Diszkrepanciák számtani sorozatokban

Diplomamunka

Valkó Benedek

Témavezető:
Sárközy András

Eötvös Loránd Tudományegyetem
Természettudományi Kar
2000

Tartalomjegyzék

Bevezetés

Az angol discrepancy szó (egyik) magyar jelentése: egyenetlenség, eltérés. A matematikában a diszkrepancia általában egy adott eloszlás távolságának mértéke az "ideális" (általában egyenletes) eloszlástól. Klasszikus példa a következő: legyen $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$ véges ponthalmaz $[0,1)$-ben. Ha $\mathcal{P}$ eloszlása egyenletes lenne, akkor egy $(x,y) \subseteq [0,1)$ intervallumba nagyjából $n\,(y-x)$ pont kellene, hogy essen. Így nem meglepő, hogy a pontsorozat diszkrepanciáját a következőképpen definiáljuk:

$$D(\mathcal{P}) = \sup_{0 \le x < y < 1} \left| \sum_{x < p_i < y} 1 - n \cdot (x - y) \right| .$$

Látható, hogy fix n mellett létezik "nagyon egyenletes" eloszlású ponthalmaz, hiszen $\mathcal{P} = \left\{0, \frac{1}{n}, \ldots, \frac{n-1}{n}\right\}$ esetén $D(\mathcal{P}) = 2$, azaz n-től független korlát alatt marad, és az is könnyen meggondolható, hogy a kapott eredmény éles. Lényegesen bonyolultabb a helyzet d-dimenzióban (itt a $[0,1)^d$-beli tengelypárhuzamos téglákon vett eltérések szuprémumaként definiáljuk a diszkrepanciát). 1954-ben Roth bebizonyította, hogy $d \ge 2$ esetén tetszőleges n-elemű $\mathcal{P} \subset [0,1)^d$ ponthalmazra $D(\mathcal{P}) \ge c_d (\log n)^{\frac{d-1}{2}}$. Másrészt Halton konstruált tetszőleges d-re és n-re olyan n-elemű $\mathcal{P} \subset [0,1)^d$ ponthalmazt, amelyre $D(\mathcal{P}) \le c_d' (\log n)^{d-1}$. Schmidtnek sikerült bebizonyítania, hogy $d = 2$-re ez éles, de a többi esetben az alsó és felső becslést nem sikerült sokkal közelebb hozni. Szintén érdekes, az eredeti problémával szoros kapcsolatban álló kérdés, hogy mit mondhatunk egy végtelen $\mathcal{P} \subset [0,1)^d$ pontsorozat kezdőszeleteinek diszkrepanciájáról. Itt az első eredmény van Aardenne-Ehrenfest nevéhez fűződik, aki belátta, hogy a kezdőszeletek diszkrepanciái még egy dimenzióban sem lehetnek korlátosak.

Egy pontsorozat eloszlásának egyenletességét ill. irregularitását a tengelypárhuzamos téglatesteken kívül többféle geometriai objektumra nézve is vizsgálták. A terület eredményeinek egy összefoglalása megtalálható például [6]-ban, amelynek irodalomjegyzékében az előbb felsorolt eredményekhez tartozó cikkek is fellelhetőek.

Az eddigi példák alapján a következő (általunk is használt) diszkrepancia definícióhoz jutunk: legyen adott egy X mérhető tér, azon egy μ mérték és mérhető halmazoknak egy $\mathcal{H}$ rendszere. Akkor egy $\mathcal{P} = \{p_1, p_2, \ldots, p_n\} \subset X$ véges ponthalmaz diszkrepanciáját így definiáljuk:

$$D(\mathcal{P}) = \sup_{H \in \mathcal{H}} \left| \sum_{p_i \in H} 1 - n \cdot \mu(H) \right|.$$

Esetünkben X mindig diszkrét lesz, valamely M-re az M-nél nem nagyobb pozitív egészek vagy valamely q-ra a mod q maradékosztályok.

Ezen dolgozat kiindulási problémájával az 1. részben ismerkedhetünk meg. 1964-ben megjelent cikkében ([9]) Roth vizsgálta, hogy az $[1, N] = \{1, 2, \ldots, N\}$ halmaz egy $\eta \cdot N$ elemszámú $\mathcal{A}$ részhalmaza mennyire egyenletesen oszolhat el a számtani sorozatokban. Ha az $n, n+q, \ldots, n+(k-1)q$ számtani sorozatnak t eleme esik $[1, N]$-be, akkor egy "egyenletes" eloszlású $\mathcal{A}$ halmaznak nagyjából $\eta \cdot t$ eleme kellene, hogy essen ebbe a számtani sorozatba. Roth bebizonyította, hogy a nem triviális eseteken kívül (amikor $\eta = 1$ vagy 0) nem létezhet "nagyon egyenletes" $\mathcal{A}$ részhalmaz, van olyan $c > 0$, hogy mindig létezik olyan számtani sorozat, amelyben az eltérés legalább $c\sqrt{\eta(1-\eta)}N^{\frac{1}{4}}$. (A $\sqrt{\eta(1-\eta)}$ faktor 0-vá válik a két triviális esetben.) Tehát ha egy $\mathcal{A}$ halmaz $D(\mathcal{A})$ diszkrepanciáját a számtani sorozatokbeli megfelelő eltérések maximumaként definiáljuk, akkor Roth tétele szerint $D(\mathcal{A}) \geq c\sqrt{\eta(1-\eta)}N^{\frac{1}{4}}$ egy fix pozitív c konstanssal. (Roth célja az akkor még Erdős-Turán sejtésként ismert Szemerédi-tétel bizonyítása volt, és egy 5 cikkből álló sorozatot szentelt a témának. Mint később kiderült ez az út nem volt járható a bizonyításhoz, de így is több, magában is érdekes eredmény adódott a cikkekből.) A másik irányú állításhoz egy rokon problémát vizsgáltak: ha kiszínezzük az $[1, N]$ halmazt két színnel, és tekintjük azt a számtani sorozatot, amelyben a legnagyobb a két szín előfordulása számának különbsége, akkor mennyire kicsivé tehető ez a maximális különbség. (A két probléma közti kapcsolatot az 1.2. részben részletesen tisztázzuk.) Roth cikkéből adódik, hogy ez az eltérés legalább $O\left(N^{\frac{1}{4}}\right)$. Furcsa módon Roth nem gondolta, hogy az eredménye éles, ő azt sejtette, hogy az igazság $N^{\frac{1}{2}-o(1)}$. Ezt látszott alátámasztani az, hogy viszonylag egyszerű valószínűségi eszközökkel bizonyítható, hogy létezik olyan színezés, ahol a legnagyobb eltérés $O\left(\sqrt{N \log N}\right)$. Ezt az eredményt lényegesen megjavította Sárközy ([3]), aki belátta, hogy létezik olyan színezés is, ahol a maximális eltérés legfeljebb $N^{\frac{1}{3}+o(1)}$ (ezzel egyúttal Roth sejtését is megdöntötte). A nagy áttörést Beck 1981-es eredménye hozta ([1]), ő belátta, hogy Roth eredeti eredménye lényegében éles, van olyan színezés, amelyben a legnagyobb eltérés $O\left(N^{\frac{1}{4}} \log^{\frac{5}{2}} N\right)$. Végül 1996-ban megjelent cikkükben Spencer és Matoušek ([11]) végleg lezárták a kérdést, Beck módszerét továbbfejlesztve belátták, hogy Roth eredménye konstans szorzótól eltekintve éles. (Fontos megjegyeznünk, hogy míg a két színnel színezés esetén a maximális abszolútértékű eltérés nagyságrendje ismert, addig a természetesen felmerülő maximális pozitív eltérés kérdése közel sem tisztázott. A problémával kapcsolatos eredmények megtalálhatók például [12], [13], [14], [15]-ben, illetve ezek irodalomjegyzékeiben.)

A dolgozat 2. és 3. fejezetében az előbb ismertetett probléma különböző általánosításai, rokon problémái szerepelnek. A 2. fejezetben a d-dimenziós megfelelőt tárgyaljuk: egy $\mathcal{A} \subseteq [1, N]^d$ halmaz diszkrepanciáját vizsgáljuk a d-dimenziós számtani sorozatokra vonatkozóan. Bebizonyítjuk Roth tételének megfelelőjét, és azt is belátjuk, hogy a kapott eredmény lényegében éles. A kapott eredményt alkalmazzuk egy Knieper által felvetett problémára ([5]). A 3. fejezetben kéttagú összegek eloszlásának irregularitásait vizsgáljuk. Ehhez persze meg kell mondanunk, hogy milyen eloszlástól való eltérést tekintünk, azaz mit tekintünk "ideálisnak". Legyen megint $\mathcal{A} \subseteq [1, N]$ egy $\eta \cdot N$ elemszámú halmaz, és tekintsük az $a_1 + a_2$ alakú összegeket, ahol $a_1, a_2 \in \mathcal{A}$. Legyen $f(n) = \sum\limits_{\substack{a_1+a_2=n \\ a_1,a_2\in\mathcal{A}}} 1$ és $g(n) = \sum\limits_{1\le k,n-k\le N} 1$ (ezek adják meg, hogy n hányféleképpen áll elő $\mathcal{A}$-beli ill. $[1, N]$-beli kéttagú összegként). Ha véletlenszerűen konstruálnánk $\mathcal{A}$-t, hogy minden $n \in [1, N]$ számot egymástól függetlenül η valószínűséggel választanánk be $\mathcal{A}$-ba, akkor $f(n)$ várható értéke körülbelül $\eta^2 g(n)$ lenne (pontosabban a várható érték $\eta^2 g(n) - (\eta^2 - \eta)$ ha n páros, egyébként $\eta^2 g(n)$). Így az $n, n + q, \dots, n + (k - 1) q$ számtani sorozatban "ideális" esetben nagyjából $\sum\limits_{i=0}^{k-1} \eta^2 g(n + iq)$ darab $a_1 + a_2$ alakú összeg kellene, hogy legyen, és ezért érthető, hogy itt a diszkrepanciát a $\left|\sum\limits_{i=0}^{k-1} (f(n + iq) - \eta^2 g(n + iq))\right|$ eltérések maximumaként definiáljuk. Erre a diszkrepanciára bizonyítunk majd alsó becslést, és felső becslést is adunk. Megvizsgáljuk a probléma moduláris változatát is, szintén alsó és felső becsléseket adva a megfelelő diszkrepanciára. A dolgozat utolsó, 4. részében a nyitott kérdéseket összegezzük.

Köszönettel tartozom Sárközy András tanár úrnak a diplomamunka megírásához nyújtott segítségéért, és az évek során kapott rengeteg törődésért, tanításért, továbbá Károlyi Gyulának értékes megjegyzéseiért.

1. Fejezet

Az alapprobléma

Legyen $\mathcal{A} \subseteq [1, N]$ és $\frac{|\mathcal{A}|}{N} = \eta$. Tetszőleges n, $k > 0$, $q > 0$ egészekre legyen

$$V(n,q,k) = \left| \sum_{\substack{0 \le i < k \\ n+iq \in \mathcal{A}}} 1 - \eta \sum_{\substack{0 \le i < k \\ 1 \le n+iq \le N}} 1 \right|,$$

ami (mint a bevezetésben láttuk) azt "méri", hogy az $n, n+q, \ldots, n+(k-1)q$ számtani sorozatban mennyire "egyenletes" az $\mathcal{A}$ eloszlása. Mi azt vizsgáljuk, hogy mennyire lehet kicsi $\max\limits_{n,q,k} V(n,q,k)$.

1.1. Roth tétele és következményei

Roth-tól származik a következő tétel ([9]):

1.1.1. Tétel (Roth). *Tetszőleges $\mathcal{A} \subseteq [1, N]$ halmazhoz léteznek $n, 1 \le q \le \left\lfloor \sqrt{N} \right\rfloor$ egészek, hogy*

$$V(n,q,k) \ge c\sqrt{\eta(1-\eta)}N^{\frac{1}{4}}$$

(ahol c egy N-től független konstans).

A tétel szerint ha $\mathcal{A}$ nem az üres vagy az egész $[1, N]$ halmaz, akkor nem lehet "nagyon" egyenletes az eloszlása a számtani sorozatok között illetve azokon belül. (Ha az előbbi esetek valamelyike áll fenn, akkor $\eta(1-\eta)=0$, ami egybevág $V(n,q,k)\equiv 0$-val.) A tétel bizonyításának alapja a következő állítás, amelyet később mi is többször használni fogunk.

1.1.2. Tétel. *Legyen M pozitív egész, $R \geq 2$ egész, $R_1 = \left\lfloor \frac{R}{2} \right\rfloor$. Legyenek $s_1, s_2, \ldots, s_M$ komplex számok, és definiáljuk s_j-t 0-nak, ha $j \leq 0$ vagy $j > M$. Jelöljük a $\sum\limits_{i=0}^{k-1} s_{n+iq}$ összeget $D(n,q,k)$-val. Ekkor*

$$\sum_{q=1}^{R} \sum_{n=1-(R_1-1)q}^{M} |D(n,q,R_1)|^2 \geq \left(\frac{2}{\pi}R_1\right)^2 \sum_{m=1}^{M} |s_m|^2.$$

Bizonyítás. A bizonyítás exponenciális összegek segítségével történik. Jelölje a továbbiakban $e^{2\pi i\alpha}$-t $e(\alpha)$. Legyen $S(\alpha) = \sum_{n=1}^{M} s_n e(n\alpha)$ (az s_n sorozat generátorfüggvénye), és $H_k(\alpha) = \sum_{n=0}^{k-1} e(n\alpha)$. A kívánt egyenlőtlenséget a

$$J = \int_0^1 |S(\alpha)|^2 \sum_{q=1}^{R} |H_{R_1}(q\alpha)|^2 \, d\alpha$$

kifejezés becslésével nyerjük. $|H_{R_1}(\alpha)| = \left|\frac{\sin(\pi R_1 \alpha)}{\sin(\pi\alpha)}\right|$, és mivel $\frac{2}{\pi}|x| \leq |\sin x| \leq |x|$, ha $|x| \leq \frac{\pi}{2}$, ezért könnyen ellenőrizhető, hogy $|H_{R_1}(\alpha)| \geq \frac{2}{\pi}R_1$, ha $|\alpha| \leq \frac{1}{2R_1}$. Ismert, hogy tetszőleges α-ra léteznek olyan p, q relatív prím R-nél nem nagyobb pozitív egészek, hogy $\left|\alpha - \frac{q}{p}\right| \leq \frac{1}{qR}$. Akkor $|q\alpha - p| \leq \frac{1}{R} \leq \frac{1}{2R_1}$, és így

$$|H_{R_1}(q\alpha)|^2 = |H_{R_1}(p - q\alpha)|^2 \geq \left(\frac{2}{\pi}R_1\right)^2.$$

Ebből következik, hogy tetszőleges α -ra

$$\sum_{q=1}^{R} |H_{R_1}(q\alpha)|^2 \geq \left(\frac{2}{\pi}R_1\right)^2.$$

Ezzel máris egy alsó becslést kaptunk J-re:

$$J \geq \min_{\alpha} \sum_{q=1}^{R} \left| H_{R_1}(q\alpha) \right|^2 \int_0^1 |S(\alpha)|^2 \, d\alpha \geq \left(\frac{2}{\pi} R_1 \right)^2 \sum_{m=1}^{M} |s_m|^2 ,$$

ahol az utolsó egyenlőtlenségnél a Parseval-formulát is alkalmaztuk. Másrészt J definíciójából:

$$\begin{aligned}
J &= \int_0^1 \sum_{q=1}^{R} \left| S(\alpha) H_{R_1}(q\alpha) \right|^2 d\alpha = \sum_{q=1}^{R} \int_0^1 \left| \sum_{m=1}^{M} s_m e(m\alpha) \sum_{j=0}^{R_1-1} e(jq\alpha) \right|^2 d\alpha \\
&= \sum_{q=1}^{R} \int_0^1 \left| \sum_{\substack{1 \leq m \leq M \\ 0 \leq j \leq R_1-1}} s_n e((m+jq)\alpha) \right|^2 d\alpha = \sum_{q=1}^{R} \int_0^1 \left| \sum_{t=1}^{M+(R_1-1)q} \sum_{j=0}^{R_1-1} s_{t-jq} e(t\alpha) \right|^2 d\alpha \\
&= \sum_{q=1}^{R} \int_0^1 \left| \sum_{t=1}^{M+(R_1-1)q} D(t-(R_1-1)q, q, R_1) e(t\alpha) \right|^2 d\alpha \\
&= \sum_{q=1}^{R} \sum_{t=1}^{M+(R_1-1)q} \left| D(t-(R_1-1)q, q, R_1) \right|^2 = \sum_{q=1}^{R} \sum_{n=1-(R_1-1)q}^{M} \left| D(n, q, R_1) \right|^2 .
\end{aligned}$$

(Az átalakítások során változótranszformációt, a Parseval-formulát, illetve a megfelelő definíciókat használtuk.) A nyert eredményt összevetve a J-re kapott alsó becsléssel következik a tétel állítása. □

1.1.3. Következmény. *Létezik n, $1 \leq q \leq R$, hogy*

$$|D(n, q, R_1)| \geq \frac{2}{\pi} R_1 \sqrt{\sum_{m=1}^{M} |s_m|^2} \left(M + \frac{R^2}{4} \right)^{-\frac{1}{2}} R^{-\frac{1}{2}}.$$

Bizonyítás. Legyen $T = \max_{n, 1 \leq q \leq R} |D(n, q, R_1)|$. Akkor az előző tétel állításából adódik, hogy

$$\sum_{q=1}^{R} \sum_{n=1-(R_1-1)q}^{M} T^2 \geq \left(\frac{2}{\pi} R_1 \right)^2 \sum_{m=1}^{M} |s_m|^2 .$$

Egyszerűsítve a bal oldalt:

$$\begin{aligned}\sum_{q=1}^{R}\sum_{n=1-(R_1-1)q}^{M} T^2 &= T^2\sum_{q=1}^{R}(M+(R_1-1)\,q) = T^2\left(MR+(R_1-1)\,\frac{R\,(R+1)}{2}\right)\\ &\le T^2\left(M+\frac{R^2}{4}\right)R.\end{aligned}$$

Innen átrendezéssel következik a bizonyítandó állítás. □

Az alábbi (számunkra igen fontos) következmény egyszerű behelyettesítéssel adódik.

1.1.4. Következmény. *Létezik n, $1 \le q \le \left\lfloor\sqrt{M}\right\rfloor$, hogy*

$$\left|D\left(n,q,\left\lfloor\frac{1}{2}\left\lfloor\sqrt{M}\right\rfloor\right\rfloor\right)\right| \ge c\sqrt{\frac{\sum_{m=1}^{M}|s_m|^2}{M}}M^{\frac{1}{4}}.$$

(Itt c fix konstans, $M \ge M_\varepsilon$ esetén választható $\left(\frac{2}{\pi\sqrt{5}}-\varepsilon\right)$-nak.)

Most már készen állunk az 1.1.1. tétel bizonyítására.

Az 1.1.1. tétel bizonyítása. Használjuk a $Q = \left\lfloor\sqrt{N}\right\rfloor$ és $Q_1 = \left\lfloor\frac{1}{2}Q\right\rfloor$ jelöléseket. Definiáljuk az s_n számokat a következőképpen: $s_n = \eta$ ha $n \notin \mathcal{A}$ és $1 \le n \le N$, $s_n = \eta - 1$ ha $n \in \mathcal{A}$ és $s_n = 0$ egyébként. Az 1.1.4. következmény szerint létezik n, $1 \le q \le Q$, hogy

$$\begin{aligned}\left|\sum_{i=0}^{Q_1-1} s_{n+iq}\right| &\ge c\sqrt{\frac{\sum_{m=1}^{N}|s_n|^2}{N}}N^{\frac{1}{4}} = c\sqrt{\frac{\eta^2\,(1-\eta)\,N+(1-\eta)^2\,\eta N}{N}}N^{\frac{1}{4}}\\ &= c\sqrt{\eta\,(1-\eta)}N^{\frac{1}{4}}.\end{aligned}$$

Másrészt vegyük észre, hogy tetszőleges n, $k>0$, $q>0$ egészekre

$$\left|\sum_{i=0}^{k-1} s_{n+iq}\right| = \left|\sum_{\substack{0\le i<k\\ n+iq\in\mathcal{A}}}(\eta-1) + \sum_{\substack{0\le i<k\\ n+iq\notin\mathcal{A}\\ 1\le n+iq\le N}}\eta\right| = \left|\eta\sum_{\substack{0\le i<k\\ 1\le n+iq\le N}}1 - \sum_{\substack{0\le i<k\\ n+iq\in\mathcal{A}}}1\right| = V\,(n,q,k),$$

amiből következik a tétel állítása. □

Érdemes megjegyeznünk, hogy Roth bizonyítása nem csak azt mutatja, hogy létezik olyan számtani sorozat, amelyben "nagy" az egyenletes eloszlástól való eltérés, hanem azt is, hogy ezek az eltérések négyzetes középben nagyok.

Tekintsünk még egy számunkra lényeges alkalmazást.

1.1.5. Állítás. *Bárhogyan színezzük két színnel az $1, 2, \ldots, N$ számokat, létezik olyan számtani sorozat, amelyben legalább $c\sqrt[4]{N}$-nel több van az egyik színből, mint a másikból (c fix konstans).*

Bizonyítás. Jelöljük a két színt $+1$-gyel és -1-gyel, és definiáljuk az s_n számokat a színezésnek megfelelően ($s_n = 0$ ha $n \leq 0$ vagy $n > N$). Az 1.1.4. következményből azonnal adódik a bizonyítandó állítás. □

1.2. A diszkrepancia felső becslése

Roth tétele alsó becslést ad a legnagyobb eltérésre. Ha felső becslést szeretnénk, akkor olyan (nem triviális) $\mathcal{A} \subseteq [1, N]$ halmazt kell keresnünk, ami minden számtani sorozatban egyenletesen oszlik el (a lehetőségekhez mérten), azaz minden számtani sorozatban az eltérés $O\left(\sqrt[4]{N}\right)$. Mint a bevezetőben is említettük, a felső becsléshez nem konkrétan ezt a problémát vizsgálták, hanem az 1.1.5. állítás megfelelőjét, azaz, hogy ki lehet-e színezni két színnel $[1, N]$-et úgy, hogy mindegyik számtani sorozatban a két szín előfordulásának eltérése $O\left(\sqrt[4]{N}\right)$. A következő állítás a két probléma közötti szoros kapcsolatra világít rá. (A továbbiakban egy H halmaz két színnel színezése alatt mindig egy $f : H \to \{-1, 1\}$ függvényt értünk. Ekkor egy adott H_1 részhalmazban a két szín előfordulásának eltérése $\left|\sum_{h \in H_1} f(h)\right|$.)

1.2.1. Állítás. *Tegyük fel, hogy f az $[1, N]$ egy olyan két színnel színezése, amelyre minden számtani sorozatban a két szín előfordulásának eltérése legfeljebb C. Ekkor létezik olyan $\mathcal{A} \subseteq [1, N]$, hogy $|\mathcal{A}| = \left\lfloor \frac{N}{2} \right\rfloor$, és tetszőleges n, $k > 0$, $q > 0$ egészekre $V(n, q, k) \leq C + \frac{1}{2}$.*

Bizonyítás. Mivel az $1, 2, \ldots, N$ sorozat is számtani sorozat, így $\left|\sum_{n=1}^{N} f(n)\right| \leq C$. Akkor legfeljebb $\frac{C}{2}$ helyen az ellentettjére változtatva f-et elérhető, hogy a $+1$-ekből vagy a -1-ekből éppen $\left\lfloor \frac{N}{2} \right\rfloor$ darab legyen. Nyilván feltehetjük, hogy a $+1$-ekből van ennyi. Így most minden számtani sorozatban a két szín előfordulásának eltérése legfeljebb $C + 2\frac{C}{2} = 2C$. Legyen $\mathcal{A} = \{n \,|\, f(n) = 1\} \subseteq [1, N]$, belátjuk, hogy ez teljesíti az állítás feltételeit. Ehhez azt kell belátnunk, hogy tetszőleges k elemű $H \subseteq [1, N]$ számtani sorozatra

$$\left| \sum_{n \in H \cap \mathcal{A}} 1 - \eta k \right| \leq C + \frac{1}{2}.$$

Mivel $\left|\eta - \frac{1}{2}\right| \leq \frac{1}{2N}$, és $k \leq N$, ezért elég igazolni, hogy

$$\left| \sum_{n \in H \cap \mathcal{A}} 1 - \frac{1}{2} k \right| \leq C.$$

Ehhez vegyük észre, hogy

$$\sum_{n \in H \cap \mathcal{A}} 1 - \frac{1}{2} k = \frac{1}{2} \sum_{n \in H} f(n),$$

és így az előzőek miatt következik a bizonyítandó állítás. □

A bevezetőben leírtuk, hogy meglehetősen hosszú ideig tartott, amíg bebizonyították, hogy az 1.1.5. állítás éles. Viszont az, hogy a bizonyítás nem javítható, már lényegesebben korábban ismert volt (lásd pl. [13]). Mint már korábban is megjegyeztük, a bizonyításból nem csak az jön ki, hogy van olyan H számtani sorozat, amire

$$\left| \sum_{n \in H} f(n) \right| \geq c\sqrt[4]{N},$$

hanem hogy ez négyzetes középben is teljesül, pontosabban, hogy

$$\sum_{q=1}^{Q} \sum_{n=1-(Q_1-1)q}^{N} |D(n,q,Q_1)|^2 \geq \left(\frac{2}{\pi}Q_1\right)^2 \sum_{m=1}^{N} |s_m|^2 \geq c' N^2.$$

(Itt az előző részben megismert jelöléseket használjuk, $Q = \left\lfloor \sqrt{N} \right\rfloor$, $Q_1 = \left\lfloor \frac{1}{2}Q \right\rfloor$, $s_n = f(n)$, ha $1 \leq n \leq N$, és 0 egyébként, és $D(n,q,Q_1) = \sum_{i=0}^{Q_1-1} s_{n+iq}$.) Célunk először az, hogy megmutassuk, hogy ez éles, azaz minden N-re létezik olyan színezés, hogy

$$\sum_{q=1}^{Q} \sum_{n=1-(Q_1-1)q}^{N} |D(n,q,Q_1)|^2 \leq cN^2$$

teljesül alkalmas fix c-vel.

1.2.2. Állítás. *Ha $S(\alpha) = \sum_{n=1}^{N} f(n)\, e(n\alpha)$-ra teljesül, hogy $|S(\alpha)| \leq c_1\sqrt{N}$ minden α-ra, akkor*

$$\sum_{q=1}^{Q} \sum_{n=1-(Q_1-1)q}^{N} |D(n,q,Q_1)|^2 \leq cN^2$$

valamely c_1-től függő c-vel.

Bizonyítás. Tudjuk, hogy

$$\sum_{q=1}^{Q} \sum_{n=1-(Q_1-1)q}^{N} |D(n,q,Q_1)|^2 = \int_0^1 |S(\alpha)|^2 \sum_{q=1}^{Q} |H_{Q_1}(q\alpha)|^2\, d\alpha.$$

A jobb oldalt triviálisan becsülve:

$$\int_0^1 |S(\alpha)|^2 \sum_{q=1}^{Q} |H_{Q_1}(q\alpha)|^2\, d\alpha \leq c_1^2 N \int_0^1 \sum_{q=1}^{Q} |H_{Q_1}(q\alpha)|^2\, d\alpha.$$

Mivel a definíció szerint $H_k(\alpha) = \sum_{n=0}^{k-1} e(n\alpha)$, ezért a Parseval-formula szerint

$$c_1^2 N \int_0^1 \sum_{q=1}^{Q} |H_{Q_1}(q\alpha)|^2\, d\alpha = c_1^2 N Q Q_1.$$

Innen pedig Q és Q_1 definíciója miatt következik az állítás. $\square$

Így most már elég találnunk N-hez N-edfokú polinomot, amelynek konstans tagja 0, többi együtthatója ± 1, és egyenletesen kis abszolútértékű az egységkörön. Ehhez az ismert Rudin-Shapiro konstrukciót használjuk (pl. [10]). Legyen $P_0(z) = Q_0(z) = 1$, és $n \geq 1$-re legyen

$$P_n(z) = P_{n-1}(z) + z^{2^{n-1}} Q_{n-1}(z), \text{ és } Q_n(z) = P_{n-1}(z) - z^{2^{n-1}} Q_{n-1}(z).$$

Teljes indukcióval könnyen bizonyítható, hogy $|z| = 1$ esetén

$$|P_n(z)|^2 + |Q_n(z)|^2 = 2^{n+1},$$

amiből következik, hogy $|P_n(z)|$ legfeljebb $\sqrt{2}\sqrt{2^n}$ az egységkörön. Így tetszőleges n-re $zP_n(z)$ olyan 2^n fokszámú polinom, amely eleget tesz a kívánt feltételeknek, és ezek segítségével tetszőleges N-hez tudunk konstruálni megfelelő polinomot. A konstrukcióból látszik, hogy létezik olyan $\varepsilon_1, \varepsilon_2, \ldots$ ± 1-ekből álló végtelen sorozat, hogy $zP_n(z) = \sum_{i=1}^{2^n} \varepsilon_i z^i$, legyen $N \geq 1$-re $S_N(\alpha) = \sum_{j=1}^{N} \varepsilon_i e(j\alpha)$. Egyszerűen igazolható, hogy $|S_N(\alpha)| \leq 5\sqrt{N}$ tetszőleges α-ra, azaz $S_N(\alpha)$ kielégíti az 1.2.2. állításhoz szükséges feltételeket. Ezzel beláttuk, hogy valóban éles a négyzetes középre vonatkozó alsó becslés.

Most a maximumra vonatkozó felső becslés tárgyalására térünk rá. A nagy áttörést Beck 1981-es tétele hozta ([1]).

1.2.3. Tétel (Beck). *Minden N-re létezik olyan $f : [1, N] \to \{-1, 1\}$ színezés, hogy tetszőleges $\{n, n+q, \ldots, n+(k-1)q\} \subseteq [1, N]$ számtani sorozatra*

$$\left| \sum_{i=0}^{k-1} f(n+iq) \right| \leq c\sqrt[4]{N} (\log N)^{\frac{5}{2}}.$$

Az állítás egy sokkal általánosabb, hipergráfok diszkrepanciájára vonatkozó tételből következik. Ahhoz, hogy ezt kimondhassuk, először be kell vezetnünk néhány jelölést.

Hipergráf alatt itt véges halmazok egy véges rendszerét értjük. Egy adott $\mathcal{H}$ hipergráf esetén legyen

$$\begin{aligned} S(\mathcal{H}) &= \bigcup_{A\in\mathcal{H}} A && \text{(a csúcsok halmaza)},\\ \deg(\mathcal{H},x) &= |\{A\in\mathcal{H} : x\in A\}| && (x \text{ foka } \mathcal{H}\text{-ban}),\\ \deg(\mathcal{H}) &= \max_x \deg(\mathcal{H},x) && (\mathcal{H} \text{ foka}). \end{aligned}$$

Legyen továbbá

$$\operatorname{disc}(\mathcal{H}) = \min_{g:S(\mathcal{H})\to\{-1,1\}} \max_{A\in\mathcal{H}} \left|\sum_{x\in A} g(x)\right|.$$

(Ez mutatja meg, hogy mennyire egyenletesen lehet kiszínezni két színnel a hipergráfunkat.)

1.2.4. Tétel (Beck). *Legyen $\mathcal{H}$ hipergráf, és tegyük fel, hogy létezik olyan t valós szám, hogy*

$$\deg(\{A\in\mathcal{H} : |A|\geq t\}) \leq t.$$

Akkor

$$\operatorname{disc}(\mathcal{H}) \leq c_0\sqrt{t}\sqrt{(\log|\mathcal{H}|)}\log|S(\mathcal{H})|,$$

ahol c_0 fix konstans.

Először megmutatjuk, hogy hogyan következik az 1.2.3. tétel a 1.2.4. tételből.

Az 1.2.3. tétel bizonyítása. A továbbiakban $i\leq j$ esetén jelöljük $\mathrm{AP}(a,d,i,j)$-vel azt a d-differenciájú számtani sorozatot, amelynek első eleme $a+id$, utolsó eleme pedig $a+jd$. A következő nagyon fontos fogalmat Beck vezette be. Egy számtani sorozatot *eleminek* nevezünk, ha a hossza 2-hatvány (pl. 2^s, $s\geq 0$), a differenciája

$d \geq 1$, és az első eleme $b + (i2^s)\, d$, ahol $1 \leq b \leq d$, $i \geq 0$. Azaz formálisan, ha $\mathrm{AP}(b, d, i2^s, (i+1)\, 2^s - 1)$ alakú, ahol $1 \leq b \leq d$, $d \geq 1$, $i \geq 0$ és $s \geq 0$. Jelöljük $\mathcal{H}_N$-nel az $[1, N]$-be eső elemi számtani sorozatok családját. A definícióból adódóan

$$\begin{aligned}\deg\left(\{A \in \mathcal{H}_N : |A| \geq k\}\right) &= \max_m \left|\{m \in \mathrm{AP}\left(b, d, i2^s, (i+1)\, 2^s - 1\right) \subseteq [1, N] : 2^s \geq k\}\right| \\ &= \max_m \sum_{1 \leq d \leq \frac{N}{k}} \sum_{\substack{1 \leq b \leq d \\ b \equiv m \bmod d}} \sum_{\substack{2^s \geq k \\ b + (2^s - 1) d \leq N}} 1.\end{aligned}$$

(A rövidség kedvéért nem írtuk bele a második tagba az összes szükséges feltételt.) Könnyen látható, hogy

$$\sum_{\substack{2^s \geq k \\ b + (2^s - 1) d \leq N}} 1 \leq \log_2\left(\frac{N}{dk}\right),$$

így

$$\deg\left(\{A \in \mathcal{H}_N : |A| \geq k\}\right) \leq \max_m \sum_{1 \leq d \leq \frac{N}{k}} \sum_{\substack{1 \leq b \leq d \\ b \equiv m \mod d}} \log_2\left(\frac{N}{dk}\right) = \sum_{1 \leq d \leq \frac{N}{k}} \log_2\left(\frac{N}{dk}\right) \leq c_1 \frac{N}{k}$$

egy megfelelő c_1 konstanssal (az utolsó lépés következik például a Stirling formulából). Ezért $t = \sqrt{c_1 N}$ választással alkalmazható az 1.2.4. tétel:

$$\mathrm{disc}\left(\mathcal{H}_N\right) \leq c_0 \sqrt{t} \sqrt{\left(\log |\mathcal{H}_N|\right) \log \left|S\left(\mathcal{H}_N\right)\right|}.$$

Egyszerű leszámlálással adódik, hogy $|\mathcal{H}_N| \leq 2N^2$, és mert $S\left(\mathcal{H}_N\right) = [1, N]$, ezért

$$\mathrm{disc}\left(\mathcal{H}_N\right) \leq c_2 \sqrt[4]{N} \left(\log N\right)^{\frac{3}{4}}.$$

Ez azt jelenti, hogy létezik olyan $f : [1, N] \to \{-1, 1\}$ színezés, hogy tetszőleges $A \subseteq [1, N]$ elemi számtani sorozatra

$$\left|\sum_{n \in A} f(n)\right| \leq c_2 \sqrt[4]{N} \left(\log N\right)^{\frac{3}{4}}.$$

Belátjuk, hogy ez a színezés eleget tesz a tételünk feltételeinek. Először is vegyük észre, hogy tetszőleges $H = \{a, a+d, \ldots, a+md\} \subseteq [1, N]$ számtani sorozat előáll

$$\mathrm{AP}\,(b, d, 0, p_1) \setminus \mathrm{AP}\,(b, d, 0, p_2)$$

alakban, ahol $a = b + p_2 d$, $1 \leq b \leq d$, és $p_1 = m + p_2$. $i = 1, 2$-re legyen $p_i + 1$ kettes számrendszerbeli felírása

$$p_i + 1 = \sum_{j=1}^{l_i} 2^{s(i,j)},\ s\,(i,1) > s\,(i,2) > \ldots > s\,(i, l_i)\,.$$

Akkor

$$\mathrm{AP}\,(b, d, 0, p_i) = \bigcup_{r=1}^{l_i} \mathrm{AP}\left(b, d, \sum_{j=1}^{r-1} 2^{s(i,j)}, \sum_{j=1}^{r} 2^{s(i,j)} - 1\right),$$

ahol láthatóan diszjunkt unió szerepel. Azaz $\mathrm{AP}(b, d, 0, p_i)$ felbontható $l_i \leq \log_2 N$ diszjunkt elemi számtani sorozat uniójára. Ez viszont az elemi számtani sorozatok diszkrepanciájáról kapott becsléssel együtt azt adja, hogy

$$\left|\sum_{n \in H} f\,(n)\right| \leq (2 \log_2 N)\, c_2 \sqrt[4]{N}\,(\log N)^{\frac{3}{4}} = c\sqrt[4]{N}\,(\log N)^{\frac{5}{4}}\,,$$

és éppen ezt kellett belátnunk. □

Az 1.2.4. tétel bizonyításának alapja a következő lemma:

1.2.5. Lemma. *Az 1.2.4. tétel feltételei mellett létezik olyan* $f : S\,(\mathcal{H}) \to \{0, -1, +1\}$ *függvény, hogy*

$$|\{x \in S\,(\mathcal{H}) : f\,(x) = 0\}| \leq \frac{9}{10}\,|S\,(\mathcal{H})|\,, \tag{1}$$

és

$$\left|\sum_{x \in A} f\,(x)\right| \leq c_2 \sqrt{t} \sqrt{\log |\mathcal{H}|}\ \textit{minden}\ A \in \mathcal{H}\ \textit{halmazra}, \tag{2}$$

ahol c_2 *fix konstans.*

A lemma szerint a hipergráfunknak létezik olyan részleges egyenletes színezése, hogy az elemek legalább $\frac{1}{10}$-ed része ki van színezve. A nekünk szükséges teljes egyenletes színezést a lemma sorozatos egymás utáni alkalmazásával kapjuk majd.

Bizonyítás. A bizonyítás tulajdonképpen leszámlálással történik, de a háttérben valószínűségszámítási megfontolások vannak.

Legyen $\mathcal{H}^* = \{A \in \mathcal{H} : |A| \geq t\}$, $|S(\mathcal{H})| = N$, és $|\mathcal{H}^*| = K$. Jelöljük G-vel a $g : S(\mathcal{H}) \to \{-1, +1\}$ függvények halmazát. Tetszőleges $A \in \mathcal{H}$ halmazra

$$\left\{ g \in G : \left| \sum_{x \in A} g(x) \right| \geq \mu \sqrt{|A|} \right\} = 2^{N-|A|} \sum_{|i-|A|/2| \geq \frac{1}{2}\mu\sqrt{|A|}} \binom{|A|}{i} \leq 2^{N-|A|} 2^{|A|} \left(2e^{-2\mu^2} \right),$$

ahol az utolsó egyenlőtlenség az ismert Chernoff-egyenlőtlenségből következik ([2]). Ebből adódik, hogy egy megfelelően nagy c_3 konstanssal a

$$G_1 = \left\{ g \in G : \left| \sum_{x \in A} g(x) \right| \geq c_3 \sqrt{|A| \log |\mathcal{H}|} \text{ minden } A \in \mathcal{H}\text{-ra} \right\}$$

halmaz számossága legalább 2^{N-1} (az előző egyenlőtlenség segítségével meg tudjuk becsülni a "rossz" függvények számát).

Legyen $\mathcal{H}^* = \{A_1, A_2, \ldots, A_K\}$, és minden $1 \leq i \leq K$ egészre osszuk fel az

$$I_i = \left[-c_3 \sqrt{|A_i| \log |\mathcal{H}|}, c_3 \sqrt{|A_i| \log |\mathcal{H}|} \right]$$

intervallumot $r_i = \left\lfloor \sqrt{\frac{|A_i|}{t}} \right\rfloor$ darab egyenlő részre:

$$I_i = \bigcup_{j=1}^{r_i} I_{i,j}.$$

Egy tetszőleges $g \in G_1$ függvényhez rendeljünk hozzá egy K-dimenziós $\underline{v}(g)$ vektort a következő módon:

$$\underline{v}(g) = (j_1, j_2, \ldots, j_K),$$

ahol minden $1 \le i \le K$ egészre

$$\sum_{x \in A_i} g(x) \in I_{i,j_i}.$$

Belátjuk, hogy legfeljebb $2^{\frac{3N}{10}}$ darab ilyen vektor képződött. A definíció szerint

$$|\{\underline{v}(g) : g \in G_1\}| \le \prod_{i=1}^{K} r_i \le \prod_{i=1}^{K} \sqrt{\frac{|A_i|}{t}} \le \exp\left(\frac{\sum_{i=1}^{K} |A_i|}{2et}\right) \le \exp\left(\frac{\sum_{i=1}^{K} |A_i|}{5t}\right).$$

Közben felhasználtuk a következő ismert egyenlőtlenséget: tetszőleges $b_1, b_2, \ldots, b_K$ valós számokra

$$\prod_{i=1}^{K} b_i \le \exp\left(\frac{\sum_{i=1}^{K} b_i}{e}\right).$$

A lemma feltételei szerint $\deg(\mathcal{H}^*) \le t$, emiatt

$$\sum_{i=1}^{K} |A_i| = \sum_{x \in S(\mathcal{H})} \deg(\mathcal{H}^*, x) \le |S(\mathcal{H})| \deg(\mathcal{H}^*) \le |S(\mathcal{H})| t = Nt,$$

és így valóban

$$|\{\underline{v}(g) : g \in G_1\}| \le e^{\frac{N}{5}} \le 2^{\frac{3N}{10}}.$$

Akkor a skatulya-elv miatt létezik G_1-nek olyan G_2 részhalmaza, amire

$$|G_2| \ge |G_1| 2^{-\frac{3N}{10}} \ge 2^{-\frac{7N}{10}-1},$$

és $\underline{v}(g_1) = \underline{v}(g_2)$ minden $g_1, g_2 \in G_2$ függvényre.

Válasszunk egy tetszőleges $g_0 \in G_2$ függvényt, és legyen

$$F_2 = \left\{\frac{g_0 - g_1}{2} : g \in G_2\right\}.$$

Vizsgáljuk meg, milyen függvények lesznek F_2-ben. Látható, hogy a halmazban olyan $f : S(\mathcal{H}) \to \{0, -1, +1\}$ függvények vannak, amelyekre

$$\left|\sum_{x \in A} f(x)\right| \le 2 \max_{g \in G_2} \left|\sum_{x \in A} g(x)\right| \le 2c_3 \sqrt{|A| \log |\mathcal{H}|} \le 2c_3 \sqrt{t \log |\mathcal{H}|}$$

minden $A \in \mathcal{H} \setminus \mathcal{H}^* = \{A \in \mathcal{H} : |A| < t\}$ halmazra, és ha $A \in \mathcal{H}^*$, akkor

$$\left|\sum_{x\in A} f(x)\right| \leq \max_{i,j} |I_{i,j}| \leq \max_i 2c_3 \sqrt{|A_i| \log |\mathcal{H}|} / \left\lfloor \sqrt{\frac{|A_i|}{t}} \right\rfloor \leq c_4 \sqrt{t \log |\mathcal{H}|}$$

egy megfelelő c_4 konstanssal. Összegezve eredményeinket azt kapjuk, hogy F_2 minden eleme teljesíti a (2) feltételt, és így elég találnunk egyetlen olyan F_2-beli elemet, amely teljesíti (1)-et.

Legyen F^* azon $f : S(\mathcal{H}) \to \{0, -1, +1\}$ függvények halmaza, amelyekre

$$|\{x \in S(\mathcal{H}) : f(x) = 0\}| \geq \frac{9}{10} |S(\mathcal{H})| = \frac{9}{10} N.$$

Látható, hogy

$$|F^*| = \sum_{i=0}^{\lfloor N/10 \rfloor} \binom{N}{i} 2^i \leq 2 \binom{N}{\lfloor N/10 \rfloor} 2^{\frac{N}{10}} < 2^{-\frac{7N}{10}-1} \leq |F_2|,$$

ezért az $F_2 \setminus F^*$ halmaz nem üres, és ebből már következik a lemma állítása. □

Az 1.2.4. tétel bizonyítása. Az 1.2.5. lemma szerint létezik olyan $f_1 : S(\mathcal{H}) \to \{0, -1, +1\}$ függvény, amire teljesül (1) és (2). Jelölje $\mathcal{H}_1$ a $\mathcal{H}$ megszorítását arra a halmazra, ahol f_1 eltűnik, azaz legyen

$$\mathcal{H}_1 = \left\{ A \cap f_1^{-1}(\{0\}) : A \in \mathcal{H} \right\}.$$

Nyilván

$$\deg(\{B \in \mathcal{H}_1 : |B| \geq t\}) \leq \deg(\{A \in \mathcal{H} : |A| \geq t\}) \leq t,$$

azaz $\mathcal{H}_1$-re is alkalmazható a 1.2.5. lemma, létezik olyan $f_2 : S(\mathcal{H}_1) \to \{0, -1, +1\}$ függvény, amire teljesül (1) és (2). Folytatva ezt az eljárást, az i-dik lépésben egy olyan $f_i : S(\mathcal{H}_{i-1}) \to \{0, -1, +1\}$ függvényt kapunk, amire

$$|\{x \in S(\mathcal{H}_{i-1}) : f_i(x) = 0\}| \leq \frac{9}{10} |S(\mathcal{H}_{i-1})|,$$

és

$$\left|\sum_{x\in B} f_i(x)\right| \leq c_2\sqrt{t}\sqrt{\log|\mathcal{H}_{i-1}|} \text{ minden } B\in\mathcal{H}_{i-1} \text{ halmazra.}$$

Az eljárás megáll, ha olyan függvényt kapunk, amely csak +1-et és −1-et vesz fel. Mivel a lemma állításából adódóan

$$|S(\mathcal{H}_i)| \leq \frac{9}{10}|S(\mathcal{H}_{i-1})| \leq \left(\frac{9}{10}\right)^i |S(\mathcal{H})|,$$

ezért ez be is következik legfeljebb $\left\lfloor \log|S(\mathcal{H})| / \log\left(\frac{10}{9}\right)\right\rfloor + 1$ lépésen belül. Legyen $g = \sum_{i\geq 1} f_i$. Látható, hogy így egy $S(\mathcal{H}) \to \{-1,+1\}$ függvényt kaptunk. Adott $A\in\mathcal{H}$ esetén $i\geq 1$-re jelölje A_i az $A\cap S(\mathcal{H}_i)$ halmazt, és $A_0 = A$. Az eljárás szabályából következik, hogy

$$\begin{aligned}
\left|\sum_{x\in A} g(x)\right| &= \left|\sum_{i\geq 1}\sum_{x\in A_{i-1}} f_i(x)\right| \leq \sum_{i\geq 1}\left|\sum_{x\in A_{i-1}} f_i(x)\right| \\
&\leq \sum_{i\geq 1} c_2\sqrt{t}\sqrt{\log|\mathcal{H}_{i-1}|} \leq c_2\sqrt{t}\sqrt{\log|\mathcal{H}|}\left(\left\lfloor \log|S(\mathcal{H})| / \log\left(\frac{10}{9}\right)\right\rfloor + 1\right) \\
&\leq c_0\sqrt{t}\sqrt{\log|\mathcal{H}|}\log|S(\mathcal{H})|
\end{aligned}$$

egy megfelelő fix c_0 konstanssal. Ezzel pedig beláttuk a tétel állítását. □

A következőkben az lesz a célunk, hogy teljes általánosságban belássuk, hogy az 1.1.1. tétel lényegében éles.

1.2.6. Tétel. *Legyenek N és K adott pozitív egészek, és $0<\eta=\frac{K}{N}<1$. Akkor létezik olyan $\mathcal{A}\subseteq[1,N]$, hogy $|\mathcal{A}| = K = \eta N$, és tetszőleges n, $k>0$, $q>0$ egészekre*

$$V(n,q,k) \leq c\sqrt[4]{N}(\log N)^{\frac{5}{2}}.$$

A bizonyításhoz az 1.2.4. tétel egy általánosabb alakja szükséges. A továbbiakban tegyük fel, hogy $\mathcal{H}$ hipergráf, melyre $S(\mathcal{H}) = [1, N]$. A definíció szerint

$$\operatorname{disc}(\mathcal{H}) = \min_{g:[1,N]\to\{-1,1\}} \max_{A\in\mathcal{H}} \left| \sum_{i\in A} g(i) \right|.$$

Ezt kicsit más alakban felírva:

$$\operatorname{disc}(\mathcal{H}) = 2 \min_{g:[1,N]\to\{0,1\}} \max_{A\in\mathcal{H}} \left| \sum_{i\in A} \left(g(i) - \frac{1}{2} \right) \right|.$$

Így már könnyen összehasonlítható a diszkrepancia az alább definiált *lineáris diszkrepanciával*:

$$\operatorname{lindisc}(\mathcal{H}) = \max_{\alpha_1,\dots,\alpha_N\in[0,1]} \min_{g:[1,N]\to\{0,1\}} \max_{A\in\mathcal{H}} \left| \sum_{i\in A} (g(i) - \alpha_i) \right|,$$

világos, hogy

$$2\operatorname{lindisc}(\mathcal{H}) \geq \operatorname{disc}(\mathcal{H}).$$

Másrészt az alábbi tétel szerint a lineáris diszkrepancia felülről becsülhető az ún. *öröklött diszkrepanciával*, amelynek definíciója:

$$\operatorname{herdisc}(\mathcal{H}) = \max_{X\subseteq[1,N]} \operatorname{disc}(\{A\cap X : A \in \mathcal{H}\}),$$

(azaz $\mathcal{H}$ megszorításainak diszkrepanciái közül a legnagyobb).

1.2.7. Tétel (Lovász-Spencer-Vesztergombi [7]).

$$\operatorname{lindisc}(\mathcal{H}) \leq \operatorname{herdisc}(\mathcal{H}).$$

Vegyük észre, hogy az 1.2.4. tétel feltétele öröklődik a megszorításra, azaz ha

$$\deg(\{A \in \mathcal{H} : |A| \geq t\}) \leq t,$$

akkor $\mathcal{H}_1 = \{A \cap X : A \in \mathcal{H}\}$-re teljesül

$$\deg\left(\{A \in \mathcal{H}_1 : |A| \geq t\}\right) \leq t.$$

Így az 1.2.4. tétel felső becslést szolgáltat herdisc($\mathcal{H}$)-ra, és az 1.2.7. tétel segítségével lindisc($\mathcal{H}$)-ra is. Tehát igaz a következő állítás:

1.2.8. Állítás. *Az 1.2.4. tétel feltételei mellett*

$$\operatorname{lindisc}(\mathcal{H}) \leq c_0\sqrt{t}\sqrt{(\log|\mathcal{H}|)\log|S(\mathcal{H})|}\,.$$

Ha a lineáris diszkrepancia definíciójában az $\{\alpha_1, \ldots, \alpha_N \in [0,1]\}$ halmaz helyett a kisebb $\{\alpha_1 = \ldots = \alpha_N = \eta \in [0,1]\}$ halmazon vesszük a maximumot, akkor nyilván nem nő a maximum értéke. Így kapjuk az alábbi következményt:

1.2.9. Következmény. *Az 1.2.4. tétel feltételei mellett tetszőleges $0 \leq \eta \leq 1$ esetén létezik olyan $f : [1,N] \to \{1-\eta, -\eta\}$ függvény, hogy tetszőleges $A \in \mathcal{H}$ esetén*

$$\left|\sum_{i \in A} f(i)\right| \leq c_0\sqrt{t}\sqrt{(\log|\mathcal{H}|)\log|S(\mathcal{H})|}\,.$$

Most már nincs nehéz dolgunk az 1.2.6. tétel bizonyításával.

Az 1.2.6. tétel bizonyítása. Az 1.2.9. következményből az 1.2.3. bizonyításával analóg módon belátható, hogy létezik olyan $f : [1,N] \to \{1-\eta, -\eta\}$ függvény, hogy tetszőleges $\{n, n+q, \ldots, n+(k-1)q\} \subseteq [1,N]$ számtani sorozatra

$$\left|\sum_{i=0}^{k-1} f(n+iq)\right| \leq c_0\sqrt[4]{N}(\log N)^{\frac{5}{2}}\,.$$

Lényegében elismételve az 1.2.1. állítás bizonyítását könnyen igazolható, hogy van olyan $f : [1,N] \to \{1-\eta, -\eta\}$ függvény, hogy $\sum\limits_{n=1}^{N} f(n) = 0$, és tetszőleges $[1,N]$-beli $\{n, n+q, \ldots, n+(k-1)q\}$ számtani sorozatra

$$\left|\sum_{i=0}^{k-1} f(n+iq)\right| \leq c\sqrt[4]{N}(\log N)^{\frac{5}{2}}$$

egy alkalmas c konstanssal. Az $\mathcal{A} = \{n : f(n) = 1 - \eta\}$ definícióval így éppen egy $K = \eta N$ elemű halmazt definiáltunk, és egyszerűen ellenőrizhető, hogy erre teljesülnek a 1.2.6. tétel feltételei. $\square$

2. Fejezet

d-dimenziós számtani sorozatok diszkrepanciája

Az évek során Roth eredményét többen általánosították különböző irányokban. Knieper a következő problémát vizsgálta ([5]): legyen $d \geq 1$, és jelöljük $\mathcal{S}$-sel $[1,N]^d$ azon részhalmazainak halmazát, amelyek előállnak d darab $[1,N]$-beli számtani sorozat direkt szorzata; mekkora lesz $\mathcal{S}$ diszkrepanciája. (Látható, hogy a $d=1$ eset visszaadja az eredeti problémát.) Belátta, hogy $\operatorname{disc}(\mathcal{S}) \geq cN^{\frac{d}{4}}$, és hogy ez a becslés log-hatványtól eltekintve éles. Mi most egy másik természetesen felmerülő általánosítást vizsgálunk. Legyen $\mathcal{H}$ az $[1,N]^d$-be eső számtani sorozatok halmaza, azaz

$$\mathcal{H} = \left\{ \{\underline{a} + k \cdot \underline{b} : 0 \leq k \leq r\} \subset [1,N]^d \right\},$$

(ez szintén visszadja az eredeti problémát $d=1$-re). Megmutatjuk, hogy

$$\operatorname{disc}(\mathcal{H}) \geq cN^{\frac{d}{2d+2}},$$

és ez a becslés log-hatványtól eltekintve éles, továbbá a kapott eredményt akalmazzuk egy Knieper által felvetett problémára.

A továbbiakban az aláhúzott változók d-dimenziós vektorokat jelölnek ($\mathbb{R}^d$ vagy $\mathbb{Z}^d$-belieket), $\langle .,. \rangle$ a megfelelő skaláris szorzat.

2.1. A diszkrepancia alsó becslése

A bizonyításhoz az 1.1.2. tételt és következményeit igazoljuk általánosabb formában.

2.1.1. Tétel. *Legyen* $\left\{c_{\underline{a}}, \underline{a} \in [1,N]^d\right\}$ *komplex számok egy rögzített halmaza, és legyen* $c_{\underline{a}} = 0$ *ha* $\underline{a} \notin [1,N]^d$. *Legyenek továbbá* Q, Q_1 *pozitív egészek, amelyekre teljesül* $Q^d \geq 2Q_1$, $N \geq Q$. *Tetszőleges* $\underline{a}, \underline{b} \in \mathbb{Z}^d$ *esetén legyen* $D(\underline{a},\underline{b}) = \sum_{k=0}^{Q_1-1} c_{\underline{a}+k\cdot\underline{b}}$, *és vezessük be az*

$$\mathcal{A} = \{\underline{b} : \underline{b} = (b_1, b_2, \ldots, b_d) \neq \underline{0}, |b_i| \leq Q \text{ minden } 1 \leq i \leq d\text{-re}\}$$

és

$$\mathcal{B}(\underline{b}) = \bigcup_{k=0}^{Q_1-1} \left([1,N]^d - k \cdot \underline{b}\right)$$

jelöléseket. Akkor

$$\sum_{\underline{b}\in\mathcal{A}} \sum_{\underline{a}\in\mathcal{B}(\underline{b})} |D(\underline{a},\underline{b})|^2 \geq \left(\frac{2}{\pi}Q_1\right)^2 \sum_{\underline{a}\in[1,N]^d} |c_{\underline{a}}|^2 .$$

Bizonyítás. A bizonyítás az 1.1.2. tétel bizonyításával analóg módon történik. $\underline{\alpha} \in [0,1]^d$-re legyen $S(\underline{\alpha}) = \sum_{\underline{a}\in[1,N]^d} c_{\underline{a}} \cdot e(\langle \underline{a}, \underline{\alpha} \rangle)$ és $x \in [0,1]$-re $H(x) = \sum_{k=0}^{Q_1-1} e(k \cdot x)$. Az alábbi integrált fogjuk vizsgálni:

$$J = \int_{[0,1]^d} |S(\underline{\alpha})|^2 \sum_{\underline{b}\in\mathcal{A}} |H(\langle \underline{b}, \underline{\alpha} \rangle)|^2 \, d\underline{\alpha}.$$

Legyen $\underline{b} \in \mathcal{A}$ tetszőleges fix vektor, és tekintsük $\int\limits_{[0,1]^d} |S(\underline{\alpha})|^2 |H(\langle \underline{b}, \underline{\alpha} \rangle)|^2 \, d\underline{\alpha}$-t:

$$\begin{aligned}\int\limits_{[0,1]^d} |S(\underline{\alpha})|^2 |H(\langle \underline{b}, \underline{\alpha} \rangle)|^2 \, d\underline{\alpha} &= \int\limits_{[0,1]^d} \left| \left(\sum_{\underline{a} \in [1,N]^d} c_{\underline{a}} \cdot e(\langle \underline{a}, \underline{\alpha} \rangle) \right) \left(\sum_{k=0}^{Q_1-1} e(k \cdot \langle \underline{b}, \underline{\alpha} \rangle) \right) \right|^2 d\underline{\alpha} \\ &= \int\limits_{[0,1]^d} \left| \sum_{\underline{a} \in [1,N]^d} c_{\underline{a}} \cdot \sum_{k=0}^{Q_1-1} e(\langle \underline{a} + k \cdot \underline{b}, \underline{\alpha} \rangle) \right|^2 d\underline{\alpha}.\end{aligned}$$

$\mathcal{B}(\underline{b})$ definíciójából könnyen belátható, hogy

$$\sum_{\underline{a} \in [1,N]^d} c_{\underline{a}} \cdot \sum_{k=0}^{Q_1-1} e(\langle \underline{a} + k \cdot \underline{b}, \underline{\alpha} \rangle) = \sum_{\underline{a} \in \mathcal{B}(\underline{b})} e(\langle \underline{a}, \underline{\alpha} \rangle) \left(\sum_{k=0}^{Q_1-1} c_{\underline{a}+k\cdot\underline{b}} \right).$$

A Parseval formula d-dimenziós változata szerint, ha $G(\underline{\alpha}) = \sum\limits_{\underline{a} \in \mathbb{Z}^d} h_{\underline{a}} \cdot e(\langle \underline{a}, \underline{\alpha} \rangle)$ (ahol az összeg konvergens), akkor $\int\limits_{[0,1]^d} |G(\underline{\alpha})|^2 \, d\underline{\alpha} = \sum\limits_{\underline{a} \in \mathbb{Z}^d} |h_{\underline{a}}|^2$. Ezt felhasználva

$$\begin{aligned}\int\limits_{[0,1]^d} \left| \sum_{\underline{a} \in [1,N]^d} c_{\underline{a}} \cdot \sum_{k=0}^{Q_1-1} e(\langle \underline{a} + k \cdot \underline{b}, \underline{\alpha} \rangle) \right|^2 d\underline{\alpha} &= \int\limits_{[0,1]^d} \left| \sum_{\underline{a} \in \mathcal{B}(\underline{b})} e(\langle \underline{a}, \underline{\alpha} \rangle) \left(\sum_{k=0}^{Q_1-1} c_{\underline{a}+k\cdot\underline{b}} \right) \right|^2 d\underline{\alpha} \\ &= \sum_{\underline{a} \in \mathcal{B}(\underline{b})} \left| \sum_{k=0}^{Q_1-1} c_{\underline{a}+k\cdot\underline{b}} \right|^2 = \sum_{\underline{a} \in \mathcal{B}(\underline{b})} |D(\underline{a}, \underline{b})|^2,\end{aligned}$$

és így

$$J = \sum_{\underline{b} \in \mathcal{A}} \sum_{\underline{a} \in \mathcal{B}(\underline{b})} |D(\underline{a}, \underline{b})|^2.$$

Tehát a tétel bizonyításához J-re kell alsó becslést adnunk. A 2.1.2. lemmában majd belátjuk, hogy tetszőleges $\underline{\alpha} \in [0,1]^d$-re

$$\sum_{\underline{b} \in \mathcal{A}} |H(\langle \underline{b}, \underline{\alpha} \rangle)|^2 \geq \left(\frac{2}{\pi} Q_1 \right)^2.$$

Ebből pedig már következik a bizonyítandó állítás, hiszen

$$\begin{aligned} J &\geq \min_{\underline{\alpha}\in[0,1]^d} \sum_{\underline{b}\in\mathcal{A}} \left|H\left(\langle \underline{b}, \underline{\alpha}\rangle\right)\right|^2 \int\limits_{[0,1]^d} \left|S\left(\underline{\alpha}\right)\right|^2 d\underline{\alpha} \\ &= \min_{\underline{\alpha}\in[0,1]^d} \sum_{\underline{b}\in\mathcal{A}} \left|H\left(\langle \underline{b}, \underline{\alpha}\rangle\right)\right|^2 \sum_{\underline{a}\in[1,N]^d} \left|c_{\underline{a}}\right|^2 \geq \left(\frac{2}{\pi}Q_1\right)^2 \sum_{\underline{a}\in[1,N]^d} \left|c_{\underline{a}}\right|^2. \end{aligned}$$

□

2.1.2. Lemma.

$$\sum_{\underline{b}\in\mathcal{A}} \left|H\left(\langle \underline{b}, \underline{\alpha}\rangle\right)\right|^2 \geq \left(\frac{2}{\pi}Q_1\right)^2$$

Bizonyítás. Korábban már láttuk, hogy $\left|H\left(x\right)\right|^2 = \frac{\sin^2(\pi Q_1 x)}{\sin^2(\pi x)}$, és ha $\|x\| \leq \frac{1}{2Q_1}$, akkor $\left|H\left(x\right)\right|^2 \geq \left(\frac{2}{\pi}Q_1\right)^2$ ($\|x\|$ az x távolságát jelöli a legközelebbi egésztől). A Dirichlet-féle szimultán approximáció tétel szerint tetszőleges $\underline{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_d) \in [0,1]^d$ vektorhoz létezik olyan $\underline{b}^* \in \mathcal{A}$, hogy $\|\langle \underline{b}^*, \underline{\alpha}\rangle\| \leq \frac{1}{Q^d} \leq \frac{1}{2Q_1}$ teljesül. Innen már következik a lemma:

$$\sum_{\underline{b}\in\mathcal{A}} \left|F\left(\langle \underline{b}, \underline{\alpha}\rangle\right)\right|^2 \geq \left|F\left(\langle \underline{b}^*, \underline{\alpha}\rangle\right)\right|^2 \geq \left(\frac{2}{\pi}Q_1\right)^2.$$

□

2.1.3. Tétel. $Q = \left\lfloor 2N^{\frac{1}{d+1}} \right\rfloor$, $Q_1 = \left\lfloor \frac{Q^d}{2} \right\rfloor$ *választással létezik olyan* $\underline{a}, \underline{b} \in \mathbb{Z}^d$, *hogy*

$$\left|D\left(\underline{a}, \underline{b}\right)\right| \geq c \cdot N^{\frac{d}{2d+2}} \sqrt{\frac{\sum_{\underline{a}\in[1,N]^d} \left|c_{\underline{a}}\right|^2}{N^d}},$$

ahol c d-től függő konstans.

Bizonyítás. Alkalmazzuk a 2.1.1. tételt (a feltételek teljesülnek), és az egyszerűség kedvéért a továbbiakban legyen $S = \sum_{\underline{a}\in[1,N]^d} \left|c_{\underline{a}}\right|^2$. A tétel szerint

$$\sum_{\underline{b}\in\mathcal{A}} \sum_{\underline{a}\in\mathcal{B}(\underline{b})} \left|D\left(\underline{a}, \underline{b}\right)\right|^2 \geq \left(\frac{2}{\pi}Q_1\right)^2 S.$$

Jelöljük $\max\limits_{\underline{b}\in\mathcal{A},\underline{a}\in\mathcal{B}(\underline{b})} |D(\underline{a},\underline{b})|$-et M-mel. Az előző egyenlőtlenségből:

$$M^2 \sum_{\underline{b}\in\mathcal{A}} |\mathcal{B}(\underline{b})| \geq \left(\frac{2}{\pi}Q_1\right)^2 S. \tag{1}$$

Legyen $\underline{b}=(b_1,b_2,\ldots,b_d)\in\mathcal{A}$ rögzített vektor. Akkor

$$\begin{aligned}
\mathcal{B}(\underline{b}) &= \bigcup_{k=0}^{Q_1-1}\left([1,N]^d - k\cdot\underline{b}\right)\\
&= \left(\bigcup_{k=0}^{Q_1-2}\left([1,N]^d - k\cdot\underline{b}\right)\setminus\left([1,N]^d-(k+1)\cdot\underline{b}\right)\right)\bigcup\left([1,N]^d-(Q_1-1)\cdot\underline{b}\right),
\end{aligned}$$

és egyszerűen ellenőrizhető, hogy a jobb oldalon álló Q_1 darab halmaz diszjunkt. Látható, hogy

$$\begin{aligned}
\left|\left([1,N]^d - k\cdot\underline{b}\right)\setminus\left([1,N]^d-(k+1)\cdot\underline{b}\right)\right| &= \left|\left([1,N]^d\right)\setminus\left([1,N]^d-\underline{b}\right)\right|\\
&= N^d - \prod_{i=1}^{d}(N-|b_i|),
\end{aligned}$$

(felhasználva, hogy $|b_i|\leq Q\leq N$ minden $1\leq i\leq d$-re), és ezért

$$|\mathcal{B}(\underline{b})| = (Q_1-1)\left(N^d-\prod_{i=1}^{d}(N-|b_i|)\right)+N^d = Q_1N^d-(Q_1-1)\prod_{i=1}^{d}(N-|b_i|).$$

Így

$$\begin{aligned}
\sum_{\underline{b}\in\mathcal{A}}|\mathcal{B}(\underline{b})| &= \left(\sum_{-Q\leq b_1\leq Q}\ \sum_{-Q\leq b_2\leq Q}\cdots\sum_{-Q\leq b_d\leq Q}|\mathcal{B}(\underline{b})|\right)-|\mathcal{B}(\underline{0})|\\
&= \left(\sum_{-Q\leq b_1\leq Q}\ \sum_{-Q\leq b_2\leq Q}\cdots\sum_{-Q\leq b_d\leq Q}\left(Q_1N^d-(Q_1-1)\prod_{i=1}^{d}(N-|b_i|)\right)\right)-N^d\\
&= \left((2Q+1)^dQ_1-1\right)N^d-(Q_1-1)\prod_{i=1}^{d}\sum_{-Q\leq b_i\leq Q}(N-|b_i|)\\
&= \left((2Q+1)^dQ_1-1\right)N^d-(Q_1-1)\left((2Q+1)N-Q(Q+1)\right)^d.
\end{aligned}$$

Ha $x \geq y \geq 0$, akkor

$$dx^{d-1}y \geq y \sum_{j=0}^{d-1} x^{d-1-j} (x-y)^j = x^d - (x-y)^d,$$

ezért

$$(x-y)^d \geq x^d - dx^{d-1}y.$$

Alkalmazva ezt $x = (2Q+1)N$ és $y = Q(Q+1)$ választással:

$$\begin{aligned}
\sum_{\underline{b} \in \mathcal{A}} |\mathcal{B}(\underline{b})| &\leq \left((2Q+1)^d Q_1 - 1\right) N^d - \\
&\quad - (Q_1 - 1)\left((2Q+1)^d N^d - dQ(Q+1)(2Q+1)^{d-1} N^{d-1}\right) \\
&= \left((2Q+1)^d - 1\right) N^d + d(Q_1-1) Q(Q+1)(2Q+1)^{d-1} N^{d-1} \\
&\leq 3^d Q^d N^d + d\, 3^d Q_1 Q^{d+1} N^{d-1} \leq c_1(d) Q_1 N^{d-1} (N + QQ_1).
\end{aligned}$$

Összevetve ezt a korábban nyert (1) egyenlőtlenséggel:

$$M \geq \sqrt{c_2(d) \frac{Q_1^2 S}{Q_1 N^{d-1}(N+QQ_1)}} \geq c(d) N^{\frac{d}{2d+2}} \sqrt{\frac{S}{N^d}},$$

és éppen ezt kellett belátnunk. □

2.1.4. Következmény.

$$\operatorname{disc}(\mathcal{H}) \geq cN^{\frac{d}{2d+2}},$$

ahol a c konstans csak d-től függ.

Bizonyítás. Azt kell belátnunk, hogy tetszőleges $f : [1,N]^d \to \{-1,1\}$ függvényhez létezik olyan $\underline{a}, \underline{a}+\underline{b}, \dots, \underline{a}+r\cdot\underline{b}$ számtani sorozat $[1,N]^d$-ben, amelyre

$$\left| \sum_{k=0}^{r} f(\underline{a} + k \cdot \underline{b}) \right| \geq cN^{\frac{d}{2d+2}}.$$

Alkalmazva a 2.1.3. tételt a $c_{\underline{a}} = f(\underline{a})$ ($\underline{a} \in [1,N]^d$) számokra éppen a bizonyítandó állítást kapjuk. □

Könnyen bizonyítható az alábbi, 1.1.1. tétellel analóg állítás is:

2.1.5. Következmény. *Tetszőleges $\mathcal{A} \subseteq [1,N]^d$ halmazhoz létezik olyan $[1,N]^d$-beli $\{\underline{a} + i \cdot \underline{b} : 0 \le i < k\}$ számtani sorozat, amelyre*

$$\left| \sum_{\substack{0 \le i < k \\ \underline{a} + i \cdot \underline{b} \in \mathcal{A}}} 1 - \eta k \right| \ge c \sqrt{\eta (1 - \eta)} N^{\frac{d}{2d+2}},$$

ahol $\eta = \frac{|\mathcal{A}|}{N^d}$, és c d-től függő konstans.

2.2. A diszkrepancia felső becslése

Először megmutatjuk, hogy az előbb belátott 2.1.4. és 2.1.5. állítások élesek. Ehhez az 1.2.6. tétel bizonyítását fogjuk adaptálni.

2.2.1. Tétel. *Minden N-re létezik olyan $f : [1,N]^d \to \{-1, 1\}$ színezés, hogy tetszőleges $\{\underline{a}, \underline{a} + \underline{b}, \dots, \underline{a} + (k-1)\underline{b}\} \subseteq [1,N]^d$ számtani sorozatra*

$$\left| \sum_{i=0}^{k-1} f(n + iq) \right| \le c N^{\frac{d}{2d+2}} (\log N)^{\frac{5}{2}}.$$

Bizonyítás. Jelöljük $i \le j$ esetén $\mathrm{AP}(\underline{a}, \underline{b}, i, j)$-vel azt a $\underline{b}$-differenciájú számtani sorozatot, amelynek első eleme $\underline{a} + i\underline{b}$, utolsó eleme pedig $\underline{a} + j\underline{b}$. Szükségünk lesz a d-dimenziós elemi számtani sorozatokra. Egy számtani sorozatot eleminek nevezünk, ha a hossza 2-hatvány (pl. 2^s, $s \ge 0$), a differenciája $\underline{b} \ne \underline{0}$, és az első eleme $\underline{a} + (i 2^s)\underline{b}$, ahol $i \ge 0$ és $\underline{a} \in [1,N]^d \setminus \left([1,N]^d - \underline{b}\right)$. Azaz formálisan, ha $\mathrm{AP}(\underline{a}, \underline{b}, i2^s, (i+1)2^s - 1)$ alakú, ahol i, s, $\underline{a}$, $\underline{b}$ teljesíti az előbb felsorolt feltételeket (d = 1-re ez lényegében visszadja az eredeti definíciót). Jelöljük $\mathcal{H}_N$-nel az $[1,N]^d$-be eső elemi számtani sorozatok családját. Próbájuk meg megbecsülni egy fix k-ra a

$\deg(\{A \in \mathcal{H}_N : |A| \geq k+1\})$ értékét. A definícióból adódóan

$$\deg\left(\{A \in \mathcal{H}_N : |A| \geq k+1\}\right) =$$
$$= \max_{\underline{m}} \left|\left\{\underline{m} \in \mathrm{AP}\left(\underline{a}, \underline{b}, i2^s, (i+1)\,2^s - 1\right) \subseteq [1,N]^d : 2^s \geq k+1\right\}\right|$$

(ahol persze a második tagban $\mathrm{AP}(\underline{a}, \underline{b}, i2^s, (i+1)\,2^s - 1)$ elemi számtani sorozat). Ahhoz, hogy létezzen $\underline{b}$ differenciájú legalább $k+1$ hosszú számtani sorozat $[1,N]^d$-ben, minden $1 \leq j \leq d$-re teljesülnie kell az alábbi egyenlőtlenségnek:

$$-\frac{N}{k} \leq b_j \leq \frac{N}{k},$$

(ahol $\underline{b} = (b_1, \ldots, b_d)$). Fix $\underline{b}, \underline{m} \in [1,N]^d$-re pontosan egy olyan $[1,N]^d \setminus \left([1,N]^d - \underline{b}\right)$-beli $\underline{a}$ vektor van, amelyből $\underline{b}$ differenciájú számtani sorozattal el tudunk jutni $\underline{m}$-be (vegyük a legnagyobb olyan $l \geq 0$-t, amelyre még teljesül $\underline{m} - l \cdot \underline{b} \in [1,N]^d$, akkor csak a kapott $\underline{m} - l \cdot \underline{b}$ lehet megfelelő $\underline{a}$-ra). Ha $\underline{a}, \underline{b} \in [1,N]^d$ és $s \geq 0$ rögzített, akkor ahhoz, hogy létezzen $\mathrm{AP}(\underline{a}, \underline{b}, i2^s, (i+1)\,2^s - 1) \subseteq [1,N]^d$ elemi számtani sorozat, $\underline{a} + (2^s - 1)\,\underline{b} \in [1,N]^d$-nek kell teljesülnie. (Világos, hogy ha ez teljesül, akkor legfeljebb egy olyan $i \geq 0$ van, amire $\underline{m} \in \mathrm{AP}(\underline{a}, \underline{b}, i2^s, (i+1)\,2^s - 1)$.) Látható, hogy ha $\underline{a}, \underline{b} \in [1,N]^d$ rögzített, akkor s legfeljebb $\log_2\left(\frac{N}{k \max\limits_{1\leq j\leq d} |b_j|}\right)$ olyan különböző értéket vehet fel, amire $2^s \geq k+1$, és $\underline{a} + (2^s - 1)\,\underline{b} \in [1,N]^d$. Bevezetve a $\|b\|_d = \max\limits_{1\leq j\leq d} |b_j|$ jelölést, eddigi eredményeink így összegezhetők:

$$\deg\left(\{A \in \mathcal{H}_N : |A| \geq k+1\}\right) \leq \sum_{\|b\|_d \leq \frac{N}{k}} \log_2\left(\frac{N}{k\,\|b\|_d}\right).$$

Rögzített $z \geq 1$ egész esetén

$$\left|\left\{\|\underline{m}\|_d = z : \underline{m} \in \mathbb{Z}^d\right\}\right| = \left|[-z, z]^d \setminus [-(z-1), z-1]^d\right| = (2z+1)^d - (2z-1)^d,$$

ahol $[-z, z] = \{-z \leq n \leq z : n \in \mathbb{Z}\}$. Emiatt

$$\sum_{\|b\|_d \leq \frac{N}{k}} \log_2\left(\frac{N}{k\,\|b\|_d}\right) = \sum_{1 \leq z \leq \frac{N}{k}} \left((2z+1)^d - (2z-1)^d\right) \log_2\left(\frac{N}{kz}\right).$$

Az $f(z) = (2z-1)^d$ jelölést bevezetve:

$$\sum_{1 \le z \le \frac{N}{k}} \left((2z+1)^d - (2z-1)^d\right) \log_2\left(\frac{N}{kz}\right) = \int_1^{\lfloor \frac{N}{k} \rfloor + 1} \log_2\left(\frac{N}{k\lfloor z \rfloor}\right) df(z)$$

$$= \left(3^d - 1\right) \log_2\left(\frac{N}{k}\right) + \int_2^{\lfloor \frac{N}{k} \rfloor + 1} \log_2\left(\frac{N}{k\lfloor z \rfloor}\right) df(z).$$

Az $f(z)$ függvény monoton nő, $\log_2\left(\frac{N}{k\lfloor z \rfloor}\right) \le \log_2\left(\frac{N}{k(z-1)}\right)$, ha $z > 1$, ezért

$$\left(3^d - 1\right) \log_2\left(\frac{N}{k}\right) + \int_2^{\lfloor \frac{N}{k} \rfloor + 1} \log_2\left(\frac{N}{k\lfloor z \rfloor}\right) df(z) \le$$

$$\le \left(3^d - 1\right) \log_2\left(\frac{N}{k}\right) + \int_1^{\lfloor \frac{N}{k} \rfloor} \log_2\left(\frac{N}{kz}\right) df(z).$$

Mivel

$$\int \log_2\left(\frac{u}{z}\right) df(z) = \int d \log_2\left(\frac{u}{z}\right) z^{d-1} dz = z^d \left(\log_2\left(\frac{u}{z}\right) + \frac{1}{d \log 2}\right),$$

ezért

$$\int_1^{\lfloor \frac{N}{k} \rfloor} \log_2\left(\frac{N}{kz}\right) df(z) = \left\lfloor \frac{N}{k} \right\rfloor^d \left(\log_2\left(\frac{N}{k\left\lfloor \frac{N}{k} \right\rfloor}\right) + \frac{1}{d\log 2}\right) - \left(\log_2\left(\frac{N}{k}\right) + \frac{1}{d \log 2}\right).$$

Ezek után már könnyen ellenőrizhető, hogy létezik olyan csak d-től függő c_1 konstans, amellyel

$$\deg\left(\{A \in \mathcal{H}_N : |A| \ge k+1\}\right) \le \sum_{1 \le z \le \frac{N}{k}} \left((2z+1)^d - (2z-1)^d\right) \log_2\left(\frac{N}{kz}\right) \le c_1 \left(\frac{N}{k+1}\right)^d.$$

Így $t = (c_1 N)^{\frac{d}{d+1}}$ választással $\mathcal{H}_N$-re teljesül az 1.2.4. tétel feltétele, és a tétel állítása szerint ezért

$$\operatorname{disc}(\mathcal{H}_N) \le c_0 \sqrt{t} \sqrt{(\log |\mathcal{H}_N|) \log |S(\mathcal{H}_N)|}.$$

Ha $\mathrm{AP}(\underline{a}, \underline{b}, i2^s, (i+1)\,2^s-1) \subseteq [1,N]^d$ elemi, akkor $1 \leq j \leq d$-re $b_j = 0$ vagy $\mathrm{AP}(a_j, b_j, i2^s, (i+1)\,2^s-1) \subseteq [1,N]$ elemi számtani sorozat egydimenzióban. Egyszerű leszámlálás mutatja, hogy egydimenziós elemi számtani sorozatból legfeljebb $2N^2$ darab van, ezért

$$|\mathcal{H}_N| \leq c_2 N^{2d}$$

valamely c_2 konstanssal. Mivel $|S(\mathcal{H}_N)| = N^d$, ezért az előző egyenlőtlenségekből

$$\mathrm{disc}\,(\mathcal{H}_N) \leq cN^{\frac{d}{2d+2}}\,(\log N)^{\frac{3}{2}}$$

adódik, ahol a konstans csak d-től függ.

Innen a már látott úton fejezhető be a bizonyítás. Tetszőleges $[1,N]^d$-be eső számtani sorozat felírható

$$\mathrm{AP}\,(\underline{a}, \underline{b}, 0, p_1) \setminus \mathrm{AP}\,(\underline{a}, \underline{b}, 0, p_2)$$

alakban, ahol $\underline{a} \in [1,N]^d \setminus \left([1,N]^d - \underline{b}\right)$, és mindkét számtani sorozat $[1,N]^d$-be esik. $\mathrm{AP}(\underline{a}, \underline{b}, 0, p_i)$ viszont $i = 1,2$-re felírható legfeljebb $\log_2 N$ elemi számtani sorozat diszjunkt uniójaként, ebből pedig következik a tétel állítása. □

Knieper azt is vizsgálta, hogy mi mondható az $[1,N]^2$ négyzetrács szakaszainak diszkrepanciájáról ([5]). Tehát most a hipergráfunk

$$\mathcal{H}_L = \left\{\mathrm{AP}\,(\underline{a}, \underline{b}, 0, k) \subseteq [1,N]^2 : \underline{b} = (b_1, b_2) \neq \underline{0} \text{ és } b_1, b_2 \text{ relatív prímek}\right\},$$

és $\mathrm{disc}(\mathcal{H}_L)$ becslése a feladat. Knieper valószínűségszámítási módszerekkel bizonyítja, hogy

$$\mathrm{disc}\,(\mathcal{H}_L) \leq c\sqrt{N \log N},$$

és részletes bizonyítás nélkül közli a

$$\operatorname{disc}(\mathcal{H}_L) \geq c_1 \sqrt[4]{N}$$

eredményt. Vegyük észre, hogy az általunk bizonyított 2.2.1. tételből lényegesen erősebb felső becslés jön ki disc($\mathcal{H}_L$)-re. Mivel $\mathcal{H}_L$ elemei 2-dimenziós $[1, N]^2$-beli számtani sorozatok, ezért nyilván

$$\operatorname{disc}(\mathcal{H}_L) \leq \operatorname{disc}(\mathcal{H}),$$

ahol $\mathcal{H}$ az összes 2-dimenziós $[1, N]^2$-beli számtani sorozat halmaza. A 2.2.1. tétel $d = 2$-re a

$$\operatorname{disc}(\mathcal{H}) \leq c\sqrt[3]{N}\,(\log N)^{\frac{5}{2}}$$

felső becslést adja, és ez így felső becslés disc($\mathcal{H}_L$)-ra is. Valószínűleg az igazság $\sqrt[3]{N}$ "körül" van, de ezt nem sikerült bebizonyítani.

3. Fejezet

Kéttagú összegek eloszlásának irregularitása

Ebben a részben Roth tételének egy másik lehetséges általánosítását tárgyaljuk. Legyen ismét $\mathcal{A} \subseteq [1, N]$, és $\eta = \frac{|\mathcal{A}|}{N}$. $\mathcal{A}$ eloszlása helyett most vizsgáljuk az $\mathcal{A}$-ból elkészíthető kéttagú összegek eloszlását (multiplicitással). Az, hogy a kéttagú összegek eloszlásában fellelhetők irregularitások, nem meglepő, ha figyelembe vesszük Erdős, Sárközy és T. Sós egy tételét ([4]). Ez "lényegében" azt mondja ki, hogy ha egy végtelen, egészekből álló halmaz komplementerére teljesülnek bizonyos gyenge feltételek, akkor a belőle készített kéttagú összegek között "több" a páros, mint a páratlan. Mi kvantitatív jellegű állításokat fogunk bizonyítani az irregularitásokról. Legyen

$$f(n) = \sum_{\substack{a_1 + a_2 = n \\ a_1, a_2 \in \mathcal{A}}} 1,$$

$f(n)$ azt mutatja meg, hogy n hányféleképpen áll elő kéttagú összegként $\mathcal{A}$-beli tagokkal. Azt vizsgáljuk, hogy mennyire lehet ez a függvény közel az "ideálishoz" a számtani sorozatokban. Persze ehhez meg kell mondanunk, hogy mi az az ideális függvény, amihez viszonyítunk. Jelöljük $g(n)$-nel azt, hogy n hányféleképpen áll elő kéttagú összegként $[1, N]$-beli tagokkal, azaz

$$g(n) = \sum_{\substack{1 \le k \le N \\ 1 \le n-k \le N}} 1.$$

Ha véletlenszerűen konstruálnánk $\mathcal{A}$-t, hogy minden $n \in [1, N]$ számot egymástól függetlenül η valószínűséggel választanánk be $\mathcal{A}$-ba, akkor $f(n)$ várható értéke körülbelül $\eta^2 g(n)$ lenne (pontosabban a várható érték $\eta^2 g(n) - (\eta^2 - \eta)$ ha n páros, egyébként $\eta^2 g(n)$). Így ésszerű, hogy az $f(n)$ függvényt az $\eta^2 g(n)$-hez viszonyítjuk, ez utóbbit tekintjük "ideális"-nak. (Egy másik lehetséges magyarázat: az eredeti problémában $\mathcal{A}$ eloszlását egy η sűrűségű $[1, N]$-en egyenletes eloszláshoz viszonyítottuk. Az $f(n)$ függvényt megkaphatjuk az $\mathcal{A}$ generátorfüggvénye négyzetének megfelelő együtthatóiból, és ha ugyanezt elvégezzük az előbbi egyenletes eloszlásra, akkor az együtthatók éppen rendre $\eta^2 g(n)$-et adnak.) Vegyük észre, hogy a két szélsőséges esetben, amikor $\eta = 0$ vagy 1, akkor $f(n) = \eta^2 g(n)$ minden n-re, azaz csakúgy, mint az eredeti problémánál ezekben az esetekben az eloszlás megegyezik az ideális eloszlással.

Egy adott $n, n+q, \dots, n+(k-1)q$ számtani sorozatban az ideálistól való eltérést méri az alábbi függvény:

$$A(n, q, k) = \left| \sum_{i=0}^{k-1} \left(f(n+iq) - \eta^2 g(n+iq) \right) \right|,$$

mi azt fogjuk vizsgálni, hogy mennyire lehet kicsi ezen eltérések maximuma. Az 1.1.1. tétellel analóg módon alsó becslést adunk az eltérések maximumára, azaz belátjuk, hogy a kéttagú összegek eloszlása nem lehet túl közel az ideálishoz a számtani sorozatokban (kivéve a két triviális esetet). A felső becsléshez olyan nem triviális $\mathcal{A}$-t konstruálunk, amire a számtani sorozatok egy nagy részén alacsony a fenti eltérés. Végül megvizsgáljuk a probléma moduláris változatát is.

3.1. Alsó becslés

3.1.1. Tétel. *Legyen $\varepsilon > 0$ és $N > N_\varepsilon$, akkor tetszőleges $\mathcal{A} \subseteq [1, N]$-re léteznek olyan n és q egészek, hogy $1 \le q \le \left\lfloor \sqrt{N} \right\rfloor$, és*

$$A(n, q, \left\lfloor \frac{\left\lfloor \sqrt{N} \right\rfloor}{2} \right\rfloor) \ge \left(\frac{1}{6\sqrt{3}\pi} - \varepsilon \right) \eta(1-\eta) N^{\frac{3}{4}}.$$

A korábban bevezetett jelöléseket fogjuk használni, legyen $Q = \left\lfloor \sqrt{N} \right\rfloor$ és $Q_1 = \left\lfloor \frac{\lfloor \sqrt{N} \rfloor}{2} \right\rfloor$. A bizonyítás alapja az 1.1.2. tétel lesz, de először szükségünk lesz az alábbi lemmára.

3.1.2. Lemma. *Ha $N \ge 8$, akkor*

$$\sum_{i=1}^{2N} \left(f(i) - \eta^2 g(i) \right)^2 \ge \frac{1}{48} \left(\eta \left(1 - \eta \right) N \right)^2.$$

Bizonyítás. Ha $\eta = 0$ vagy 1 (azaz $\eta\,(1-\eta) = 0$), akkor $\sum_{i=1}^{2N} \left(f(i) - \eta^2 g(i) \right)^2 = 0$. Ha $|\mathcal{A}| = 1$ (azaz $\eta = \frac{1}{N}$), és $\mathcal{A} = \{a\}$, akkor

$$\sum_{i=1}^{2N} \left(f(i) - \eta^2 g(i) \right)^2 \ge \left(f(2a) - \eta^2 g(2a) \right)^2 \ge \left(1 - \frac{1}{N^2} N \right)^2 = \left(\eta \left(1 - \eta \right) N \right)^2.$$

Ha $|\mathcal{A}| = N - 1$ ($\eta = 1 - \frac{1}{N}$), és $\mathcal{A} = [1, N] \setminus \{a\}$, akkor

$$f(a) = g(a) = a - 1,$$

és

$$f(N + a + 1) = g(N + a + 1) = \max\left(N - a - 1, 0 \right).$$

Könnyen látható, hogy $\max\left(g(a), g(N+a+1)\right) \geq \frac{N}{3}$, így ebben az esetben

$$\sum_{i=1}^{2N} \left(f(i) - \eta^2 g(i)\right)^2 \geq \left(\frac{N}{3} - \eta^2 \frac{N}{3}\right)^2 = \frac{1}{9}\left(\left(1-\eta^2\right)N\right)^2 \geq \frac{1}{9}\left(\eta\left(1-\eta\right)N\right)^2.$$

Tehát a továbbiakban feltehetjük, hogy $2 \leq |\mathcal{A}| \leq N-2$.

Legyen $F(\alpha) = \sum\limits_{i=1}^{2N} f(i)e(i\alpha)$, és $G(\alpha) = \sum\limits_{i=1}^{2N} \eta^2 g(i)e(i\alpha)$. A definíciókból látszik, hogy

$$F(\alpha) = \left(\sum_{a\in\mathcal{A}} e(a\alpha)\right)^2,$$

és

$$G(\alpha) = \eta^2 \left(\sum_{i=1}^{N} e(i\alpha)\right)^2 = \eta^2 \left(\frac{e((N+1)\alpha) - e(\alpha)}{e(\alpha)-1}\right)^2.$$

A Parseval formulából következik, hogy

$$\sum_{i=1}^{2N} \left(f(i) - \eta^2 g(i)\right)^2 = \int_0^1 |F(\alpha) - G(\alpha)|^2 \, d\alpha. \tag{1}$$

A Cauchy-Schwarz egyenlőtlenségből:

$$\sqrt{\int_0^1 |F(\alpha) - G(\alpha)|^2 \, d\alpha} \geq \int_0^1 |F(\alpha) - G(\alpha)| \, d\alpha. \tag{2}$$

Mivel $2 \geq \left|e(\left\lfloor \frac{N}{2} \right\rfloor \alpha) - 1\right|$, ezért

$$4\int_0^1 |F(\alpha) - G(\alpha)| \, d\alpha \geq \int_0^1 |F(\alpha) - G(\alpha)| \left|e(\left\lfloor \frac{N}{2} \right\rfloor \alpha) - 1\right|^2 d\alpha. \tag{3}$$

Triviálisan becsülve a jobb oldalon integrált függvényt:

$$|F(\alpha) - G(\alpha)| \left|e(\left\lfloor \frac{N}{2} \right\rfloor \alpha) - 1\right|^2 \geq \left|F(\alpha)(e(\left\lfloor \frac{N}{2} \right\rfloor \alpha) - 1)^2\right| - \left|G(\alpha)(e(\left\lfloor \frac{N}{2} \right\rfloor \alpha) - 1)^2\right|.$$

Egyszerű átalakításokkal, és a Parseval formula felhasználásával:

$$\begin{aligned}
\int_0^1 \left| G(\alpha)(e(\left\lfloor \frac{N}{2} \right\rfloor \alpha) - 1)^2 \right| d\alpha &= \int_0^1 \eta^2 \left| \left(\frac{e((N+1)\alpha) - e(\alpha)}{e(\alpha) - 1} \right)^2 \left(e(\left\lfloor \frac{N}{2} \right\rfloor \alpha) - 1 \right)^2 \right| d\alpha \\
&= \eta^2 \int_0^1 \left| \frac{e(\left\lfloor \frac{N}{2} \right\rfloor \alpha) - 1}{e(\alpha) - 1} (e((N+1)\alpha) - e(\alpha)) \right|^2 d\alpha \\
&= \eta^2 \int_0^1 \left| \sum_{i=0}^{\left\lfloor \frac{N}{2} \right\rfloor - 1} e(i\alpha) \right|^2 |e((N+1)\alpha) - e(\alpha)|^2 \, d\alpha \\
&= \eta^2 \int_0^1 \left| - \sum_{i=1}^{\left\lfloor \frac{N}{2} \right\rfloor} e(i\alpha) + \sum_{i=N+1}^{N + \left\lfloor \frac{N}{2} \right\rfloor} e(i\alpha) \right|^2 d\alpha \\
&= 2\eta^2 \left\lfloor \frac{N}{2} \right\rfloor \le \eta^2 N.
\end{aligned}$$

Ezért

$$\int_0^1 |F(\alpha) - G(\alpha)| \left| e(\left\lfloor \frac{N}{2} \right\rfloor \alpha) - 1 \right|^2 d\alpha \ge \int_0^1 \left| F(\alpha) \left(e(\left\lfloor \frac{N}{2} \right\rfloor \alpha) - 1 \right)^2 \right| d\alpha - \eta^2 N.$$

Másrészt,

$$F(\alpha) \left(e(\left\lfloor \frac{N}{2} \right\rfloor \alpha) - 1 \right)^2 = \left(\left(\sum_{a \in \mathcal{A}} e(a\alpha) \right) \left(e(\left\lfloor \frac{N}{2} \right\rfloor \alpha) - 1 \right) \right)^2 = \left(\sum_{i=1}^{i = N + \left\lfloor \frac{N}{2} \right\rfloor} a_i e(i\alpha) \right)^2,$$

ahol

$$a_i = \begin{cases} -1 & \text{ha} \quad i \in \mathcal{A} \text{ és } i - \left\lfloor \frac{N}{2} \right\rfloor \notin \mathcal{A}, \\ 1 & \text{ha} \quad i \notin \mathcal{A} \text{ és } i - \left\lfloor \frac{N}{2} \right\rfloor \in \mathcal{A}, \\ 0 & \quad \text{egyébként.} \end{cases}$$

Mivel

$$\int_0^1 \left| F(\alpha) \left(e(\left\lfloor \frac{N}{2} \right\rfloor \alpha) - 1 \right)^2 \right| d\alpha = \sum_{i=1}^{N + \left\lfloor \frac{N}{2} \right\rfloor} |a_i|^2 = \sum_{i=1}^{N + \left\lfloor \frac{N}{2} \right\rfloor} |a_i|,$$

ezért az integrál értéke megegyezik azon i egészek számával, amelyekre $a_i \neq 0$. Ha $1 \leq i \leq \left\lfloor \frac{N}{2} \right\rfloor$, és $i \in \mathcal{A}$, akkor $a_i = -1$, mert $i - \left\lfloor \frac{N}{2} \right\rfloor \leq 0$, és így $i - \left\lfloor \frac{N}{2} \right\rfloor \notin \mathcal{A}$. Hasonlóan, ha $N - \left\lfloor \frac{N}{2} \right\rfloor < i \leq N$, és $i \in \mathcal{A}$, akkor $a_{i+\left\lfloor \frac{N}{2} \right\rfloor} = 1$. Ha $i \in \mathcal{A}$,akkor $1 \leq i \leq \left\lfloor \frac{N}{2} \right\rfloor$ vagy $N - \left\lfloor \frac{N}{2} \right\rfloor < i \leq N$, és ha N páratlan, akkor $i = \left\lfloor \frac{N}{2} \right\rfloor + 1$ is lehetséges. Az előzőekből következik, hogy az integrál értéke legalább $|\mathcal{A}| - 1 = \eta N - 1$, és ezért

$$\int_0^1 |F(\alpha) - G(\alpha)| \left| e(\left\lfloor \frac{N}{2} \right\rfloor \alpha) - 1 \right|^2 d\alpha \geq \eta N - \eta^2 N - 1 = \eta\,(1-\eta)\,N - 1.$$

$2 \leq |\mathcal{A}| \leq N - 2$, és $N \geq 8$, ezért

$$\eta\,(1-\eta)\,N \geq \frac{2\,(N-2)}{N} \geq \frac{3}{2},$$

és

$$\eta\,(1-\eta)\,N - 1 \geq \frac{1}{3}\eta\,(1-\eta)\,N.$$

Akkor pedig az (1), (2) és (3) felhasználásával következik a lemma állítása. □

A 3.1.1. tétel bizonyítása. Az 1.1.3. következményt fogjuk használjuk az $M = 2N$, $s_j = f(j) - \eta^2 g(j)$, ha $1 \leq j \leq M$, és $R = Q = \left\lfloor \sqrt{N} \right\rfloor$ értékekkel. A következmény szerint létezik n, $1 \leq q \leq Q$, hogy

$$|A(n, q, Q_1)| \geq \frac{2}{\pi} Q_1 \sqrt{\sum_{m=1}^{2N} |s_m|^2} \left(2N + \frac{Q^2}{4} \right)^{-\frac{1}{2}} Q^{-\frac{1}{2}}.$$

A 3.1.2. lemmából

$$\sqrt{\sum_{m=1}^{2N} |s_m|^2} \geq \frac{1}{4\sqrt{3}} \eta\,(1-\eta)\,N, \text{ ha } N \geq 8.$$

Ezért ha N elég nagy ($N > N_\varepsilon$), akkor

$$\frac{2}{\pi} Q_1 \sqrt{\sum_{m=1}^{2N} |s_m|^2} \left(2N + \frac{Q^2}{4} \right)^{-\frac{1}{2}} Q^{-\frac{1}{2}} \geq \left(\frac{1}{6\sqrt{3}\pi} - \varepsilon \right) \eta(1-\eta) N^{\frac{3}{4}},$$

és ebből már következik a bizonyítandó állítás. (A bizonyításból az is látszik, hogy az alsó becslés nem csak a maximumra, hanem az eltérések egy jelentős részének négyzetes középére is teljesül.) $\square$

3.2. Felső becslés

A 3.1.1. tétel alsó becslést adott a $\max_{n,1\leq q\leq Q} A(n,q,Q_1)$ kifejezésre, most megpróbálunk olyan $\mathcal{A}$-t konstruálni, amire ez a maximum minél kisebb. A 3.2.1. tételben minden elég nagy N-re mutatunk olyan $\mathcal{A} \subseteq [1,N]$ halmazt (amire $\eta \approx \frac{1}{2}$), hogy $A(n,q,Q_1) \leq cN$ minden n, $1 \leq q \leq Q$ egészre, és a "legtöbb" ilyen n és q párra $A(n,q,Q_1) \leq c_1 N^{\frac{5}{6}} \log N$ (a konstansok mindenhol rögzítettek). A bizonyításban Sárközy azon módszerét adaptáljuk, amellyel felső becslést adott az eredeti Roth problémára ([3]).

3.2.1. Tétel. *Legyen N pozitív egész, p prímszám, melyre $N^{\frac{2}{3}} < p \leq 2N^{\frac{2}{3}}$. Legyen $\mathcal{A}$ az $[1,N]$-beli mod p kvadratikus maradékok halmaza, azaz*

$$\mathcal{A} = \left\{ a : \left(\frac{a}{p}\right) = 1, 1 \leq a \leq N \right\}.$$

(Ahol $\left(\frac{y}{p}\right)$ az ismert Legendre-szimbólum, $\left(\frac{y}{p}\right) = 0$ ha $y \equiv 0 \mod p$.) Erre a halmazra

$$\left| \eta - \frac{1}{2} \right| \leq c_1 N^{-\frac{2}{3}} \log N,$$

és

$$A(n,q,Q_1) \leq c_2 N$$

minden n, $1 \leq q \leq Q$ egészre. Továbbá ha $N > N_\varepsilon$, és tekintjük azon (n,q) párokat, amelyekre $1 \leq q \leq Q$, és $1-(Q-1)q \leq n \leq N$, akkor a párok legalább $(1-\varepsilon)$-

részére teljesül, hogy

$$A(n, q, Q_1) \le c_3 N^{\frac{5}{6}} \log N.$$

(A konstansok mind rögzítettek.)

Mauduit és Sárközy következő tételét ([8]) gyakran fogjuk használni. (Ez A. Weil híres tételének egy következménye ([17]).)

3.2.2. Tétel (Mauduit-Sárközy). *Ha p prím, $h(x) \in F_p[x]$ egy legfeljebb k-adfokú polinom, amely nem írható fel $b(h_1(x))^2$ alakban (ahol $b \in F_p$, és $h_1(x) \in F_p[x]$), továbbá X, Y egészek, melyekre $0 < Y \le p$, akkor*

$$\left| \sum_{X < n \le X+Y} \left(\frac{h(n)}{p} \right) \right| < 9k\sqrt{p} \log p.$$

A 3.2.1. tétel bizonyítása előtt szükségünk lesz néhány lemmára.

3.2.3. Lemma. *A 3.2.1. tételben definiált $\mathcal{A} \subseteq [1, N]$ halmazra:*

$$\left| \eta - \frac{1}{2} \right| \le c_1 N^{-\frac{2}{3}} \log N.$$

Bizonyítás. A Csebisev tétel biztosítja, hogy létezik megfelelő p prím a konstrukcióhoz. Tekintsük a következő halmazokat $j = -1, 0, 1$-re:

$$B_j = \left\{ i \,\middle|\, \left(\frac{i}{p} \right) = j,\ 1 \le i \le N \right\}.$$

Látszik, hogy $|B_0| = \left\lfloor \frac{N}{p} \right\rfloor$, $B_1 = \mathcal{A}$ és

$$\sum_{i=1}^{N} \left(\frac{i}{p} \right) = |B_1| - |B_{-1}| = 2\eta N - N + \left\lfloor \frac{N}{p} \right\rfloor.$$

Tetszőleges a egészre $\sum_{i=a}^{a+p-1} \left(\frac{i}{p}\right) = 0$, és felhasználva a 3.2.2. tételt $h(x) = x$ választással (vagy az ismert Pólya-Vinogradov egyenlőtlenséget):

$$\left|\sum_{i=1}^{N} \left(\frac{i}{p}\right)\right| = \left|\sum_{i=\left\lfloor \frac{N}{p} \right\rfloor p}^{N} \left(\frac{i}{p}\right)\right| \leq 9\sqrt{p}\log p.$$

Tehát $|2\eta N - N| \leq 9\sqrt{p}\log p + \left\lfloor \frac{N}{p} \right\rfloor$, és ezért

$$\left|\eta - \frac{1}{2}\right| \leq \frac{1}{2N}\left(9\sqrt{p}\log p + \left\lfloor \frac{N}{p} \right\rfloor\right).$$

Mivel $N^{\frac{2}{3}} < p \leq 2N^{\frac{2}{3}}$, ezért ebből már következik a lemma állítása. □

3.2.4. Lemma. *Ha $2 \leq n \leq 2N$, akkor*

$$\left|f(n) - \sum_{k=x_0}^{x_1} \left(\frac{\left(\frac{k}{p}\right) + 1}{2}\right)\left(\frac{\left(\frac{n-k}{p}\right) + 1}{2}\right)\right| \leq cN^{\frac{1}{3}},$$

ahol $x_0 = 1$, és $x_1 = n - 1$, ha $2 \leq n \leq N$, illetve $x_0 = n - N$, és $x_1 = N$, ha $N + 1 \leq n \leq 2N$.

Bizonyítás. Legyen először n rögzített egész, melyre $2 \leq n \leq N$. Akkor

$$f(n) = \sum_{\substack{a_1+a_2=n \\ a_1,a_2\in\mathcal{A}}} 1 = \sum_{k=1}^{n-1} \alpha_k,$$

ahol $\alpha_k = 1$ ha $k, n-k \in \mathcal{A}$, és $\alpha_k = 0$ egyébként. Legyen

$$C_1 = \{k \,|k \text{ or } n-k \equiv 0 \mod p,\, 1 \leq k \leq n-1\},$$

és

$$C = \{1, 2, \ldots, n-1\} \setminus C_1.$$

Akkor $f(n) = \sum_{k\in C} \alpha_k + \sum_{k\in C_1} \alpha_k$. Ha $k \in C$, akkor $\left(\frac{k}{p}\right) = \pm 1$, és $\alpha_k = 1$ pontosan akkor, ha $\left(\frac{k}{p}\right) = \left(\frac{n-k}{p}\right) = 1$. Ennek segítségével ellenőrizhető, hogy $k \in C$ esetén

$$\alpha_k = \left(\frac{\left(\frac{k}{p}\right)+1}{2}\right)\left(\frac{\left(\frac{n-k}{p}\right)+1}{2}\right).$$

Ha $k \in C_1$, azaz k vagy $n-k$ többszöröse p-nek, akkor $\alpha_k = 0$, és látszik, hogy

$$\left(\frac{\left(\frac{k}{p}\right)+1}{2}\right)\left(\frac{\left(\frac{n-k}{p}\right)+1}{2}\right) = \frac{\left(\frac{n}{p}\right)+1}{4}.$$

Ezért

$$\begin{aligned}\left|f(n) - \sum_{k=1}^{n-1}\left(\frac{\left(\frac{k}{p}\right)+1}{2}\right)\left(\frac{\left(\frac{n-k}{p}\right)+1}{2}\right)\right| &= \left|\sum_{k\in C_1}\left(\alpha_k - \left(\frac{\left(\frac{k}{p}\right)+1}{2}\right)\left(\frac{\left(\frac{n-k}{p}\right)+1}{2}\right)\right)\right| \\ &= |C_1|\left|\frac{\left(\frac{n}{p}\right)+1}{4}\right| \le 2\left\lfloor\frac{n-1}{p}\right\rfloor\left|\frac{\left(\frac{n}{p}\right)+1}{4}\right|.\end{aligned}$$

Emiatt

$$\left|f(n) - \sum_{k=1}^{n-1}\left(\frac{\left(\frac{k}{p}\right)+1}{2}\right)\left(\frac{\left(\frac{n-k}{p}\right)+1}{2}\right)\right| \le \left\lfloor\frac{n-1}{p}\right\rfloor \le \frac{N}{p},$$

és mert $N^{\frac{2}{3}} < p \le 2N^{\frac{2}{3}}$, ezért következik a bizonyítandó állítás.

Ha $N+1 \le n \le 2N$, akkor

$$f(n) = \sum_{\substack{a_1+a_2=n \\ a_1,a_2\in\mathcal{A}}} 1 = \sum_{k=N-n}^{N} \alpha_k,$$

ahol $\alpha_k = 1$, ha $k, n-k \in \mathcal{A}$, és $\alpha_k = 0$ egyébként. A bizonyítás az előző esethez hasonlóan befejezhető. $\square$

3.2.5. Lemma. *Ha $2 \le n \le 2N$, és $p \nmid n$, akkor*

$$\left|\frac{1}{4}g(n) - \sum_{k=x_0}^{x_1}\left(\frac{\left(\frac{k}{p}\right)+1}{2}\right)\left(\frac{\left(\frac{n-k}{p}\right)+1}{2}\right)\right| \le cN^{\frac{1}{3}}\log N,$$

ahol $x_0 = 1$, *és* $x_1 = n-1$, *ha* $2 \le n \le N$, *illetve* $x_0 = n - N$, *és* $x_1 = N$, *ha* $N+1 \le n \le 2N$. *(A konstans rögzített.) Ha* $p \mid n$, *akkor*

$$\left| \frac{1}{4} g(n) - \sum_{k=x_0}^{x_1} \left(\frac{\left(\frac{k}{p}\right)+1}{2} \right) \left(\frac{\left(\frac{n-k}{p}\right)+1}{2} \right) \right| \le N.$$

Bizonyítás. Legyen először n rögzített egész, melyre $2 \le n \le N$, és $p \nmid n$. Akkor

$$g(n) = \sum_{\substack{1 \le k \le N \\ 1 \le n-k \le N}} 1 = n-1,$$

és

$$\frac{1}{4} g(n) - \sum_{k=x_0}^{x_1} \left(\frac{\left(\frac{k}{p}\right)+1}{2} \right) \left(\frac{\left(\frac{n-k}{p}\right)+1}{2} \right) = \frac{1}{4}(n-1) - \frac{1}{4} \sum_{k=1}^{n-1} \left(\frac{k(n-k)}{p} \right) -$$

$$- \frac{1}{2} \sum_{k=1}^{n-1} \left(\frac{k}{p} \right) - \frac{1}{4}(n-1) = -\frac{1}{4} \sum_{k=1}^{n-1} \left(\frac{k(n-k)}{p} \right) - \frac{1}{2} \sum_{k=1}^{n-1} \left(\frac{k}{p} \right).$$

Ismert, hogy ha $(a,p)=1$, akkor $\sum_{k=1}^{p} \left(\frac{k(a-k)}{p}\right) = -\left(\frac{-1}{p}\right)$ (pl. [16, 5. fejezet]). Továbbá ha $p \nmid n$, akkor $x(n-x)$ nem írható fel $b\left(h_1(x)\right)^2$ alakban $F_p[x]$, és így alkalmazható a 3.2.2. tétel. Ezekből:

$$\left| \sum_{k=1}^{n-1} \left(\frac{k(n-k)}{p} \right) \right| \le \left\lfloor \frac{n-1}{p} \right\rfloor + 18\sqrt{p}\log p \le \frac{N}{p} + 18\sqrt{p}\log p.$$

A 3.2.2. tételből, és $\sum_{k=a}^{a+p-1} \left(\frac{k}{p}\right) = 0$-ból, a már látott módon

$$\left| \sum_{k=1}^{n-1} \left(\frac{k}{p} \right) \right| \le 9\sqrt{p}\log p.$$

A kapott egyenlőtlenségekből (figyelembe véve az $N^{\frac{2}{3}} < p \le 2N^{\frac{2}{3}}$ egyenlőtlenséget) esetünkben következik a bizonyítandó állítás .

Ha n egész, melyre $N+1 \le n \le 2N$, és $p \nmid n$, akkor

$$g(n) = \sum_{\substack{1 \le k \le N \\ 1 \le n-k \le N}} 1 = 2N - n + 1.$$

A bizonyítás az előző esetben látott módon befejezhető.

Ha $1 \leq n \leq 2N$, és $p \mid n$, akkor

$$\sum_{k=1}^{n-1} \left(\frac{k(n-k)}{p}\right) = \sum_{k=1}^{n-1} \left(\frac{-k^2}{p}\right) = (n-1)\left(\frac{-1}{p}\right),$$

így az előbbi bizonyítás nem vihető véghez. De mert

$$0 \leq \sum_{k=x_0}^{x_1} \left(\frac{\left(\frac{k}{p}\right)+1}{2}\right)\left(\frac{\left(\frac{n-k}{p}\right)+1}{2}\right) \leq N$$

(ahol x_0 és x_1 a korábban látott módon definiáltak), és $g(n) \leq N$, ezért

$$\left|\frac{1}{4}g(n) - \sum_{k=x_0}^{x_1} \left(\frac{\left(\frac{k}{p}\right)+1}{2}\right)\left(\frac{\left(\frac{n-k}{p}\right)+1}{2}\right)\right| \leq N,$$

és ez kellett a 3.2.5. lemma bizonyításnak befejezéséhez. □

A 3.2.1. tétel bizonyítása. Felhasználva a 3.2.3. lemmát, és $g(n) \leq N$-et:

$$\left|\frac{1}{4}g(n) - \eta^2 g(n)\right| = g(n)\left|\frac{1}{2}+\eta\right|\left|\frac{1}{2}-\eta\right| \leq N\frac{3}{2}c_1 N^{-\frac{2}{3}} \log N \leq c_1' N^{\frac{1}{3}} \log N.$$

A 3.2.4. és 3.2.5. lemmákból következik, hogy ha $2 \leq n \leq 2N$, és $p \nmid n$, akkor

$$\left|f(n) - \eta^2 g(n)\right| \leq cN^{\frac{1}{3}} \log N$$

(a konstans rögzített), és ha $p \mid n$, akkor

$$\left|f(n) - \eta^2 g(n)\right| \leq N.$$

Világos, hogy ha $n < 2$ vagy $2N < n$, akkor $f(n) = g(n) = 0$.

Legyen most n és $1 \leq q \leq Q$ rögzített. Mivel $Q_1 \leq \frac{\sqrt{N}}{2}$, és $N^{\frac{2}{3}} < p$ prím, ezért az $n, n+q, \ldots, n+(Q_1-1)q$ egészek közül legfeljebb egy osztható p-vel. Ezért

$$A(n,q,Q_1) = \left|\sum_{k=0}^{Q_1-1} \left(f(n+kq) - \eta^2 g(n+kq)\right)\right| \leq cN^{\frac{1}{3}} Q \log N + N \leq cN^{\frac{5}{6}} \log N + N.$$

Ez mutatja, hogy

$$A(n, q, Q_1) \leq c_2 N$$

egy fix c_2 konstanssal. De az is következik, hogy ha az $n, n+q, \dots, n+(Q_1-1)q$ egészek egyike sem osztható p-vel, akkor

$$A(n, q, Q_1) \leq cN^{\frac{5}{6}} \log N.$$

Ha tekintjük az összes olyan $n, n+q, \dots, n+(Q_1-1)q$ számtani sorozatot, amely belemetsz $[1, N]$-be, és $1 \leq q \leq Q$ (ezek pontosan azok, amelyekre teljesül az $1-(Q-1)\,q \leq n \leq N$ egyenlőtlenség), akkor könnyen meggondolható, hogy legalább az $\left(1-\frac{2Q}{p}\right)$-részük nem tartalmaz p-vel osztható elemet. Mivel $\frac{2Q}{p} \leq 4N^{-\frac{1}{3}} \leq \varepsilon$, ha $N \geq N_\varepsilon$, ezért ebből következik a 3.1.1. tétel utolsó állítása is. $\square$

Korábban megjegyeztük, hogy a 3.1.1. tétel bizonyításából kijön, hogy a maximális eltérésre bizonyított alsó becslés igaz lesz az eltérések egy bizonyos részének négyzetes közepére is. (Éppen az előbbi bizonyítás végén tekintett számtani sorozatokban vett eltérések négyzetes közepéről van szó.) Az előbbi bizonyítás eredményeit felhasználva könnyen igazolható, hogy a definiált $\mathcal{A}$ halmaz esetén a megfelelő négyzetes közép felülről becsülhető $cN^{\frac{5}{6}} \log N$-nel.

Látható, hogy itt nem sikerült belátni, hogy a 3.1.1. tétel éles (vagy legalább log-hatványtól eltekintve éles). A sejtés az, hogy ez igaz, de a bizonyítása valószínűleg nehéz (figyelembe véve, hogy az eredeti problémánál is csak nehézségek árán lehetett ezt igazolni).

3.3. Moduláris változat

Legyen $\mathcal{A} \subseteq \{0, 1, \dots, q-1\}$, és $\eta = \frac{|\mathcal{A}|}{q}$. Legyen

$$h(i) = \sum_{\substack{a_1 + a_2 \equiv i \mod q \\ a_1, a_2 \in \mathcal{A}}} 1.$$

Látható, hogy $h(i)$ azt mutatja, hogy az $i \bmod q$ maradékosztály hányféleképpen áll elő kéttagú összegként $\mathcal{A}$-beli tagokkal. Mivel

$$\frac{1}{q} \sum_{i=0}^{q-1} h(i) = \frac{1}{q} |\mathcal{A}|^2 = \eta^2 q,$$

ezért az $\mathcal{A}$-ból készített kéttagú összegek eloszlása akkor lesz "egyenletes" $\bmod q$, ha $\max\limits_{0 \le i \le q-1} |h(i) - \eta^2 q|$ "kicsi". A következő tétel és következménye alsó becslést ad az előbbi maximumra.

3.3.1. Tétel. *Tetszőleges $\mathcal{A} \subseteq \{0, 1, \dots, q-1\}$ esetén (ha $q \ge 2$):*

$$\sum_{i=0}^{q-1} \left(h(i) - \eta^2 q\right)^2 \ge \frac{q^3}{q-1} \eta^2 (1-\eta)^2.$$

3.3.2. Következmény. *Tetszőleges $\mathcal{A} \subseteq \{0, 1, \dots, q-1\}$ halmazra, ahol $q \ge 2$, létezik olyan $0 \le i \le q-1$ egész, hogy*

$$\left|h(i) - \eta^2 q\right| \ge \sqrt{q} \eta (1-\eta).$$

A 3.3.1. tétel bizonyítása. Legyen $S(\alpha) = \sum\limits_{a \in \mathcal{A}} e(a\alpha)$. Látható, hogy ha k egész, akkor

$$\left(S(\frac{k}{q})\right)^2 = \sum_{i=0}^{q-1} h(i) e(i\frac{k}{q}).$$

Ismert (diszkrét Parseval formula), hogy ha $B(\alpha) = \sum\limits_{j=0}^{q-1} b_i e(j\alpha)$, akkor

$$\frac{1}{q} \sum_{k=0}^{q-1} \left| B\left(\frac{k}{q}\right) \right|^2 = \sum_{j=0}^{q-1} |b_j|^2.$$

Legyen $b_j = h(j) - \eta^2 q$ $(0 \le j \le q-1)$, akkor

$$\sum_{i=0}^{q-1} \left(h(i) - \eta^2 q\right)^2 = \frac{1}{q} \sum_{k=0}^{q-1} \left| B\left(\frac{k}{q}\right) \right|^2 .$$

$B(0) = \sum\limits_{i=0}^{q-1} h(i) - \eta^2 q^2 = 0$, és ha $1 \le k \le q-1$, akkor

$$\begin{aligned} B\left(\frac{k}{q}\right) &= \sum_{j=0}^{q-1} \left(h(j) - \eta^2 q\right) e\left(j\frac{k}{q}\right) = \sum_{j=0}^{q-1} h(j)\, e\left(j\frac{k}{q}\right) - \eta^2 q \sum_{j=0}^{q-1} e\left(j\frac{k}{q}\right) \\ &= \sum_{j=0}^{q-1} h(j)\, e\left(j\frac{k}{q}\right) = \left(S(\frac{k}{q})\right)^2 . \end{aligned}$$

Ezért

$$\sum_{i=0}^{q-1} \left(h(i) - \eta^2 q\right)^2 = \frac{1}{q} \sum_{k=1}^{q-1} \left| S\left(\frac{k}{q}\right) \right|^4 .$$

$S(0) = |\mathcal{A}| = \eta q$, ezért

$$\frac{1}{q} \sum_{k=1}^{q-1} \left| S\left(\frac{k}{q}\right) \right|^2 = \frac{1}{q} \sum_{k=0}^{q-1} \left| S\left(\frac{k}{q}\right) \right|^2 - \frac{1}{q}\eta^2 q^2 = \eta q - \eta^2 q = q\eta\,(1-\eta) .$$

A Cauchy-Schwarz egyenlőtlenséget használva:

$$\begin{aligned} \sum_{i=0}^{q-1} \left(h(i) - \eta^2 q\right)^2 &= \frac{1}{q} \sum_{k=1}^{q-1} \left| S\left(\frac{k}{q}\right) \right|^4 \ge \frac{1}{q\,(q-1)} \left(\sum_{k=1}^{q-1} \left| S\left(\frac{k}{q}\right) \right|^2 \right)^2 = \\ &= \frac{1}{q\,(q-1)} q^4 \eta^2 (1-\eta)^2 = \frac{q^3}{q-1} \eta^2 (1-\eta)^2 . \end{aligned}$$

Ezzel beláttuk a bizonyítandó állítást. □

A 3.3.1. tétel általánosításaként vizsgálhatjuk a $\sum\limits_{i=1}^{k} a_i$ alakú összegek eloszlását mod q, ahol $a_1, a_2, \ldots, a_k \in \mathcal{A}$, és $k \ge 2$ rögzített egész. Legyen

$$h_k(n) = \sum_{\substack{a_1 + a_2 + \ldots + a_k \equiv n \mod q \\ a_1, a_2, \ldots, a_k \in \mathcal{A}}} 1.$$

Világos, hogy $\frac{1}{q}\sum_{i=0}^{q-1} h_k(i) = \eta^k q^{k-1}$, és a 3.3.1. tétel bizonyításához hasonló módon belátható, hogy

$$\sum_{i=0}^{q-1}\left(h_k(i)-\eta^k q^{k-1}\right)^2 \geq \frac{q^{2k-1}}{(q-1)^{k-1}}\eta^k(1-\eta)^k.$$

A következő tételek azt mutatják, hogy mennyire éles a 3.3.1. tétel és a következménye. A 3.3.3. tétel azt mutatja, hogy a 3.3.1. tétel végtelen sok egészre lényegében éles, és a következő tétel szerint a 3.3.2. következmény log-hatványtól eltekintve mindig véges. (Ebből az is következik, hogy a 3.3.1. tétel is log-hatványtól eltekintve mindig véges.)

3.3.3. Tétel. *Legyen $p>2$ prímszám, és $\mathcal{A}=\left\{a : \left(\frac{a}{p}\right)=1, 0\leq a\leq p-1\right\}$. Erre a részhalmazra*

$$\sum_{i=0}^{p-1}\left(h(i)-\eta^2 p\right)^2 \leq \frac{p^3}{p-1}\eta^2(1-\eta)^2+p.$$

Bizonyítás. $|\mathcal{A}|=\frac{p-1}{2}$, $\eta=\frac{1}{2}-\frac{1}{2p}$, és

$$\eta^2 p=\frac{(p-1)^2}{4p}=\frac{p-2}{4}+\frac{1}{4p}.$$

Mivel $\left(\frac{a}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{p-a}{p}\right)$, ezért $h(0)=0$, ha $\left(\frac{-1}{p}\right)=-1$, és $h(0)=\frac{p-1}{2}$, ha $\left(\frac{-1}{p}\right)=1$. Emiatt

$$\left(h(0)-\eta^2 p\right)^2 \leq \left(\frac{p-1}{2}-\frac{(p-1)^2}{4p}\right)^2=\frac{p^2}{16}-\frac{1}{8}+\frac{1}{16p^2}.$$

Legyen most $1\leq a\leq p-1$. Belátjuk, hogy

$$h(a)=\sum_{i=0}^{p-1}\frac{\left(\left(\frac{i}{p}\right)+1\right)\left(\left(\frac{a-i}{p}\right)+1\right)}{4}-\frac{\left(\frac{a}{p}\right)+1}{2}=\sum_{\substack{0\leq i\leq p-1\\ i\neq 0,a}}\frac{\left(\left(\frac{i}{p}\right)+1\right)\left(\left(\frac{a-i}{p}\right)+1\right)}{4}.$$

Legyen $f(n) = \sum\limits_{\substack{a_1+a_2=n \\ a_1,a_2\in\mathcal{A}}} 1$, akkor $h(a) = f(a) + f(a+p)$. i és $a-i$ pontosan akkor lesznek egyszerre $\mathcal{A}$ elemei, ha

$$\frac{\left(\left(\frac{i}{p}\right)+1\right)\left(\left(\frac{a-i}{p}\right)+1\right)}{4} = 1,$$

egyébként

$$\frac{\left(\left(\frac{i}{p}\right)+1\right)\left(\left(\frac{a-i}{p}\right)+1\right)}{4} = 0,$$

ha $i \neq 0, a$. Hasonlóan i és $a+p-i$ pontosan akkor lesznek egyszerre $\mathcal{A}$-ban, ha

$$\frac{\left(\left(\frac{i}{p}\right)+1\right)\left(\left(\frac{a-i}{p}\right)+1\right)}{4} = 1,$$

és egyébként

$$\frac{\left(\left(\frac{i}{p}\right)+1\right)\left(\left(\frac{a-i}{p}\right)+1\right)}{4} = 0,$$

ha $i \neq 0, a$. Ebből következik, hogy

$$\sum_{\substack{0\le i\le p-1 \\ i\neq 0,a}} \frac{\left(\left(\frac{i}{p}\right)+1\right)\left(\left(\frac{a-i}{p}\right)+1\right)}{4} = f(a) + f(a+p) = h(a).$$

Ezért

$$\begin{aligned} h(a) &= \sum_{i=0}^{p-1} \frac{\left(\left(\frac{i}{p}\right)+1\right)\left(\left(\frac{a-i}{p}\right)+1\right)}{4} - \frac{\left(\frac{a}{p}\right)+1}{2} \\ &= \frac{1}{4}\sum_{i=0}^{p-1}\left(\frac{i(a-i)}{p}\right) + \frac{1}{2}\sum_{i=0}^{p-1}\left(\frac{i}{p}\right) + \frac{p-2}{4} - \frac{1}{2}\left(\frac{a}{p}\right). \end{aligned}$$

Mivel $\sum\limits_{i=0}^{p-1}\left(\frac{i}{p}\right) = 0$, és $\sum\limits_{i=0}^{p-1}\left(\frac{i(a-i)}{p}\right) = -\left(\frac{-1}{p}\right)$, így

$$h(a) = \frac{p-2}{4} - \frac{1}{4}\left(\frac{-1}{p}\right) - \frac{1}{2}\left(\frac{a}{p}\right),$$

ha $1 \leq a \leq p-1$. Akkor

$$\left(h(a)-\eta^2 p\right)^2 = \left(\frac{p-2}{4} - \frac{1}{4}\left(\frac{-1}{p}\right) - \frac{1}{2}\left(\frac{a}{p}\right) - \frac{p-2}{4} - \frac{1}{4p}\right)^2 \leq 1.$$

Összegezve eredményeinket:

$$\sum_{i=0}^{p-1} \left(h(i)-\eta^2 p\right)^2 \leq \frac{p^2}{16} - \frac{1}{8} + \frac{1}{16p^2} + p - 1,$$

és mert

$$\frac{p^3}{p-1}\eta^2 (1-\eta)^2 + p = \frac{1}{16}p^2 + \frac{17}{16}p - \frac{1}{16} - \frac{1}{16p},$$

ezért a bizonyítandó állítás következik. □

3.3.4. Tétel. *Legyen $q > 1$ egész, és p prím, melyre $2q < p \leq 4q$. Tekintsük a következő $\mathcal{A} \subseteq \{0, 1, 2, \ldots, q-1\}$ halmazt:*

$$\mathcal{A} = \left\{ a : \left(\frac{a}{p}\right) = 1, 1 \leq a \leq q \right\}.$$

(q nem oszthatja p-t, így ez valóban a mod *q maradékosztályok egy részhalmaza lesz.) Erre a részhalmazra*

$$\left|\eta - \frac{1}{2}\right| \leq 9\frac{\log(4q)}{\sqrt{q}},$$

és

$$\left|h(i) - \eta^2 q\right| \leq 50\sqrt{q}\log(4q)$$

minden $0 \leq i \leq q-1$-re.

Bizonyítás. A Csebisev-tétel miatt létezik olyan p prím, melyre $2q < p \leq 4q$. A halmaz definíciójából következik, hogy

$$\sum_{i=1}^{q} \left(\frac{i}{p}\right) = q\eta - q(1-\eta) = q(2\eta - 1),$$

és a 3.2.2. tételből (vagy a Pólya-Vinogradov egyenlőtlenségből) így

$$q\,|2\eta-1| = \left|\sum_{i=1}^{q}\left(\frac{i}{p}\right)\right| \le 9\sqrt{p}\log p \le 18\sqrt{q}\log(4q).$$

Emiatt pedig

$$\left|\eta-\frac{1}{2}\right| \le 9\frac{\log(4q)}{\sqrt{q}}.$$

Legyen a egész, melyre $1 \le a \le q$. A már látott technikával bizonyítható, hogy

$$f(a) = \sum_{i=1}^{a-1}\frac{\left(\left(\frac{i}{p}\right)+1\right)\left(\left(\frac{a-i}{p}\right)+1\right)}{4} = \frac{1}{4}\sum_{i=1}^{a-1}\left(\frac{i(a-i)}{p}\right)+\frac{1}{2}\sum_{i=1}^{a-1}\left(\frac{i}{p}\right)+\frac{a-1}{4}.$$

$1 \le a < p$, ezért $x(a-x)$ nem írható fel $b\,(h_1(x))^2$ alakban $F_p\,[x]$-ben, ezért használhatjuk a 3.2.2. tételt az első tagra, és nyílván a másodikra is:

$$\left|\frac{1}{4}\sum_{i=1}^{a-1}\left(\frac{i(a-i)}{p}\right)+\frac{1}{2}\sum_{i=1}^{a-1}\left(\frac{i}{p}\right)\right| \le \left(\frac{18}{4}+\frac{9}{2}\right)\sqrt{p}\log p \le 18\sqrt{q}\log(4q).$$

Tehát

$$\left|f(a)-\frac{a-1}{2}\right| \le 18\sqrt{q}\log(4q).$$

Hasonlóan

$$\begin{aligned} f(a+q) &= \sum_{i=a}^{q}\frac{\left(\left(\frac{i}{p}\right)+1\right)\left(\left(\frac{q+a-i}{p}\right)+1\right)}{4} \\ &= \frac{1}{4}\sum_{i=a}^{q}\left(\frac{i(q+a-i)}{p}\right)+\frac{1}{2}\sum_{i=a}^{q}\left(\frac{i}{p}\right)+\frac{q-a+1}{4}. \end{aligned}$$

$1 \le a+q < p$, ezért az előzőekhez hasonló módon belátható, hogy

$$\left|f(a+q)-\frac{q-a+1}{4}\right| \le 18\sqrt{q}\log(4q).$$

Ha $1 \le i \le q$, akkor $h(i) = f(i)+f(q+i)$ (és $h(q)=h(0)$), ezért a most belátott egyenlőtlenségek miatt

$$\left|h(i)-\frac{q}{4}\right| \le 36\sqrt{q}\log(4q)$$

minden $1 \leq i \leq q$-re.

Látszik, hogy

$$\left|\frac{q}{4} - \eta^2 q\right| = \frac{q}{4}\,|2\eta - 1|\,|2\eta + 1| \leq \frac{3}{4}q\,|2\eta - 1| \leq \frac{27}{2}\sqrt{q}\log(4q).$$

Ezért

$$\left|h(i) - \eta^2 q\right| \leq \left|h(i) - \frac{q}{4}\right| + \left|\frac{q}{4} - \eta^2 q\right| \leq \frac{99}{2}\sqrt{q}\log(4q)$$

minden $0 \leq i \leq q - 1$ egészre, és ezzel beláttuk a bizonyítandó állítást. $\square$

Nyitott kérdések

Ebben a részben a dolgozat során felmerült nyitott problémákat összegezzük. Mint láttuk, Roth eredeti, számtani sorozatok színezésére vonatkozó problémája teljesen megoldott, az ismert alsó és felső becslés csak konstans szorzóban tér el egymástól. A d-dimenziós általánosítások esetében már nem ez a helyzet, mind az általunk, mind a Knieper által vizsgált problémánál ([5]) a felső becslés egy log-hatvány szorzóval rosszabb az alsó becslésnél. Mindkét esetben a bizonyítás Beck módszerét alkalmazza, esetleg Matoušek és Spencer bizonyítását adaptálva kihozható lenne a pontos felső becslés. (Knieper az általa vizsgált esetben sikertelenül próbálkozott ezzel.)

Megoldatlan az $N \times N$-es rácson tekintett szakaszok diszkrepanciájának meghatározása. A 2.2. részben bizonyítottunk egy felső becslést, a sejtés az, hogy ez log-hatvány szorzó erejéig éles, eddig azonban alsó becslést nem sikerült bizonyítani.

A kéttagú összegek eloszlásának irregularitásairól szóló tételeknél is van hézag az ismert alsó és felső becslés között. Itt nem világos, hogy az alsó becslés vajon éles-e, bár az tűnik valószínűnek. A moduláris verzióban az alsó és felső becslés között a különbség csak egy log-hatvány szorzó, de esetleg ez is csökkenthető.

Irodalomjegyzék

[1] J. Beck. Roth's estimate of the discrepancy of integer sequences is nearly sharp. *Combinatorica*, 1:319–325, 1981.

[2] H. Chernoff. A measure of asymptotic tests of a hypothesis based on the sum of observations. *Ann. Math. Stat.*, 23:493–509, 1952.

[3] P. Erdős and A. Sárközy. Some solved and unsolved problems in combinatorial number theory. *Math. Slovaca*, 28:407–421, 1978.

[4] P. Erdős, A. Sárközy, and V. T. Sós. Problems and results on additive properties of general sequences, V. *Monatshafte Math.*, 102:183–197, 1986.

[5] P. Knieper. *Discrepancy of Arithmetic Progressions.* PhD thesis, Institute für Informatic, Humboldt-Universität zu Berlin, 1997.

[6] Gy. Károlyi. Geometric discrepancy theorems in higher dimensions. *Studia Sci. Math. Hung.*, 30:59–94, 1995.

[7] L. Lovász, J. H. Spencer, and K. Vesztergombi. Discrepancy of set-systems and matrices. *European J. Combin.*, 7:151–160, 1986.

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

[9] K. F. Roth. Remark concerning integer sequences. *Acta Arithmetica*, IX:257–260, 1964.

[10] W. Rudin. Some theorems on Fourier coefficients. *Proc. Amer. Math. Soc.*, 10:855–859, 1959.

[11] J. Matoušek and J. Spencer. Discrepancy in arithmetic progressions. *J. Amer. Math. Soc.*, 9:195–204, 1996.

[12] A. Sárközy. Some remarks concerning irregulaties of distribution of sequences of integers in arithmetic progressions, I. *Coll. Math. Soc. J. Bolyai*, 13:287–303, 1974.

[13] A. Sárközy. Some remarks concerning irregulaties of distribution of sequences of integers in arithmetic progressions, II. *Studia Sci. Math. Hung.*, 11:79–104, 1976.

[14] A. Sárközy. Some remarks concerning irregulaties of distribution of sequences of integers in arithmetic progressions, III. *Periodica Math. Hungar.*, 9:127–144, 1978.

[15] A. Sárközy. Some remarks concerning irregulaties of distribution of sequences of integers in arithmetic progressions, IV. *Acta Math. Acad. Sci. Hung.*, 30:155–162, 1977.

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

[17] A. Weil. Sur les courbes algébriques et les variétés qui en déduisent. *Actualités Sci. et Ind.*, 1041, 1948.