NYILATKOZAT

Név: Gálffy Veronika

ELTE Természettudományi Kar, szak: Matematika

NEPTUN azonosító: OHUR40

Szakdolgozat címe:
Pszeudovéletlen sorozatok és rácsok

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2022. 05. 21.

Gálffy Veronika

a hallgató aláírása

EÖTVÖS LORÁND TUDOMÁNYEGYETEM

TERMÉSZETTUDOMÁNYI KAR

PSZEUDOVÉLETLEN SOROZATOK ÉS RÁCSOK

Szakdolgozat

Gálffy Veronika

Matematika BSc

Alkalmazott matematikus szakirány

Témavezető:

Dr. Gyarmati Katalin

Algebra és Számelmélet Tanszék

Budapest

2022

Tartalomjegyzék

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani témavezetőmnek, Dr. Gyarmati Katalinnak, aki felkeltette érdeklődésemet nem csak e téma, hanem általánosságban a számelmélet iránt is, illetve végig szakmai segítséget nyújtott.

Köszönöm továbbá családomnak és barátaimnak, hogy mellettem álltak és támogattak. Külön köszönet illeti a barátomat, aki egyetemi tanulmányaim során végig hitt bennem és legnagyobb támaszom volt.

1. Bevezetés

1.1. Motiváció

Általában egy számsorozatra akkor mondjuk, hogy pszeudovéletlen, ha statisztikailag véletlennek tűnik, annak ellenére, hogy egy determinisztikus algoritmus által készült. Az, hogy pontosan mit értünk jó pszeudovéletlen sorozat alatt, vagyis milyen tulajdonságokat várunk el tőle, alkalmazástól is függ.

A legtöbb esetben a véletlen szám generálásához használt algoritmus a DRBG (Deterministic Random Bit Generator), melynek először szüksége van egy számra, ún. magra ('seed'), és ettől függően kapunk egy pszeudorandom számot eredményként. Mivel ez egy determinisztikus algoritmus, azaz ugyanabból a magból ugyanazt a számot kapjuk, ezért a magot jól titkosítva kell tárolni. Ma már gyakorlatilag minden számítógépes szoftvernek beépített része egy randomszámtáblázat, ezek többsége számelméleti eszközök felhasználásával készül.

Ahol nagyon fontos a szám vagy sorozat megjósolhatatlansága, szoktak használni fizikai mennyiségeket, például billentyűnyomások közötti időt vagy elektromágneses zajt két állomás közé hangolt rádióból.

A modern számítógépek előtt a tudósoknak egyszerűbb eszközökre kellett hagyatkozniuk, például kockákra, kártyákra, rulettekre, vagy előre elkészített randomszámtáblázatokra.

A véletlen számsorozatok legfontosabb alkalmazásai a numerikus analízishez (pl. Monte-Carlo módszer) és a kriptográfiához kapcsolódnak, melyek közül most a kriptográfián belül a Vernam-rejtjelezést emelem ki. [2], [7]

A dolgozatban a modern (kvantitatív) pszeudovéletlen szám generálásának témakörét járom körbe, főleg az ehhez felhasznált matematikai algoritmusokra koncentrálva.

1.2. A Vernam-rejtjelezés

A Vernam féle titkosítás ('Vernam-cipher') algoritmusát a 20. század elején dolgozta ki Gilbert Vernam. [7] Az algoritmus az adott hosszúságú szöveget egy azonos hosszúságú kulcs segítségével titkosítja a következőképpen:

1.1. Definíció (Gyarmati, Sárközy [7]). *Először a titkosítandó szöveget* $(a_1, \ldots, a_N)$ *bitsoro-*

zat formára hozzuk, ahol $a_i \in \{0,1\}^N \ \forall i$*, majd ehhez hozzárendelünk egy ugyanilyen alakú* $(e_1, \ldots, e_N)$,
$e_i \in \{0,1\}^N \ \forall i$ *(lehetőleg véletlenszerűen, vagy pszeudovéletlen generált) kulcsot. Ezután a szöveget és a kulcsot bitenként összeadjuk modulo* 2 *(másképp: 'XOR' művelet), így egy harmadik* N *hosszúságú* $\{0,1\}$ *sorozatot kapunk, ez a titkosított szöveg (ciphertext).*

Ebből az eredeti szöveget a kulcs és a kód segítségével ugyanilyen módon lehet visszakapni, összeadjuk a két sorozat megfelelő elemeit modulo 2. Biztonságosabb módszert kapunk, hogyha a kód valóban véletlenszerűen van generálva, azaz hogy minden $\{0,1\}^N$ sorozatot azonos $\frac{1}{2^N}$ valószínűséggel választunk (ezt egyszer használatos kulcsnak, vagy 'one time pad'-nek nevezzük). Claude Shannon bizonyította be, hogy ekkor ha a kulcs tökéletesen titokban van tartva és sosincs egynél többször használva, akkor a titkosítás tulajdonképpen megfejthetetlen. [7]

1.2. Példa.

$$\begin{aligned} &(10110) && \leftarrow \text{a kódolandó szöveg} \\ \oplus\ &(00101) && \leftarrow \text{a kulcs} \\ =\ &(10011) && \leftarrow \text{a kapott kódolt szöveg} \end{aligned}$$

2. Pszeudovéletlen sorozatok

A pszeudovéletlen tulajdonság többféleképpen értelmezhető, leginkább attól függően, hogy milyen módon szeretnénk használni az objektumot, ezért több megközelítés létezik a sorozatok konstruálására és tesztelésére is. A sorozat háromféleképpen is kinézhet:

1. sorozatok a $[0, 1)$ intervallumból
2. az $\{1, \dots N\}$ halmazból választott egészek sorozata
3. bináris sorozat.

Itt bináris $\{+1, -1\}$ sorozatokra fogok koncentrálni, ugyanis a három megközelítés kapcsolatban áll egymással, egyikből előállítható a másik és fordítva. A célunk bizonyos ismert sorozatok pszeudorandom tulajdonságainak vizsgálata, és több konstrukció megadása. Ehhez új mértékeket kell bevezetnünk, amelyekkel vizsgálhatjuk a sorozatokat. [14]

A 'Pszeudovéletlen sorozatok' rész Mauduit, Sárközy [14] és Goubin, Mauduit, Sárközy [3] cikkei alapján íródott. A dolgozatban innentől a 'pszeudorandom' szót többször 'PR'-ként rövidítem.

2.1. A pszeudovéletlenség mértékei bináris sorozatokon

Eleinte véges bináris sorozatok pszeudovéletlen tesztelése úgynevezett 'a posteriori' teszteléssel történt, azaz bizonyos jól definiált statisztikai tesztek megmondták, hogy az adott sorozat pszeudovéletlen-e vagy sem. A probléma ezzel az, hogy egy sorozat így csak „rossz" vagy „jó" lehet, nincs a kettő közötti lehetőség, ezért egy flexibilisebb mértékre lesz szükségünk. A legfontosabb véletlen tulajdonságok, melyeket elvárunk egy pszeudovéletlen sorozattól, a következők:

1. normalitás
2. egyenletes eloszlás a számtani sorozatokon
3. kicsi többszörös korreláció

Azt szeretnénk, hogy a mérték tükrözze egy sorozat ezen tulajdonságait. További elvárásaink a PR mértékkel kapcsolatban:

4. Egy sorozat pszeudovéletlensége jellemezhető legyen egy valós értékű, az összes véges bináris sorozaton értelmezett függvénnyel.

5. Ez a mérték legyen kiszámolható legalább a „szebb" sorozatokra. Mivel egyféle mértékkel ezt nehéz megoldani, legyen a 6. követelmény:

6. A mértéknek legyenek különböző szintjei, és legalább az alacsonyabb szintek értékét jól tudjuk közelíteni.

A végtelen hosszú $E = (e_1, e_2, \ldots) \in \{-1, 1\}^\infty$ sorozatokon Mauduit és Sárközy a fenti 1-6 elvárásoknak megfelelő mértékeket vezettek be:

2.1. Definíció (Mauduit, Sárközy [14]). *Minden $k \in \mathbb{N}$, $M \in \mathbb{N}$, $X = (x_1, x_2, \ldots, x_k) \in \{-1, 1, \}^k$, $a \in \mathbb{Z}, b \in \mathbb{N}$, $D = (d_1, \ldots d_k) \in \mathbb{N}^k, d_1 < \ldots < d_k$-re legyen*

$$T(E, M, X) = |\{n : 0 \leq n < M, (e_{n+1}, e_{n+2}, \ldots e_{n+k}) = X\}|,$$

$$U(E, M, a, b) = \sum_{j=1}^{M} e_{a+jb},$$

és

$$V(E, M, D) = \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \ldots e_{n+d_k}.$$

Ekkor E-t normálisnak nevezzük, ha

$$\left| T(E, M, X) - \frac{M}{2^k} \right| = o(M)$$

minden adott k-ra és X-re, ha $M \to \infty$, és a másik két tulajdonságra teljesül, hogy:

$$U(E, M, a, b) = o(M),$$

és

$$V(E, M, D) = o(M)$$

minden adott a, b, D-re, és $M \to \infty$.

Véges sorozatokra az alábbi mértékeket definiálták, szintén az 1-6 elvárásainknak megfelelően:

2.2. Definíció (Mauduit, Sárközy [14]). *1. k-ad rendű normalitás-mérték:*

$$N_k(E_N) = \max_{X \in \{-1,1\}^k} \max_{0 < M \leq N+1-k} |T(E_N, M, X) - \frac{M}{2^k}|.$$

2. Normalitás-mérték:

$$N(E_N) = \max_{k \le (\log N)/\log 2} N_k(E_N)$$

3. Eloszlás-mérték:

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

ahol $a \in \mathbb{Z}$, $b, t \in \mathbb{N}$, *és* $1 \le a + b \le a + tb \le N$.

4. k-ad rendű eloszlás-mérték:

$$C_k(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \dots e_{n+d_k} \right|$$

ahol $D = (d_1, \dots d_k)$, *és M-re* $M + d_k \le N$.

5. Korreláció- mérték:

$$C(E_N) = \max_{k \le \log N/\log 2} C_k(E_N)$$

Ekkor a normalitás és a korreláció között van kapcsolat:

2.3. Állítás (Mauduit, Sárközy [14]). *Minden* N, E_N, *és* $k < N$*-re*

$$N_k(E_N) \le \max_{1 \le t \le k} |C_t(E_N)|$$

Bizonyítás. ([14]) Minden $k, N \in \mathbb{N}$, $X = (x_1, \dots, x_k) \in \{-1, 1\}^k$-ra és $1 \le M \le N + 1 - k$-ra

$$\begin{aligned}
&|T(E_N, M, X) - M/2^k| = \\
&= \left| |\{n : 0 \le n < M,\ (e_{n+1}, e_{n+2}, \dots, e_{n+k}) = X\}| - \frac{M}{2^k} \right| \\
&= \left| \sum_{n=0}^{M-1} \frac{x_1 \dots x_k}{2^k} \prod_{j=1}^{k} (e_{n+j} + x_j) - \frac{M}{2^k} \right| \\
&= \left| \frac{x_1 \dots x_k}{2^k} \sum_{1 \le d_1 < \dots < d_t \le k} \left(\prod_{j \in \{1,\dots,k\} \setminus \{d_1,\dots,d_t\}} x_j \right) \sum_{n=0}^{M-1} e_{n+d_1} \dots e_{n+d_t} \right| \\
&\le \frac{1}{2^k} \sum_{\substack{D \subset \{1,2,\dots,k\} \\ D \ne \emptyset}} |V(E_N, M, D)| \le \frac{1}{2^k} \sum_{t=1}^{k} \binom{k}{t} C_t(E_N) \\
&\le \max_{1 \le t \le k} |C_t(E_N)|.
\end{aligned}$$

□

Tehát ha a korrelációmérték kicsi, akkor a normalitásmérték is az, azonban ez a másik irányban nem feltételnül igaz. Előfordulhat, hogy a normalitás-és eloszlásmérték is kicsi, de a korreláció mégis nagy:

2.4. Példa (Mauduit, Sárközy [14])**.** Legyen az $E_N = (e_1, \dots e_N) \in \{-1, 1\}^N$ olyan sorozat, melyre a normalitás és a korreláció mérték is kicsi, és legyen $E'_{2N} = (e'_1, \dots e'_{2N}) \in \{-1, 1\}^{2N}$ egy másik sorozat, úgy, hogy

$$e'_n = \begin{cases} e_n & \text{ha } 1 \le n \le N, \\ e_{n-N} & \text{ha } N < n \le 2N \end{cases}$$

Ekkor a normalitás-és eloszlásmértéke E'_{2N}-nek lgefeljebb egy konstansszorosa E_N megfelelő mértékének, de

$$C_2(E'_N) \ge \left| \sum_{n=1}^{N} e'_n e'_{n+N} \right| = N.$$

Tehát ahhoz, hogy megmutassuk, hogy egy sorozat pszeudorandom, vagyis rendelkezik a kívánt 1-3 pszeudovéletlen tulajdonságokkal, elég megmutatni, hogy az eloszlás és a korrelációmértéke kicsi, de mindkettőt ellenőrizni kell. Ebből a két mértékből készített Mauduit és Sárközy egy kombinált mértéket:

2.5. Definíció (Mauduit, Sárközy [14])**.** *k-ad rendű kombinált mérték:*

$$Q_k(E_N) = \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \dots e_{a+jb+d_k} \right| = \max_{a,b,t,D} |Z(a, b, t, D)|$$

ahol

$$|Z(a, b, t, D)| = \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \dots e_{a+jb+d_k}$$

minden $a, b, t, D = (d_1, d_2, \dots d_k)$*-ra, úgy, hogy* $a + jb + d_l \in \{1, \dots, N\}$.

kombinált mérték:

$$Q(E_N) = \max_{k \le (\log N)/\log 2} Q_k(E_N)$$

2.6. Példa (Mauduit, Sárközy [14])**.** Legyen az $E_N = (e_1, \dots e_N) \in \{-1, 1\}^N$ sorozat olyan, hogy a korreláció-és eloszlásmértéke is kicsi, és legyen $E'_{2N} = (e'_1, \dots e'_{2N}) \in \{-1, 1\}^{2N}$ olyan sorozat, amelyre:

$$e'_n = \begin{cases} e_n & \text{ha } 1 \le n \le N, \\ e_{2N-n} & \text{ha } N < n \le 2N \end{cases}$$

Ekkor E'_{2N}-nek a korreláció és az eloszlásmértéke legfeljebb konstansszorosa E_N megfelelő mértékének, tehát a kombinált mértéke is kicsi. Ennek alapján tehát a korábbi definíció szerint pszeudorandomnak mondanánk sorozatot, pedig látható, hogy egy igazán véletlen sorozat nem lehetne ennyire szimmetrikus.

A szimmetria vizsgálatára Gyarmati vezette be az ún. szimmetria mértéket [4]. Látható tehát, hogy újabb és újabb mértékek vezethetők be, azonban a gyakorlati alkalmazások azt mutatják, hogy legtöbbször elegendő a W és C_k mértékekre szorítkozni.

2.2. A Legendre-szimbólum pszeudovéletlen tulajdonságai

Meg kell még néznünk, hogy a korábban definiált kombinált mérték alkalmas-e szép sorozatok tesztelésére. Figyeljük meg a Legendre-szimbólumot:

2.7. Tétel (Mauduit, Sárközy [14]). *Létezik olyan p_0, amelyre ha $p > p_0$, p prímszám, $k \in \mathbb{N}, k < p$ és*

$$E_{p-1} = \left(\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \ldots, \left(\frac{p-1}{p}\right)\right),$$

akkor

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

és ha $N = p - 1$, akkor

$$Q(E_N) = \max_{k \leq (\log N)/\log 2} Q_k(E_N) \leq 27N^{1/2}(\log N)^2$$

és

$$Q^*(E_N) = \sum_{k=1}^{\infty} Q_k(E_N)/2^k \leq 33N^{1/2} \log N.$$

Ilyen módon csak kevés jó pszeudorandom sorozatot lehet generálni, holott bizonyos alkalmazásokban, pl. a kriptográfiában, sok sorozatra lesz szükségünk. Megmutatjuk egy módját a több sorozat generálásának:

2.3. Egy másik konstrukció a Legendre-szimbólum segítségével

Hoffstein és Liemann bevezetett egy nagyon általános Legendre szimbólumra és polinomokra alapozott családot [12], ez a következő:

$$N = p-1,\ e_n = \left(\frac{f(n)}{p}\right), E_N = (e_1, e_2, \dots e_N)$$

Azonban Hoffstein és Liemann a sorozatok pszeudovéletlenségéről semmit nem igazolt. Felmerül a kérdés, hogy milyen legyen a konstrukcióhoz használt f polinom? Gaubin, Mauduit és Sárközy megmutatott egy nagy, megfelelő polinomcsaládot, a következő definíciók és jelölések tőlük származnak és a konstrukcióhoz szükségesek:

2.8. Definíció (Gaubin, Mauduit, Sárközy [3]). *Ha $M \in \mathbb{N}$, és $\mathscr{A}, \mathscr{B} \subset \mathbb{Z}_m$ és $\mathscr{A} + \mathscr{B}$-ben $\mathbb{Z}_m$ minden eleme páros multiplicitással fordul elő, azaz minden $c \in \mathbb{Z}_m$-re*

$$a + b = c, a \in \mathscr{A}, b \in \mathscr{B}$$

megoldásainak száma páros (beleértve azt az esetet is, amikor nincs megoldás), akkor az $\mathscr{A} + \mathscr{B}$ összegre azt mondjuk, hogy rendelkezik a P tulajdonsággal.

2.9. Definíció (Gaubin, Mauduit, Sárközy [3]). *Ha $k, l, m \in \mathbb{N}$ és $k, l \leq m$, akkor a (k, l, m) számhármast* megengedett hármasnak *nevezzük, ha nincs olyan $\mathscr{A}, \mathscr{B} \subset \mathbb{Z}_m$, hogy $|\mathscr{A}| = k, |\mathscr{B}| = l$, és $\mathscr{A} + \mathscr{B}$ rendelkezik a P tulajdonsággal.*

Gaubin, Mauduit és Sárközy a következőt igazolták:

2.10. Tétel (Gaubin, Mauduit, Sárközy [3]). *Legyen p prímszám, és $f(x) \in \mathbb{F}_p$ k-ad fokú, úgy, hogy nincs többszörös gyöke $\overline{\mathbb{F}_p}$-ben. Ekkor ha az $E_p = (e_1, \dots e_p)$ sorozatot úgy definiáljuk, hogy*

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

akkor

(i)

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

(ii) *ha $l \in \mathbb{N}$-re az (r, l, p) számhármas megengedett minden $r \leq k$-ra, akkor*

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

Bizonyítás. (i) Legyen $a \in \mathbb{Z},\ b, t \in \mathbb{N}$, úgy, hogy teljesül rájuk

$$1 \leq a \leq a + (t-1)b \leq p, \tag{2.2}$$

és legyen $g(x) = f(a + bx)$, vagyis $g(x) \in \mathbb{F}_p[x]$.
A $g(x)$ definíciója miatt a $g(x) \equiv 0 \pmod{p}$ kongruenciának legfeljebb k darab megoldása lehet, így ha $(\frac{a}{p})$-t 0-nak definiáljuk abban az esetben, amikor $p|a$, akkor

$$|U(E_p, t, a, b)| = \left|\sum_{j=0}^{t-1} e_{a+jb}\right| \leq \left|\sum_{j=0}^{t-1} \left(\frac{f(a+jb)}{p}\right)\right| + k = \left|\sum_{j=0}^{t-1} \left(\frac{g(j)}{p}\right)\right| + k.$$

Látható, hogy f és g azonos fokúak, és ha f $\overline{\mathbb{F}_p}$-beli szorzattá bontva

$$f(x) = c(x - x_1)\dots(x - x_k),$$

ahol $x_i \neq x_j$, ha $i \neq j$, akkor

$$g(x) = f(a + bx) = cb^k(x - b^{-1}(x_1 - a))\dots(x_b^{-1}(x_k - a)),$$

vagyis g(x)-nek szintén nincsen többszörös gyöke. A következőkben szükségünk lesz az alábbi lemmára, mely A. Weil tételének egy következménye:

2.11. Tétel (Weil [18])**.** *Legyen p egy prímszám, χ egy d-ed rendű, mod p (nem triviális) karakter, $f(x) \in \mathbb{F}_p[x]$ (ahol $\mathbb{F}_p$ a modulo p maradékosztályok teste) k-ad fokú és a faktorizációja: $f(x) = b(x - x_1)^{d_1}...(x - x_s)^{d_s}$ (ahol $x_i \neq x_j$ ha $i \neq j$) $\overline{\mathbb{F}_p}$-beli ($\mathbb{F}_p$ lezártja), és*

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

Legyen X, Y valós, úgy, hogy $0 < Y \leq p$. Ekkor

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

A 2.11-es tételt felhasználva, rendre $(\frac{n}{p})$-t, 2-t és $g(n)$-et írva $\chi(n), d$ és $f(n)$ helyébe, kapjuk, hogy

$$|U(E_p, t, a, b)| = \left|\sum_{j=0}^{t-1} \left(\frac{g(j)}{p}\right)\right| + k < 9kp^{1/2}\log p + k < 10kp^{1/2}\log p.$$

(ii) Írjuk át $f(x)$-et $f(x) = bf_1(x)$ alakba, ahol f_1 főegyütthatója 1, és $b \in \mathbb{Z}_p$. Minden $d_1, \dots d_l$ egészre és $M \in \mathbb{N}$-re, ha feltesszük, hogy

$$0 \leq d_1 < \ldots < d_l, \quad M + d_l \leq p, \tag{2.3}$$

akkor a

$$f(n + d_i) \equiv 0 \ (mod\ p), \quad 1 \leq n \leq M, 1 \leq i \leq l$$

kongruenciának legfeljebb kl darab megoldása van. Ekkor ha $(\frac{0}{p})$-t itt is 0-nak definiáljuk, a következőt kapjuk:

$$\begin{aligned} V(E_p, M, D) &= \left| \sum_{n=1}^{M} e_{n+d_1} \dots e_{n+d_l} \right| \leq \\ &\leq \left| \sum_{n=1}^{M} \left(\frac{f(n+d_1)}{p} \right) \left(\frac{f(n+d_2)}{p} \right) \dots \left(\frac{f(n+d_l)}{p} \right) \right| + kl = \\ &= \left| \left(\frac{b^l}{p} \right) \sum_{n=1}^{M} \left(\frac{f_1(n+d_1) f_1(n+d_2) \dots f_1(n+d_l)}{p} \right) \right| + kl \end{aligned}$$

Legyen $h(n) = f_1(n+d_1) f_1(n+d_2) \dots f_1(n+d_l)$. A következő lemmát fogjuk felhasználni, melynek bizonyítása megtalálható [3]-ban:

2.12. Lemma (Gaubin, Mauduit, Sárközy [3])**.** *Ha f, k, l a 2.10-es tétel szerint vannak definiálva, akkor $h(x)$-nek van legalább egy páratlan multiplicitású gyöke $\overline{\mathbb{F}_p}$-ben.*

Így tehát a 2.11-es tétel feltétele teljesül $\left(\frac{n}{p}\right)$, 2, és $h(x)$-re χ, d és f(x) helyében, vagyis a tételt felhasználva kapjuk, hogy (mivel $h(x)$ foka kl)

$$|V(E_p, t, a, b)| \leq \left| \sum_{n=1}^{M} \left(\frac{h(n)}{p} \right) \right| + kl < 9kl p^{1/2} \log p < 10kl p^{1/2} \log p$$

minden $d_1, \dots d_l$, M-re, ami teljesíti (2.3)-at. Ezzel a tétel állítását igazoltuk. [3] □

2.4. Elégséges feltétel a megengedettségre, jó prímek

Ahhoz, hogy használhassuk a 2.10-es tételt, szükségünk van megengedett számhármasokra. Egy elégséges feltétel a megengedettségre a következő:

2.13. Tétel (Gaubin, Mauduit, Sárközy [3]). *(i) Minden p prímre és $k \in \mathbb{N}, k < p$-re a $(k, 2, p)$ megengedett.*

(ii) Ha p prím, $k, l \in \mathbb{N}$ és

$$(4l)^k < p. \tag{2.4}$$

akkor (k, l, p) megengedett.

(iii) Ha p olyan prím, hogy a 2 primitív gyök modulo p, akkor minden $k, l \in \mathbb{N}$ pár, amire $k < p, l < p$, a (k, l, p) hármas megengedett.

Az (iii) tulajdonság segítségével tehát kontrollálhatjuk a magas rendű korrelációkat is, ha van sok olyan p prím, amire a 2 primitív gyök mod p.

Hogy jobban megértsük a megengedettség fogalmát, és ellenkezőjére is kapjunk egy elégséges feltételt, tovább vizsgáljuk a megengedett hármasokat. Ehhez egy újabb definíció:

2.14. Definíció (Gaubin, Mauduit, Sárközy [3]). *Egy pozitív egész m számra azt mondjuk, hogy jó, ha minden $k, l \in \mathbb{N}$ párra, ahol $k < m, l < m$, a (k, l, m) számhármas megengedett.*

A következő tétel bizonyításának segítségével könnyen mutathatunk majd példát nem megengedett számhármasokra és $\mathscr{A} + \mathscr{B}$ összegekre, amik rendelkeznek a P tulajdonsággal:

2.15. Tétel (Gaubin, Mauduit, Sárközy [3]). *Egy páratlan p prím akkor és csak akkor jó, ha a 2 primitív gyök modulo p.*

Bizonyítás. Bármely $\mathscr{C} \subset \mathbb{Z}_p$-re definiáljuk a $P_{\mathscr{C}}(X) \in \mathbb{F}_2[X]$ polinomot a következőképpen:

$$P_{\mathscr{C}}(X) = \sum_{c \in \mathscr{C}} X^{s(c)},$$

ahol $s(c)$ jelöli a c maradékosztály modulo p legkisebb nemnegatív elemét.

Minden $u \in \mathbb{Z}_p$-re a $P_{u+\mathscr{C}}(X)$ polinom egyenlő $X^u P_{\mathscr{C}}(X)$ maradékával modulo $(1 + X^p)$ $F_2[X]$-ben. Emiatt bármely $\mathscr{A}, \mathscr{B} \subset \mathbb{F}_p$-re az $\mathscr{A} + \mathscr{B}$ összeg akkor és csak akkor rendelkezik a P tulajdonsággal, ha $(1 + X^p)$ osztja $P_{\mathscr{A}}(X) P_{\mathscr{B}}(X)$-et $\mathbb{F}_2[X]$-ben.

Ha $1 + X + \ldots + X^{p-1}$ reducibilis $\mathbb{F}_2[X]$-ben, akkor írjuk át

$$1 + X + \ldots + X^{p-1} = P_1(X) P_2(X)$$

alakba, ahol $2 \leq \deg P_i \leq p-3,\ i = 1, 2$-re (elsőfokú polinomok nem osztják az $1 + X + \ldots + X^{p-1}$ polinomot $\mathbb{F}_2[X]$-ben). Ha $\mathscr{A}, \mathscr{B}$-t úgy definiáljuk, hogy

$$P_1(X) = \sum_{a \in \mathscr{A}} X^{s(a)}$$

és

$$(1+X)P_2(X) = \sum_{b \in \mathscr{B}} X^{s(b)},$$

akkor láthatjuk, hogy az $\mathscr{A} + \mathscr{B}$ összeg rendelkezik a P tulajdonsággal, vagyis p nem jó prím. Ellenben ha $1 + X + \ldots + X^{p-1}$ irreducibilis $\mathbb{F}_2[X]$-ben, akkor bármely olyan $\mathscr{A}, \mathscr{B} \subset \mathbb{Z}_p$-re, melyre $\mathscr{A} + \mathscr{B}$ rendelkezik a P tulajdonsággal, az $1 + X + \ldots + X^{p-1}$ polinomnak osztania kell vagy $P_{\mathscr{A}}(X)$-et vagy $P_{\mathscr{B}}(X)$-et, amiből következik, hogy $\mathscr{A} = \mathbb{Z}_p$ vagy $\mathscr{B} = \mathbb{Z}_p$, vagyis p egy jó prím.

Tehát tudjuk, hogy egy p prím akkor és csak akkor jó, ha a $1 + X + \ldots + X^{p-1}$ polinom irreducibilis $\mathbb{F}_2[X]$-ben.

Ismert tétel a körosztási polinomokról (lásd pl [15] 2.4 tétel, 65. o.), hogy a $1 + X + \ldots + X^{p-1}$ polinom $\frac{p-1}{d}$ darab azonos d fokú polinom szorzatára bomlik $\mathbb{F}_2[X]$-ben, ahol d az a legkisebb pozitív egész, melyre $2^d \equiv 1 \mod p$. Ebből látszik, hogy a p prím akkor és csak akkor jó, ha a 2 primitív gyök modulo p, ami a bizonyítandó állítás. [3] □

2.16. Példa (Gaubin, Mauduit, Sárközy [3]). Legyen $p = 17$ (2 nem primitív gyök modulo 17, tehát a tétel szerint lesz olyan $(k, l, 17)$ számhármas, ami nem megengedett). Bontsuk fel $1 + x^{17}$-ent a következőképp $F_2[x]$-ben: $(1 + x + x^3 + x^6 + x^8 + x^9)(1 + x + x^2 + x^4 + x^6 + x^7 + x^8)$. Ekkor ha $\mathscr{A} = \{0, 1, 3, 6, 8, 9\}$ és $\mathscr{B} = \{0, 1, 2, 4, 6, 7, 8\}$ akkor $\mathscr{A} + \mathscr{B}$ rendelkezik a P tulajdonsággal, azaz a $(6, 7, 17)$ és a $(7, 6, 17)$ számhármasok nem megengedettek.

2.5. Az algoritmus

A 2.10-es tételből és a 2.13 tétel (i) részéből következik:

2.17. Következmény (Gaubin, Mauduit, Sárközy [3]). *Ha p, f, k, E_p a 2.10-es tétel alapján vannak definiálva, akkor*

$$W(E_p) < 10kp^{1/2} \log p \tag{2.5}$$

és

$$C_2(E_p) < 20kp^{1/2}\log p. \tag{2.6}$$

Tehát az eloszlás és a másodrendű korrelációmérték mindig elég kicsi. Ha magasabb rendű korrelációmértéket is szeretnénk, hogy biztosan kicsi legyen, a 2.10-es tételt a 2.13 tétel (ii) és (iii) részével kell kombinálnunk:

2.18. Következmény (Gaubin, Mauduit, Sárközy [3])**.** *Ha p, f, k, E_p a 2.10 tétel szerint vannak definiálva, és legalább valamelyik a kettő közül teljesül:*

(i) a 2 primitív gyök modulo p

(ii) igaz a következő:

$$l < \frac{p^{1/4}}{4}, \tag{2.7}$$

akkor (2.5) *és*

$$C_l(E_p) < 10klp^{1/2}\log p \tag{2.8}$$

is teljesül.

A 2.18-as következmény alapján az algoritmusunk adott p prím hosszúságú PR sorozat generálására:

Algoritmus (Gaubin, Mauduit, Sárközy [3])**.** Adott egy p prím, a sorozat hossza, és egy $L \in \mathbb{N}$, melyre:

$$L < \begin{cases} p & \text{minden } p\text{-re} \\ \frac{p}{4} & \text{ha a 2 nem primitív gyök modulo } p \end{cases}$$

Tfh. a sorozat l-ed rendű korrelációmértékét szeretnénk korlátozni minden $l \leq L$-re.

Legyen $L < p$ nagy, de hogyha a 2 nem primitív gyök modulo p, akkor (mivel a 2.13 tétel (ii) feltételének teljesülni kell) legyen olyan, hogy

$$k < \frac{\log p}{\log(4L)}. \tag{2.9}$$

Legyen $t = [k/2]$, és tekintsük a következő alakban adott $g(x) \in \mathbb{F}_p$ polinomokat:

$$g(x) = x^k + \sum_{i=0}^{t} a_i x^i, \tag{2.10}$$

ahol $a_i \in \mathbb{Z}_p$ minden $i = 0, 2, \ldots, t-1$-re, és $a_t \in \mathbb{Z}_p \backslash 0$.

Legyen $d(x)$ a $g(x)$ és $g'(x)$ polinomok legnagyobb közös osztója, és legyen

$$f(x) = \frac{g(x)}{d(x)} \tag{2.11}$$

Az ezekkel az értékekkel adott 2.10 tétel szerinti pszeudorandom sorozatot kiszámolva egy jó sorozatot kapunk, ugyanis:

Az f(x) polinomnak nincsen többszörös gyöke, mivel így alkottuk meg (2.11)-ben, a foka pedig $\deg(f(x)) \leq \deg(g(x)) = k$.

Továbbá $l \leq L < p$ minden p-re, és ha 2 nem primitív gyök modulo p, akkor $l \leq L < \frac{1}{4}p^{1/4}$ a (2.9)-es feltevés miatt, vagyis a 2.13 tétel feltételei teljesülnek, ezért a kívánt (2.5) és (2.8) pszeudovéletlen tulajdonságok is.

3. Pszeudovéletlen rácsok

A 'Pszeudovéletlen rácsok' rész Gyarmati, Sárközy, Stewart [10] és [11] cikkei és Hubert, Mauduit, Sárközy [13] cikke alapján készült.

3.1. Definíció és mérték

Hasonlóan a sorozatokhoz, pszeudovéletlen rácsokat használhatunk a kriptográfiában, ha nem egy szöveget, hanem esetleg egy térképet, fényképet kell titkosítani. A sorozatok analógiájára működik így is a Vernam cipher, csak a szöveg karakterei helyett például a kép pixeleit titkosítjuk. A kulcs pedig egy véletlen bináris rács. Hubert, Mauduit és Sárközy vezette be a következő definíciókat [13]:

Legyen I_N^n azoknak az n dimenziós vektoroknak a halmaza, melyeknek minden koordinátája 0 és $N-1$ közötti egész szám:

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

I_N^n-t n-dimenziós N-rácsnak, vagy röviden N-rácsnak nevezzük. Ezt a definíciót általánosíthatjuk a következőképpen: Legyenek $\mathbf{u}_1, \ldots \mathbf{u}_n$ lineárisan független n dimenziós vektorok úgy, hogy minden $\mathbf{u}_i$ vektornak egyedül az i. koordinátája nem nulla, a többi nulla. Azaz $\mathbf{u}_i = (0, \ldots, 0, z_i, 0, \ldots, 0)$. Legyenek $t_1, \ldots, t_n$ egészek, úgy, hogy $0 \leq t_1, \ldots, t_n < N$. Definiáljuk a B_N^n halmazt:

$$B_N^n = \{\mathbf{x} = (x_1\mathbf{u}_1 + \ldots + x_n\mathbf{u}_n) \ : 0 \leq x_i|\mathbf{u}_i| \leq t_i \ \forall \ i \in \{1, \ldots, n\}\}$$

Ekkor B_N^n-t n-dimenziós N-téglarácsnak, vagy röviden N-téglarácsnak nevezzük. Hubert, Mauduit, Sárközy a sorozatok esetét a következőféleképpen terjesztette ki több dimenzióra [13]:

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

Az egyszerűség kedvéért $\eta(\mathbf{x}) = \eta((x_1, \ldots, x_n))$ helyett $\eta(x_1, \ldots, x_n)$-et írunk. Szemléletesen az $\mathbf{x}$ vektor helyén (a "koordinátáit" adja meg a rácsban) az $\eta(\mathbf{x})$ szám, azaz +1 vagy -1 ('+' vagy '-' karakter) áll.

Hubert, Mauduit, Sárközy a következő mértéket definiálta rácsokra:

3.1. Definíció (Hubert, Mauduit, Sárközy [13]). *Legyen*

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

Ekkor η-nak az l-ed rendű pszeudorandom mértéke:

$$Q_l(\eta) = \max_{B,\boldsymbol{d}_1,\dots,\boldsymbol{d}_l} \left| \sum_{\boldsymbol{x}\in B} \eta(\boldsymbol{x}+\boldsymbol{d}_1)\dots(\boldsymbol{x}+\boldsymbol{d}_l) \right|$$

ahol $\boldsymbol{d}_1,\dots \boldsymbol{d}_l \in I_N^n$, és B téglarács, úgy, hogy $B+\boldsymbol{d}_1,\dots B+\boldsymbol{d}_l \subseteq I_N^n$

Egy triviális felső becslés Q_l-re adott N,n,l esetén N^n. Egy bináris rács jó pszeudovéletlen rács, ha $Q_l(\eta)$ ennél jelentősen kisebb. Ilyen rácsot a sorozatokhoz hasonlóan a Legendre-szimbólum segítségével tudunk készíteni.

3.2. Degenerált polinomok, konstrukció

Gyarmati, Sárközy és Stewart először a következő konstrukció tulajdonságait vizsgálta:

3.2. Konstrukció (Gyarmati, Sárközy, Stewart [10]). Legyen p páratlan prím, $f(x_1,x_2) \in \mathbb{F}_p[x_1,x_2]$ kétváltozós polinom, és $\eta \ : \ I_p^2 \ \to \ \{-1,+1\}$:

$$\eta(x_1,x_2) = \begin{cases} \left(\frac{f(x_1,x_2)}{p}\right), & \text{ha } (f(x_1,x_2),p)=1, \\ +1, & \text{ha } p \mid f(x_1,x_2). \end{cases} \tag{3.1}$$

A következő példák azt mutatják, hogy van néhány f polinom, amire biztosan nagy lesz $Q_l(\eta)$:

3.3. Példa (Gyarmati, Sárközy, Stewart [10]). Ha

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

ahol $c \in \mathbb{F}_p$, $f(x_1,x_2) \in \mathbb{F}_p[x_1,x_2]$, akkor a (3.1) szerint definiált η rács minden eleme $\left(\frac{c}{p}\right)$ lesz, kivéve f gyökeit. Vagyis ha f foka nem nagyon magas (nincsen sok gyöke), akkor $Q_1(\eta)$ nagy.

3.4. Példa (Gyarmati, Sárközy, Stewart [10]). Ha $f(x_1,x_2) = g(x_1)$, ahol $g(x) \in \mathbb{F}_p[x]$, akkor

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

kivéve $g(x)$ gyökeire. Vagyis hasonlóan, $Q_2(\eta)$ nagy.

3.5. Példa (Gyarmati, Sárközy, Stewart [10]). Ha $f(x_1, x_2) = g(x_1)h(x_2)$, ahol $g(x), h(x) \in \mathbb{F}_p[x]$, akkor megmutatható, hogy $Q_4(\eta)$ nagy.

A példákban szereplő f polinomok mind a következő eset egyszerűbb változatai:

3.6. Definíció (Gyarmati, Sárközy, Stewart [10]). *Egy $f(x_1, x_2)$ polinomra azt mondjuk, hogy* degenerált, *ha felírható a következő formában:*

$$f(x_1, x_2) = \left(\prod_{j=1}^{r} f_j(\alpha_j x_1 + \beta_j x_2) \right) (g(x_1, x_2))^2, \tag{3.2}$$

ahol $\alpha_j, \beta_j \in \mathbb{F}_p$, $f_j(x) \in \mathbb{F}_p[x]$ $\forall\, j \in \{1, \ldots, r\}$.

A korábbi példák mutatják, hogy ha egy polinom ilyen alakú, akkor lehet, hogy valamelyik hozzá tartozó $Q_l(\eta)$ nagy. A következő tételt mondta ki és bizonyította Gyarmati, Sárközy és Stewart a csak nemdegenerált polinomok esetéről (ez egy kiterjesztése a Goubin, Mauduit és Sárközy által f-re adott egydimenziós feltételnek [3], mely garantálja a generált sorozat jó PR tulajdonságait):

3.7. Tétel (Gyarmati, Sárközy, Stewart [10]). *Legyen $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ k-ad fokú polinom. Tegyük fel, hogy f nem degenerált, és hogy a következő feltételek közül teljesül legalább egy:*

1. $f(x_1, x_2)$ irreducibilis $\mathbb{F}_p[x_1, x_2]$-ben,

2. $l = 2$,

3. a 2 primitív gyök modulo p,

4. $4^{k+l} < p$

5. l és $f(x_1, x_2)$ foka valamelyik változójában páratlan.

Ekkor az (3.1) szerint definiált η-ra és a hozzá tartozó p-rácsra igaz, hogy:

$$Q_l(\eta) \leq 11klp^{3/2} \log p. \tag{3.3}$$

3.3. Degenerált polinomok vizsgálata

Vizsgáljuk meg, hogy mi mondható degenerált polinomok használata esetén. Kiderül, hogy a degenerált polinomok (konstans szorzótól és sorrendtől eltekintve) egyértelmű alakra hozhatóak az alábbi módon [11]:

Legyen a T halmaz $\mathbb{F}_p \times \mathbb{F}_p$ egy részhalmaza:

$$T = \{(0,1),(1,0),(1,1),(2,1),\ldots,(p-1,1)\},$$

Ekkor Gyarmati, Sárközy, Stewart a következő tételt mondták ki:

3.8. Tétel (Gyarmati, Sárközy, Stewart [11]). *Legyen f egy nem konstans, x_1-ben és x_2-ben is kevesebb, mint p-ad fokú $\mathbb{F}_p[x_1,x_2]$-beli polinom. Ekkor létezik $\lambda \in \mathbb{F}_p$, $\lambda \neq 0$, r nemnegatív egész, különböző $(\gamma_1,\delta_1),\ldots,(\gamma_r,\delta_r) \in T$, $\psi \in \mathbb{F}_p[x_1,x_2]$, és $\varphi_1,\ldots,\varphi_r$ négyzetmentes (azaz egyiküknek sincsen olyan osztója, mely egy nem konstans polinom négyzete) $\mathbb{F}_p[x]$-beli polinomok, és ezekre teljesül:*

$$f(x_1,x_2) = \lambda \left(\prod_{j=1}^{r} \varphi_j(\gamma_j x_1 + \delta_j x_2) \right) (\psi(x_1,x_2))^2 \tag{3.4}$$

ahol (a,b)-ben a reprezentálja az a maradékosztályt modulo p, és b hasonlóan.
Itt r egyértelmű, és $\varphi_j(\gamma_j x_1 + \delta_j x_2)$ és $\psi(x_1,x_2)$ a konstans szorzótól és a φ_j függvények sorrendjétől eltekintve egyértelmű. A tétel bizonyítása [11]-ben megtalálható.
Az f polinom (3.4) szerinti alakját a normál alakjának nevezzük, r-et a rangjának.

Azt már láttuk, hogy ha a polinom nem degenerált, akkor Q_l kicsi. Azonban ez akkor is teljesül, ha a polinom degenerált, de l kicsi:

3.9. Tétel (Gyarmati, Sárközy, Stewart [11]). *Legyen $f(x_1,x_2) \in \mathbb{F}_p[x_1,x_2]$ k-adfokú polinom, a* (3.4) *szerinti alakban. Tegyük fel, hogy l nem nagyobb, mint f rangja, azaz r, és a következő 5 feltétel közül legalább egy teljesül:*

1. $f(x_1,x_2)$ irreducibilis $\mathbb{F}_p[x_1,x_2]$-ben,

2. $l = 2$,

3. a 2 primitív gyök modulo p,

4. $(4k)^l < p$, vagy $(4l)^k < p$,

5. l és $f(x_1,x_2)$ foka valamelyik változójában páratlan.

Ekkor a (3.1) *szerint definiált η-ra és a hozzá tartozó p-rácsra igaz, hogy:*

$$Q_l(\eta) \leq 11klp^{3/2}\log p.$$

A tétel bizonyítása szintén megtalálható [11]-ben. Tehát azt már tudjuk, hogy ha $l < r$, akkor Q_l kicsi, de ha l nagyobb, akkor mit tudunk mondani a konstrukcióról degenerált polinomokkal? Biztos, hogy nem teljesül rájuk valamilyen hasonló jó felső becslés?

Gyarmati, Sárközy és Stewart tétele azt mondja ki, hogy van olyan $l \leq 2^r$, amire $Q_l(\eta)$ nagy:

3.10. Tétel (Gyarmati, Sárközy, Stewart [11]). *Legyen $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ r-ed rangú polinom, melynek foka x_1, x_2-ben rendre m, n. Ekkor létezik olyan pozitív egész $l \leq 2^r$, amire:*

$$Q_l(\eta) \geq p^2 - 4rp^{3/2} - 2l(m+n)p.$$

Már tudunk egy felsőbecslést degenerált polinomok esetére is, azonban még így is kedvezőbb nem degenerált polinomok használata a konstrukcióhoz. Gyarmati, Sárközy és Stewart adott egy konstrukciót nemdegenerált polinomok készítésére, és belátott egy felsőbecslést is az ezekkel készült rácsok PR mértékére:

3.11. Tétel (Gyarmati, Sárközy, Stewart [11]). *Legyen $f(x_1, x_2) \in \mathbb{F}[x_1, x_2]$ olyan polinom, mely felírható a következő alakban:*

$$f(x_1, x_2) = x_1^k + x_1 x_2 g(x_1, x_2) + x_2 h(x_2), \tag{3.5}$$

ahol $g \in \mathbb{F}_p[x_1, x_2]$, deg $g \leq k-3$, $h(x) \in \mathbb{F}_p[x]$, deg $h \leq k-2$, és x_2 nem osztója $h(x_2)$ − nek. Ekkor a (3.1) *szerint definiált η bináris rácsra:*

$$Q_l(\eta) \leq 11klp^{3/2} \log p.$$

Bizonyítás. A bizonyításhoz szükségünk lesz egy lemmára, a Schönemann-Eisenstein kritérium egy általánosítására:

3.12. Lemma. *Ha $f(x) = a_n x^n + \ldots + a_1 x + a_0$ polinom egy R integritási tartomány (nullosztómentes kommutatív gyűrű) felett, és $\mathfrak{a}$ R egy maximális ideálja. Ha*

$$\begin{aligned} a_n &\not\equiv 0 \pmod{\mathfrak{a}} \\ a_{n-1} \equiv \ldots \equiv a_0 &\equiv 0 \pmod{\mathfrak{a}} \\ a_0 &\not\equiv 0 \pmod{\mathfrak{a}^2}, \end{aligned}$$

akkor $f(x)$ R[x]-ben nem bontható nemkonstans polinomok szorzatára.

Bizonyítása megtalálható [17]-ben a 282. tételnél.

Az $R = \mathbb{F}_p[x_2]$ egy integritási tartomány, amiben $\mathfrak{a} =< x_2 >$ egy maximális ideál. Ekkor a lemma feltételei teljesülnek a (3.5) szerint alkotott $f(x_1, x_2) \in R[x_1]$ polinomra, azaz $f(x_1, x_2)$ irreducibilis.

Így ahhoz, hogy használhassuk a 3.7 tételt, azt kell még belátnunk, hogy f nem degenerált (mert az 5 feltétel egyike már teljesül, az irreducibilitás), és a tétel egyértelműen következik. Mivel f irreducibilis, ezért a normálalakja is speciális kell, hogy legyen. Azt kell belátnunk, hogy f nem írható fel az alábbi formában:

$$f(x_1, x_2) = f_1(\alpha_1 x_1 + \beta_1 x_2)$$

Tegyük fel, hogy mégis felírható így. Legyen ekkor h az f_1 foka, és vegyük külön a pontosan h-ad fokú tényezőket:

$$f_1(\alpha_1 x_1 + \beta_1 x_2) = c(\alpha_1 x_1 + \beta_1 x_2)^h + f_2(\alpha_1 x_1 + \beta_1 x_2),$$

ahol f_2 foka $\leq h-1$, és $c \neq 0 \in \mathbf{F}_p$. A $c(\alpha_1 x_1 + \beta_1 x_2)^h$ tag csak az f-nek a k-ad fokú tagjainak összege lehet, azaz

$$c(\alpha_1 x_1 + \beta_1 x_2)^h = x_1^k.$$

Feltehetjük, hogy $k < p$, mert különben az állítás rögtön következik. A fentiekből következik, hogy $h = k$, $c = \alpha_1 = 1$ és $\beta_1 = 0$, azaz

$$f(x_1, x_2) = f_1(x_1)$$

Azonban f-et úgy alkottuk meg, hogy abban mindenképpen van x_2-nek egy hatványa, ez pedig ellentmond ennek. Vagyis f nem írható fel a (3.4) szerinti normálalakban, azaz nem degenerált polinom. Azt is beláttuk, hogy az így alkotott f irreducibilis, így a 3.7 tétel alapján teljesül a tétel állítása. [11]

□

3.4. Konstrukció kvadratikus karakter segítségével

A Legendre-szimbólum felhasználásával készített rácsok előnye, hogy egy természetesebb, gyorsabb előállításmódot adnak, azonban az így kapott rácsok pszeudovéletlen mértékére a felső korlát nagy, ennél lehet jobbat elérni a véges testek és karakterek segítségével. Ennek egy változata a következő tétel, mely a Mauduit és Sárközy [16]-os cikkének 1. és 2. tételének kombinálásából következik:

3.13. Tétel (Mauduit, Sárközy [16])**.** *Legyen p egy páratlan prím, $n \in \mathbb{N}$, $q = p^n$, és jelölje γ az $\mathbb{F}_q$ kvadratikus karakterét ($\gamma(0) = 0$). Tekintsük az $\mathbb{F}_q$ elemei által $\mathbb{F}_p$ felett alkotott lineáris*

vektorteret, és legyen ennek egy bázisa $v_1, \ldots, v_n$. Legyen $f(x) \in \mathbb{F}_q[x]$ k-ad fokú polinom, aminek nincs többszörös gyöke $\overline{\mathbb{F}}_q$ úgy, hogy

$$0 < k < p. \tag{3.6}$$

Definiáljuk az $\eta(\boldsymbol{x}) : \ I_p^n \ \rightarrow \ \{ -1, 1 \}$ n dimenziós bináris p-rácsot a következőféleképpen:

$$\begin{aligned} \eta(x) &= \eta((x_1, \ldots, x_n)) = \\ &= \begin{cases} \gamma(f(x_1 v_1 + \ldots + x_n v_n)), & ha\ f(x_1 v_1 + \ldots + x_n v_n) \neq 0 \\ 1, & haf(x_1 v_1 + \ldots + x_n v_n) = 0 \end{cases} \end{aligned} \tag{3.7}$$

Tegyük fel, hogy $l \in \mathbb{N}$-re teljesül, hogy

$$4^{n(k+l)} < p. \tag{3.8}$$

Ekkor

$$Q_l(\eta) \leq kl \left(q^{1/2} (1 + \log p)^n + 2 \right) \tag{3.9}$$

A következő tétel a 3.13 tételből következik, az $n = 2$ esetben, v_1, v_2 és f speciális választásával, és segítségével kombinálhatjuk a két módszert azoknak az előnyeivel együtt: optimális felső becslést kapunk és lévén egy Legendre-szimbólum konstrukció, gyorsan és egyszerűen implementálható.

3.14. Tétel (Gyarmati, Sárközy, Stewart [11])**.** *Legyen p egy páratlan prím, r egy kvadratikus nem-maradék modulo p. Ekkor az $x^2 - r$ polinom irreducibilis $\mathbb{F}_p$-ben. Jelöljük az egyik gyökét θ-val, és tekintsük $\mathbb{F}_p$ θ-val való kiterjesztését: $\mathbb{F}_p[\theta]$. Legyenek k és l egészek, melyekre teljesül (3.6) és (3.8).*
Legyenek $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{F}_p$, és tegyük fel, hogy teljesül rájuk, hogy

$$a_i + b_i\theta \neq a_j + b_j\theta, \text{ és } a_i + b_i\theta \neq a_j - b_j\theta, \text{ ahol } 1 \leq i < j \leq k. \tag{3.10}$$

Legyen

$$\tilde{f}(x_1, x_2) = \prod_{i=1}^{k} \left((x_1 - a_i)^2 - r(x_2 - b_i)^2 \right)$$

és

$$\tilde{\eta}(\boldsymbol{x}) = \tilde{\eta}((x_1, x_2)) = \begin{cases} \left(\frac{\tilde{f}(x_1, x_2)}{p} \right), & ha \quad (\tilde{f}(x_1, x_2), p) = 1, \\ 1, & ha \quad p \mid \tilde{f}(x_1, x_2) \end{cases}$$

Minden l pozitív egészre, amelyre teljesül, hogy

$$4^{2(l+k)} < p$$

igaz, hogy

$$Q_l(\eta) \leq lk\left(p(1+\log p)^2+2\right).$$

Bizonyítás. θ definíciója és az Euler-lemma miatt

$$\theta^p = (\theta^2)^{\frac{p-1}{2}}\theta = r^{\frac{p-1}{2}}\theta = -\theta \tag{3.11}$$

Az előző, 3.13 tételt alkalmazzuk $n = 2$ esetben, úgy, hogy $q = p^2$, $v_1 = 1, v_2 = \theta$. Így $\mathbb{F}_q = \mathbb{F}_{p^2}$ elemei $x_1 + x_2\theta$ formában írhatóak. Ekkor az Euler-lemma $\mathbb{F}_q$-ra történő általánosítása és (3.11) miatt minden $x_1 + x_2\theta \in \mathbb{F}_{p^2}^*$ -re, ahol $(x_1, x_2) \neq 0$

$$\begin{aligned}
\gamma(x_1+x_2\theta) &= (x_1+x_2\theta)^{\frac{p^2-1}{2}} = (x_1+x_2\theta)^{\frac{p^2-p}{2}}(x_1+x_2\theta)^{\frac{p-1}{2}} = \\
&= ((x_1+x_2\theta)^p)^{\frac{p-1}{2}}(x_1+x_2\theta)^{\frac{p-1}{2}} = (x_1^p + x_2^p\theta^p)^{\frac{p-1}{2}}(x_1+x_2\theta)^{\frac{p-1}{2}} = \\
&= (x_1-x_2\theta)^{\frac{p-1}{2}}(x_1+x_2\theta)^{\frac{p-1}{2}} = (x_1^2 - x_2^2\theta^2)^{\frac{p-1}{2}} = (x_1^2 - rx_2^2)^{\frac{p-1}{2}} = \\
&= \left(\frac{x_1^2 - rx_2^2}{p}\right)
\end{aligned} \tag{3.12}$$

Az $f(x_1 + x_2\theta)$-t a következőképp definiáljuk:

$$f(x_1+x_2\theta) = \prod_{i=1}^{k}((x_1+x_2\theta) - (a_i+b_i\theta))$$

Ekkor γ és a Legendre-szimbólum multiplicitása miatt, ha $\eta(\mathbf{x}) = \eta((x_1, x_2))$ (3.7) alapján, akkor

$$\begin{aligned}
\eta(\mathbf{x}) &= \gamma(f(x_1+x_2\theta)) = \gamma\left(\prod_{i=1}^{k}((x_1+x_2\theta)-(a_i+b_i\theta))\right) \\
&= \prod_{i=1}^{k}\gamma((x_1+x_2\theta)-(a_i+b_i\theta)) = \prod_{i=1}^{k}\gamma((x_1-a_i)+(x_2-b_i)\theta) \\
&= \prod_{i=1}^{k}\left(\frac{(x_1-a_1)^2 - r(x_2-b_i)^2)}{p}\right) = \left(\frac{\prod_{i=1}^{k}((x_1-a_1)^2 - r(x_2-b_i)^2)}{p})\right) = \\
&= \left(\frac{\tilde{f}(x_1,x_2)}{p}\right) = \tilde{\eta}(\mathbf{x}), \qquad (\text{ahol } f(x_1+x_2\theta) \neq 0)
\end{aligned} \tag{3.13}$$

a korábban definiált $\tilde{f}$, $\tilde{\eta}$-val. Ha $f(x_1 + x_2\theta) = 0$, akkor is

$$\eta(\mathbf{x}) = \tilde{\eta}(\mathbf{x}). \tag{3.14}$$

A (3.10) feltétel és r definíciója miatt $\tilde{f}$-nek nincs többszörös gyöke, (3.8)-t pedig feltettük, hogy teljesül $n = 2$-re. Így a 3.7 tételt használhatjuk, (3.13) és (3.14) miatt (3.9)-ból következik a tétel állítása. [11] □

Megjegyezzük, hogy a tétel használatához szükségünk van egy r kvadratikus nem-maradékra modulo p, és ennek determinisztikus keresése elvben nehézséget okozhat (valószínűségi módszereket használva gyorsan találunk kvadratikus nem-maradékot). Az általános Riemann-sejtésből következik, hogy a legelső kvadratikus nem-maradék modulo p kisebb, mint $(\log p)^c$, és egy adott maradék kvadratikus karakterét ki tudjuk számolni polinomidőben, azaz így az első kvadratikus maradék megtalálása is menne polinomidőben. Azonban olyan módszer eddig nem ismert, ami végig bizonyított állításokra alapul. Ezt meg lehet kerülni, ha nem egy konkrét adott p-hez keresünk r-t, hanem p-t kicsit rugalmasabban mi adjuk meg. Ha $p = 4k - 1$ alakú, akkor tudjuk, hogy az $r = -1$ kvadratikus nem-maradék. Állítsunk össze tehát egy listát $4k - 1$ alakú prímekből, és ha például egy N nagyságrendű $4k - 1$ alakú prímre van szükségünk, akkor válasszuk a listából a legkisebb olyat, ami már nála nagyobb, és ahhoz $r = -1$-et. $4k - 1$ alakú prímek például a Mersenne-prímek. [11]

4. Sorozatok és rácsok közötti összefüggések vizsgálata

A rácsok és sorozatok pszeudovéletlen tulajdonságai közötti összefüggést vizsgáljuk. Egy már adott rácsból könnyen készíthetünk sorozatot, úgy, hogy sorban vesszük egymás mögé a rács első sorát, majd a következőt, és így tovább. A kérdés az, hogy vajon ha az ilyen módon alkotott sorozatnak jók a pszeudovéletlen tulajdonságai, akkor a rácsé is jó lesz-e? Rácsot úgy is készíthetünk, hogy minden sora egy-egy különböző pszeudovéletlen sorozat. Jó pszeudovéletlen rács lesz-e, amit így kapunk? Általánosabban, vissza lehet-e vezetni valahogyan a több dimenziós esetet az egydimenziósra? Ez jelentősen leegyszerűsítené a helyzetünket, hiszen többdimenziós rács konstruálása láttuk, hogy lényegesen bonyolultabb, mint a sorozaté. Ha ez igaz lenne, ilyen módon egy jó, egyszerűbben megkonstruálható sorozatot véve, és azt ráccsá alakítva egy jó pszeudovéletlen rácsot kapnánk. Sajnos azonban ez nem így van, ezt fogjuk belátni, és mutatunk néhány példát. Ez a rész Gyarmati, Mauduit és Sárközy [6] cikke alapján készült.

4.1. Rácsok, melyek sorai különböző jó PR sorozatok

Gyarmati, Mauduit és Sárközy először azt az esetet vizsgálták, amikor több jó pszeudovéletlen sorozatból készítünk rácsot, úgy, hogy a rács sorai a sorozatok. A következő fogalmak és jelölések tőlük származnak [6]:

Legyenek ezek a sorozatok $E_N^{(1)}, E_N^{(2)}, \dots E_N^{(N)}$, és az η rács j. sora $E_N^{(j)}$, azaz

$$\eta((i, j-1)) = e_{i+1}^{j} \quad \text{minden } j = 1, 2, \dots N \text{ és } i = 0, 1, \dots N\text{-re.} \tag{4.1}$$

Persze hogyha nagyon összefüggenek ezek a sorozatok, például $E_N^{(1)} = E_N^{(2)} = \dots = E_N^{(N)}$, akkor a rács sem lehet eléggé pszeudovéletlen, ezért tehát szeretnénk feltenni, hogy a sorozatok között kicsi az összefüggés, például közel ortogonálisak (a skaláris szorzatuk kicsi):

$$|E_N^{(i)}, E_N^{(j)}| = |e_1^{(i)} e_1^{(j)} + e_2^{(i)} e_2^{(j)} + \dots e_N^{(i)} e_N^{(j)}| \text{ kicsi} \tag{4.2}$$

minden $1 \le i < j \le N$-re.

Gyarmati, Mauduit és Sárközy belátták, hogyha $E_N^{(1)}, E_N^{(1)}, \dots E_N^{(N)}$ jó sorozatok, és (4.2) is teljesül, abból még nem következik, hogy a fenti módon definiált η rács is jó pszeudovéletlen rács:

4.1. Tétel (Gyarmati, Mauduit, Sárközy [6]). *Legyen p prímszám, és definiáljuk $j = 1, 2, \dots p$-re az $E_p^{(j)}$ sorozatokat a következőképpen:*

$$e_i^{(j)} = \begin{cases} \left(\frac{i+j}{p}\right) & ha\ p \nmid i+j \\ +1 & ha\ p \mid i+j \end{cases} \tag{4.3}$$

Ezután definálunk az η rácsot 4.1 szerint, vagyis

$$\eta((x,y)) = \begin{cases} \left(\frac{x+y+2}{p}\right) & ha\ p \nmid x+y+2 \\ +1 & ha\ p \mid x+y+2 \end{cases}$$

Ekkor $k \in \mathbb{N}$-re és $j = 1, 2, \dots p$-re teljesül, hogy

$$Q_k(E_p^{(j)}) < 10kp^{1/2}\log p \tag{4.4}$$

és

$$|E_p^{(i)}, E_p^{(j)}| < 4p^{1/2}, \quad \forall\, 1 \le i < j \le p, \tag{4.5}$$

viszont

$$Q_2(\eta) \ge (p-1)^2. \tag{4.6}$$

Bizonyítás. Jelöljük $\mathbb{F}_p$ kvadratikus karakterét χ^*-gal:

$$\chi^*(n) = \begin{cases} \left(\frac{n}{p}\right) & \text{ha } p \nmid n, \\ +1, & \text{ha } p \mid n. \end{cases}$$

Ekkor

$$\begin{aligned} Q_k(E_p^{(j)}) &= \max_{a,t,\underline{D}} \left| \sum_{i=0}^{t} e_{ia+d_1}^{(j)} \dots e_{ia+d_k}^{(j)} \right| \\ &\le \max_{a,t,\underline{D}} \left(\left| \sum_{\substack{0\le i\le t \\ p\nmid (j+ia+d_1)\dots(j+ia+d_k)}} \left(\frac{(j+ia+d_1)\dots(j+ia+d_k)}{p} \right) \right| \right. \\ &\quad \left. + \sum_{\substack{0\le i\le t \\ p\mid (j+ia+d_1)\dots(j+ia+d_k)}} 1 \right) \\ &\le \max_{a,t,\underline{D}} \left(\left| \sum_{i=0}^{t} \chi^*((j+ia+d_1)\dots(j+ia+d_k)) \right| + k \right), \end{aligned}$$

amiből a 2.11 tétel miatt következik (4.4). A sorozatok távolságára teljesül minden $1 \leq i < j \leq p$-re, hogy

$$|(E_p^{(i)}, E_p^j)| = \left|\sum_{l=1}^{p} e_l^{(i)} e_l^{(j)}\right| \leq \left|\sum_{\substack{1\leq l\leq p \\ p\nmid (l+i)(l+j)}} \left(\frac{(l+i)(l+j)}{p}\right)\right| + \sum_{\substack{1\leq l\leq p \\ p\mid (l+i)(l+j)}} 1$$

$$\leq \left|\sum_{l=1}^{p} \chi^*((l+i)(l+j))\right| + 2 \tag{4.7}$$

Weil tétele miatt az első szumma $\leq 2p^{1/2}$, és innen következik (4.5). Végül $Q_k(\eta)$ definíciójából következik, hogy

$$Q_2(\eta) \geq \left|\sum_{j_1=0}^{p-2}\sum_{j_2=1}^{p-1} \eta((j_1,j_2)+(0,0))\eta((j_1,j_2)+(+1,-1))\right|$$

$$= \left|\sum_{j_1=0}^{p-2}\sum_{j_2=1}^{p-1} \eta((j_1,j_2))\eta((j_1+1,j_2-1))\right|. \tag{4.8}$$

Mivel

$$\eta((j_1,j_2))\eta((j_1+1,j_2-1)) = \left(\frac{j_1+j_2+2}{p}\right)\left(\frac{j_1+j_2+2}{p}\right)$$

$$= +1, \text{ha } p \nmid j_1+j_2+2 \tag{4.9}$$

és

$$\eta((j_1,j_2))\eta((j_1+1,j_2-1)) = (+1)(+1) = +1, \text{ha } p \mid j_1+j_2+2$$

ezért (4.8) alapján

$$Q_2(\eta) \geq \sum_{j_1=0}^{p-2}\sum_{j_2=1}^{p-1} 1 = (p-1)(p-1) = (p-1)^2,$$

ami pont (4.6) állítás, azaz ezzel a tételt beláttuk. [6] □

4.2. Rácsok, melyek sorai egy jó PR sorozat részsorozatai

Itt azt az esetet vizsgáljuk, amikor egy N^2 hosszú jó PR sorozatból készítünk egy N-rácsot, először a rács első sorát véve, majd a másodikat, és hasonlóan, mindegyikhez hozzárendeljük a PR sorozat egy részsorozatát. A következő jelölések és fogalmak Gyarmati, Mauduit és Sárközy [6] cikkéből származnak:

Minden 2 dimenziós N rácshoz

$$\eta(\underline{x}) : I_N^2 \to \{-1, +1\}$$

egyértelműen hozzá tudunk rendelni egy N^2 hosszú bináris sorozatot: $E_{N^2} = E_{N^2}(\eta) = (e_1, e_2, \dots e_{N^2})$. Vagyis általánosan:

$$e_{iN+j} = \eta((j-1, i)) \; \forall \; 0 \leq i \leq N-1, \; 1 \leq j \leq N. \tag{4.10}$$

Felmerül a kérdés, hogyha E_{N^2} jó PR sorozat, akkor vajon η is jó PR rács-e? Vagyis igaz-e, hogy a jó PR sorozatok egyben egy jó PR rácsot is generálnak? Meg fogjuk mutatni, hogy van olyan rács, amire E_{N^2} kicsi, de a rács megfelelő PR-mértéke mégis nagy, vagyis sajnos ez nem igaz.

E_{N^2} mértékeit W, C_k, Q_k-val fogjuk jelölni, az η rács mértékeit pedig a könnyebb olvashatóság érdekében $\overline{Q}_k$-val. Gyarmati, Mauduit és Sárközy az alábbi tételt mondta ki az elsőrendű mértékekről, vagyis $Q_1 = W$-ről és $\overline{Q}_1$-ről:

4.2. Tétel (Gyarmati, Mauduit, Sárközy [6])**.** *Minden $N = 2R \in \mathbb{N}$ páros számra létezik η bináris rács, amire $W(E_{N^2})$ kicsi:*

$$W(E_{N^2}) < 4N, \tag{4.11}$$

azonban $\overline{Q}_1$ nagy:

$$\overline{Q}_1(\eta) > \frac{1}{2}N^2 \tag{4.12}$$

Bizonyítás. Legyen az η N-rács a következőképp definiálva:

$$\eta((i,j)) = \begin{cases} +1 & \text{ha } i = 0, 1, \dots R-1, \text{és } j = 0, 1, \dots N-1 \\ -1 & \text{ha } i = R, R+1, \dots N-1, \text{és } j = 0, 1, \dots N-1 \end{cases}$$

Azt fogjuk belátni, hogy η-ra teljesül (4.11) és (4.12).
A W mérték definíciója:

$$Q_1(E_{N^2(\eta)}) = W(E_{N^2}(\eta)) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|$$

ahol a maximum olyan a, b, t felett keresendő, amikre $1 \leq a \leq a + (t-1)b \leq N^2$. Vegyük ezeknek a szummáknak az egyikét: $\sum_{j=0}^{t-1} e_{a+jb}$. Ekkor léteznek olyan $u.v$ egészek, amikre:

$$\begin{gathered} 0 \leq u \leq v \leq N-1, \\ a \in (uN, uN+N] \\ a + (t-1)b \in (vN, vN+N] \end{gathered} \tag{4.13}$$

Ekkor

$$\sum_{j=0}^{t-1} e_{a+jb} = \sum_{\substack{0\le j\le t-1 \\ a+jb\in(uN,(u+1)N]}} e_{a+jb} + \sum_{u<w<v} \sum_{\substack{0\le j\le t-1 \\ a+jb\in(wN,(w+1)N]}} e_{a+jb} + \sum_{\substack{0\le j\le t-1 \\ a+jb\in(vN,(v+1)N]}} e_{a+jb} \tag{4.14}$$

Látható, hogy

$$\left| \sum_{\substack{0\le j\le t-1 \\ a+jb\in(uN,(u+1)N]}} e_{a+jb} \right| \le \sum_{a+jb\in(uN,(u+1)N]} 1 \le N, \tag{4.15}$$

$$\left| \sum_{\substack{0\le j\le t-1 \\ a+jb\in(vN,(v+1)N]}} e_{a+jb} \right| \le \sum_{a+jb\in(vN,(v+1)N]} 1 \le N, \tag{4.16}$$

és minden $u < w < v$-re η és E_{N^2} definíciója szerint

$$\begin{aligned}
&\left| \sum_{j:\ a+jb\in(wN,(w+1)N]} e_{a+jb} \right| = \left| \sum_{j:\ a+jb\in(wN,wN+R]} \eta((a+jb-wN-1,w)) \right| \\
&+ \left| \sum_{j:\ a+jb\in(wN+R,(w+1)N]} \eta((a+jb-wN-1,w)) \right| \\
&= \left| \sum_{j:\ a+jb\in(wN,wN+R]} 1 \right| + \left| \sum_{j:\ a+jb\in(wN+R,(w+1)N]} 1 \right| \\
&= ||\{m : m \equiv a \mod b, wN < m \le wN+R| \\
&- |\{m : m \equiv a \mod b, wN+R < m \le (w+1)N||| \\
&= |(|\{m : m \equiv a \mod b, wN \le m \le wN+R| - R/b) \\
&- (\,|\{m : m \equiv a \mod b, wN+R \le m \le (w+1)N\}| - R/b)| \\
&\le 1+1 = 2.
\end{aligned} \tag{4.17}$$

Azaz (4.15), (4.16) és (4.17) alapján

$$\sum_{j=0}^{t-1} e_{a+jb} \le N + 2(v-u-1) + N < 4N,$$

ami bizonyítja (4.11)-et. Ezen kívül

$$\overline{Q}_1(\eta) \geq \left| \sum_{j_1=0}^{R-1} \sum_{j_2=0}^{N-1} \eta((j_1, j_2)) \right| = \sum_{j_1=0}^{R-1} \sum_{j_2=0}^{N-1} 1 = RN = \frac{1}{2}N^2,$$

amiből pedig (4.12) következik. Ezzel tehát a tételt igazoltuk. [6] □

Láttuk, hogy ha E_{N^2}-nek csak az elsőrendű mértékét követeljük meg, hogy kicsi legyen, abból még nem feltétlenül lesz jó rács. Próbálkozhatunk másodrendű mérték szabályozásával is, azt fogjuk látni, hogy sajnos ebből sem következik, hogy a rács PR rács lenne:

4.3. Tétel (Gyarmati, Mauduit, Sárközy [6]). *Minden $N = 2R \in \mathbb{N}$ páros számhoz létezik η bináris rács, amire $Q_1(E_{N^2})$ és $C_2(E_{N^2})$ kicsi:*

$$Q_1(E_{N^2}(\eta)) = W(E_{N^2}(\eta)) < 6N(\log N)^{1/2},$$

és

$$C_2(E_{N^2}(\eta)) < 12N(\log N)^{1/2},$$

de mégis, $\overline{Q}_2(\eta)$ nagy:

$$\overline{Q}_2(\eta) \geq \frac{1}{4}N^2$$

A 4.3 tételben láttuk, hogy ha $C_2(E_{N^2})$ kicsi, attól még $\overline{Q_2}(\eta)$ lehet nagy. Az ellenkezője azonban nem lehetséges:

4.4. Tétel (Gyarmati, Mauduit, Sárközy [6]). *Minden η N-rácsra és $k \in \mathbb{N}$-re teljesül, hogy*

$$Q_k(E_{N^2}(\eta)) \leq 3N(\overline{Q_k}(\eta))^{1/2}$$

5. Sorozat-és rácscsaládok kombinált keresztezett mértéke, tulajdonságai

A korábban bemutatott konstrukciókkal ugyan garantáltan jó PR sorozatot vagy rácsot kapunk, a gyakorlatban sok különböző jó sorozatra és rácsra lesz szükségünk. Először a sorozatok esetét vizsgálva: olyan sorozatcsaládokat szeretnénk kapni, amik struktúrája gazdag, komplex, elég "függetlenek" benne a sorozatok. Ez a rész Gyarmati [5] cikke alapján készült.

5.1. Sorozatcsaládok

A sorozatcsaládok vizsgálatára vezette be Ahlswede, Khachatrian, Mauduit és Sárközy [1] a családkomplexitás (family-complexity, röviden: f-complexity) fogalmát:

5.1. Definíció (Ahlswede, Khachatrian, Mauduit, Sárközy [1]). *Az $\mathcal{F}$ bináris sorozatcsalád ($E_N \in \{-1,1\}^N$) családkomplexitása az a legnagyobb j egész szám, amire teljesül, hogy minden $\epsilon_1, \epsilon_2, \dots \epsilon_j \in \{-1,+1\}$-re létezik legalább egy $E_N \in \mathcal{F}$, ami teljesíti a következőt:*

$$e_{i_1} = \epsilon_1, \ \dots, \ e_{i_j} = \epsilon_j, (1 \leq i_1 < \dots < i_j \leq N).$$

Jelölés: $\Gamma(\mathcal{F})$. *Ha nincs ilyen* $j \in \mathbb{N}$, *akkor* $\Gamma(\mathcal{F}) = 0$.

Gyarmati bevezetett egy általános, kombinált mértéket sorozatcsaládokra, mely a Gyarmati, Mauduit, Sárközy által definált [9] egydimenziós keresztkombinált mérték természetes kiterjesztése több dimenzióra:

5.2. Definíció (Gyarmati [5]). *Legyen $N, l \in \mathbb{N}$, és minden $E_N^{(1)}, E_N^{(2)}, \dots E_N^{(l)}$ bináris sorozatra, ahol*

$$E_N^{(i)} = \left(e_1^{(i)}, e_2^{(i)}, \dots e_N^{(i)}\right) \in \{-1,+1\}^N \ \forall i = 1,2,\dots,l$$

és minden $M \in \mathbb{N}, D = (d_1, d_2, \dots d_l)$-re, ahol $0 \leq d_1 < d_2 < \dots < d_l < M + d_l \leq N$, és d_i egész minden $i = 1,2,\dots l$-re, legyen

$$V_l\left(E_N^{(1)}, E_N^{(2)}, \dots E_N^{(l)}, M, D\right) = \sum_{n=1}^{M} e_{n+d_1}^{(1)} e_{n+d_2}^{(2)} \dots e_{n+d_l}^{(l)}.$$

Definiáljuk $\tilde{C}_l$-t a következő módon:

$$\tilde{C}_l\left(E_N^{(1)},\dots E_N^{(l)}\right)=\max_{M,D}\left|V_l\left(E_N^{(1)},\dots E_N^{(l)},M,D\right)\right|,$$

ahol a maximumot minden $D=(d_1,d_2,\dots d_l), M\in\mathbb{N}$-re keressük, úgy hogy $0\le d_1<\dots<d_l<M+d_l\le N$, és ha $E_N^{(i)}=E_N^{(j)}$ valamilyen $i\neq j$-re, akkor $d_i\neq d_j$. Ekkor az $\mathcal{F}$ bináris sorozatcsalád keresztezett kombinált mértéke*:*

$$\Phi_l(\mathcal{F})=\max\tilde{C}_l\left(E_N^{(1)},\dots E_N^{(l)}\right),$$

ahol a maximumot minden olyan $\left(E_N^{(1)},\dots E_N^{(l)}\right)$ l tagú rendezett listán keressük, ahol $E_N^{(i)}\in\mathcal{F}\ \forall i=1,\dots,l$.

Célunk ennek a keresztezett-kombinált mértéknek magasabb dimenzióra való kiterjesztése.

5.2. Rácscsaládok

Rácsok esetében hasonló a kérdés, olyan rácscsaládokat szeretnénk konstruálni, ahol az egyes rácsok külön-külön is jó PR rácsok, de azt is szeretnénk, hogy a család struktúrája "gazdag", komplex legyen, sok egymástól "független" ráccsal. Erre vezetett be Gyarmati, Mauduit és Sárközy [9] új tulajdonságokat, családmértékeket:

5.3. Definíció (Gyarmati, Mauduit, Sárközy [9])**.** *Tegyük fel, hogy egy η bináris rácsokból álló $\mathcal{G}$ rácscsalád a következő alakú*

$$\mathcal{G}=\mathcal{G}(\mathcal{S})=\{\eta_s:\ s\in\boldsymbol{S}\},$$

ahol $\boldsymbol{s}$ egy adott halmaz, melynek minden eleméhez egyértelműen hozzá van rendelve egy η_s rács. Ekkor ha bármely $s\in\boldsymbol{S}$-re s-et $s'\neq s$-re cserélve $\eta_s: I_N^n\to\{-1,+1\}$-nek sok eleme megváltozik, akkor azt mondjuk, hogy a $\mathcal{G}=\mathcal{G}(\boldsymbol{S})$ család rendelkezik a lavina tulajdonsággal*. Ha bármely $s,s'\in\mathcal{S}, s\neq s'$-re legalább $\left(\frac{1}{2}-o(1)\right)N^n$ eleme különbözik η_s-nek és $\eta_{s'}$-nek, akkor azt mondjuk, hogy $\mathcal{G}$ rendelkezik a* szigorú lavina tulajdonsággal*.*

5.4. Definíció (Gyarmati, Mauduit, Sárközy [9])**.** *Ha $n,N\in\mathbb{N},\eta: I_N^n\to\{-1,1\},\eta': I_N^n,$ $\to\{-1,+1\}$, akkor a $d(\eta,\eta')$ távolság η és η' között*

$$d(\eta,\eta')=|\{x_1,x_2,\dots x_n):(x_1,\dots x_n)\in I_N^n,\ \eta(x_1,\dots x_n)\neq\eta'(x_1,\dots x_n)\}|.$$

Ha $\mathcal{G}$ bináris rácsok egy családja, akkor az $m(\mathcal{G})$ távolságminimumot a következőképp definiáljuk:

$$m(\mathcal{G}) = \min_{\substack{\eta,\eta' \in \mathcal{G} \\ \eta \neq \eta'}} d(\eta, \eta').$$

Azt mondjuk, hogy $\mathcal{G}$ ütközésmentes, *ha $m(\mathcal{G}) > 0$, és akkor rendelkezik a szigorú lavina tulajdonsággal, ha*

$$m(\mathcal{G}) \geq \left(\frac{1}{2} - o(1)\right) N^n. \tag{5.1}$$

Gyarmati kiterjesztette a keresztkombinált mérték fogalmát magasabb dimenzióra:

5.5. Definíció (Gyarmati [5])**.** *Legyen $N, l \in \mathbb{N}$, és bármely $\eta_1, \eta_2, \dots \eta_l$ bináris N-rácsra, azaz:*

$$\eta_i : I_N^n \to \{-1, +1\}^N \quad \forall i = 1, 2, \dots, l,$$

és bármely B téglarácsra és $D = (\boldsymbol{d}_1, \boldsymbol{d}_2, \dots \boldsymbol{d}_l)$ l elemű rendezett listára, úgy, hogy $\boldsymbol{d}_i \in I_N^n \quad \forall i = 1, \dots l$, legyen

$$V_l(\eta_1, \eta_2, \dots \eta_l, B, D) = \sum_{x \in B} \eta_1(\boldsymbol{x} + \boldsymbol{d}_1) \dots \eta_l(\boldsymbol{x} + \boldsymbol{d}_l), \tag{5.2}$$

illetve

$$\tilde{Q}_l(\eta_1, \dots \eta_l) = \max_{B,D} V_l(\eta_1, \eta_2, \dots \eta_l, B, D) \tag{5.3}$$

ahol a maximumot minden $D = (d_1, \dots d_l)$ és olyan B téglarács felett nézzük, amire igaz, hogy $B + \boldsymbol{d}_1, B + \boldsymbol{d}_2, \dots B + \boldsymbol{d}_l \subseteq I_N^n$, azzal a megkötéssel, hogy ha $\eta_i = \eta_j$ valamilyen $i \neq j$-re, akkor $\boldsymbol{d}_i \neq \boldsymbol{d}_j$. Ekkor a $\mathcal{G}$, $\eta \in \{-1, +1\}^N \quad \forall \eta \in \mathcal{G}$ rácscsalád keresztkombinált mértéke

$$\Phi_l(\mathcal{G}) = \max \tilde{Q}_l(\eta_1, \dots \eta_l), \tag{5.4}$$

ahol a maximumot minden $(\eta_1, \dots \eta_l)$ rendezett listán keressük, ahol $\eta_i \in \mathcal{G} \quad \forall i = 1, \dots l$.

A $\tilde{Q}_l$ definíciója miatt $\tilde{Q}_l(\eta, \dots \eta) = Q_l(\eta)$, amiből rögtön következik (5.4) alapján, hogy

5.6. Állítás (Gyarmati [5])**.**

$$\Phi_l(\mathcal{G}) \geq \max_{\eta \in \mathcal{G}} Q_l(\eta).$$

Tehát ha van egy jó felső határunk $\Phi_l(\mathcal{G})$-re, az garantálja, hogy minden $\mathcal{G}$-beli rács jó PR tulajdonságokkal rendelkezik.

Ezután Gyarmati a keresztkombinált mérték más családmértékekkel való kapcsolatát vizsgálta:

5.7. Állítás (Gyarmati [5]). *Ha $n, N \in \mathbb{N}$, és $\mathcal{G}$ bináris rácsoknak egy nagy családja, $\eta \in \mathcal{G}$: $I_N^n \to \{-1, 1\}$, akkor minden $\eta_1, \eta_2 \in \mathcal{G}$-re*

$$\left| d(\eta_1, \eta_2) - \frac{N^n}{2} \right| \leq \frac{1}{2} \tilde{Q}_2(\eta_1, \eta_2) \leq \frac{1}{2} \Phi_2(\mathcal{G}). \tag{5.5}$$

Bizonyítás. A definícióból nyilvánvalóan

$$d(\eta_1, \eta_2) = \sum_{\mathbf{x} \in I_N^n} \frac{(\eta_1(\mathbf{x}) - \eta_2(\mathbf{x}))^2}{4} = \frac{N^n}{2} - \frac{1}{2} \sum_{\mathbf{x} \in I_N^n} \eta_1(\mathbf{x}) \eta_2(\mathbf{x}),$$

amiből (5.2), (5.3), (5.4) alapján

$$\left| d(\eta_1, \eta_2) - \frac{N^n}{2} \right| = \frac{1}{2} \left| \sum_{\mathbf{x} \in I_N^n} \eta_1(\mathbf{x}) \eta_2(\mathbf{x}) \right| \leq \frac{1}{2} \tilde{Q}_2(\eta_1, \eta_2) \leq \frac{1}{2} \Phi_2(\mathcal{G}),$$

ami bizonyítja az 5.7 állítást. [5] □

Ha a $\mathcal{G}$ család keresztkombinált mértéke $o(N^n)$, akkor a távolságminimum 5.4 definíciója és (5.5) miatt

$$m(\mathcal{G}) = \min_{\substack{\eta, \eta' \in \mathcal{G} \\ \eta \neq \eta'}} d(\eta, \eta') \geq \frac{N^n}{2} - \frac{1}{2} \Phi_2(\mathcal{G}) = \frac{N^n}{2} - o(N^n),$$

azaz (5.1) teljesül, ami bizonyítja a alábbi állítást:

5.8. Állítás (Gyarmati [5]). *Ha $n, N \in \mathbb{N}$ és $\mathcal{G}$ bináris $\eta : I_N^n \to \{-1, 1\}$ rácsok egy családja, és $\Phi_2(\mathcal{G}) = o(N^n)$, akkor a $\mathcal{G}$ család rendelkezik a szigorú lavina tulajdonsággal.*

5.3. Kvadratikus karakter segítségével készült bináris rácscsaládok keresztkombinált mértéke

Mauduit és Sárközy kidolgozott egy konstrukciót jó PR tulajdonságokkal rendelkező bináris rácsok létrehozására kvadratikus karakterek segítségével. Az ezen módon készült rácsok PR mérékére egy felső korlátot is beláttak, ez a korábban itt már említett 3.13 tétel [16]. Gyarmati az eszerint készült bináris rácscsaládok keresztkombinált mértékét, családmértékét vizsgálta, és ehhez bevezette az alábbi egyszerűbb jelöléseket [5] (előre lefixált $p, n, q = p^n$-re) :

5.9. Konstrukció. Jelölje $\mathcal{P}_{\leq K}$ a $q < \deg f \leq K$-ad fokú f polinomokat, melyek főegyütthatója egy. Legyen $\mathcal{G}_{\leq K,kvadratikus}$ a 3.13 tétel szerint definiált $f \in \mathcal{P}_{\leq K}$ polinomokhoz tartozó η bináris rácsok családja.

Minden $\eta \in \mathcal{G}_{\leq K,kvadratikus}$ rács, amely teljesíti a 3.13 tétel feltételeit, jó PR tulajdonságokkal rendelkezik.

A jelölések egyszerűsítése érdekében bevezetünk egy új függvényt [5]: $\tau : \mathbb{F}_p^n \to \mathbb{F}_q$. Feltehetjük, hogy I_p^n reprezentálja $\mathbb{F}_p^n$ összes elemét, így τ-t úgy is tekinthetjük, mint $\tau : I_p^n \to \mathbb{F}_q$. Legyen $v_1, \dots v_n$ $\mathbb{F}_q$ egy bázisa $\mathbb{F}_p$ fölött a 3.13 szerint definiálva. Egy $\mathbf{x} = (x_1, \dots x_n) \in \mathbb{F}_p^n$-re legyen

$$\tau(\mathbf{x}) = x_1 v_1 + \dots x_n v_n.$$

Ekkor τ egy bijekció. Szintén teljesül, hogy **a, b** $\in \mathbb{F}_p^n$-re $\tau(\mathbf{a+b}) = \tau(\mathbf{a}) + \tau(\mathbf{b})$. Ekkor (3.7) írható a 3.13-as tételben így is:

$$\eta(\mathbf{x}) = \begin{cases} \gamma(f(\tau(\mathbf{x}))) & \text{ha} f(\tau(\mathbf{x})) \neq 0, \\ +1 & \text{ha} f(\tau(\mathbf{x})) = 0. \end{cases} \tag{5.6}$$

Gyarmati, Mauduit és Sárközy belátta [8], hogy a $\mathcal{G}_{\leq K,kvadratikus}$ család családmértéke optimális. A távolságminimumra is adtak egy közelítést, illetve azt is bebizonyították, hogy $K < \frac{1}{2}q^{1/2}$ esetén $\mathcal{G}_{\leq K,kvadratikus}$ ütközésmentes. Továbbá ha $q \to \infty, K = o(q^{1/2})$, akkor $\mathcal{G}_{\leq K,kvadratikus}$ rendelkezik a lavina-tulajdonsággal. Gyarmati belátta, hogy $K \geq 2$ esetén $\mathcal{G}_{\leq K,kvadratikus}$ keresztkombinált-mértéke rossz:

5.10. Állítás (Gyarmati [5]). *$K \geq 2$-re* $\Phi_3(\mathcal{G}_{\leq K,kvadratikus}) \geq q - 2$.

Bizonyítás. [5] Tekintsük a következő három polinomot: $f_1(x) = x, f_2(x) = x + 1, f_3(x) = x(x+1) \in \mathbb{F}_q[x]$.Legyen η_i az f_i polinom által 3.13 szerint konstruált bináris rács, ahol $i = 1, 2, 3$. Ekkor (5.6)-ot felhasználva:

$$\begin{aligned} \Phi_3(\mathcal{G}_{\leq K,kvadratikus}) \geq \tilde{Q}_3(\eta_1, \eta_2, \eta_3) \geq V_3(\eta_1, \eta_2\eta_3, I_p^n, (0,0,0)) &= \sum_{\mathbf{x} \in I_p^n} \eta_1(\mathbf{x})\eta_2(\mathbf{x})\eta_3(\mathbf{x}) \\ &= \sum_{\substack{\tau(\mathbf{x}) \in I_p^n \\ \tau(\mathbf{x})(\tau(\mathbf{x})+1) \neq 0}} \gamma(\tau(\mathbf{x}))\gamma(\mathbf{x}+1)\gamma(\mathbf{x}(\mathbf{x}+1)) + \gamma(1) + \gamma(-1) \\ &= \sum_{\substack{y \in \mathbb{F}_q \\ y(y+1) \neq 0}} \gamma(y^2(y+1)^2) + \gamma(1) + \gamma(-1) \geq q - 2 \end{aligned}$$

□

Az állítás kiterjeszthető magasabb rendű keresztkombinált mértékre is, tehát $\mathcal{G}_{\leq K,kvadratikus}$-t le kell szűkítenünk egy olyan részhalmazára, amelynek már jó a családmértéke. Egydimenziós esetben ez a következőképp lehetséges:

5.11. Konstrukció (Gyarmati, Mauduit, Sárközy [9])**.** Tekintsük az olyan irreducibilis $f(x) = x^k + a_{k-2}x^{k-2} + a_{k-3}x^{k-3} \dots a_1 x + a_0$ alakba írható polinomokat (azaz amik főegyütthatója 1, és az x^{k-1} tag együtthatója 0), melyek foka $0 < \deg f \leq K$, és legyen $\mathcal{F}_{\leq K,irreducibilis,Legendre}$ az ezekhez tartozó (2.1) által definiált bináris sorozatok halmaza.

Ekkor a $\mathcal{F}_{\leq K,irreducibilis,Legendre}$ család optimális keresztkombinált mértékkel rendelkezik:

5.12. Tétel (Gyarmati, Mauduit, Sárközy [9])**.**

$$\Phi_l(\mathcal{F}_{\leq K,irreducibilis,Legendre}) \leq 10Klp^{1/2}\log p.$$

Visszatérve a többdimenziós esetre:

5.13. Konstrukció (Gyarmati [5])**.** Jelölje $\mathcal{G}_{\leq K,irreducibilis,kvadratikus}$ a $\mathcal{G}_{\leq K,kvadratikus}$ család egy részhalmazát: tekintsük azokat az $\eta \in \mathcal{G}_{\leq K,kvadratikus}$ rácsokat, melyek 3.13 szerinti konstrukciójához felhasznált f polinom irreducibilis, $f(x) = x^k + a_{k-2}x^{k-2} + a_{k-3}x^{k-3} \dots a_1 x + a_0$ alakú és $0 < k \leq K$ fokú. Legyen $\mathcal{G}_{\leq K,irreducibilis,kvadratikus}$ az így kapott η-k halmaza. Látható, hogy $\mathcal{G}_{\leq K,irreducibilis,kvadratikus} \subset \mathcal{G}_{\leq K,kvadratikus}$.

Gyarmati a következő tételt bizonyította erről a családról:

5.14. Tétel (Gyarmati [5])**.**

$$\Phi_l(\mathcal{G}_{\leq K,irreducibilis,kvadratikus}) \leq Klq^{1/2}(\log p + 1)^n + 2l.$$

5.4. Legendre-szimbólum segítségével készült bináris rácscsaládok keresztkombinált-mértéke

A kiindulási a pont a Gyarmati, Sárközy és Stewart által definiált konstrukció [10]:

5.15. Konstrukció (Gyarmati, Sárközy, Stewart [10])**.** Legyen p egy páratlan prím. Jelölje $\mathcal{R}_{\leq K}$ azon $f \in \mathbb{F}_p[x_1, x_2]$ polinomokat, melyek főegyütthatója 1 és $0 < \deg f \leq K$. Jelölje $\mathcal{G}_{\leq K,Legendre}$ azon $\eta : I_p^2 \to \{-1, +1\}$ bináris rácsok halmazát, melyek a következő formába írhatóak:

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

valamilyen $f \in \mathcal{R}_{\leq K}$-ra.

Korábban már szerepelt a 3.11-es tételben, hogy bizonyos megkötéseket alkalmazva f-re és p-re

$$Q_l(\eta) \leq 11klp^{3/2} \log p.$$

Hasonlóan (5.10)-hez, az derült ki, hogy $\mathcal{G}_{\leq K,Legendre}$ keresztkombinált mértéke rossz:

5.16. Állítás (Gyarmati [5])**.** *Ha $K \geq 2$, akkor $\Phi_3(\mathcal{G}_{\leq K,Legendre}) \geq p^2 - 2$.*

Tehát $\mathcal{G}_{\leq K,Legendre}$-t itt is le kéne szűkíteni egy olyan részhalmazra, amely keresztkombinált mértéke már jó, és az ötlet ehhez itt is az irreducibilis polinomok használata. Az alábbi tétel [10]-ben az 1. tétel (Theorem 1) egy speciális változata:

5.17. Tétel (Gyarmati, Sárközy, Stewart [10])**.** *Legyen p páratlan prím, $f \in \mathbb{F}_p[x_1, x_2]$ kétváltozós irreducibilis k-ad fokú polinom. Definiáljuk $\eta : I_p^2 \to \{-1, +1\}$-t 5.15 szerint. Ha $f(x_1, x_2)$ nem írható*

$$f(x_1, x_2) = \varphi(\gamma x_1 + \delta x_2) \tag{5.7}$$

alakban, ahol $\gamma, \delta \in \mathbb{F}_p$, $\varphi \in \mathbb{F}_p[x]$, akkor a 5.15 szerint definiált η p-rácsra

$$Q_l(\eta) \leq 11klp^{3/2} \log p.$$

Ezek alapján $\mathcal{G}_{\leq K,Legendre}$ részcsaládjának konstrukciója:

5.18. Konstrukció (Gyarmati [5])**.** Jelölje $\mathcal{G}_{\leq K,irreducibilis,Legendre}$ a $\mathcal{G}_{\leq K,Legendre}$ család azon részcsaládját, mely elemei olyan $\eta \in \mathcal{G}_{\leq K,Legendre}$ rácsok, amelyekhez a 5.15 konstrukcióban használt f polinom irreducibilis, és nem írható (5.7) alakba. Ekkor látható, hogy $\mathcal{G}_{\leq K,irreducibilis,Legendre} \subset \mathcal{G}_{\leq K,Legendre}$.

Ennek a családnak a keresztkombinált mértéke már viszonylag kicsi:

5.19. Tétel (Gyarmati [5])**.**

$$\Phi_l(\mathcal{G}_{\leq K,irreducibilis,Legendre}) \leq 11Klp^{3/2}\log p.$$

5.20. Következmény (Gyarmati [5]). *$\mathcal{G}_{\leq K,irreducibilis,Legendre}$-nak minden $\mathcal{G}_0$ részcsaládjára:*

$$\Phi_l(\mathcal{G}_0) \leq 11Klp^{3/2}\log p.$$

A következmény fontossága abban rejlik, hogy kétváltozós irreducibilis polinomokat könnyen tudunk készíteni a Schönemann-Eisenstein kritérium segítségével:

5.21. Lemma. *Legyen $f \in \mathbb{F}_p[x_1, x_2]$ a következő alakú:*

$$f(x_1, x_2) = x_1^k + x_1x_2g(x_1, x_2) + x_2h(x_2), \tag{5.8}$$

ahol $g \in \mathbb{F}_p[x_1, x_2], \deg g \leq k-3, h \in \mathbb{F}_p[x_2], \deg h \leq k-2$, és $x_2 \nmid h(x_2)$. Ekkor $f(x_1, x_2)$ irreducibilis, és nem (5.7) *alakú.*

Ez a tétel [11]-ben a 3. tétel (Theorem 3) egy következménye.

Így (5.8)-at felhasználva gyorsan és könnyen tudunk egy nagy bináris rácscsaládot konstruálni:

5.22. Konstrukció (Gyarmati [5])**.** Jelölje $\mathcal{G}_{\leq K,Sch-Eis,Legendre}$ a $\mathcal{G}_{\leq K,irreducibilis,Legendre}$ család azon részcsaládját, mely elemei azok az $\eta \in \mathcal{G}_{\leq K,Legendre}$ bináris rácsok, melyek 5.15 szerinti konstrukciójához felhasznált f polinom (5.8) alakú. Látható, hogy $\mathcal{G}_{\leq K,Sch-Eis,Legendre} \subset \mathcal{G}_{\leq K,irreducibilis,Legendre} \subset \mathcal{G}_{\leq K,Legendre}$.

Tehát a $\mathcal{G}_{\leq K,Sch-Eis,Legendre}$ család gyorsan legenerálható, keresztkombinált mértéke közel optimális, és a család mérete nagy (több, mint $p^{K(K-1)/2}$ darab különböző bináris rácsot tartalmaz).

Összefoglalva az mondható, hogy a titkosítási eljárások során a Legendre szimbólumon és kvadratikus karakteren alapuló módszerek kiemelten fontosak, a gyorsan programozhatóság mellett előnyük a természetes definíciójuk. Ezek a konstrukciók a mai napig a legerősebb konstrukciók között vannak számontartva.

Hivatkozások

[1] R. AHLSWEDE, L. H. KHACHATRIAN, C. MAUDUIT, AND K. GYARMATI, *A complexity measure for families of binary sequences*, Periodica Mathematica Hungarica 46, (2003), pp. 107 – 118.

[2] W. CONTRIBUTORS, *Pseudorandomness — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Pseudorandomnessoldid=1085841673, 2022. Online; accessed 6-May-2022.

[3] L. GOUBIN, C. MAUDUIT, AND A. SÁRKÖZY, *Construction of large families of pseudorandom binary sequences*, Journal of Number Theory 106, (2004), pp. 56–69.

[4] K. GYARMATI, *On a pseudorandom property of binary sequences*, Ramanujan J. 8, (2004), pp. 289 – 302.

[5] ——, *On the cross-combined measure of families of binary lattices and sequences* , in Number-Theoretic Methods in Cryptology. Lecture Notes in Computer Science (10737), Springer, 2018, pp. 217 – 238.

[6] K. GYARMATI, C. MAUDUIT, AND A. SÁRKÖZY, *Pseudorandom binary sequences and lattices*, Acta Arithmetica 135, (2008), pp. 181 – 197.

[7] K. GYARMATI AND A. SÁRKÖZY, *Pszeudovéletlenség*, (2012). A számítógépes számelmélet tárgy Neal Koblitznek A Course in Number Theory and Cryptography című könyvére épülő anyagának kiegészítése.

[8] K. GYARMATI, A. SÁRKÖZY, AND C. MAUDUIT, *Measures of pseudorandomness of finite binary lattices, I. (The measures Qk, normality.)*, Acta Arithmetica 144, (2010), pp. 295 – 313.

[9] ——, *The cross-correlation measure for families of binary sequences*, in Applications of Algebra and Number Theory (Lectures on the occasion of Harald Niederreiter's 70th Birthday), 2014.

[10] K. GYARMATI, A. SÁRKÖZY, AND C. L. STEWART, *On Legendre symbol lattices*, Uniform Distribution Theory 4, (2009), pp. 81 – 95.

[11] ——, *On Legendre symbol lattices, 2*, Uniform Distribution Theory 8, (2013), pp. 47 – 65.

[12] J. HOFFSTEIN AND D. LIEMAN, *The distribution of the quadratic symbol in function fields and a faster mathematical stream cipher*, in Cryptography and Computational Number Theory, K.-Y. Lam, I. Shparlinski, H. Wang, and C. Xing, eds., Basel, 2001, Birkhäuser Basel, pp. 59–68.

[13] P. HUBERT, C. MAUDUIT, AND A. SÁRKÖZY, *On pseudorandom binary lattices*, Acta Arithmetica 125, (2006), pp. 51 – 62.

[14] C. MAUDUIT AND A. SÁRKÖZY, *On finite pseudorandom binary sequences 1: Measure of pseudorandomness, the Legendre symbol*, Acta Arithmetica 82.4, (1997), pp. 356–377.

[15] ——, *On finite pseudorandom binary sequences 2: The Champernowne, Rudin-Shapiro, and Thue-Morse sequences. A further construction*, Journal of Number Theory 73, (1998), pp. 256 – 276.

[16] ——, *On large families of pseudorandom binary sequences*, Uniform Distribution Theory 2, (2007), pp. 23 – 37.

[17] L. RÉDEI, *Algebra*, Oxford, New York, Pergamon Press, 1967.

[18] A. WEIL, *Sur les courbes algebriques et les varietes qui s'en deduent.*, Act. Sci. Ind. 1041, Paris, Hermann, 1948.