Szakmai zárójelentés az OTKA PD72264 számú pályázatról

Az ókortól kezdve napjainkig a véletlengenerálás mindig fontos szerepet játszott. Kutatásaimban főképp számítógép által generálható pszeudovéletlen objektumokat tanulmányoztam.

A pszeudovéletlen sorozatoknak rengeteg alkalmazása van. Ezek közül a legfontosabbak a híres Vernam-féle titkosító eljáráshoz kapcsolódnak. Több mint 15 évvel ezelőtt Mauduit és Sárközy [21] bevezetett egy új, konstruktív megközelítést. Cikkükben új pszeudovéletlen mértéket vezettek be véges, bináris +1,-1 sorozatok pszeudovéletlen tulajdonságainak vizsgálatára. (Azóta rengeteg cikk született a témában, [22]-ben Sárközy egy kitűnő összefoglalást ad a legfontosabb eredményekről.)

Mostanában a pszeudovéletlen sorozatok mellett a többdimenziós pszeudovéletlen objektumok is bekerültek a kutatás főirányvonalába. Hubert, Mauduit és Sárközy [20] kiterjesztette a pszeudovéletlenség fogalmát egy dimenzióról több dimenzióra. Bevezették az n-dimenziós bináris rács fogalmát. Új mértékeket vezettek be bináris rácsok pszeudovéletlen tulajdonságainak vizsgálatára.

A projekt időtartama alatt 19 cikket írtam, ezek közül 11 dolgozatom jelent meg, és 4 dolgozatomat fogadtak el már közlésre neves hazai vagy külföldi folyóiratokban. További 4 cikket nyújtottam be közlésre. Az alábbiakban szeretném főbb eredményeimet röviden összefoglalni.

Bináris sorozatok pszeudovéletlen tulajdonságai

2003-ban Ahlswede, Khachatrian, Mauduit és Sárközy bevezették egy új mértéket bináris sorozatok családjainak a „bonyolultságára", és becsülték a legfontosabb ilyen, a Legendre szimbólumot használó családnak a bonyolultságát. [3]-ben meghatároztam -konstans szorzótól eltekintve- e mérték pontos értékét.

Egy bináris véges sorozat kriptográfiai alkalmazása során előfordulhat, hogy a sorozat nem elég hosszú. [2]-ben és [10]-ben azt vizsgálom, hogy pszeudovéletlen sorozatok egy adott nagy családjából hogyan illeszthetünk egymás után több sorozatot úgy, hogy az így kapott jóval hosszabb sorozatnak még mindig erős pszeudovéletlen tulajdonságai legyenek.

A bizonyítás során Ahlswede, Khachatrian, Mauduit és Sárközy által bevezették bináris sorozatok család bonyolultságának fogalmát kiterjesztve, bevezettem egy új mértéket, amely azt tanulmányozza, hogy bináris sorozatok egy nagy családjában mennyire függetlenek a sorozatok.

[6]-ban a diszkrét logaritmust használva adtam meg pszeudovéletlen sorozatoknak egy új konstrukcióját. A konstrukció érdekes vonása, hogy speciális esetekben elliptikus görbéken alapuló pszeudovéletlen sorozatokat ad. Ilyenkor a sorozat n-edik tagja, egy elliptikus görbe adott pontjának y-koordinátájától függ.

[13]-ban Mauduittal egy korábbi eredményemet általánosítottuk. Mauduit 2002-ben vetette fel híres sejtését miszerint, ha egy $E_N \in \{-1,+1\}^N$ sorozatra $C_2(E_N)$ nagy, akkor $C_3(E_N)$ kicsi. Ezt a sejtést bizonyítottam egy korábbi cikkemben. Az eredményt általánosítottam magasabb rendű mértékekre is, azaz bebizonyítottam, hogyha $2k < 2\ell + 1$, és $C_{2k}(E_N)$ nagy, akkor $C_{2\ell+1}(E_N)$ mindenképpen kicsi. [13]-ban Mauduittal közösen vizsgáltuk a $2k > 2\ell + 1$ esetet. A következő eredményt igazoltuk: Ha

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

akkor

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

ahol az alkalmazott konstansok csak k-tól és ℓ-től függnek.

A [17] cikkben azt vizsgálom, hogy egy adott sorozatnak mikor rendelkeznek a rövid részsorozatai is erős pszeudovéletlen tulajdonságokkal. Dolgozatomban olyan sorozatot konstruáltam, amelyben a rövid részsorozatoknak az

korreláció mértéke is optimális. Ez a kérdés különösen fontos, mert a Vernam-féle titkosító eljárás során fontos, hogy a használt pszeudovéletlen kulcsnak a rövid részsorozatai is erős pszeudovéletlen tulajdonságokkal rendelkezzenek.

A bizonyítás során a következő karakterösszeg becslésre volt szükségem: Legyen p egy páratlan prím, $q = p^2$ és jelöljük γ-val a kvadratikus karaktert $\mathbb{F}_q$ felett. Ekkor $\mathbb{F}_p \subseteq \mathbb{F}_q$. Legyen $I = [a, a+1, a+2, \ldots, b] \subseteq \mathbb{F}_p$ és $f(x) \in \mathbb{F}_q[x]$ egy polinom, amely nem $cg(x)h^2(x)$ alakú, ahol $c \in \mathbb{F}_q$, $g(x) \in \mathbb{F}_p[x]$ és $h(x) \in \mathbb{F}_q[x]$. Tegyük fel, hogy $f(x)$-nek m különböző gyöke van $\overline{\mathbb{F}}_p$ felett. Ekkor

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

$$b) \quad \left| \sum_{x \in I} \gamma(f(x)) \right| \leq 18mp^{1/2} \log p.$$

E tételnek az a) része Vantól származik, míg a b) részt, az „incomplete" esetet cikkemben bizonyítottam.

Bináris rácsok pszeudovéletlen tulajdonságai

[1]-ben Mauduittal és Sárközyvel közösen a bináris sorozatok, illetve bináris rácsok (az előbbiek n-dimenziós általánosításai) pszeudovéletlensége közti kapcsolatot vizsgáltuk. Ugyanis, minden több dimenziós rácshoz egyértelmű módon hozzárendelhetünk egy bináris sorozatot. Dolgozatunkban megmutattuk, hogy az ily módon kapcsolódó rács és sorozat pszeudovéletlen mértékeinek értékei között nincs összefüggés. Vagyis a többdimenziós eset nem vezethető vissza természetes módon az egydimenziós esetre, valóban szükség van a többdimenziós elméletre.

[4]-ben Christian Mauduittal és Sárközy Andrással folytattuk a közös kutatómunkát. Három egydimenziós konstrukciót kiterjesztve, konstrukciókat adtunk erős pszeudovéletlen tulajdonságokkal rendelkező kétdimenziós bináris rácsokra. Az ily módon kapott rácsoknak becsültük a pszeudovéletlen mértékeit.

[5]-ben Sárközyvel és Stewarttal erős pszeudovéletlen tulajdonságokkal rendelkező 2 dimenziós bináris rácsot konstruáltunk kiterjesztve egy korábbi egydimenziós, a Legendre szimbólumra épülő konstrukciót. Becsültük a rács pszeudovéletlen mértékeinek értéket. Habár a kapott becslés nem volt optimális, még mindig lényegesen jobb becslést tudtunk megadni a triviálisnál. [18]-ban folytattuk a közös kutatómunkát, bebizonyítva, hogy az általunk megadott konstrukció speciális esetben megegyezik egy Mauduit és Sárközy által korábban megadott konstrukcióval. Így ebben az esetben a konstrukció egyszerre könnyen implementálható, ugyanakkor optimális becslések adhatóak a pszeudovéletlen mértékekre.

[8], [9], [12] sorozatban társszerzőimmel kétdimenziós bináris rácsok esetében vizsgáltuk a kétdimenziós pszeudovéletlen mértékek tulajdonságait. Így [8]-ban összehasonlítottuk a különböző rendű mértékeket, valamint a normális mértéket a Q_k mértékek maximumával becsültük. [9]-ben új mértékeket vezetünk be bináris rácsok szimmetria tulajdonságainak becslésére. A 3 újonnan definiált mérték közül az egyenes mérték a legáltalánosabb; segítségével a másik két szimmetria mérték is jól becsülhető, kezelhető. Alulról becsültük a szimmetria mértékek minimumát, bebizonyítottuk, hogy nagy valószínűséggel a szimmetria mérték egy adott (a minimumhoz közeli) korlát alatt van. Végül olyan konstrukciókat adunk meg, melyekre a 3 szimmetria mérték mindegyike kicsi. [12]-ben először egydimenzió esetén vizsgáltuk a Q_k mértékek minimumát. Ezután kétdimenziós rácsok esetében bevezettük a korreláció mértéket (C_k), és a C_k, Q_k mértékek minimumát vizsgáltuk.

[11]-ban új pszeudovéletlen mértékeket definiálok bináris rácsok esetében. Az új mértékek sokkal általánosabbak mint az eddig definiált mértékek, és segítségükkel a Q_k mértékek felülről becsülhetőek. Dolgozatomban az új mértékek tulajdonságait vizsgáltam, és olyan konstrukciókat adtam meg, melyekre ezek a mértékek kicsik.

Rácsok kriptográfiai alkalmazása során nem elég, hogy egy bináris rácsnak erős pszeudovéletlen tulajdonságai vannak, fontos az is, hogy a rácsok egy megadott nagy családjában a sorozatok függetlenek legyenek. Az egydimen-

ziós esetben Tóth Viktória vezette be az ütközés és a lavina hatás fogalmát. Ezeket a fogalmakat általánosítottuk [14]-ben a több dimenziós esetre, majd egy, bináris rácsok Legendre szimbólumon alapuló nagy családját vizsgáltuk a fenti szempontokból. [15]-ben folytattuk ezirányú kutatásainkat, bináris rácsoknak egy további nagy családját konstruáltuk, majd itt is megvizsgáltuk mind az ütközés és a lavina hatást, mind a család bonyolultságát.

Egyéb bináris pszeudovéletlen objektumok tulajdonságai

[7]-ban Huberttel és Sárközyvel közösen definiáltuk az r-majdnem s-egyenletes fa fogalmát, majd ilyen fákon definiált bináris függvények pszeudovéletlenségét vizsgáltuk.

Additív problémák

[16]-ban színezési problémákat vizsgáltunk. Schur híres eredménye szerint, az egész számokat k színnel színezve, az $x + y = z$ egyenletnek mindig van egyszínű megoldása. Ezt az eredményt próbáltuk meg kiterjeszteni és vizsgálni különböző esetekben. Egész számoknak, illetve véges testek elemeinek több színnel való színezése esetén vizsgáltuk magasabbfokú, 3 vagy 4 ismeretlenes egyenletek egyszínű megoldásait.

[19]-ben Ruzsa Imrével közösen négyzetszámok között vizsgálunk additív jellegű problémát: Mekkora lehet egy négyzetszámokból álló 3-tagú számtani sorozatot nem tartalmazó halmaz sűrűsége? Megadtunk egy olyan A halmazt, amely része $\{1^2, 2^2, \ldots, N^2\}$-nek, nem tartalmaz 3-tagú számtani sorozatot, valamint az elemszámára

$$|A| \gg \frac{N}{\sqrt{\log \log N}}$$

teljesül.

Hivatkozások

[1] Katalin Gyarmati, Christian Mauduit, András Sárközy, *Pseudorandom binary sequences and lattices*, Acta Arith. 135, 181-197., 2008.

[2] Katalin Gyarmati, *Concatenation of pseudorandom binary sequences*, Periodica Math. Hungar. 58, 99-120, 2009.

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

[4] Katalin Gyarmati, Christian Mauduit, András Sárközy, *Constructions of pseudorandom binary lattices*, Unif. Distr. Theory 4, 59-80, 2009.

[5] Katalin Gyarmati, András Sárközy, Cameron L. Stewart, *On Legendre symbol lattices*, Unif. Distr. Theory 4, 81-95, 2009.

[6] Katalin Gyarmati, *Elliptic curve analogues of a pseudorandom generator*, Period. Math. Hungar., közlésre elfogadva, 2010.

[7] Katalin Gyarmati, Pascal Hubert, András Sárközy, *Pseudorandom binary functions on almost uniform trees*, J. Combin. Number Theory 2, 1-24, 2010.

[8] Katalin Gyarmati, Christian Mauduit, András Sárközy, *Measures of pseudorandomness of finite binary lattices, I (The measures Q_k, normality.)*, Acta Arith. 144, 295-313, 2010.

[9] Katalin Gyarmati, Christian Mauduit, András Sárközy, *Measures of pseudorandomness of binary lattices, III. (Q_k, correlation, normality, minimal values.)*, Unif. Distrib. Theory. 5, 183-207, 2010.

[10] Katalin Gyarmati, *Concatenation of Legendre symbol sequences*, Studia Sci. Math. Hungar. 48, 193-204., 2011.

[11] Katalin Gyarmati, *On new measures of pseudorandomness of binary lattices*, Acta Math. Hung. 131, 346-359, 2011.

[12] Katalin Gyarmati, Christian Mauduit, András Sárközy, *Measures of pseudorandomness of finite binary lattices, II (The symmetry measures.)*, Ramanujan J. 25, 155-178, 2011.

[13] Katalin, Gyarmati, Christian Mauduit, *On the correlation of binary sequences, II*, Discrete Math., közlésre elfogadva, 2011.

[14] Katalin Gyarmati, Christian Mauduit, András Sárközy, *Measures of pseudorandomness of families of binary lattices, I (Definitions, a constructions using quadratic characters.)*, Publi. Math. Debrecen, közlésre elfogadva, 2011.

[15] Katalin Gyarmati, Christian Mauduit, András Sárközy, *Measures of pseudorandomness of families of binary lattices, II (A further construction.)*, Publi. Math. Debrecen, közlésre elfogadva, 2011.

[16] Péter Csikvári, Katalin Gyarmati, András Sárközy, *Density and Ramsey type results on algebraic equations with restricted solution sets*, Combinatorica, közlésre leadva, 2008

[17] Katalin Gyarmati, *On the correlation of subsequences*, Unif. Distrib. Theory, közlésre leadva, 2011.

[18] Katalin Gyarmati, András Sárközy, Cameron L. Stewart, *On Legendre symbol lattices II,* Unif. Distrib. Theory, közlésre leadva, 2011.

[19] Katalin Gyarmati, Imre Ruzsa, *A set of squares without arithmetic progression*, Acta Arith., közlésre leadva, 2011.

[20] Pascal Hubert, Christian Mauduit, András Sárközy, *On pseudorandom binary lattices*, Acta Arith. 125, 51-62 (2006).

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

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