Egyenesmentes halmazok a háromelemű test felett

Szakdolgozat
Matematika alapszak
Matematikus szakirány

készítette:
Markó Ádám

témavezető:
Dr. Frenkel Péter
Adjunktus
Algebra és Számelmélet Tanszék

Eötvös Loránd Tudományegyetem
Természettudományi Kar
Matematikai Intézet

Budapest, 2019

Köszönetnyilvánítás

Ezúton is szeretném megköszönni a témavezetőmnek, Frenkel Péternek az érdekes témát és a sok hasznos tanácsot.

Tartalomjegyzék

Bevezetés

Az additív kombinatorika egyik fontos kérdése különböző Abel-csoportok felett a 3 hosszú számtani sorozatot nem tartalmazó részhalmazok számosságának becslése. Ez a tulajdonság a háromelemű test vektorterei felett megegyezik azzal, hogy az adott részhalmaz egyenesmentes. Ez a szakdolgozat felső korlátot próbál adni ilyen halmazokra. Először Behrend és Buhren bizonyította, hogy egy $\mathbb{F}_3^n$ vektortéren egy egyenesmentes halmaz számossága legfeljebb $o(3^n)$ [3]. Később Roy Meshulam bizonyította, hogy egy ilyen halmaz számossága legfeljebb $\frac{3^n}{n}$ [8]. Ezután Bateman és Katz talált jobb felső korlátot [1], ami szerint létezik olyan $\varepsilon > 0$, hogy a legnagyobb egyenesmentes részhalmaz számossága legfeljebb $O(\frac{3^n}{n^{1+\varepsilon}})$. Először Ben Green fogalmazta meg a sejtést[6], hogy létezik olyan $\lambda < 3$ konstans, amire az egyenesmentes halmazok számossága $O(\lambda^n)$. Ezt Croot, Lev és Pach módszerével [4] sikerült Ellenbergnek és Gijswijtnak bizonyítania [5]. A szakdolgozat elsődleges témája ezen bizonyítás lesz. Az 1. és 2. fejezetben bizonyítjuk a tételt, először az eredeti módszerrel, másodszor Tao módszerével [10]. A 3. fejezetben áttérünk a 4 hosszú számtani sorozatokat nem tartalmazó részhalmazok esetére, amit hasonló módszerekkel próbálunk meg közelíteni. A 4. fejezetben becslést adunk az imént említett λ kontansra. A szakdolgozat végén pedig vektorterek mellett más Abel-csoportokban fogunk becslést adni 3 hosszú részsorozatot nem tartalmazó halmazok méretére. Az 5.fejezetben bizonyítjuk Meshulam tételét, ami tetszőleges páratlan elemszámú Abel-csoportra érvényes. A 6. és 7. fejezetben pedig a Z_k^n alakú Abel-csoportok esetét vizsgáljuk, ahol a 6. fejezetben k tetszőleges páratlan szám, a 7. fejezetben pedig prímhatvány. Értelemszerűen minél speciálisabb egy Abel-csoport annál jobb becslést tudunk adni.

1. fejezet

Az Ellenberg-Gijswijt tétel

Először az eredeti Ellenberg-Gijswijt tételt bizonyítjuk. Az eredeti cikk [5] bizonyításánál most elemibb módszereket használunk, később tárgyalásra kerülnek pontosabb becslések is. Először definiáljuk az alapfogalmakat, amiket használni fogunk a dolgozat során. Legyen q páratlan prímszám, $\mathbb{F}_q$ a modulo q maradékosztályok által alkotott test, n természetes szám, $\mathbb{F}_q^n$ vektortere $\mathbb{F}_q$ -nak. Legyen $d \in \mathbb{R}$ olyan, hogy $0 \leq d \leq (q-1)n$. Ha tekintjük az $\mathbb{F}_q^n$ -ből $\mathbb{F}_q$ -ba menő függvényeket, ezeket tekinthetjük úgy, mint n változós polinomokat. A polinomokat fel lehet írni, mint monomok összegét. Legyen $M_{n,d}$ azon monomok halmaza, amikben a változók fokainak összege legfeljebb d, és minden változó foka legfeljebb $q-1$:

$$M_{n,d} := \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha_1 + \cdots + \alpha_n \leq d, \alpha_i \leq q-1\}$$

Legyen $m_{n,d} := |M_{n,d}|$, ami felírható olyan alakban is, hogy

$$m_{n,d} = \dim(\mathrm{span}(M_{n,d})).$$

Lemma Legyen $A \subset \mathbb{F}_q^n$, $\alpha, \beta, \gamma \in \mathbb{F}_q$, $\gamma \neq 0$, $\alpha + \beta + \gamma = 0$, $P \in \mathrm{span}(M_{n,d})$ olyan, hogy $\forall a_1, a_2 \in A, a_1 \neq a_2 : P(\alpha a_1 + \beta a_2) = 0$. Ekkor

$$\#\{a \in A; P(-\gamma a) \neq 0\} \leq 2m_{n,d/2}.$$

Bizonyítás Legyen $B \in \mathbb{F}_q^{|A|\times|A|}$, $B(i,j) = P(\alpha a_i + \beta a_j)$. A $P(\alpha x + \beta y)$ polinomot fel tudjuk írni monomok összegére (x és y szerint), amiknek a foka kisebb, mint d, tehát egy ilyen monomban az x-beli és y-beli változók fokainak az összege közül valamelyiknek kisebbnek kell lennie, mint $d/2$. Ezek szerint némi átírással

$$P(\alpha x + \beta y) = \sum_{m \in M_{n,d/2}} m(x)F_m(y) + \sum_{m \in M_{n,d/2}} G_m(x)m(y).$$

Tetszőleges $m \in M_{n,d/2}$-re legyen $B_{m,F} \in \mathbb{F}_q^{|A|\times|A|}$, ahol $B_{m,F}(i,j) = m(a_i)F_m(a_j)$. Hasonló módon $B_{m,G} \in \mathbb{F}_q^{|A|\times|A|}$, ahol $B_{m,F}(i,j) = G_m(a_i)m(a_j)$. Értelemszerűen a B_m

mátrixok rangja 1, mivel minden sor a legelső nemnulla sor skalárszorosa.

$$B = \sum_{m \in M_{n,d/2}} B_{m,F} + \sum_{m \in M_{n,d/2}} B_{m,G}$$

Ezek szerint B-t fel lehet írni, mint $2m_{n,d/2}$ egy rangú mátrix összege. Ez alapján B rangja sem lehet nagyobb, mint $2m_{n,d/2}$. Vegyük észre, hogy B minden nem a főátlón lévő eleme nulla. Ezek alapján a főátlóin is maximum $2m_{n,d/2}$ elem lehet. Ezzel a lemmát beláttuk.

Lemma Legyen $A \subset \mathbb{F}_q^n$ és $\alpha, \beta, \gamma \in \mathbb{F}_q$, $\gamma \neq 0$,$\alpha + \beta + \gamma = 0$ olyan, hogy $\forall a_1, a_2, a_3 \in A$; $\alpha a_1 + \beta a_2 + \gamma a_2 = 0 \Leftrightarrow a_1 = a_2 = a_3$. Ekkor $|A| \leq 3m_{n,(q-1)n/3}$.

Bizonyítás Legyen $A \subset \mathbb{F}_q^n$ -re $\mathcal{S}(A) := \{\alpha a_1 + \beta a_2 \mid a_1, a_2 \in A, a_1 \neq a_2\}$. Ekkor a lemmában szereplő A halmaz tulajdonsága átírható olyan módon, hogy $-\gamma A$ diszjunkt $\mathcal{S}(A)$-tól. Legyen P polinom $P \in \text{span}(M_{n,d})$ olyan, hogy$P$ eltűnik a $\mathbb{F}_q^n \setminus (-\gamma A)$ halmazon. Ekkor nyilván az $\mathcal{S}(A)$ halmazon is eltűnik. Az előző lemma alapján ekkor azon A - beli elemek száma, amiken P nem vesz fel nullát, legfeljebb $2m_{d/2,n}$. Vegyük észre, hogy az ilyen P polinomok, amik eltűnnek a $\mathbb{F}_q^n \setminus (-\gamma A)$ halmazon vektorteret alkotnak, legyen ez $\mathcal{P}$. Ekkor $\dim(\mathcal{P}) = \max\{0, m_{n,d} - (|\mathbb{F}_q^n| - |A|)\}$ ha P maximális tartójú, akkor

$$\#\{a \in \mathbb{F}_q^n \mid P(a) \neq 0\} \geq \dim(\mathcal{P}).$$

Amiből, ha felhasználjuk az eddigi egyenlőtlenségeket,

$$2m_{n,d/2} \geq \#\{a \in \mathbb{F}_q^n \mid P(a) \neq 0\} \geq \dim(\mathcal{P}) \geq m_{n,d} - (|\mathbb{F}_q^n| - |A|)\}.$$

Most az egyenlőtlenség két vége átrendezhető olyan módon, hogy az egyenlőtlenség egyik végén csak $|A|$ álljon: $|A| \leq 2m_{n,d/2} + q^n - m_{n,d}$. Ekkor $q^n - m_{n,d}$ elképzelhető úgy, mint azon monomok által kifeszített polinomok, amik foka nagyobb, mint d. Ez bijekcióba állítható azon monomok által kifeszített polinomokkal, amik foka kisebb, mint $= (q-1)n - d$; ezt úgy lehet elképzelni, hogy minden egyes monomnak vesszük az inverzét és beszorozzuk $x_1^{q-1} ... x_n^{q-1}$ -gyel. Ez alapján $|A| \leq 2m_{n,d/2} + m_{n,(q-1)n-d}$ Mivel $m_{n,d}$, mint d függvénye monoton növő, ezért d -re behelyettesítve $2/3(q-1)n$ -t azt kapjuk, hogy:

$$|A| \leq 3m_{n,(q-1)n/3}$$

Ezzel a lemmát beláttuk.

Most legyen $q = 3$ és $\alpha = \beta = \gamma = 1$, ekkor a fent meghatározott tulajdonságú A halmaz egyenesmentes. Az a_1, a_2, a_3 különböző pontok pontosan akkor alkotnak egyenest, ha az összegük nulla, azaz minden koordinátájukban vagy megyeznek, vagy páronként különböznek. Ekkor létezik olyan $\lambda < 3$, amire $\mid A \mid < \lambda^n$. Sőt, általában is meg lehet mutatni elemi módszerekkel, ha létezik olyan $\epsilon > 0$, hogy $\frac{d}{n} < \frac{1}{2} - \epsilon$ akkor létezik olyan

$\lambda < q$, hogy $m_{n,d} < \lambda^n$. Legyen $X_i, i \in \{1, \cdots, n\}$ valószínűségi változó $\{0, \cdots q-1\}$, ahol Ekkor

$$m_{n,d} = q^n P(X_1 + \cdots + X_n \leq d) = q^n P(\exp(\phi(X_1 + \cdots + X_n)) \geq \exp(\phi d)),$$

ahol ϕ tetszúleges negatív valós szám. Ekkor a fenti kifejezést a Markov egyenlőtlenséggel becsülve:

$$m_{n,d} \leq q^n E(\exp(\phi * (X_1 + \cdots + X_n)) \exp(-\phi d) = q^n E(\exp \phi(X_1))^n \exp(-\phi d) =$$

Mivel ezek a változók függetlenek, várható értéke a szorzatnak a várható értékek szorzata. A várható értéket összegként felírva:

$$= \left(\sum_{i=0}^{q-1} \exp(\phi i - \phi d/n) \right)^n = \left(\sum_{i=0}^{q-1} x^{i-d/n} \right)^n$$

$$\left(\sum_{i=0}^{q-1} x^{i-d/n} \right)^n \leq \left(\sum_{i=0}^{q-1} x^{i-\frac{q-1}{2}+\epsilon} \right)^n,$$

minden $0 < x < 1$-ra. Itt $\lim_{x \to 1} \left(\sum_{i=0}^{q-1} x^{i-d/n} \right) = q$ A kifejezés deriváltja egyhez közelítve pozitív (ha $\frac{d}{n} < \frac{q-1}{2}$). Ha a d változót n többszöröseként képzeljük el akkor valamilyen $\epsilon > 0$ konstansra, tehát λ n-től független, és ha $d > \frac{(q-1)n}{2}$, akkor $m_{n,d} > \frac{q^n}{2}$, tehát q-nál kisebb λ létezésére a határ éles.

Tétel(Ellenberg-Gijswijt) Legyen q egy kettőtől különböző prím. Ekkor létezik olyan $\lambda < q$, ha $\alpha, \beta, \gamma \in \mathbb{F}_q$ olyan, hogy $\alpha + \beta + \gamma = 0$, és $\gamma \neq 0$. Ha $A \subset \mathbb{F}_q^n$ olyan, hogy $a, b, c \in A$ elemekre $\alpha a + \beta b + \gamma c = 0$ pontosan akkor, ha $a = b = c$, akkor

$$|A| < \lambda^n.$$

Felmerül a kérdés, hogy mit állíthatunk abban az esetben, ha $\mathbb{F}_q$ páratlan prímhatványrendű test. Legyen $q = p^k$, ebben az esetben $\mathbb{F}_q$ elképzelhető úgy, mint egy vektortér a $\mathbb{F}_p$ test egy vektortere, és így az Ellenberg-Gijswijt tétel általánosítható prímhatványrendű testekre is.

2. fejezet

A rang általánosítása

Legyen l egy természetes szám. Először vegyük az $l \times l$ -es mátrixokon a rang egy ekvivalens bevezetését. Legyen $[l] := \{1, \cdots, l\}$. A mátrixok itt függvények, az $[l] \times [l]$ halmazból $\mathbb{F}_q$ -ba. Ez természetesen vektortér $\mathbb{F}_q$ fölött. Más tulajdonságát a mátrixoknak nem fogjuk használni, így lehetőség van a rang általánosítására. Itt egy 0-tól különböző B mátrix akkor 1 rangú, ha létezik egy-egy f, g függvény $[l]$ -ből $\mathbb{F}_q$-ba, hogy minden $i, j \in [l]$ -hez $B(i,j) = f(i)g(j)$. Egy B mátrix rangja a legkisebb olyan k szám, hogy B előáll k darab egy rangú mátrix összegeként, illetve az azonosan 0 mátrix rangja nulla. Ez láthatóan ekvivalens a rang egyéb definícióival. Most ezen elv alapján általánosítjuk a rangot. Legyen n egy természetes szám, $n \geq 2$. Nevezzük a $\times_{i=1}^{n}[l]$ halmazon értelmezett $\mathbb{F}_q$ -ba tartó függvényeket hipermátrixoknak. Ezeknek a vektorterén értelmezzük a rang függvényt a következőképpen: Az 1 rangú elemek legyenek azon B elemek, melyekhez létezik olyan $i \in [n]$, $f_i : [l] \to \mathbb{F}_q$, $g_i : [l]^{n-1} \to \mathbb{F}_q$ nem azonosan 0 függvények, hogy $B(j_1, \cdots, j_i, \cdots, j_n) = f_i(j_i)g_i(j_1, \cdots, j_{i-1}, j_{i+1}, \cdots, j_n)$ minden $(j_1, \cdots, j_n) \in [l]^n$-re. Egy B elem rangja pedig legyen a legkisebb k szám, hogy B előáll k darab 1 rangú mátrix összegeként. Végül az azonosan nulla hipermátrix rangja legyen nulla. Egy diagonális mátrix rangja, aminek a főátlón kívül elemei mind nullák megegyezik a főátló nemnulla elemeinek számával. Ez a viszonylag egyszerű állítás általánosítható hipermátrixokra is. [10] szerint:

Állítás Legyen B olyan hipermátrix, hogy

$$B(j_1, \cdots, j_n) = \sum_{i=1}^{l} c_i \delta_i(j_1) \cdots \delta_i(j_n)$$

valamilyen c_i konstansokra, ahol δ a Kronecker delta. Ekkor

$$\mathrm{rank}(B) = \#\{i \in [l] \mid c_i \neq 0\}.$$

Bizonyítás A bizonyításban n-re való indukciót használunk. Az $n = 2$ eset mátrixokra megfogalmazva ismert. Most tegyük fel egy adott n-re, hogy minden n -nél kisebb számosságra már megoldottuk a problémát. Az látható, hogy a nemnulla elemek száma nagyobb vagy egyenlő, mint a rang, mert könnyen meg lehet adni olyan konstrukciót, ami pont annyi elemből áll, mint a főátlón szereplő nemnulla elemek száma. Minden olyan i -re, amire c_i nem nulla, legyen $f_i(x_1) = \delta_i(x_1), g_i(x_2, \cdots, x_n) = c_i\delta_i(x_2)\cdots\delta_i(x_n)$ Ezek láthatóan csak egy helyen vesznek fel nemnulla értéket, és pont a megfelelő helyeken. Másrészt tegyük fel, hogy a rang kisebb, mint a nemnulla elemek száma. Vegyük észre, hogy azon hipersíkok, amik metszeténél a főátló helyén nulla van, és amik párhuzamosak a hipermátrix oldalaival, csupa nullát vesznek fel mindenhol, így ha ezeket kihúzzuk és vesszük a részhipermátrixot, nem csökkentünk a rangon. Szemléletesen ez ahhoz hasonló, mintha egy mátrixban van egy teljesen nulla sor és oszlop is, akkor az ennek a sornak és oszlopnak a kihúzásával keletkezett részmátrix rangja is megegyezik az eredeti mátrixéval. Hogyha a részhipermátrixot le tudjuk generálni k megfelelő f_j, g_j függvénypárral, akkor ezeket bővíteni tudjuk úgy, hogy a megfelelő i-edik főátlóbeli elemet f_j-hez $(1-\delta_i(x_j))$-vel szorozzuk, g_j-t pedig $(1-\delta_i(x_1))\cdots(1-\delta_i(x_{j-1}))(1-\delta_i(x_{j+1}))\cdots(1-\delta_i(x_n))$ -vel. Ez alapján elég bizonyítani az állítást olyan hipermátrixokra, ahol a főátlón sehol sincs nemnulla elem. Ez indirekten fog történni, tegyük fel, hogy létezik olyan legfeljebb $l-1$ függvénypárosból álló rendszer, amivel B előállítható. Ekkor

$$\sum_{i=1}^{l} c_i\delta_i(j_1)\cdots\delta_i(j_n) = \sum_{i=1}^{n}\sum_{\alpha\in I_i} f_{i,\alpha}(j_i)g_{i,\alpha}(j_1, \cdots, j_{i-1}, j_{i+1}, \cdots, j_n)$$

valamilyen I_i halmazokra, melyek számosságának összege legfeljebb l_1 és valamilyen $f_{i,\alpha} : [l] \to \mathbb{F}_q$ és $g_{i,\alpha} : [l]^{n-1} \to \mathbb{F}_q$ függvényekre. Itt létezik olyan I_i ami nemüres, ezt válasszuk ki azután nézzük azon $[l] \to \mathbb{F}_q$ függvények H vektorterét, melyek ortogonálisak minden $f_{i,\alpha}, \alpha \in I_i$ függvényre, nevezetesen, $h \in H$ esetén:

$$\sum_{j=1}^{l} f_{i,\alpha}(j)h(j) = 0$$

Ekkor H dimenzióját nevezzük d-nek, ez legalább $l - |I_i|$. Így H bázisának elemeit egymás után írva kapunk egy $l \times d$ méretű mátrixot, aminek a rangja d, tehát ennek van olyan $d \times d$ méretű részmátrixa, aminek a rangja d, tehát invertálható, ezért egy d dimenziós vektortér bármelyik nemnulla elemét ezzel a mátrixszal szorozva nemnulla elemet kapunk. Ebből következik, hogy a H vektortérnek létezik olyan eleme, amire legalább d olyan x elem van az $[l]$ halmazból amire $h(x)$ nem egyenlő nullával. Legyen $g_{0,i,\alpha} : [l]^{n-2} \to \mathbb{F}_q$ a következő módon megkonstruálva:

$$g_{0,i,\alpha}(x_1, x_2, \cdots, x_{n-2}) = \sum_{j=1}^{l} h(j)g_{0,i,\alpha}(x_1, x_2, \cdots, x_{n-2}, j).$$

Most nézzük a következő összeget:

$$\sum_{k=1}^{l}\sum_{i=1}^{n}\sum_{\alpha\in I_i} f_{i,\alpha}(j_i)g_{i,\alpha}(j_1, \cdots, j_{i-1}, j_{i+1}, \cdots, j_{n-1}, k)h(k).$$

Ez egyoldalról egyenlő a

$$\sum_{k=1}^{l}\sum_{i=1}^{l} c_i\delta_i(j_1)\cdots\delta_i(k) = \sum_{i=1}^{l} c_i h(i)\delta_i(j_1)\cdots\delta_i(j_{n-1})$$

kifejezéssel. Ez egy függvény $[l]^{n-1}$ ből $\mathbb{F}_q$-ba, tehát egy hipermátrix, és olyan, ami csak a főátlón vesz fel nemnulla elemeket. Ennek a hipermátrixnak a rangja pontosan a nemnulla $h(i)$-k száma, ahol $i \in [l]$ ez egyenlő d-vel. Másrészt h ortogonális minden $f_{i,\alpha}$-ra egy bizonyos i-re. Az általánosság elvesztése nélkül feltehetjük, hogy ez az i az n, mert a változókat át lehet indexelni. Ekkor az előző összeget ki tudjuk fejezni a következőképpen:

$$\sum_{i=1}^{n-1}\sum_{\alpha\in I_i} f_{i,\alpha}(j_i)g_{i,\alpha,0}(j_1,\cdots,j_{i-1},j_{i+1},\cdots,j_{n-1})$$

Ennek a hipermátrixnak a rangja legfeljebb $\sum_{i=1}^{n-1}|I_{i,\alpha}|$, ami kisebb mint $l-|I_{i_n,\alpha}|-1$, viszont $d \geq l-|I_{n,\alpha}|$. Ez ellentmondás, tehát az eredeti feltevésünk hamis volt, ezzel az állítást beláttuk.

A következőkben a fenti állítás felhasználásával általánosítani fogjuk az Ellenberg-Gijswijt-tétel első állítását a következőképpen:

Állítás Legyen $\mathbb{F}_q$ véges test, $k > 2$ természetes szám, $\alpha_1,\cdots,\alpha_k \in \mathbb{F}_q, \sum_{i=1}^{k}\alpha_i = 0, \alpha_k \neq 0, A \subset \mathbb{F}_q^n$ és $P \in \operatorname{span}(M_{n,d})$ olyan, hogy minden $a_1,a_2,\cdots,a_{k-1} \in A, \exists a_i, a_j \in \{a_1,\cdots,a_k\}; a_i \neq a_j$ esetén $P(\sum_{i=1}^{k-1}\alpha_i a_i) = 0$. Ekkor igaz, hogy

$$\#\{a \in A \mid P(\alpha_k a) \neq 0\} \leq (k-1)m_{n,d/(k-1)}.$$

Bizonyítás Legyenek $x_1,\cdots,x_{k-1}$ n-dimenziós sorvektorok, melyek elemei határozatlanok. Ha tekintjük a $P(\sum_{i=1}^{k-1}\alpha_i x_i)$ polinomot, mint monomok összegét, akkor minden egyes monom legfeljebb $k-1$-ed fokú, tehát a skatulyaelv szerint minden egyes monomhoz létezik olyan x_i vektora a változóknak, hogy a monomban az x_i-beli változók összfoka legfeljebb $\frac{d}{k-1}$. Eszerint P-t fel lehet írni a következő módon:

$$P\left(\sum_{i_1}^{k-1}\alpha_i x_i\right) = \sum_{i=1}^{k-1}\sum_{m\in M_{n,d/(k-1)}} m(x_i)F_{i,m}(x_1,\cdots,x_{i-1},x_{i+1},\cdots,x_{x-1})$$

ahol $F_{i,m}$ megfelelő polinomok. Most legyen B olyan $\times_{i=1}^{k-1} \mid A \mid$ méretű hipermátrix, ami az $(a_1,\cdots,a_{k-1})$ helyen $P(\sum_{i=1}^{k-1}\alpha_i a_i)$ értéket vesz fel. Ez a hipermátrix felírható, mint legfeljebb $(k-1)m_{n,d/(k-1)}$ mátrix összege, $B_{i,m,F}$ legyen olyan, hogy $i \in \{1,\cdots,k-1\}$, $m \in M_{n,d}$ illetve $F_{i,m} : \mathbb{F}_q^{n\times(k-2)} \to \mathbb{F}_q$

$$B_{i,m,F}(a_1,\cdots,a_{k-1}) = m(a_i)F_{i,m}(a_1,\cdots,a_{i-1},a_{i+1},\cdots a_k-1).$$

Ekkor természetesen

$$B = \sum_{i=1}^{k-1} \sum_{m \in M_{n,d}} B_{i,m,F}.$$

Ebből jól látszik, hogy B rangja legfeljebb $(k-1)M_{n,d}$, másrészt B csak a főátlón vesz fel nem nulla elemeket, tehát a rang általánosításánál bizonyított lemma szerint a nemnulla elemek száma legfeljebb $(k-1)M_{n,d}$.

Állítás Legyen $\mathbb{F}_q$ véges test, $k > 2$ természetes szám, $\alpha_1, \cdots, \alpha_k \in \mathbb{F}_q$, $\sum_{i=1}^{k} = 0, \alpha_k \neq 0$ és $A \subset \mathbb{F}_q^n$ olyan részhalmaz, amire a $\sum_{i=1}^{k} \alpha_i a_i = 0, a_i \in A$ egyenletnek csak olyan megoldásai vannak, amire $a_1 = \cdots = a_k$. Ekkor

$$|A| \leq k m_{n, \frac{(q-1)n}{k}}.$$

Bizonyítás A $k = 3$ esettel teljesen analóg módon. Az állítás tulajdonságával ekvivalens, hogy A diszjunkt az

$$\mathcal{S}(A) := \left\{ \sum_{i=1}^{k-1} \alpha_i a_i \mid a_i \in A, \exists a_i, a_j : a_i \neq a_j \right\}$$

halmaztól. Ha vesszük azon legfeljebb d fokú P polinomok vektorterét, amik eltűnnek az A komplementerén, ezek dimenziója nagyobb vagy egyenlő, mint $m_{n,d} - (q^n - |A|)$. Ezek szerint, ha kiválasztjuk a legnagyobb tartójú $p \in P$ polinomot, az legalább $m_{n,d} - (q^n - |A|)$ helyen nem tűnik el. Másrészt a fenti állítás alapján p legfeljebb $m_{n,d/(k-1)}$ helyen tűnik el, tehát:

$$m_{n,d/(k-1)} \geq m_{n,d} - (q^n - |A|);$$

ezt átrendezve:

$$|A| \leq m_{n,d/(k-1)} + m_{n,(q-1)n-d},$$

ahol $d = \frac{(k-1)(q-1)n}{k}$ választással:

$$|A| \leq k m_{n, \frac{(q-1)n}{k}}.$$

Ezzel az állítást beláttuk.

A következőkben a rang általánosításánál ismertetett állítást felhasználva lehet bizonyítani az Ellenberg-Gijswijt tételt más módon is, ahol szimmetrikusan tekintjük az A halmaz elemeit. Legyen $A \subset \mathbb{F}_q^n$; az A halmaz pontosan akkor egyenesmentes, ha $a_1, a_2, a_3 \in A$-ra

$$\delta_{0^n}(a_1 + a_2 + a_3) = \sum_{\alpha \in A} \delta_\alpha(a_1)\delta_\alpha(a_2)\delta_\alpha(a_3).$$

Ez könnyen látható, mivel az egyenlet bal oldala pontosan akkor vesz fel 1-et, ha a_1, a_2, a_3 egyenesen vannak, vagy megegyeznek. Ha A egyenesmentes, akkor ez csak úgy állhat elő, ha $a_1 = a_2 = a_3$, de ekkor a jobb oldal is 1-et vesz fel.

Állítás: Legyen $B : (\mathbb{F}_3^n)^3 \to \mathbb{F}_3$ olyan, hogy minden $x, y, z \in \mathbb{F}_q^n$-re

$$B(x, y, z) = \delta_{0^n}(x + y + z).$$

Ekkor B rangja legfeljebb $3m_{n,2n/3}$.

Bizonyítás: Ha $x_0 \in \mathbb{F}_3$, akkor $\delta_0(x_0) = 1 - x_0^2$. Több dimenzióban a Kronecker-delta felírható, mint egydimenziós Kronecker-delták szorzata, tehát B kifejezhető a következő módon:

$$B(x, y, z) = \prod_{i=1}^{n}(1 - (x_i + y_i + z_i)^2).$$

A szorzatban minden egyes kifejezés foka 2 tehát az egész kifejezés foka $2n$ ezt a polinomot monomokra bonthatjuk, amiknek foka kisebb, mint $2n$, tehát a skatulyaelv szerint minden monomban az x-beli az y-beli, vagy a z -beli változók foka legfeljebb $\frac{2n}{3}$. Ez alapján B felírható a következő módon:

$$B(x, y, z) = \sum_{m \in M_{n,2n/3}} m(x)F_m(y, z) + \sum_{m \in M_{n,2n/3}} m(y)G_m(x, z) + \sum_{m \in M_{n,2n/3}} m(z)H_m(x, z).$$

Így felírtuk B-t mint legfeljebb $3m_{n,2n/3}$ darab 1 rangú mátrix összegét, eszerint B rangja is legfeljebb $3m_{n,2n/3}$. Ha B-t csak az A elemein néznénk, mint egy B' minorját a B hipermátrixnak a rangja ennek sem lehet nagyobb, és mivel ennek a mátrixnak csak a főátlón vannak elemei, ezért B' legfeljebb $3m_{n,2n/3}$. helyen vesz fel nemnulla értéket. Másrészt A minden eleméhez kell, hogy B' vegyen fel nemnulla értéket, tehát A elemszáma legfeljebb $3m_{n,d}$.

3. fejezet

Négy hosszúságú számtani sorozatot nem tartalmazó halmazok

A három hosszú sorozat után felmerül a kérdés, hogy még milyen, valamilyen adott halmaz affin képét nem tartalmazó halmazok mérete becsülhető az eddig bemutatott módszerekkel. Legyen q továbbra is páratlan prím. A [10] munkában merül fel, hogy a 4 hosszú számtani sorozatot nem tartalmazó A halmazokra van-e olyan $\lambda < q$, hogy $|A| < \lambda^n$. Itt feltehetjük, hogy q nagyobb, mint 3. Ez egyelőre nyitott kérdés. Azt, hogy A nem tartalmaz 4 hosszú számtani sorozatot, többféle módon is fel lehet írni. Például A pontosan akkor nem tartalmaz 4 hosszú számtani sorozatot, ha $a, b, c, d \in A$-ra

$$\delta_{0^n}(a-2b+c)\delta_{0^n}(b-2c+d) = \sum_{\alpha \in A} \delta_\alpha(a)\delta_\alpha(b)\delta_\alpha(c)\delta_\alpha(d).$$

Valóban, $a-2b+c=0, b-2c+d=0$ pontosan akkor, ha $b-a=c-b=d-c$, ami azt jelenti, hogy a, b, c, d 4 hosszú számtani sorozatot alkotnak. Fel lehet írni ehhez hasonló egyenlőséget olyan módon is, hogy, az egyenletünk bal oldalán csak egy Kronecker-delta álljon. Vezessük be $\mathbb{F}_q^n$ elemein a szorzást, mint koordinátánkénti szorzást. Az így kapott gyűrű izomorf $\bigoplus_{i=1}^n \mathbb{F}_q$ -val. Jelölje $x \in \mathbb{F}_q^n$ -ra x^2 a koordinántánkénti négyzetreemelést, és legyen $\gamma \in \mathbb{F}_q$, $\left(\frac{\gamma}{q}\right) = -1$. Ekkor az A halmaz pontosan akkor nem tartalmaz 4 hosszú számtani sorozatot, ha

$$\delta_{0^n}((a-2b+c)^2 - \gamma(b-2c+d)^2) = \sum_{\alpha \in A} \delta_\alpha(a)\delta_\alpha(b)\delta_\alpha(c)\delta_\alpha(d).$$

Elég azt megnézni, hogy a bal oldal pontosan akkor vesz fel nullát, ha a, b, c, d 4 hosszú számtani sorozatot alkotnak. Ha számtani sorozatot alkotnak, $0 - \gamma 0 = 0$, tehát a bal oldali kifejezés nem vesz föl nullát. Ha pedig nem alkotnak számtani sorozatot, akkor lesz olyan koordináta, ahol $(a_i - 2b_i + c_i)^2 \neq 0$ vagy $\gamma(b_i - 2c_i + d_i)^2 \neq 0$, ekkor ezek különbsége nem lehet nulla, csak ha az egyik kifejezés nem nulla. Ha mindkét kifejezés nem nulla, akkor sem lehet a különbségük nulla, mert az egyik kvadratikus maradék, a másik nem. $\delta_a(x) = \prod_{i=1}^{n}(1-(x_i-a_i)^{q-1})$, tehát a fenti polinomoknak a foka $2(q-1)n$. Ezek $2(q-1)n$ fokú monomokra bomlanak, amikben vannak a, b, c, d beli változók, tehát a fent megadott hipermátrixok rangja legfeljebb $m_{n,2(q-1)n/4} = m_{n,(q-1)n/2} = \frac{q^n}{2}$. Ha létezik olyan polinom ami pontosan akkor vesz fel nem nullát az a, b, c, d változókra, ha ezek egymás után 4 hosszú számtani sorozatot alkotnak, és a változók összfoka kisebb, mint $2n(q-1)$, akkor a 3 hosszú részsorozatot nem tartalmazó esethez hasonlóan tudnánk bevezetni olyan $\lambda < q$ számot amire egy 4 hosszú számtani sorozatot nem tartalmazó halmaz számossága legfeljebb $O(\lambda^n)$. Ilyen polinom azonban nem létezik.

Állítás: Legyen $P : \mathbb{F}_q^{n\times 4} \to \mathbb{F}_q$ olyan, hogy $\forall a, b, c, d \in \mathbb{F}_q^n$ esetén:

$$P(a, b, c, d) \neq 0 \Leftrightarrow a - 2b + c = b - 2c + d = 0.$$

Ekkor $\deg(P) \geq 2(q-1)n$.

Bizonyítás: Feltehetjük, hogy egy ilyen polinomban minden változó foka legfeljebb $q-1$, ha nem így lenne, a $\mathbb{F}_q$ test felett $x^c = x^{c-(q-1)}$, tehát találhatnánk egy kisebb fokú polinomot. Legyen $x := a - 2b + c$ és $y := b - 2c + d$. Ekkor $b = y + 2c - d$ és $a = x + 2y + 3c - 2d$. Legyen $P' : \mathbb{F}_q^{n\times 4} \to \mathbb{F}_q$ olyan, hogy $x, y, c, d \in \mathbb{F}_q^n$-re

$$P'(x, y, c, d) = P(x + 2y + 3c - 2d, y + 2c - d, c, d).$$

Ekkor $\deg(P') = \deg(P)$ és $P'(x, y, c, d)$ pontosan akkor vesz fel nullát, ha $x = 0$ és $y = 0$. Tekintsük a c, d vektorokat konstansnak, ekkor a P' polinomot úgy lehet tekinteni, mint egy $2n$ változós polinomot, ami pontosan akkor nem vesz fel nullát, ha minden változójában nulla. Legyen $f \in \mathbb{F}_q^{2n}$-re

$$P'_f(x, y) := P(x_1 - f_1, \cdots, x_n - f_n, y_1 - f_{n+1}, \cdots, y_n - f_{2n}).$$

Ez a P'_f függvény csak az f pontban vesz fel nem nulla értéket, tehát ilyen P'_f függvények lineáris kombinációjából tetszőleges függvény előállítható. Mivel lineáris kombináció, tetszőleges c_f konstansokra:

$$\deg\left(\sum_{f\in\mathbb{F}_q^n} c_f P'_f\right) \leq \deg(P).$$

Ez alapján minden $\mathbb{F}_q^{2n} \to \mathbb{F}_q$ függvény előállítható egy legfeljebb $\deg(P)$ fokú polinom segítségével. Az $\mathbb{F}_q^{2n} \to \mathbb{F}_q$ alakú függvények száma $q^{q^{2n}}$, ami megegyezik a legfeljebb $2n(q-1)$ összfokú, minden változójukban legfeljebb $q-1$ fokú polinomok számával. Ez azt jelenti, hogy létezik injektív leképezés, a legfeljebb $2n(q-1)$ fokú polinomokból a legfeljebb P' fokú, minden változójukban legfeljebb $q-1$ fokú polinomokba, tehát $\deg(P) \geq 2n(q-1)$.

A következőben megpróbáljuk a 4 hosszú számtani sorozatot nem tartalmazó tulajdonságot leírni hasonló módon, mint ahogy először leírtuk a három hosszú számtani sorozatot nem tartalmazó tulajdonságot.

Állítás: Legyen $A \subset \mathbb{F}_q^n$. Az A halmaz pontosan akkor nem tartalmaz 4 hosszú számtani sorozatot, ha az $\{\binom{a}{a} \mid a \in A\}$ és a $\{\binom{2b-c}{3c-2d} \mid b,c,d \in A, b \neq c, b \neq d, c \neq d\}$ halmazok diszjunktak.

Bizonyítás: Valóban, ha $\binom{a}{a} = \binom{2b-c}{3c-2d}$ valamilyen $a,b,c,d \in A$ elemekre, az ekvivalens azzal, hogy $a = 2b-c = 3c-2d$, ami átrendezve $a-2b+c = b-2c+d = 0$, tehát a,b,c,d 4 hosszú számtani sorozatot alkot.

Itt ismét lehet meg lehet nézni, hogy milyen becslést lehet felírni az Ellenberg-Gijswijt tétel bizonyításának módszerével, de ismét csak a triviálisnál gyengébbet lehet kapni. Legyen $A \subset \mathbb{F}_q^n, P \in \mathrm{span}(M_{2n,d})$ olyan polinom, ami eltűnik az $\{\binom{2b-c}{3c-2d} \mid b,c,d \in A, b \neq c, b \neq d, c \neq d\}$ halmazon. Ekkor az $\{\binom{a}{a} \mid a \in A\}$ halmaznak legfeljebb $3m_{2n,d}$ olyan a eleme van ami $P(a)$ nem vesz fel nullát. Legyen B olyan az A^3 halmazon értelmezett hipermátrix, ahol $B(b,c,d) = P\binom{2b-c}{3c-2d}$. Az eddigi bizonyításokkal analóg módon B rangja legfeljebb $3m_{2n,d/3}$, és csak a főátlón vesz fel nemnulla értéket, tehát legfeljebb $3m_{2n,d/3}$ helyen vesz fel nemnulla értéket.

Most legyen A olyan, ami nem tartalmaz 4 hosszú számtani sorozatot. Ekkor legyen $\mathcal{P}$ azon legfeljebb d fokú n változós polinomok vektortere, amik eltűnnek az $\{\binom{a}{a} \mid a \in A\}$ halmaz komplementerén. Ekkor legyen $p \in \mathcal{P}$ maximális tartójú. p tartója nagyobb vagy egyenlő, mint $\mathcal{P}$ dimenziója és kisebb vagy egyenlő, mint $3m_{2n,d}$. Ez alapján

$$3m_{2n,d/3} \geq m_{2n,d} - (q^n - |A|).$$

Rendezve, és a minimumra hozva $d = \frac{3n(q-1)}{2}$ választással:

$$|A| \leq 4m_{2n,(q-1)n/2}.$$

Mivel $m_{2n,(q-1)n/2} \geq m_{n,(q-1)n/2} = \frac{q^n}{2}$, ezért ez a becslés is a triviálisnál rosszabb eredményt ad.

4. fejezet

$m_{n,d}$ értékének becslése

Azt már a korábbiakban beláttuk, hogy tetszőleges q prímre, n természetes számra, $d \in [(q-1)n]$ egészre pontosan akkor létezik valamilyen $\lambda < q$, amire $m_{n,d} \leq \lambda^n$, ha $d < \frac{(q-1)n}{2}$. Most szeretnénk $m_{n,d}$ értékét pontosabban becsülni.

Először legyen $q = 3$, az [7]-ben bemutatott módszert fogjuk alkalmazni. Itt olyan monomok számát nézzük, amikben minden változó foka 0, 1 vagy 2:

$$m_{n,d} = \#\{x_1^{i_1} \cdots x_n^{i_n}; i_1, \cdots i_n \in \{0,1,2\}, i_1 + \cdots + i_n \leq d\}.$$

Legyen a azon változók száma, amiknek a kitevője egy monomban 0, b amiknek 1, és c amiknek 2. Ekkor pontosan m monom foka kisebb vagy egyenlő, mint d pontosan akkor, ha $b(m) + 2c(m) \leq d$. Az is látható, hogy a_0, b_0, c_0 konstansokra az olyan m monomok száma, amikre $a(m) = a_0$, $b(m) = b_0$, $c(m) = c_0$ igaz, egyenlő a $\frac{(a_0+b_0+c_0)!}{a_0!b_0!c_0!}$ kifejezéssel.

$$m_{n,d} = \sum_{a,b,c \in \mathbb{N}, a+b+c=n, b+2c \leq d} \#\{m \in M_{n,d}; a(m) = a, b(m) = b, c(m) = c\} =$$

$$= \sum_{a,b,c \in \mathbb{N}, a+b+c=n, b+2c \leq d} \frac{n!}{a!b!c!}$$

A fenti kifejezést a Stirling-formulával becsüljük:

$$\frac{n!}{a!b!c!} = \left(\frac{n}{e}\right)^n \left(\frac{e}{a}\right)^a \left(\frac{e}{b}\right)^b \left(\frac{e}{c}\right)^c \sqrt{\frac{2\pi n}{8\pi^3 abc}} \left(1+O\left(\frac{1}{n}\right)\right) \left(1+O\left(\frac{1}{a}\right)\right) \left(1+O\left(\frac{1}{b}\right)\right) \left(1+O\left(\frac{1}{c}\right)\right).$$

Ami egyszerűbben felírva, felhasználva, hogy $a + b + c = n$

$$\frac{n^n}{2\pi a^a b^b c^c} \sqrt{\frac{n}{abc}} \left(1 + O\left(\frac{1}{n} + \frac{1}{a} + \frac{1}{b} + \frac{1}{c}\right)\right).$$

Az exp függvény segítségével kifejezve

$$\frac{1}{2\pi} \exp\left(\left(n+\frac{1}{2}\right)\log(n) - \left(a+\frac{1}{2}\right)\log(a) - \left(b+\frac{1}{2}\right)\log(b) - \left(c+\frac{1}{2}\right)\log(c)\right)\left(1+O\left(\frac{1}{n}+\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right)\right).$$

Most megkeressük a maximumát a

$$(n+1/2)\log(n)-(a+1/2)\log(a)-(b+1/2)\log(b)-(c+1/2)\log(c)$$

függvénynek az $a,b,c \geq 0$, $a+b+c=n$ és $b+2c \leq d$ feltételek mellett. Helyettesítsünk be $\alpha = a/n$, $\beta = b/n$ és $\gamma = c/n$ kifejezésekkel. Ekkor a következő kifejezés maximumát keressük:

$$-\log(n) - n(-\left(\alpha+\frac{1}{2n}\right)\log(\alpha) - \left(\beta+\frac{1}{2n}\right)\log(\beta) - \left(\gamma+\frac{1}{2n}\right)\log(\gamma)$$

Ezt az adott feltételek mellett Lagrange multiplikátor módszerével ki lehet számolni. $d = 2n/3$ értékre behelyettesítve, a következő értékek jönnek ki:

$$\alpha = \frac{32}{3(15+\sqrt{33})}$$

$$\beta = \frac{4(\sqrt{33}-1)}{3(15+\sqrt{33})}$$

$$\gamma = \frac{2(17-\sqrt{33})}{3(15+\sqrt{33})}$$

Ez alapján valamilyen c_0 konstansra:

$$m_{n,2n/3} \leq c_0 n^2 \exp((n+1/2)\log(n)-(a+1/2)\log(a)-(b+1/2)\log(b)-(c+1/2)\log(c)),$$

behelyettesítve pedig elég nagy n-re

$$m_{n,2n/3} = O\left(\frac{\sqrt[3]{5589+891\sqrt{33}}}{8}\right)^n$$

A fenti kifejezés körülbelül $2,756^n$. Nevezzük ezt a konstanst θ-nak.

Ezzel becslést adtunk olyan λ konstansra amelyikre $m_{n,3n/2} = O(\lambda^n)$ A következőkben azt szeretnénk megmutatni, hogy ez a becslés éles.

Lemma Ha α, β, γ tetszőleges valós számok 0 és 1 között melyekre $\alpha+\beta+\gamma = 1$, akkor tetszőleges $\epsilon > 0$ valós számra létezik olyan N egész szám, hogy minden $n > N$ egész számra léteznek a_n, b_n, c_n egészek, hogy $a_n + b_n + c_n = n$ és

$$\max(|a_n - \alpha n|, |b_n - \beta n|, |c_n - \gamma n|) < \epsilon n.$$

Bizonyítás Legyen $N := 2\lfloor \epsilon^{-1} \rfloor + 1$, ekkor tetszőleges $n > N$ egészre $n^{-1} < \epsilon$, tehát $\frac{k+1}{n} - \frac{k}{n} < \epsilon$. Ekkor α és β értékekre léteznek a_n és $a_n + b_n$ egészek, hogy $\frac{a_n}{n} \leq \alpha \leq \frac{a_n+1}{n}$ és $\frac{b_n}{n} \leq \beta \leq \frac{b_n+1}{n}$. Ebből a két egyenlőtlenségből rendre $\frac{a_n}{n}$ és $\frac{b_n}{n}$ értékeket kivonva megkapjuk, hogy $0 \leq \alpha - \frac{a_n}{n} \leq \frac{\epsilon}{2}$ és $0 \leq \beta - \frac{b_n}{n} \leq \frac{\epsilon}{2}$. A lemma feltételét átírhatjuk olyan módon, hogy $\gamma = 1 - \alpha - \beta$ és az előzőekből $|(1 - \alpha - \beta) - (1 - a_n/n - b_n/n)| \leq |\alpha - a_n/n| + |\beta - b_n/n| < \epsilon/2 + \epsilon/2 = \epsilon$, tehát $c_n := n - a_n - b_n$ választással a lemma teljesül.

A következőkben fixáljunk le egy $\epsilon > 0$ konstanst. Megmutatjuk, hogy elég nagy n egészre $m_{n,d} > (\theta - \epsilon)^n$. Legyenek α, β, γ az előzőekben a Langrange multiplikátor módszerrel kiszámolt konstansok. Ekkor, mint azt az előző lemmában láttuk, az α, β, γ értékeket jól tudjuk közelíteni megfelelő racionálisakkal, melyeknek n a nevezője. Az előző állítás bizonyításánál láttuk, hogy

$$m_{n,d} = \sum_{a,b,c \in \mathbb{N}, a+b+c=n, b+2c \leq 2n/3} \frac{n!}{a!b!c!}.$$

Ekkor a jobboldali összeget a következő módon becsülhetjük:

$$\sum_{a,b,c \in \mathbb{N}, a+b+c=n, b+2c \leq 2n/3} \frac{n!}{a!b!c!} > \frac{n!}{a_n!b_n!c_n!}$$

a megfelelő a_n, b_n, c_n értékekre. Ezt a kifejezést ismét a Stirling formulával lehet becsülni.

$$\frac{n^n}{2\pi {a_n}^{a_n} {b_n}^{b_n} {c_n}^{c_n}} \sqrt{\frac{n}{a_n b_n c_n}} \left(1 + O\left(\frac{1}{n} + \frac{1}{a_n} + \frac{1}{b_n} + \frac{1}{c_n}\right)\right)$$

Létezik olyan $\delta > 0$ konstans, hogy fenti kifejezés kisebb, mint

$$\delta \exp((n + 1/2)\log(n) - (a_n + 1/2)\log(a_n) - (b + 1/2)\log(b_n) - (c + 1/2)\log(c_n)).$$

Most felhasználjuk, hogy $n = a_n + b_n + c_n$ és átalakítjuk a köveztkező képletet úgy, hogy n-edik hatvány legyen. Az előző kifejezés nagyobb, vagy egyenlő, mint

$$\left(\sqrt[n]{\delta n^{-1}} \exp\left(-\left(\frac{a_n}{n}+\frac{1}{2n}\right)\log\left(\frac{a_n}{n}\right)-\left(\frac{b_n}{n}+\frac{1}{2n}\right)\log\left(\frac{b_n}{n}\right)-\left(\frac{c_n}{n}+\frac{1}{2n}\right)\log\left(\frac{c_n}{n}\right)\right)\right)^n.$$

Ha a_n, b_n és c_n olyanok, hogy $\max(|a_n/n - \alpha|, |b_n/n - \beta|, |c_n/n - \gamma|) < \eta$ megfelelő η pozitív valósra, akkor

$$\exp(\eta(\log(a_n/n) + \log(b_n/n) + \log(c_n/n))) \leq ((\alpha - \eta)(\beta - \eta)(\gamma - \eta))^\eta \leq (\alpha/2)^{3\eta}$$

a fenti kifejezés tovább becsülhető alulról a

$$\left(\sqrt[n]{\delta n^{-1}} \exp\left(-\left(\alpha+\frac{1}{2n}\right)\log\left(\frac{a_n}{n}\right)-\left(\beta+\frac{1}{2n}\right)\log\left(\frac{b_n}{n}\right)-\left(\gamma+\frac{1}{2n}\right)\log\left(\frac{c_n}{n}\right)\right)\left(\frac{\alpha}{2}\right)^\eta\right)^n$$

kifejezéssel. Ehhez még a $\log(a_n/n) \geq \log(\alpha-\eta) \geq \log(\alpha)+\frac{2\eta}{\alpha}$ egyenlőtlenség segítségével

$$\exp\Bigg(-\left(\alpha+\frac{1}{2n}\right)\log\left(\frac{a_n}{n}\right)\Bigg) \leq \exp\Bigg(-\left(\alpha+\frac{1}{2n}\right)\log(\alpha)\Bigg)\Bigg(\exp\Bigg(-\frac{1}{2}-\frac{1}{2n\alpha}\Bigg)\Bigg)^{\eta}.$$

Ez alapján, az eddigi egyenlőtlenségek felhasználásával valamilyen ζ pozitív valós értékre:

$$m_{n,2n/3} \leq \sqrt[n]{\delta n^{-1}}\zeta^{\eta n}\theta^n.$$

Itt a korábban lefixált ϵ értékhez létezik olyan η, hogy $\zeta^\eta\theta > \theta - \epsilon$. Ezen kívül $\lim_{n\to\infty}\sqrt[n]{dn^{-1}} = 1$, tehát ha n elég nagy, akkor

$$m_{n,2n/3} > (\theta-\epsilon)^n.$$

Látható, hogy ha $2n/3$ helyett más d értéket nézünk, az $m_{n,d}$ értékének a Lagrange multiplikátor módszerrel való becslésének, és ezen becslés lényegében vett élességének bizonyításának elvén nem változtat. Most nézzük, mi van akkor, ha q nem 3. Ebben az esetben olyan monomokat keresünk, amelyekben minden változó foka a $0,\cdots,q-1$ halmaz valamelyik eleme. Ha n változónk van, akkor az $\{1,\cdots,n\}$ halmaz olyan $I_0,\cdots,I_{q-1}$ particionálásait kell nézni, ahol $\sum_{i=0}^{q-1} i|I_i| \leq d$. Ez alapján

$$m_{n,d} = \sum_{i_0,\cdots,i_{q-1}\in\mathbb{N};i_0+\cdots i_{q-1}=n;1i_1+\cdots+(q-1)i_{q-1}\leq d} \frac{n!}{i_0!\cdots i_{q-1}!}.$$

Ha itt a Stirling formulát használnánk, akkor ismét kaphatnánk egy a Lagrange multiplikátor módszerrel megoldható rendszert. Más módszerrel [2] -ben a $d=(q-1)n/3$ esetre $m_{n,d}$ meg van adva a $q=3,\cdots,31$ esetekre.

5. fejezet

Az Abel-csoportok esete

Most legyen G tetszőleges Abel - csoport, ekkor G részhalmazain a vektorterekhez hasonló módon tudjuk értelmezni a 3 hosszú számtani sorozatot nem tartalmazó részhalmazokat. Az $A \subset G$ halmaz nem tartalmaz 3 hosszú számtani sorozatot, ha az $a-b=c-b$ egyenletnek az A halmazon csak $a=b=c$ alakú megoldásai vannak. A következőkben Abel-csoportok 3 hosszú számtani sorozatot nem tartalmazó részhalmazainak méretét fogjuk becsülni. [8]-ból származik a következő tétel:

Tétel Legyen G véges Abel-csoport, $G \simeq Z_{k_1} \times \cdots \times Z_{k_n}$, semelyik k_i nem osztható kettővel, A pedig a G csoport egy 3 hosszú számtani sorozatot nem tartalmazó részhalmaza. Ekkor:

$$|A| \leq \frac{2|G|}{n}.$$

A bizonyításban diszkrét Fourier transzformációt fogunk alkalmazni, úgyhogy felírjuk annak alapfogalmait, és jelöléseit. Legyen $\hat{G}$ a G karaktercsoportja. Ha $f : G \to \mathbb{C}$, akkor legyen $\hat{f} : \hat{G} \to \mathbb{C}$, ahol minden $\chi \in \hat{G}$ elemre

$$\hat{f}(\chi) := \sum_{x \in G} f(x)\chi(-x),$$

ahol $\hat{f}$ az f függvény Fourier-transzformáltja. Ha $f, g : G \to \mathbb{C}$, akkor jelöljük f és g konvolúcióját $f * g$ módon.

$$f * g(x) := \sum_{y \in G} f(y)g(x-y).$$

Jelöljük az f függvény k-adik, önmagával vett konvolúcióját f^{*k} segítségével. Ezen kívül még bevezetünk néhány fogalmat. Ha $H \leq G$ akkor legyen $H^{\perp} \leq \hat{G}$, ahol

$$H^{\perp} := \{\chi \in \hat{G} \mid \forall x \in H; \chi(x) = 1\}.$$

A karaktercsoport egységelemét jelöljük χ_0 -lal. Ha $S \subseteq G$, akkor legyen $1_S : G \to \mathbb{C}$ az S halmaz karakterisztikus függvénye: $1_S(x) = 1$ ha $x \in S$ és 0 egyébként.

Lemma Legyen $A \subset G$ egy 3 hosszú számtani sorozatot nem tartalmazó részhalmaz. Ekkor
$$1_A^{*2} * 1_{-2A}(0) = |A|.$$

Bizonyítás Némi átírással:
$$1_A^{*2} * 1_{-2A}(0) = \sum_{x\in G} 1_A^{*2}(x) 1_{-2A}(-x) = \sum_{x\in G} \left(\sum_{y\in G} 1_A(y) 1_A(x-y) \right) 1_{-2A}(-x).$$
A $1_{-2A}(-x)$ pontosan akkor vesz fel 1 értéket, ha létezik $z \in A$, hogy $2z = x$. Tehát $1_A(y)1_A(x-y)1_{-2A}(-x) = 1$ pontosan akkor igaz, ha $y \in A$ és létezik $z \in A$ hogy $2z-y$, $z \in A$. Ha $z \neq y$, akkor az $y, z, 2z-y$ hármas 3 hosszú számtani sorozatot alkot, tehát az előző feltétel csak akkor teljesülhet, ha $y = z$. Ez alapján a fenti összegben csak az A halmaz elemeit számláljuk le, ezzel a lemmát beláttuk.

Most legyen $f := \widehat{1_A}$ és $g := \widehat{1_{-2A}}$.

Lemma
$$\sum_{\chi\in\hat{G}} (f(\chi))^2 g(\chi) = |G||A|.$$
Itt, ha kihasználjuk, hogy a konvolúció Fourier-transzformáltja a Fourier-transzformáltak szorzata:
$$\sum_{\chi\in\hat{G}} (f(\chi))^2 g(\chi) = \sum_{\chi\in\hat{G}} \widehat{1_A^{*2}}(\chi) g(\chi) = \sum_{\chi\in\hat{G}} \widehat{1_A^{*2} * 1_{-2A}}(\chi) = |G||A|$$
Tetszőleges H véges Abel-csoport felírható, mint pímhatványrendű ciklikus csoportok direkt szorzata. Legyen minden véges H Abel-csoportra $c(H)$ az a szám, hogy hány prímhatványrendű ciklikus szorzata izomorf a H csoporttal, $D(H)$ pedig legyen a H legnagyobb 3 hosszú számtani sorozatot nem tartalmazó részhalmazának számossága. Legyen $d : \mathbb{N} \to \mathbb{R}$,
$$d(n) := \sup\{D(H)/|H| \colon c(H) \geq n\}.$$
Mivel tetszőleges H véges páratlan rendű Abel-csoportra $D(H) \leq |H|$, az előző definíció értelmes és minden n számra korlátos. Az is látszik, hogy $d(n)$ monoton csökken. Azt szeretnénk belátni, hogy $d(n) \leq \frac{2}{n}$. Ezt indukcióval szeretnénk elérni. $n = 1, 2$-re az állítás triviális. Tegyük fel, hogy minden n -nél kisebb egész számra már sikerült bizonyítanunk az állítást. Most legyen $h : \hat{G} \to \mathbb{C}$, ahol $h(\chi) = d(n-1)|G|$ ha $\chi = \chi_0$, és 0 egyébként. Ekkor igaz, hogy:
$$\sum_{\chi\in\hat{G}} (f(\chi))^2 h(\chi) = (f(\chi_0))^2 h(\chi_0) = |G||A|^2 d(n-1).$$
Most bevezetünk még egy függvényt. Legyen $u : G \to \mathbb{C}$, ahol
$$u(x) = d(n-1) - 1_{-2A}(x).$$
Ekkor $\hat{u}(\chi) = h(\chi) - g(\chi)$.

Lemma

$$\max_{\chi\in\hat{G}}(|\hat{u}(\chi)|) = d(n-1)|G| - |A|$$

Bizonyítás Legyen $\chi \in \hat{G}$ tetszőleges. Ekkor $\ker(\chi)$ a G csoport egy részcsoportja, jelöljük H_χ -vel, és mivel χ irreducibilis karakter, ezért $c(H_\chi) \geq n-1$. Ha $x \in G$ tetszőleges, akkor a $H_\chi \cap (\{x\}+2A)$ halmaz nem tartalmaz 3 hosszú számtani sorozatot. Valóban, ha, a G csoportot alkotó ciklikusok rendje között nincs kettőhatvány, akkor $a, b, c \in G$ elemekre $2b-2a = 2c-2b$, akkor $b-a = c-b$. Az szintén látszik, hogy a 3 hosszú részsorozatot nem tartalmazó tulajdonság transzlációinvariáns. Ez alapján

$$|H_\chi \cap (\{x\}+2A)| \leq |H_\chi| c(\chi) \leq |H_\chi| d(n-1).$$

Mivel az egyik halmaz a másik eltoltja, ezért

$$|H_\chi \cap (\{x\}+2A)| = |(-2A) \cap (\{x\}-H_\chi)|.$$

Ezt felhasználva:

$$1_{H_\chi} * u(x) = \sum_{z\in H_\chi} u(x-z) = |H_\chi| d(n-1) - |(-2A) \cap (\{x\}-H_\chi)| \geq 0.$$

A Fourier-transzformációt nézve:

$$|H_\chi||\hat{u}(\chi)| = \widehat{1_{H_\chi} * u}(\chi) = \left|\sum_{x\in G} 1_{H_\chi} * u(x)\chi(-x)\right| \leq \sum_{x\in G} 1_{H_\chi} * u(x).$$

$$\sum_{x\in G} 1_{H_\chi} * u(x) = |H_\chi||G| d(n-1) - \sum_{x\in G} |(-2A) \cap (\{x\}-H_\chi)| =$$

És mivel minden $a \in -2A$ és $z \in H_\chi$ elemhez létezik pontosan egy $x \in G$, hogy $a = x - w$

$$= |H_\chi||G| d(n-1) - |H_\chi||A|$$

Ha most megnézzük az egyenlőtlenség elejét és végét, és leosztunk a $|H_\chi|$ számmal:

$$|\hat{u}(\chi)| \leq |G| d(n-1) - |A|.$$

A másik oldalról pedig létezik olyan $\chi \in \hat{G}$, amire az egyenlőtlenség éles, mert a χ_0 triviális karakterre:

$$|\hat{u}(\chi_0)| = h(\chi_0) - g(\chi_0) = |G| d(n-1) - |A|.$$

Ezzel a lemmát beláttuk.

Lemma

$$|d(n-1)|A| - 1| \leq d(n-1)|G| - |A|$$

Bizonyítás A korábban belátott

$$\sum_{\chi\in\hat{G}}(f(\chi))^2 g(\chi)=|G||A|$$

és

$$\sum_{\chi\in\hat{G}}(f(\chi))^2 h(\chi)=|G||A|^2 d(n-1)$$

egyenlőségek segítségével:

$$|A||G|(|d(n-1)|A|-1|)=\left|\sum_{\chi\in\hat{G}}((f(\chi))^2 h(\chi)-g(\chi))\right|=$$

$$=\sum_{\chi\in\hat{G}}(f(\chi))^2\hat{u}(\chi)\leq\sum_{\chi\in\hat{G}}(f(\chi))^2\max_{\chi\in\hat{G}}\hat{u}(\chi).$$

Az imént belátott lemmát behelyettesítve:

$$\sum_{\chi\in\hat{G}}|f(\chi)|^2\max_{\chi\in\hat{G}}\hat{u}(\chi)=\sum_{\chi\in\hat{G}}|f(\chi)|^2(d(n-1)|G|-|A|)$$

A Parseval-egyenlőtlenséget felhasználva

$$\sum_{\chi\in\hat{G}}|f(\chi)|^2(d(n-1)|G|-|A|)\leq\sum_{x\in G}|1_A(x)|^2(d(n-1)|G|-|A|)=$$

$$=|G||A|(d(n-1)|G|-|A|).$$

Az egyenlőtlenség elejét és végét tekintve megkapjuk a kívánt egyenlőtlenséget. Ezzel a lemmát beláttuk.

Most nézzük meg, hogy az $\frac{|A|}{|G|}$ kifejezés értékét hogyan tudjuk becsülni az előző lemmával. Az előző egyenlőtlenséget rendezve:

$$|A|\leq\frac{1+d(n-1)|G|}{d(n-1)+1}.$$

Amiből, ha leosztunk a $|G|$ értékkel, becslést kapunk. Tudjuk, hogy $|G|$ pontosan n darab páratlan prímhatvány szorzata, így $|G|\geq 3^n$. Ennek, és az indukciós feltevésnek a segítségével:

$$\frac{|A|}{|G|}\leq\frac{|G|^{-1}+d(n-1)}{d(n-1)+1}\leq\frac{3^{-n}+d(n-1)}{d(n-1)+1}\leq\frac{3^{-n}+2/(n-1)}{2/(n-1)+1}\leq\frac{2}{n}.$$

Mivel ez minden megfelelő G csoportra igaz, ezért ezzel az indukció következő lépését, és így a tételt is beláttuk.

6. fejezet

Az általánosított rang és a tenzor rang kapcsolata, függvények instabilitása

Legyen k egy tetszőleges páratlan természetes szám, ekkor az n darab k rendű ciklikus csoport direkt szorzataként előálló Abel-csoport 3 hosszú számtani sorozatot nem tartalmazó részhalmazainak elemszámának becsléséhez szeretnénk adni az Ellenberg-Gijswijt tételben megfogalmazotthoz hasonló korlátot. Ehhez elsősorban a [2] munka definícióit és állításait fogjuk használni. Szükségünk lesz néhány új fogalom bevezetésére. Legyenek X, Y, Z véges halmazok, $\mathbb{F}$ pedig valamilyen test. Az $F : X \times Y \times Z \to \mathbb{F}$ függvények vektorterén vezessük be a tenzor rangot a következőképpen: legyenek a 1 tenzorragú függvények azon nem azonosan nulla F_i függvények, amikre léteznek olyan $f_i : X \to \mathbb{F}, g_i : Y \to \mathbb{F}, h_i : Z \to \mathbb{F}$, hogy tetszőleges $(x, y, z) \in X \times Y \times Z$ elemre

$$F_i(x, y, z) = f_i(x)g_i(y)h_i(z)$$

Egy F függvény tenzor rangja pontosan akkor k, ha előáll k darab 1 tenzorrangú függvény összegeként, és nem áll elő k -nál kevesebb 1 rangú függvény összegeként. Végül az azonosan 0 függvény tenzorrangja legyen nulla. Jelöljük a tenzor rangot a trank kifejezéssel, míg a rank jelölje az általánosított rangot.

Állítás Legyenek X, Y, Z véges halmazok $\mathbb{F}$ valamilyen test, $F : X \times Y \times Z \to \mathbb{F}$, akkor

$$\operatorname{rank}(F) \max(|X|, |Y|, |Z|) \geq \operatorname{trank}(F) \geq \operatorname{rank}(F).$$

Bizonyítás Ha $\operatorname{trank}(F) = k$ és $F(x, y, z) = \sum_{i=1}^{k} f_i(x)g_i(y)h_i(z)$ egy felírás 1 tenzor rangú függvények összegeként, akkor legyen $l_i : Y \times Z \to \mathbb{F}$, ahol $l_i(y, z) := g_i(y)h_i(z)$. Ekkor $F(x, y, z) = \sum_{i=1}^{k} f_i(x)l_i(y, z)$, tehát $\operatorname{rank}(F) \leq k$. A másik oldalról egy 1 általánosított rangú függvényben a 2 változós tagot el tudjuk képzelni, mint egy legfeljebb $\max(|X|, |Y|, |Z|)$ rangú mátrixot. Ekkor, ha minden ilyen 2 változós függvényt felírunk mint legfeljebb $\max(|X|,|Y|,|Z|)$ 1 rangú mátrix összege, megkapjuk a kívánt egyenlőtlenséget. Legyen F általánosított rangja k, ekkor létezik olyan $k_1, k_2, k_3 \in \mathbb{N}$, $k_1 + k_2 + k_3 = k$, hogy

$$F(x,y,z) = \sum_{i=1}^{k_1} f_i(x) g_i(y,z) + \sum_{j=1}^{k_2} f_{k_1+j}(y) g_{k_1+j}(x,z) + \sum_{l=1}^{k_3} f_{k_1+k_2+l}(z) g_{k_1+k_2+l}(x,y).$$

Itt minden f_i -t átírva a megfelelő 1 rangúak összegére készen vagyunk.

A következőkben legyenek X', Y', Z' és X'', Y'', Z'' véges halmazok, legyen $\mathbb{F}$ valamilyen test, $F : X' \times Y' \times Z' \to \mathbb{F}$ és $G : X'' \times Y'' \times Z'' \to \mathbb{F}$ függvények, legyen $X = X' \times X'', Y = Y' \times Y'', Z = Z' \times Z''$ és legyen $H : X \times Y \times Z \to \mathbb{F}$ olyan, hogy minden $((x', x''), (y', y''), (z', z'')) \in X \times Y \times Z$ elemre

$$H((x', x''), (y', y''), (z', z'')) := F(x', y', z') G(x'', y'', z'').$$

A következőkben ezen H függvény rangjával kapcsolatos egyenlőtlenségekkel fogunk foglalkozni. Először nézzük meg H tenzor rangja hogy függ F és G tenzor rangjától.

Állítás

$$\operatorname{trank}(H) \leq \operatorname{trank}(F) \operatorname{trank}(G)$$

Bizonyítás Legyen $\operatorname{trank}(F) = k$ és $\operatorname{trank}(G) = l$, ekkor ha tetszőleges $(x', y', z') \in X' \times Y' \times Z'$ és $(x'', y'', z'') \in X'' \times Y'' \times Z''$ elemekre

$$F(x', y', z') = \sum_{i=1}^{k} f_i'(x') g_i'(y') h_i'(z')$$

és

$$G(x'', y'', z'') = \sum_{j=1}^{l} f_j''(x'') g_j''(y'') h_j''(z''),$$

akkor

$$H((x', x''), (y', y''), (z', z'')) = \sum_{i=1}^{k} \sum_{j=1}^{l} f_i'(x') g_i'(y') h_i'(z') f_j''(x'') g_j''(y'') h_j''(z'')$$

Legyen $(i,j) \in [k] \times [l]$ párra $f_{ij}(x', x'') := f_i'(x') f_j''(x'')$ illetve g_{ij}, h_{ij} hasonló módon definiálva, ekkor

$$H((x', x''), (y', y''), (z', z'')) = \sum_{(i \in [k], j \in [l]} f_{ij}(x', x'') g_{ij}(y', y'') h_{ij}(z', z'')$$

ebből látszik, hogy a fenti egyenlőtlenség igaz.

Állítás Legyen H a fentebb definiált függvény, ekkor

$$\operatorname{rank}(H) \leq \operatorname{rank}(F) \operatorname{trank}(G)$$

és

$$\operatorname{rank}(H) \leq \operatorname{rank}(F) \max(|X''|, |Y''|, |Z''|).$$

Bizonyítás Legyen $\operatorname{rank}(F) = k, \operatorname{trank}(G) = l$. Legyenek $k_1, k_2, k_3 \in \mathbb{N}$,$k_1 + k_2 + k_3 = k$ olyanok, hogy a megfelelő f'_i, g'_i függvényekre:

$$F(x', y', z') = \sum_{i_1=1}^{k_1} f'_{i_1}(x')g'_{i_1}(y', z') + \sum_{i_2=1}^{k_2} f'_{i_2+k_1}(y')g'_{i_2+k_1}(x', z') + \sum_{i_3=1}^{k_3} f'_{i_3+k_1+k_2}(z')g'_{i_3+k_1+k_2}(x', y').$$

A G függvényt pedig írjuk fel a megfelelő $\alpha_i, \beta_i, \gamma_i$, függvényekkel ahol $i \in [l]$

$$G(x'', y'', z'') = \sum_{i=1}^{l} \alpha_i(x'')\beta_i(y'')\gamma_i(z'').$$

Legyen $x := (x', x''), y := (y', y''), z = (z', z'')$ és $i_1 \in [k_1]$, $i_2 \in \{k_1\} + [k_2]$, $i_3 \in \{k_1 + k_2\} + [k_3]$, $j \in [l]$. Ekkor vezessük be a következő függvényeket:

$$f_{i_1,j}(x, y) := f'_{i_1}(x', y')\alpha_j(x'')\beta_j(y'') \quad g_{i_1,j}(z) := g'_{i_1}(z')\gamma_j(z'')$$

$$f_{i_2,j}(x, z) := f'_{i_2}(x', z')\alpha_j(x'')\gamma_j(z'') \quad g_{i_2,j}(y) := g'_{i_2}(y')\beta_j(y'')$$

$$f_{i_3,j}(y, z) := f'_{i_3}(y', z')\beta_j(y'')\gamma_j(z'') \quad g_{i_1,j}(z) := g'_{i_3}(x')\alpha_j(x'').$$

Ekkor az újonnan definiált függvényekkel felírva a H függvényt

$$H(x, y, z) = \sum_{i_1 \in [k_1], j \in [l]} f_{i_1,j}(x, y)g_{i_1,j}(z) + \sum_{i_2 \in \{k_1\}+[k_2], j \in [l]} f_{i_2,j}(x, z)g_{i_2,j}(y) + (y, z)g_{i_1,j}(z) +$$

$$+ \sum_{i_3 \in \{k_1+k_2\}+[k_3], j \in [l]} f_{i_3,j}.$$

Ezzel a H függvényt felírtuk, mint kl megfelelő függvény összegét: ezzel az állítás első felét beláttuk. A második részhez legyen tetszőleges $\zeta \in X'', \psi \in Y'', \xi \in Z''$ elemekre és $i_1 \in [k_1]$, $i_2 \in \{k_1\} + [k_2]$, $i_3 \in \{k_1 + k_2\} + [k_3]$, $j \in [l]$ számokra legyen

$$f_{i_1\xi}(x, y) := f'_{i_1}(x', y')G(x'', y'', \xi) \quad g_{i_1\xi}(z) = g'_{i_1}(z')\delta_\xi(z'')$$

$$f_{i_2\psi}(x, z) := f'_{i_2}(x', z')G(x'', z'', \psi) \quad g_{i\psi}(y) = g'_{i_2}(y')\delta_\psi(y'')$$

$$f_{i_3\zeta}(y, z) := f'_{i_3}(y', z')G(y'', z'', \zeta) \quad g_{i_3\zeta}(z) = g'_{i_3}(x')\delta_\zeta(x''),$$

ahol δ a Kronecker-delta. Ezek a függvények segítségével H felírható a következő módon:

$$H(x, y, z) = \sum_{i_1 \in [k_1], \xi \in Z''} f_{i_1,\xi}(x, y)g_{i_1,\xi}(z) + \sum_{i_2 \in \{k_1\}+[k_2], \psi \in Y''} f_{i_2\psi}(x, z)g_{i\psi}(y) +$$

$$+ \sum_{i_3 \in \{k_1+k_2\}+[k_3], \zeta \in X''} f_{i_3\zeta}(y,z) g_{i_3\zeta}(z)$$

A jobb oldalon függvények száma

$$k_1|Z''|+k_2|Y''|+k_3|X''| \leq (k_1+k_2+k_3)\max(|X''|,|Y''|,|Z''|) = k\max(|X''|,|Y''|,|Z''|),$$

ezzel az állítás második felét is beláttuk.

A következőkben bevezetjük az $F : X \times Y \times Z \to \mathbb{F}$ függvényeken az instabilitás fogalmát. Ez algebrailaig zárt testekben hasonló fogalom, mint az invariánselméletben használt instabilitás [9], de most nem algebrailag zárt testekkel fogunk foglalkozni.

Definíció Legyenek X, Y, Z véges halmazok, $\mathbb{F}$ valamilyen test. Az $F : X \times Y \times Z \to \mathbb{F}$ függvényt instabilnak mondjuk, ha léteznek az $X \to \mathbb{F}$, $Y \to \mathbb{F}$, $Z \to \mathbb{F}$ függvényeknek olyan f_a, g_b, h_c bázisai A, B, C indexhalmazzal, aminek az elemeire létezik olyan $u_a, v_b, w_c \in \mathbb{R}$ súlyozás, $r_{a,b,c} \in \mathbb{F}$ együtthatók, hogy

$$F(x,y,z) = \sum_{u_a+v_b+w_c<\bar{u}+\bar{v}+\bar{w}} r_{a,b,c} f_a(x) g_b(y) h_c(z)$$

igaz minden x, y, z elemre, ahol $\bar{u}, \bar{v}, \bar{w}$ a megfelelő indexek számtani közepei. Legyen u_{max} az u_a elemek közül a legnagyobb, u_{min} pedig a legkisebb, illetve v_b, w_c súlyoknál ugyanígy értelmezzük. Legyen ε a szuprémuma minden olyan ϵ elemének amire

$$R_\epsilon := \bar{u} + \bar{v} + \bar{w} - \epsilon(u_{max} - u_{min} + v_{max} - v_{min} + w_{max} - w_{min})$$

esetén megfelelő f_a, g_b, h_c függvényekkel és súlyozással

$$F(x,y,z) = \sum_{u_a+v_b+w_c<R_\epsilon} r_{a,b,c} f_a(x) g_b(y) h_c(z).$$

Ezt a ε számot nevezzük az F függvény instabilitásának.

Látható, hogy egy függvény instabilitása pontosan akkor pozitív, hogyha a függvény instabil. Ha minden u_a súlyból levonjuk u_{min} értékét, akkor ismét egy olyan súlyozást kapunk, ami teljesíti a feltételeket, tehát feltehető, hogy $u_{min} = 0$ és ezzel bizonyos esetekben a képlet egyszerűbbé tehető. A következőkben az általánosított rang és az instabilitás kapcsolatával fogunk foglalkozni.

Tétel Legyenek X, Y, Z véges halmazok, $\mathbb{F}$ valamilyen test, $F : X \times Y \times Z \to \mathbb{F}$. Ha

$$\mathrm{rank}(F) < \min(|X|, |Y|, |Z|)$$

akkor F instabil.

Bizonyítás Legyen $(x, y, z) \in X \times Y \times Z$ tetszőleges, ekkor legyen

$$F(x,y,z) = \sum_{i_1=1}^{p} f_{i_1}(x)\alpha_{i_1}(y,z) + \sum_{i_2=1}^{q} g_{i_2}(y)\beta_{i_2}(x,z) + \sum_{i_3=1}^{r} h_{i_3}(z)\gamma_{i_2}(x,y),$$

ahol $p + q + r = \mathrm{rank}(F) < \min(|X|, |Y|, |Z|)$. Ekkor az $f_{i_1} : X \to \mathbb{F}$ függvények linárisan függetlenek, különben lenne egy kevesebb függvénnyel való felbontás. Ennek következményeképp az f_{i_1} függvények kiegészíthetőek bázissá az $X \to \mathbb{F}$ függvények között. Hasonló módon az f_{i_2}, f_{i_3} függvények is kiegészíthetőek bázissá. Az $X \to \mathbb{F}$ függvények így kapott bázisának elemeit sorbarendezzük úgy, hogy az első p elemet használtuk fel F megkonstruálásához. Ekkor vezessük be a következő súlyozást:

$$u_i := -\chi_{1 \geq i \geq p} \quad v_i := -\chi_{1 \geq i \geq p} \quad w_i := -\chi_{1 \geq i \geq r}.$$

Minden $\alpha_i(y, z)$ függvényt fel lehet írni, mint $g_{i_2}(y), f_{i_3}(z)$ függvények szorzatainak lineáris kombinációja. Ha F előző felírásában minden egyes kétváltozós függvényt felírunk, mint egyváltozós függvények szorzatának lineáris kombinációja, akkor csak olyan $f_{i_1}, g_{i_2}, h_{i_3}$ függvények szorzatainak lineáris kombinációját kapjuk amiknek a súlyozásainak összege legfeljebb -1. Másrészt

$$\bar{u} + \bar{v} + \bar{w} = -\frac{p}{|X|} - \frac{q}{|Y|} - \frac{r}{|Z|} \geq \frac{-p-q-r}{\min(|X|, |Y|, |Z|)} > -1$$

Tehát előállítottunk egy a feltételnek megfelelő súlyozást, és ezzel a tételt beláttuk.

Mivel $\mathrm{rank}(F) \leq \min(|X|, |Y|, |Z|)$, ezért a tételt úgy is meg lehet fogalmazni hogy, ha F instabil, akkor $\mathrm{rank}(F) = \min(|X|, |Y|, |Z|)$, de erre nem lesz szükségünk. Most legyen $X = Y = Z$. Korábban a rang általánosításánál már láttuk, hogy ha F csak a főátlón vesz fel nem nulla elemeket, akkor $\mathrm{rank}(F) = \#\{x \in X \mid F(x, x, x) \neq 0\}$. Ennek segítségével általánosítani tudjuk egy korábbi állításunkat.

Lemma Legyen H egy páratlan rendű Abel-csoport, $F : H \times H \times H \to \mathbb{F}$ olyan, hogy $F(x, y, z) = \chi_{x-2y+z=0}$, ekkor ha A a H egy 3 hosszú számtani sorozatot nem tartalmazó részhalmaza, akkor

$$|A| \leq \mathrm{rank}(F).$$

A bizonyítás ugyanaz, mint testek esetében: A pontosan akkor nem tartalmaz 3 hosszú számtani sorozatot, ha az F az A^3 halmazon csak a főátlón vesz fel nemnulla elemet. Ha pedig csak a főátlón vesz fel nemnulla elemet, akkor A elemszáma ez eddigiek alapján legfeljebb $\mathrm{rank}(F)$.

Tétel Legyenek X, Y, Z véges halmazok, $\mathbb{F}$ valamilyen test, $F : X \times Y \times Z \to \mathbb{F}$. Legyen $F^n : (X \times Y \times Z)^n \to \mathbb{F}^n$, ahol

$$F^n((x_1, y_1, z_1), \cdots, (x_n, y_n, z_n)) := F(x_1, y_1, z_1) \cdots F(x_n, y_n, z_n).$$

Legyen F instabil és legyen az instabilitása ε, ekkor

$$\mathrm{rank}(F^n) \leq (|X|^n + |Y|^n + |Z|^n) \exp(-2\varepsilon^2 n).$$

Bizonyítás Legyen $\epsilon < \varepsilon$ tetszőleges. Ekkor létezik olyan súlyozás és felbontása az F függvénynek, amiben az R_ϵ számmal becsülhető összsúlyú függvények vannak:

$$F(x,y,z) = \sum_{u_a+v_b+w_c<R_\epsilon} r_{a,b,c} f_a(x) g_b(y) h_c(z).$$

Feltehetjük, hogy $u_{min} = v_{min} = w_{min} = 0$. Ekkor legyen $u_0 := \bar{u} - \epsilon u_{max}$ illetve v_0, w_0 hasonló módon definiálva. Ekkor

$$R_\epsilon = u_0 + v_0 + w_0.$$

A súlyozásnál használt indexhalmazok legyenek ismét A, B, C. Ekkor tekintsük a következő függvényt: $I : A^n \times B^n \times C^n \to \{0,1\}$ ahol

$$I((a_1, \cdots, a_n)(b_1, \cdots, b_n)(c_1, \cdots, c_n)) = 1$$

pontosan akkor, ha $u_{a_i} + v_{b_i} + w_{c_i} \leq u_0 + v_0 + w_0$ minden $i \in \{1, \cdots, n\}$-re. Ekkor F^n felírható a következő módon: tetszőleges $(\underline{x}, \underline{y}, \underline{z}) \in X^n \times Y^n \times Z^n$ elemre

$$F^n(\underline{x}, \underline{y}, \underline{z}) = \sum_{(\underline{a},\underline{b},\underline{c}) \in A\times B\times C, I(\underline{a},\underline{b},\underline{c})=1} \prod_{i=1}^n r_{a_i,b_i,c_i} f_{a_i}(x_i) g_{b_i}(y_i) h_{c_i}(z_i).$$

Most az eredeti Ellenberg-Gijswijt tétel bizonyításához hasonló eljárást fogunk alkalmazni. Ha egy $(\underline{a}, \underline{b}, \underline{c})$ hármasra $I(\underline{a}, \underline{b}, \underline{c}) = 1$, akkor igaz, hogy

$$\sum_{i=1}^n u_{a_i} + v_{b_i} + w_{c_i} \leq nu_0 + nv_0 + nw_0.$$

Ekkor a skatulyaelv miatt minden megfelelő $\underline{a}, \underline{b}, \underline{c}$ hármasra a

$$\sum_{i=1}^n u_{a_i} \leq nu_0 \quad \sum_{i=1}^n v_{b_i} \leq nv_0 \quad \sum_{i=1}^n w_{c_i} \leq nw_0$$

egyenlőtlenségek közül legalább egynek teljesülnie kell. Ezért az $F^n(\underline{x}, \underline{y}, \underline{z})$ függvényt át tudjuk írni a következőképpen; nevezzük azon $\underline{a} \in A^n$ elemek halmazát, melyekre $\sum_{i=1}^n u_{a_i} \leq nu_0$ teljesül, A_0^n-nek, illetve definiáljuk a B_0^n, C_0^n halmazokat hasonló módon, ekkor

$$F^n(\underline{x}, \underline{y}, \underline{z}) =$$

$$= \sum_{\underline{a} \in A_0^n} \left(\prod_{i=1}^n f_{a_i}(x_i) \right) E_{\underline{a}}(\underline{y}, \underline{z}) + \sum_{\underline{b} \in B_0^n} \left(\prod_{i=1}^n g_{b_i}(y_i) \right) E_{\underline{b}}(\underline{x}, \underline{z}) + \sum_{\underline{c} \in C_0^n} \left(\prod_{i=1}^n h_{c_i}(z_i) \right) E_{\underline{c}}(\underline{x}, \underline{y})$$

megfelelő E függvényekkel. Most $|A_0^n|$ értékét fogjuk becsülni. Ezt a Hoeffding-egyenlőtlenséggel fogjuk becsülni [11]. Ez azt mondja ki, hogy ha $X_1, \cdots, X_n$ független változók, amik 0 és 1 között vesznek fel értéket, és $\bar{X}$ az átlaguk, akkor $P(\bar{X} - E(\bar{X}) \geq t) \leq e^{nt^2}$.

Feltehető, hogy $u_{max} > 0$, egyéb esetben F a konstans nulla függvény, ekkor leosztva u_{max} értékével minden u_a érték 0 és 1 közé esik, ami eleget tesz a Hoeffding tétel feltételének. Ekkor annak a valószínűsége, hogy egy $\underline{a} \in A$ elemre $\frac{1}{u_{max}} \sum u_a < \bar{u} - \epsilon$ legfeljebb $\exp(-2\epsilon^2 n)$. Mivel $|A|= |X|$, ezért

$$|A_0^n|= |A|^n P\bigg(\sum u_a < \bar{u} - \epsilon) \leq |X|^n \exp(-2\epsilon^2 n \bigg).$$

Mivel ez minden $\epsilon < \varepsilon$ valósra igaz ezért igaz a szuprémumukra is. Hasonló számolást végzünk a B_0^n, C_0^n halmazok számosságára is, majd ezt a hármat összeadva megkapjuk a rangot, ezzel a tételt beláttuk.

Tétel Legyen k egy tetszőleges páratlan szám Z_k egy k rendű ciklikus csoport. Ekkor létezik $\lambda < k$, hogy ha a A a $\bigoplus_{i=1}^n Z_k$ csoport egy 3 hosszú számtani sorozatot nem tartalmazó részhalmaza, akkor

$$|A| \leq \lambda^n.$$

Bizonyítás A korábbi lemma alapján $|A| \leq \text{rank}(\delta_{0^n}(x-2y+z))$. Az előző tétel alapján létezik olyan $\varepsilon > 0$, hogy $\text{rank}(\delta_{0^n}(x-2y+z)) \leq k^n \exp(-2\varepsilon^2 n) = (k \exp(-2\varepsilon^2))^n$, és mivel $k \exp(-2\varepsilon^2) < k$ ezzel a tételt beláttuk.

7. fejezet

A háromszög rang, a prímhatványrendű ciklikus csoportok esete

Az előző fejezetben már beláttuk, hogy bizonyos Abel-csoportra megadható az Ellenberg-Gijwijt tételéhez hasonló korlát. Most az a kérdés, hogy ezt a korlátot milyen jól tudjuk becsülni. Ehhez először jobb felírásait keressük a súlyfüggvények eloszlásának. Először vezessünk be egy következő függvényt; ha X, Y, Z véges halmazok, $\mathbb{F}$ valamilyen test, $F : X \times Y \times Z \to \mathbb{F}$, ekkor legyen az F függvény háromszög rangja a legkisebb olyan pozitív egész k amire léteznek olyan $A, B, C \subset \{0, \cdots, k-1\}$ indexhalmazok, hogy minden $a \in A$ elemhez hozzárendelve egy $f_a : X \to \mathbb{F}$ függvényt, a $b \in B, c \in C$ elemekhez $g_b : Y \to \mathbb{F}, h_c : Z \to \mathbb{F}$ függvényeket rendelünk, és $r_{a,b,c} : A \times B \times C \to \mathbb{F}$ súlyokat, hogy minden $(x, y, z) \in X \times Y \times Z$ elemre

$$F(x, y, z) = \sum_{(a,b,c) \in A \times B \times C, a+b+c<k} r_{a,b,c} f_a(x) g_b(y) h_c(z).$$

A konstans 0 függvény háromszög rangja legyen 0, és jelöljük a háromszög rangot a hrank kifejezéssel.

Állítás Legyen p egy kettőtől különböző prímszám. Legyen $F : \mathbb{F}_p^3 \to \mathbb{F}_p$ olyan, hogy $F(x, y, z) = P(x - 2y + z)$ valamilyen polinomra. Ekkor

$$\text{hrank}(F) \leq p.$$

Bizonyítás Valóban, a P polinomot fel tudjuk bontani monomok összegére, ahol minden egyes monomnak a foka legfeljebb $p - 1$, tehát a $f_a(x) := x^a \quad g_b(y) := y^b \quad h_c(z) := y^c$ választással tudunk csinálni egy jó konstrukciót. Megfelelő $r_{a,b,c}$ konstansokra

$$F(x, y, z) = \sum_{a+b+c<p} r_{a,b,c} x^a y^b z^c$$

igaz, ezzel az állítást beláttuk.

A következőkben keresünk kapcsolatot a háromszögrang és az instabilitás között.

Állítás Legyen X véges halmaz, $\mathbb{F}$ valamilyen test, $F : X^3 \to \mathbb{F}$ és legyen $\mathrm{hrank}(F) \leq |X|$. Ekkor F instabilitása legalább $\frac{1}{6}$.

Bizonyítás Legyen $|X|= k$; ekkor definíció szerint létezik az F fügvénynek olyan felírása, ahol tetszőleges $x_1, x_2, x_3 \in X$ elemekre

$$F(x_1, x_2, x_3) = \sum_{a+b+c<k} r_{a,b,c} f_a(x_1) g_b(x_2) h_c(x_3).$$

Feltehetjük, hogy az f_a függvények lineárisan függetlenek, különben választhatunk egy másik felírást, illetve ugyanezt feltehetjük a g_b, h_c függvényekre is. Egészítsük ki a függvényeket bázissá, és legyen $u_a := a$ minden $a \in A$ elemre, ekkor $u_{min} = 0$ $u_{max} = k-1$ és $\bar{u} = \frac{k-1}{2}$. Ekkor tetszőleges $\epsilon < 1/6$ valós számra$R_\epsilon = \frac{3(k-1)}{2} - 3\epsilon(k-1) > k-1$, tehát erre az eddig használt f_a, g_b, h_c felbontása az F függvénynek működni fog. Ebből már következik, hogy F instabilitása legalább $\frac{1}{6}$.

Most szeretnénk $\mathrm{hrank}(F) \leq k$ esetén F^n általánosított rangját becsülni. Ehhez szükségünk lesz arra, hogy meg tudjuk becsülni m, n pozitív egészek esetén az $\{0, \cdots, m\}^n$ halmaz azon a elemeinek számát, amelyekre $\sum_{i=1}^n a_i \leq \frac{mn}{3}$. Ehhez vezessük be a következő függvényt: $m > 0$ egészre és $\alpha \in (0, 1/2)$ valósra legyen

$$I(\alpha, m) := \sup_{\theta<0} \left(\alpha\theta - \log \left(\frac{1 - e^{(1+1/m)\theta}}{(m+1)(1 - e^{\theta/m})} \right) \right).$$

Lemma Legyen $\alpha \in (0, 1/2)$ valós m, n pozitív egészek. Ha $A \subset \{0, \cdots, m\}^n$, hogy tetszőleges $a \in A$ elemre $\sum_{i=1}^n a_i \leq \alpha mn$, akkor

$$|A| \leq m^n \exp(-I(\alpha, m)n).$$

Illetve, fix α valósra $I(\alpha, m)$, mint egy sorozat, ahol m az index, monoton nő, korlátos és

$$\lim_{m\to\infty} I(\alpha, m) = \sup_{\theta<0} \left(\alpha\theta - \log \left(\frac{e^\theta - 1}{\theta} \right) \right).$$

Bizonyítás Osszuk le $|A|$ értékét az m^n számmal ekkor

$$\frac{|A|}{m^n} = P\left(a \in \{0, \cdots, m\}^n; \sum_{i=1}^n a_i \leq \alpha mn \right) = P\left(a \in \left\{ \frac{0}{m}, \cdots, \frac{m}{m} \right\}^n; \sum_{i=1}^n a_i \leq \alpha n \right).$$

Ezt átalakítva, legyenek $x_1, \cdots x_n$ diszkrét egyenletes eloszlású független valószínűségi változók a $\{\frac{0}{m}, \cdots \frac{m}{m}\}$ halmazon. Ekkor a fenti érték átalakítható a következő módon:

$$P\bigg(\sum_{i=1} nx_i \leq n\alpha\bigg).$$

Ekkor tetszőleges $\theta < 0$ számmal beszorozva, és mind a két oldalt az exp függvénnyel véve

$$P\bigg(\sum_{i=1} n\theta x_i \geq n\alpha\theta\bigg) = P\bigg(\exp\left(\theta\sum_{i=1} n\theta x_i\right) \geq e^{n\alpha\theta}\bigg).$$

Ezt a valószínűséget becsülhetjük a Markov egyenlőtlenséggel, amit, felhasználva, hogy az x_i változók függetlenek, szorzatra bonthatunk.

$$\frac{|A|}{m^n} \leq \frac{E\bigg(\exp\left(\theta\sum_{i=1} nx_i\right)\bigg)}{e^{n\alpha\theta}} = \frac{(E(e^{\theta x_1}))^n}{e^{n\alpha\theta}}$$

Az $\exp(\theta/m)$ számot nevezzük x-nek, ekkor $x \in (0,1)$. Behelyettesítve

$$\frac{\left(\sum_{i=0}^m x^i\right)^n}{(m+1)^n x^{nm\alpha}} = \frac{(x^{m+1}-1)^n}{((x-1)(m+1))^n x^{nm\alpha}} = \left(\frac{x^m-1}{(m+1)(x-1)x^\alpha}\right)^n.$$

Átrendezve:

$$|A| = m^n \inf_{x\in(0,1)}\left(\left(\frac{x^m-1}{(m+1)(x-1)x^\alpha}\right)^n\right) =$$

$$= m^n \exp\left(n\log\left(\inf_{x\in(0,1)}\left(\frac{x^m-1}{(m+1)(x-1)x^\alpha}\right)\right)\right).$$

Visszahelyettesítve a θ változóra megkapjuk az állítás első felét. A bizonyítás második feléhez legyen $G : \mathbb{R}\times\mathbb{R}^+ \to \mathbb{R}$, ahol $G(t,x) := \frac{1-e^{t(1+x)}}{(1+1/x)(1-e^{tx})}$, illetve legyen $G(0,x) = 1$; könnyű ellenőrizni, hogy így G folytonos $(0,x)$-ben. Definíció szerint $I(\alpha,m)$ az $\alpha\theta - G(\theta,1/m)$ kifejezés szuprémuma θ-ra tekintve ahol, $\theta < 0$. Az exponenciális függvényt hatványsorba fejtve

$$\frac{1-e^{t(1+x)}}{(1+\frac{1}{x})(1-e^{tx})} = \frac{x}{1+x}\,\frac{\frac{(x+1)t}{2}+O(t^2)}{\frac{xt}{2}+O(t^2)}.$$

Kiegyszerűsítve azt kapjuk, hogy $G(t,x) = 1+\frac{t}{2}+O(t^2)$. Eszerint a $G(t,x)$ függvény t szerinti deriváltja 0-ban $\frac{1}{2}$. Ebből következik, hogy a $\alpha\theta - G(\theta,1/m)$ függvény θ szerinti deriváltja negatív nullában tetszőleges $\alpha \in (0,1/2)$ számra. Ebből következik, hogy létezik $\theta < 0$, amire $\alpha\theta - G(\theta,1/m)$ pozitív, tehát $I(\alpha,m)$ mindig pozitív.

A következőkben legyen $h(x) := \frac{e^{tx}-1}{x}$ valamilyen t-re, ekkor $\frac{h(x+1)}{h(x)} = G(t,x)$. Ebből következik, hogy G x szerinti deriváltja pontosan akkor pozitív, amikor $h'(x+1)h(x) >$

$h(x+1)h'(x)$, mivel $h^2(x)$ pozitív, így deriváljuk a G függvényt x szerint, szorzunk $h^2(x)$-vel, és rendezünk. Mivel az x változót pozitívnak tekintettük, ezért $h(x)$ is pozitív, így rendezhető tovább az egyenlőtlenség olyan módon, hogy $\frac{h'(x+1)}{h(x+1)} > \frac{h'(x)}{h(x)}$. Tehát ahhoz, hogy belássuk, a G függvény x szerint monoton nő, elég belátni, hogy a h függvény logaritmikus deriváltja monoton nő, ami ekvivalens azzal, hogy $\log(h(x))$ második deriváltja pozitív.

$$(\log(h(x)))^{(2)} = \left(-\frac{1}{x} - \frac{te^{tx}}{1-e^{tx}}\right)' = \frac{1}{x^2} - \frac{t^2e^{tx}}{(1-e^{tx})^2}$$

A jobb oldali kifejezés pontosan akkor pozitív, ha $x^2t^2e^{tx} < (1-e^{tx})^2$. Legyen $z = -tx$, vonjunk gyököt az előző egyenlőtlenségből (megtehetjük, mert mind a két oldal pozitív), az egyenlőtlenség két oldalát fejtsük hatványsorba z illetve $z/2$ szerint ekkor azt kapjuk, hogy

$$\sum_{n=1}^{\infty} \frac{z^n}{n!} > \sum_{n=1}^{\infty} \frac{z^n}{2^{n-1}(n-1)!}.$$

Mivel minden $n > 2$ egész számra $n(n-1)! < 2^{n-1}(n-1)!$ és $n = 1, 2$ -re pedig egyenlőség áll fenn, ezzel az egyenlőtlenséget beláttuk.

Az utolsó részben belátjuk, hogy $I(\alpha, m)$ konvergens, ha m tart végtelenbe.

$$\lim_{m\to\infty} I(\alpha, m) = \lim_{m\to\infty} (\sup_{\theta<0}(\alpha\theta - \log(G(\theta, 1/m))))$$

Mivel $-\log(G(\theta, x))$ monoton csökkenő x szerint, ezért $\alpha\theta - \log(G(\theta, 1/m))$ monoton nő m-re nézve, és $G(\theta, 1/m)$ folytonosan függ θ-tól, tehát, ha $\lim_{m\to\infty} G(\theta, 1/m)$ létezik, akkor a határérték és a szuprémum felcserélhető egymással. Legyen $x = \frac{1}{m}$ ekkor

$$\sup_{\theta<0}(\alpha\theta - \lim_{m\to\infty}(\log(G(\theta, 1/m)))) = \sup_{\theta<0}\left(\alpha\theta - \log\left(\lim_{x\to 0}\left(\frac{h(x+1)}{h(x)}\right)\right)\right).$$

Mivel $\lim_{x\to 0} h(x) = -\theta$, és $h(1) = e^{-\theta} - 1$, ezért a fenti határérték értelmes,

$$\lim_{m\to\infty} I(\alpha, m) = \sup_{\theta<0}\left(\alpha\theta - \log\left(\frac{1-e^{\theta}}{-\theta}\right)\right)$$

és ezzel a lemmát beláttuk.

Tétel Ha X véges halmaz, $|X| = k$, $\mathbb{F}$ valamilyen test, $F : X^3 \to \mathbb{F}$, olyan, hogy $\mathrm{hrank}(F) \leq k$, akkor $\mathrm{rank}(F^n) \leq 3(k\exp(-I(1/3, k-1)))^n$.

Bizonyítás Definíció szerint ilyen esetben létezik az F függvénynek egy olyan felírása, hogy tetszőleges $x_1, x_2, x_3 \in X$ elemekre:

$$F(x_1, x_2, x_3) = \sum_{a+b+c<k} r_{a,b,c} f_a(x_1) g_b(x_2) h_c(x_3).$$

Ekkor tetszőleges $(\bar{x}), (\bar{y}), (\bar{z}) \in X^n$ elemekre

$$F^n(\bar{x}, \bar{y}, \bar{z}) = \prod_{i=1}^{n} \Bigg(\sum_{a+b+c<k} r_{a,b,c} f_a(x_i) g_b(y_i) h_c(z_i) \Bigg).$$

Legyen $I : \{1, \cdots, k-1\}^{n\times 3} \to \{0,1\}$ olyan, hogy $\bar{a}, \bar{b}, \bar{c} \in [k-1]^n$ elemekre $I(a,b,c) = 1$ pontosan akkor, ha minden $i \in [n]$ számra $a_i + b_i + c_i < k$. Ha kifejtjük a szorzatot, a következő kifejezést kapjuk:

$$\sum_{\bar{a},\bar{b},\bar{c} \in [k-1]^n; I(a,b,c)=1} \prod_{i=1}^{n} r_{a_i b_i c_i} f_{a_i}(x_i) g_{b_i}(y_i) h_{c_i}(z_i).$$

Ha $I(\bar{a}, \bar{b}, \bar{c}) = 1$, akkor a skatulyaelv szerint az $\bar{a}, \bar{b}, \bar{c}$ vektorok közül legalább egyre igaz, hogy az elemeinek az összege kisebb mint $\frac{nk}{3}$, ha eszerint rendezzük a szumma elemeit, megfelelő E függvényekre

$$\sum_{\bar{a} \in [k-1]^n; a_1+\cdots+a_n \le nk/3} \Bigg(\prod_{i=1}^{n} f_{a_i}(x_i) \Bigg) E_{0,\bar{a}}(\bar{y}, \bar{z}) + \sum_{\bar{b} \in [k-1]^n; b_1+\cdots+b_n \le nk/3} \Bigg(\prod_{i=1}^{n} g_{b_i}(y_i) \Bigg) E_{\bar{b},1}(\bar{x}, \bar{z}) +$$

$$+ \sum_{\bar{c} \in [k-1]^n; c_1+\cdots c_n \le nk/3} \Bigg(\prod_{i=1}^{n} f_{c_i}(z_i) \Bigg) E_{\bar{c},2}(\bar{x}, \bar{y}).$$

Az előző lemma szerint ilyen $\bar{a}$ elemekből csak $(k \exp(-I(1/3, k-1)))^n$ darab van, ezzel a tételt beláttuk.

Látható, hogy a háromszögrang hatékony módszer bizonyos részhalmazok méretének becslésére. Kérdéses még az, hogy milyen Abel csoportokon találhatunk még olyan függvényt, amivel becsülhetjük a 3 hosszú számtani sorozatot nem tartalmazó részhalmazok méretét.

Állítás Legyen p egy tetszőleges, 2-től különböző prím, $q = p^k$ valamilyen k pozitív egészre, ekkor legyen $D : Z_q^3 \to \mathbb{F}_p$ olyan, hogy $D(x,y,z) = \delta_0(x - 2y + z)$, ekkor

$$\mathrm{hrank}(D) \le q.$$

Bizonyítás Legyen $H : Z_q^3 \to \mathbb{F}_p$ olyan, hogy $H(x,y,z) = \delta_0(x{+}y{+}z{+}1)$, és $\mathrm{hrank}(H) = \mathrm{hrank}(D)$. Valóban, ha $\mathrm{hrank}(H) = n$, akkor megfelelő f_a, g_b, h_c függvényekre

$$H(x,y,z) = \sum_{a+b+c<n} r_{a,b,c} f_a(x) g_b(y) h_c(z).$$

Vegyük észre, hogy $D(x,y,z) = H(x,-2y-1,z)$. Legyen $g'_b(y) = g(-2y-1)$ ekkor

$$D(x,y,z) = \sum_{a+b+c<n} r_{a,b,c} f_a(x) g'_b(y) h_c(z),$$

tehát elég belátni, hogy $\mathrm{hrank}(H) = q$. A következő azonosságot fogjuk használni, tetszőleges w természetes számra:

$$\binom{w}{q-1} \equiv \begin{cases} 1 \mod p & \text{ha} \quad w \equiv -1 \mod q \\ 0 \mod p & \text{egyébként.} \end{cases}$$

Ez könnyen ellenőrizhető, mert ha w nem kongruens -1-el modulo q akkor a $\prod_{i=0}^{q-2}(w-i)$ szorzatban lesz q-val osztható elem $(q-1)!$-ban pedig nem lesz. Ha viszont $w \equiv -1 \mod q$, akkor minden p hatvány kiesik a szorzatból, és a maradék tagok szorzata kongruens a $(q-1)(p-1)!$ kifejezéssel,ez pedig a Wilson tétel szerint 1 lesz. Mivel tetszőleges n_1, n_2, n_3, i számokra igaz a következő azonosság:

$$\binom{n_1+n_2+n_3}{i} = \sum_{a,b,c\in\mathbb{N}, a+b+c=i} \binom{n_1}{a}\binom{n_2}{b}\binom{n_3}{c},$$

ezért a $\binom{x+y+z}{q-1}$ függvényt át tudjuk írni a következőképpen

$$\binom{x+y+z}{q-1} = \sum_{a,b,c\in\mathbb{N}, a+b+c=q-1} \binom{x}{a}\binom{y}{b}\binom{z}{c}.$$

Ez alapján a $H(x,y,z) = \binom{x+y+z}{q-1}$ függvény megfelelő, és ezzel beláttuk, hogy $\mathrm{hrank}(D) \le q$.

Az állítás segítségével általánosíthatjuk az Ellenberg-Gijswijt tételt prímek helyett prímhatványokra is.

Tétel Ha q egy páratlan prímhatvány, n valamilyen természetes szám és $A \subset Z_q^n$ három hosszú számtani sorotot nem tartalmazó részhalmaz, akkor

$$|A| \le 3(q\exp(-I(1/3, q-1)))^n$$

Bizonyítás Az imént definiált D függvény az A^3 halmazon értelmezve csak a főátlón vesz fel elemeket, mivel $\mathrm{hrank}(D) \leq q$ tehát

$$\mathrm{rank}(H) \leq 3(q \exp(-I(1/3, q-1)))^n$$

és mivel egy olyan függvény ami csak a főátlón vesz fel elemeket, csak legfeljebb annyi helyen vehet fel nemnulla elemet, amennyi az általánosított rangja. Mivel minden $a \in A$ elemre $H(a) \neq 0$ ezért A elemszáma legfeljebb az általánosított rang nagysága lehet. Ezzel a tételt beláttuk.

Irodalomjegyzék

[1] M. Bateman and N. Katz, *New bounds on cap sets,* Journal of the American Mathematical Society 25 (2012), no. 2, 585–613.

[2] Jonah Blasiak, Thomas Church, Henry Cohn, Joshua A. Grochow, Eric Naslund, William F. Sawin,and Chris Umans. *On cap sets and the group-theoretic approach to matrix multiplication.* Discrete Analysis, 2017:3 27pp 1, 2

[3] T. C. Brown and J. P. Buhler, *A density version of a geometric Ramsey theorem,* Journal of Combinatorial Theory, Series A 32 (1982), no. 1, 20–34.

[4] E. Croot, V. F. Lev, and P. P. Pach, *Progression-free sets in* $\mathbb{Z}_4^N$ *are exponentially small,* Ann. of Math. (2) 185 (2017), no. 1, 331–337

[5] J. S. Ellenberg and D. Gijswijt *On large subsets of* $\mathbb{F}_q^n$ *with no three-term arithmetic progression,* Ann. of Math. (2) 185 (2017), no. 1, 339–343

[6] B. Green, *Finite field models in additive combinatorics,* Surveys in combinatorics 2005, London Math. Soc. Lecture Note Ser., vol. 327, Cambridge Univ. Press, Cambridge, 2005, pp. 1–27,

[7] JOSHUA A. GROCHOW, *NEW APPLICATIONS OF THE POLYNOMIAL METHOD: THE CAP SET CONJECTURE AND BEYOND* BULLETIN (New Series) OF THE AMERICAN MATHEMATICAL SOCIETY Volume 56, Number 1, January 2019, Pages 29–64

[8] Roy Meshulam: *On Subsets of Finite Abelian Groups with No 3-Term Arithmetic Progressions,* JOURNAL OF COMBINATORIAL THEORY, Series A 71, 168 172 (1995)

[9] D. Mumford, J. Fogarty, F. Kirwan: *Geometric Invariant Theory (3rd edition).* Springer-Verlag, Berlin 1994

[10] T. Tao, *A symmetric formulation of the Croot–Lev–Pach–Ellenberg–Gijswijt capset bound,* https://terrytao.wordpress.com/2016/05/18/a-symmetric-formulationof-the-croot-lev-pach-ellenberg-gijswijt-capset-bound/

[11] Hoeffding, Wassily, *Probability inequalities for sums of bounded random variables* Journal of the American Statistical Association. 58 (301): 13–30.