Bináris rácsok implementációjának idő analízise

Diplomamunka

Írta: Kodila Tamás

Alkalmazott matematikus szak

Témavezetők:

Gyarmati Katalin, egyetemi adjunktus

Algebra és Számelmélet Tanszék

Sárközy András, egyetemi tanár

Algebra és Számelmélet Tanszék

Eötvös Loránd Tudományegyetem

Természettudományi Kar

2012

Előszó

A kriptográfiában egy szöveg titkosításánál gyakran előfordul, hogy véletlen bitsorozatot kell használni. Egy ilyen sorozat általában egy algoritmus kulcsa vagy inicializáló értéke lehet. Valódi véletlen sorozatok előállítása azonban rendkívül bonyolult és nehézkes feladat, így a gyakorlatban pszeudorandom bitsorozatokkal dolgoznak. Az utóbbi időben egyre elterjedtebb a fényképek illetve térképek rejtjelezésének igénye, így a pszeudorandom bitsorozatok mellett komoly igény mutatkozik a pszeudorandom rácsok iránt is.

Diplomamunkám középpontjában a fent említett pszeudorandom rácsok, azok implementációja illetve véletlensége áll. Az első fejezetben közlöm a témában alapvető fontosságú definíciókat és tételeket. Ezeket az első fejezetben közlöm. A következő fejezetben néhány módszert mutatok be bináris rácsok implementációjára. Ezen konstrukciók közül hárommal részletesebben is foglalkozom. Különböző szempontok szerint vizsgálom ezen módszereket a harmadik fejezetben, illetve itt közlöm numerikus adataimat. Az utolsó fejezet célja a kapott eredmények elemzése.

Diplomamunkámban közölt futásidők mérését 3 GHz-es processzoron 3 GB RAM mellett végeztem. Ezen futásidők a ténylegesen eltelt időt mérik, nem pedig a processzor azon idejét, amíg a feladattal foglalkozik. A módszerek implementálását, illetve a pszeudorandom bináris rácsok másodrendű korrelációjának számítását Ubuntu 10.10 operációs rendszer alatt a Sage 4.6 komputeralgebrai programmal oldottam meg.

Szeretnék köszönetet mondani témavezetőimnek, Sárközy Andrásnak a diplomamunkám elkészítéséhez nyújtott segítségért és az inspiráló konzultációkért, illetve Gyarmati Katalinnak a Sage programnyelv használatában nyújtott segítségért és remek ötleteiért.

Tartalomjegyzék

1. Bevezetés

Hubert, Mauduit és Sárközy kiterjesztette a pszeudorandom bináris sorozatok fogalmát több dimenzióra [6]. Az I_N^n jelentse azon n-dimenziós vektorok halmazát, amelyek minden koordinátája $\{0, 1, ..., N-1\}$-beli:

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

Az így kapott (megcsonkított) n-dimenziós rácsot hívjuk n-dimenziós N-rácsnak, vagy röviden (fix n esetén) N-rácsnak. Ekkor a bináris rácsot mint az I_N^n halmazon értelmezett bináris függvényt definiáljuk:

$$\eta(\boldsymbol{x}) : I_N^n \to \{-1, +1\}.$$

Mauduit és Sárközy [9] többfajta véletlenségi mértéket is definiált pszeudorandom bináris sorozatokra. Azon célból, hogy bevezessék egy bináris rács véletlenségi mértékét, természetesen adódott az ötlet, hogy az egy-dimenziós mértékből induljanak ki. A magasabb dimenziós véletlenségi mértéket a kombinált (jól-eloszlás-korrelációs) mérték Q_k általánosításával nyerték.

Legyen $\eta = \eta(\boldsymbol{x})$ egy n-dimenziós bináris N-rács, $k \in \mathbb{N}$, és $\boldsymbol{u}_i$ (i=1,2...,n) jelölje azon n-dimenziós vektorokat amelyek i-edik koordinátája 1, a többi pedig 0.

Definíció. Az η *bináris rács k-adrendű véletlenségi mértéke* a

$$Q_k(\eta) = \max_{\boldsymbol{B}, \boldsymbol{d}_1, \ldots, \boldsymbol{d}_k, \boldsymbol{T}} \left| \sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} \eta(j_1 b_1 \boldsymbol{u}_1 + \cdots + j_n b_n \boldsymbol{u}_n + \boldsymbol{d}_1) \right.$$

$$\left. \ldots \eta(j_1 b_1 \boldsymbol{u}_1 + \cdots + j_n b_n \boldsymbol{u}_n + \boldsymbol{d}_k) \right|,$$

ahol $\boldsymbol{d}_1, \ldots, \boldsymbol{d}_k$ illetve $\boldsymbol{B} = (b_1, \ldots, b_n)$, $\boldsymbol{T} = (t_1, \ldots, t_n)$ koordinátáik nemnegatív egészek, $b_1, \ldots, b_n$ nem nulla, $\boldsymbol{d}_1, \ldots, \boldsymbol{d}_k$ különbözőek, és minden előforduló $j_1 b_1 \boldsymbol{u}_1 + \cdots + j_n b_n \boldsymbol{u}_n + \boldsymbol{d}_i$ vektor benne van az n-dimenziós N-rácsban, I_N^n-ben.

Megjegyezzük, hogy speciálisan 1-dimenziós esetben $Q_1(\eta)$ megegyezik a sorozatokra definiált jól-eloszlás mértékkel, míg minden $k \in \mathbb{N}$ esetén $Q_k(\eta)$ a kombinált mértékkel.

A már említett cikkben [6] Hubert, Mauduit és Sárközy vizsgálta, hogyan viselkedik az újonnan bevezetett pszeudovéletlen mérték valódi véletlen rács esetén. Legyen $N \in \mathbb{N}$, $n \in \mathbb{N}$, $Z = |I_N^n| = N^n$, I_N^n elemeit jelöljük $\boldsymbol{x_1}, \boldsymbol{x_2}, \ldots, \boldsymbol{x_Z}$-vel, és mindet azonos valószínűséggel választjuk ki (2^{-Z}). Definiáljuk η-t úgy, hogy $\eta(\boldsymbol{x_1}), \eta(\boldsymbol{x_2}), \ldots \eta(\boldsymbol{x_Z})$ független valószínűségi változók, amelyekre a következő teljesül:

$$P(\eta(\boldsymbol{x_i}) = +1) = P(\eta(\boldsymbol{x_i}) = -1) = \frac{1}{2}.$$

Tétel. *Ha $k \in \mathbb{N}$ és $\varepsilon > 0$, akkor vannak olyan számok $N_0 = N_0(k, \varepsilon)$ és $\delta = \delta(k, \varepsilon) > 0$ amelyekre, $N > N_0$ esetén*

$$P(Q_k(\eta) > \delta N^{n/2}) > 1 - \varepsilon$$

és

$$P(Q_k(\eta) > (KN^n(\log N)^n)^{1/2}) < \varepsilon,$$

ahol $K = 81k$.

A tétel szerint hogyha $\eta(\boldsymbol{x}) : I_N^n \to \{-1, +1\}$ valódi véletlen rács, akkor $Q_k(\eta) \ll \sqrt{kN^n(\log N)^n}$. Ezek alapján egy η bináris rácsot jó pszeudovéletlen tulajdonságú rácsnak tekintünk, ha mértékére hasonló korlát adható, legalábbis kis k rendek esetén. A tétel néhány oldalas bizonyítása megtalálható a cikkben, ld. [6].

A következő fejezetben néhány alapvető bináris N-rács konstrukcióról lesz szó.

2. Módszerek ismertetése

Az első bináris rács konstrukciót Hubert, Mauduit és Sárközy ismertette [6], melynek alapja a véges testek kvadratikus karaktere (a félreértések elkerülése végett jelzem, hogy későbbi hivatkozásaimban szereplő kvadratikus karakteres módszer alatt nem ezt a konstrukciót értem). A konstrukcióhoz tartozó tétel bizonyításának ugyanezen cikkben nézhet utána a kedves Olvasó.

Legyen p páratlan prím, $n \in \mathbb{N}$, $q = p^n$, és γ a kvadratikus karaktere $\mathbb{F}_q$-nak. $\mathbb{F}_q$-t mint $\mathbb{F}_p$ feletti vektorteret tekintjük. Jelöljük ezen vektortér n lineárisan független elemét $v_1, v_2, \ldots, v_n$-nel. Definiáljuk az $\eta(x)$ leképezést

$$\eta(\boldsymbol{x}) : I_p^n \to \{-1, +1\}$$

a következőképpen:

$$\eta(\boldsymbol{x}) = \eta((x_1, \ldots, x_n)) = \begin{cases} \gamma(x_1 v_1 + \cdots + x_n v_n) & \text{ha } x_1, \ldots, x_n \neq (0, 0, \ldots, 0) \\ 1 & \text{ha } x_1, \ldots, x_n = (0, 0, \ldots, 0) \end{cases}$$

minden x_1,...,$x_n \in \mathbb{F}_p$.

Tétel. *Ha p páratlan prím, $n \in \mathbb{N}$, $q = p^n$, és az n-dimenziós bináris p-rács az előző konstrukció szerint van definiálva, akkor*

$$Q_k(\eta) < kq^{1/2}(1 + \log p)^n.$$

A most következő módszerekre épült a programozási feladatom, így ezen módszerekkel részletesebben is foglalkozom a 3. fejezetben, most csak a konstrukciót és a hozzájuk tartozó elméleti becslést ismertetem.

2.1. Kvadratikus karakteres módszer

Az első konstrukció alapján Mauduit és Sárközy [11] egy nagy családját mutatta be pszeudorandom bináris rácsoknak, melyek jó pszeudorandom tulajdonsággal rendelkeznek. Ahhoz, hogy ezen családdal megismerkedhessünk, szükségünk lesz a P tulajdonság, illetve a megengedhetőség fogalmára.

Definíció. Ha $q = p^n$ prímhatvány, $\mathcal{A}$,$\mathcal{B} \subset \mathbb{F}_q$ halmazok, és $\mathcal{A}+\mathcal{B}$ összegben az $\mathbb{F}_q$ minden eleme páros sokszor van reprezentálva, azaz minden $c \in \mathbb{F}_q$ esetén az

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

egyenletnek páros sok megoldása van (beleértve azt az esetet is, ha nincs megoldása az egyenletnek), akkor $\mathcal{A}+\mathcal{B}$-t P *tulajdonságúnak* nevezzük.

Definíció. Ha $q = p^n$ prímhatvány, $k, \ell \in \mathbb{N}$ és $k, \ell \leq q$, ekkor (k, ℓ, q) hármast *megengedhetőnek* nevezzük, ha nem létezik $\mathcal{A}$,$\mathcal{B} \subset \mathbb{F}_q$, amire $|\mathcal{A}| = k$, $|\mathcal{B}| = \ell$, illetve $\mathcal{A}+\mathcal{B}$ P tulajdonságú.

Ezen fogalmak bevezetése után a szerzők az alábbi konstrukciót definiálták majd bizonyították az utána szereplő tételt.

Konstrukció (Kvadratikus karakter). *Legyen p egy páratlan prím, $n \in \mathbb{N}, q = p^n$, és γ jelentse a $\mathbb{F}_q$ kvadratikus karakterét (legyen $\gamma(0) = 0$). Tekintsük $\mathbb{F}_q$-t, mint $\mathbb{F}_p$ feletti vektorteret. Legyen ezen vektortér bázisa $v_1, v_2, \ldots, v_n$. Az $f(x) \in \mathbb{F}_q[x]$ polinom fokát jelölje ℓ, amire teljesül*

$$0 < \ell < p,$$

és tegyük fel, hogy az $f(x)$ polinomnak nincs többszörös gyöke $\overline{\mathbb{F}}_q$-ban. Definiáljuk az n-dimenziós bináris p-rácsot $\eta(\boldsymbol{x}) : I_p^n \to \{+1, -1\}$ a következőképpen:

$$\eta(\boldsymbol{x}) = \eta((x_1, \ldots, x_n)) = \\ = \begin{cases} \gamma(f(x_1v_1 + \cdots + x_nv_n)) & ha\ f(x_1v_1 + \cdots + x_nv_n) \neq 0 \\ 1 & ha\ f(x_1v_1 + \cdots + x_nv_n) = 0 \end{cases} \tag{1}$$

Tétel. *Feltesszük továbbá, hogy $k \in \mathbb{N}$ és az (r, k, q) hármas megengedhető minden $r \leq \ell$ esetén. Ekkor*

$$Q_k(\eta) < k\ell(q^{1/2}(1 + \log p)^n + 2). \tag{2}$$

Ahhoz, hogy ezen konstrukciót használni tudjuk, először szükségünk van elégséges feltételre a megengedhetőséghez.

Tétel.

(*i*) *Minden prímhatvány $q = p^n$ és minden $\ell \in \mathbb{N}$, $\ell < p$ esetén az $(\ell, 2, q)$ hármas megengedhető.*

(*ii*) *Ha $q = p^n$ prímhatvány, $k, \ell \in \mathbb{N}$ és $4^{n(k+\ell)} < p$ fennáll, akkor a (k, ℓ, q) hármas megengedhető.*

(*iii*) *Ha $q = p^n$ prímhatvány, amire a 2 primitív gyök modulo p, akkor minden $k, \ell \in \mathbb{N}$, $k < p$, $\ell < p$ esetén teljesül, hogy a (k, ℓ, q) megengedhető.*

E feltételek elégségességének bizonyításához meglehetősen mély kombinatorikus, illetve véges testeket használó bizonyításokra van szükség. Ezen megengedhetőségi feltételek teszik lehetővé, hogy olyan bináris rácsot készítsünk, melyről bizonyított a jó pszeudovéletlen tulajdonság.

2.2. Multiplikatív inverzes módszer

Mauduit és Sárközy egy olyan konstrukciót mutatott be pszeudorandom bináris sorozatokra [10], melynek alapja a multiplikatív inverz modulo p. A szerzők kiterjesztették illetve adaptálták a konstrukciójukat magasabb dimenzióra is [12]. Ezen konstrukció erőssége nem csak abban rejlik, hogy gyors (multiplikatív inverz számítása polinomiális idejű), hanem kezelhetőség szempontjából is ideális.

Konstrukció (Multiplikatív inverz). *Tegyük fel, hogy $q = p^n$ egy páratlan prímhatvány, $\ell \in \mathbb{N}$, $a_1, \ldots, a_\ell$ különböző $\mathbb{F}_q$-beli elemek, és legyen*

$$f(x) = (x + a_1)(x + a_2)\ldots(x + a_\ell)\ (\in \mathbb{F}_q[x])\ (\textit{ahol } a_i \neq a_j,\ \textit{ha } i \neq j).$$

Legyenek $v_1, \ldots, v_n$ lineárisan független elemei $\mathbb{F}_q$-nak az $\mathbb{F}_p$ prímtest fölött (aminek az elemeit úgy definiáljuk, mint a modulo p maradék osztályok által alkotott testet, és i-vel jelöljük azt a maradék osztályt, melynek elemei kongruensek i-vel modulo p). Definiáljuk az alábbi halmazokat a következőképpen:

$$B_1 = \left\{ \sum_{i=1}^{n} u_i v_i : 0 \leq u_1 \leq \frac{p-3}{2}, u_2, \ldots, u_n \in \mathbb{F}_p \right\},$$

$$B_j = \left\{ \sum_{i=1}^{n} u_i v_i : u_1 = \cdots = u_{j-1} = \frac{p-1}{2}, 0 \leq u_j \leq \frac{p-3}{2}, u_{j+1}, \ldots, u_n \in \mathbb{F}_p \right\},$$

$$\textit{ha } j = 2, \ldots, n \textit{ és}$$

$$B = \bigcup_{j=1}^{n} B_j.$$

Definiáljuk az $\eta(x)$ leképezést $\eta(\boldsymbol{x}) : I_p^n \to \{-1, +1\}$ a következőképpen:

$$\eta(\boldsymbol{x}) = \eta((x_1, \ldots, x_n)) = \begin{cases} +1 & \textit{ha } f(x_1 v_1 + \ldots x_n v_n) \neq 0 \textit{ és} \\ & (f(x_1 v_1 + \ldots x_n v_n))^{-1} \in B \\ -1 & \textit{máskülönben.} \end{cases} \tag{3}$$

Ezek után megmutatjuk, hogy ha k nem nagy, akkor $Q_k(\eta)$ "kicsi" az ilyen bináris rács konstrukció esetén.

Tétel. *Ha $p, q, n, l, f(x), B$ és η a fentiek szerint definiált, $k \in \mathbb{N}$,*

$$k, \ell < p, \qquad k + \ell \leq p + 1$$

és

$$k\ell < \frac{q}{2},$$

akkor

$$Q_k(\eta) < (2^{k+3} + 1) k \ell n^k q^{1/2} (\log p + 2)^{n+k}. \tag{4}$$

Meg kell jegyeznünk, hogy a B halmaz kissé komplikáltnak tűnik, valójában viszont nem az. A B halmaznak könnyen kezelhetőnek kell lennie, illetve számosságát tekintve jól meg kell közelítenie a $\frac{q}{2}$-t. Egy dimenzióban egy p páratlan számosságú pont sorozatot legegyszerűbben úgy oszthatunk fel két, közel egyenlő számosságú ponthalmazra, hogyha elvágjuk $\frac{p-1}{2}$ pont után, hisz a maradék, csak 1-gyel lesz több, nevezetesen $\frac{p+1}{2}$. Két dimenzióban viszont ugyanezen módszerrel már nem kapunk megfelelő eredményt, hisz a két halmaz számosságának különbsége már p lesz. n-dimenziós kockánál az eltérés pedig már p^{n-1}. Emiatt van szükségünk a B halmaz precíz definíciójára.

2.3. Legendre-szimbólumos módszer

Egy dimenzióban a legjobb és legintenzívebben tanulmányozott módszer alapja a Legendre-szimbólum. Legyen p prím, $f(x) \in \mathbb{F}_p[x]$ polinom, és definiáljuk az $E_p = \{e_1, \ldots, e_n\}$ sorozatot a következőképpen

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

Ezen konstrukció kétdimenziós kiterjesztését publikálta Gyarmati,Sárközy és Stewart [4].

Konstrukció (Legendre-szimbólum). *Legyen p páratlan prím, $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ egy kétváltozós polinom. Definiáljuk az $\eta : I_p^2 \to \{-1, +1\}$ a következőképpen*

$$\eta(x_1, x_2) = \begin{cases} \left(\frac{f(x_1,x_2)}{p}\right) & \textit{ha } (f(x_1, x_2), p) = 1 \\ +1 & \textit{ha } p \mid f(x_1, x_2) \end{cases} \tag{5}$$

Ahhoz, hogy erős pszeudovéletlen mértékű bináris rácsunk legyen, az f polinomra megkötést kell tennünk. Ehhez szükségünk lesz az alábbi fogalom bevezetésére.

Definíció. Az $f(x_1, x_2)$ kétváltozós polinomot *degeneráltnak* hívjuk, ha nem írható fel a következő alakban

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

ahol $\alpha_j, \beta_j \in \mathbb{F}_p$, $f_j(x) \in \mathbb{F}_p[x]$ minden $j = 1, \ldots, r$ esetén és $g(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$.

Amennyiben egy $f \in \mathbb{F}_p[x, y]$ polinom az előző alakba írható, úgy degeneráltnak hívjuk, ellenkező esetben pedig nem-degenerált polinomnak. Ezen definíció ismertetése után nézzük, a pszeudovéletlen mértékre vonatkozó elméleti korlátot ezen konstrukció esetén.

Tétel. *Legyen $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ egy ℓ-edfokú polinom. Feltételezzük, hogy az $f(x_1, x_2)$ egy nem-degenerált polinom és valamelyik feltétel teljesül az alábbiak közül:*
a) $f(x_1, x_2)$ irreducibilis polinom $\mathbb{F}_p[x_1, x_2]$,
b) $k = 2$,
c) 2 primitív gyök modulo p,
d) $4^{k+\ell} < p$,
e) k és az $f(x_1, x_2)$ polinomban x_1 (vagy x_2) foka páratlan.
Ekkor az (5) szerint definiált η bináris p-rács pszeudovéletlen mértékére

$$Q_k(\eta) \leq 11k\ell p^{3/2} \log p. \tag{6}$$

2.4. További módszerek

A már említett módszereken kívül természetesen ismerünk további konstrukciókat is. A teljesség igénye nélkül szeretnék ismertetni ezek közül néhányat.

Ismeretes, hogy az elliptikus görbék véges testek fölött erős pszeudorandom tulajdonsággal bírnak, ezért széles körben alkalmazzák pszeudovéletlen bináris sorozatok konstrukciójához. Ilyen konstrukciót alkotott Chen [1], illetve Chen, Li és Xiao [2]. Elliptikus görbéken alapuló pszeudorandom bináris rács konstrukciót Mérai definiált [15].

Gyarmati, Mauduit és Sárközy további 1-dimenziós konstrukciókat terjesztett ki 2-dimenzióra [3]. Ezen konstrukciók alapjául a multiplikatív inverz, valamint a diszkrét logaritmus szolgált. Mérai további konstrukciói a multiplikatív karakter használatán [13], illetve a k szimbólum használatán alapszanak [14]. H. Liu [8] ismertetett olyan bináris rács konstrukciót, mely egyszerre használja a multiplikatív inverzet és a kvadratikus karaktert.

3. Célkitűzés és megvalósítás

Diplomamunkám kapcsán az önálló feladatom az volt, hogy az előző fejezetben ismertetett módszerek 2-dimenziós esetét implementáljam egy tetszőleges programmal, illetve ezután vizsgáljam az így kapott η bináris rácsok k-adrendű véletlenségi mértékét, kis k-kra, majd a kapott eredmények alapján hasonlítsam össze a három módszert. Ehhez természetesen további ismeretekre volt szükségem, melyeket a már eddig is idézet cikkekből nyertem, nevezetesen [4],[5],[11]. Az általam ismertetett tételek bizonyításaikkal illetve az azokra vonatkozó észrevételek mind ezekben olvashatóak.

Témavezetőm, Gyarmati Katalin javaslatára a Sage komputeralgebrai programban kezdtem el dolgozni, mely kiváló választásnak bizonyult. Ezen program használata során nem kellett külön bajlódnom olyan függvények megírásával, mint a Legendre-szimbólum, vagy a multiplikatív inverz, hiszen ezek már kezdettől rendelkezésemre álltak.

3.1. Idő analízis

3.1.1. Kvadratikus karakteres módszer 2-dimenzióban

Először a kvadratikus karakteres módszer implementálását mutatom be. A következő módszer az (1) konstrukció egy speciális esete, amikor $n = 2$ illetve az f polinomot és a v_1, v_2-t is speciálisan választjuk.

Konstrukció (Kvadratikus karakter 2-dimenzióban). *Legyen p egy páratlan prím és legyen r egy kvadratikus nem-maradék modulo p. Ekkor az $x^2 - r$ irreducibilis $\mathbb{F}_p$ fölött; gyökét jelöljük θ-val, és bővítsük $\mathbb{F}_p$-t θ-val: $\mathbb{F}_p[\theta](\cong \mathbb{F}_{p^2})$ (így most v_1=1, $v_2 = \theta$). γ jelentse a $\mathbb{F}_q$ kvadratikus karakterét (legyen $\gamma(0) = 0$). Az $f(x) \in \mathbb{F}_q[x]$ polinom fokát jelölje ℓ, amire teljesül*

$$0 < \ell < p,$$

illetve ezen $f(x)$ polinomnak nincs többszörös gyöke $\overline{\mathbb{F}}_q$-ban. Definiáljuk a 2-dimenziós bináris p-rácsot $\eta(\boldsymbol{x}) : I_p^2 \to \{+1, -1\}$ a következőképpen:

$$\eta(\boldsymbol{x}) = \eta((x_1, x_2)) = \begin{cases} \gamma(f(x_1 + x_2\theta)) & ha\ f(x_1 + x_2\theta) \neq 0, \\ 1 & ha\ f(x_1 + x_2\theta) = 0. \end{cases} \tag{7}$$

Az $f(x)$ polinom ilyen feltételek mellett a következő alakú:

$$f(x) = f(x_1 + x_2\theta) = \prod_{i=1}^{\ell}((x_1 + x_2\theta) - (a_i + b_i\theta)), \tag{8}$$

ahol a ℓ polninom fokára igaz, hogy $0 < \ell < p$, illetve az $a_1, a_2, \ldots, a_\ell$, $b_1, b_2, \ldots, b_\ell \in \mathbb{F}_p$ teljesítik a polinom gyökeire tett feltételt, azaz

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

Miután már ismerjük az $f(x)$ alakját, könnyedén tudunk generálni ilyen polinomot, hisz csak $a_1, a_2, \ldots, a_\ell, b_1, b_2, \ldots, b_\ell \in \mathbb{F}_p$ elemeket kell kiválasztanunk úgy, hogy teljesítsék a fent közölt feltételeket. Ezek után minden lehetséges $x_1, x_2 \in \mathbb{F}_p$ elemet be kell helyettesítenünk az f polinomba, melynek értékkészlete $\mathbb{F}_q$. Ezzel elértünk a konstrukció sarkalatos pontjára: Hogyan kell kiszámolni egy $\mathbb{F}_q$-beli elem kvadratikus karakterét? A következő tétel segít ebben a kérdésben, melyet Gyarmati, Sárközy és Stewart [5] bizonyítottak.

Tétel. *Legyen p, q, r, k, n és $f(x)$ definiálva a fentiek szerint. Legyen*

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

és

$$\tilde{\eta}(\boldsymbol{x}) = \tilde{\eta}((x_1, x_2)) = \begin{cases} \left(\frac{\tilde{f}(x_1,x_2)}{p}\right) & ha\ (\tilde{f}(x_1, x_2), p) = 1, \\ 1 & ha\ p \mid \tilde{f}(x_1, x_2). \end{cases} \tag{9}$$

Ekkor $\eta(\boldsymbol{x}) = \tilde{\eta}(\boldsymbol{x})$.

Bizonyítás. A θ definíciója és az Euler lemma felhasználásával kapjuk, hogy

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

Használjuk az előző jelölések alapján, hogy $\mathbb{F}_q$ elemeit $x_1 + x_2\theta$ alakban reprezentáljuk. Használjuk az általánosított Euler lemmát, illetve az előző levezetést az $x_1 + x_2\theta \in \mathbb{F}^*_{p^2}$-ra (azaz $(x_1, x_2) \neq (0, 0)$), ekkor kapjuk, hogy

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

A γ és a Legendre-szimbólum multiplikatív tulajdonsága miatt írhatjuk a következőket

$$\begin{aligned}
\eta(\boldsymbol{x}) &= \gamma(f(x_1 + x_2\theta)) = \gamma\left(\prod_{i=1}^{\ell}((x_1 + x_2\theta) - (a_i + b_i\theta))\right) \\
&= \prod_{i=1}^{\ell}\gamma((x_1 + x_2\theta) - (a_i + b_i\theta)) = \prod_{i=1}^{\ell}\gamma((x_1 - a_i) + (x_2 - b_i)\theta) \\
&= \prod_{i=1}^{\ell}\left(\frac{(x_1 - a_i)^2 - r(x_2 - b_i)^2}{p}\right) = \left(\frac{\prod_{i=1}^{\ell}(x_1 - a_i)^2 - r(x_2 - b_i)^2}{p}\right) \\
&= \left(\frac{\tilde{f}(x_1, x_2)}{p}\right) = \tilde{\eta}(\boldsymbol{x}) \qquad (\text{ha } f(x_1 + x_2\theta) \neq 0\ ).
\end{aligned}$$

Triviálisan teljesül a következő is:

$$\eta(\boldsymbol{x}) = \tilde{\eta}(\boldsymbol{x}) \text{ ha } f(x_1 + x_2\theta) = 0.$$

Így kapjuk a tétel állítását, miszerint $\eta(\boldsymbol{x}) = \tilde{\eta}(\boldsymbol{x})$ minden $\boldsymbol{x} = (x_1, x_2) \in \mathbb{F}_{p^2}$ esetén. □

Mivel az $\tilde{f}$ függvény elég bonyolult, így egyszerűbb másképp számolni. Felhasználjuk a tényt, miszerint ha $f(x_1 + x_2\theta) = p(x_1, x_2) + \theta q(x_1, x_2)$ (ahol

$f(z) \in \mathbb{F}_p[z], p(x_1, x_2), q(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ valamint θ és r a fentiek szerint definiált), akkor kapjuk, hogy

$$\gamma(f(x_1 + x_2\theta)) = \gamma(p(x_1, x_2) + q(x_1, x_2)\theta) = \left(\frac{p^2(x_1, x_2) - rq^2(x_1, x_2)}{p}\right).$$

Ezen implementáció kritikus pontja egy r kvadratikus nem-maradék megtalálása. Ha p fix, akkor a GRH biztosítja, hogy a legkisebb kvadratikus nem-maradék modulo p kisebb, mint $(\log p)^c$ (valamilyen pozitív c konstans mellett), és mivel tudjuk, hogy egy adott maradék kvadratikus karakterét polinomiális időben meg tudjuk határozni (Jacobi-szimbólum segítségével), azért az r-et választhatjuk a legkisebb kvadratikus nem-maradéknak modulo p ami így szintúgy polinomiális időt vesz igénybe. Másrészről viszont nem ismerünk polinomiális futásidejű algoritmust, amely minden hipotézis nélkül megtalálná a legkisebb kvadratikus nem-maradékot. Mindazonáltal a legtöbb esetben nem kell p-t rögzítenünk, így a fenti nehézség elkerülhető. Nevezetesen abból a tényből indulhatunk ki, hogy ha p egy $4k-1$ alakú prím, akkor a -1 kvadratikus nem-maradék modulo p. (Ha nagy $4k-1$ alakú p prímre van szükségünk, akkor használnunk kell a tényt, miszerint a Mersenne-prímek $4k-1$ alakúak.)

Ezért az implementációmat csak $4k-1$ alakú p prímekre végeztem el ($r = -1$ választás mellett). Így jutottam el a végleges konstrukcióhoz, amit implementáltam:

$$\eta(\boldsymbol{x}) = \eta((x_1, x_2)) = \begin{cases} \left(\frac{p^2(x_1,x_2)-rq^2(x_1,x_2)}{p}\right) & \text{ha } f(x_1 + x_2\theta) \neq 0, \\ 1 & \text{ha } f(x_1 + x_2\theta) = 0. \end{cases} \tag{10}$$

3.1.2. Multiplikatív inverzes módszer 2-dimenzióban

Ezen konstrukció a (3) speciális esete. Ennél a módszernél a legegyszerűbb az f polinom meghatározása. 2-dimenzióban talán a B halmaz definíciója is könnyebben érthető. Idézzük fel tehát a módszert $n = 2$ esetén.

Konstrukció (Multiplikatív inverz 2-dimenzióban). *Tegyük fel, hogy $q = p^2$ egy páratlan prímhatvány, $\ell \in \mathbb{N}$, $a_1, \ldots, a_\ell$ különböző $\mathbb{F}_q$-beli elemek, és legyen*

$$f(x) = (x + a_1)(x + a_2)\ldots(x + a_\ell)\ (\in \mathbb{F}_q[x])\ (\textit{ahol } a_i \neq a_j,\ \textit{ha } i \neq j). \quad (11)$$

$\mathbb{F}_q$-t most is, mint $\mathbb{F}_p[\theta]$ tekintjük, így $v_1 = 1, v_2 = \theta$ bázist alkotnak. Definiáljuk az alábbi halmazokat a következőképpen:

$$B_1 = \left\{ u_1 + u_2\theta : 0 \leq u_1 \leq \frac{p-3}{2}, u_2 \in \mathbb{F}_p \right\},$$

$$B_2 = \left\{ u_1 + u_2\theta : u_1 = \frac{p-1}{2}, 0 \leq u_2 \leq \frac{p-3}{2} \right\},$$

és

$$B = B_1 \cup B_2.$$

Definiáljuk az $\eta(x)$ leképezést $\eta(\boldsymbol{x}) : I_p^2 \to \{-1, +1\}$ a következőképpen:

$$\eta(\boldsymbol{x}) = \eta((x_1, x_2)) = \begin{cases} +1 & \textit{ha } f(x_1 + x_2\theta) \neq 0 \textit{ és} \\ & (f(x_1 + x_2\theta))^{-1} \in B \\ -1 & \textit{ellenkező esetben.} \end{cases} \quad (12)$$

3.1.3. Legendre-szimbólumos módszer 2-dimenzióban

A Legendre-szimbólumos módszer (5) alapjában véve is csak 2 dimenzióba volt átültetve, így ezen módszer implementálásához, csak egy "jó" f polinomra volt szükségem. "Jó" alatt természetesen a már előző fejezetben ismertetett nem-degenerált polinomokat értem. Gyarmati, Sárközy és Stewart [5] készítettek egy ilyen polinom családot. Ezen polinom családot ismertetem a módszer felelevenítése után.

Konstrukció (Legendre-szimbólum). *Legyen p páratlan prím, $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ egy kétváltozós polinom. Definiáljuk az $\eta : I_p^2 \to \{-1, +1\}$ a következőképpen:*

$$\eta(x_1, x_2) = \begin{cases} \left(\frac{f(x_1,x_2)}{p}\right) & \textit{ha } (f(x_1, x_2), p) = 1, \\ +1 & \textit{ha } p \mid f(x_1, x_2). \end{cases} \quad (13)$$

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

$$f(x_1, x_2) = x_1^\ell + x_1 x_2 g(x_1, x_2) + x_2 h(x_2), \tag{14}$$

ahol $g \in \mathbb{F}_p[x_1, x_2]$, $\deg g \leq \ell - 3$, $h \in \mathbb{F}_p[x_2]$, $\deg h \leq \ell - 2$ *és* $x_2 \nmid h(x_2)$. *Az ilyen* f *alakú polinomok nem-degeneráltak, így ha a Legendre-szimbólumos* (13) *módszert ilyen* f *polinommal készítjük el, akkor teljesül a már ismertetett becslés:*

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

3.1.4. Eredményeim

Miután mindhárom módszerhez megadtuk a választható f polinom leírását ((8), (11), (14)), már csak azt kellett meghatároznom, hogy mennyi legyen az ℓ, azaz a polinomok fokszáma. Sárközy András Tanár Úr javaslatára 100 alatti p prímek esetén az f polinomok fokát legfeljebb 3-nak, 100 és 150 közötti p-k esetén legfeljebb 4-nek, míg 150 és 200 közötti prímek esetén legfeljebb 5-nek választottam. Minden egyes prím esetén véletlenszerűen generáltam az adott módszernek megfelelő 5 különböző f polinomot, majd ezekkel elkészítettem a 2-dimenziós bináris p-rácsokat. Ezen bináris rácsokat kiértékeltem $\mathbb{F}_{p^2}$ minden elemén. Ezen p^2 elem behelyettesítési idejét mértem meg, majd ez alapján hasonlítottam össze a módszereket.

A többoldalnyi terjedelemre való tekintettel az implementáláshoz véletlenszerűen választott f polinomokat és a hozzájuk tartozó generálási időket tartalmazó táblázatok közül csak néhányat ismertetek az utolsó fejezetben. A következő táblázat csak a generálási idők átlagát (módszerenként 5 különböző polinommal) mutatja az egyes módszerek szerint. A $4k + 1$ alakú prímekre a kvadratikus karakteres módszert nem teszteltem, így a táblázat erre vonatkozó soraiban n.a. (nincs adat) szerepel.

	Kvadratikus karakter (7)	Multiplikatív inverz (12)	Legendre - szimbólum (13)
$p = 7$	0,02 s	0,17 s	0,03 s
$p = 11$	0,05 s	0,34 s	0,05 s
$p = 13$	n.a.	0,46 s	0,06 s
$p = 17$	n.a.	0,77 s	0,11 s
$p = 19$	0,16 s	1,01 s	0,13 s
$p = 23$	n.a. s	1,41 s	0,20 s
$p = 29$	n.a.	2,34 s	0,34 s
$p = 31$	0,57 s	2,60 s	0,38 s
$p = 37$	n.a.	3,69 s	0,54 s
$p = 41$	n.a.	4,53 s	0,66 s
$p = 43$	1,06 s	5,30 s	0,74 s
$p = 47$	1,26 s	5,88 s	0,84 s
$p = 53$	n.a.	7,46 s	1,06 s
$p = 59$	2,03 s	9,30 s	1,30 s
$p = 61$	n.a.	9,84 s	1,40 s
$p = 67$	2,83 s	11,84 s	1,64 s
$p = 71$	3,31 s	13,42 s	1,87 s
$p = 73$	n.a.	14,14 s	1,98 s
$p = 79$	4,07 s	16,58 s	2,25 s
$p = 83$	4,21 s	18,14 s	2,48 s
$p = 89$	n.a.	20,90 s	2,85 s
$p = 97$	n.a.	24,84 s	3,56 s
$p = 101$	n.a.	27,28 s	3,81 s
$p = 103$	4,77 s	28,22 s	3,85 s
$p = 107$	5,05 s	31,72 s	4,14 s
$p = 109$	n.a.	34,54 s	4,28 s

1. táblázat. *Generálási idők* 1

	Kvadratikus karakter (7)	Multiplikatív inverz (12)	Legendre - szimbólum (13)
$p = 113$	n.a	37,23 s	4,56 s
$p = 127$	6,85 s	46,97 s	5,92 s
$p = 131$	7,30 s	45,59 s	6,24 s
$p = 137$	n.a.	49,71 s	6,73 s
$p = 139$	8,25 s	51,38 s	6,91 s
$p = 149$	n.a.	59,03 s	7,95 s
$p = 151$	10,63 s	60,74 s	8,46 s
$p = 157$	n.a.	65,37 s	8,95 s
$p = 163$	12,27 s	72,63 s	9,68 s
$p = 167$	12,93 s.	75,67 s	10,10 s
$p = 173$	n.a.	81,44 s	10,78 s
$p = 179$	14,75 s	86,79 s	11,80 s
$p = 181$	n.a.	88,69 s	11,91 s
$p = 191$	16,84 s	99,07 s	13,20 s
$p = 193$	n.a.	101,28 s	13,35 s
$p = 197$	n.a.	105,37 s	13,99 s
$p = 199$	18,13 s	107,89 s	14,92 s

2. táblázat. *Generálási idők* 2

Az adatokból jól látszik, hogy a leggyorsabban generálható bináris rács konstrukció, a Legendre-szimbólumos módszer.

3.2. Korreláció analízis

Felelevenítésként nézzük, hogy mit is értünk egy n-dimenziós bináris p-rács pszeudovéletlenségi mértékén. Legyen $\eta = \eta(\boldsymbol{x})$ egy n-dimenziós bináris N-rács, $k \in \mathbb{N}$, és $\boldsymbol{u}_i$ (i=1,2...,n) jelölje azon n-dimenziós vektorokat amelyek i-edik koordinátája 1, a többi pedig 0.

Definíció. Az η *bináris rács* k*-adrendű véletlenségi mértéke* a

$$Q_k(\eta) = \max_{\boldsymbol{B},\boldsymbol{d}_1,\ldots,\boldsymbol{d}_k,\boldsymbol{T}} \left| \sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} \eta(j_1 b_1 \boldsymbol{u}_1 + \cdots + j_n b_n \boldsymbol{u}_n + \boldsymbol{d}_1) \right.$$

$$\left. \ldots \eta(j_1 b_1 \boldsymbol{u}_1 + \cdots + j_n b_n \boldsymbol{u}_n + \boldsymbol{d}_k) \right|.$$

A maximum az olyan $\mathbb{B}$,$_1, \ldots,$ $_k$,$\mathbb{T}$-n fut, ahol $\boldsymbol{d}_1, \ldots, \boldsymbol{d}_k$ illetve $\boldsymbol{B} = (b_1, \ldots, b_n)$, $\boldsymbol{T} = (t_1, \ldots, t_n)$ koordinátái nemnegatív egészek, $b_1, \ldots, b_n$ nem nulla, $\boldsymbol{d}_1, \ldots, \boldsymbol{d}_k$ különbözőek, és minden előforduló $j_1 b_1 \boldsymbol{u}_1 + \cdots + j_n b_n \boldsymbol{u}_n + \boldsymbol{d}_i$ vektor benne van az n-dimenziós N-rácsban, I_N^n-ben.

Definíció. A B, T valamint $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ segítségével úgynevezett *tégla rácsokat* (box lattice) definiálhatunk. Ha ugyanis adott $(b_1, \ldots, b_n)$, $(t_1, \ldots, t_n)$, akkor a

$$\sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} (j_1 b_1 \boldsymbol{u}_1 + \cdots + j_n b_n \boldsymbol{u}_n)$$

összeggel definiált ponthalmaz éppen egy n-dimenziós tégla rácshálóját adja.

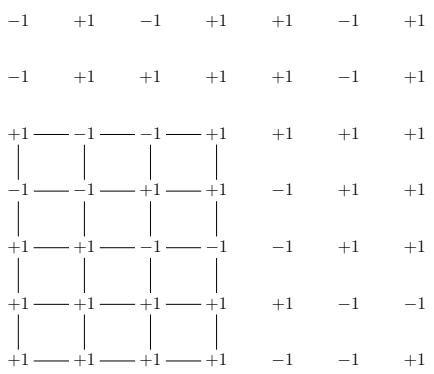
A definícióban szereplő $(b_1, \ldots, b_n)$-k a tégla rács lépésközeit, míg a $(t_1, \ldots, t_n)$-k az adott dimenzióban a téglarács rácspontjainak számát határozzák meg. Pontosabban $b_i = j$ azt jelenti, hogy az i-edik dimenziós lépésköz j, míg $t_k = l$ esetén a k-adik dimenzióban a tégla rácsnak $l + 1$ darab rácspontja van.

A k-adrendű véletlenségi mérték definíciója ezáltal egyszerűbben megérthető. Ugyanis ha adott egy n-dimenziós tégla rács, akkor vesszük ennek k

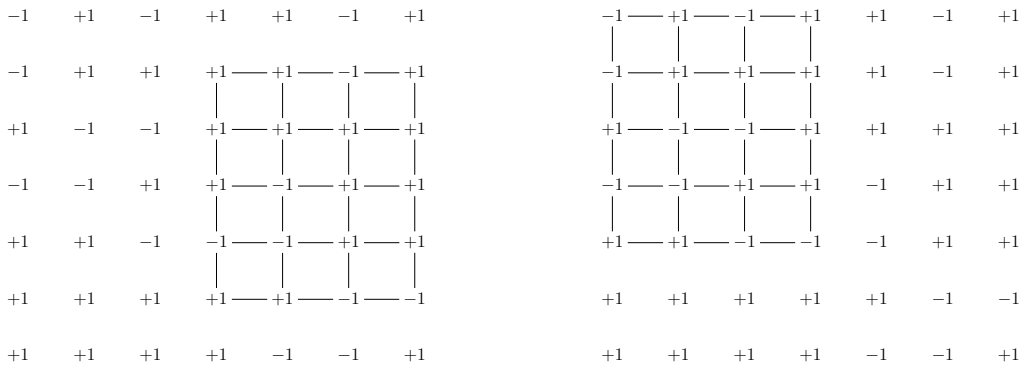
különböző eltoltját, mely még mindig az I_N^n n-dimenziós N-rácsba belefér. Az azonos ősképpel rendelkező rácspontokat behelyettesítjük az η függvénybe, majd a kapott értékeket (+1 vagy -1) összeszorozzuk. Ezt elvégezzük a tégla rács minden pontjára. Az így kapott szám belekerül abba a számhalmazba, amelyre a maximumot képezzük. Ha ezt a műveletsort az összes lehetséges k darab eltolttal, illetve nem csak egy adott tégla rácsra hanem az összes tégla rácsra elvégezzük, akkor az így kapott maximumot értjük az η binárics rács k-adrendű véletlenségi mértékén.

Példaként vegyük a Legendre-szimbólumos módszert 2-dimenzióban $p = 7$ esetén. Tekintsük az $(f = x_1^3 - 3x_1x_2 - 2x_2^2 - 3x_2)$ polinom segítségével generált táblát, majd nézzük ezen azt a tégla rácsot, melyet az alábbi B és T generál,

$$\boldsymbol{B} = (b_1, b_2) = (1, 1) \qquad \text{valamint} \qquad \boldsymbol{T} = (t_1, t_2) = (3, 4).$$



Vegyünk most két eltolás vektort ($\boldsymbol{d}_1 = (3, 1)$ és $\boldsymbol{d}_2 = (0, 2)$) és ábrázoljuk így is. Az összetartozó számokat összeszorozzuk, majd az így kapott szorzatokat összeadjuk.



$$\sum_{j_1=0}^{3}\sum_{j_2=0}^{4}\eta\{(j_1+3)+(j_2+1)\theta\}\cdot\eta\{j_1+(j_2+2)\theta\}=$$

$$\begin{aligned}= \quad & (+1\cdot+1)+(-1\cdot-1)+(+1\cdot+1)+(+1\cdot-1)+(+1\cdot-1)+\\ & (+1\cdot+1)+(-1\cdot-1)+(-1\cdot-1)+(+1\cdot+1)+(+1\cdot+1)+\\ & (-1\cdot-1)+(+1\cdot+1)+(+1\cdot-1)+(+1\cdot+1)+(-1\cdot-1)+\\ & (-1\cdot-1)+(+1\cdot+1)+(+1\cdot+1)+(+1\cdot+1)+(+1\cdot+1)=\\ & 14\end{aligned}$$

Számolással igazoltam, hogy a fenti eredmény valójában épp $Q_2(\eta)$, azaz ez a $\boldsymbol{B}=(b_1,b_2)=(1,1)$, $\boldsymbol{T}=(t_1,t_2)=(3,4),\boldsymbol{d}=((3,1),(0,2))$ hármas egyike azoknak a hármasoknak, amelyeken az összes lehetséges ($\boldsymbol{B}$,$\boldsymbol{T}$ és $\boldsymbol{d}$) hármason felvett érték maximuma realizálódik.

3.2.1. Másodrendű korreláció

Először a $k = 2$ esetet néztem, azaz a másodrendű korrelációs mértékeket vizsgáltam. Az alábbi táblázat csak a kapott mértékek átlagát tartalmazza.

	Kvadratikus karakter (7)	Multiplikatív inverz (12)	Legendre - szimbólum (13)
$p = 7$	13,4	12,4	14,4
$p = 11$	22,4	23,8	24,4
$p = 13$	n.a.	27,4	29,4
$p = 17$	n.a.	41,0	48,8
$p = 19$	50,2	48,6	50,8
$p = 23$	60,4	63,0	64,0

3. táblázat. *Másodrendű korrelációk*

Ennél nagyobb p esetén, sajnos már túl sokáig tart a pszeudovéletlenségi mérték meghatározása, ezért az ennél nagyobb bináris rácsok esetén csak egy becslést adok ezen mértékekre. A becslést a következő követelmények mellett végeztem:

- Minden vizsgált tégla rácsnak legalább p rácspontot kell tartalmaznia, tehát nem lehet kicsi.
- A vizsgált tégla rácsot bármely irányba legalább $p/3$ helyre lehessen eltolni (azaz a lehetséges d_i-k elemszáma ne legyen kisebb,mint $p/3$).
- A becslés körülbelül fél óránál tovább ne tartson.

Ezen feltételekre azért van szükség, mert 2-dimenziós esetben bizonyított, hogy valódi véletlen rácsokra $Q_2(\eta) \ll \sqrt{2p^2 \log p^2} = o(p \log p)$. Számunkra az lenne negatív eredmény, ha a kapott becslés ennél nagyobb lenne, emiatt

elég csak azokon a tégla rácsokon tekinteni a maximumot, melyek legalább p rácspontot tartalmaznak. A nagyon nagy boxokat csak kevés helyre lehet eltolni, így azok nem adnak elég szabadságot a becsléshez. Az időkorlátra természetesen a megvalósíthatóság miatt van szükség. Mindezek alapján a becsléshez a következőképpen módosítottam a másodrendű korreláció számításomat. A definícióban szereplő maximumot nem az összes tégla rácson néztem, hanem csak a következőkön:

- Egy tégla rács bármely dimenziós hossza minimum $p/3$ és maximum $2p/3$
- Egy tégla rács bármely dimenzióban legalább $p/3$ rácspontot tartalmaz
- Az ennek megfelelő tégla rácsokat pedig nem az összes lehetséges eltolás párral vizsgáltam, hanem csak néhány véletlenszerűen kiválasztottal.

Precízebben:

Definíció. Az η *bináris rács másodrendű véletlenségi mértékének becslése:*

$$\tilde{Q}_{2,r}(\eta) = \max_{\boldsymbol{B},|\boldsymbol{D}|<r,\boldsymbol{T}} \left| \sum_{j_1=0}^{t_1} \sum_{j_2=0}^{t_2} \eta(j_1 b_1 + j_2 b_2 \theta + \boldsymbol{d}_1)\eta(j_1 b_1 + j_2 b_2 \theta + \boldsymbol{d}_2) \right|,$$

ahol r valamint $\boldsymbol{D} = (\boldsymbol{d}_1, \boldsymbol{d}_2)$, $\boldsymbol{B} = (b_1, b_2)$ és $\boldsymbol{T} = (t_1, t_2)$ koordinátáik nemnegatív egészek, b_1, b_2 nem nulla, $\boldsymbol{d}_1, \boldsymbol{d}_2$ függetlenek és $\boldsymbol{d}_1, \boldsymbol{d}_2$ eltolás párok száma $< r$, illetve minden előforduló $j_1 b_1 + j_2 b_2 \theta + \boldsymbol{d}_i$ vektor benne van az n-dimenziós N-rácsban, I_N^n-ben.

Felvetődhet a kérdés, hogy miért tart ilyen sokáig viszonylag "kis" p-k esetén is a másodrendű korreláció kiszámolása? Megnéztem tehát, hogy bizonyos p-k esetében a korreláció számítás definíciójában szereplő maximumot hány tagra kell képezni.

Jelöljük S-sel a másodrendű korrelációban szereplő abszolút értékek számát, azaz azt, hogy összesen hányféleképpen lehet kiválasztani a $(\boldsymbol{B}, (\boldsymbol{d}_1, \boldsymbol{d}_2), \boldsymbol{T})$ hármast,

$$S = \Big|(\boldsymbol{B}, (\boldsymbol{d}_1, \boldsymbol{d}_2), \boldsymbol{T})\Big|$$

p	S
$p = 7$	25245
$p = 11$	494960
$p = 13$	1486494
$p = 17$	8681160
$p = 19$	18030416
$p = 23$	63197200
$p = 29$	288590200
$p = 31$	446458775

4. táblázat. *A vizsgálandó tégla rács párok száma*

A $p = 23$ esetben kapott $S = 63197200$ azt jelenti, hogy a másodrendű korreláció kiszámításához több mint 63 millió tégla rács párt kell megvizsgálni. Ezen hatalmas számok okozzák, hogy $p > 23$ prímek esetén már csak becslést tudtam adni a másodrendű korrelációkra.

3.2.2. Eredményeim

Azt, hogy mennyi véletlenszerűen kiválasztott eltolás párt (r) alkalmaztam egy adott bináris rácsnál, az időkorlát határozta meg. Például $p = 37$ esetén az összes, a feltételnek megfelelő tégla rácsot 5000 véletlenszerűen kiválasztott eltolás párral vizsgáltam. Természetesen az egyre nagyobb p-k egyre kevesebb eltolás párhoz vezettek. Legvégül ($p = 199$ esetén) már csak 10 eltolás párt tudtam figyelembe venni a számítás időigénye miatt. Azt, hogy adott prím

esetén mennyi $(\boldsymbol{d}_1, \boldsymbol{d}_2)$ párral futattam a programot, a táblázatok címében ismertetem.

Nézzük tehát, hogy a 23-nál nagyobb p prímek esetén milyen becsléseket kaptam a másodrendű korrelációs mértékekre.

	Kvadratikus karakter (7)	Multiplikatív inverz (12)	Legendre - szimbólum (13)
$p = 29$	n.a.	71,4	76,4
$p = 31$	72	77,6	75,2
$p = 37$	n.a.	90,6	96,4
$p = 41$	n.a.	102,6	117,8
$p = 43$	106,75	113,2	108,8
$p = 47$	116	123,4	123,2
$p = 53$	n.a.	142	153
$p = 59$	141,5	157,8	158,8
$p = 61$	n.a.	165,2	160,5
$p = 67$	167,5	165	201,4
$p = 71$	178,25	185,8	199,6
$p = 73$	n.a.	185,2	191,75
$p = 79$	192,5	214	212
$p = 83$	205,25	224,4	209
$p = 89$	n.a.	240	239,5
$p = 97$	n.a.	261	243,4
$p = 101$	n.a.	257,6	260,25
$p = 103$	276,5	257,2	269
$p = 107$	274,25	270	278,6
$p = 109$	n.a.	281,8	271,75

5. táblázat. *Másodrendű korrelációk becslése* 1

	Kvadratikus karakter (7)	Multiplikatív inverz (12)	Legendre - szimbólum (13)
$p = 113$	n.a.	281,4	305
$p = 127$	305,25	309,2	321
$p = 131$	327	339,6	345
$p = 137$	n.a.	362	361,75
$p = 139$	327,5	367	346,2
$p = 149$	n.a.	385,8	421,75
$p = 151$	375,25	368,4	372,4
$p = 157$	n.a.	414,6	401,25
$p = 163$	430,4	403,2	386,2
$p = 167$	425,6	432	400,4
$p = 173$	n.a.	423,2	421,75
$p = 179$	428,4	431,6	436,8
$p = 181$	n.a.	447,8	404,25
$p = 191$	454	455,4	458,4
$p = 193$	n.a.	451	471,5
$p = 197$	n.a.	484,8	489
$p = 199$	493	479,8	510,4

6. táblázat. *Másodrendű korrelációk becslése* 2

3.2.3. Magasabb rendű korrelációk

Sajnos, a számolásigény már $k = 3$ esetén is rendkívül nagy. Próbaképpen megnéztem, hogy $p = 19$ esetén mennyi időt venne igénybe a harmadrendű korreláció kiszámítása. Programomat több mint 5 óra futtatás után állítottam le az eredmény ismerete nélkül. Ebben az esetben p rendkívül kicsi volt, míg a futásidő hatalmas. Így nem láttam értelmét megpróbálni magasabb rendű Q_k-k kiszámítását, sem becslését.

3.3. Fokszám analízis

A következőekben azt vizsgálom, miként változik az implementáció idő igénye és a másodrendű korreláció becslés, ha megváltoztatom az f polinomok fokszámát (azaz ℓ-t). $p = 199$ prímhez az eddigi ötödfokú polinomok után, lefuttattam a programomat $\ell = 3$ illetve $\ell = 4$ esetén is, annak reményében, hogy valami érdekes eredményt kapok. Az eredmény a következő lett:

	Kvadratikus karakter (7)	Multiplikatív inverz (12)	Legendre - szimbólum (13)
$\ell = 3$	15,71 s	107,20 s	14,85 s
$\ell = 4$	16,68 s	107,79 s	14,68 s
$\ell = 5$	18,13 s	107,89 s	14,92 s

7. táblázat. *Generálási idők* 3

	Kvadratikus karakter (7)	Multiplikatív inverz (12)	Legendre - szimbólum (13)
$\ell = 3$	518,5	482,2	497,25
$\ell = 4$	527,2	481,6	492,6
$\ell = 5$	493	479,8	510,4

8. táblázat. *Másodrendű korrelációk becslése* 3

4. Eredmények elemzése

4.1. Idő analízis

A 3.1. Idő analízis alfejezetben ismertetett 1. és 2. táblázat adataiból láthatjuk, hogy a kvadratikus karakteres és a Legendre-szimbólumos módszerek közel azonos gyorsaságúak, míg a multiplikatív inverzes módszer lényegesen lassabb náluk. Egy $\mathbb{F}_q$-beli elem multiplikatív inverzének meghatározáshoz szükséges számításigény nem ennyivel nagyobb, mint a Legendre-szimbólum meghatározása, így a különbség nyilvánvalóan a programkódban rejlik.

A Sage sokkal gyorsabban számol $\mathbb{F}_p$ felett, mint $\mathbb{F}_{p^2}$ felett. Ez teljesen természetes, viszont ez csak azt magyarázza, hogy a Legendre-szimbólumos módszer miért gyorsabb a multiplikatív inverzesnél. A Legendre-szimbólumos módszernél az f polinom a következő alakú (14):

$$f(x_1, x_2) = x_1^{\ell} + x_1 x_2 g(x_1, x_2) + x_2 h(x_2),$$

ahol $x_1, x_2 \in \mathbb{F}_p$, azaz $f(x_1, x_2) \in \mathbb{F}_p[x1, x2]$. A kvadratikus karakteres és a multiplikatív inverzes módszer esetén $f(z) = (z + a_1)(z + a_2) \dots (z + a_l)$ ahol $z, a_1, \dots, a_l \in \mathbb{F}_{p^2}$. Hogy lehet mégis, hogy a kvadratikus karakteres módszer futásideje a Legendre-szimbólumos módszer körül van?

Kvadratikus karakteres módszer esetén az $f(z)$-t a következő alakban számolom

$$f(z_1+z_2\theta) = (z_1+z_2\theta+a_{11}+a_{12}\theta)(z_1+z_2\theta+a_{21}+a_{22}\theta)\dots(z_1+z_2\theta+a_{l1}+a_{l2}\theta),$$

ahol z_1, z_2 valamint $a_{ij} \in \mathbb{F}_{p^2}$ minden $i = 1, \dots, l$ és j=1,2 esetén, továbbá $\theta^2 = -1$. $f(x_1, x_2) = p(x_1, x_2) + q(x_1, x_2)\theta$, ami számunkra tökéletes, hisz a módszernél nekünk épp erre volt szükségünk. Tehát ebben az esetben a Sage ugyanúgy $\mathbb{F}_p$-ben számol, mint a Legende-szimbólumos esetben. Felmerül természetesen a kérdés, hogy miért nem alkalmaztam ugyanezt a multiplikatív inverzes módszer esetén is? A válasz abban rejlik,hogy az

$f(x_1, x_2) = p(x_1, x_2) + q(x_1, x_2)\theta$-ból nem tudunk $\mathbb{F}_{p^2}$-beli multiplikatív inverzet számolni.

Fontos megemlítenem azt is, hogy azért nem teszteltem $p = 199$-nél nagyobb prímek esetén a konstrukciókat, mivel másodrendű korrelációt is akartam számolni, ami így erősen korlátozta p méretét. A kriptográfiában azonban egy 199x199-es méretű rács meglehetősen kicsi és gyakorlatilag használhatatlan. Épp ezért megnéztem, hogy az egyes konstrukciókkal mekkora táblákat lehet generálni 10 perc futásidőt engedélyezve.

	Kvadratikus karakter (7)	Multiplikatív inverz (12)	Legendre - szimbólum (13)
p	1123	331	1249

9. táblázat. *Maximális p-k 10 perc futásidő alatt*

A táblázatból látszik, hogy a kvadratikus karakteres és a Legendre-szimbólumos módszert lehetne használni kriptográfiai célból (természetesen csak akkor, ha tudjuk, hogy a generált bináris rács erős pszeudovéletlen tulajdonságú).

4.2. Korreláció analízis

A megfelelő táblázatokból látszik, hogy a konstrukciók másodrendű korrelációjának becslései között nincs lényeges eltérés. Azt is meg kell említeni, hogy a kapott becslések mindegyik esetben $\tilde{Q}_{2,r}(\eta) \ll \sqrt{2}p \log p$, azaz amit vártunk. Fontos észrevételhez jutunk, ha megnézzük mennyi a $\frac{\tilde{Q}_{2,r}(\eta)}{\sqrt{2}p} = Q'$ hányados értéke a $\log p$-hez viszonyítva. Kis p-k esetén Q' értéke fele a $\log p$-nek, míg $p = 199$ esetén már csupán csak a harmada. Mindez arra enged következtetni, hogy azon tégla rács párra a másodrendű korreláció definíciójában szereplő összeg közelebb van p-hez, mint $p \log p$-hez.

4.3. Fokszám analízis

A 3.3 Fokszám analízis alfejezet eredményei alapján arra a következtetésre juthatunk, hogy a különböző konstrukciók esetén bizonyított $Q_k(\eta)$ becslések ((2), (4) és (6)) tovább javíthatók.

Kvadratikus karakteres módszer esetén:

$$Q_k(\eta) < k\ell(q^{1/2}(1+\log p)^n + 2).$$

Multiplikatív inverzes módszer esetén:

$$Q_k(\eta) < (2^{k+3}+1)k\ell n^k q^{1/2}(\log p + 2)^{n+k}.$$

Legendre-szimbólumos módszer esetén:

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

A 8. táblázat eredményei azt mutatják, hogy az f polinom fokszámának (ℓ) megváltoztatása nincs lényeges hatással a másodrendű korrelációs becslésre. Mindez arra enged következtetni, hogy az is lehet, hogy a $Q_k(\eta)$ felső becslésében az ℓ szorzó elhagyható, vagy legalábbis az ℓ-től való függés javítható. A számelméletben gyakori, hogy a bizonyított felső becsléseknél jóval erősebb állítás is igaz, melyekre csak numerikus számítások alapján lehet következtetni.

Fontos, hogy szót ejtsünk a 7. táblázatról is. Az adatok alapján jól látszik, hogy az f polinom fokának növelése a generálási időt is megnöveli, de csak minimálisan. Ez azt jelenti, hogy fokszám növelése egy gyors és hatékony módszer a konstrukciók valódi véletlen magjának növelésére, hisz a módszerek véletlen magja az f polinomok együtthatói. A p prím növelése szintúgy a véletlen magot növeli, de az egy sokkal lassabb megoldás erre a célra.

Függelék

További előismeretek

A véges testek elmélete kiemelkedő fontosságú a kriptográfiában, ezért fontosnak tartom, hogy ismertessek néhány tételt és definíciót ezen témakörből, melyeket diplomamunkám során említettem. Akit részletesebben érdekel a témakör, ajánlanám N. Koblitz *A Course in Number Theory and Cryptography* című könyvét [7].

Tétel. *Jelöljük $\mathbb{Z}_p$-vel a modulo p maradékosztályokat. Ezen maradékosztályok akkor és csak akkor alkotnak testet, ha p prím.*

Definíció. Az $\mathbb{F}$ test *karakterisztikája* az a legkisebb m természetes szám, amelyre $ma = 0$ minden $a \in \mathbb{F}$ esetén. Ha nem létezik ilyen természetes m szám, akkor a test karakterisztikája 0.

Tétel. *$\mathbb{Z}_p$ karakterisztikája p.*

Ennek következményeként kapjuk, hogy $(a+b)^p = a^p + b^p$ amennyiben $a, b \in \mathbb{Z}_p$

Tétel. *Minden véges test tekinthető egy $\mathbb{Z}_p$ feletti vektortérnek, és ha ez a vektortér $n \in \mathbb{N}$ dimenziós, akkor a test elemeinek száma p^n, ahol p prím. Jelölés: $\mathbb{F}_{p^n}$.*

Definíció. Egy $a \in \mathbb{F}_{p^n}$ véges test elemének *multiplikatív inverzén* azt a $b \in \mathbb{F}_{p^n}$ elemet értjük, melyre $ab = 1$.

A következőkben szeretném felsorolni azokat a számelméleti fogalmakat és tételeket, melyek ismerete szükséges a diplomamunkám témájának feldolgozásához.

Definíció. Legyen $p > 2$ prím és $(a, p) = 1$. Az a számot aszerint nevezzük *kvadratikus maradék*nak, illetve *kvadratikus nemmaradéknak modulo p,* hogy az $x^2 \equiv a \pmod{p}$ kongruencia megoldható-e, vagy sem.

Tétel.

(*i*) *Az a szám akkor és csak akkor kvadratikus maradék modulo p, ha $a^{(p-1)/2} \equiv 1 \pmod{p}$. Ezzel ekvivalens, hogy az a (bármely primitív gyök szerinti) indexe páros.*

(*ii*) *Az a szám akkor és csak akkor kvadratikus nemmaradék modulo p, ha $a^{(p-1)/2} \equiv -1 \pmod{p}$. Ezzel ekvivalens, hogy az a (bármely primitív gyök szerinti) indexe páratlan.*

Definíció. Az $\left(\frac{a}{p}\right)$ *Legendre-szimbólumot* a következőképpen értelmezzük:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \textit{ha } a \textit{ kvadratikus maradék mod } p, \\ -1 & \textit{ha } a \textit{ kvadratikus nemmaradék mod } p. \end{cases}$$

A Legendre-szimbólum definícióját összevetve az előző tétellel kapjuk, hogy bármely a esetén

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Definíció. Az $\mathbb{F}_q$ *kvadratikus karakterének* azt az $\mathbb{F}_q$-n értelmezett függvényt nevezzük, melynek definíciója $a \in \mathbb{F}_q$, $a \neq 0$ esetén

$$\gamma(a) = \begin{cases} +1 & \textit{ha } x^2 = a \textit{ megoldható } \mathbb{F}_q\textit{-ban}, \\ -1 & \textit{ha } x^2 = a \textit{ nem megoldható } \mathbb{F}_q\textit{-ban}, \end{cases}$$

és $\gamma(0) = 0$.

Táblázatok

Az összes táblázat és a numerikus számításokhoz használt Sage programkódok megtalálhatóak a diplomamunkámhoz csatolt DVD-n, illetve az alábbi címen: `http://bolyai.cs.elte.hu/~kodila` .

A következőekben illusztrációként ismertetek néhány táblázatot. Kiválasztottam négy prímet 50, 100, 150 és 200 körül, melyekre mindhárom konstrukciót el tudtam végezni.

Kvadratikus karakter	Generálási idő	Q_2becslése
$z^3 + (21\theta + 17)z^2 + (31\theta + 20)z + 24\theta + 35$	1,05 s	118
$z^3 + (27\theta + 40)z^2 + (2\theta + 36)z + 2\theta + 6$	1,32 s	124
$z^3 + (29\theta + 30)z^2 + (37\theta + 42)z + 11\theta + 46$	0,98 s	114
$z^3 + (35\theta + 8)z^2 + (2\theta + 45)z + 34\theta + 35$	1,45 s	108
$z^3 + (17\theta + 10)z^2 + (25\theta + 4)z + 16\theta + 31$	1,50 s	106

Multiplikatív inverz	Generálási idő	Q_2becslése
$z^3 + (8\theta + 45)z^2 + (13\theta + 40)z + 35\theta + 34$	6,16 s	128
$z^3 + (34\theta + 43)z^2 + (9\theta + 18)z + 13\theta + 16$	5,80 s	114
$z^3 + (6\theta + 26)z^2 + (15\theta + 31)z + 3\theta + 35$	5,80 s	125
$z^3 + (31\theta + 12)z^2 + (26\theta + 45)z + 28\theta + 42$	5,75 s	120
$z^3 + (28\theta + 25)z^2 + (34\theta + 21)z + 4\theta + 9$	5,88 s	130

Legendre-szimbólum	Generálási idő	Q_2becslése
$x_1^3 + 7x_1x_2 + 10x_2^2 + 18x_2$	0,95 s	140
$x_1^3 + 3x_1x_2 - 23x_2^2 + 14x_2$	0,84 s	114
$x_1^3 + 19x_1x_2 + 22x_2^2 + 7x_2$	0,82 s	126
$x_1^3 + 14x_1x_2 + x_2^2 + 15x_2$	0,81 s	120
$x_1^3 + 21x_1x_2 + x_2^2 + 4x_2$	0,82 s	116

10. táblázat. *Módszerek eredményei $p = 47$ esetén (2000 eltolás pár)*

Kvadratikus karakter	Gen. idő	Q_2 becslése
$z^4+(8\theta+29)z^3+(31\theta+27)z^2+$ $(25\theta+43)z+48\theta+15$	5,15 s	252
$z^4+(74\theta+3)z^3+(86\theta+20)z^2+$ $(60\theta+102)z+37\theta+90$	4,80 s	249
$z^4+(\theta+62)z^3+(101\theta+89)z^2+$ $(36\theta+16)z+67\theta+99$	4,71 s	332
$z^4+(72\theta+93)z^3+(16\theta+91)z^2+$ $(52\theta+25)z+56\theta+93$	4,64 s	273
$z^4+(44\theta+88)z^3+(60\theta+100)z^2+$ $(42\theta+43)z+87\theta+59$	4,58 s	274

Multiplikatív inverz	Gen. idő	Q_2 becslése
$z^4+(27\theta+10)z^3+(72\theta+28)z^2+$ $(60\theta+76)z+68\theta+55$	30,25 s	261
$z^4+(94\theta+3)z^3+(52\theta+11)z^2+$ $(41\theta+19)z+19\theta+24$	30,45 s	250
$z^4+(8\theta+24)z^3+(92\theta+19)z^2+$ $(23\theta+8)z+54\theta+50$	37,48 s	264
$z^4+(85\theta+66)z^3+(56\theta+7)z^2+$ $67z+31\theta+56$	30,33 s	263
$z^4+(37\theta+59)z^3+(83\theta+97)z^2+$ $72\theta z+30\theta+12$	30,09 s	248

Legendre-szimbólum	Gen. idő	Q_2 becslése
$x_1^4+12x_1^2x_2-18x_1x_2^2+33x_2^3+$ $43x_1x_2-6x_2^2-25x_2$	4,06 s	252
$x_1^4+12x_1^2x_2+44x_1x_2^2+18x_2^3-$ $48x_1x_2-8x_2^2-27x_2$	3,86 s	262
$x_1^4+26x_1^2x_2-51x_1x_2^2-45x_2^3-$ $50x_1x_2-46x_2^2-15x_2$	3,76 s	277
$x_1^4+47x_1^2x_2-6x_1x_2^2+$ $14x_1x_2-38x_2^2+17x_2$	3,79 s	273
$x_1^4-47x_1^2x_2-28x_1x_2^2-44x_2^3+$ $31x_1x_2-42x_2^2+7x_2$	3,78 s	281

11. táblázat. *Módszerek eredményei* $p=103$ *esetén (120 eltolás pár)*

Kvadratikus karakter	Gen. idő	Q_2 becslése
$z^5+(20\theta+112)z^4+(70\theta+131)z^3+$ $(136\theta+51)z^2+(25\theta+30)z+124\theta+9$	11,55 s	390
$z^5+(104\theta+106)z^4+(135\theta+148)z^3+$ $(62\theta+50)z^2+(125\theta+130)z+92\theta+89$	10,45 s	344
$z^5+(126\theta+22)z^4+(159\theta+159)z^3+$ $(19\theta+49)z^2+(53\theta+17)z+49\theta+70$	10,26 s	421
$z^5+(116\theta+13)z^4+(36\theta+101)z^3+$ $(79\theta+40)z^2+(34\theta+79)z+40\theta+114$	10,48 s	346
$z^5+(132\theta+93)z^4+(115\theta+72)z^3+$ $(7\theta+21)z^2+(148\theta+72)z+111\theta+141$	10,43 s	347

Multiplikatív inverz	Gen. idő	Q_2 becslése
$z^5+(119\theta+21)z^4+(115\theta+24)z^3+$ $(144\theta+106)z^2+(88\theta+72)z+49\theta+96$	62,52 s	366
$z^5+(67\theta+100)z^4+(125\theta+143)z^3+$ $(59\theta+5)z^2+(126\theta+118)z+144\theta+59$	60,38 s	356
$z^5+(141\theta+111)z^4+(71\theta+56)z^3+$ $(7\theta+21)z^2+(57\theta+75)z+71\theta+16$	60,29 s	338
$z^5+(111\theta+124)z^4+(122\theta+65)z^3+$ $(74\theta+19)z^2+(75\theta+9)z+116\theta+59$	60,39 s	362
$z^5+(113\theta+55)z^4+(36\theta+3)z^3+$ $(131\theta+115)z^2+(23\theta+139)z+131\theta+111$	60,14 s	420

Legendre-szimbólum	Gen. idő	Q_2 becslése
$x_1^5-59x_1^3x_2-22x_1^2x_2^2+39x_1x_2^3+40x_2^4-$ $5x_1^2x_2-14x_1x_2^2-40x_2^3-15x_1x_2+50x_2^2+12x_2$	9,41 s	422
$x_1^5-28x_1^3x_2-35x_1^2x_2^2-19x_1x_2^3+61x_2^4-$ $29x_1^2x_2-59x_1x_2^2+44x_2^3+71x_1x_2-66x_2^2+16x_2$	8,18 s	416
$x_1^5-6x_1^3x_2+49x_1^2x_2^2-59x_1x_2^3+24x_2^4+$ $10x_1^2x_2-54x_1x_2^2+40x_2^3-24x_1x_2+55x_2^2+43x_2$	8,23 s	334
$x_1^5-48x_1^3x_2-62x_1^2x_2^2+4x_1x_2^3-73x_2^4+$ $19x_1^2x_2+53x_1x_2^2-19x_2^3-63x_1x_2-58x_2^2-22x_2$	8,22 s	350
$x_1^5+52x_1^3x_2+38x_1^2x_2^2-47x_1x_2^3+72x_2^4+$ $20x_1^2x_2+38x_1x_2^2-18x_2^3-67x_1x_2+22x_2^2-14x_2$	8,23 s	340

12. táblázat. *Módszerek eredményei* $p=151$ *esetén (26 eltolás pár)*

Kvadratikus karakter	Gen. idő	Q_2 becslése
$z^5 + (126\theta + 186)z^4 + (13\theta + 66)z^3 +$ $116\theta + 136)z^2 + (110\theta + 81)z + 75\theta$	18,23 s	491
$z^5 + (32\theta + 84)z^4 + (134\theta + 59)z^3 +$ $(40\theta + 56)z^2 + (46\theta + 189)z + 68\theta + 24$	18,13 s	471
$z^5 + (126\theta + 22)z^4 + (159\theta + 159)z^3 +$ $(19\theta + 49)z^2 + (53\theta + 17)z + 49\theta + 70$	18,18 s	457
$z^5 + (42\theta + 120)z^4 + (151\theta + 111)z^3 +$ $(196\theta + 82)z^2 + (25\theta + 13)z + 164\theta + 195$	18,51 s	520
$z^5 + (83\theta + 5)z^4 + (165\theta + 158)z^3 +$ $(85\theta + 31)z^2 + (86\theta + 155)z + 155\theta + 116$	18,13 s	526

Multiplikatív inverz	Gen. idő	Q_2 becslése
$z^5 + (80\theta + 74)z^4 + (183\theta + 98)z^3 +$ $(137\theta + 33)z^2 + (171\theta + 39)z + 54\theta + 139$	108,60 s	489
$z^5 + (138\theta + 8)z^4 + (20\theta + 49)z^3 +$ $(85\theta + 113)z^2 + (182\theta + 169)z + 180\theta + 174$	108,28 s	450
$z^5 + (140\theta + 75)z^4 + (164\theta + 121)z^3 +$ $(50\theta + 84)z^2 + (181\theta + 47)z + 182\theta + 120$	108,02 s	434
$z^5 + (162\theta + 144)z^4 + (34\theta + 153)z^3 +$ $(139\theta + 43)z^2 + (30\theta + 190)z + 29\theta + 58$	108,35 s	536
$z^5 + (5\theta + 34)z^4 + (108\theta + 104)z^3 +$ $(134\theta + 89)z^2 + (3\theta + 98)z + 150\theta + 139$	108,72 s	490

Legendre-szimbólum	Gen. idő	Q_2 becslése
$x_1^5 - 32x_1^3x_2 - 37x_1^2x_2^2 - 68x_1x_2^3 + 94x_2^4 +$ $18x_1^2x_2 + 18x_1x_2^2 - 35x_2^3 + 20x_1x_2 + 47x_2^2 + 53x_2$	15,49 s	533
$x_1^5 + 50x_1^3x_2 + 56x_1^2x_2^2 + 60x_1x_2^3 - 97x_2^4 +$ $51x_1^2x_2 + 66x_1x_2^2 - 61x_2^3 + 41x_1x_2 + 53x_2^2 + 82x_2$	14,51 s	518
$x_1^5 + 76x_1^3x_2 + 40x_1^2x_2^2 + 15x_1x_2^3 + 84x_2^4 +$ $x_1^2x_2 + 57x_2^3 + 53x_1x_2 + 8x_2^2 - 79x_2$	14,27 s	544
$x_1^5 - 90x_1^3x_2 + 86x_1^2x_2^2 + 44x_1x_2^3 - 70x_2^4 +$ $56x_1^2x_2 - 48x_1x_2^2 - 54x_2^3 + 11x_1x_2 - 52x_2^2 + 17x_2$	14,67 s	501
$x_1^5 - 56x_1^3x_2 + 10x_1^2x_2^2 + 92x_1x_2^3 + 15x_2^4 -$ $2x_1^2x_2 - 42x_1x_2^2 - 85x_2^3 + 50x_1x_2 + 36x_2^2 - 73x_2$	14,31 s	456

13. táblázat. *Módszerek eredményei* $p = 199$ *és* $\ell = 5$ *esetén (10 eltolás pár)*

Irodalomjegyzék

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

[2] Z.Chen, S.Li, G.Xiao, *Construction of pseudorandom binary sequences from elliptic curves by using discrete logarithm*, Lecture Notes in Comput. Sci., 4086, Springer, Berlin, (2006) 286-294

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

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

[5] K. Gyarmati, A. Sárközy, C. L. Stewart, *On Legendre symbol lattices, II*, Unif. Distrib. Theory, submitted

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

[7] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, (1994)

[8] H. Liu, *A large family of pseudorandom binary lattices*, Proc. Amer. Math. Soc. 237 (2009), 793-803

[9] C. Mauduit, A. Sárközy, *On finite psedorandom binary sequences I: Measure of pseudorandomness, The Legendre symbol*, Acta Arith. 82 (1997), 365-377

[10] C. Mauduit, A. Sárközy, *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. 108 (2005), 239-252

[11] C. Mauduit, A. Sárközy, *On large families of pseudorandom binary lattices*, Unif. Distrib. Theory 2 (2007), 23-37

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

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

[14] L. Mérai, *On finite pseudorandom lattices of k symbols*, Monatsh. Math. 161 (2010), 173-191

[15] L. Mérai, *Construction of pseudorandom binary lattices using elliptic curves*, Proc. Amer. Math. Soc. 139 (2011), 407-402