használtuk, amely ugyancsak Weil tételéből vezethető le, és Niederreitertől [50], illletve Tietäväinentől [62] származik. Ebben a cikkben a következő konstrukciót vizsgáltuk:

Legyen p prím, $f(x) \in F_p[x]$, és definiáljuk az $E_p = (e_1, \dots, e_p) \in \{-1, +1\}^p$ sorozatot a következőképpen: $1 \le n \le p$ esetén legyen

$$e_n = \begin{cases} +1, & \text{ha } r_p(f(n)) < p/2 \\ -1, & \text{ha } r_p(f(n)) \ge p/2. \end{cases}$$

Ez a sorozat nagyon gyorsan generálható, és megmutattuk, hogy erre a sorozatra $W(E_p)$ és $k < \deg f(x)$ esetén, $C_k(E_p)$ is „kicsi"; ugyanakkor e konstrukció gyengéje, hogy $k \ge \deg f(x)$ esetén $C_k(E_N)$ lehet nagy.

[60]-ban az alábbi konstrukciót vizsgáltam: Legyen p páratlan prím, $N = p - 1$, és definiáljuk az $E_N = \{e_1, \dots, e_N\} \subset \{-1, +1\}^N$ sorozatot úgy, hogy $1 \le n \le N$ esetén legyen

$$e_n = \begin{cases} +1 & \text{ha } 1 \le \operatorname{ind} n \le \frac{p-1}{2} \\ -1 & \text{ha } \frac{p+1}{2} \le \operatorname{ind} n \le p-1, \end{cases} \tag{17}$$

ahol $\operatorname{ind} n$ az n szám g alapú indexét (vagy diszkrét logaritmusát) jelöli egy rögzített g primitív gyök mellett. Megmutattam (ismét a karakterösszegekre vonatkozó 2. tételre támaszkodva), hogy ez a sorozat majdnem olyan jó PV-tulajdonságokkal rendelkezik, mint az 1. tételben vizsgált Legendre-szimbólum.

Ezt a konstrukciót Gyarmati [26] kiterjesztette jó PV-tulajdonságokkal rendelkező bináris sorozatok nagy családjává: megmutatta, hogy ha az $f(x) \in F_p[x]$ polinom kielégít bizonyos feltételeket, akkor (17)-ben n-et $f(n)$-nel helyettesítve, továbbra is jó PV-tulajdonságokkal rendelkező sorozatot kapunk. Ha p nem nagyon nagy, és így van lehetőség táblázat készítésére, akkor ez a konstrukció majdnem olyan jó, mint a 7. tételben leírt. Ha viszont p nagy, akkor ez a sorozat csak lassan generálható, mert nincs jó algoritmus a diszkrét logaritmus kiszámítására. Ezért később Gyarmati [27] kidolgozta ennek a konstrukciónak a gyorsított változatát is.

Kodila [36] elkészítette a 4. és az 5. fejezetben ismertetett konstrukciók futásidő-analízisét, és numerikus számításokat is végzett e konstrukcióknak, valamint két gyakran használt, a bevezetésben is említett „kriptográfiailag is biztonságos" PVBG-nek az összehasonlítására futásidő és PV-értékek szempontjából. Többek közt megállapította, hogy az RSA PVBG messze lassabb a többinél, de a Blum–Blum–Shub-féle PVBG is lassabb az új konstrukcióknál.

Megjegyzem, hogy valamennyi eddig ismertetett új konstrukció moduláris természetű, pontosabban a konstruált sorozatok elemeit modulo p kongruenciafeltételekkel definiáljuk, ahol p prímszám. Természetes ötlet e konstrukciók kiterjesztése összetett modulusra. Rivat-val [56] vizsgáltuk ezt a kérdést, és megállapítottuk, hogy RSA-típusú modulus esetén, tehát ha a modulus $m = pq$ alakú, ahol p és q egymáshoz közeli prímek, akkor a so-

rozatok PV-mértékeire csak $O(m^{3/4}(\log m)^c)$ korlát adható (amely lényegesen gyengébb a prím esetben adottaknál), és ez a lehető legjobb. Ez a tény arra int, hogy a bonyolultságelméleti értelemben kriptográfiailag biztonságos PVBG-k kimenő sorozatai esetleg nem igazán véletlen jellegűek.

Számelméleti alkalmazások

A pszeudovéletlenség vizsgálatára kidolgozott fogalmak és eszközök nemcsak a kriptográfiában alkalmazhatók, hanem a matematika más területein is, így főként a számelméletben speciális sorozatok véletlenszerű viselkedésének a tanulmányozására.

Mauduit-val közös [43] cikkünkben az (1) Legendre-szimbólum-konstrukció permutációpolinomokra való kiterjesztése mellett vizsgáltuk a Thue–Morse-, Rudin–Shapiro- és Champernowne-sorozatok véletlenszerű viselkedését is.

A Liouville-függvény definíciója: $\lambda(n) = (-1)^{\Omega(n)}$, ahol $\Omega(n)$ az n szám összes (multiplicitással számolt) prímosztóinak a számát jelöli. Ez a függvény rendkívül fontos szerepet játszik a prímszámelméletben. E függvény véletlenszerűségének, így például a másodrendű korrelációnak a vizsgálata klasszikus és nagyon nehéz problémakör. Cassaigne-nyel, Ferenczivel, Mauduit-val és Rivat-val közös [10], [11] cikkeinkben további részeredményeket értünk el ezen a területen.

Minthogy a Liouville-függvény ennyire nehezen kezelhető, ezért Daboussival közös [14], [15] cikkeinkben helyette részben más, általánosabb ± 1 értékű multiplikatív függvényeket vizsgáltunk, részben a „csonkított" Liouville-függvényt, amely a Liouville-függvényből úgy keletkezik, hogy a „nagy" prímszámokon felvett értéket -1-ről $+1$-re változtatjuk, és továbbra

is megköveteljük a multiplikativitást. E függvények PV-mértékeire részben kombinatorikus szitamódszerek, részben Daboussi konvolúciós módszere segítségével sikerült meglehetősen éles becsléseket adnunk.

Mauduit-val közös [44], [45] cikkeinkben Erdős Pál egy problémájából indultunk ki. Legyen k adott természetes szám, α adott irracionális szám, és legyen $n = 1, 2, \dots$ esetén

$$e_n = \begin{cases} +1, & \text{ha } 0 \le \{n^k\alpha\} < 1/2 \\ -1, & \text{ha } 1/2 \le \{n^k\alpha\} < 1. \end{cases}$$

Az α szám lánctörtjegyeire vonatkozó feltételek mellett sikerült az így keletkező $E_N(e_1, \dots, e_N)$ sorozat PV-mértékeit becsülnünk (exponenciális összegek felhasználásával). E vizsgálatainkhoz később Philipp és Tichy [53] is kapcsolódtak.

Mauduit-val és Rivat-val közösen [40] vizsgáltuk az

$$e_n = \begin{cases} +1, & \text{ha } \{n^c\} < 1/2 \\ -1, & \text{ha } 1/2 \le \{n^c\} \end{cases}$$

által definiált $e_1, e_2, \dots$ sorozat PV-tulajdonságait.

Jelöljük n legnagyobb prímfaktorát $P(n)$-nel, és legnagyobb olyan prímfaktorát, amely $\le y$, $P_y(n)$-nel. $n = 1, 2, \dots$ esetén legyen

$$e_n = \begin{cases} +1, & \text{ha } P(n+1) > P(n) \\ -1, & \text{ha } P(n+1) < P(n). \end{cases}$$

Ugyancsak Erdős kérdése nyomán vizsgálta Rivat az így keletkezett $E_N = (e_1, \dots, e_N)$ sorozat, valamint a $P(n)$ helyett $P_y(n)$-nel képezett analóg sorozat PV-tulajdonságait.

Fouvryval, Michellel és Rivat-val közös [20] cikkünkben a Kloostermann-összegek előjele által alkotott bináris sorozat PV-mértékeit becsültük.

Szintén Erdős egy kérdéséből kiindulva, Oon [51] vizsgálta azt a sorozatot, amelynek n-edik eleme

$$e_n = \begin{cases} +1, & \text{ha } P(n) \equiv +1 \pmod 4 \text{ vagy } n = 2^k \\ -1, & \text{ha } P(n) \equiv -1 \pmod 4. \end{cases}$$

($P(n)$ ismét n legnagyobb prímfaktorát jelöli.)

Általánosítások, kiterjesztések

Mauduit-val közös [46] cikkünkben kiterjesztettük vizsgálatainkat 2 szimbólumból álló sorozatokról k szimbólumból állókra. Ahlswedével és Mauduit-val közös [3], [4] cikkeinkben kiterjesztettük az f-bonyolultság fogalmát erre az esetre, és konstrukciót adtunk k szimbólumból álló sorozatok nagyszámosságú és nagy bonyolultságú családjára.

Az előző fejezetekben vizsgált PV-sorozatok $1/2$ paraméterű binomiális eloszlásból vett mintát imitálnak. Hubert-rel közös [33] cikkünkben kiterjesztettük a vizsgálatokat a p paraméterű binomiális eloszlás esetére, és bevezettük a p-pszeudovéletlenség fogalmát.

E kiterjesztések mindegyikére jellemző, hogy az alapesetben nyert eredmények jelentős része bizonyos módosításokkal átvihető az általános esetre, és a konstrukciókkal kapcsolatban Weil tétele továbbra is fontos szerepet játszik. Ugyanakkor mindegyik esetben fellépnek váratlan nehézségek is, és előfordul, hogy nem sikerül olyan viszonylag teljes választ nyerni, mint az alapesetben.

Jelenleg Hubert-rel, Mauduit-val és Stewarttal a vizsgálatok több dimenzióra való kiterjesztésén dolgozunk. E munka befejezését az akadályozza, hogy *bizonyíthatóan* igazán jó konstrukciót máig nem sikerült találnunk.

Irodalomjegyzék

[1] Ahlswede, R., Cassaigne, J. and Sárközy, A.: On the correlation of binary sequences. Applied *Discrete Math.*, sajtó alatt.

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

[3] Ahlswede, R., Mauduit, C. and Sárközy, A.: Large families of pseudorandom sequences of k symbols and their complexity, *I. Proceedings on General Theory of Information Transfer and Combinatorics,* sajtó alatt.

[4] Ahlswede, R., Mauduit, C. and Sárközy, A.: Large families of pseudorandom sequences of k symbols and their complexity, *II. Proceedings on General Theory of Information Transfer and Combinatorics,* sajtó alatt.

[5] Alexi, W., Chor, B., Goldreich, O. and Schnorr, C. P.: RSA and Rabin functions: Certain parts are as hard as the whole. *SIAM J. Computing* **17** (1988), 194–209.

[6] Bach, E.: Realistic analysis of some randomized algorithms. 19th *ACM Sympos. on Theory of Computing,* 1987.

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

[8] Blum, M. and Micali, S.: How to generate cryptographically strong sequences of pseudo-random bits. *SIAM J. Computing* **13** (1984), 850–864.

[9] Borel, E.: Leçons sur la théorie des fonctions, 2nd ed., 1914, 182–216.

[10] Cassaigne, J., Ferenczi, S., Mauduit, C., Rivat, J. and Sárközy, A.: On finite pseudorandom binary sequences, III. (The Liouville function, I). *Acta Arith.* **87** (1999), 367–390.

[11] Cassaigne, J., Ferenczi, S., Mauduit, C., Rivat, J. and Sárközy, A.: On finite pseudorandom binary sequences, IV: The Liouville function, II. *Acta Arith.* **95** (2000), 343–359.

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

[13] Chaitin, G. J.: On the length of programs for computing finite binary sequences. *J. Association Computing Machinery* **13** (1966), 547–569.

[14] Daboussi, H. and Sárközy, A.: On pseudorandom properties of multiplicative functions. *Acta Math. Hungar.* **98** (2003), 273–300.

[15] Daboussi, H. and Sárközy, A.: On the correlation of the truncated Liouville function. *Acta Arith.* **108** (2003), 61–76.

[16] Damgård, I.: On the randomness Legendre and Jacobi sequences. *Lect. Notes in Comp. Sci.* 403, Springer-Verlag, Berlin, 1990, 163–172.

[17] Davenport, H.: On the distribution of quadratic residues (mod p). *J. London Math. Soc.* **6** (1931), 49–54.

[18] Davenport, H.: On the distributions of quadratic residues (mod p). *J. London Math. Soc.* **8** (1933), 46–52.

[19] Elliott, P. D. T. A.: On the correlation of multiplicative and the sum of additive arithmetic functions. *Mem. Amer. Math. Soc.* **538** (1994).

[20] Fouvry, E., Michel, P., Rivat, J. and Sárközy, A.: On the pseudorandomness of the signs of Kloosterman sums. *J. Australian Math. Soc.*, sajtó alatt.

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

[22] Golomb, S. W.: *Shift Register Sequences.* Holden-Day, San Francisco, 1967. Reprinted by Aegean Park Press, 1982.

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

[24] Gyarmati, K.: On a pseudorandom property of binary sequences. *Ramanujan J.*, sajtó alatt.

[25] Gyarmati, K.: On the correlation of binary sequences. *Studia Sci. Math. Hungar.*, sajtó alatt.

[26] Gyarmati, K.: On a family of pseudorandom binary sequences. *Periodica Math. Hungar.*, sajtó alatt.

[27] Gyarmati, K.: On a fast version of a pseudorandom generator. *Proceedings on General Theory of Information Transfer and Combinatorics*, sajtó alatt.

[28] Gyarmati, K.: An inequality between the measures of pseudorandomness. *Annales Univ. Sci. Budapest. Eötvös*, sajtó alatt.

[29] Gyarmati, K., Pethő, A. and Sárközy, A.: On linear recursions and pseudorandomness. *Acta Arithmetica,* sajtó alatt.

[30] Hildebrand, A.: On consecutive values of the Liouville function. *Enseign. Math.* **32** (1986), 219–226.

[31] Hoffstein, J. and Lieman, D.: The distribution of the quadratic symbol in function fields and a faster mathematical stream cipher. *Progress in Computer Science and Applied Logic,* vol. 20, Birkhäuser Verlag, Basel, Switzerland, 2001, 59–68.

[32] Honkala, I. and Tietäväinen, A.: Codes and Number Theory. In: *Handbook of Coding Theory, Elsevier Science,* 1998, 1141–1194.

[33] Hubert, P. and Sárközy, A.: On p-pseudorandom binary sequences. *Periodica Math. Hungar.*, sajtó alatt.

[34] Jacobstahl, E.: *Anwendungen einer Formel aus der Theorie der quadratischen Reste. Dissertation,* Berlin, 1906, 26–32.

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

[36] Kodila, D.: Running time analysis of constructions of pseudorandom binary sequences. *Annales Univ. Sci. Budapest.* Eötvös, sajtó alatt.

[37] Kohayakawa, Y., Mauduit, C., Moreira, C. G. and Rödl, V.: Measures of pseudorandomness for finite sequences: minimum and typical values. *J. London Math. Soc.*, sajtó alatt.

[38] Kolmogorov, A.: Three approaches to the definition of the concept „quantity of information". *Problemy Peredachi Informatsii* **1** (1965), 3–11.

[39] Matousek, J. and Spencer, J.: Discrepancy in arithmetic progressions. *J. Amer. Math. Soc.* **9** (1996), 195–204.

[40] Mauduit, C., Rivat, J. and Sárközy, A.: On the pseudo-random properties of n^c. *Illinois J. Math.* **46** (2002), 185–197.

[41] Mauduit, C., Rivat, J. and Sárközy, A.: Construction of pseudorandom binary sequences using additive characters. *Monatshefte Math.* **141** (2004), 197–208.

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

[43] Mauduit, C. and Sárközy, A.: On finite pseudorandom binary sequences, II. (The Champernowne, Rudin–Shapiro and Thue–Morse sequences. A further construction.) *J. Number Theory* **73** (1998), 256–276.

[44] Mauduit, C. and Sárközy, A.: On finite pseudorandom binary sequences, V. On $(n\alpha)$ and $(n^2\alpha)$ sequences. *Monatshefte Math.* **129** (2000), 197–216.

[45] Mauduit, C. and Sárközy, A.: On finite pseudorandom binary sequences, VI. (On $(n^k\alpha)$ sequences), *Monatshefte Math.* **130** (2000), 281–298.

[46] Mauduit, C. and Sárközy, A.: On finite pseudorandom sequences of k symbols. *Indag. Mathem.* **13** (2002), 89–101.

[47] Mauduit, C. and Sárközy, A.: On the measures of pseudorandomness of binary sequences. *Discrete Math.* **271** (2003), 195–207.

[48] Mauduit, C. and Sárközy, A.: Construction of pseudorandom binary sequences by using the multiplicative inverse. *Acta Math. Hungar.*, sajtó alatt.

[49] Menezes, A. van Oorshot, P. and Vanstone, S. A.: *Handbook of Applied Cryptography*. CRC Press, Boca Raton, 1997.

[50] Niederreiter, H.: Statistical independence of non-linear congruential pseudorandom numbers. *Monatshefte Math.* **106** (1988), 149–159.

[51] Oon, S.-M.: Pseudorandom properties of prime factors. *Periodica Math. Hungar.*, sajtó alatt.

[52] Peralta, R.: On the distribution of quadratic residues and nonresidues modulo a prime number. *Math. Comp.* **58** (1992), 433–440.

[53] Philipp, W. and Tichy, R.: Metric theorems for distribution measures of pseudorandom sequences. *Monatshefte Math.* **135** (2002), 321–326.

[54] Rivat, J.: On pseudo-random properties of $P(n)$ and $P(n+1)$. *Periodica Math. Hungar.* **43** (2001), 121–136.

[55] Rivat, J. and Sárközy, A.: On pseudo-random binary sequences and their applications. *Proceedings on General Theory of Information Transfer and Combinatorics,* sajtó alatt.

[56] Rivat, J. and Sárközy, A.: *Modular constructions of pseudorandom binary sequences with composite moduli.* preprint.

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

[58] Russell, A. and Shparlinski, I.: *Classical and quantum function reconstruction via character evaluation.* sajtó alatt.

[59] Sárközy A.: *Számelmélet és alkalmazásai.* Műszaki Könyvkiadó, Budapest, 1978.

[60] Sárközy, A.: A finite pseudorandom binary sequence. *Studia Sci. Math. Hungar.* **38** (2001), 377–384.

[61] Sárközy, A. and Stewart, C. L.: *On pseudorandomness in families of sequences derived from the Legendre symbol.* preprint.

[62] Tietäväinen, A.: Incomplete sums and two applications of Deligne's result, Algebra, Some Current Trends. *Lecture Notes Math.,* vol. 1352, Springer, 1988, 190–205.

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

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

Érdy János
Podhradczky József
Wenzel Gusztáv
Fábián Gábor
Nagy János
Arany János
Polya József

Tekintetes Nagygyülés!

…démia fennálló szabályainak 32-ka egy szót:
„Minden újonnan választott tag, a külsők kivéte-
lével, osztályába tartozó dolgozat felolvasásával,
vagy személyes megnem jelenhetés esetén beküldé-
sével, legfelebb egy év alatt széket foglal; különben meg-
választása megsemmisülvén."

Lehetnek esetek, melyekben kivált vidéken la-
kók gátoltatnak a határidőt megtartani: de hallga-
tag elnézni e szabály meg nem tartatását, annyit
tesz, mint összes szabályzatunkat erőtlennek tekinteni.
A következményekre figyelmessé tenni a T. Akadém-
át szükségtelen.

Inditványba hozzákik tehát, hogy egyelőre a…
…szerfoglalás által meg nem…
…választott s …ből kitöröltessenek, az 18…
…tessenek, j…