A kötet az Eötvös Loránd Tudományegyetem tankönyv- és jegyzettámogatási pályázatán elnyert forrás felhasználásával jelent meg.
A kézirat bővítve: 2020.

Additív Kombinatorika

Hegyvári Norbert

ISBN 978-963-489-088-1

Jelölések

G általában véges kommutatív csoport

$A, B \subseteq G$,
$A + B := \{a + b : \ a \in A; \ b \in B\}$,
$A - B := \{a - b : \ a \in A; \ b \in B\}$

$\mathbb{N}$, $\mathbb{N}_{\geq}$, $\mathbb{Z}$, $\mathbb{Z}_n$ $\mathbb{F}_p$, $\mathbb{F}_p^*$ a természetes számok (tehát az $1, 2, \ldots$ egészek), a nemnegatív egészek, az egészek halmaza, a mod n maradékosztályok az összeadás műveletével, prímrendű véges test, $\mathbb{F}_p$ multiplikatív részcsoportja

Ha $A \subseteq G$, ahol G egy csoport, akkor $\langle A \rangle$ jelöli az A által generált részcsoportot (azaz az A-t tartalmazó összes részcsoport metszetét)

$k \cdot A = \{ka : a \in A\}$

$kA = \{a_1 + a_2 + \cdots + a_k : a_i \in A\}$

Az $A = \{a_1 < a_2 < \cdots < a_k < \ldots\}$ sorozat konvex, ha bármely $i \in \mathbb{N}$ esetén $a_{i+1} - a_i < a_{i+3} - a_{i+2}$ teljesül

$\cup$ az unió, $\sqcup$ a diszjunkt unió jele

Egy A halmaz $A(x)$ indikátor függvényén az

$$A(x) = \begin{cases} 0 & \text{ha } x \notin A, \\ 1 & \text{ha } x \in A \end{cases}$$

függvényt értjük. Néhány esetben – például amikor a norma jelölést használjuk, az $1_A(x)$ lesz az $A(x)$.

$\|\alpha\|$ jelöli α távolságát a legközelebbi egésztől, azaz $\|\alpha\| = \min_{k \in \mathbb{Z}}\{|k - \alpha|\}$

$ind_g a$ index modulo p, (vagy diszkrét logaritmus); legyen g egy fix primitív gyök modulo p és legyen $a \in \mathbb{F}_p^*$. Ekkor a felírható $a = g^x : x \in \{1, 2, \ldots, p - 1\}$ formában. Az index (diszkrét logaritmus) tehát $ind_g a = ind\ a := x$.

Előszó

Az utóbbi másfél évtized egyik igen gyorsan fejlődő ága a kombinatorikus számelméletnek az *Additív Kombinatorika*. Hogy mit takar ez a kifejezés, legegyszerűbb ha idézzük Ben Green – aki e terület vezető matematikusa, és aki Terence Taoval együtt annak a sokak által reménytelennek tűnő sejtésnek a bizonyítói, hogy a prímszámok sorozata tetszőlegesen hosszú (nem triviális; értsd nem $p, p, \ldots, p$) számtani sorozatot tartalmaz – meghatározását. Ő így ír: *"Well one might say that additive combinatorics is a marriage of number theory, harmonic analysis, combinatorics, and ideas from ergodic theory, which aims to understand very simple systems: the operations of addition and multiplication and how they interact."* ("Nos, az additív kombinatorika a számelmélet, a harmonikus analízis, a kombinatorika, az ergodelmélet eredményeinek az együttese, melynek célja egy nagyon egyszerű struktúra megértése, melyben két művelet, az összeadás és szorzás van, továbbá, hogy ezek milyen viszonyban vannak egymással").

Ebben a könyvben olyan eredményeket tárgyalunk, amelyek valóban ezen eszközök csaknem mindegyikét használják, sőt számos egyébb módszert is (lásd pl. a gráf spektrum technikát). Nem kíván versenyezni olyan klasszikusnak számító könyvvel, mint "T.Tao, V.Vu Additive Combinatorics", sőt sok tekintetben el is tér e műtől (kivéve a nevezetes Gowers-Balog-Szemerédi tétel tárgyalásától).

Az additív kombinatorikának számos magyar és igen neves külhoni művelője van. (Gyors számvetéssel három Fields medállal kitüntetett, Abel-díjas, Fulkerson díjas matematikust sikerült összegyűjteni.) A szerző reménye, hogy haszonnal fogják forgatni matematika szakos és PhD hallgatók, fiatal kutatók, sőt, mivel számos fejezet nem igényel különösebb előismeretet, középiskolai tanárok, tehetséges tanulók is találnak benne számukra érdekes eredményeket.

A könyv az ELTE Doktori Iskolájában és speciális kurzusaimon tartott előadásaim kibővített változata. Köszönettel tartozom sok diákomnak, akik megjegyzéseikkel javították az elkészült munkát. Mint majdnem minden jegyzetben/könyvben (sajnos) marad(hat)nak elírások, e könyv olvasóinak minden megjegyzéseit köszönettel fogadom az n.hegyvari@gmail.com címen.

Mivel e könyv elektromos változatban jelenik meg, nem lesz különösebbben nehéz az (esetleges) javítás.

Külön köszönet illeti Pach Péter Pált, aki gondos lektorálásával nagyban segítette a munkámat.

2018. Göd

A szerző

Tartalomjegyzék

1. fejezet

Alapvető problémák

1.1. Bevezető tételek

1.1.1. Tétel. *Legyenek* $A, B \subseteq \mathbb{Z}$.

$$(1) \qquad |A| + |B| - 1 \leq |A + B| \leq |A||B|,$$

ahol $A + B := \{a + b : \ a \in A; \ b \in B\}$ *a Minkowski összeg,*

$$(2) \qquad |A| + |B| - 1 = |A + B|$$

akkor és csak akkor, ha A *és* B *közös differenciájú számtani sorozatok.*

Bizonyítás:

(1) Legyen $|A| = k; \ |B| = n$. Az $A+B$ halmazban nyilván legfeljebb annyi elem lehet, ahány (a, b) párt képeztünk, azaz $|A + B| \leq |A||B|$. Továbbá az

$$a_1 + b_1 < a_1 + b_2 < \cdots < a_1 + b_n < a_2 + b_n < \cdots < a_k + b_n$$

sorozatban minden elem különböző, ezek elemei $A + B-$nek és e sorozat $k + n - 1$ elemből áll.

(2) $|A + B| = k + n - 1$ teljesül, ha mind A, mind B egy-egy számtani sorozat, melyeknek di□erenciája azonos. Megmutatjuk, hogy másként nem lehet. Ehhez tekintsük a következő mátrixot (csak a jobb érthetőség kedvéért rendeztük mátrixba az összeg elemeit)

$$\begin{pmatrix} a_1+b_n & \cdot & \cdot & \cdot & \cdot & \cdot & \to & a_k+b_n \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \uparrow & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & a_i+b_{j+1} & a_{i+1}+b_{j+1} \to & \cdot & \cdot & \\ \cdot & \cdot & \to & a_i+b_j & a_{i+1}+b_j & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \uparrow & \to \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\ a_1+b_1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a_k+b_1 \end{pmatrix}$$

E mátrixban bármely elemtől jobbra illetve a felette levő elemek nagyobbak. Közlekedjünk a bal alsó saroktól (a_1+b_1 elemtől) a jobb felső sarokba (a_k+b_n) jobbra-felfelé lépésekkel. Jegyezzük meg, hogy $k+n-1$ különböző elemet érintettünk. (Tehát nem csak az (1) részben feltüntetett sorozat ad magyarázatot az alsó becslésre.) Közlekedjünk most úgy, hogy az utunkban az $a_i+b_j < a_{i+1}+b_j < a_{i+1}+b_{j+1}$ elemek legyenek. Cseréljük ki az $a_{i+1}+b_j$ elemet az a_i+b_{j+1} elemre. Ekkor nyilván teljesül az is, hogy $a_i+b_j < a_i+b_{j+1} < a_{i+1}+b_{j+1}$. Azaz az a_i+b_j és az $a_{i+1}+b_{j+1}$ elemek között van az $a_{i+1}+b_j$ és az a_i+b_{j+1} elem, és mivel mindkét esetben $k+n-1$ különböző összeget kaptunk, azt kapjuk, hogy $a_{i+1}+b_j = a_i+b_{j+1}$ teljesül minden i,j párra. Átrendezve és $i-$t egynek választva azt kapjuk, hogy

$$b_{j+1}-b_j = a_2-a_1 := d$$

teljesül minden $j-$re. Így B egy számtani sorozat. A szerepeket megcserélve kiderül, hogy A is egy ugyanakkora di□erenciájú számtani sorozat. □

G a következőkben kommutatív csoportot jelent. Ha külön nem jelezzük, akkor halmazaink mindig egy ilyen csoport véges részhalmazai.

1.1.2. Tétel. *Legyen $A, B \subseteq G$. Az alábbi állítások ekvivalensek:*

(a) $|A+B| = |A|$

(b) $|A-B| = |A|$

(c) Létezik $G' < G$, hogy A halmaz G' szerinti mellékosztályok uniója, B pedig egy mellékosztályban van.

Bizonyítás:

Az általánosság megszorítása nélkül feltehetjük, hogy $0 \in B$, így $A+B = A$, ugyanis ekkor $A + B \supseteq A$ és $|A + B| = |A|$. Most k szerinti indukcióval következik, hogy

$$A + kB = A$$

és így

$$A + \langle B \rangle = A$$

ahol $\langle X \rangle$ jelöli az X által generált részcsoportot. Tehát $G' := \langle B \rangle$ és ebből (a), (b) és (c) ekvivalenciája következik. □

1.1.3. Tétel. *Legyen $A \subset \mathbb{Z}$ véges részhalmaz. Ekkor*

$$|A + 2 \cdot A| \geq 3|A| - 2.$$

(Itt és a továbbiakban is a $k \cdot A$ a ka alakú elemek halmazát jelenti. kA alatt az $a_1 + a_2 + \cdots + a_k$ alakú elemek halmazát értjük. Tehát $k \cdot A \subseteq kA$).

Bizonyítás:

Az általánosság megszorítása nélkül feltehetjük, hogy A páratlan és páros elemeket is tartalmaz. Ezért $A = A_0 \sqcup A_1$ ahol A_0 a páros, A_1 a páratlan elemeket tartalmazza. Így $(A_0 + 2 \cdot A) \cap (A_1 + 2 \cdot A) = \emptyset$ és ezért

$$|A+2\cdot A| = |A_0+2\cdot A|+|A_1+2\cdot A| \geq |A_0|+|2\cdot A|-1+|A_1|+|2\cdot A|-1 = 3|A|-2,$$

felhasználva a 1.1.1 tétel (1) bal oldalát. □

Feladatok

1. a.) Ha egy G Additív csoportban $X, Y \subseteq G$ és $|X| + |Y| > |G|$, akkor

$$X + Y = G.$$

b.) Legyen Q a kvadratikus maradékok halmaza modulo p (p páratlan prímszám). Ekkor minden maradék felírható legfeljebb két Q-beli elem összegeként.

2. Legyenek A, B nem negatív egészek, ahol a $|A| = k$ véges halmaz és tegyük fel, hogy $A + B = \mathbb{N}_{\geq 0}$ egyértelmű, azaz bármely n egyértelműen

írható fel egy A-beli és egy B-beli elem összegeként. Legyen $A(x)$ és $B(x)$ a két halmaz karakterisztikus függvénye.

a.) Igazoljuk, hogy ekkor bármely $n \geq k = \max A$ egészre

$$1 = B(n) + \sum_{j=1}^{k} A(j)B(n-j).$$

b.) Mutassuk meg, hogy létezik $k \leq n_1 < n_2 \leq 2^k + k$, hogy az $\{B(n_1 - 1), B(n_1 - 2), \ldots, B(n_1 - k)\}$ rendezett k-as egyenlő a $\{B(n_2 - 1), B(n_2 - 2), \ldots, B(n_2 - k)\}$-val!

c.) Mutassuk meg, hogy bármely $z \geq -k$ számra $B(n_1 + z) = B(n_2 + z)$ és bizonyítsuk be, hogy a B halmaz periodikus, azaz létezik P, hogy $B = \mathbb{N} \cdot P + C$ (C egy véges halmaz)!

Megoldások

1.a.) Ha van olyan $g \in G$, amelyre $g \notin X + Y$, akkor a $g - X$, és az Y halmazok diszjunktak, azaz $g - X, Y \subseteq G$ miatt

$$|X| + |Y| = |g - X| + |Y| \leq |G|,$$

ellentmondás.

b.) $|Q \cup \{0\}| = \frac{p+1}{2}$. Használjuk az a.)-t.

2. a.) Mivel bármely n-re $r_{A+B}(n) = 1$, továbbá $j > k = \max A$ esetén $A(j) = 0$ azt kapjuk, hogy $r_{A+B}(n) = \sum_{j=0}^{k} A(j)B(n-j) = B(n)A(0) + \sum_{j=1}^{k} A(j)B(n-j)$. Mivel 0 mindkét halmazban benne kell, hogy legyen (a 0-t is elő kell állítani) ezért $A(0) = 1$ amiből kapjuk az állítást.

b.) Mivel $B(x)$ 1 vagy 0, ilyen rendezett k-asból legfeljebb 2^k van.

c.) Az állítás a b.) feladat miatt igaz a $-k \leq z \leq 0$ számokra. Használjunk teljes indukciót! Az a.) feladat miatt

$$B(n_2+z) = 1 - \sum_{j=1}^{k} A(j)B(n_2+z-j) =^{induk.} = 1 - \sum_{j=1}^{k} A(j)B(n_1+z-j) = B(n_1+z).$$

Az $m + 1 \leq z \leq n_1$ számokra $B(n_1 - z) = B(n_2 - z)$ bizonyítása hasonló.

Ezért tehát a B halmaz $P = n_2 - n_1$ szerint periódikus.

1.1.1. Freiman homomorfizmus; Projekciós módszer

1. Definíció. *Egy $g : A \mapsto B$ függvényről azt mondjuk, hogy k-Freiman homomorfizmus, ha bármely $a_1, a_2, \ldots, a_k, a'_1, a'_2, \ldots, a'_k \in A$ esetén fennáll, hogy amennyiben*

$$a_1 + a_2 + \cdots + a_k = a'_1 + a'_2 + \cdots + a'_k,$$

akkor

$$g(a_1) + g(a_2) + \cdots + g(a_k) = g(a'_1) + g(a'_2) + \cdots + g(a'_k)$$

teljesül. g k-Freiman izomorfizmus, ha létezik g^{-1} és g^{-1} k-Freiman homomorfizmus.

A következő feladatsor segít a fenti fogalom megértésében:

FELADATOK

1. Legyen $g : \mathbb{Z} \mapsto \mathbb{Z}$, $g(x) = ax + b; a \neq 0$. Bizonyítsuk be, hogy g 2-Freiman izomorfizmus.

2. Legyen $f : \mathbb{Z}^d \mapsto \mathbb{Z}$ a következő: bármely $\underline{x} = (x_1, x_2, \ldots, x_d) \in \mathbb{Z}^d$, pontnak feleljen meg a

$$g : (x_1, x_2, \ldots, x_d) \mapsto x_1 + x_2 \cdot M + \cdots + x_d M^{d-1}.$$

Tegyük fel továbbá, hogy $(x_1, x_2, \ldots, x_d) \in [0, N]^d$. Milyen M mellett lesz e leképezés 2-Freiman izomorfizmus? k-Freiman izomorfizmus?

3. Legyen $A := \{0, 1, 10, 11\}$; $B := \{0, 1, 100, 101\}$. Igazoljuk, hogy A és B halmazok k-Freiman izomorfak $k \leq 9$ esetén, ám $k > 9$ esetén már nem.

1.1.4. Tétel. *Létezik olyan $X \subseteq \mathbb{F}_p$, melynek nincs 2-Freiman izomorf képe az egészeken, és amelyre*

$$X \leq 2\left\lfloor \frac{\log p}{\log 2} \right\rfloor + 1.$$

Bizonyítás

Legyen $p > 2$ prímszám és írjuk fel a kettes számrendszerben:

$$p = 2^{a_1} + 2^{a_2} + \cdots + 2^{a_n}.$$

Ekkor nyilván $n \leq \lfloor \log_2 p \rfloor + 1 := N + 1$. Tekintsük a következő $X \subseteq \mathbb{Z}_p$ halmazt:

$$X = \{0\} \cup \{1, 2, 4, \ldots, 2^N\} \cup \{2^{a_1}+2^{a_2}, 2^{a_1}+2^{a_2}+2^{a_3}, \ldots, 2^{a_1}+2^{a_2}+\cdots+2^{a_{n-1}}\}.$$

$|X| \leq 2N+1$. Igazolni fogjuk, hogy X nem lehet 2-Freiman izomorf egyetlen $Y \subseteq \mathbb{Z}$ halmazzal sem.

Indirekt tegyük fel, hogy létezik ilyen $Y \subseteq \mathbb{Z}$ és $g : X \mapsto Y$ ez a leképezés. Nyilván feltehetjük, hogy $g(0) = 0$ és így legyen

$$Y = \{0\} \cup \{u_0, u_1, \ldots, u_N\} \cup \{v_2, v_3, \ldots, v_{n-1}\},$$

ahol a megfelelő elemek az X megfelelő elemeinek a képeiként állnak elő.

Mivel $0+2^{i+1} = 2^i+2^i$, ezért (mint könnyen látható 0 képe a 0) $0+u_{i+1} = 2u_i$, amiből $u_1 = 2u_0;\ u_2 = 2u_1 = 4u_0;\ \ldots$ következik, vagyis $u_i = 2^i u_0;\ i = 1, 2, \ldots N$ esetén.

Mivel $0+2^{a_1}+2^{a_2} = 2^{a_1}+2^{a_2}$, ezért $v_2 = 0+v_2 = u_{a_1}+u_{a_2} = (2^{a_1}+2^{a_2})u_0$, az előző miatt; így $v_2 = (2^{a_1} + 2^{a_2})u_0$,

$v_3 = v_2 + u_{a_3}$ és ezért $\Rightarrow v_3 = (2^{a_1} + 2^{a_2} + 2^{a_3})u_0$;

Általában $0 + (2^{a_1} + 2^{a_2} + \cdots + 2^{a_i} + 2^{a_{i+1}}) = (2^{a_1} + 2^{a_2} + \cdots + 2^{a_i}) + 2^{a_{i+1}}$ ezért $v_{i+1} = v_i + u_{a_{i+1}}$ és az előző gondolatot felhasználva kapjuk, hogy $v_{i+1} = v_i + u_{a_{i+1}};\ i = 2, \ldots, N-2$ és ezért $v_{n-1} = (2^{a_1} + 2^{a_2} + \cdots + 2^{a_{n-1}})u_0$.

Az előzőekből speciálisan $v_{n-1} = (2^{a_1} + 2^{a_2} + \cdots + +2^{a_{n-1}})u_0$, így

$$v_{n-1} + u_{a_n} = (2^{a_1} + 2^{a_2} + \cdots + 2^{a_n})u_0 = pu_0,$$

hiszen $p = 2^{a_1} + 2^{a_2} + \cdots + 2^{a_n}$ és az egészek körében ez nem nulla, másfelől $(2^{a_1} + 2^{a_2} + \cdots + 2^{a_{n-1}}) + 2^{a_n}$ $\mathbb{Z}_p$-ben éppen a nulla ellentmondásként. □

Másfelől igaz, hogy

1.1.5. Tétel. *Legyen $W \subseteq \mathbb{F}_p$,*

$$|W| \leq \left\lfloor \frac{\log p}{2 \log 2} \right\rfloor.$$

Ekkor létezik W-nek egy 2-Freiman izomorf képe az egészeken.

Bizonyítás:
Felhasználjuk Dirichlet (könnyen bizonyítható) állítását:

1. Lemma. *Legyen $t > 1$, $t \in \mathbb{N}$, $z_1, z_2, \ldots, z_k$ valós számok. Ekkor van olyan d, $1 \leq d \leq t^k$, hogy*

$$\|d \cdot z_i\| < \frac{1}{t},$$

ahol $\|x\| = \min\{x, 1-x\}$ $x-$hez legközelebb eső egésztől való távolsága.

(Ezt a lemmát újra kimondjuk a 13.12 pontban)

Legyen $t = 4$, $z_i = \frac{w_i}{p}$, $1 \leq i \leq |W|$. Ekkor $d \leq p$, a dw_i elemek mind a $(-p/4, p/4)$ intervallumba esnek, így az összegük is a $(-p/2, p/2)$ intervallumba esik. A megfelelő 2-Freiman izomorf egészekből álló halmaz ez lesz tehát. □

1.2. A Cauchy, a Hölder és az általánosított Hölder egyenlőtlenségek

A bizonyítások során számtalanszor használni fogjuk a Cauchy egyenlőtlenséget:

Ha $a_1, a_2, \ldots, a_n; b_1, b_2, \ldots, b_n$ tetszőleges valós számok, akkor

$$a_1b_1 + a_2b_2 + \cdots + a_nb_n \leq \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}\sqrt{b_1^2 + b_2^2 + \cdots + b_n^2}.$$

Ennek bizonyítása egyszerű (pl. a $p_2(x) = (a_1x - b_1)^2 + (a_2x - b_2)^2 + \cdots + (a_nx - b_n)^2$ polinom nemnegatívitási vizsgálatából).

A későbbiekben látni fogjuk, hogy az additív energia típusú állításokhoz a tényezőket nem szimmetrikusan (mint a Cauchy egyenlőtlenségnél) hanem asszimetrikusan kell használni. Ezekre az esetekre hasznos a Hölder egyenlőtlenség

1.2.1. Tétel. *Legyen $\alpha, \beta > 1$; $\forall i$, $a_i, b_i \geq 0$; $\frac{1}{\alpha} + \frac{1}{\beta} = 1$. Ekkor*

$$\sum_{i=1}^{k} a_ib_i \leq \left(\sum_{i=1}^{k} a_i^\alpha\right)^{1/\alpha} \left(\sum_{i=1}^{k} b_i^\beta\right)^{1/\beta}.$$

Szokás bevezetni a

$$\|a\|_p := \left(\sum_{i=1}^{k} a_i^p\right)^{1/p}$$

jelölést. Az általánosított Hölder egyenlőtlenség pedig a következő:

1.2.2. Tétel. *Legyen* $r, p_1, p_2, \ldots, p_n > 0$; *továbbá* $\forall i\ a_i \geq 0$, *és*

$$\sum_{j=1}^{n} \frac{1}{p_j} = \frac{1}{r},$$

akkor

$$\left\| \prod_{j=1}^{n} a_j \right\|_r \leq \prod_{j=1}^{n} \|a_j\|_{p_j},$$

vagy a szokásosabb formában idézve

$$\sum_{i=1}^{n} \left(\left| \prod_{k=1}^{m} a_{ik} \right|^r \right)^{1/r} \leq \prod_{k=1}^{m} \left(\sum_{i=1}^{n} |a_{ik}|^{p_i} \right)^{1/p_i}$$

Az általánosított Hölder egyenlőtlenség bizonyítása n szerinti indukcióval visszavezethető az eredeti Hölder egyenlőtlenségre.

Bizonyítás:
Legyen

$$p := \frac{p_n}{p_n - r} \qquad q := \frac{p_n}{r}.$$

Nyilván ekkor $\frac{1}{p} + \frac{1}{q} = 1$. Használjuk az eredeti Hölder-t

$$\left\| |a_1 a_2 \ldots a_{n-1}|^r |a_n|^r \right\|_1 \leq \left\| |a_1 a_2 \ldots a_{n-1}|^r \right\|_p \cdot \left\| |a_n|^r \right\|_q .$$

Vonjunk $r-$edik gyököt mindkét oldalból, ekkor a bal oldalon éppen $\left\| \prod_{j=1}^{n} a_j \right\|_r$ adódik és így

$$\left\| \prod_{j=1}^{n} a_j \right\|_r \leq \|a_1 a_2 \ldots a_{n-1}\|_{p \cdot r} \cdot \|a_n\|_{q \cdot r} .$$

Az utolsó $\|a_n\|_{q\cdot r}$ tényező $\|a_n\|_{p_n}$, mivel $q \cdot r = p_n$.

$$\frac{1}{pr} = \frac{p_n - r}{p_n \cdot r} = \frac{1}{r} - \frac{1}{p_n} = \sum_{i=1}^{n-1} \frac{1}{p_i},$$

így az első $\|a_1 a_2 \dots a_{n-1}\|_{p\cdot r}$ tényezőre használhatjuk az indukciós feltevést és így kapjuk a bizonyítandó állítást is.

Hogy $n = 2$-re az általánosabb formára is igaz az állítás az eredeti Hölder $\leq$ csekély módodításával megkapható ami egy könnyű (házi)feladat. $\square$

2. fejezet

Cauchy-Davenport tétel; Kneser tétel

Az 1.1.1 tétel egészek körében ad becslést az $A + B$ halmaz elemszámára. Ebben a pontban azt vizsgáljuk, van e hasonló állítás más csoportokban. Kézenfekvő $\mathbb{Z}_N-$ben kezdeni a vizsgálatot. Ha N összetett, lásd a fejezet 2. feladatát. Az N prím esetén valóban van analóg állítás, melyet Cauchy és később tőle függetlenül Davenport bizonyított be:

2.0.1. Tétel. *Legyen p prím és legyenek $A, B \subseteq \mathbb{Z}_p$ nem üres részhalmazok. Ekkor*

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Az 2.0.1 tétel helyett egy általánosabb állítást igazolunk, az egyik Kneser tételt, amiből következik a Cauchy-Davenport tétel:

2.0.2. Tétel. *Legyen G véges kommutatív csoport, $A, B \subseteq G$ nem üres részhalmazok és tegyük fel, hogy $|A| + |B| \leq |G|$*

Ekkor létezik olyan $H \neq G$ részcsoportja $G-$nek, hogy

$$|A + B| \geq |A| + |B| - |H|.$$

Megjegyzés:
Az első fejezet 1. feladata szerint, ha $|A| + |B| > |G|$, akkor $A + B = G$, azaz $|A + B| = |G|$. Tehát az $|A| + |B| \leq |G|$ feltétel helyett úgy is fogalmazhattunk volna, hogy $|A + B| \geq \min\{|G|, |A| + |B| - |H|\}$.

Az 2.0.2 tétel bizonyítása

A bizonyításban $|B|$ szerinti indukciót használunk. Szükségünk van egy olyan transzformációra, amelyik csökkentheti B elemszámát:

DYSON-TRANSZFORMÁCIÓ

Legyen $x \in G$ és legyenek

$$A_x := A \cup (B + x); \qquad B_x := B \cap (A - x).$$

A definícióból nyilván következik, hogy

$$A_x + B_x \subseteq A + B,$$

továbbá igazoljuk, hogy

$$|A_x| + |B_x| = |A| + |B|.$$

Valóban,

$$|A_x| + |B_x| = |A \cup (B + x)| + |B \cap (A - x)| =$$
$$= |A \cup (B + x)| + |(B + x) \cap A| = |A| + |B + x| = |A| + |B|$$

felhasználva azt a (későbbiekben is sokszor használt) tényt, hogy csoportban egy halmaz eltolása nem változtatja meg a halmaz elemszámát.

Tehát ha találunk olyan x elemet, amelyre B_x nem üres és elemszáma kisebb, mint B elemszáma (amire van esélyünk a $B_x := B \cap (A - x)$ miatt, azaz x-nek $a - b$ alakúnak kell lennie), akkor az indukció így néz ki:

Az állítás nyilvánvaló, ha B egy elemből áll.

Ha $B_x \neq B$ és nem üres, akkor az indukciós feltevés miatt létezik $H \neq G$ részcsoport, hogy

$$|A + B| \geq |A_x + B_x| \geq^{ind.} |A_x| + |B_x| - |H| = |A| + |B| - |H|.$$

A bizonyítás tehát teljes lesz, ha megvizsgáljuk mikor nem alkalmazható az indukciós lépés a Dyson transzformáció segítségével. Azaz mikor lesz

$$B_x = \emptyset,$$

vagy

$$B_x = B.$$

Ezeket kizárhatjuk, ha tudunk olyan $x-$et mondani, amelyre B_x-nek van $A-$beli és $A-$n kívüli eleme is.

Mivel $B_x := B \cap (A - x)$, ezért kézenfekvő $x-$et $a - b$ alakban keresni, ugyanis $A - x = A - (a - b) \ni a - (a - b) = b$, ekkor tehát B_x nem üres. Tehát már csak az marad hátra, mi történik, ha $\forall (a, b) \in A \times B$

$$B \subseteq A - (a - b) \quad \Leftrightarrow \quad B + (a - b) \subseteq A.$$

Ez másként

$$B + A - B \subseteq A,$$

ekkor viszont minden $n \in \mathbb{N}$ esetén (indukcióval)

$$A + n(B - B) \subseteq A.$$

Elég nagy $n-$re $n(B-B)$ részcsoportja lesz $G-$nek, méghozzá $H := \langle B-B \rangle$, ezért

$$A + H \subseteq A \subseteq G,$$

és mivel $A \neq G$, ($|B| + |A| \leq |G|$ és nem üres részhalmazok) így $H \neq G$.

Ekkor nyilván $|H| \geq |B|$, amikor is triviálisan teljesül, hogy

$$|A + B| \geq |A| + |B| - |H|. \quad \square$$

Megjegyzés:

Bizonyítás nélkül említjük, hogy létezik egy erősebb Kneser tétel is, amit az egészek körében fogalmazunk meg:

Jelentse egy $A \subseteq \mathbb{N}$ halmaz alsó sűrűségét $\underline{d}(A) := \liminf_{n \to \infty} \frac{|A \cap [1,n]|}{n}$.

2.0.3. Tétel. *Ha* $\underline{d}(A+B) < \underline{d}(A) + \underline{d}(B)$, *akkor létezik* G, $g > 0$, *hogy* $G \subseteq [0, g-1]$, $|G| = m$,

$$(1)\ A + B \subseteq G + g\mathbb{N}; \quad (2)\ \exists t \in \mathbb{N}, (A+B) \cap [t, \infty) = (G + g\mathbb{N}) \cap [t, \infty),$$

továbbá

$$(3)\ \underline{d}(A+B) = \frac{m}{g} \geq \underline{d}(A) + \underline{d}(B) - \frac{1}{g}.$$

Feladatok

1. Vezessük le a Kneser tételből a Cauchy-Davenport tételt!

2. Adjunk meg olyan $\mathbb{Z}_N$ csoportot és $A, B \subseteq \mathbb{Z}_N$ halmazokat, amelyekre $A, B \neq \mathbb{Z}_N$ és amelyre $|B| \leq |A| = |A+B|$.

3. (Cauchy-Davenport speciális eset). Legyen $A, B \subseteq \mathbb{Z}_p$, p prímszám, $|A| = 2$ és B nem üres.

a.) Igazoljuk (a Cauchy-Davenport tétel felhasználása nélkül), hogy $|A+B| \geq \min\{p, |B|+1\}$.

b.) Legyenek $A_1, A_2, \ldots, A_k \subseteq \mathbb{Z}_p$ p prímszám, $|A_i| = 2$, $i = 1, 2, \ldots, k$. Ekkor $|A_1 + A_2 + \cdots + A_k| \geq \min\{p, k+1\}$.

4. (Erdős-Ginzburg-Ziv) Adottak az $a_1, a_2, \ldots a_{2n-1}$ egész számok. Ekkor kiválasztható közülük n, melyeknek összege osztható $n-$nel.

a.) $2n-1$ helyett $2n-2$-vel az állítás nem igaz.

b.) Elég az állítást prímekre bizonyítani

c.) Ha $0 \leq a_1 \leq a_2 \leq \cdots \leq a_{2p-1} \leq p-1$ és az $A_1 = \{a_1, a_p\}, A_2 = \{a_2, a_{p+1}\}, \ldots, A_{p-1} = \{a_{p-1}, a_{2p-2}\}$ halmazok nem mindegyike két elemű akkor triviális az állítás. Egyébként alkalmazzuk a 3.b) feladatot

5. Bizonyítsuk be, hogy a Cauchy-Davenport tétel ekvivalens a következő állítással:

Legyen $A, B, C \subseteq \mathbb{Z}_p$, három nem üres részhalmaz. Ha

$$|A| + |B| + |C| \geq p + 2,$$

akkor

$$A + B + C = \mathbb{Z}_p.$$

6. a.) Legyen $A \subseteq \mathbb{F}_p$ egy legalább kételemű részhalmaz. Az A halmaz iterált di□erenciahalmaza alatt a következőt értjük: legyen $A_0 = A$ és $i \geq 0$ esetén legyen $A_{i+1} = A_i - A_i$. Legyen továbbá $T(A) := \min\{k : A_{k+1} = A_k\}$, az az "időpont", amikor az iteráció stbilizálódik. Mutassuk meg, hogy $T(A)$ jól definiált (létezik) és

$$T(A) \leq \log_2 \Big(\frac{p-1}{|A|-1} \Big).$$

b.) Mutassuk meg, hogy a fenti becslés éles.

Megoldások

1. Legyen $G = \mathbb{Z}_p$. Nyilván a nem triviális H részcsoport a $H = \{0\}$.

2. Ilyen A és B halmazok mindig adhatók, ha N összetett. Legyen $d|N; 1 < d < N$ és álljon A halmaz d többszöröseiből. Ekkor bármely $B \subseteq A$ halmazra $A + B = A$.

3. a.) Az általánosság megszorítása nélkül feltehetjük, hogy A egyik eleme a 0 a másikat jelölje $a \neq 0$. Emiatt elég azt igazolni, hogy van olyan $b \in B$, amelyikre $a + b \notin B$. Ha $a + b = b_1$ akkor képezzük az $a + b_1 = 2a + b$ és általában a $ka + b;\ k = 1, 2, \ldots p$ elemeket. Ezek mind különbözőek és ha mind B-ben van, akkor $B = \mathbb{Z}_p$. Ellenkező esetben $|A + B| \geq |B| + 1 = |A| + |B| - 1$.

b.) k szerinti indukcióval.

4. a.) $n - 1$ db 0 és $n - 1$ db 1.

b.) Indukcióval. Ha $n = p \cdot q$ alakú, (p prím) akkor a $2n - 1 = 2pq - 1$ elem egy $2p - 1$-es halmazából kiválasztható p melyek összege osztható p-vel. A maradék $2n - 1 - p$ elemmel ismételjük meg az eljárást. Kaptunk $2q - 1$ darab p tagú összeget, melyek egyenként p-vel oszthatóak. Jelöljük ezeket $p \cdot s_j$, $j = 1, \ldots 2q - 1$. Az indukció miatt a $2q - 1$ s_j-ből kiválasztható q melyek összege q-val osztható. Ez az összesen $pq = n$ tagú összeg $pq = n$-nel osztható.

c.) Valóban, ha valamely i-re $1 \leq i \leq p-1$ $a_i = a_{i-1+p}$, akkor a monoton növekvő sorozatban p egymást követő elem megegyezik. Ellenkező esetben használjuk az előző feladat b.) pontját és így $|A_1 + A_2 + \cdots + A_{p-1}| = p$. Azaz $-a_{2p-1}$ előáll $p-1$ elem összegeként, azaz $a_{2p-1}+$ a $p-1$ elem összege éppen a 0.

5. Ha $|A| + |B| > p$, akkor $A + B = \mathbb{Z}_p$, tehát $A + B + C = \mathbb{Z}_p$.
Ha $|A| + |B| \leq p$, akkor a Cauchy-Davenport tétel miatt

$$|A + B| \geq |A| + |B| - 1,$$

és így

$$|A + B| + |C| \geq |A| + |B| + |C| - 1 > p,$$

mivel $|A| + |B| + |C| \geq p + 2$, így tehát $(A + B) + C = \mathbb{Z}_p$.

Indirekt tegyük fel, hogy van ellenpélda a Cauchy-Davenport lemmára, az $A, B, C - re$ tett feltételekkel mellett. Ekkor nyilván

$$|A| + |B| \leq p,\ |A + B| < p.$$

Legyen

$$C := -(\mathbb{Z}_p \setminus (A + B)).$$

Ekkor

$$|C| = p - |A + B| > p - |A| - |B| + 1;\ \Rightarrow\ |A| + |B| + |C| > p + 1.$$

Ekkor $|A|+|B|+|C| \geq p+2$, és így a feltétel miatt $A+B+C = \mathbb{Z}_p$. Például $a+b+c = 0$, valamilyen $a \in A; b \in B; c \in C$ elemekkel. Vagyis $c = -(a+b)$, ami lehetetlen, mivel $c \notin -(A + B)$.

6. a.) Tegyük fel, hogy $A_i \neq \mathbb{F}_p$ $i = 1, 2, \ldots, k$ esetén. Ekkor a Cauchy-Davenport lemma miatt

$$|A_{i+1}| \geq 2|A_i| - 1,$$

amiből indukcióval adódik, hogy

$$|A_i| \geq 2^i(|A| - 1) + 1.$$

Továbbá, mivel $|A_k| \leq p$, adódik a felső becslés.

b.) Legyen $A := \{0, 1\}$.

3. fejezet

Az $r_{A+B}(x), r_{A-B}(x)$ és az $E(A,B)$ függvények

Legyen adva két halmaz: A és B. Az összeg- ill. különbséghalmaz reprezentáció függvényén az

$$r_{A\pm B}(x) := \{(a,b) \in A \times B, a \pm b = x\}$$

függvényeket értjük.

A két halmaz *additív energiája* pedig legyen

$$E_{\pm}(A,B) := |\{(a,b,a',b') : a \pm b = a' \pm b'\}|.$$

Világos, hogy $E_+ = E_-$ mivel az egyenletek átrendezéssel egymásba vihetők. Így néha az indexben a $+/-$ jelet el is hagyjuk. Most Z-vel egy véges additív csoportot jelölünk.

3.0.1. Tétel.

$$(a)\ \sum_{x\in Z} r_{A+B}(x) = \sum_{x\in Z} r_{A-B}(x) = |A||B|.$$

$$(b)\ \sum_{x\in Z} r^2_{A+B}(x) = \sum_{x\in Z} r^2_{A-B}(x) = E(A,B).$$

$$(c)\ |A||B| \leq E(A,B) \leq |A||B| \cdot min\{|A|,|B|\}.$$

Bizonyítás:

Az (a) részhez; a definícióból tudjuk, hogy $r_{A\pm B}(x)$ azokat az (a,b) párokat számolja le, melyek összege (különbsége) x. Ha ezt összeadjuk az összes x-re akkor az összes (a,b) párt számláltuk le.

(b) bal oldalán az első összeg E_+ , a második E_-, mint már említettük ezek egyenlők.

(c) Az $a = a'; b = b'$ megoldás, ezért igaz az alsó becslés. Ha a, a', b elemeket rögzítjük, akkor legfeljebb egy b'-re teljesül az egyenlőség. □

3.0.2. Tétel.

$$E(A,B) \geq \frac{|A|^2|B|^2}{|A \pm B|}.$$

Bizonyítás:

Használjuk a Cauchy egyenlőtlenséget:

$$(|A||B|)^2 = \Big(\sum_{x\in Z} r_{A\pm B}(x)\Big)^2 \leq \sum_{x\in Z; r_{A\pm B}(x)\neq 0} 1 \sum_{x\in Z} r^2_{A\pm B}(x) = |A\pm B|E(A,B). \quad \square$$

3.1. Energiák

A bevezetőben definiáltuk az additív (és hasonlóan definiálható multiplikatív) energiát. Maga az elnevezés Terence Tao-tól származik. Az elnevezés magyarázatául ő így szolgált:

"Meg lehet kérdezni, honnan ered az 'energia' elnevezés. Azt hiszem az elnevezéssel homályosan e kifejezés kvadratikus eredetére akartunk utalni, továbbá, hogy monoton (bővebb halmaznak nagyobb az energiája)... Néha úgy képzeltem el, az additív négyeseket, mint 'négy atom kémiai kötését'; az additív energia valami olyan mint e négyes látens energiája".

Amint $A = B$, jelöljük röviden: $E(A) = E(A,A)$. Az $r_{A-B}(x)$ reprezentációs függvényre a $d_{A,B}(x)$ jelölést használjuk. ($A = B$ esetén röviden $d_{A,A}(x) = d_A(x)$ lesz).

2. Definíció (Konvolúciók). *Legyen A egy kommutatív csoport részhalmaza. Legyen*

(I)

$$A \circ A(s) = \sum_y A(y)A(s+y);$$

(II)

$$A * A(s) = \sum_y A(y)A(s-y).$$

ahol $A(x)$ az A halmaz indikátora.

Könnyű látni, hogy $A \circ A(s) = |A \cap (A-s)| = d_A(s)$ és $A * A(s) = |A \cap (s-A)| = r_A(s)$.

3.1.1. Tétel. *1. Egy additív csoportban*

$$E(A,B) \leq \sqrt{E(A) \cdot E(B)}.$$

2. Jelölje $E(A_1,A_2,A_3,A_4)$ azon $a_1 \in A_1, a_2 \in A_2, a_3 \in A_3, a_4 \in A_4$ négyesek számát, melyekre $a_1+a_2 = a_3+a_4$. Ekkor

$$E(A_1,A_2,A_3,A_4) \leq \sqrt[4]{\prod_{i=1}^{4} E(A_i)}.$$

Bizonyítás: 1. Az $a_1+b_1 = a_2+b_2$ egyenlőség ekvivalens az $a_1-a_2 = b_2-b_1$ egyenlőséggel, ezért

$$E(A,B) = \sum_x d_A(x)d_B(x).$$

A Cauchy egyenlőtlenség miatt

$$E(A,B)^2 \leq \sum_x d_A^2(x) \sum_y d_B^2(x) = E(A)E(B)$$

2. $E(A_1,A_2,A_3,A_4) = \sum_x d_{A_1,A_3}(x)d_{A_4,A_2}(x)$. Használjuk a Cauchy egyenlőtlenséget és mivel $\sum_x d^2_{A_i,A_j}(x) = E(A_i,A_j)$ az előző eredményből következik az állítás. □

3.1.2. Tétel. *Legyen G egy additív csoport, $X, Y, B \subseteq G$ véges részhalmazok. Ekkor*

$$\sqrt{E(X \sqcup Y, B)} \leq \sqrt{E(X, B)} + \sqrt{E(Y, B)}$$

ahol $X \sqcup Y$ a két halmaz diszjunkt unióját jelöli.

Bizonyítás:
A diszjunkt únió következményeképpen

$$E(X \sqcup Y, B) = \sum_x (d_{X+B}(x) + d_{Y+B}(x))^2 =$$

$$= \sum_x d^2_{X+B}(x) + \sum_x d^2_{Y+B}(x) + 2\sum_x d_{X+B}(x) d_{Y+B}(x) =$$

$$= E(X, B) + E(Y, B) + 2\sum_x d_{X+B}(x) d_{Y+B}(x) \leq$$

$$\leq E(X, B) + E(Y, B) + 2\sqrt{\sum_x d^2_{X+B}(x)}\sqrt{\sum_x d^2_{Y+B}(x)}$$

a Cauchy egyenlőtlenség miatt. Így

$$E(X \sqcup Y, B) \leq E(X, B) + E(Y, B) + 2\sqrt{E(X, B)}\sqrt{E(Y, B)} =$$

$$= \left(\sqrt{E(X, B)} + \sqrt{E(Y, B)}\right)^2$$

amiből négyzetgyökvonással következik az állítás. □

3.1.1. Konvex sorozatok energiája

Idézzük fel; egy $A = \{a_1 < a_2 < \dots\} \subseteq \mathbb{N}$ sorozat konvex, ha $a_2 - a_1 \leq \dots \leq a_{i+1} - a_i \leq \dots$.

Természetes gondolat, hogy egy konvex sorozat esetében a lehetséges maximális számú négyesek számánál jóval kevesebb "additív négyes" található, azaz jóval kisebb az ilyen halmazok additív energiája, és így az összeg halmaza is nagyobb a minimálisnál.

3.1.3. Tétel. *Legyen $A = \{a_1 < a_2 < \dots\} \subseteq \mathbb{N}$ sorozat konvex. Ekkor bármely $B \subseteq \mathbb{N}$ sorozatra*

$$E(A, B) \ll |A||B|^{3/2}.$$

1. Következmény. *Legyen* $A = \{a_1 < a_2 < \dots\} \subseteq \mathbb{N}$ *sorozat konvex. Ekkor bármely* $B \subseteq \mathbb{N}$ *sorozatra*

$$|A|\sqrt{|B|} \ll |A+B|.$$

Következmény bizonyítása:
Mint láttuk

$$\frac{|A|^2|B|^2}{E(A,B)} \leq |A+B|.$$

A 3.1.3 tétel bizonyítása:
A rövidség kedvéért használjuk a $w := \frac{E(A,B)}{2|A||B|}$ és $r(x) = r_{A+B}(x)$ jelöléseket. Ekkor

$$\sum_{x;r(x)<w} r^2(x) < w \sum_x r(x) = w|A||B| = \frac{E(A,B)}{2}.$$

Most belátjuk, hogy

$$\sum_{x;r(x)\geq w} r^2(x) \ll \frac{|A||B|^2}{w}.$$

A "diadikus szintek" szerint rendezve

$$\sum_{x;r(x)\geq w} r^2(x) = \sum_{k\geq 0} \sum_{x;w2^k\leq r(x)<w2^{k+1}} r^2(x) < (*)$$

A bizonyítás kulcslépése a következő lemma lesz, melyet egy incidencia tételből vezetünk le (lásd a 11.1.6 incidencia tételt a 11. fejezetben)

2. Lemma. *Legyen* $A = \{a_1 < a_2 < \dots < a_n\}$ *valós számok egy konvex sorozata (azaz bármely* $i = 1, 2, \dots, n-1$ *esetén* $a_i - a_{i-1} \leq a_{i+1} - a_i$ *teljesül). Legyen* $B \subseteq \mathbb{R}$ *és* $r(x) = r_{A+B}(x)$*. Ekkor*

$$|\{x : r(x) \geq T\}| \ll \frac{|A||B|^2}{T^3}.$$

Ezt felhasználva

$$(*) < \sum_k w^2 (2^{k+1})^2 \frac{|A||B|^2}{(2^k w)^3} < 8\frac{|A||B|^2}{w}.$$

Most

$$E(A,B) = \sum_{x;r(x)\geq w} r^2(x) + \sum_{x;r(x)<w} r^2(x)$$

így a fenti becsléseket felhasználva

$$\frac{E(A,B)}{2} \leq \sum_{x;r(x)\geq w} r^2(x) < 8\frac{|A||B|^2}{w} = 8\frac{|A||B|^2}{E(A,B)/2|A||B|},$$

amiből

$$E(A,B) \leq 8|A||B|^{3/2}. \quad \square$$

3.1.2. Magasabb rendű energiák

Az előzőekben láttuk, hogy $E(A,B) = \sum_x d^2_{A,B}(x)$; azaz $E(A,B)$ azon négyesek számát számlálja, melyekre $a-b = a'-b'$.

Sejthető, hogy egy $\sum_x d^s_A(x)$ alakú összeg még pontosabb információt ad egy adott A halmaz struktúrájáról. Hasonló érvvel a $\sum_x d^s_A(x)$ azokat a $2s$-eseket számlálja, melyekre $a_1 - a'_1 = a_2 - a'_2 = \cdots = a_s - a'_s$. Még általánosabban az s-edik energiát racionális $s-$ekre is definiálhatjuk:

$$E_s(A) := \sum_x d^s_A(x);\ s \in \mathbb{Q}^+.$$

Használjuk a következő jelöléseket:

Legyen $\underline{s} = \{s_1, \ldots, s_{k-1}\}$ egy G kommutatív csoport $(k-1)$-ese. Vezessük be az $A_{\underline{s}} := A \cap (A - s_1) \cap \cdots \cap (A - s_{k-1})$ jelölést.

3.1.4. Tétel.

(a) Bármely $s,t \in A - A$ esetén $A_s \circ A_s(t) = A_t \circ A_t(s)$.

(b) $\sum_s E(A, A_s) = E_3(A)$.

(c)

$$E_k(A) := \sum_{s_1,\ldots,s_{k-1}\in G} |A_{\underline{s}}|^2.$$

(d) Legyen $|A-A| = K|A|$. Ekkor

$$E_s \geq \frac{|A|^{s+1}}{K^{s-1}}.$$

(e)

$$\sum_{s,t\in A-A} E(A_s, A_t) = E_4(A).$$

(f) Jelölje $\underline{w} = \{w_1, \ldots, w_n\}$ *mellett* $|\underline{w}| = n$. *Ekkor*

$$\sum_{|\underline{s}|=k-1,|\underline{t}|=n-1} E(A_{\underline{s}}, A_{\underline{t}}) = E_{k+n}(A).$$

(g)

$$\frac{|A|^6}{2E_3(A)} \leq \sum_s |A + A_s|.$$

Bizonyítás:
(a) Az $A_s \circ A_s(t) = A_t \circ A_t(s)$ állítást úgy is írhatjuk, hogy $d_{A_s}(t) = d_{A_t}(s)$. Most vegyük észre, hogy mivel $A_s(x) = A(x)A(x+s)$, ezért

$$A_s(x)A_s(x+t) = A(x)A(x+s)A(x+t)A(x+t+s) =$$

$$A(x)A(x+t)A(x+s)A(x+s+t) = A_t(x)A_t(x+s),$$

így

$$d_{A_s}(t) = \sum_x A_s(x)A_s(x+t) = \sum_x A_t(x)A_t(x+s) = d_{A_t}(s).$$

(b) Mivel bármely X, Y halmazokra $\sum_r d_{XY}^2(r) = \sum_r d_X(r)d_Y(r)$, ezért

$$E(A, A_s) = \sum_x d_A(x)d_{A_s}(x),$$

és így

$$\sum_s E(A, A_s) = \sum_s \sum_x d_A(x)d_{A_s}(x) = \sum_x d_A(x) \sum_s d_{A_s}(x).$$

Most

$$d_{A_s}(x) = \sum_y A_s(y)A_s(x+y) = \sum_y A(y)A(y+s)A(y+x)A(y+x+s).$$

Ezért megcserélve az összegzést és előre írva az s-től nem függő tagokat

$$\sum_s d_{A_s}(x) = \sum_y A(y+x)A(y) \sum_s A(y+s)A(y+x+s) = d_A(x) \cdot d_A(x),$$

így

$$\sum_s E(A, A_s) = \sum_x d_A(x)^3 = E_3(A).$$

(c) $A_{\underline{s}}$–be azokat az $a \in A$ elemeket számoljuk le, amelyekre $a + s_1, a + s_2, \ldots, a + s_k \in A$ is teljesül. Így $|A_{\underline{s}}|^2$–ban azokat az (a, a') párokat számoljuk le, melyekre $a' + s_1, a' + s_2, \ldots, a' + s_k \in A$, így viszont $(a, a', a + s_1, a' + s_1, \ldots, a + s_k, a' + s_k)$ olyan $2k$–as, melyre

$$a - a' = (a + s_1) - (a' + s_1) = \cdots = (a + s_k) - (a' + s_k),$$

azaz ezeket $E_k(A)$–ban számoljuk.

(d) Mivel $|A|^2 = \sum_{x \in A-A} d(x)$, ezért a Hölder egyenlőtlenség miatt

$$|A|^2 \leq \Big(\sum_{x \in A-A} 1^{\frac{s}{s-1}} \Big)^{1-1/s} \Big(\sum_{x \in A-A} d^s(x) \Big)^{1/s}.$$

s–edik hatványra emelve és használva, hogy $E_s(A) := \sum_x d_A^s(x)$, valamint, hogy $|A - A| = K|A|$, kapjuk az állítást.

(e) Az $E(A_s, A_t)$–ben azokat az $(a_1, b_1, a_2, b_2) \in A^4$ négyeseket számoljuk le, amelyekre igaz, hogy $a_1 + s, a_2 + s, b_1 + t, b_2 + t \in A$, és amelyekre $a_1 - b_1 = a_2 - b_2$. De így $(a_1, b_1, a_2, b_2, a_1 + s, a_2 + s, b_1 + t, b_2 + t) \in A^8$ olyan nyolcas, melyre

$$a_1 - a_2 = b_1 - b_2 = (a_1 + s) - (a_2 + s) = (b_1 + t) - (b_2 + t),$$

azaz $E_4(A)$-ben számlált elem.

(f) Az $A_{\underline{s}}$–ben, $|\underline{s}| = k - 1$, azokat az $a_1 \in A$ elemeket számoljuk le, amelyekre $a_1 + s_1, a_1 + s_2, \ldots, a_1 + s_{k-1} \in A$, hasonlóan $A_{\underline{t}}$–ben, $|\underline{t}| = n - 1$, azokat az $a_1' \in A$ elemeket számoljuk le, amelyekre $a_1' + t_1, a_1 + t_2, \ldots, a_1 + t_{n-1} \in A$.

Most $E(A_{\underline{s}}, A_{\underline{t}})$–ben az $a_1, a_2 \in A_{\underline{s}}$, és $a_1', a_2' \in A_{\underline{t}}$, négyeseket számoljuk le, amelyekre $a_1 - a_1' = a_2 - a_2'$. De ekkor

$$a_1 - a_2 = a_1' - a_2' = (a_1 + s_1) - (a_2 + s_1) = (a_1' + t_1) - (a_2' + t_1) = \ldots$$

$$\cdots = (a_1 + s_{k-1}) - (a_2 + s_{k-1}) =$$

$$= (a_1' + t_{n-1}) - (a_2' + t_{n-1})$$

összesen $2(k + n)$ elemet számolunk le, azaz éppen $E_{k+n}(A)$–t számoljuk.

(g) A Cauchy-egyenlőtlenség miatt

$$|A||A_s| = \sum_x d_{A,A_s}(x) \leq \sqrt{E(A,A_s)}\sqrt{|A+A_s|}.$$

Így négyzetre emelve, $s-$re összegezve és használva megint a Cauchy-egyenlőtlenséget, valamint, hogy $\sum_s |A_s| = |A|^2$

$$|A|^6 \leq \sum_s E(A,A_s) \sum_s |A+A_s|.$$

A b.) pontban láttuk, hogy $\sum_s E(A,A_s) = E_3(A)$, amivel bizonyítottuk az állítást. □

Feladatok

1. Legyen az A sorozat konvex. Bizonyítsuk be, hogy

$$|A+A-A| \gg |A|^2.$$

Megoldások

1. Legyen $1 < i \leq n$, ahol $n = |A|$. Tekintsük az összes $1 \leq j < i \leq n$ (i,j) párra az $a_i + a_{j+1} - a_j \in A+A-A$ kifejezést. Ekkor

$$a_i < a_i + a_{j+1} - a_j < a_{i+1}$$

ahol az első az A sorozat szigorú monotonitásából, a második egyenlőtlenség pedig ekvivalens az

$$a_{j+1} - a_j \leq a_{i+1} - a_i$$

egyenlőtlenséggel, ami a $j < i$ feltétel miatt a konvexitásból következik. Az-az $a_i + a_{j+1} - a_j$ számok mind az (a_i, a_{i+1}) intervallumba esnek, továbbá ugyancsak a konvexitás miatt

$$a_i + a_{j+1} - a_j = a_i + a_{k+1} - a_k$$

pontosan akkor, amikor $j = k$.Tehát

$$|A+A-A| \geq \sum_{i=1}^{n}(i-1) = \frac{|A|(|A|-1)}{2}$$

amiből következik az állítás.

4. fejezet

Plünnecke-Ruzsa tétel

4.1. Távolság tételek

4.1.1. Tétel. *Adott három halmaz $C, D, X \subseteq G$. Ekkor*

$$|C - D||X| \leq |C - X||X - D|.$$

Bizonyítás:

Ha a $C - D$ halmazban egy különbségnek több előállítása van, akkor ezek közül jelöljünk ki egyet (véges halmazokról van szó, sorszámozva az elemeket pl. a legkisebb indexű elemet a különbség két tagja közül). Mivel

$$\{(C - x) \times (x - D); x \in X\} \subseteq (C - X) \times (X - D)$$

és

$\forall x \in X$ teljesül, hogy $c - d = c - x + x - d$, ezért

$$|C - X||X - D| = |(C - X) \times (X - D)| \geq$$

$$\geq |\{(C - x) \times (x - D); x \in X\}| = |X||C - D|. \quad \square$$

Ezt és a következő tételt Freiman egy érdekes kérdése motiválta:

Freiman: Igaz-e?

(i) Ha $|A+A| \leq K_1|A|$ akkor $\exists K_1' = K_1'(K_1)$, hogy $|A-A| \leq K_1'|A|$.
(ii) Ha $|A-A| \leq K_2|A|$ akkor $\exists K_2' = K_2'(K_2)$, hogy $|A+A| \leq K_2'|A|$.

A sejtés elég természetes; a "kis" összeg ill. különbséghalmazt "számtani sorozat jellegű" halmazoknál várjuk, ahol valóban igaz (i) és (ii).

A 4.1.1. és a következő 4.1.2. tételből mindkét kérdésre igenlő a válasz (lásd a fejezet végén a 3. és 4. feladatokat).

4.1.2. Tétel. *$\forall A, B, C, D \subseteq G$ esetén igazak az*

$$|A||B||C-D| \leq |A-C||B-D||A+B|$$

és az

$$|A||B||C-D| \leq |A-C||B-D||A-B|.$$

becslések

A 4.1.2 tétel bizonyítása egy kicsit komplikáltabb. Először az

$$|A||B||C-D| \leq |A-C||B-D||A+B|$$

becslést igazoljuk.

Szükségünk van a következő lemmára:

Lemma: *$\forall A, B \subseteq G$ esetén $\exists m \in G$, hogy*

$$r_{A-B}(m) \geq \frac{|A||B|}{|A+B|}$$

Megjegyzés: Jegyezzük meg, hogy az $r_{A-B}(m) \geq \frac{|A||B|}{|A+B|}$ becslés helyett az $r_{A+B}(m) \geq \frac{|A||B|}{|A+B|}$ becslés triviális lenne; ez utóbbi azt jelentené, hogy az átlagosnál ($|A||B|/|A+B|$) nem kisebb reprezentációs érték is van.

A Lemma bizonyítása:

A 3.0.2 tétel miatt

$$\frac{|A|^2|B|^2}{|A+B|} \leq \sum_x r^2_{A+B}(x) = \sum_y r^2_{A-B}(y) \leq$$

$$\leq \max_y r_{A-B}(y) \sum_y r_{A-B}(y) = \max_y r_{A-B}(y)|A||B|. \square$$

A 4.1.2 Tétel bizonyítása:

Vegyük észre, hogy

$$r_{A-B}(m) = |A \cap (m+B)|.$$

Továbbá alkalmazzuk az 4.1.1 tételt az

$$X := A \cap (m+B)$$

halmazzal és vegyük észre, hogy

$$|C - (A \cap (m+B))| \leq |A - C|$$

valamint

$$|(A \cap (m+B)) - D| \leq |B - D|$$

és alkalmazzuk a lemmát.

Az $|A||B||C-D| \leq |A-C||B-D||A-B|$ becslésnél az egyszerűbb $r_{A-B}(m) \geq \frac{|A||B|}{|A-B|}$ becslést használjuk. $\square$

Feladatok

1.(Bourgain) Legyen $A_1, A_2, A_3 \subseteq G$. Tegyük fel, hogy

$$|A_1 \cap A_3| \geq \frac{|A_1|}{K}, \quad |A_2 \cap A_3| \geq \frac{|A_2|}{K},$$

és

$$|A_i + A_i| \leq K|A_i| \quad i = 1, 2, 3.$$

Ekkor

$$|A_1 + A_2| \leq K^5|A_3|.$$

2. Bizonyítsuk be, hogy Freiman (i) kérdésére a válasz igen!

3. Bizonyítsuk be, hogy ha $K \geq 2$, és

$$|A - B| \leq K\sqrt{|A||B|}$$

teljesül, akkor igazak az

$$|A + B| \leq K^3\sqrt{|A||B|}; \qquad DB(A) \leq K^4$$

becslések, ahol $DB(A) := |A + A|/|A|$.

Vezessük le ebből Freiman (ii) állítását!

4. Legyen $A, B \subseteq G$, A és B távolságán a

$$d(A, B) = \log \frac{|A - B|}{\sqrt{|A|}\sqrt{|B|}}$$

kifejezést értjük.

Bizonyítsuk be a háromszög-egyenlőtlenséget!

Metrika-e d?

5. a.)

$$d(A, B) \leq \frac{1}{2}\log|A| + \frac{1}{2}\log|B|.$$

b.)

Egyenlőség akkor és csak akkor, ha

$$d(A, -B) = \frac{1}{2}\log|A| + \frac{1}{2}\log|B|.$$

6. Legyen $G, H \subseteq Z$, ahol G, H részcsoportok Z csoportban. Ekkor a.)

$$d(G, H) = \log \frac{\sqrt{|G|}\sqrt{|H|}}{|G \cap H|}.$$

b.) Bizonyítsuk be, hogy

$$d(G, H) = d(G, G + H) + d(G + H, H) = d(G, G \cap H) + d(G \cap H, H).$$

7.

$$d(A+C,B+D) \geq d(A,B) - \frac{1}{2}\log|C||D|.$$

8. a.) Legyen $S \subseteq G$. Bizonyítsuk be, hogy bármely $n \in \mathbb{N}$ egészre

$$|nS| \geq |S|^{\frac{1}{2^{n-1}}}|S-S|^{1-\frac{1}{2^{n-1}}}.$$

b.) Tegyük fel, hogy $S \subseteq \mathbb{Z}_p$ (p prímszám) melyre $S-S=\mathbb{Z}_p$. Igazoljuk, hogy ekkor van olyan $m \in \mathbb{N}$, $m=o(p)$, melyre $mS=\mathbb{Z}_p$. Adjunk felső becslést $m-$re.

9. Legyen $A \subseteq \mathbb{F}_2^n$ az $n-$dimenziós $\mathbb{F}_2$ feletti vektortér olyan részhalmaza, melyre $|A+A+A| \leq K|A|$. Igazoljuk, hogy akkor bármely $m \geq 3$ esetén $|mA| \leq K^{m-2}|A|$.

10. Bizonyítsuk be, hogy bármely $x \in G$ elemre $r_{A+B}(x)|A+B| \leq |A-B|^2$.

11. Legyen G egy véges abel csoport. Ekkor bármely $c \in \mathbb{R}$ esetén

$$\sum_{g\in G}(r_A(g)-c)^2 \geq \frac{|G||A|^2}{|G|-1}\Big(1-\frac{|A|}{|G|}\Big)^2.$$

Megjegyzés: Ez az állítás tulajdonképpen a végtelen természetes számok sorozatáról szóló *Erdős-Fuchs tétel* véges analogonja.

Megoldások

1. A második távolságtétel szerint

$$|U||V||X-Y| \leq |X-U||Y-V||U-V|.$$

Legyen

$$U := A_1 \cap A_3; \quad V := -(A_2 \cap A_3) \quad X := -A_1; Y = A_2.$$

Ekkor

$$|A_1 \cap A_3||-(A_2 \cap A_3)||-A_1-A_2| \leq |-A_1-(A_1 \cap A_3)||A_2+(A_2 \cap A_3)||(A_1 \cap A_3)+(A_2 \cap A_3)|,$$

azaz

$$|A_1 \cap A_3||A_2 \cap A_3||A_1 + A_2| \leq |A_1 + (A_1 \cap A_3)||A_2 + (A_2 \cap A_3)||(A_1 \cap A_3) + (A_2 \cap A_3)|.$$

Így a feladat feltételeiből

$$\frac{1}{K^2}|A_1||A_2||A_1 + A_2| \leq |A_1 \cap A_3||A_2 \cap A_3||(A_1 \cap A_3) + (A_2 \cap A_3)| \leq$$

$$\leq |(A_1 \cap A_3) + A_1||(A_2 \cap A_3) + A_2||(A_1 \cap A_3) + (A_2 \cap A_3)| \leq$$

$$\leq |A_1 + A_1||A_2 + A_2||A_3 + A_3| \leq K|A_1|K|A_2|K|A_3|,$$

amiből

$$|A_1 + A_2| \leq K^5|A_3|.$$

2. Használjuk az első távolságtételt az $X = -A; C = D = A$ mellett. Ekkor $K_1' = K_1^2$.

3. A második távolságtétel miatt $|U||V||X - Y| \leq |X - U||Y - V||U + V|$ egyenlőtlenségben legyen $U = -Y = B;\ X = -V = A$. Ekkor

$$|B|| - A||A + B| \leq |A - B|| - B + A||B - A| =$$

$$= |A - B|^3 \leq K^3(|A||B|)^{3/2}.$$

$|A||B|-$vel egyszerűsítve megkapjuk az első állítást.

Az első távolságtétel miatt

$$\frac{|A + A|}{|A|} \leq \frac{|A - B||A + B|}{|A||B|} \leq \frac{K\sqrt{|A||B|}K^3\sqrt{|A||B|}}{|A||B|} = K^4.$$

Végül Freiman (ii) az $A = B$ választással a $K_2' = K_2^3$ mellett igaz.

4. A $d(\cdot, \cdot)$ szimmetrikus, a háromszögegyenlőtlenség az első távolságtétellel ekvivalens, $d = 0$ akkor és csak akkor, ha $|A - A| = |A|$ ami, mint láttuk azt jelenti, hogy A az általa generált csoportnak valamely részcsoportjai szerinti mellékosztályok uniója. Azaz nem metrika.

Kis változtatással azzá tehető (megadásos távolságfüggvényt kell definiálni).

5. a.) A definició és $|A - B| \leq |A||B|$ következménye.

b.)

$|A-B|=|A||B|$ nyilván akkor és csak akkor,ha $|A+B|=|A||B|$.

6. a.)

$$d(G,H)=\log\frac{|G-H|}{\sqrt{|G|}\sqrt{|H|}}=\log\frac{\sqrt{|G|}\sqrt{|H|}}{|G\cap H|},$$

azzal ekvivalens, hogy

$$|G||H|=|G-H||K|,$$

ahol $K=G\cap H$. Ez pedig ekvivalens a

$$|G/K||H/K|=|G/K-H/K|$$

állítással, azaz elég a $K=0$ esetet igazolni, vagyis hogy

$$|G||H|=|G-H|.$$

A

$$g_1-h_1=g_2-h_2,$$

$$g_1-g_2=h_1-h_2\in G,H$$

feltétellel azonos, azaz $g_1-g_2=h_1-h_2=0$. Minden különbség különböző.

b.)

Az a.) miatt

$$d(G,H)=d(G,G+H)+d(G+H,H)$$

igazolásához kell, hogy

$$\log\frac{\sqrt{|G|}\sqrt{|H|}}{|G\cap H|}=\log\frac{\sqrt{|G|}\sqrt{|G+H|}}{|G\cap(G+H)|}+\log\frac{\sqrt{|G+H|}\sqrt{|H|}}{|(G+H)\cap H|},$$

és mivel $(G+H)\cap H=H$, $G\cap(G+H)=G$, azt kell igazolni, hogy

$$\frac{\sqrt{|G|}\sqrt{|H|}}{|G\cap H|}=\frac{\sqrt{|G|}\sqrt{|G+H|}}{|G|}\cdot\frac{\sqrt{|G+H|}\sqrt{|H|}}{|H|},$$

amiből

$$|G||H|=|G+H||K|,$$

ám a.)-ban igazoltuk, hogy $|G||H| = |G-H||K|$, és nyilván $G+H = G-H$, G, H részcsoportok.

A

$$d(G,H) = d(G, G\cap H) + d(G\cap H, H),$$

egyenlőséghez kell, hogy

$$\frac{\sqrt{|G|}\sqrt{|H|}}{|G\cap H|} = \frac{\sqrt{|G|}\sqrt{|H|}}{|K|} = \frac{\sqrt{|G|}\sqrt{|K|}}{|K|}\cdot\frac{\sqrt{|H|}\sqrt{|K|}}{|K|}.$$

7. Átírva azt kell igazolni, hogy

$$\frac{|A-B|}{\sqrt{|A|}\sqrt{|B|}\sqrt{|C|}\sqrt{|D|}} \le \frac{|(A-B)+(C-D)|}{\sqrt{|A+C|}\sqrt{|B+D|}}.$$

A számlálókra külön igaz a becslés, a nevezőkben azt használjuk, hogy $|A+C| \le |A||C|$, illetve $|B+D| \le |B||D|$.

8. A 4.1.1 tételt $C = D = T; X = -S$ választással alkalmazva

$$|T-T||-S| \le |T-(-S)||-S-T|,$$

amiből

$$|S+T| \ge \sqrt{|S|}\sqrt{|T-T|}.$$

Most indukcióval igazolni fogjuk, hogy $n \ge 2$ esetén

$$|nS| \ge |S|^{\frac{1}{2^{n-1}}}|S-S|^{1-\frac{1}{2^{n-1}}}.$$

$n = 2$ esetén az előbb említett becslés adódik $S = T$ mellett. Az indukciós feltevést és az $n = 2$ esetet felhasználva kapjuk, hogy

$$|(n+1)S| = |nS+S| \ge |nS|^{1/2}|S-S|^{1/2} \ge$$

$$\ge (|S|^{\frac{1}{2^{n-1}}}|S-S|^{1-\frac{1}{2^{n-1}}})^{1/2}|S-S|^{1/2} =$$

$$|S|^{\frac{1}{2^n}}|S-S|^{1-\frac{1}{2^n}}.$$

b.) Mivel $S-S = \mathbb{Z}_p$ azt kapjuk, hogy $p = |S-S| \le |S|^2$ és így $|S| \ge \sqrt{p}$. Az a.) miatt

$$|nS| \ge |S|^{\frac{1}{2^{n-1}}}|S-S|^{1-\frac{1}{2^{n-1}}} \ge p^{\frac{1}{2^n}}p^{1-\frac{1}{2^{n-1}}} = p^{1-\frac{1}{2^n}}.$$

Így, ha $n = \lceil \log_2 \log_2 p \rceil$ akkor $|nS| > \frac{p}{2}$. Ekkor Cauchy-Davenport tétel miatt $|2nS| = p$. Tehát van olyan $m \leq 2\lceil \log_2 \log_2 p \rceil$ melyre $mS = \mathbb{Z}_p$.

9. m szerinti indukcióval; $m = 3$-ra éppen a feltétellel azonos az állítás. Legyen $m \geq 4$, és jegyezzük meg, hogy $\mathbb{F}_2^n$-ben a távolságtétel a

$$|Y + Z| \leq \frac{|X + Z||Y + Z|}{|X|}$$

formában is felírható (bármely U-ra $U = -U$). Legyen $Y = 2A$, $Z = (m-1)A$ és $X = A$. Ekkor

$$|(m+1)A| = |2A + (m-1)A| \leq \frac{|A + (m-1)A||A + A + A|}{|A|} =$$

$$= \frac{|mA||A + A + A|}{|A|} \leq K^{m-2}|A|K = K^{m-1}|A|$$

az indukciós feltétel miatt és a hármas összegre vonatkozó feltétel miatt.

10. $r_{A+B}(x) = |\{(a_i, b_i) : x = a_i + b_i\}$. Írjuk fel $|A + B|$ elemeit egyértelműen (pl. lexikografikusan sorszámozva az elemeket a legkisebb indexűeket véve). Legyen $\phi : (a_i, b_i, a + b) \mapsto (a_i - b, a - b_i) \in (A - B)^2$. Tegyük fel, hogy $\phi(a_i, b_i, a + b) = (a_i - b, a - b_i)$ és $\phi(a_i', b_i', a' + b') = (a_i - b, a - b_i)$ is teljesül. Ekkor

$$a_i - b = a_i' - b'; \quad a - b_i = a' - b_i' \quad a_i + b_i = a_i' + b_i'.$$

A második egyenlőtlenségből kivonva az elsőt és felhasználva a harmadikat, azt kapjuk, hogy $a+b = a'+b'$ amiből az egyértelműség miatt $a = a'; \quad b = b'$. Ezeket felhasználva $a_i = a_i'$ és $b_i = b_i'$ következik. Tehát ϕ injektív, amiből az állításunk is következik.

11. A bizonyítandó becslés bal oldalának, mint c függvényének könnyen láthatóan a $c = |A|^2/|G|$-ben van a minimuma, így

$$\sum_{g \in G} (r_A(g) - c)^2 \geq \sum_{g \in G} r_A^2(g) - \frac{|A|^4}{|G|}.$$

Most a Cauchy egyenlőtlenséget alkalmazva

$$\Big(\sum_{0 \neq g \in G} r_A(g) \Big)^2 \leq (|G| - 1) \sum_{0 \neq g \in G} r_A^2(g).$$

Felhasználva, hogy $\sum_{g\in G} r_A^2(g) = \sum_{g\in G} d_A^2(g)$ (d a di□erencia reprezentációs függvény), továbbá $d_A^2(0) = |A|^2$, kapjuk a Cauchy becsléssel, hogy

$$\sum_{g\in G} r_A^2(g) - \frac{|A|^4}{|G|} = \sum_{0\neq g\in G} r_A^2(g) + |A|^2 - \frac{|A|^4}{|G|} \geq$$

$$\geq \frac{1}{|G|-1}\Big(\sum_{0\neq g\in G} r_A(g)\Big)^2 + |A|^2 - \frac{|A|^4}{|G|} =$$

$$= \frac{1}{|G|-1}\Big(|A|^2 - |A|\Big)^2 + |A|^2 - \frac{|A|^4}{|G|}$$

és amiből négyzetre emeléssel és rendezéssel kapjuk az állítást.

4.2. Plünnecke-Ruzsa tétel

Az előző fejezet 3. és 4. feladata Freiman egy kérdésére adta meg a választ; a "nehezebb" kérdésre, ami szerint, ha $|A-A| \leq K|A|$, akkor azt kaptuk, hogy $|A+A| \leq K^3|A|$. A kérdés, javítható-e a K^3? A válasz igenlő, az alábbi tétel általánosabb formájával javítható.

4.2.1. Tétel. *Ha* $|A_0 + B| \leq K_0|A_0|$, *akkor bármely* $k, h \in \mathbb{N}^+$ *esetén*

$$|kB - hB| \leq K_0^{k+h}|A_0|.$$

A $kA, (hA), ...$ majd az A elemeiből képzett k-tagú (h-tagú...) összegeket jelenti.

Bizonyítás nélkül megjegyezzük, hogy létezik a 4.1. Tétel egy erősebb változata, melyet sok esetben tudunk használni:

4.2.2. Tétel. *Legyenek egy kommutatív csoport részhalmazai* $A_0, B_1, B_2, \ldots, B_k$. *Ekkor létezik olyan nem üres* $A \subseteq A_0$, *hogy*

$$|A + B_1 + B_2 + \cdots + B_k| \leq \prod_{i=1}^{k} (|A_0 + B_i|/|A_0|) \cdot |A|.$$

Sőt, van olyan $A \subseteq A_0$, *hogy* $|A| > |A_0|/2$.

Legyen most $k = 2$, és $B_1 = B_2 = -A$. Ekkor

$$|A + A| = |-A - A| \leq |A - A - A| \leq \frac{|A - A|}{|A|} \cdot \frac{|A - A|}{|A|}|A| = K^2|A|.$$

Tehát Freiman kérdésére a javítás:

$$|A - A| \leq K|A| \Rightarrow |A + A| \leq K^2|A|.$$

A későbbi fejezetekben látunk példát, amikor ezt az erősebb változatot kell használnunk.

Ezt a tételt először Plünnecke, majd általánosítva, gráfelméleti tételt (Menger-tétel) alkalmazva Ruzsa bizonyította. A most következő egy igen rövid bizonyítás a 4.2.1 Tételre, mely Petridistől származik.

A 4.2.1 Tétel bizonyítása:

Legyen $A_0, B \subseteq Z$, amelyre $|A_0 + B| \leq K_0|A_0|$, és legyen $A \subseteq A_0$, az a nem üres részhalmaz, amelyre a $|A + B|/|A|$ értéke a legkisebb és jelölje e hányados értékét K. Így bármely $Y \subseteq A_0$,

$$|Y + B| \geq K|Y|$$

és így nyilván $K \leq K_0$.

Lemma: *Bármely C-re*

$$|A + B + C| \leq K|A + C|.$$

Ebből már következik a tétel, ugyanis n szerinti indukcióval azt kapjuk, hogy

$$|A + nB| \leq K^n|A|,$$

azaz megkaptuk az általánosabb tételt a $B_1 = \cdots = B_k := B$ esetén (Azt nem, hogy $|A| > |A_0|/2$). Továbbá az 4.1.1 Tétel miatt

$$|-A||kB - hB| \leq |A + kB||A + hB| \leq K^{k+h}|A|^2,$$

így

$$|kB - hB| \leq |A + kB||A + hB| \leq K^{k+h}|A| \leq K_0^{k+h}|A_0|.$$

A lemma bizonyítása:

$|C|$ szerinti indukcióval történik: ha $C = \{y\}$, akkor a feltétel miatt

$$|A + B + y| \leq K|A + y|.$$

Tegyük fel, hogy $C' = C \cup \{x\}$ és hogy

$$|A + B + C| \leq K|A + C|.$$

Most egy kicsit ügyesebben kell eljárnunk. Ha csak azt használnánk fel, hogy

$$A + B + C' = (A + B + C) \cup (A + B + x),$$

akkor $A + B + C'$ elemszámát az unió két tagjának elemszámának összegével becsülhetnénk felül, ami túl durva becslés. Vannak ugyanis a második halmazban olyan elemek, amelyek az első halmazban is benne vannak. Ezért legyen

$$Z := \{a \in A : a + B + x \subseteq A + B + C\} \subseteq A.$$

Ekkor

$$A + B + C' = (A + B + C) \cup [(A + B + x) \setminus (Z + B + x)]$$

és mivel $Z \subseteq A$, ezért $|Z + B| \geq K|Z|$.
Így

$$|A + B + C'| \leq |A + B + C| + |A + B + x| - |Z + B + x| =$$

$$= |A + B + C| + |A + B| - |Z + B| \leq (*)$$

az indukciós feltevés miatt és $Z-$re vonatkozó becslés miatt

$$(*) \leq K|A + C| + K|A| - K|Z|.$$

Ha még igazoljuk, hogy

$$|A + C| + |A| - |Z| \leq |A + C'|,$$

akkor a lemma bizonyítása kész.

Most $A + C'$ elemszámát becsüljük meg. Hasonlóan, mint az előbbi lépésnél legyen

$$W := \{a \in A : a + x \in A + C\} \subseteq A,$$

ekkor, mint az előbb

$$A + C' = (A + C) \cup ((A + x) \setminus (W + x))$$

és így

$$|A + C'| = |A + C| + |A + x| - |W + x| = |A + C| + |A| - |W|.$$

Mivel minden $a \in W$ elemre $a + x \in A + C$, így $a + x + B \subseteq A + B + C$, azaz $W \subseteq Z$ is teljesül kapjuk, hogy

$$|A + C'| \geq |A + C| + |A| - |Z|. \qquad \square$$

Egy szép alkalmazást mutatunk most.

4.2.3. Tétel. *Létezik végtelen sok n, A és B halmazok úgy, hogy $|A| = n$, $|A + B| \leq 3n$ és bármely $X \subseteq A$ halmazra*

$$|X - B| \geq \frac{\log n}{\log 8}|X|.$$

Másfelöl ha $|A + B| \leq K|A|$, akkor van olyan $X \subseteq A$ halmaz, hogy

$$|X - B| \leq Ke^{2\sqrt{\log K \log n}}|X|.$$

Megjegyzés:

A 4.2.3 tételben a két állítás "csaknem" kiegészítő állítások, tehát majdnem leírják a jelenséget. A "csaknem" kijelentésre jegyezzük meg a következő becsléssort:

$$(\log x)^M \prec e^{c\sqrt{\log x}} \prec x^{\varepsilon}$$

ahol $f(x) \prec g(x)$ jelentse azt, hogy $f(x)/g(x) \to 0$, amint $x \to \infty$ és a fentiek úgy értendők, hogy minden nagy M-re kis ε és $0 < c < 1$ esetén van olyan x_0, hogy $x > x_0$ esetén ezek teljesülnek. A fenti becsléssort a L'Hospital-szabály segítségével könnyen bizonyíthatjuk.

Tehát a fenti tételben ugyan $\log n$ és $e^{\sqrt{\log n}}$ különböző nagyságrendűek, mégis jóval n akármilyen kis hatványán belül maradnak, azaz a két becslés nincs túl távol egymástól.

A tétel első felének a bizonyításához használni fogjuk a következő trükköt, az úgynevezett *projekciós módszert*:

Elég egy összeg-különbség tételt a $\mathbb{Z}^d$ rács A és B részhalmazain bizonyítani. Azaz ha valamely $A, B \subseteq \mathbb{Z}^d$ halmazokra igaz, hogy

$$|kA + mB| = f(|A|, |B|),$$

akkor van olyan $A', B' \subseteq \mathbb{Z}$ is, hogy

$$|kA' + mB'| = f(|A'|, |B'|).$$

Ehhez az A, B halmazokat csak le kell vetíteni egy alkalmas módon.

Könnyű látni, hogy az $\underline{x} = (x_1, x_2, \ldots, x_d) \in \mathbb{Z}^d$,

$$(x_1, x_2, \ldots, x_d) \mapsto x_1 + x_2 \cdot M + \cdots + x_d M^{d-1}$$

vetület, ha M elég nagy, akkor $A + B$ művelettartóan izomorf (Freiman-izomorf) $A' + B'$-vel.

4.2.3 Tétel bizonyítása:

Az állítás első felét igazoljuk először.

Az $A, B \subseteq \mathbb{Z}^d$ halmazokat definiáljuk így: álljon B halmaz az egységvektorokból, tehát legyen $B := \{b = (0, \ldots, 0, 1, 0, \ldots 0)\}$ (tehát egy koordináta 1, a többi 0) és legyen A halmaz azon vektorok halmaza, amelyeknek a koordinátái nemnegatív egészek és az összegük k, ahol $d = 2k$. Ezek szerint $A+B$ azon vektorok halmaza, amelyeknek a koordinátái nem negatív egészek és az összegük $k+1$. Elemszámaikat az ismétléses kombináció segítségével adhatjuk meg:

$$|A| = \binom{d+k-1}{d-1} \quad |A+B| = \binom{d+k}{d-1}.$$

Így

$$\frac{|A+B|}{|A|} = \frac{d+k}{k+1} = \frac{3k}{k+1} < 3.$$

Legyen $X \subseteq A$. Az A-beli vektoroknál legalább $d-k$ helyen 0 áll, így X vektorainál is. Az $X-B$ halmazban tehát benne vannak azok a vektorok is, ahol a legalább $d-k$ hely egyikén -1 áll, a többi helyen nem negatív és és az összegük k. Ezen vektoroknál tehát egy $x-b$ vektorból egyértelműen visszakövetkeztethetünk x és b vektorokra (azaz ez egy injektív megfeleltetés). Ezért tehát

$$|X-B| \geq (d-k)|X|.$$

Végül

$$n = |A| = \binom{d+k-1}{d-1} = \binom{3k-1}{2k-1} < 2^{3k} = 8^k.$$

Tehát

$$|X-B| \geq (d-k)|X| = k|X| > \frac{\log n}{\log 8}|X|. \quad \square$$

Most rátérünk a másik állítás igazolására.

A Plünnecke-Ruzsa általánosabb tételből tudjuk, hogy létezik $X \subseteq A$, hogy bármely $j \in \mathbb{N}$ esetén

$$|X+jB| \leq K^j|X|.$$

Az 4.1.1. tétel (háromszög egyenlőtlenség) miatt

$$|X-B| \leq \frac{|X+jB||(j+1)B|}{|jB|} \leq \frac{|(j+1)B|}{|jB|}K^j|X| \tag{4.1}$$

teljesül. Legyen $N \in \mathbb{N}$ és jelölje

$$\lambda := \min_{1 \leq j \leq N} \frac{|(j+1)B|}{|jB|}.$$

Ekkor tehát minden j-re $1 \leq j \leq N$ re

$$\lambda \leq \frac{|(j+1)B|}{|jB|}.$$

Szorozzuk össze ezeket az egyenlőtlenségeket, kapjuk, hogy

$$\lambda^N \leq \prod_{i=1}^{N} \frac{|(i+1)B|}{|iB|} = \frac{|(N+1)B|}{|B|}.$$

Most a Plünnecke-Ruzsa becslésből

$$|(N+1)B| \leq (|A+B|/|A|)^{N+1}|A| \leq K^{N+1}|A|.$$

Másfelől

$$\lambda^N \leq \frac{|(N+1)B|}{|B|} \leq \frac{|B|^{N+1}}{|B|} = |B|^N,$$

így azt kapjuk, hogy

$$\lambda \leq \min\{|B|, K^{1+1/N}\frac{|A|^{1/N}}{|B|^{1/N}}\}.$$

Számolással adódik, hogy

$$K^{1+1/N}\frac{|A|^{1/N}}{|B|^{1/N}} < |B|$$

pontosan akkor, ha

$$K^{1+1/N}\frac{|A|^{1/N}}{|B|^{1/N}} < K|A|^{1/(N+1)}.$$

Ezért tehát

$$\lambda < K|A|^{1/(N+1)}. \tag{4.2}$$

(4.1) miatt és mivel $K \geq 1$

$$|X-B| \leq \frac{|(j+1)B|}{|jB|}K^j|X| \leq \frac{|(j+1)B|}{|jB|}K^N|X|$$

és legyen j ahol a minimum teljesül, azaz, ahol $\lambda = \frac{(j+1)B|}{|jB|}$.

(4.2) miatt tehát

$$|X-B| \leq K|A|^{1/(N+1)}K^N|X| = K^{N+1}|A|^{1/(N+1)}|X|.$$

Most megadjuk N-et; minimalizálnunk kell $|A|^{1/(N+1)}K^{N+1}$ kifejezést. Ez ott van, ahol $|A|^{1/(N+1)} = K^{N+1}$, amiből

$$N \leq \sqrt{\log|A|/\log K}$$

amit beírva a becslésbe, kapjuk a bizonyítandó állítást.

Zárjuk ezt a szakaszt egy olyan állítással, melyik nem olvasható ki a Ruzsa-Plünnecke tételből (habár közeli kapcsolata van ezzel)

4.2.4. Tétel. *Legyen G egy nem feltétlenül kommutatív csoport. Ekkor bármely $X, Y, Z \subseteq G$ halmazokra*

$$|X+Y+Z| \leq \sqrt{\max_{y\in Y} |X+y+Z||X+Y||Y+Z|}.$$

A 4.2.4 Tétel bizonyítása:

A bizonyítás $|Y|$ szerinti indukcióval, és az $|X+Y+Z|^2 \leq \max_{y\in Y} |X+y+Z||X+Y||Y+Z|$ formában történik.

Legyen $|Y| = 1$. Ekkor

$$|X+y+Z| \leq |X+y||Z| = |X||Z| \leq |X+Z||y+Z|,$$

és ezt az egyenlőtlenséget $|X+y+Z|$-kel megszorozva kapjuk az $|Y| = 1$ esetén az állítást.

Legyen tehát most $|Y| > 1$. Válasszuk ki Y-ból azt az y elemet, melyre $|X+y+Z|$ maximális. Definiáljuk a következő halmazokat és elemszámaikat:

$Y' = Y \setminus \{y\}$, $M := |X+y+Z|$, $A := |(X+Y+Z) \setminus (X+Y'+Z)|$,

$B := |(X+Y) \setminus (X+Y')|$ és $C := |(Y+Z) \setminus (Y'+Z)|$,

Amit tehát most igazolnunk kell:

$$(|X+Y'+Z| + A)^2 \leq M(|X+Y'| + B)^2(|Y'+Z| + C)^2.$$

A zárójelet felbontva így elég lesz a következőket igazolni

$$(1)\ |X+Y'+Z|^2 \leq M|X+Y'||Y'+Z|,$$
$$(2)\ A^2 \leq MBC,$$
$$(3)\ 2A|X+Y'+Z| \leq M(C|X+Y'| + B|Y'+Z|).$$

Az (1) az indukciós feltevéssel valamilyen $M' \leq M$ értékkel teljesül (így M-mel is).

A (2)-höz először jegyezzük meg, hogy $A \leq M$. Az $A \leq BC$, azaz az $|(X+Y+Z) \setminus (X+Y'+Z)| \leq |(X+Y) \setminus (X+Y')||(Y+Z) \setminus (Y'+Z)|$ egy injektív leképezésből adódik: Vegyünk egy tetszőleges elemet $x+y+z \in (X+Y+Z) \setminus (X+Y'+Z)$ és rendeljük ehhez az

$$x+y+z \to (x+y, y+z)$$

elemet. Vegyük észre, hogy ez injektív; $(x+y, y+z)$-ből meghatározható $(x, y+z)$ (kivonva az első koordinátából az y-t) amiből $x+y+z$.

A (3) bizonyításához a (2) négyszeresét az (1)-gyel összeszorozva és gyököt vonva azt kapjuk, hogy

$$2A|X+Y'+Z| \leq M\sqrt{C|X+Y'|B|Y'+Z|}.$$

Az egyenlőtlenség jobb oldalára alkalmazva a számtani-mértani egyenlőtlenséget, megkapjuk (3)-at. □

• Feladatok

1. Legyen G véges kommutatív csoport és legyen $U \subseteq G$, melyre $|U| = |G|^\alpha$, $0 < \alpha < 1$. Tegyük fel, hogy ha az $X, Y \subseteq G$ halmazpárra az $X + Y$ halmaz U-t lefedi, akkor $|X|, |Y| < |G|^\beta$.

Tegyük fel, hogy $\beta < \frac{2}{3}\alpha$. Bizonyítsuk be, hogy ekkor nem létezik $A, B, C \subseteq G$, melyekre $A + B + C$ lefedné U-t.

Útmutatás: Használjuk a 4.2.4 tételt kommutatív csoportra az $|A + B + C| \leq \sqrt{|A + B||A + C||B + C|}$ formában.

2. (Freiman-Pigaev) Bizonyítsuk be, hogy

$$|A + A|^{3/4} \leq |A - A| \leq |A + A|^{4/3}.$$

Megoldás

1. Ha lefedhető lenne, akkor $U \subseteq (A+B)+C = A+(B+C) = B+(A+C)$ miatt, a feladat feltétele és az előző feladatot felhasználva

$$|G|^\alpha = |U| \leq |A + B + C| \leq \sqrt{|A + B||A + C||B + C|} < |G|^{\frac{3\beta}{2}}$$

következne ellentmondásként.

2. Mint láttuk a Freiman kérdés javításánál: $|A + A||A| \leq |A - A|^2$, továbbá mivel $|A + A| \leq |A|^2$, ez utóbbiból gyököt vonva és az első egyenlőtlenséggel összeszorozva kapjuk, hogy $|A + A|^{3/4} \leq |A - A|$. A másik egyenlőtlenség a távolság tétel, $|A - A||A| \leq |A + A|^2$ és az $|A - A| \leq |A|^2$ egyenlőtlenség párból kapható.

5. fejezet

Additív komplementerek

A számelmélet klasszikus kérdése, hogy mely additív halmazok fedik le a természetes számokat. Ilyen kérdés vezetett pl. a Goldbach sejtéshez. Említsük meg továbbá Erdős által is vizsgált kérdést, mely így hangzik: Igaz-e, hogy $n = 2^k + p$ megoldható, ha $n \geq 3$ páratlan, $k \in \mathbb{Z}$ és p prímszám?

Erdős kérdését – többek között – az is motiválhatta, hogy $\pi(x) \sim \frac{x}{\ln x}$ és a 2 hatványok száma x-ig $\leq \log_2(x)$, azaz, ha nincs sok "összeesés" a fenti számok között, akkor esélyünk van arra, hogy e sejtés igaz legyen (a sejtés egyébként hamis).

A fentiek alapján kérdezhetjük: legyen G véges csoport, $A \subseteq G$. Azt mondjuk, hogy $X \subseteq G$ *A additív komplementere*, ha $A + X = G$. Kérdezhetjük, mi $\min |X|$ értéke?

5.0.1. Tétel. *Legyen $A \subseteq G$, ahol G véges kommutatív csoport. Ekkor létezik $X \subseteq G$, melyre $A + X = G$ és*

$$|X| \leq \frac{|G|}{|A|} \log |G|.$$

Bizonyítás:
Legyen $A, B \subseteq G$. Mivel

$$\sum_{x \in G} r_{A-B}(x) = \sum_{x \in G} |A \cap (B + x)| = |A||B|,$$

ezért van olyan $x \in G$, melyre

$$|A \cap (B+x)| \leq \frac{|A||B|}{|G|}.$$

Ebből következik, hogy a fenti $x \in G$ elemre

$$\frac{|G| - |A \cup (B+x)|}{|G|} \leq \frac{|G| - |A|}{|G|} \cdot \frac{|G| - |B|}{|G|}.$$

Valóban

$$\frac{|G| - |A| - |B|}{|G|} = \frac{|G| - |A \cup (B+x)| - |A \cap (B+x)|}{|G|} \geq$$

$$\geq \frac{|G| - |A \cup (B+x)| - \frac{|A||B|}{|G|}}{|G|},$$

és így

$$|G| - |A \cup (B+x)| \leq |G| - |A| - |B| + \frac{|A||B|}{|G|} = |G| \left(1 - \frac{|A|}{|G|}\right) \cdot \left(1 - \frac{|B|}{|G|}\right).$$

Ezért, ha $A = B$, akkor

$$|G| - |A \cup (A+x)| \leq |G| \left(1 - \frac{|A|}{|G|}\right)^2.$$

Legyen most $x = x_1$ és a fenti eljárást használjuk a $A \cup (A + x_1)$ halmazra; így van olyan x_2 melyre

$$|G| - |A \cup (A+x_1) \cup (A+x_2)| \leq |G| \left(\frac{|G| - |A \cup (A+x_1)|}{|G|}\right) \left(1 - \frac{|A+x_2|}{|G|}\right) \leq$$

$$\leq |G| \left(1 - \frac{|A|}{|G|}\right)^3,$$

mivel $|A + x_1| = |A|$.

Iteráljuk a fenti eljárást; kapjuk az $X = \{x_1 = 0, x_2, \ldots, x_s\}$ halmazt, melyre

$$|G| - |A + X| \leq |G| \big(1 - \frac{|A|}{|G|}\big)^{|X|} < |G| \cdot e^{\frac{-|A||X|}{|G|}}.$$

Ha most

$$|G| \cdot e^{\frac{-|A||X|}{|G|}} \leq 1$$

teljesül, akkor $A + X \subseteq G$ és $|A + X| \leq |G|$, azaz azt kapjuk, hogy $|G| = |A + X|$, vagyis $G = A + X$.

Erre az X halmazra $|X| \leq \frac{|G|}{|A|} \log |G|$.

Megjegyzés:

Mivel $|G| = |A + X|$ ezért

$$|G| = |A + X| \leq |A||X| \Leftrightarrow |X| \geq \frac{|G|}{|A|}.$$

Becslésünk a $\log$ faktortól eltekintve éles.

6. fejezet

Additív kombinatorika nemkommutatív csoportokban

6.1. Nemkommutatív Kneser tétel

Nem kommutatív esetben erősebb feltételek mellett mondható ki bizonyos lefedési tétel. G tehát most nem (feltétlenül) kommutatív csoport. Ezért tehát a multiplikatív írásmódot használjuk.

6.1.1. Tétel. *Legyen $0 < \varepsilon < 1$, $S \subseteq G$ nem üres véges részhalmaz. Az $A \subseteq G$ halmazra, melyre $|A| \geq |S|$ tegyük fel, hogy*

$$|S \cdot A| \leq (2 - \varepsilon)|S|.$$

Ekkor van olyan $H < G$ részcsoport, hogy $|H| \leq (2/\varepsilon - 1)|S|$ és S lefedhető nem több, mint $2/\varepsilon - 1$ jobb oldali mellékosztályával, azaz

$$S \subseteq \cup_{i=1}^{t} Hx_i; \quad t \leq 2/\varepsilon - 1.$$

A 6.1.1 tétel bizonyítása:
Bármely $K \in \mathbb{R}^+$ valósra és bármely A halmazra definiáljuk a hiátust:

$$C_{K,S}(A) = C(A) := |A \cdot S| - K|A|.$$

Ez nyilván eltolás invariáns, azaz $\forall x \in G\ C(xA) = C(A)$.

Most bizonyítunk egy ú.n. szubmodularitási lemmát:

Lemma:
$\forall A, B, S \subseteq G$ és $K \in \mathbb{R}^+$ esetén

$$C(A \cup B) + C(A \cap B) \leq C(A) + C(B).$$

Bizonyítás:
Mivel

$$|(A \cdot S) \cup (B \cdot S)| + |(A \cdot S) \cap (B \cdot S)| = |A \cdot S| + |B \cdot S|,$$

továbbá mivel

$$(A \cup B) \cdot S = \{xs : s \in S;\ x \in A\ \vee\ x \in B\} = (A \cdot S) \cup (B \cdot S)$$

és

$$(A \cap B) \cdot S = \{ys : s \in S;\ x \in A\ \wedge\ x \in B\} \subseteq (A \cdot S) \cap (B \cdot S)$$

így összeadva a két utolsó elemszámát és az első $K-$szorosát kivonva kapjuk az állítást. □

(Jegyezzük meg, hogy a metszetnél valóban csak tartalmazás van; lehetséges ugyanis az $a's_1 = b's_2$ is az AS és BS metszetében).

Fix $K-$ra és S-re definiáljuk a következő fogalmakat:

(1) Definiáljuk a κ-paramétert a következő módon::

$$\kappa_K(S) = \kappa := \inf_{A \neq \emptyset} C(A).$$

ez létezik, mert diszkrét értékeket vesz fel $C(A)$. (Továbbá, ha $K \leq 1$, akkor $C(A)$ pozitív, és így $\kappa_K(S)$ nemnegatív.)

(2) A halmazt nevezzük *optimálisnak*, ha $C(A) = \kappa$. Az előbbiek miatt tehát létezik optimális halmaz.

(3) A halmazt nevezzük *atomnak*, ha $|A|$ minimális és A optimális, így tehát létezik atom is.

Legyen $K = 1 - \varepsilon/2$. Ekkor $\forall A-$ra

$$C(A) = |A \cdot S| - K|A| \geq |A| - K|A| = \varepsilon/2|A|.$$

Ha A atom, akkor nyilván $\forall x \in G$ elemre xA is atom.
Legyen A és B két optimális halmaz. Ekkor a szubmodularitás miatt

$$(\kappa \leq)C(A \cup B) + (\kappa \leq)C(A \cap B) \leq C(A) + C(B) = 2\kappa.$$

Így

$$\kappa = C(A \cup B) \qquad \kappa = C(A \cap B),$$

ami a definíció miatt azt jelenti, hogy $A \cup B$ és $A \cap B$ is optimális. A bal invariancia miatt tehát létezik H, hogy $1_G \in H$ amelyre tehát vagy $xH = H$ vagy $H \cap xH = \emptyset$. Azt kapjuk, hogy H részcsoportja $G-$nek.
Mivel bármely $A - ra$, amelyikre $|A| \geq |S|$, $|A \cdot S| \leq (2 - \varepsilon)|S|$, így

$$C(A) = |A \cdot S| - K|A| \leq (2 - \varepsilon)|S| - (1 - \varepsilon/2)|S| = (1 - \varepsilon/2)|S|.$$

Így

$$\varepsilon/2|H| \leq C(H) = \kappa \leq c(A) \leq (1 - \varepsilon/2)|S|,$$

amit átrendezve azt kapjuk, hogy

$$|H| \leq (2/\varepsilon - 1)|S|.$$

Továbbá mivel

$$C(H) = |H \cdot S| - K|H| \leq (1 - \varepsilon/2)|S|,$$

azt kapjuk, hogy

$$|H \cdot S| \leq (2/\varepsilon - 1)|H|,$$

más szóval S lefedhető $\leq (2/\varepsilon - 1)$ H szerinti mellékosztállyal. □

6.2. Szorzathalmaz bázis

Legyen G egy tetszőleges (nem feltétlenül kommutatív) véges csoport. Ebben a pontban arra vagyunk kíváncsiak, hogy egy hármas szorzat mikor adja ki az egész csoportot. Bizonyítjuk a következőt:

6.2.1. Tétel. *Legyen G egy tetszőleges véges csoport és $A, B, C \subseteq G$. Ekkor létezik olyan $\alpha = \alpha(G)$ konstans, mely mellett, ha $|A||B||C| > \alpha|G|^3$, akkor*

(i) Az $ab = c; \quad a \in A; b \in B; c \in C$ egyenlet megoldható,

(ii) $ABC = G$

továbbá az (i) és (ii) ekvivalens állítások.

Megjegyzés: A bizonyításban elemi módon az

$$\alpha(G) = 2\sqrt[3]{\|1_A - \mathbb{E}(A)\|_2^2 \|1_B - \mathbb{E}(B)\|_2^2 \|1_C - \mathbb{E}(C)\|_2^2}$$

olvasható ki. (Valójában csak az $\alpha(G) = 2|1_B - \mathbb{E}(B)| = |B| - \frac{|B|^2}{|G|}$ formát használjuk; mivel A-ban, B-ben és C-ben szimmetrikus a bizonyítás, a kapott becsléseket összeszorozva és köbgyököt vonva kapjuk a fenti α-t.) Egy jóval erősebb becslés Babai-Nikolov-Pyber egy tételéből nyerhető, amelyik Gowers eredeti tételének egy új bizonyítását adja.

Bizonyítás:

Első lépésként az ekvivalenciát bizonyítjuk. Legyen $g \in G$ és helyettesítsük a C halmazt a gC^{-1} halmazzal. Nyilván a tétel feltételei igazak maradnak. Ekkor (i) miatt léteznek az a, b, gc^{-1} elemek, melyekre $ab = gc^{-1}$ vagy ekvivalens felírásban $abc = g$.

Most tekintsük az A, B, C^{-1} halmazokat és tegyük fel (ii)-t. Ekkor léteznek az a, b, c^{-1} elemek, melyek szorzata kiadja az egységelemet, azaz $abc^{-1} = e$, vagy ekvivalens felírásban $ab = c$.

Szükségünk lesz a következő lemmára:

Lemma:

Legyen $f_1, f_2 \in L^2(G)$. Ekkor

$$\|f_1 * f_2\|_2 \leq \sqrt{|G|}\|f_1\|_2\|f_2\|_2$$

Bizonyítás:

A definíció szerint

$$\|f_1 * f_2\|_2^2 = \sum_{x \in G} \Big(\sum_{y \in G} f_1(xy^{-1}) f_2(y) \Big)^2 \leq$$

$$\leq \sum_{x \in G} \sum_{y \in G} f_1^2(xy^{-1}) \sum_{y \in G} f_2^2(y)$$

a Cauchy egyenlőtlenséget használva. Bevezetve a $z := xy^{-1}$ ismeretlent, a jobb oldalon a $|G|\|f_1\|_2^2\|f_2\|_2^2$ kifejezést kapjuk. □

Mint láttuk, $A * B(x)$ az x elem reprezentációinak a számát jelenti és ezért az átlaga: $\mathbb{E}(A * B) = \frac{|A||B|}{|G|}$.

Lemma:
Legyen $S = \{x \in G : A * B(x) = 0\}$. *Ekkor*

$$|S| \leq \Big(\frac{|G|}{|A||B|}\Big)^2 \|A * B - \mathbb{E}(A * B)\|_2^2,$$

ahol $\mathbb{E}(\cdot)$ *a várhatóértéket jelenti.*

Bizonyítás:

$$\|A * B - \mathbb{E}(A * B)\|_2^2 = \|A * B - \frac{|A||B|}{|G|}\|_2^2 = \sum_{x \in G} \Big(A * B(x) - \frac{|A||B|}{|G|}\Big)^2 \geq$$

$$\geq \sum_{x \in S} \Big(\frac{|A||B|}{|G|}\Big)^2 = |S|\Big(\frac{|A||B|}{|G|}\Big)^2 \quad \square$$

Ezek után

$$|S| \leq \Big(\frac{|G|}{|A||B|}\Big)^2 \|A * B - \mathbb{E}(A * B)\|_2^2 = \Big(\frac{|G|}{|A||B|}\Big)^2 \|A * (B - \mathbb{E}(B))\|_2^2$$

a konvolúció disztributivitás miatt. Most az első lemma miatt

$$\|A * (B - \mathbb{E}(B))\|_2^2 \leq |G|\|A\|_2^2 \|1_B - \mathbb{E}(B)\|_2^2 = \alpha(G)|G||A||B|$$

és így

$$|S| \leq \alpha(G)\Big(\frac{|G|}{|A||B|}\Big)^2 |G||A||B| < |C|$$

azaz van olyan $c \in C$, melyre $A * B(c) \neq 0$, ami éppen (i).

A csoportok reprezentációjának elméletében minden csoport egy alkalmas vektortérből vektortérbe menő lineáris leképezéssel reprezentálható (a részletekért számos könyv található az interneten). Ezen alkalmas leképezés mátrixának dimenzióját jelölje $m(G)$. Pl. a p test feletti (p prím) 2×2 invertálható mátrixok csoportjában ez $(p-1)/2$. Kimondunk egy tételt, mely Gowers tételének Babai-Nikolov-Pyber bizonyításban használható, és amelyik a bizonyításunk első lemmájának egyfajta erősítése:

6.2.2. Tétel (Babai-Nikolov-Pyber). *Legyen $f_1 \in L^2(G)$ és $f_2 \in L_0^2(G)$, ahol $L_0^2(G) = \{f \in L^2(G) : \mathbb{E}(f) = 0\}$. Ekkor*

$$\|f_1 * f_2\|_2 \leq \sqrt{\frac{|G|}{m(G)}}\|f_1\|_2\|f_2\|_2.$$

E tételből az előző bizonyítást követve az erősebb állítás következik:

6.2.3. Tétel (Gowers). *Legyen G egy tetszőleges véges csoport és $A, B, C \subseteq G$. Tegyük fel, hogy $|A||B||C| > \frac{|G|^3}{m(G)}$, ekkor*
(i) Az $ab = c; \quad a \in A; b \in B; c \in C$ egyenlet megoldható,
(ii) $ABC = G$
továbbá az (i) és (ii) ekvivalens állítások.

6.2.4. Tétel. *Legyen $n > 3$ és*

$$A_n = \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n} : a_i \in A;\ \varepsilon_i \in \{1, -1\}\}.$$

Tegyük fel, hogy létezik $n \in \mathbb{N}$, melyre $|A_n| > |A|^{1+c}$; $c > 0$. Ekkor

$$|A \cdot A \cdot A| > |A|^{1+\frac{c}{3n-6}}.$$

Bizonyítás:
Nyilván $A_n = A_{n-2} \cdot A_2$ és így $|A_n| \leq |A_{n-2}||A_2|$. Használjuk az első távolságtételt

$$\frac{|A_{n-2}||A_2|}{|A|} \leq \frac{|A_{n-1}||A_3|}{|A|^2}$$

azaz

$$\frac{|A_n|}{|A|} \leq \frac{|A_{n-1}|}{|A|}\frac{|A_3|}{|A|}$$

ebből indukcióval azt kapjuk, hogy

$$\frac{|A_n|}{|A|} \leq \Big(\frac{|A_3|}{|A|}\Big)^{n-2}.$$

Most felső becslést adunk $|A_3|$-ra.

Megint az első távolság tételből azt kapjuk, hogy

$$|AAA^{-1}| \leq \frac{|AAA||A^{-1}A^{-1}|}{|A|} \leq \frac{|AAA|^2}{|A|},$$

amiből – felhasználva, hogy $(AA^{-1}A^{-1})^{-1} = AAA^{-1}$

$$|AA^{-1}A| \leq \frac{|AA^{-1}A^{-1}||AA|}{|A|} = \frac{|AAA^{-1}||AA|}{|A|} \leq \frac{|AAA|^3}{|A|^2}.$$

Továbbá

$$|A^{-1}AA| \leq \frac{|A^{-1}A^{-1}||AAA|}{|A^{-1}|} \leq \frac{|AAA|^2}{|A|}.$$

Végül, mivel $|AA^{-1}A^{-1}| = |AAA^{-1}|$, $|A^{-1}A^{-1}A| = |A^{-1}AA|$, $|A^{-1}AA^{-1}| = |AA^{-1}A|$, $|A^{-1}A^{-1}A^{-1}| = |AAA|$ és $\frac{|AAA|^3}{|A|^2} > \frac{|AAA|^2}{|A|}$ azt kapjuk, hogy

$$|A_3| \leq \frac{|AAA|^3}{|A|^2}.$$

Ezért

$$|A|^c < \frac{|A_n|}{|A|} \leq \Big(\frac{|A_3|}{|A|}\Big)^{n-2} \leq \Big(\frac{|AAA|}{|A|}\Big)^{3n-6} \quad \square$$

Feladat

Legyen $A, B \subseteq G$, $H < G$. (G nem feltétlenül kommutatív). Tegyük fel, hogy az A halmaz t számú H-beli mellékosztályba metsz bele.

a.) Ekkor

$$|AB| \geq t|H \cap B|.$$

b.) Bizonyítsuk be, hogy

$$|A^{-1}A \cap H| \geq \frac{|A|}{t}.$$

c.) Legyen $A_k = \{g_1 g_2 \cdots g_k : g_i \in A^{-1}A\}$. Ekkor

$$|A_{k+1}| \geq \frac{|A_k \cap H|}{|A^{-1}A \cap H|}|A|.$$

MEGOLDÁS

a.) Jelölje $x_1, x_2, \ldots, x_t$ az A halmaz olyan elemeit, amelyek H különböző mellékosztályaiba tartoznak. Ekkor

$$|AB| \geq |A(B \cap H)| \geq |\{x_1, x_2, \ldots, x_t\}(B \cap H)| = |\cup_{1 \leq i \leq t} x_i(B \cap H)| = t|(B \cap H)|.$$

b.) Valamelyik gH mellékosztályban $|gH \cap A| \geq |A|/t$. Ekkor bármelyik $a \in gH \cap A$ esetén

$$g^{-1}a \in H \cap g^{-1}A \subseteq H \cap A^{-1}A.$$

c.) Az a.) és b.) miatt és mivel $A_{k+1} = A^{-1}AA_k$, kapjuk, hogy

$$|A_{k+1}| = |A^{-1}AA_k| \geq t|H \cap A_k|$$

és

$$|A^{-1}A \cap H| \geq \frac{|A|}{t}.$$

Összeszorozva a két becslést kapjuk a c.) állítást.

7. fejezet

Fedési tételek

Kezdjük egy feladattal, ami Erdős és Sárközy egy publikálatlan eredménye:

FELADAT
Legyen $A \subseteq \mathbb{Z}$, olyan sorozat, amelynek felső sűrűsége, azaz

$$\overline{d}(A) := \limsup_{n\to\infty} \frac{|A \cap [1,n]|}{n} = \gamma$$

pozitív.

a.) Legyen X olyan halmaz, amelyre bármely $x, x' \in X$, $x \neq x'$ esetén $(x + A) \cap (x' + A) = \emptyset$ teljesül. Ekkor $|X| \leq 2\gamma$.

b.) Igazoljuk, hogy $|\mathbb{N} \setminus (X + A - A)| < \infty$.

c.) (Erdős, Sárközy) Ha $\overline{d}(A) = \gamma > 0$, akkor $A - A$ korlátos hézagú sorozat.

d.) Ez a hézag nem függ $\gamma-$tól; nagysága akármilyen nagy lehet.

7.1. Két fedési tétel

Erdős és Sárközy fenti eredményének az általánosítását vizsgáljuk ebben a pontban. Általában is igaz a következő lefedési tétel:

7.1.1. Tétel. *Legyenek $A, B \subseteq G$ véges részhalmazok. Ekkor van olyan $X \subseteq B$, hogy $|X| \leq \frac{|A+B|}{|A|}$; továbbá, hogy $|A + X| = |A||X|$ és*

$$B \subseteq X + (A - A).$$

Az $|A+X| = |A||X|$ feltétel tehát azt jelenti, hogy az $A+X$ összeghalmaz elemei csak egyféleképpen reprezentálhatóak.

Bizonyítás:
Az ötlet a Feladat a.) részéhez hasonlóan történik: veszünk $B-$ből egy olyan maximális X kollekciót, amelyre ha $b_1, b_2 \in X$, és $b_1 \neq b_2$, akkor $(b_1 + A) \cap (b_2 + A) = \emptyset$ teljesül. Mivel

$$\cup_{b_i \in X}(b_i + A) \subseteq A + B$$

és ezen $b_i + A$ halmazok páronként diszjunktak, kapjuk, hogy

$$|X| \leq \frac{|A + B|}{|A|}.$$

Ha most lenne olyan $b \in B$, hogy $b \notin X + (A - A)$, akkor ez azt jelentené, hogy

$$(b + A) \cap (X + A) = \emptyset$$

lenne, ami ellentmond X maximalitásának. □

Még egy alkalmazást mutatunk, ahol az előző gondolat szerepel. Bergelson vetette fel a következő kérdést: Ha $A \subseteq \mathbb{N}$, és $\overline{d}(A) > 0$, akkor az $A - A$ különbséghalmaz tartalmaz egy végtelen összeghalmazt. Pontosabban igazolta a következő tételt:

7.1.2. Tétel. *Legyen $A \subseteq \mathbb{N}$, és $\overline{d}(A) > 0$. Ekkor bármely k-hoz létezik egy végtelen $B \subseteq \mathbb{N}$ halmaz úgy, hogy*

$$A - A \supseteq B + B + \cdots + B = kB.$$

E tétel bizonyításához Bergelson Fürstenberg ergodelméleti átviteli elvét alkalmazza, amit nem részletezünk.

Egy érdekes következménye e tételnek:

7.1.3. Tétel. *Legyen $A \subseteq \mathbb{N}$, és $\overline{d}(A) > 0$. Ekkor bármely k-hoz létezik k-hosszúságú nem triviális számtani sorozat A differencia halmazában.*

A 7.1.3 tétel I. bizonyítása:

Egyszerűen a 7.1.2 tételt használjuk. Mivel B végtelen, ezért létezik $b_1, b_2 \in B$, $b_1 \neq b_2$. Ekkor a $kb_1, (k-1)b_1 + b_2, (k-2)b_1 + 2b_2, \ldots, kb_2 \in kB \subseteq A - A$ sorozat egy $b_2 - b_1$ di□erenciájú számtani sorozat. □

E tételre még visszatérünk a fejezet végén egy másik bizonyítást adva rá.

A 7.1.2 tételt egy általánosabb formában elemi módszerrel igazoljuk:

Legyen $A \subseteq \mathbb{Z}^n$ az $A(x)$ számláló függvényt definiáljuk az

$$A(x) = \sum_{a \in A; |a| \leq x} 1$$

segítségével.

Az A halmaz felső sűrűsége legyen

$$\overline{d}(A) = \limsup_{x \to \infty} \frac{A(x)}{x}.$$

7.1.4. Tétel. *Legyen $A \subseteq \mathbb{Z}^n$ és tegyük fel, hogy $\overline{d}(A) = \gamma > 0$. Ekkor bármely $M \in \mathbb{N}$ esetén létezik egy végtelen $B \subseteq \mathbb{Z}^n$, hogy*

$$A - A \supseteq B \widehat{+} B \widehat{+} \cdots \widehat{+} B = \widehat{M}B,$$

ahol $\widehat{+}$ azt az összeadást jelenti, ahol az összeadandók páronként különbözőek (lásd megszorított összeg).

Bizonyítás: Tekintsük az $\{x_i\}_{i=1}^{M^n}$; $\underline{x}_i = (x_{i_1}, x_{i_2}, \ldots, x_{i_n})$; $0 \leq x_{i_j} \leq M - 1$ vektorokat.

Azt mondjuk, hogy

$$\underline{u} \equiv \underline{v} \pmod{M}$$

akkor és csak akkor, ha minden $1 \leq j \leq n$ esetén

$$u_j \equiv v_j \pmod{M}.$$

Az A halmaz elemeit beosztjuk aszerint, hogy az M hosszú hiperkocka mely pontjával kongruensek. Azaz legyen

$$A_i := \{\underline{a} \in A : \underline{a} \equiv \underline{x}_i \pmod{M}\}; \quad 1 \leq i \leq M^n.$$

Ekkor valamely i-re nyilván teljesül, hogy $\overline{d}(A_i) = \rho > 0$.

Legyen

$$A' = A_i - \underline{x}_i \subseteq L := \{\underline{u} : \underline{u} \equiv \underline{0} \pmod{M}\}.$$

Mivel

$$A' - A' = (A_i - \underline{x}_i) - (A_i - \underline{x}_i) = A_i - A_i \subseteq A - A,$$

ezért elég lesz $A' - A'$-ben keresni nagy összeghalmazt.

A lefedési tétel miatt, mivel $\overline{d}(A_i) = \rho > 0$, létezik egy $X \subseteq \mathbb{Z}^n$, hogy

$$A' - A' + U = \mathbb{Z}^n,$$

továbbá $s := |U| \leq \frac{1}{\rho}$.

Legyen χ a $\mathbb{Z}^n$ összes M-esének egy s-színezése, azaz legyen:

$$\chi : (\mathbb{Z}^n)^M \mapsto \{1, 2, \ldots, s\},$$

és színezzünk egy M-est az i-edik színre,

$$\chi(\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_M) = i,$$

ha

$$\underline{x}_i + \underline{x}_i + \cdots + \underline{x}_i \in A' - A' + \underline{u}_i.$$

(A színezés nem feltétlenül egyértelmű, ha több eltoltban is benne van, válasszuk a legkisebb i-t.)

Ismeretes, hogy egy megszámlálható halmaz M-eseinek az s színezései esetén létezik egy végtelen monokromatikus részhalmaz, azaz olyan, amelynek bármely M-ese egyszínű (ez az ú.n. végtelen Ramsey-tétel). Azaz létezik egy i és egy $B' \subseteq \mathbb{Z}^n$ végtelen halmaz, hogy bármely $\{\underline{x}_1, \underline{x}_2, \ldots \underline{x}_M\} \in B'^M$ halmazra

$$\underline{x}_1 + \underline{x}_2 + \cdots + \underline{x}_M \in A' - A' + \underline{u}_i.$$

Végül legyen

$$B := B' - \frac{\underline{u}_i}{M}.$$

Jegyezzük meg, hogy $B \subseteq \mathbb{Z}^n$, mivel $\underline{u}_i \equiv \underline{0} \pmod{M}$. Így

$$A' - A' + \underline{u}_i \supseteq B' \widehat{+} B' \widehat{+} \cdots \widehat{+} B' = \widehat{M} B' =$$

$$= \left(B + \frac{\underline{u}_i}{M}\right) \widehat{+} \left(B + \frac{\underline{u}_i}{M}\right) \ldots \widehat{+} \left(B + \frac{\underline{u}_i}{M}\right) = \widehat{M} \left(B + \frac{\underline{u}_i}{M}\right) = \widehat{M} B + \underline{u}_i.$$

Ezért

$$A' - A' \supseteq B\widehat{+}B\widehat{+}\cdots\widehat{+}B = \widehat{M}B. \quad \square$$

A fejezet végén két további tételt igazolunk. Az első a 7.1.3 tételt – egy erősebb formában – is kiadja:

7.1.5. Tétel. *Legyen $A \subseteq \mathbb{Z}$ véges halmaz, melyre $|A-2A| = K|A|$. Ekkor $A-A$-ban található egy $\lfloor \frac{\log|A|}{\log K}) \rfloor$ hosszú számtani sorozat.*

1. Megjegyzés. *Mivel egy olyan $A \subseteq \mathbb{Z}$ sorozatra, melyre $\overline{d}(A) > 0$ végtelen sokszor teljesül, hogy az $A' := A \cap [1,n]$ halmazra $|A'-2A'| = K|A'|$, ahol K csak $\overline{d}(A)-$tól függ, így egy második bizonyítást kaptunk a 7.1.3 tételre.*

A 7.1.5 tétel bizonyítása: Találnunk kell egy $d \in A-A$ számot melyre $id \in A-A$ teljesül $i = 1,2,\ldots M := \lfloor \frac{\log|A|}{\log K}) \rfloor$ esetén. Legyen tehát $d = a_1 - a_1' \in A-A$ és találnunk kell $a_j, a_j', a_{j+1}, a_{j+1}'$ elemeket, melyekre

$$a_{j+1} - a_{j+1}' = a_j - a_j' + a_1 - a_1'$$

teljesül $j = 1,\ldots,M-1$ esetén. Átrendezve

$$a_{j+1} - a_j - a_1 = a_{j+1}' - a_j' - a_1'$$

azaz ha találunk $2M$ elemet, melyre e fenti teljesül, akkor megkaptuk az M tagú számtani sorozatot. Vegyük A-ból ki az összes M tagú sorozatot: $a_1, a_2, \ldots, a_M$. Ez $|A|^M$ féle rendezett M-es. Mindegyikhez elkészítjük az

$$(a_2 - a_1 - a_1, a_3 - a_2 - a_1, \ldots, a_M - a_{M-1} - a_1)$$

$M-1$-est. Ezek a koordináták az $A-2A$ halmazban vannak; tehát a feltétel miatt ilyen $M-1$-es legfeljebb $K^{M-1}|A|^{M-1}$ féle lehet. Ha most a lehetséges $a_1, a_2, \ldots, a_M$ $M-$esek száma több, mint $K^{M-1}|A|^{M-1}$, akkor lesz két ilyen $M-1$-es, amelyik megegyezik és ez egy M tagú számtani sorozatot biztosít. Azaz, ha

$$|A|^M > K^{M-1}|A|^{M-1}$$

teljesül, amiből $M > \frac{\log|A|}{\log K} + 1$, amint azt állítottuk. $\square$

A 7.1.3 tétel hátterében valójában a következő tétel áll:

7.1.6. Tétel. *Legyen $A = \{a_1 < a_2 < \dots\}$ egészek egy korlátos hézagú egészek sorozata, azaz létezik $K > 0$, hogy bármely $i = 1, 2, \dots$ teljesül $a_{i+1} - a_i \leq K$. Ekkor A tartalmaz tetszőleges hosszú számtani sorozatot.*

A fedési tétel következménye, hogy ha egy $A \subseteq \mathbb{N}$ halmazra teljesül, hogy $\overline{d}A > 0$, akkor $A - A$ korlátos hézagú. Azaz a fenti tétel egy újabb bizonyítást ad a 7.1.3 tételre.

Bizonyítás:
A bizonyításhoz szükségünk lesz van der Waerden tételre:

3. Lemma. *Tekintsük a természetes számok egy tetszőleges $r \geq 2$ színezését. Ekkor minden $k \in \mathbb{N}$ egészhez található egy olyan színosztály, melyik tartalmaz egy legalább k hosszúságú nem triviális számtani sorozatot.*

A van der Waerden tétel bizonyítása megtalálható például Graham, Rothschild és Spencer - Ramsey Theory c. könyvében.

Tekintsük most az $\{iK\}_{i=0}^{\infty}$ sorozatot. A korlátos hézag tulajdonság miatt bármely $i \geq 0$ esetén az $[iK, (i+1)K)$ intervallum tartalmaz egy A-beli elemet. Most színezzük $\mathbb{N}$ halmazt a következőképpen: az i természetes szám kapja meg az $a - iK$ ($0 \leq a - iK < K$) színt, ahol a az $[iK, (i+1)K)$ intervallumba eső A-beli elemek közül az iK eleméhez legközelebb eső elem.

A fenti lemma miatt bármely $k \in \mathbb{N}$ egészhez található egy olyan színosztály, amelyik tartalmaz egy legalább k hosszúságú nem triviális számtani sorozatot. Legyen ez a szín $0 \leq t < K$ és a számtani sorozat: $r, r+d, r+2d, \dots, r+k'd;\ k' \geq k$. A fenti konstrukció miatt így az $rK + t, (r+d)K + t, (r+2d)K + t, \dots, (r+k'd)K + t$ mind A-beliek. □

FELADAT
Bizonyítsuk be, hogy van olyan $A = \{a_1 < a_2 < \dots\}$, melyre $i = 1, 2, \dots$ esetén teljesül, hogy $a_{i+1} - a_i \leq 2$ és A nem tartalmaz *végtelen* nem triviális számtani sorozatot.

MEGOLDÁS:
Mivel $a_{i+1} - a_i \leq 2$ tulajdonsággal rendelkező sorozatból kontinuum sok van ($a_{i+1} - a_i = 1$ vagy 2) és végtelen nem triviális számtani sorozatból $\aleph_0$ sok (csak a kezdőtagot és a di□erenciát kell megadni), van olyan $a_{i+1} - a_i \leq$

2 sorozat melynek komplementere minden végtelen nem triviális számtani sorozatba belemetsz. □

Végül egy további fedési tétellel zárjuk a fejezetet:

7.1.7. Tétel. *Legyen $X \subseteq [1, N]$; $|X| = n$ és $1 \leq k \leq n$. Ekkor létezik V és W, melyekre $|W| = k$ és*

$$X = V + W \quad \text{és} \quad |V| \geq \frac{\binom{n}{k}}{\binom{N-1}{k-1}}.$$

Bizonyítás:

A bizonyítás hasonló lesz a 7.1.5 tétel bizonyításához; vegyük egy tetszőleges k elemű részhalmazát X-nek: $\{x_1, x_2, \ldots x_k\}$. Nyilván $\binom{n}{k}$ ilyen van és készítsük el hozzá a

$$\{x_2 - x_1, \ldots x_k - x_1\} \subseteq \{1, 2, \ldots, N-1\}$$

$k-1$ elemű halmazt. Mivel $\{1, 2, \ldots, N-1\}$-nek $\binom{N-1}{k-1}$ darab $k-1$ elemű részhalmaza van, így van olyan $\{d_1, d_2, \ldots, d_{k-1}\}$, amelyiket legalább $T \geq \frac{\binom{n}{k}}{\binom{N-1}{k-1}}$ számú $\{x_{j,1}, x_{j,2}, \ldots x_{j,k}\}$; $j = 1, 2, \ldots T$ halmazhoz készítettük el. Álljon V ezen halmazok első elemeiből, azaz legyen

$$V := \{x_{1,1}, x_{2,1} \ldots, x_{T,1}\}.$$

Legyen $W := \{0, d_1, d_2, \ldots, d_{k-1}\}$. Mivel ezen elemek $x - x_{j,1}$ alakúak, ezért $V + W \subseteq X$. Könnyű látni, hogy mivel a k elemű részhalmazok valamelyik koordinátában különböznek, ugyanazt a $\{d_1, d_2, \ldots, d_{k-1}\}$ különbség sorozatot állítják elő, ezért az első elemek, azaz V elemei is mind különbözőek. □

7.2. Approximatikus csoportok, Sym-halmazok

3. Definíció. *Legyen G kommutatív csoport. Egy $H \subseteq G$ részhalmaz $K-$approximatikus csoport, ha létezik $K \geq 1$, és*

- $0 \in H$

- *szimmetrikus, azaz* $H = -H$ *és*
- $H + H$ *lefedhető a* H *legfeljebb* K *eltoltjával, azaz*

$$H + H \subseteq H + X,$$

ahol $|X| \leq K$.

Egy egyszerű példa 2-approximatikus csoportra a következő:
Legyen $g \in G$ és legyen $A = \{-ng, (-n+1)g, \ldots, -g, 0, g, 2g, \ldots, ng\}$. Ekkor A 2-approximatikus csoport.

7.2.1. Tétel. *Ha egy* $A \subseteq G$ *halmazra teljesül, hogy* $|A + A| \leq K|A|$ *vagy* $|A - A| \leq K|A|$. *akkor* $A - A$ *egy* K^5*-approximatikus csoport.*

Bizonyítás:
$A - A$ szimmetrikus és a 0-t tartalmazza. Legyen most $B := (A - A) + (A - A)$. A Plünnecke-Ruzsa tétel miatt (lásd 4. fejezet) teljesül, hogy

$$|A + B| \leq K^5|A|.$$

Használjuk az első lefedési tételt; létezik egy $X \subseteq G$, melyre $|X| \leq K^5$ és $(A - A) + (A - A) = B \subseteq (a - A) + X$, azaz $A - A$ egy K^5-approximatikus csoport. □

A Bevezető tételek c. fejezetben láttuk, hogy egy csoportban $|A \pm B| = |A|$ pontosan akkor igaz, ha létezik egy $G' < G$ részcsoport és A a G' mellékosztályainak az uniója. A bizonyításban (implicit) a

$$Sym_1(A) = \{h : A + h = A\}$$

halmaz játszott szerepet. E halmaz általánosítása a

4. Definíció. *Legyen* $\alpha > 0$

$$Sym_\alpha(A) = \{h : |A \cap (A + h)| \geq \alpha|A|\}$$

halmaz.

Mivel $Sym_\alpha(A)$ szimmetrikus, $0 < \alpha \leq 1$ esetén tartalmazza a 0-t, ésszerű megkérdezni, $Sym_\alpha(A)$ ($2Sym_\alpha(A)$ stb) vajon $P-$approximatikus csoport-e valamely (nem túl nagy) P halmazra?

7.2.2. Tétel. *Legyen $A \subseteq G$ és tegyük fel, hogy $|A-A| = K|A|$ ($K \geq 1$). Legyen tovább $0 < \alpha < \frac{1}{K}$. Ekkor $2Sym_\alpha(A)$ egy $K^{16}\left(\frac{1-\alpha}{1-\alpha K}\right)^2-$approximatikus csoport.*

Bizonyítás:

Mivel $0 < \alpha < \frac{1}{K} \leq 1$, ezért a $Sym_\alpha(A) \setminus \{0\}$ halmaz nem üres. $|A \cap (A+h)| \geq \alpha|A|$ pontosan akkor teljesül valamely h-ra, amikor $|A \cap (A-h)| \geq \alpha|A|$, azaz $Sym_\alpha(A) = -Sym_\alpha(A)$.

Továbbá $|A \cap (A+h)| \geq \alpha|A| > 0$ ezért $h \in A - A$, és így $Sym_\alpha(A) \subseteq A - A$.

Legyen $L = K^{16}\left(\frac{1-\alpha}{1-\alpha K}\right)^2$. Meg fogjuk mutatni, hogy $4Sym_\alpha(A)$ lefedhető $2Sym_\alpha(A)$ L darab eltoltjával. Idézzük fel a Plünnecke-Ruzsa tételt:

4. Lemma. *Legyen $A \subseteq G$ és tegyük fel, hogy $|A - A| = K|A|$. Ekkor*

$$|mA - nA| \leq K^{m+n}|A|.$$

Szükségünk lesz még a következő lemmára:

5. Lemma. *Legyen $A \subseteq G$ és tegyük fel, hogy $|A - A| = K|A|$ ($K \geq 1$) Ekkor*

$$|Sym_\alpha(A)| \geq |A| \cdot \frac{1 - \alpha K}{1 - \alpha}.$$

Az 5. lemma bizonyítása:

Vegyük észre, hogy $|A \cap (A+h)|$ a $h = a - a'$ $a, a' \in A$ megoldásainak a száma amit röviden $d_{A-A}(h) = d(h)$-vel jelöljük.

Nyilván $d(h) < \alpha|A|$ a $h \notin Sym_\alpha(A)$ esetén és $d(h) \leq |A|$ a $h \in Sym_\alpha(A)$ esetén. Így

$$|A|^2 = \sum_{h \in A-A} d(h) \leq |Sym_\alpha(A)||A| + \alpha|A| \cdot (|A - A| - |Sym_\alpha(A)|).$$

Használva az $|A - A| = K|A|$ feltételt és átrendezve az egyenlőtlenséget kapjuk, hogy

$$|Sym_\alpha(A)| \geq |A| \frac{1 - \alpha K}{1 - \alpha}. \square$$

Használni fogjuk a lefedési tételnél használt ötletet; legyen $x_i - Sym_\alpha(A)$, ahol $x_i \in 2Sym_\alpha(A) - Sym_\alpha(A) = 3Sym_\alpha(A)$. Mivel $Sym_\alpha(A) \subseteq A - A$,

$$x_i - Sym_\alpha(A) \subseteq 2Sym_\alpha(A) - 2Sym_\alpha(A) = 4Sym_\alpha(A) \subseteq 4A - 4A,$$

és a diszjunktság miatt, valamint 4. Lemma ($n = m = 4$-re használva) és 5. Lemma miatt

$$\left| \cup_{i=1}^{t} (x_i - Sym_\alpha(A)) \right| = t \cdot |Sym_\alpha(A)| \leq K^8 |A| \leq$$

$$\leq K^8 \frac{1 - \alpha}{1 - \alpha K} |Sym_\alpha(A)|,$$

így

$$t \leq K^8 \frac{1 - \alpha}{1 - \alpha K}.$$

Legyen $X = \{x_1, x_2, \ldots x_t\}$. Bebizonyítjuk, hogy $3Sym_\alpha(A)$ lefedhető $X + 2Sym_\alpha(A)$ halmazzal és hogy $4Sym_\alpha(A)$ pedig $2X + 2Sym_\alpha(A)$ halmazzal.

X maximalitása miatt bármely $y \in 3Sym_\alpha(A)$, $y = x_i + s + s'$ alakba írható, ahol $x_i \in X$, $s, s' \in Sym_\alpha(A)$, azaz

$$3Sym_\alpha(A) \subseteq X + 2Sym_\alpha(A),$$

és ezért

$$4Sym_\alpha(A) \subseteq X + 3Sym_\alpha(A) \subseteq 2X + 2Sym_\alpha(A).$$

A $2X$ halmaz számossága legfeljebb

$$|X|^2 \leq K^{16} \left(\frac{1 - \alpha}{1 - \alpha K} \right)^2.$$

Azt kaptuk, hogy $2Sym_\alpha(A)$ egy legfeljebb $K^{16} \left(\frac{1-\alpha}{1-\alpha K} \right)^2$−approximatikus csoport, ahogy azt állítottuk. $\square$

Várható, hogy maga $Sym_\alpha(A)$ olyan approximatikus csoport, ahol a kiegészítő X halmaz mérete függ az A halmaz méretétől. Valóban igazolni fogjuk, hogy $Sym_\alpha(A)$ egy $f(\alpha, K, r) \log |A|$−approximatikus csoport.

7.2.3. Tétel. *Tegyük fel, hogy a G csoport minden elemének a rendje $r \geq 2$. Legyen $K \geq 1$, és legyen $A \subseteq G$, melyre $|A-A| = K|A|$. Ekkor $Sym_\alpha(A)$ egy $P-$approximatikus csoport, ahol $L = K^{16}\left(\frac{1-\alpha}{1-\alpha K}\right)^2$ és $P = \frac{(1-\alpha)K^4 r^L \cdot \log|A|}{(1-\alpha K)} + \frac{(1-\alpha)K^4 r^L \log(K^4 r^L)}{(1-\alpha K)} + 1$.*

Bizonyítás:

Néhány lemma bizonyításával kezdjük;

6. Lemma. *Legyen G egy kommutatív csoport, melynek minden elemének a rendje legfeljebb $r \geq 2$. Legyen $H \subseteq G$ egy $L-$approximatikus csoport. Ekkor $\langle H \rangle$ rendje legfeljebb $r^L|H|$.*

Mivel H egy $L-$approximatikus csoport, a definíció miatt létezik egy X legfeljebb L elemű halmaz, melyre $H+H \subseteq H+X$. Belátjuk, hogy $H+\langle X \rangle$ részcsoport.

Valóban

$$H + \langle X \rangle \subseteq H + \langle X \rangle + H + \langle X \rangle = H + H + \langle X \rangle \subseteq$$

$$\subseteq H + \langle X \rangle + X = H + \langle X \rangle,$$

így

$$(H + \langle X \rangle) + (H + \langle X \rangle) = H + \langle X \rangle.$$

Mivel

$$\langle H \rangle \subseteq H + \langle X \rangle$$

és mivel G minden elemének a rendje legfeljebb r, azt kapjuk, hogy $|\langle H \rangle| \leq |H + \langle X \rangle| \leq r^L|H|$.

A 7.2.2 tétel miatt a $2Sym_\alpha(A)$ halmaz egy $K^{16}\left(\frac{1-\alpha}{1-\alpha K}\right)^2-$approximatikus csoport. Jelölje $L = K^{16}\left(\frac{1-\alpha}{1-\alpha K}\right)^2$ és legyen $\widetilde{G} := \langle 2Sym_\alpha(A) \rangle$. A 4. és 6. lemmák miatt

$$|2Sym_\alpha(A)| \leq K^4|A|,$$

és

$$|\widetilde{G}| \leq K^4 r^L |A|.$$

Végül idézzük fel az $5.$ fejezet additív komplementer tételét

7. Lemma. *Legyen $U \subseteq \widetilde{G}$. Ekkor létezik egy Y halmaz, melyre $\widetilde{G} = U + Y$, és*

$$|Y| \leq \frac{|\widetilde{G}|}{|U|} \log |\widetilde{G}| + 1.$$

Legyen $U := Sym_\alpha(A)$. A 7. Lemma miatt létezik egy olyan Y halmaz,

$$|Y| \leq \frac{|\widetilde{G}|}{|U|} \log |\widetilde{G}| + 1,$$

melyre $Y + Sym_\alpha(A)$ lefedi $\widetilde{G}$-t és így lefedi $2Sym_\alpha(A)$-t is. Ami azt jelenti, hogy $Sym_\alpha(A)$ egy $|Y|-$approximatikus csoport.

Végül megbecsüljük $|Y|$-t.

Mivel $|\widetilde{G}| \leq K^4 r^L |A|$, azt kapjuk, hogy

$$|Y| \leq \frac{K^4 r^L |A|}{|A|^{\frac{1-\alpha K}{1-\alpha}}} \cdot \log(K^4 r^L |A|) + 1 =$$

$$= \frac{(1-\alpha) K^4 r^L \cdot \log |A|}{(1-\alpha K)} + \frac{(1-\alpha) K^4 r^L \log(K^4 r^L)}{(1-\alpha K)} + 1. \square$$

7.3. Véges csoport "majdnem zárt" részhalmazairól

Véges csoportok zárt részhalmazai részcsoportok. Természetesen tovább lehet kérdezni; ha egy G csoport adott véges részhalmaza "majdnem zárt" a műveletre nézve, akkor mennyire térhet el egy részcsoporttól? Itt nem tesszük fel, hogy kommutatív G, így ismételjük meg a Sym halmaz definícióját:

$$Sym_{1-\varepsilon} := \{x \in G : |A \cap Ax| \geq (1-\varepsilon)|A|\}.$$

Itt $|A \cap Ax|$-et jelölhetjük $q(x)$-szel.

Elsőként a Sym halmazok néhány további tulajdonságát vizsgáljuk.

1. Propozíció. *1. Legyen* $\varepsilon_1 < \varepsilon_2$. *Ekkor*

$$Sym_{1-\varepsilon_1} \subseteq Sym_{1-\varepsilon_2}.$$

2. Bármely $0 < \varepsilon_1, \varepsilon_2 < 1$ *esetén*

$$Sym_{1-\varepsilon_1} \cdot Sym_{1-\varepsilon_2} \subseteq Sym_{1-\varepsilon_1-\varepsilon_2}.$$

3. Bármely $0 < \varepsilon < 1$ *esetén*

$$|Sym_{1-\varepsilon}| \leq \frac{|A|}{1-\varepsilon}.$$

Bizonyítás:

1. A definíció egyszerű következménye.
2. Legyen $x_1 \in Sym_{1-\varepsilon_1}$ és $x_2 \in Sym_{1-\varepsilon_2}$. Ekkor

$$|\{a \in A;\ ax_1x_2 \notin A\}| = |\{a \in A;\ ax_1 \notin A\} \cup \{a \in A;\ ax_1 \in A\, ax_1x_2 \notin A\}| \leq$$

$$\leq \varepsilon_1|A| + \varepsilon_2|A| = (\varepsilon_1 + \varepsilon_2)|A|$$

3.

$$|A|^2 = \sum_x q(x) \geq \sum_{x \in Sym_{1-\varepsilon}} q(x) \geq |Sym_{1-\varepsilon}|(1-\varepsilon)|A|. \quad \square$$

Most pontosan definiáljuk, mit értünk az alatt, hogy egy halmaz "majdnem zárt" a műveletre:

5. Definíció. *Legyen*

$$Z(A) := \frac{|\{(a_1, a_2) : a_1a_2 \in A\}|}{|A|^2}.$$

$Z(A)-$t felírhatjuk most

$$Z(A)|A|^2 = \sum_{a \in A} q(a) = \sum_{a \in A} |A \cap Aa|$$

formában is.

7.3.1. Tétel. *Legyen A a G csoport egy véges részhalmaza, melyre $Z(A) > 1-\delta$; (pl. legyen $\delta = \frac{1}{50}$). Ekkor létezik egy $H < G$ részcsoport, melyre*

$$|H| \leq \frac{10}{9}|A|, \quad |A \cap H| \geq \frac{4}{5}|A|.$$

2. Megjegyzés. *A bizonyításban a $Sym_{1-\varepsilon}$ halmazról bizonyítottak lesznek a segítségünkre. A fenti tételben a $\delta = \frac{1}{50}$ és $\varepsilon = \frac{1}{20}$ párossal dolgozunk. A paramétereket másként is választhatjuk; egy δ, ε párosnak, mint látni fogjuk a bizonyításban a*

$$2 - \frac{2\delta}{\varepsilon} < \frac{1}{1-5\varepsilon} \quad (*)$$

feltételt kell csak kielégítenie.

Bizonyítás:

Legyen a δ paraméter a tétel feltételeinek megfelelő (pl. $\frac{1}{50}$). Elsőként igazoljuk a következő lemmát:

8. Lemma. *Bármely $\varepsilon > \delta > 0$ esetén a tétel feltételei mellett*

$$(1 - \delta/\varepsilon)|A| \leq |A \cap Sym_{1-\varepsilon}|.$$

Valóban Jelölje $T := A \cap Sym_{1-\varepsilon}$

$$(1-\delta)|A|^2 = Z(A) = \sum_{a \in A} |A \cap Aa| = \sum_{a \in T} |A \cap Aa| + \sum_{a \in A \setminus T} |A \cap Aa|.$$

Nyilván $|A \cap Aa| \leq |A|$ és $a \in A \setminus T$ esetén $|A \cap Aa| \leq (1-\varepsilon)|A|$. Így

$$(1-\delta)|A|^2 = Z(A) = \sum_{a \in A} |A \cap Aa| = \sum_{a \in T} |A \cap Aa| + \sum_{a \in A \setminus T} |A \cap Aa| \leq$$

$$\leq (|A| - |T|)(1-\varepsilon)|A| + |T||A|.$$

Így az

$$(1-\delta)|A|^2 \leq (|A| - |T|)(1-\varepsilon)|A| + |T||A|.$$

egyenlőtlenséget átrendezve kapjuk a lemma állítását.

Továbbá szükségünk van még egy állításra:

9. Lemma. *Tegyük fel, hogy az ε, δ párosra $(*)$ teljesül. Ekkor*

$$Sym_{1-2\varepsilon} = Sym_{1-4\varepsilon}$$

Bizonyítás:

Nyilván $Sym_{1-2\varepsilon} \subseteq Sym_{1-4\varepsilon}$. Legyen $x \in Sym_{1-4\varepsilon}$, megmutatjuk, hogy $x \in Sym_{1-2\varepsilon}$ amiből következik a lemma állítása.

Tekintsük a $Sym_{1-\varepsilon}$ és $xSym_{1-\varepsilon}$ halmazokat. Mindkettő részhalmaza lesz a Propozíció 2. pontja miatt a $Sym_{1-5\varepsilon}$ halmaznak. Ez a halmaz a Propozíció 3. pontja miatt legfeljebb $\frac{|A|}{1-5\varepsilon}$ elemű. A $Sym_{1-\varepsilon}$ és $xSym_{1-\varepsilon}$ halmazok a 8. Lemma miatt legalább $(1-\delta/\varepsilon)|A|$ eleműek. Ha most

$$2 - \frac{2\delta}{\varepsilon} < \frac{1}{1-5\varepsilon}$$

teljesül (ami paramétereink mellett teljesül), akkor $Sym_{1-\varepsilon}$ és $xSym_{1-\varepsilon}$ halmazoknak van közös elemük, azaz x két $Sym_{1-\varepsilon}$-beli elem hányadosa, ám mivel ha $b \in Sym_{1-\varepsilon}$, akkor $b^{-1} \in Sym_{1-\varepsilon}$ is teljesül (a definíció miatt), azt kapjuk, hogy x két $Sym_{1-\varepsilon}$-beli elem szorzata, de akkor x eleme $Sym_{1-2\varepsilon}$ halmaznak is. Ez volt a bizonyítandó állítás. □

Ebből a lemmából bizonyítjuk, hogy a $H := Sym_{1-2\varepsilon}$ részcsoport.

Valóban a Propozíció 2. pontja miatt

$$Sym_{1-2\varepsilon} \subseteq Sym_{1-2\varepsilon} \cdot Sym_{1-2\varepsilon} \subseteq Sym_{1-4\varepsilon} = Sym_{1-2\varepsilon},$$

azaz $HH = H$.

Végül a Propozíció 3. pontja és a 8. Lemma miatt

$$|H| \leq \frac{10}{9}|A|, \quad |A \cap H| \geq \frac{4}{5}|A|.$$

7.4. Freiman tétele csoportokban

Az additív kombinatorika egyik legtöbbször használt és vizsgált tétele a Freiman tétel:

7.4.1. Tétel. *Legyen $A \subseteq \mathbb{Z}$ melyre $|A+A| < K|A|$. Ekkor A benne van egy $d = d(K)$ dimenziós, $f(K)|A|$ méretű*

$$P = \{v_0 + h_1 v_1 + h_2 v_2 + \ldots h_d v_d : 0 \leq h_i < L_i\}, \quad L_1 L_2 \cdots L_d = f(K)|A|$$

általánosított számtani sorozatban. (Azaz mind a dimenzió, mind az általánosított számtani sorozat mérete csak K-tól függ)

E tétel bizonyítása hosszadalmasabb; itt e tétel analogonját bizonyítjuk bizonyos kommutatív csoportokban.

7.4.2. Tétel. *Legyen G olyan kommutatív csoport, melyben minden elem rendje legfeljebb $r \geq 2$. Ha $|A+A| < K|A|$ (vagy $|A-A| < K|A|$ is feltehető), akkor létezik olyan $H < G$ részcsoport, ami A-t lefedi, és melynek mérete*

$$|H| \leq K^2 r^{K^4} |A|.$$

Bizonyítás:

Legyen $x_1, x_2, \ldots, x_k \in 2A - A$ az a maximális sorozat, melyre az $x_i - A$ ($i = 1, 2, \ldots, k$) halmazok páronként diszjunktak. Mivel mind részhalmazai a $2A-2A$ halmaznak, egyesítésük $k|A|$ méretű, így a Plünnecke-Ruzsa tételt felhasználva

$$k|A| \leq |2A - 2A| \leq K^4 |A|,$$

azaz $k \leq K^4$.

Ahogy a fedési tételnél láttuk, most hasonlóan bizonyítható, hogy

$$2A - A \subseteq X + A - A,$$

ahol $X = \{x_1, x_2, \ldots, x_k\}$. (Ha lenne $y \in 2A - A$, amelyik nem lenne eleme $X + A - A$-nak, evvel az y elemmel bővíthető lenne X.)

Az n szerinti indukcióval könnyen igazolható, hogy

$$nA - A \subseteq (n-1)X + A - A,$$

és így ha U jelöli az X által generált részcsoportot, akkor $nA-A \subseteq U+A-A$ is teljesül. Végül jelölje $H := \cup_n (nA - A)$ részcsoportot (könnyű látni, hogy H valóban részcsoport). Ekkor

$$H \subseteq U + A - A,$$

tehát $|H| \leq |U||A - A| \leq r^k K^2 |A| \leq K^2 r^{K^4} |A|$, felhasználva, hogy minden elem rendje legfeljebb r és mint bizonyítottuk ha $|A + A| \leq K|A|$ akkor $|A - A| \leq K^2 |A|$.

Végül $A \subseteq 2A - A \subseteq H$. □

Feladatok

1. Bizonyítsuk be, hogy ha $A \subseteq \mathbb{N}$ halmazra $d(A) = 1$, akkor létezik olyan C végtelen halmaz, melyre $A \supseteq FS(C) := \{\sum_{x \in X} x : X \subseteq C; |X| < \infty\}$.

2. Készítsünk olyan ha $A \subseteq \mathbb{N}$ halmazt, amelyre $\underline{d}(A) > 1 - \varepsilon$ ($\varepsilon > 0$) és ha $B \subseteq A$ és létezik $d(B)$, akkor $d(B) = 0$. (Azaz nem igaz, hogy egy nagyon sűrű halmazból el lehet hagyni "kevés" elemet melynek pozitív sűrűsége legyen.)

3. Legyen A egy $K-$approximatikus csoport. Bizonyítsuk be, hogy az $m-$szeres összeghalmazára teljesül

$$|mA| \leq K^{m-1}|A|.$$

Megoldások

1. A halmazt rekurzív módon adjuk meg; az első elemet x_1-et nyilván tetszőlegesen választhatjuk meg. Tegyük most fel, hogy az $x_1 < x_2 < \cdots < x_k$ elemeket már definiáltuk. Mivel A halmaz sűrűsége 1, ezért A-ban tetszőleges hosszúságú sorozata van egymást követő elemeknek (valóban ellenkező esetben létezne egy K hogy minden K hosszúságú intervallumban lenne egy A-n kívüli elem, ekkor azonban $\overline{d}(A) \leq 1-1/K < 1$ lenne ellentmondásként). Azaz létezik olyan $a \in A$, hogy $a, a+1, a+2, \ldots, a+T \in A$, ahol $T > \sum_{i=1}^{k} x_i$. Legyen most $x_{k+1} = a$ és ekkor nyilván $FS(x_1 < x_2 < \cdots < x_k < x_{k+1}) \subseteq A$ is teljesül.

2. A feladatot abban a formában igazoljuk, hogy az A komplementer halmazáról $U := \mathbb{N} \setminus A$ halmazról igazoljuk a következőt:

Létezik olyan U, melyre $\overline{d}U < \delta$, és ha $W \supseteq U$, melyre létezik $d(W)$, akkor $dW = 1$.

Legyen $1/2^k < \delta$ és álljon U a következő elemekből:

$$U = \{u : 2^n \leq u < 2^n + 2^{n-k};\ n \in \mathbb{N}\}.$$

Vegyünk egy tetszőleges elemet $2^n \leq x < 2^{n+1}$, melyre még $x > 2^k$ is teljesül. Ekkor

$$\frac{|U \cap [1,x]|}{x} \leq \frac{|U \cap [1, 2^n + 2^{n-k}]|}{2^n} \leq \frac{k + \sum_{i=k}^{n} 2^{i-k}}{2^n} <$$

$$< \frac{k}{2^n} + \frac{2^{n-k+1}}{2^n} = \frac{k}{2^n} + \frac{1}{2^{k-1}},$$

azaz $\overline{d}U < \delta$.

Legyen most $W \supseteq U$, melyre létezik $d(W) = \nu$.

Ekkor $n > k$ esetén

$$|W \cap [1, 2^n + 2^{n-k}]| = |W \cap [1, 2^n]| + 2^{n-k}.$$

Ezért

$$\frac{|W \cap [1, 2^n + 2^{n-k}]|}{2^n + 2^{n-k}} = \frac{|W \cap [1, 2^n]|}{2^n + 2^{n-k}} + \frac{2^{n-k}}{2^n + 2^{n-k}}.$$

Itt

$$\lim_{n\to\infty} \frac{2^{n-k}}{2^n + 2^{n-k}} = \frac{1}{2^k + 1}$$

és

$$\lim_{n\to\infty} \frac{|W \cap [1, 2^n]|}{2^n + 2^{n-k}} = \lim_{n\to\infty} \frac{|W \cap [1, 2^n]|}{2^n} \frac{2^n}{2^n + 2^{n-k}} = \nu \frac{2^k}{2^k + 1}.$$

Ezért

$$\nu = \lim_{n\to\infty} \frac{|W \cap [1, 2^n + 2^{n-k}]|}{2^n + 2^{n-k}} = \frac{1}{2^k + 1} + \nu \frac{2^k}{2^k + 1},$$

amiből viszont $\nu = 1$ következik.

3. Indukcióval könnyű látni, hogy

$$mA \subseteq A + (m-1)X.$$

Felhasználva a $K-$approximatikus csoport definícióját és a triviális $|U+V| \leq |U||V|$ becslést, kapjuk az állítást.

8. fejezet

Algebrai módszerek

8.1. Megszorított összegek

Az első fejezet egyik triviális megjegyzése volt az $|A| + |B| - 1 \leq |A + B|$ becslés. Mit mondhatunk akkor, ha azt is megkötjük, hogy csak olyan tagokat tekintünk, amelyekben az összeadandók mind különbözőek?

Legyen tehát

$$A \widehat{+} B := \{a + b : a \in A; b \in B; a \neq b\}$$

az ú.n. megszorított összeg. Ha felidézzük az egészek körében az $|A| + |B| - 1 \leq |A + B|$ bizonyítását:

$$A = \{a_1 < a_2 < \cdots < a_k\} \quad B = \{b_1 < b_2 < \cdots < b_m\},$$

akkor

$$a_1 + b_1 < a_2 + b_1 < \cdots < a_k + b_1 < a_k + b_2 < \cdots < a_k + b_m$$

adja a legalább $k + m - 1$ elemet. Ha a megszorított összeget nézzük, akkor ebben a sorban legfeljebb csak két helyen szerepelhet olyan összeg, amelyben az összeadandó tagok azonosak, így $|A \widehat{+} B| \geq |A| + |B| - 3$.

Mint láttuk $A+B$ moduláris analogonja már egy nehezebb tétel (Cauchy-Davenport) volt, mint az egészek körében.

1964-ben Erdős és Heilbronn sejtették a megszorított összeg moduláris változatát.

A következőkben olyan módszert mutatunk be, amellyel mind e sejtés, mind a Cauchy-Davenport tétel bizonyítható (azaz ez utóbbi tétel egy második bizonyítását kapjuk). Továbbá egy olyan tételt, amelynek segítségével az Erdős-Ginzburg-Ziv tételre kapunk egy új bizonyítást.

Egy test feletti polinom foka és gyökeinek a számáról közismert tétel:

8.1.1. Tétel. *$\mathbb{F}$ test felett legyen $P(x) \in \mathbb{F}[x]$, és $\deg P = d$. Ha valamely S halmazra $|S| > d$, akkor van olyan $s \in S$, hogy $P(s) \neq 0$.*

A következő tétel az előbbi tétel többdimenziós változata. Most többféle fokszámot is definiálhatunk: pl a $P(x, y, z) = 2xy^2z^3 - 4x^4y^7$ polinomban $\deg_x p = 4,\ \deg_y p = 7$ és $\deg_z p = 3$ míg a teljes fokszám $\deg p = 11$. Az általános esetben hasonló a definíció.

8.1.2. Tétel. *Legyen $\mathbb{F}$ egy test, $p \in \mathbb{F}[x_1, x_2, \ldots, x_n] \setminus \{0\}$ egy n változós $\mathbb{F}$ test feletti polinom. Legyenek $S_1, S_2, \ldots, S_n \subseteq \mathbb{F}$ n olyan halmaz, melyekre $|S_i| > \deg_{x_i} p$. Ekkor van olyan $(s_1, s_2, \ldots, s_n) \in S_1 \times S_2 \times \cdots \times S_n$, melyre $p(s_1, s_2, \ldots, s_n) \neq 0$.*

Bizonyítás: n szerinti indukcióval. $n = 1$-re éppen a bevezető tétel. Tegyük fel, hogy a p polinom az $S_1 \times S_2 \times \cdots \times S_n$ elemein nulla. Megmutatjuk, ellentmondásra jutva, hogy p az azonosan 0 polinom. Jelölje d $\deg_{x_1} p$-et. Írjuk fel p-t x_1 polinomjaként:

$$p = \sum_{i=0}^{d} x_1^i p_i(x_2, \ldots, x_n).$$

Most bármely $(s_2, s_3, \ldots, s_n) \in S_2 \times S_3 \times \cdots \times S_n$ esetén $p(x_1, s_2, s_3, \ldots, s_n) = \sum_{i=0}^{d} x_1^i p_i(s_2, s_3, \ldots, s_n) = 0$. E polinom az indirekt feltevés miatt S_1 minden értékére, nulla. Így, mivel $|S_1| > d$ a fejezet első tétele miatt azt kapjuk, hogy $p(x_1, s_2, s_3, \ldots, s_n)$ azonosan nulla polinom és így $\forall i = 1, 2, \ldots n$, $p_i(s_2, s_3, \ldots, s_n) = 0$, ami az indukciós feltevés (indirekt megfogalmazása szerint) csak úgy lehet, hogy $\forall i = 1, 2, \ldots n$ $p_i(x_2, x_3, \ldots, x_n) \equiv 0$ és így p is az azonosan nulla polinom. □

A következő tételt szokás "Combinatorial Nullstellensatz"-nak is nevezni:

8.1.3. Tétel. *Legyen $\mathbb{F}$ egy test, $p \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ egy n változós $\mathbb{F}$ test feletti (nem nulla) polinom. Tegyük fel, hogy* $\deg p = d$ *ahol van olyan nem nulla együtthatójú $x_1^{d_1} x_2^{d_2} \ldots, x_n^{d_n}$; $d_1 + \cdots + d_n = d$ monom. Legyenek az S_i halmazok olyanok, hogy $\forall i = 1, 2, \ldots n, \quad |S_i| > d_i$, akkor léteznek az $s_i \in S_i$ $i = 1, 2, \ldots n$, elemek hogy*

$$p(s_1, s_2, \ldots, s_n) \neq 0.$$

Bizonyítás:

$M = d_1 + \cdots + d_n$ szerinti indukcióval. $M = 0$-ra $p \neq 0$ konstans polinom, igaz a tétel. Tegyük fel, hogy $M > 0$ és tegyük fel megint indirekt, hogy p eltűnik minden $S_1 \times S_2 \times \cdots \times S_n$ elemen. Tegyük fel, hogy $d_1 > 0$ és legyen $\alpha \in S_1$ valamint írjuk fel p-t

$$p = (x_1 - \alpha)q + r$$

alakban. Itt $q \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ és $r \in \mathbb{F}[x_2, \ldots, x_n]$ (az r nem tartalmaz x_1 változót, azt az első tagba csoportosítottuk).

Mivel $(\alpha, s_2, \ldots, s_n) \in S_1 \times S_2 \times \cdots \times S_n$ helyettesítésre p nulla, a második tag is nulla, így $r(s_2, \ldots, s_n) = 0$ minden helyettesítési értékre. Továbbá mivel p nulla minden $\{S_1 \setminus \alpha\} \times S_2 \times \cdots \times S_n$ helyettesítésre (és r is nulla, valamint $x_1 - \alpha \neq 0$) kapjuk, hogy q eltűnik $\{S_1 \setminus \alpha\} \times S_2 \times \cdots \times S_n$ halmazon.

A q foka $M - 1 = d_1 - 1 + \cdots + d_n$ és benne van nem nulla együtthatóval az $x_1^{d-1} x_2^{d_2} \ldots, x_n^{d_n}; d_1 + \cdots + d_n$ tag, $|S_1| - 1 > d - 1$, tehát lehet az indukciós feltevés használni: létezik $(s_1, s_2, \ldots, s_n) \in \{S_1 \setminus \alpha\} \times S_2 \times \cdots \times S_n$ melyre $q(s_1, s_2, \ldots, s_n) \neq 0$. Erre a helyettesítésre viszont

$$p(s_1, s_2, \ldots, s_n) = (s_1 - \alpha)q(s_1, s_2, \ldots, s_n) + r(s_2, \ldots, s_n) \neq 0,$$

mivel $(s_1 - \alpha) \neq 0$, $q(s_1, s_2, \ldots, s_n) \neq 0$ és $r(s_2, \ldots, s_n) = 0$. □

Most megmutatjuk e tétel egy olyan következményét, amiből a Cauchy-Davenport tétel második bizonyítását ill. az Erdős-Heilbronn sejtést tudjuk igazolni.

8.1.4. Tétel. *Legyen $\mathbb{F}$ test, $n \geq 1$ és legyen $g \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. Legyenek $A_1, A_2, \ldots, A_n \subseteq \mathbb{F}$. Legyen $K := \sum_{i=1}^{n} (|A_i| - 1) - \deg g$. Tegyük fel, hogy az*

$$(x_1 + x_2 + \cdots + x_N)^K g(x_1, x_2, \ldots, x_n)$$

polinomban szerepel nem nulla együtthatóval az $x_1^{|A_1|-1}x_2^{|A_2|-1}\cdots x_n^{|A_n|-1}$ *tag. Ekkor*

$$|\{a_1+a_2+\cdots+a_n : a_i \in A_i, i=1,2,\ldots,n \ \wedge \ g(a_1,\ldots,a_n)\neq 0\}| \geq K+1.$$

Bizonyítás:

Indirekt tegyük fel, hogy létezik egy olyan $B := \{a_1+a_2+\cdots+a_n : a_i \in A_i, i=1,2,\ldots,n \ \wedge \ g(a_1,\ldots,a_n)\neq 0\}$ halmaz, amelyre $|B| \leq K$ (Nyilván feltehetjük az egyszerűség kedvéért, hogy $|B|=K$, pl. kiegészítve B halmazt elemekkel, ha kell.) Ekkor legyen

$$P(x_1,x_2,\ldots,x_n) = g(x_1,x_2,\ldots,x_n)\prod_{b\in B}(\sum_{i=1}^{n}x_i - b).$$

Most $\deg P = \deg g + K = \sum_{i=1}^{n}(|A_i|-1)$.

Azt is tudjuk, hogy $g(x_1,x_2,\ldots,x_n)(\sum_{i=1}^{n}x_i)^K$-ban szerepel nem nulla együtthatóval az $x_1^{|A_1|-1}x_2^{|A_2|-1}\cdots x_n^{|A_n|-1}$ tag. $P-$ben az összes többi tag kisebb fokszámú, így e tag nem egyszerűsödhet ki. A 8.1.3 tétel miatt léteznek $a_1,a_2,\ldots,a_n$, $a_i \in A_i$, hogy $P(a_1,a_2,\ldots,a_n)\neq 0$. De

$$\prod_{b\in B}\Big(\sum_{i=1}^{n}a_i - b\Big) = 0,$$

minden a_i $n-es$ választás esetén ellentmondásként.

A most következő tétel segít a következő pontban az Erdős-Ginzburg-Ziv tétel második bizonyításához. E tételt Chevalley és Warning igazolta.

8.1.5. Tétel. *Legyen adva* n *egyenként* m *változós polinom*

$$p_1(x_1,x_2,\ldots,x_m), p_2(x_1,x_2,\ldots,x_m),\ldots,p_n(x_1,x_2,\ldots,x_m)$$

az $\mathbb{F}_p$ *test felett, jelölje* $r_j = \deg p_j$ *és* N *az* n *polinom közös gyökeinek a számát. Ha*

$$\sum_{i=1}^{n} r_i < m,$$

akkor $p|N$.

Bizonyítás:
A közös N megoldásszámot a "kis-Fermat" tétel alapján könnyen felírhatjuk (A megoldásszámot $(\mathrm{mod}\ p)$-ben értjük):

$$N = \sum_{x_1,x_2,\ldots,x_m \in \mathbb{F}_p} \prod_{i=1}^{n} (1 - p_i(x_1, x_2, \ldots, x_m)^{p-1}).$$

Felbontva a hatványokat és beszorozva az egyes tagokat N ilyen alakban írható fel:

$$N = \sum_{x_1,x_2,\ldots,x_m \in \mathbb{F}_p} \cdots \prod_{i=1}^{m} x_i^{k_i} \ldots,$$

ahol a fokszámra tett feltétel miatt $\sum_{i=1}^{m} k_i < m(p-1)$. Ebből következik, hogy van olyan k_i kitevő, melyre $0 < k_i < p-1$.

10. Lemma. *Ha* $0 < k < p-1$, *akkor* $\sum_{x \in \mathbb{F}_p} x^k = 0$.

Valóban, mivel $\mathbb{F}_p^*$ ciklikus csoport, ezért legyen y egy generáló eleme. Ekkor $\sum_{x \in \mathbb{F}_p} x^k = \sum_{x \in \mathbb{F}_p} (yx)^k = y^k \sum_{x \in \mathbb{F}_p} x^k$, így $\sum_{x \in \mathbb{F}_p} x^k = 0$.

$N-$ben megcserélve a produktumot a szummával és az alkalmas változó szerint (tehát amelyik kitevőjében $0 < k_i < p-1$) összegezve minden egyes tag 0 értéket vesz fel $\mathbb{F}_p-$ben bizonyítva az állítást. □

8.2. Az Erdős-Heilbronn sejtés, a Cauchy-Davenport és az Erdős-Ginzburg-Ziv tételek (újabb) bizonyításai

Elsőként igazoljuk az Erdős-Heilbronn sejtést:

8.2.1. Tétel. *Legyenek* $A, B \subseteq \mathbb{F}_p$ *nem üres részhalmazok. Ekkor*

$$|A \widehat{+} B| \geq \min\{p, |A| + |B| - 3\}.$$

Bizonyítás:

Amikor $|A|+|B|-2 \geq p$ akkor lásd a 2. feladatot. Általában feltehetjük, hogy $|A|, |B| \geq 2$, továbbá tegyük fel, hogy, $|A| \neq |B|$, egyébként hagyjunk el egy elemet $A-$ból (a bizonyítás végén beszámítjuk). Alkalmazni fogjuk a 8.1.4 tételt $n = 2-$re, az $|A|, |B|$ halmazokra és a $g(x, y) = x - y$ polinomra. (ezzel elértük, hogy $x \neq y$ párra képezzük az összeadást, azaz megszorított összeget kapunk. Ekkor

$$K = |A| - 1 + |B| - 1 - \deg g = |A| + |B| - 3.$$

A 8.1.4 tétel szerint azt kell ellenőrizni, hogy az

$$(x + y)^K (x - y)$$

kifejezésben $x^{|A|-1}y^{|B|-1}$ nem nulla együtthatóval szerepel. Látható, hogy ez az együttható

$$\binom{K}{|A| - 2} - \binom{K}{|A| - 1} = \frac{K!}{(|A| - 2)!(|B| - 2)!}(|B| - |A|),$$

ami $|A| + |B| - 2 < p$ és $|A| \neq |B|$ miatt $\neq 0$. Kapjuk tehát, hogy

$$|A \widehat{+} B| = |\{x + y : x \in A; y \in B \wedge x - y \neq 0\}| \geq K + 1 = |A| + |B| - 2.$$

Tehát mivel esetleg egy elemet el kellett $A-$ból hagyni a kívánt állítást adja. □

Jegyezzük meg, hogy $|A| \neq |B|$, esetén az erősebb $|A \widehat{+} B| \geq \min\{p, |A| + |B| - 2\}$ állítást kapjuk.

Most rátérünk a Cauchy-Davenport tétel második bizonyítására, ami ugyancsak adódik a fenti tételből.

A Cauchy-Davenport tétel második bizonyítása:

Itt egyszerűen legyen $g(x, y) = 1$, nincsen megszorítás az összegben. Ezért $K+1 = |A|+|B|-2$. Az $(x+y)^K$ tagot kifejtve $x^{|A|-1}y^{|B|-1}$ tag együtthatója

$$\binom{|A| + |B| - 2}{|A| - 1}$$

ami az $|A| + |B| - 2 < p$ feltétel miatt nem nulla. (Az $|A| + |B| - 2 \geq p$ feltételre lásd az első fejezet feladatát). □

Végül az Erdős-Ginzburg-Ziv tételre adunk egy új bizonyítást:

Az Erdős-Ginzburg-Ziv tétel második bizonyítása:

Legyen $A = \{a_1, a_2, \ldots a_{2p-1}\} \subseteq \mathbb{Z}_p$. Legyen

$$p_1(x_1, x_2, \ldots, x_{2p-1}) = \sum_{i=1}^{2p-1} a_i x_i^{p-1};\ p_2(x_1, x_2, \ldots, x_{2p-1}) = \sum_{i=1}^{2p-1} x_i^{p-1}.$$

A $p_1 = p_2 = 0$ egyik közös gyöke az $x_1 = x_2 = \cdots = x_{2p-1} = 0$. $p \geq 2$, tehát van a nem triviálistól különböző gyöke. □

Feladatok

1. Bizonyítsuk be, hogy

$$|A \otimes B| \geq \min\{p, |A| + |B| - 3\},$$

ahol $A \otimes B := \{a + b : a \in A; b \in B \wedge a \neq \frac{1}{b}\}$.

2. Legyen G véges csoport, $A, B \subseteq G$, melyekre $|A| + |B| \geq |G| + 2$. Ekkor $A \widehat{+} B = B \widehat{+} A = G$.

Megoldások

1. Legyen $g(x, y) := (xy-1)$, (evvel $a \neq \frac{1}{b}$). Ekkor $K = |A|-1+|B|-1-2$, és könnyem ellenőrizhető, hogy az $x^{|A|-1}y^{|B|-1}$ tag együtthatója nem nulla.

2. Az ötlet hasonló, mint a nem megszorított összegnél; legyen $g \in G$. Ekkor a $(g - B) \cap A$ halmaz – a feltételek miatt – legalább két elemű, azaz g-nek van $a + b$ ($a \neq b$) előállítása is. A $b + a$ előállításnál a $(g - A) \cap B$ halmazzal végezzük el a bizonyítást.

9. fejezet

Gowers-Balog-Szemerédi tétel

Sok esetben a Minkowski (teljes) összeg helyett csak bizonyos elempárokból képzett összegek szerepelnek. Ezt különböző mellékfeltételek igénylik. Azonban, hogy tudjunk bizonyos becsléseket alkalmazni, ahhoz viszont teljes összegekre lenne szükségünk. Legyen Γ egy gráf az A és B halmazokon, mint csúcspontok halmazán definiálva és $E-$ vel jelölve az élhalmazt. Tehát precízen: $\Gamma = \Gamma(A, B, E)$. Vezessük be a következő jelölést:

$$A +^E B := \{a + b : a \in A; b \in B \wedge (a, b) \in E(\Gamma)\}.$$

Tehát csak azokat a párokat adjuk össze, amelyre a két elemet él köti össze.

Elég természetes gondolat a következő: ha sűrű az élhalmaz, akkor kiválasztható $A-$ból és $B-$ből egy "nagy" rész A' és B', hogy - bizonyos feltételek mellett az $A' + B'$ úgy viselkedik, mint az $A +^E B$.

9.0.1. Tétel. *Legyen $A, B \subseteq G$ és legyen $\Gamma(A, B, E)$ egy páros gráf, tegyük fel, hogy valamely $K_1 \geq 1$ számra $|E| \geq |A||B|/K_1$ és valamely $K_2 > 0$ számmal*

$$|A +^E B| < K_2\sqrt{|A||B|}.$$

Ekkor van olyan $A' \subseteq A,\ B' \subseteq B$, amelyekre

$$|A'| \geq \frac{|A|}{4\sqrt{2}K_1}; \qquad |B'| \geq \frac{|B|}{4K_1}$$

és

$$|A' + B'| \leq C_1\sqrt{|A||B|} < C_2\sqrt{|A'||B'|},$$

ahol

$$C_1 = 2^{12}K_1^5K_2^3, \qquad C_2 = 2^{17}K_1^5K_2^3.$$

Megjegyeznénk, hogy sok esetben a konstansok nem különösebben fontosak. Itt K_1, K_2-nek *fontos szerepük van*; mozoghatnak az A és B elemszámával együtt. A tétel ezen javított változata származik Gowerstől, eredeti formájában Balog és Szemerédi igazolták (egy gyengébb formában, ami egy adott probléma igazolásához elég is volt). A most következő gráfelméleti szemléltetése a tétel bizonyításának Tao-Vu szerzőpárostól származik.

Bizonyítás:
Két részre bontjuk a bizonyítást: Először alsó becslést adunk a 2 hosszú utak számára, majd ebből a 3 hosszú utak számára:

11. Lemma. *(2 hosszú utak száma):*
A tétel feltételei mellett $\forall \varepsilon > 0$ $\exists A' \subseteq A$, $|A'| \geq \frac{|A|}{\sqrt{2}K_1}$, *hogy legfeljebb*

$$\varepsilon\left(|A'|^2 - \frac{|A|^2}{2K_1}\right)$$

$(a, a') \in A' \times A'$ *pár kivételével az* $(a, b, a') \in A' \times B \times A'$ *utak száma*

$$\geq \varepsilon\frac{|B|}{2K_1^2}.$$

A második becslés az előző segítségével a 3 hosszú utak számára ad becslést:

12. Lemma. *(3 hosszú utak száma):*
A tétel feltételei mellett $\exists A' \subseteq A$ *és* $\exists B' \subseteq B$ *úgy, hogy* $|A'| \geq \frac{|A|}{4\sqrt{2}K_1}$, $|B'| \geq \frac{|B|}{4K_1}$ *és* $\forall a \in A'$ *és* $\forall b \in B'$ *az* (a, b', a', b) *3 utak száma*

$$\geq \frac{|A||B|}{2^{12}K_1^5}.$$

Ezekből le tudjuk vezetni a tételt:

A kívánt A', B' a második lemmából kapható. Legyen $(a, b) \in A' \times B'$, Ekkor

$$a + b = (a + b') - (b' + a') + (a' + b)$$

ahol (a, b', a', b) egy 3 hosszú út. Minden egyes $a + b$-hez $\geq \frac{|A||B|}{2^{12}K_1^5}$ út tartozik. Az $(a + b'), (b' + a'), (a' + b)$ összeg mindegyike Γ-ból van.

Kapjuk tehát

$$|A' + B'| \cdot U \leq |A +^E B|^3 < (K_2\sqrt{|A||B|})^3,$$

ahol U a 3-utak számát jelöli. Így

$$|A' + B'| \cdot \frac{|A||B|}{2^{12}K_1^5} \leq |A +^E B|^3 < (K_2\sqrt{|A||B|})^3.$$

Átrendezve az állítást kapjuk.

Először az első lemmát igazoljuk. Gráfunk egy páros gráf; "alul" az A, "felül" B pontjai vannak. A cél megmutatni, hogy sok "$\wedge$" (ú.n."cseresznye") van a gráfban. Jelölje $N(x)$ a Γ egy x pontjából induló élek végpontjainak a halmazát. Tehát $|N(x)|$ az x fokszáma. Nyilván A-ra átlagolva N-et ugyanazt kapjuk, mint B-re; éppen az élszámot, ami a feltétel alapján $\geq \frac{|A||B|}{K_1}$, így

$$\frac{|A||B|}{K_1} \leq \sum_{a\in A} |N(a)| = \sum_{b\in B} |N(b)|.$$

Eddig is láttuk, hogy a második momentum informál valójában az értékek eloszlásáról. A Cauchy egyenlőtlenség miatt:

$$\frac{|A|^2|B|^2}{K_1^2} \leq \sum_{b\in B} 1 \sum_{b\in B} |N(b)|^2.$$

$|N(b)|^2$ jelentése: hány (a, a') pár van, hogy (a, b) is (a', b) is él: azaz a $b-$re illeszkedő $\wedge$ alakok száma. Ennek átlagát másként is interpretálhatjuk: az összes a, a' pár szomszédjainak a közös részét. Az utóbbi egyenletben $|B|$-vel egyszerűsítve:

$$\frac{|A|^2|B|}{K_1^2} \leq \sum_{b\in B} |N(b)|^2 = \sum_{a,a'\in A} |N(a) \cap N(a')|.$$

Az állítás, hogy ilyenből sok van. A "rossz" a, a' párokat R halmazba gyűjtjük:

$$R := \Big\{(a, a') : |N(a) \cap N(a')| < \varepsilon \frac{|B|}{2K_1^2}\Big\}.$$

Bevezetünk egy indikátort: legyen $I_R(a, a') = 1$, ha $a, a' \in R$ és egyébként legyen az értéke 0. Az $|N(a) \cap N(a')| < \varepsilon \frac{|B|}{2K_1^2}$ feltétel ekvivalens nyilván az $\frac{1}{\varepsilon}|N(a) \cap N(a')| < \frac{|B|}{2K_1^2}$ feltétellel. Tehát az összegzést az összes a, a' párra megtéve

$$\sum_{a,a' \in A} \frac{1}{\varepsilon} I_R(a, a')|N(a) \cap N(a')| < \frac{|A|^2|B|}{2K_1^2},$$

így tehát a "jó" elemek halmazára (amely "jó" elemek indikátora $1 - I_R$)

$$\sum_{a,a' \in A} (1 - \frac{1}{\varepsilon} I_R(a, a'))|N(a) \cap N(a')| \geq \frac{|A|^2|B|}{2K_1^2}.$$

Mint láttuk $|N(a) \cap N(a')|$ felcserélhető $|N(b)^2|$-vel, ahol $(a, a') \in N(b)^2$. Tehát az összegben $(1 - \frac{1}{\varepsilon} I_R(a, a'))$ tagot annyiszor számoltuk, ahányszor $(a, a') \in N(b)^2$. Így

$$\sum_{a,a' \in A} (1 - \frac{1}{\varepsilon} I_R(a, a'))|N(a) \cap N(a')| = \sum_{b \in B} \sum_{(a,a') \in N(b)^2} (1 - \frac{1}{\varepsilon} I_R(a, a')).$$

Az átlagolás miatt tehát van olyan $b_0 \in B$, hogy

$$\sum_{(a,a') \in N(b_0)^2} (1 - \frac{1}{\varepsilon} I_R(a, a')) \geq \frac{|A|^2}{2K_1^2}.$$

A bal oldalon az összegzést elvégezve kapjuk, hogy

$$\frac{|A|^2}{2K_1^2} \leq \sum_{(a,a') \in N(b_0)^2} (1 - \frac{1}{\varepsilon} I_R(a, a')) = |N(b_0)^2| - \frac{1}{\varepsilon}|N(b_0)^2 \cap R|,$$

hiszen $\sum_{(a,a') \in N(b_0)^2} \frac{1}{\varepsilon} I_R(a, a'))$ összegben I akkor és csak akkor 1, amikor b_0 szomszédpárjai – tehát $N(b_0)^2$ éppen R-ben van. A lemma bizonyítása kész, ha A' halmazt b_0 szomszédjainak választjuk; $A' := N(b_0)$. Ekkor tehát

$$|N(b_0)^2| - \frac{1}{\varepsilon}|N(b_0)^2 \cap R| \Rightarrow |A'|^2 \geq \frac{|A|^2}{2K_1^2},$$

továbbá

$$|N(b_0)^2 \cap R| = |A'^2 \cap R| < \varepsilon\Big(|A'|^2 - \frac{|A|^2}{2K_1^2}\Big),$$

átrendezve az előző egyenlőtlenséget. Azaz legfeljebb $(|A'|^2 - \frac{|A|^2}{2K_1^2})$ A'-beli pár kivételével (a, a') "jó", azaz a hozzájuk csatlakozó b-vel az a, b, a' utak száma $\geq \varepsilon\frac{|B|}{2K_1^2}$. □

Most rátérünk a 3 hosszú utakról szóló lemma bizonyítására.

Néhány egyszerűsítő lépést teszünk; A-ból elhagyjuk először azokat az elemeket, amiknek kevés szomszédjuk van: legyen $A_0 \subseteq A$ úgy, hogy $a \in A_0$ $|N(a)| \geq \frac{|B|}{2K_1}$. Ekkor az elhagyott élek száma $\leq \frac{|A||B|}{2K_1}$, így a megmaradt élek száma $|E| \geq \frac{|A||B|}{2K_1}$. Ha $|A_0| = \alpha|A|$, ($\alpha \leq 1$) akkor

$$|E| \geq \frac{|A||B|}{2K_1} = \frac{|A_0||B|}{2K_1\alpha}.$$

Legyen az előző tételben szereplő $\varepsilon = \frac{1}{16K_1}$ és A helyén pedig A_0. Ekkor van olyan $A_1 \subseteq A_0$, hogy

$$|A_1| \geq \frac{|A_0|}{\sqrt{2}(2\alpha K_1)} = \frac{|A|}{2\sqrt{2}K_1},$$

úgy, hogy legfeljebb $\varepsilon(|A_1|^2 - \frac{|A|^2}{2K_1})$ pár kivételével az A_1 minden a, a' párjára igaz, hogy létezik legalább

$$\varepsilon\frac{|B|}{4K_1^2\alpha^2} = \frac{1}{16K_1}\frac{|B|}{2 \cdot 4K_1^2\alpha^2} =$$

$$\frac{|B|}{128K_1^3\alpha^2} \ (*)$$

olyan b, hogy a, b, a' út a gráfban és e kivételes a, a' párok számára az

$$\varepsilon\Big(|A_1|^2 - \frac{|A|^2}{2K_1}\Big) \leq \frac{|A_1|^2}{16K_1}$$

becslést kapjuk. Most tovább szűkítjük az A_1 halmazt; csak azokat az elemeit hagyjuk meg, amelyekhez legfeljebb $|A_1|/8K_1$ "rossz" a' tartozik (rossz abban

az értelemben, hogy nincs hozzá az előbbiek szerint sok b, amivel alternáló utat képezne).

Mivel "rossz" a, a' párból is legfeljebb $\frac{|A_1|^2}{16K_1}$ van, így "rossz" a-ból is legfeljebb $\frac{|A_1|}{2}$ lehet. Legyen tehát a "jó" A_1-beli elemek halmaza A'. Tehát

$$|A'| > \frac{|A_1|}{2} \geq \frac{|A|}{4\sqrt{2}K_1}.$$

Végül kiválasztjuk a B halmaz B' részhalmazát. A bizonyítás elején mondottak miatt $\forall a \in A'\ N(a) \geq |B|/2K_1$, így

$$\sum_{b \in B} |\{a \in A' : (a,b) \in E\}| \geq |A'||B|/2K_1.$$

Álljon B' halmaz azokból az elemekből, amelyekre

$$B' := \{b \in B : |\{a \in A' : (a,b) \in E\}| \geq |A'|/4K_1\},$$

azaz azokból a b elemekből, amelyeknek az átlagos felénél több A'-beli szomszédjuk van.

Az utóbbi két állítás miatt

$$|A'||B'| \geq |A'| \cdot \frac{|B|}{2K_1} - \frac{|A'|}{4K_1}|B| = \frac{|A'||B|}{2K_1},$$

így

$$|B'| \geq \frac{|B|}{4K_1}.$$

Tehát, ha $a \in A'$ és $b \in B'$, akkor egyrészt b-nek A'-ben sok szomszédja van: $|N(b) \cap A'| \geq \frac{|A'|}{4K_1}$, olyan alternáló út, amelynek a az egyik végpontja, ám A'-ben $\leq \frac{|A'|}{8K_1}$ olyan elem tartozik, amellyel kevés alternáló utat képez, így létezik legalább $\frac{|A'|}{4K_1} - \frac{|A'|}{8K_1} = \frac{|A'|}{8K_1}$ olyan $a' \in A'$, hogy (a, a') sok ((*)-szerinti) alternáló útnak a két végpontja. Így

$$\frac{|A'|}{8K_1} \geq \frac{|A|}{4\sqrt{2}K_1 8K_1} > \frac{|A|}{64K_1^2}.$$

Most már tudjuk, hogy $\forall a, a' \in A'\ a, a'$-re illeszkedő $b \in B'$ alternáló utak száma $(*)$ szerint $\geq \frac{|B|}{128K_1^3\alpha^2}$, így az (a, b, a', b') alternáló 3 utak száma legalább

$$\frac{|B|}{128K_1^3\alpha^2} \cdot \frac{|A|}{64K_1^2} = \frac{|A||B|}{2^{13}K_1^5}. \ \square$$

A következő tételben az additív energia és a nem teljes összegek közötti kapcsolatot vizsgáljuk:

9.0.2. Tétel. *Legyen Z egy kommutatív csoport, $A, B \subseteq Z$ és legyen $G \subseteq A \times B$.*

(1) *Ekkor*

$$E(A,B) \geq \frac{|G|^2}{|A +^G B|}.$$

ahol $E(A,B)$ az additív energia.

Hasonló állítás mondható ki G-n megszorított összeg helyett megszorított különbségre is.

(2) Másfelől ha $E(A,B) \geq \frac{|A|^{3/2}|B|^{3/2}}{K}$ ahol $K \geq 1$, akkor létezik olyan $G \subseteq A \times B$, $|G| \geq \frac{|A||B|}{2K}$, hogy

$$|A +^G B| \leq 2K|A|^{1/2}|B|^{1/2},$$

Bizonyítás:

(1) bizonyítása egyszerűen a Cauchy egyenlőtlenségből adódik:

Jelölje $r_G(n) = \{(a,b) \in G : a+b = n\}$ Ekkor nyilván $\sum_n r_G(n) = |G|$. Tehát

$$|G|^2 = (\sum_n r_G(n))^2 \leq |A +^G B| \sum_n r_G(n)^2 \leq |A +^G B| \sum_n r(n)^2.$$

Mivel $\sum_n r(n)^2 = E(A,B)$, (1) bizonyítása kész.

(2) bizonyítása:

Tehát most tudjuk, hogy

$$\sum_n r(n)^2 = E(A,B) \geq \frac{|A|^{3/2}|B|^{3/2}}{K}.$$

Jelölje

$$U = \{n = a+b : r(n) \geq \frac{|A|^{1/2}|B|^{1/2}}{2K}\}.$$

Ekkor

$$\sum_{n \in U} r(n)^2 \geq \frac{|A|^{3/2}|B|^{3/2}}{K} - \max_{n \notin U} r(n) \sum_n r(n) \geq$$

$$\geq \frac{|A|^{3/2}|B|^{3/2}}{K} - \frac{|A|^{1/2}|B|^{1/2}}{2K}|A||B| = \frac{|A|^{3/2}|B|^{3/2}}{2K}.$$

Továbbá

$$|U|\frac{|A|^{1/2}|B|^{1/2}}{2K} \leq \sum_{n\in U} r(n) \leq |A||B|,$$

így

$$|U| \leq 2K|A|^{1/2}|B|^{1/2}.$$

Legyen

$$G := \{(a,b) : a+b \in U\}.$$

Ekkor $A +^G B \subseteq U$, így $|A +^G B| \leq 2K|A|^{1/2}|B|^{1/2}$.

Mivel $r(n) \leq \min\{|A|,|B|\} \leq |A|^{1/2}|B|^{1/2}$, így

$$|G| = \sum_{n\in U} r(n) \geq \frac{r^2(n)}{|A|^{1/2}|B|^{1/2}} \geq \frac{\frac{|A|^{3/2}|B|^{3/2}}{2K}}{|A|^{1/2}|B|^{1/2}} =$$

$$= \frac{|A||B|}{2K}. \square$$

A Gowers-Balog-Szemerédi tétel egy szép alkalmazása (a sok közül) a következő tétel, amelyik a véges testek körében igazolja, hogy az $f(x,y) = x^2y + xy^2$ függvény feltételesen expander tulajdonságú (e tétel első olvasásra kihagyható):

9.0.3. Tétel. *Legyen $A, B \subseteq \mathbb{F}_p$ és tegyük fel, hogy $|A|, |B| \leq p^{1/2}$, $|A| \asymp |B|$. Legyen $f(x,y) = x^2y + xy^2$. Ekkor van olyan $\eta > 0$, hogy*

$$\max\{|f(A,B)|; |A \cdot B|\} \geq |A|^{1+\eta}.$$

Bizonyítás:

Megmutatjuk, hogy η választható pl. $\frac{1}{800}$−nak. Használjuk az $A^{(k)} := \{a^k : a \in A\};\ k \in \mathbb{N}$ jelölést. Definiáljuk K értékét mint

$$\max(|f(A,A)|, |A \cdot A|) = K|A|$$

és indirekt tegyük fel, hogy $K \ll |A|^{1/800}$.

Most definiálni fogunk egy $G = (V, E)$ gráfot a kövekezőképpen: Legyen $V := A^{(2)} \cdot A$ és (u_1, u_2) pontosan akkor él, amikor $u_1 = a_1^2 a_2;\ u_2 = a_1 a_2^2$. Mivel $u_1^2/u_2 = a_1^3$ és $u_2^2/u_1 = a_2^3$, ezért $|E| \gg |A|^2$.

A Plünnecke-Ruzsa tétel miatt azt kapjuk, hogy $|A \cdot A \cdot A| < K^3|A|$ és így

$$|E| \gg |A|^2 \geq |A \cdot A \cdot A|^2/K^6 \geq |A^{(2)} \cdot A|^2/K^6.$$

Egy tetszőleges $X, Y \subseteq V$ ponthalmazpárra használjuk a

$$X \overset{G}{+} Y = \{x + y \,:\, x \in X,\, y \in Y,\, (x, y) \in E\}$$

jelölést.

Ekkor $|A^{(2)} \cdot A \overset{G}{+} A^{(2)} \cdot A| = |f(A, A)| \leq K|A|$.

Most a Gowers-Balog-Szemerédi tétel miatt létezik $A_1, B_1 \subset A^{(2)} \cdot A$ úgy, hogy $|A_1| \geq |B_1|$ és $|A_1|, |B_1| \gg |A^{(2)} \cdot A|/K^6 \gg |A|/K^6$ és

$$|A_1 + B_1| \ll K^{33}|A_1|^{1/2}|B_1|^{1/2} \ll K^{33}|A_1|$$

és a háromszög egyenlőtlenség miatt $|A_1 + A_1| \ll K^{66}|A_1|$.

Továbbá az indirekt feltevés miatt $|A_1| \leq |A \cdot A \cdot A| \leq K^3|A| \leq |A|^{1+3/800} \leq p^{1/2}$ ezért A_1-re alkalmazható a következő lemma:

13. Lemma. *Legyen $A_1 \subseteq \mathbb{F}_p$ melyre $|A_1| < p^{1/2}$. Ekkor*

$$|A_1 + A_1| + |A_1 A_1| \gg |A_1|^{13/12}.$$

(Ezt a lemmát más kitevővel a 13.9 pontban igazoljuk).

Mivel $|A_1 + A_1| \ll K^{66}|A_1| \ll |A_1|^{1+66/794} < |A_1|^{13/12}$, így $|A_1 A_1| \gg |A_1|^{13/12}$.

Végül vegyük észre, hogy $A_1 \cdot A_1 \subseteq A \cdot A \cdot A \cdot A \cdot A \cdot A$, így megint a Plünnecke-Ruzsa tétel miatt

$$K^6|A| \geq |A \cdot A \cdot A \cdot A \cdot A \cdot A| \geq |A_1 \cdot A_1| \gg |A_1|^{13/12} \gg \frac{|A|^{13/12}}{K^{13/2}},$$

amiből $K \gg |A|^{1/150}$ ellentmond a $K \ll |A|^{1/800}$ feltevésünknek. □

10. fejezet

Nagy és nagyobb szita; Weyl-van der Corput becslés

Ebben a fejezetben három fontos egyenlőtlenséget bizonyítunk be. Elsőként Gallagher nagyobb szitáját, amit a 14. fejezetben használunk négyzetszámok sorozatában található Hilbert kockák méretére. Másodikként az ú.n. nagy szita egy gyengített változatát igazoljuk (e bizonyítás könnyebben követhető, és csak egy konstans szorzó erejéig gyengébb az éles változatnál). Végül egy van der Corput becslést igazolunk, ami segítségünkre lesz Sidon sorozat elemszámának a becslésére.

10.1. Gallagher nagyobb szita

Ez az eredmény meglepően egyszerűen bizonyítható; valójában csak a Cauchy egyenlőtlenségre lesz szükségünk.

10.1.1. Tétel. *Legyen $A \subseteq [1, N]$ egészek egy halmaza. Legyen $\mathcal{P}$ prímszámok egy véges hamaza és minden egyes prímre jelölje $\nu(p)$ azon maradékosztályok számát modulo p melyek tartalmaznak A elemeivel kongruens elemeket. Ekkor*

$$|A| \leq \frac{\sum_{p\in\mathcal{P}} \log p - \log n}{\sum_{p\in\mathcal{P}} \frac{\log p}{\nu(p)} - \log n}.$$

Bizonyítás:

Legyen $p \in \mathcal{P}$. Jelölje $A(h,p) := |\{a \in A : \ a \equiv h \pmod p\}|$.

Világos, hogy $|A| = \sum_{h \in \mathbb{Z}_p} A(h,p)$. Négyzetre emelve és használva a Cauchy egyenlőtlenséget azt kapjuk, hogy

$$|A|^2 = \Big(\sum_{h \in \mathbb{Z}_p} A(h,p) \Big)^2 \leq \nu(p) \sum_{h \in \mathbb{Z}_p} A^2(h,p).$$

Megszorozva ezt $\frac{\log p}{\nu(p)}$-vel, és összeadva az összes $p \in \mathcal{P}$ elemre kapjuk, hogy

$$|A|^2 \sum_{p \in \mathcal{P}} \frac{\log p}{\nu(p)} \leq \sum_{p \in \mathcal{P}} \log p \sum_{h \in \mathbb{Z}_p} A^2(h,p).$$

A jobb oldalt kifejtve

$$\sum_{p \in \mathcal{P}} \log p \sum_{h \in \mathbb{Z}_p} A^2(h,p) = \sum_{p \in \mathcal{P}} \log p \cdot A^2(0,p) + \sum_{p \in \mathcal{P}} \log p \sum_{0 \neq h \in \mathbb{Z}_p} A^2(h,p)$$

Az első tag nyilván $\sum_{p \in \mathcal{P}} \log p |A|$. A második tag

$$\sum_{p \in \mathcal{P}} \log p \sum_{0 \neq h \in \mathbb{Z}_p} A^2(h,p) \leq (|A|^2 - |A|) \sum_{p | a - a'} \log(a - a') \leq (|A|^2 - |A|) \log N.$$

□

10.2. Nagy szita

A másik tétel, (melyet egy gyengített formában bizonyítunk) az ú.n. "nagy szita". Szita abban az értelemben, hogy egy adott A halmaz elemeinek $(\mathrm{mod}\ p)$ vett eloszlásaiból következtet e halmaz méretére, "nagy" pedig abban az értelemben, hogy ha sok maradékosztályban tiltott A előfordulása, akkor következtetünk viszonylag pontosan e méretre (v.ö. a "nagyobb" szitával, ami "még kevesebb" maradékosztályban való előfordulásánál ad jó eredményt. Lásd későbbi állításokat).

Az alábbi tételben az $\epsilon(x)$ az $\epsilon(x) = e^{2\pi i x}$ függvényt jelenti. Amennyiben az argumentum x/p alakú, akkor a szokásos $\epsilon(x/p) = e_p(x)$ jelölést fogjuk használni.

Az alábbi tételek teljes megértéséhez javasoljuk előzetesen a 13. fejezet 13.1, 13.2 és a 13.3 szakaszok elolvasását.

10.2.1. Tétel. *Legyen* $\{x_n\}_{n=1}^N$ *tetszőleges komplex számokból álló sorozat. Legyen a* $0 < t_1 < t_2 < \cdots < t_R < 1$ *egy* δ*-szeparált sorozat* $(\mathrm{mod}\ 1)$*, azaz* $t_{i+1} - t_i > \delta$*, ha i ciklikusan végigfut az elemeken. Legyen végül* $S(t) = \sum_{n=1}^N x_n \epsilon(nt)$*. Ekkor*

$$\sum_{r=1}^{R} |S(t_r)|^2 \leq \left(N - 1 + \frac{1}{\delta}\right) \sum_{n=1}^{N} |x_n|^2.$$

Mint jeleztük a bizonyítás jóval egyszerűbb és rövidebb, ha egy gyengített formában állítjuk, és ami a későbbiekben elegendő lesz számunkra. Nevezetesen a $(N - 1 + \frac{1}{\delta})$ szorzat helyett a $(\pi N + \frac{1}{\delta})$ faktorral bizonyítjuk e tételt.

Bizonyítás:

Egy rövid, az ortogonalitást felhasználó állítást bizonyítunk:

Mivel $|S(t)|^2 = \sum_{n=1}^N |x_n|^2 + \sum_{n=1}^N \sum_{n \neq m} x_n \overline{x}_m \epsilon((n-m)t)$, ezért tetszőleges c-re

$$\int_c^{1+c} |S(t)|^2 dt = \sum_{n=1}^{N} |x_n|^2,$$

mivel $\int_c^{1+c} \epsilon((n-m)t)dt = 0$, $m \neq n$ esetén. Egy lemmával folytatjuk, ami "sima" függvénnyel átlaggal való jól becsülhetőségéről szól:

14. Lemma. *Legyen a* $g(x)$ *függvény az* $(a - h, a + h)$ *intevallumban deriválható. Ekkor*

$$|g(a)| \leq \frac{1}{2h} \int_{a-h}^{a+h} |g(t)|dt + \frac{1}{2} \int_{a-h}^{a+h} |g'(t)|dt.$$

A lemma bizonyítása:

Bevezetünk egy súlyfüggvényt, ami két lineáris függvényből áll; az $(a - h, a)$ intervallumon 0-tól fut h-ig, az $(a, a + h)$ intervallumon $-h$-tól fut 0-ig, azaz legyen

$$\theta(t) = \begin{cases} t - a + h, & t \in (a - h, a) \\ t - a - h, & t \in (a, a + h) \end{cases}$$

(a-ban nem értelmezzük; egy határértékkel helyettesítjük itt a becslést). Ekkor a parciális integrálási szabály miatt

$$\int_{a-h}^{a+h} \theta(t) g'(t) dt = [\theta(t) g(t)]_{a-h}^{a+h} - \int_{a-h}^{a+h} g(t) dt.$$

Felhasználva, hogy $[\theta(t)g(t)]_{a-h}^{a+h} = 2hg(a)$ azt kapjuk, hogy

$$2hg(a) = \int_{a-h}^{a+h} \theta(t)g'(t)dt + \int_{a-h}^{a+h} g(t)dt.$$

Végül a háromszög egyenlőtlenséget és hogy $|\theta(t)| \leq h$ használva és leosztva $2h$-val kapjuk a lemma állítását.

Használjuk a lemmát a $g(x) = S^2(x)$ függvényre, az a helyén a t_r értékekkel, valamint a $h = \delta/2$-val. Ekkor a $(t_r - \delta/2, t_r + \delta/2)$ intervallumoknak nincs közös része. Így $c := t_1 - \delta/2 < t_2 < \cdots < t_R < 1 + c$. Ezért

$$\sum_{r=1}^{R} |S^2(t_r)| \leq \frac{1}{\delta} \int_c^{1+c} |S^2(t)|dt + \frac{1}{2} \int_c^{1+c} |S(t)S'(t)|dt.$$

Most $S'(t) = 2\pi i \sum_{n=1}^{N} n x_n \epsilon(nt)$, amiből

$$\int_c^{1+c} |S'(t)|^2 dt \leq 4\pi^2 N^2 \sum_{n=1}^{N} |x_n|^2.$$

Végül a Cauchy-Schwarz egyenlőtlenséget és az előbbi becslést használva

$$\int_c^{1+c} |S(t)S'(t)|dt \leq \sqrt{\int_c^{1+c} |S'(t)|^2 dt} \sqrt{\int_c^{1+c} |S(t)|^2 dt} \leq$$

$$\leq \sqrt{4\pi^2 N^2 \sum_{n=1}^{N} |x_n|^2} \sqrt{\sum_{n=1}^{N} |x_n|^2} = 2\pi N \sum_{n=1}^{N} |x_n|^2,$$

amit a $\sum_{r=1}^{R} |S(t_r)|^2$ becslésbe beírva kapjuk az állítást.

Ennek segítségével a 13. fejezetben bizonyítjuk a következő tételt:

10.2.2. Tétel. *Legyen $A \subseteq [1, X]$ és legyen p olyan prím, mely $\leq \sqrt{X}$. Jelölje $E_p(A)$ a moduláris energiát, azaz mindazon (a_1, a_2, a_3, a_4) négyesek számát amelyekre $a_1 + a_2 \equiv a_3 + a_4 (mod) p$. Ekkor*

$$\sum_{p \leq \sqrt{X}} p\Big(E_p(A) - \frac{|A|^4}{p}\Big) \leq 4XE(A).$$

A fenti szitát az additív kombinatorikában az alábbi két formában használjuk:

10.2.3. Tétel. *Legyen* $S(p,h) := \sum_{n \equiv h \pmod p} x_n$. *Ekkor*

$$\sum_{p \le X} p \sum_{h=0}^{p-1} \left| S(p,h) - \frac{1}{p} S(0) \right|^2 \le (\pi N + X^2) \sum_n |x_n|^2.$$

Bizonyítás:

Vegyük észre, hogy bármely két $\frac{r}{p}$ és $\frac{r'}{p'}$ tört különbsége legalább $\frac{1}{p \cdot p'} \ge \frac{1}{X^2} := \delta$.

Elsőként igazoljuk, hogy

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

(egyébként ezt az ötletet többször használtuk, a teljesség kedvéért megismételjük ezt a gondolatot).

Mivel $S(0) = \sum_n x_n$ és $\sum_h S(p,h) = S(0)$ a négyzetre emelésnél a kettős szorzat $-\frac{2}{p} S(0)$ lesz, ezért kapjuk a jobb oldalon álló kifejezést.

Most igazoljuk, hogy

$$p^2 |S(p,h)|^2 = \Big| \sum_{r=0}^{p-1} S\Big(\frac{r}{p}\Big) e_p(-rh) \Big|^2.$$

Valóban, a $\sum_{r=0}^{p-1} S\Big(\frac{r}{p}\Big) e_p(-rh)$ kifejezésbe beírva $S\Big(\frac{r}{p}\Big)$ definícióját

$$\sum_{r=0}^{p-1} S\Big(\frac{r}{p}\Big) e_p(-rh) = \sum_r \sum_n x_n e_p(r(n-h)),$$

ami az ortogonalitás miatt éppen $pS(p,h)$.

Végül

$$\sum_{r=0}^{p-1} \Big| S\Big(\frac{r}{p}\Big) \Big|^2 - |S(0)|^2 = \sum_{r=1}^{p-1} \Big| S\Big(\frac{r}{p}\Big) \Big|^2 =$$

$$= \frac{1}{p} \sum_{r,r'=0}^{p-1} S\Big(\frac{r}{p}\Big) \overline{S\Big(\frac{r'}{p}\Big)} \frac{1}{p} \sum_{h=0}^{p-1} e_p((r'-r)h) - |S(0)|^2 =$$

$$= \frac{1}{p}\sum_h p^2|S(p,h)|^2 - |S(0)|^2 = p\sum_{h=0}^{p-1}\Big|S(p,h) - \frac{1}{p}S(0)\Big|^2$$

Ezt 10.2.1 tételbeli becsléssel kombinálva kapjuk a tétel állítását.

Amennyiben x_n egy A sorozat indikátora, akkor $S(0) = |A|$, továbbá $S(p,h) = A(p,h) := |\{a : a \in A;\ a \equiv h \pmod p\}|$, így ekkor a fenti tétel a következő formában írható:

10.2.4. Tétel.

$$\sum_{p\le X} p\sum_{h=0}^{p-1}\Big|A(p,h) - \frac{1}{p}|A|\Big|^2 \le (\pi N + X^2)|A|.$$

E tétel igen hasznos additív kombinatorikai problémák kezelésére, a paragrafus végén egy rövid példát említünk is.

10.3. A van der Corput egyenlőtlenség

Ebben a fejezetben végül a van der Corput egyenlőtlenséget igazoljuk, aminek segítségével egy felső becslést kapunk Sidon sorozatok elemszámára.

10.3.1. Tétel. *Legyen $I := (a,b]$ valós számok egy korlátos intervalluma, legyen $f : \mathbb{Z} \mapsto \mathbb{C}$ komplex értékű függvény, melyre supp $f \subseteq I$. Ekkor bármely pozitív H számra*

$$\Big|\sum_n f(n)\Big|^2 \le \frac{|I|+H-1}{H}\sum_{-H<h<H}\Big(1-\frac{|h|}{H}\Big)\sum_n f(n)\overline{f(n-h)}.$$

Bizonyítás:
Vegyük észre, hogy $H\sum_n f(n) = \sum_n \sum_{k=1}^H f(n+k)$. Valóban, mivel minden $k-$ra $\sum_n f(n) = \sum_n f(n+k)$, így

$$H\sum_n f(n) = \sum_{k=1}^H\sum_n f(n+k) = \sum_n\sum_{k=1}^H f(n+k).$$

Az $f(x)$ függyvény nulla az $a+1 \leq x \leq b$ intervallumon kívül, így $f(n+k)$ is nulla az $a+1-H \leq n \leq b-1$ intervallumon kívül, azaz amikor n eleme egy $|I|+H-1$ hosszúságú intervallumnak, mivel $1 \leq k \leq H$. Így a fenti egyenlőséget és a Cauchy becslést használva kapjuk, hogy

$$H^2\Big|\sum_n f(n)\Big|^2 \leq (|I|+H-1)\sum_n \Big|\sum_{k=1}^{H} f(n+k)\Big|^2.$$

A jobb oldal utolsó szummáját négyzetre emelve

$$H^2\Big|\sum_n f(n)\Big|^2 \leq (|I|+H-1)\sum_n \Big|\sum_{k=1}^{H} f(n+k)\Big|^2 =$$

$$= (|I|+H-1)\sum_n \sum_{k=1}^{H}\sum_{m=1}^{H} f(n+k)\overline{f(n+m)}$$

alakot kapjuk. Bevezetve a $h := k-m$ változót, az $f(n+k)\overline{f(n+m)} = f(n')\overline{f(n'-h)}$ tag $H-|h|$-szer fog szerepelni. Végül H^2-tel osztva kapjuk a tétel állítását.

10.3.1. Sidon sorozat; két bizonyítás

Egy S sorozatot *Sidon sorozatnak* nevezünk ha $S+S$ (vagy ezzel ekvivalensen $S-S$) egyértelmű módon reprezentálhatóak, azaz

6. Definíció. *Az $S \subseteq \{1,2,\ldots,N\}$ halmaz Sidon, ha $r_S(n) \leq 1$ igaz bármely n értékre, vagy másként, ha bármely $s_1,s_2,s_3,s_4 \in S$ elemekre ha $s_1+s_2 = s_3+s_4$, akkor $\{s_1,s_2\} = \{s_3,s_4\}$.*

Egyszerű leszámlálással könnyű látni, hogy $|S| \leq \sqrt{2N}$. Egy régóta fennálló sejtés, hogy a maximális S nincs túl távol (legfeljebb konstans távolságra) $\sqrt{N}$-től.

A következő tételre három különböző bizonyítást adunk, a későbbiekben a teljesség kedvéért újra kimondjuk (lásd a 13.3.2 Tételt).

10.3.2. Tétel. *Ha $S \subseteq \{1,2,\ldots,N\}$ halmaz Sidon, akkor*

$$|S| \leq \sqrt{N} + \sqrt[4]{N} + 1.$$

(Érdekes módon mindhárom bizonyításban szerepelni fog ez a $\sqrt[4]{N}+1$ "bizonytalansági" tag.)

I. Bizonyítás:

Legyen tehát $S \subseteq I := [1, N]$ egy Sidon halmaz. Használjuk a 10.3.1 tételt az $f(n) = S(n)$ indikátor függvénnyel. Ekkor a belső összegben az $\sum_n S(n)S(n-h)$ értéke S lesz, amennyiben $h = 0$ és egyébként 1. Továbbá könnyű látni, hogy $\sum_{-H<h<H}(1 - \frac{|h|}{H}) = H - 1$. Így

$$|S|^2 \leq \frac{N+H-1}{H}(|S| + H - 1).$$

Legyen $H = \lfloor N^{3/4} \rfloor - 1$ (amely H minden bizonyításban minimalizálja a becslésünket), rövid számolással adódik a tétel állítása. □

II. Bizonyítás:

A már ismert módszer szerint, ha A és B elemszáma m és n, akkor

$$mn = \sum_x r_{A+B}(x),$$

így a Cauchy egyenlőtlenség miatt

$$m^2n^2 = (\sum_x r_{A+B}(x))^2 \leq |A+B| \sum_x r^2_{A+B}(x),$$

ezért

$$\frac{m^2n^2}{|A+B|} \leq \sum_x r^2_{A+B}(x).$$

Itt $E(A,B) = \sum_x r^2_{A+B}(x)$ az additív energia, azokat az (a, a', b, b') négyesek számát méri, amelyekre $a+b = a'+b'$, ami ekvivalens azzal, hogy $a-a' = b'-b$. Ha ez a különbség nem 0, akkor a Sidon tulajdonság miatt $a - a'$ legfeljebb egyféleképpen a $b'-b$ pedig $n(n-1)$ módon állhat elő. Ha a különbség nulla, akkor egymástól függetlenül választhatunk mn féle (a, b) párt. Így

$$\frac{m^2n^2}{|A+B|} \leq \sum_x r^2_{A+B}(x) \leq n(n-1) + nm$$

amiből átrendezéssel adódik az állítás.

Ha $A \subseteq [1, N]$ és $B = \{1, 2, \ldots, n\}$, akkor

$$\frac{m^2n}{m+n-1} \leq |A+B| \leq N + n - 1,$$

most megint az $n := \lfloor m\sqrt{m} \rfloor - m + 1$ választással adódik a Sidon sorozatra az előbbi tételben szereplő becslés. □

10.3.2. Négyzetszámok számtani sorozatokban

Ismeretes, hogy a négyzetszámok száma $x-$ig $\leq \sqrt{x}$. Ezért elég természetes azt sejteni, hogy egyetlen számtani sorozatban sem oszlanak el sűrűbben a $\mathcal{Q}$ négyzetszámok. Ez Rudin sejtése (és megjegyeznénk, hogy e kérdés megoldásának a vágya vezette el Szemerédi Endrét a híressé vált tételének a felfedezéséhez). Az ismert legsűrűbb ilyen sorozat a $\{24n + 1 : 1 \leq n \leq k\}$, amelyben $\sqrt{8k/3}$ négyzetszám van, valamint a legjobb felső becslés Bombieritől és Zanniertől származik. Ők igazolták, hogy egy k hosszú számtani sorozatban legfeljebb k^c négyzetszám van, ami minden $c > \frac{3}{5}$ esetén igaz.

Ebben a paragrafusban a nagy szita segítségével bizonyítjuk, hogy

10.3.3. Tétel. *Legyen $\varepsilon > 0$ és tegyük fel, hogy $d < e^{k^{1/2+\varepsilon}}$. Ekkor*

$$|\mathcal{Q} \cap \{r + id\}_{i=1}^{k}| \ll \sqrt{k} \log k.$$

Bizonyítás:

Legyen $I := \{i_1 < i_2 < \cdots < i_t\}$ azon indexek halmaza, melyekre $r+i_j d \in \mathcal{Q}$. $I \subseteq \{1, 2, \ldots, k\}$. Legyen továbbá $\mathcal{N}_p$ a kvadratikus nem-maradékok halmaza modulo p, ahol p prímszám. Alkalmazzuk most a nagy szita 10.2.4 tételbeli formáját az I halmazra, $N = k$, $X = \sqrt{k}$ választással. Ekkor

$$\sum_{p \leq \sqrt{k}} p \sum_{h=0}^{p-1} \left| I(p,h) - \frac{1}{p}|I| \right|^2 \leq (\pi + 1)k|I| \ll k|I|.$$

Másfelől

$$\sum_{p \leq \sqrt{k}} p \sum_{h=0}^{p-1} \left| I(p,h) - \frac{1}{p}|I| \right|^2 > \sum_{p \leq \sqrt{k};\ p \nmid q} p \sum_{h \in \mathcal{N}_p} \left| I(p,h) - \frac{1}{p}|I| \right|^2$$

Az ilyen h maradékok száma $(p-1)/2$, és az I halmaz definíciója miatt $I(p,h) = 0$. Így

$$\sum_{p \leq \sqrt{k};\ p \nmid q} p \sum_{h \in \mathcal{N}_p} \left| I(p,h) - \frac{1}{p}|I| \right|^2 \geq \sum_{p \leq \sqrt{k};\ p \nmid q} p \frac{p-1}{2} \frac{1}{p}|I|^2 \gg$$

$$\gg |I|^2(\pi(\sqrt{k}) - \nu(q)),$$

ahol $\nu(q)$ q különböző prímosztóinak a számát jelöli. Amennyiben $d < e^{k^{1/2}+\varepsilon}$, úgy $\pi(\sqrt{k}) - \nu(q) \gg \pi(\sqrt{k})$, ezért a fenti becslést folytatva, és a nagy szita felső becslésével összevetve

$$k|I| \gg |I|^2(\pi(\sqrt{k})) \gg |I|^2 \frac{\sqrt{k}}{\log k}$$

amiből átrendezéssel kapjuk a tétel állítását.

Feladatok

1. Elemi módon (tehát a nagy szita nélkül) igazoljuk, hogy $|\mathcal{Q} \cap \{r + id\}_{i=1}^{k}| \leq 2\tau(d)\sqrt{k}\log k$ ahol $\tau(d)$ a d pozitív osztóinak a számával egyenlő.

2. Legyen $S \subseteq \mathcal{Q}$ a négyzetszámok egy m elemű részhalmaza. Igazoljuk, hogy ha létezik $c > 0$, hogy minden S-re $|S + S| > |S|^{1+c}$, akkor

$$|\mathcal{Q} \cap \{r + id\}_{i=1}^{k}| \ll k^{1/(1+c)}.$$

Megoldások

1. Legyen $i_1 < i_2 < \cdots < i_t$ azon indexek sorozata, melyekre $r + i_j d \in \mathcal{Q}$. Azoknak a j indexeknek a száma, melyre $i_{j+1} - i_j > \sqrt{k}$ nyilván $< \sqrt{k}$. Most egy olyan párra, amelyre

$$i_{j+1}d - i_j d = (r + i_{j+1}d) - (r + i_j d) = x^2 - y^2 = (x - y)(x + y)$$

(x, y) megoldásainak a száma rögzített j esetén, ahol $i_{j+1} - i_j \leq \sqrt{k}$ pedig $\leq \tau(i_{j+1}d - i_j d)$, ($\tau(m)$ az m pozitív osztóinak a száma). Így

$$|\mathcal{Q} \cap \{r + id\}_{i=1}^{k}| < \sqrt{k} + \sum_{m \leq \sqrt{k}} \tau(md) \leq \sqrt{k} + \tau(d) \sum_{m \leq \sqrt{k}} \tau(m)$$

felhasználva, hogy $\tau(md) \leq \tau(m)\tau(d)$. Végül, mivel $\sum_{m \leq \sqrt{k}} \tau(m) \leq \sqrt{k}\log k$, kapjuk a kívánt állítást.

2. Legyen $S := \mathcal{Q} \cap \{r + id\}_{i=1}^{k}$. Ekkor $S + S \subseteq (\{r + id\}_{i=1}^{k}) + (\{r + id\}_{i=1}^{k})$ és így

$$|S|^{1+c} < |S + S| < |(\{r + id\}_{i=1}^{k}) + (\{r + id\}_{i=1}^{k})| = 2k - 1$$

ahonnan kapjuk a kívánt becslést.

11. fejezet

Incidencia tételek

11.1. Pont-egyenes illeszkedések

7. Definíció. *Az $\mathcal{L} \subseteq \mathbb{R}^2$ halmazrendszer pszeudo-egyenesek rendszere ha bármely $l, l' \in \mathcal{L}$, $|l \cap l'| \leq 1$.*

A $|l \cap l'| \leq 1$ feltétel helyett mondhattunk volna bármilyen fix konstanst is, könnyen ellenőrizhetően a következő tétel bizonyításában csak egy konstans szorzót jelentene.

A legnevezetesebb a következő:

11.1.1. Tétel. *[Szemerédi-Trotter] Legyen $\mathcal{P}, \mathcal{L}$ pontok és (pszeudo) egyenesek egy rendszere az $\mathbb{R}^2$ síkon. Ekkor*

$$I(\mathcal{P}, \mathcal{L}) = |\{(p, l) \in \mathcal{P} \times \mathcal{L} : p \in l\}| \ll |\mathcal{P}|^{2/3}|\mathcal{L}|^{2/3} + |\mathcal{P}| + |\mathcal{L}|$$

Az alábbi incidencia tételt bizonyítás nélkül idézzük:

11.1.2. Tétel. *[Bourgain-Katz-Tao] Legyen $\mathcal{P}$ és $\mathcal{L}$ az $\mathbb{F}_p \times \mathbb{F}_p$ ponthalmaza és egyenes halmaza, továbbá tegyük fel, hogy $|\mathcal{P}|, |\mathcal{L}| \leq M < p^\alpha$, ahol $\alpha < 2$. Ekkor létezik egy $\gamma > 0$ valós, melyre*

$$|\{((x, y), l) \in \mathcal{P} \times \mathcal{L} : (x, y) \in l\}| \ll M^{3/2-\gamma}.$$

Az alábbi tételt a későbbiekben a két dimenziós esetben bizonyítjuk is:

11.1.3. Tétel. *[L.A.Vinh] Legyen $d \geq 2$, továbbá $\mathcal{P}$ és $\mathcal{H}$ pontok és hipersíkok halmaza az $\mathbb{F}_p^d$ térben. Ekkor*

$$|\{(P,H) \in \mathcal{P} \times \mathcal{H} \ : \ P \in H\}| \leq \frac{|\mathcal{P}||\mathcal{H}|}{p} + (1+o(1))p^{(d-1)/2}(|\mathcal{P}||\mathcal{H}|)^{1/2}.$$

11.1.1. A Szemerédi-Trotter tétel egyszerű bizonyítása

E tételnek több bizonyítása is ismert (pl. Matoušek polinom módszert használó bizonyítása). Mi most a legegyszerűbb (és igen szellemes) bizonyítást közöljük.

Mielőtt ezt megtennénk nézzünk egy gyengébb (és csaknem triviális) állítást:

11.1.4. Tétel. *Legyen $\mathcal{P}, \mathcal{L}$ pontok és pszeudo egyenesek egy rendszere az $\mathbb{R}^2$ síkon. Ekkor*

$$I(\mathcal{P},\mathcal{L}) \ll |\mathcal{P}|\sqrt{|\mathcal{L}|} + |\mathcal{L}|.$$

Bizonyítás:
Legyen

$$m(L) := |\{P : P \in L \ P \in \mathcal{P}; L \in \mathcal{L}\}|.$$

Nyilván

$$\sum_{L \in \mathcal{L}} m(L) = I$$

ahol $I = I(\mathcal{P},\mathcal{L})$. Ekkor a Cauchy egyenlőtlenség miatt

$$I^2 \leq |\mathcal{L}| \sum_{L \in \mathcal{L}} m(L)^2$$

A jobb oldalon azokat a (P, P', L) hármasokat számoljuk le, amelyekre $P, P' \in L$. Ha $P \neq P'$, akkor mivel két különböző pont egyértelműen meghatároz egy egyenest, ezek $|\mathcal{P}|^2$-tel járulnak a jobb oldalhoz. Ha $P = P'$, akkor pont az illeszkedést számoljuk le. Ezeket beírva a becslésbe, kapjuk az állítást. □

A Szemerédi-Trotter tétel bizonyításához először néhány ismert és egyszerűen bizonyítható állítást idézünk fel:

A 11.1.1 tétel bizonyítása:
Elsőként idézzük fel a jól ismert Euler poliéder tételt: ha e, l, c rendre egy (pl. konvex) poliéder éleinek, lapjainak és csúcsainak számát jelöli, akkor

$l+c=e+2$. Egy él két laphoz tartozik, továbbá, mivel minden lap legalább háromszög, kapjuk, hogy $2e \geq 3l$. Ezt a fenti képletbe beírva, kapjuk, hogy $e \leq 3c-6$. Ez egy gömb felületére írt (és így az összes síkbarajzolható) tetszőleges gráf éleinek és csúcsainak a száma közötti összefüggést is adja.

Definiáljuk egy n pontú, e élű egyszerű gráf kereszteződési számát, $Cr(G)$-t a következőképpen: a G gráf síkba nem rajzolhatósága esetén a legkevesebb (nem csúcsban) metsző élek száma. A fenti megjegyzés miatt indukcióval könnyű látni, hogy

$$Cr(G) \geq e-3n.$$

15. Lemma. *Tegyük fel, hogy $e \geq 4n$. Ekkor*

$$Cr(G) \geq \frac{e^3}{64n^2}.$$

A lemma bizonyítása:

A G gráfon p valószínűséggel vegyünk egy véletlen részhalmazt, majd az ezek által feszített részgráfot. E G_p részgráfnak várhatóan np pontja lesz, ep^2 éle (mindkét végpont "életbe kell", hogy maradjon), és legfeljebb $p^4Cr(G)$ kereszteződési száma lesz (egy kereszteződésnél mind a négy élvégpont kell, hogy szerepeljen, és legfeljebb, mert lehet, hogy G_p-t kevesebb kereszteződéssel is le lehet rajzolni). Így ha $E(\cdot)$ jelenti a várható értéket, akkor

$$p^4Cr(G)-p^2e+3pn \geq E(Cr(G_p)-e_p+3n_p) \geq 0,$$

amiből

$$p^4Cr(G)-p^2e+3pn \geq 0,$$

($0 \leq p \leq 1$). Egyszerű szélsőértékszámítással $p := 4n/e$, ezt beírva az előbbi egyenlőtlenségbe kapjuk az állítást. □

A lemma segítségével röviden bizonyítani tudjuk a Szemerédi-Trotter tételt. A G gráf a pont-egyenes konfigurációban legyen a következő: a ponthalmaz a G ponthalmaza, élei pedig az egy egyenesen levő szomszédos pontok közötti szakaszok legyenek. Egy t pontú egyenes esetén tehát $t-1$ él van, összesen pedig $I-|\mathcal{L}|$ élünk van.

Ha $I-|\mathcal{L}|=e<4n$, akkor

$$I<4n+|\mathcal{L}| \ll |\mathcal{P}|^{2/3}|\mathcal{L}|^{2/3}+|\mathcal{P}|+|\mathcal{L}|.$$

A metszési számok száma legfeljebb ahány (pszeudo) egyenes pár van. Azaz $Cr(G) \leq \binom{|\mathcal{L}|}{2}$. Felhasználva a lemmát

$$\frac{e^3}{64n^2} = \frac{(I - |\mathcal{L}|)^3}{64|\mathcal{P}|^2} \leq Cr(G) \leq \binom{|\mathcal{L}|}{2}.$$

Az egyenlőtlenséget I-re rendezve kapjuk az állítást. □

11.1.2. Az incidencia tételek néhány alkalmazása

Elsőként egy nevezetes, máig nem teljesen tisztázott kérdést vizsgálunk, amit az irodalomban *összeg-szorzat problémának* szokás nevezni. A kérdés így hangzik: ha adott egy n elemű A, egészekből álló halmaz, akkor mennyire lehet *együtt* kicsi az $A + A$ és AA halmaz? E kérdést a régről ismert észrevétel motiválhatta, miszerint az egészek additív és multiplikatív struktúrája egészen különböző. Erre egy igen nevezetes sejtés (ma már tétel) Fermat-tól származott: az $x^n + y^n = z^n$ egyenletnek csak triviális megoldásai vannak $n > 2$ esetén. Itt is multiplikatív struktúrát (hatványokat) kellett additív struktúrával összevetni. Visszatérve az eredeti kérdéshez: ha pl. $A = \{2^k : 1 \leq k \leq n\}$, akkor AA nyilván $2n - 1$ elemet tartalmaz, míg az összeghalmaz (a diadikus előállítás egyértelmű) $\binom{n+1}{2}$ elemet. A másik véglet, ha $A = \{k : 1 \leq k \leq n\}$, akkor az összeghalmaz $2n - 1$ elemű, míg a szorzathalmaz (vigyázat nem n^2!) $\sim n^2/(\log n)^c$ (valamilyen $c > 0$) elemű. Erdős és Szemerédi így azt sejtették, hogy $\min |\{|A+A|, |AA|\}| > n^{2-\varepsilon}$. A paragrafus végén látni fogjuk, hogy ha a problémát gráfok mentén vizsgáljuk, akkor e sejtés már nem marad igaz; létezik olyan G_n gráf, melynek csúcspontjai az A elemei lesznek, és két elem összegét ill. szorzatát akkor tekintjük, ha az általuk megadott két pont éllel van összekötve.

Az első igazán komoly lépés elhagyta azt a feltételt, hogy a halmaz elemei egészek, elég volt a valós számokra gondolni (elképzelhető, hogy az egészekre és a valósokra különböző lesz a válasz). Ez az eredmény adott nagy lökést az ilyen vizsgálatoknak. A bizonyítás Elekes Györgytől származik:

11.1.5. Tétel. *Legyen $A \subseteq \mathbb{R}$, $|A| = n$, Ekkor*

$$\min |\{|A + A|, |AA|\}| \gg n^{1.25}$$

Bizonyítás

Tekintsük a síkon az $(A+A)\times(AA)$ ponthalmazt, és legyen az egyeneseink halmaza $\{a(x-a') : a, a' \in A\}$. Az egyenesek száma nyilván n^2, a ponthalmaz elemszáma pedig $|(A+A)\times(AA)|$. Minden egyenesre illeszkednek az $(a'+a'', aa'')$ alakú pontok, így az illeszkedések száma legalább n^3. A Szemerédi-Trotter tétel értelmében így

$$n^3 \leq I \ll (|(A+A)\times(AA)|\cdot n^2)^{2/3} + |(A+A)\times(AA)| + n^2.$$

ambiből rövid számolással kapjuk a tételt. □

A ma ismert legjobb eredmény Konyagin-Shkredov szerzőpárostól származik.

Másodikként konvex halmazokra igazolunk egy állítást. Emlékeztetnénk, erre az állításra a 3.1.3 tétel bizonyításánál volt szükségünk, ahol konvex sorozatok összeghalmazára adtunk becslést.

11.1.6. Tétel. *Legyen $A = \{a_1 < a_2 < \cdots < a_n\}$ valós számok egy konvex sorozata (azaz bármely $i = 1, 2, \ldots, n-1$ esetén $a_i - a_{i-1} \leq a_{i+1} - a_i$ teljesül). Legyen $B \subseteq \mathbb{R}$ és $r(x) = r_{A+B}(x)$. Ekkor*

$$|\{x : r(x) \geq T\}| \ll \frac{|A||B|^2}{T^3}.$$

Bizonyítás:

Jelölje I az $\{1, 2, \ldots, n\}$ intervallumot, legyen $\mathcal{P} = (I+I)\times(A+B)$ a pontok halmaza és legyen $\mathcal{L} := \{l_{uv} : u \in I;\ v \in B\}$ pedig a pszeudo-egyenesek halmaza, ahol $l_{uv} = \{(r+u, a+v) : r \in I; a \in A\}$.

Mivel A konvex, így bármely két $l_{uv}, l_{u'v'}$ egyenesre teljesül, hogy $|l_{uv} \cap l_{u'v'}| \leq 1$ (l_{uv} és $l_{u'v'}$ diszkrét pontok illeszkednek egy-egy konvex függvénygörbére; tehát $\mathcal{L}$ tényleg pszeudo-egyenesek halmaza).

Jelölje $\mathcal{P}_T$ azon $\mathcal{P}$-beli pontok halmazát, melyek legalább T pszeudo-egyeneshez tartoznak. Belátjuk, hogy

$$|\{x : r(x) \geq T\}| \leq \frac{|\mathcal{P}_T|}{|A|}.$$

Valóban, jelölje $A +^T B$ azon $x \in A+B$ elemek halmazát, melyekre $r(x) \geq T$. Nyilván $\mathcal{P}_T = (I+I)\times(A+^T B)$. Mivel $|I| = |A|$ és $|I+I| = 2|I|-1$ ezért

$$|\{x \in A+B : r(x) \geq T\}| = |A +^T B| = \frac{|\mathcal{P}_T|}{|I+I|} < \frac{|\mathcal{P}_T|}{|A|}.$$

Most nyilván

$$T \cdot |\mathcal{P}_T| \leq I(\mathcal{P}_T, \mathcal{L})$$

(A definíció miatt az incidenciák száma $\mathcal{P}_T$ elemeiben legalább T.) A Szemerédi-Trotter incidencia tétel miatt most már belátjuk tételünk állítását: először is

$$I(\mathcal{P}_T, \mathcal{L}) \ll |\mathcal{P}_T|^{2/3}|\mathcal{L}|^{2/3} + |\mathcal{P}_T| + |\mathcal{L}|.$$

Mivel $|\mathcal{P}_T| < 2|I||A +^T B| \leq 2|A|^2|B| \leq |A|^2|B|^2 = |\mathcal{L}|^2$ ($|B| \geq 2$ esetén) és

$$|\mathcal{P}_T| \leq |\mathcal{L}|^2 \;\Leftrightarrow\; |\mathcal{P}_T|^{2/3}|\mathcal{L}|^{2/3} > |\mathcal{P}_T|$$

így

$$I(\mathcal{P}_T, \mathcal{L}) \ll |\mathcal{P}_T|^{2/3}|\mathcal{L}|^{2/3} + |\mathcal{L}|.$$

1. eset: $|\mathcal{P}_T|^{2/3}|\mathcal{L}|^{2/3} \leq |\mathcal{L}|$. Ekvivalens formában $|\mathcal{P}_T|^2 \leq |\mathcal{L}|$. Használva $|\mathcal{P}_T| > |I||A +^T B|$ becslést ekkor

$$|A|^2|A +^T B|^2 < |A||B|,$$

amiből

$$|A +^T B| \leq \sqrt{\frac{|B|}{|A|}} < \frac{|A||B|^2}{T^3}$$

mivel $T \leq \min\{|A|, |B|\}$.

2. eset: $|\mathcal{P}_T|^{2/3}|\mathcal{L}|^{2/3} > |\mathcal{L}|$. Ekkor

$$I(\mathcal{P}_T, \mathcal{L}) \ll |\mathcal{P}_T|^{2/3}|\mathcal{L}|^{2/3},$$

és mivel $T \cdot |\mathcal{P}_T| \leq I(\mathcal{P}_T, \mathcal{L})$ azt kapjuk, hogy

$$|\mathcal{P}_T| \leq \frac{|\mathcal{L}|^2}{T^3}.$$

Végül felhasználva $\mathcal{P}_T$ definícióját, kapjuk az állításunkat. □

11.1.3. Expander polinomok

Egy prímtestbeli $f(x, y)$ polinomot expander polinomnak nevezzük, ha a tárgyhalmazát "nagyítja" (lásd később). A következő tétel J. Bourgain-től származik,

11.1.7. Tétel. *Legyen $f(x,y) = x^2 + xy$. Ekkor létezik olyan $\delta > 0$ valós, hogy bármely $A, B \subseteq \mathbb{F}_p$, $|A| = |B| = N$ részhalmazokra*

$$|f(A,B)| > |A|^{1+\delta}.$$

Továbbá ha $N = p^\beta,\ \beta > 3/4$ akkor

$$|f(A,B)| \gg N^{1+\frac{1-\beta}{2\beta}}.$$

Bizonyítás:

Legyen $X := \{a(a+b) :\ a \in A;\ b \in B\}$ és a pontok halmaza $\mathcal{P} = X \times X$. Definiáljuk az egyeneseket $\mathcal{L} = \{y = \alpha x + \beta :\ \alpha, \beta\}$ természetes módon. Megadjuk az α és β paramétereket úgy, hogy az $\{a_1(a_1+b), a_2(a_2+b) :\ a_1, a_2 \in A;\ b \in B\}$ pontok illeszkejenek egy egyenesre. Ehhez

$$a_2(a_2+b) = \alpha a_1(a_1+b) + \beta$$

szükséges. Ha $\alpha = \frac{a_2}{a_1}$ akkor a hozzátartozó $\beta = a_1^2 - a_1 a_2$.

a_1, a_2, b értékeit szabadon választva, legalább N^3 illeszkedés található.

Most a 11.1.2 tételt felhasználva egy pozitív γ valósra

$$N^3 \ll (|X|^2)^{3/2-\gamma}$$

amiből $|X| \gg N^{1+\gamma'}$ $(\gamma' > 0)$.

Mint láttuk at egyenesek száma $\asymp N^2$. Amikor $\beta > 3/4$ használhatjuk 11.1.3 tételt; mivel az első tag dominál a második tag felett azt kapjuk, hogy

$$N^3 \ll \frac{|\mathcal{P}||\mathcal{L}|}{p} \ll \frac{|X|^2 N^2}{p}$$

amiből a tétel második fele következik. □

Háromváltozós expander polinomokra még erősebb becslés nyerhető:

11.1.8. Tétel. *Legyen $f(x,y,z) = xy + z$. Ekkor*

$$|f(A,A,A)| > p - \frac{p^2}{|A|^3}.$$

Azaz, ha $|A| = p^\alpha$, akkor $|\mathbb{Z}_p \setminus (A + AA)| \leq p^{2-3\alpha/4}$.

Bizonyítás:

Használni fogjuk két dimenzióra a 11.1.3 tételt;

Legyen a pontok halmaza a $\mathcal{P} := A \times (A + AA)$ és legyen az egyenesek $\mathcal{L}$ halmaza az

$$\ell_{a,b} = \{(x, y) \in \mathbf{F}_p^2 \,:\, y = b + ax\}, \quad a, b \in A.$$

Nyilván $|\mathcal{P}| = |A||A + AA|$ és $|\mathcal{L}| = |A|^2$. Ekkor a 11.1.3 tétel $d = 2$ esetben

$$\mathrm{Incid}(P, L) := \big|\{(\pi, \ell) \in \mathcal{P} \times \mathcal{L} \text{ melyre } \pi \in \ell\}\big| \leq \frac{|P||L|}{p} + \sqrt{p|P||L|}.$$

Minden $(c, b + ac)$ pont ($a, b, c \in A$), rajta van az $\ell_{a,b}$ egyenesen, amiből $\mathrm{Incid}(P, L)$ legalább $|A|^3$ és így

$$|A|^3 \leq \frac{|A|^3|A + AA|}{p} + \sqrt{p|A|^3|A + AA|},$$

vagy $|A|^3$-bel osztva

$$1 \leq \frac{|A + AA|}{p} + \sqrt{p\frac{|A + AA|}{|A|^{3/2}}}.$$

Legyen $\alpha = p/2|A|^{3/2}$ és $\beta = \sqrt{|A + AA|/p}$, ekkor az előző becslés az

$$1 \leq \beta^2 + 2\alpha\beta$$

alakba írható. Mivel $\beta \leq 1$, ezért

$$\beta^2 \geq 1 - 2\alpha,$$

amiből

$$|A + AA| > p - \frac{p^2}{|A|^3}. \quad \square$$

A 13.4.3 tételben – használva a diszkrét Fourier analízis módszerét – az $\alpha > \frac{4}{9}$ esetben a fenti tételnél jobb becslést kapunk.

Feladatok

1. Igazoljuk, hogy a mátrixok struktúrájában már nem igaz az összegszorzat sejtés.

2. Készítsünk olyan n elemű $A \subseteq \mathbb{R}$ halmazt és G_n gráfot, melyre $V = A$ és az összeget, szorzatot csak olyan a, a' párra tekintjük, amely párra az (a, a') a gráf egy éle, és amelyre nem teljesül, hogy $\min\{|A +_{G_n} A|, |A \cdot_{G_n} A|\} \gg |A|^{2-\epsilon(n)}$, ahol $\epsilon(n) \to 0$, amint $n \to \infty$. Az élszámra követeljük meg az $n^{1+c};\ c > 0$ alsó korlátot.

3. Legyen $A \subseteq \mathbb{R}$ és $Q = \{a^2 : a \in A\}$. Bizonyítsuk be, hogy

$$\max\{|A + A|, |Q + Q|\} \gg |A|^{5/4}.$$

4. Legyen $H < \mathbb{F}_p^*$ egy tetszőleges multiplikatív részcsoport, $A \subset \mathbb{F}_p^*$ tetszőleges halmaz. Mutassuk meg, hogy az $E(H, A)$ additív energiára igaz az

$$E(H, A) \ll \frac{|H|^2|A|^2}{p}$$

nem triviális becslés, feltéve, hogy $|H|\sqrt{|A|} > p$. (Nem triviális, ugyanis $\frac{|H|^2|A|^2}{p}$ mindig kisebb, mint a triviális $|H||A|^2$).

Megoldás

1. Vegyük az

$$A = \left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} : 1 \le k \le n \right\}$$

halmazt. Könnyű látni, hogy ekkor $A+A$ és AA együttes nagyságrendje nem különbözik A halmaz nagyságrendjétől.

2. (Ruzsa) Vegyük a következő paramétereket: legyen $k, m \in \mathbb{N}$. Legyen $U := \{p : 2 \le p \le k\}$, $V := \{q : 2 \le q \le m\}$, ahol p és q is prímszámot jelöl. Álljon A a következő racionális számokból:

$$A := \left\{ \frac{p_1 q}{p_2} : p_1, p_2 \in U;\ q \in V \right\}.$$

Ekkor $|A| = n \sim \frac{k^2}{\log^2 k} \frac{m}{\log m}$. Legyen a G_n gráf éleinek a halmaza a következő: $(a_1, a_2) \in A \times A$ él akkor és csak akkor, ha $a_1 = \frac{p_1 q_1}{p_2}$ és $a_2 = \frac{p_2 q_2}{p_1}$. Így

$$A \cdot_{G_n} A = \{q_1 q_2 : q_1, q_2 \in V\}$$

és ezért $|A \cdot_{G_n} A| \sim \frac{m^2}{\log^2 m}$, továbbá

$$A +_{G_n} A = \left\{ \frac{p_1^2 q_1 + p_2^2 q_2}{p_1 p_2} \right\}$$

és ezért $|A +_{G_n} A| \sim k^4 m$.

Most a paramétereket úgy választva, hogy $|A \cdot_{G_n} A| \simeq |A +_{G_n} A|$ teljesüljön azt kapjuk, hogy $\frac{m}{\log^2 m} \simeq k^4$ és így $|A \cdot_{G_n} A| \simeq |A +_{G_n} A| \ll n^{4/3} \log^6 n$.

3. Legyen $\mathcal{X} = (A + A) \times (Q + Q)$ pontok halmaza, a pszeudo-egyenesek (itt parabolák) pedig $\mathcal{L} = \{p_{a,a'} = y = (x - a)^2 + a'^2 : a, a' \in A\}$. Ezek szám $|\mathcal{L}| \gg |A|^2$. Ekkor bármely $(a" + a, a"^2 + a'^2)$ pont eleme ennek a parabolának. Az $a, a', a"$ elemek szabadon választhatóak, tehát az illeszkedések száma $\geq |A|^3$.

A Szemerédi-Trotter illeszkedési tétel miatt tehát az illeszkedések száma

$$\leq |(A + A) \times (Q + Q)|^{2/3} |A|^{4/3} + |(A + A) \times (Q + Q)| + |A|^2.$$

A két becslést összevetve

$$|A|^{5/2} \ll |(A + A) \times (Q + Q)|,$$

amiből az állítás következik.

4. Tekintsük a háromdimenziós tér következő síkjait:

$$hx + a = h'y + z, \quad h, h' \in H;\ a \in A,$$

és vizsgáljuk a $H \times H \times A$ ponthalmazon az illeszkedést. Ezek száma $|H|^2 E(H, A)$, mivel egy $x = h_1,\ y = h_2$ párhoz azokat a h, h', a, a' négyeseket kell megtalálni, melyekre

$$hh_1 + a = h'h_2 + a'$$

teljesül, felhasználva , hogy $hh_1, h'h_2 \in H$, ami éppen $|H|^2 E(H, A)$. MOst a ponthalmaz elemszáma és a síkok elemszáma ugyancsak $|H|^2 |A|$, az állítás feltételeit felhasználva a 11.1.3 tételben – $|H|\sqrt{|A|} > p$ miatt – a domináns tag a $\frac{|\mathcal{P}||\mathcal{L}|}{p}$ lesz, így e tételt használva

$$|H|^2 E(H, A) = I(\mathcal{P}, \mathcal{L}) \ll \frac{|\mathcal{P}||\mathcal{L}|}{p} = \frac{|H|^2 |A||H|^2 |A|}{p},$$

amiből átrendezéssel adódik az állítás.

11.2. Additív illeszkedések

A paragrafus címe "Additív illeszkedések". E címben arra kívánunk utalni, hogy bizonyos összeghalmazok speciális (itt Sidon) halmazokban való előfordulásra (illeszkedésére) milyen becslést kaphatunk. Érdekes módon – és ezt majd látni fogjuk a Gráf spektrum technika fejezetben, ahol az adjacencia mátrixok hatványai is valamilyen illeszkedésnek foghatóak fel – a geometria illeszkedések, az additív illeszkedések és a gráf spektrum technika alkalmazásával kapható illeszkedések állításai sok esetben bizonyíthatóak a másik két technika segítségével. Lássuk tehát a címben szereplő tételt:

11.2.1. Tétel. *Legyen G egy tetszőleges véges kommutatív csoport és legyen $A, B, C \subseteq G$ három nem üres részhalmaza, ahol A egy Sidon halmaz, (azaz $\forall x \in G, r_{A-A}(x) \leq 1$). Legyen $\Delta := |G| - |A|^2 > 0$. Ekkor*

$$|\{b + c \in A : b \in B \ c \in C\}| = \frac{|A||B||C|}{|G|} + \alpha\sqrt{|B||C|} \cdot \sqrt[4]{|G|},$$

ahol $\alpha \leq \sqrt{1 + \frac{\Delta}{\sqrt{|G|}}}$.

(Jegyezzük meg, hogy egy könnyű leszámolás miatt $|G| - |A|^2 > 0$, továbbá olyan csoportoknál érdekes, ahol $|G| - |A|^2 = o(|G|)$, azaz van "nagy" Sidon sorozat. Egyéb esetekben is igaz a fenti tétel, csak a második "hiba" tag dominál, az állítás nem használható jól.)

Bizonyítás:
Elsőként egy lemmát bizonyítunk.

16. Lemma.

$$\sum_{x \in G} \left(r_{A-B}(x) - \frac{|A||B|}{|G|} \right)^2 \leq |B|(|A| - 1) + |B|^2 \frac{|G| - |A|^2}{|G|}.$$

A lemma bizonyítása:
Először a $\sum_{x \in G} r_{A-B}^2(x)$ kifejezést fogjuk felülről becsülni.

$$\sum_{x \in G} r_{A-B}^2(x) = \sum_{x \in G} r_{A-A}(x) r_{B-B}(x).$$

(Ez nyilván $a-a'=b-b' \Leftrightarrow a-b=a'-b'$ közvetlen következménye.) Így mivel $r_{A-A}(x) \leq 1$

$$\sum_{x\in G} r_{A-B}^2(x) \leq |A||B| + \sum_{x\neq 0; x\in G} r_{B-B}(x) = |A||B| + |B|^2 - |B|.$$

Most

$$\sum_{x\in G} \Big(r_{A-B}(x) - \frac{|A||B|}{|G|}\Big)^2 = \sum_{x\in G} r_{A-B}^2(x) - \frac{|A|^2|B|^2}{|G|}.$$

Valóban

$$\sum_{x\in G} \Big(r_{A-B}(x) - \frac{|A||B|}{|G|}\Big)^2 = \sum_{x\in G} r_{A-B}^2(x) - 2\frac{|A||B|}{|G|}\sum_{x\in G} r_{A-B}(x) + \sum_{x\in G}\frac{|A|^2|B|^2}{|G|^2}.$$

és mivel $\sum_{x\in G} r_{A-B}(x) = |A||B|$, kapjuk a fenti kifejezést. Ezért

$$\sum_{x\in G} \Big(r_{A-B}(x) - \frac{|A||B|}{|G|}\Big)^2 \leq |A||B| + |B|^2 - |B| - \frac{|A|^2|B|^2}{|G|},$$

ami a kívánt állítást adja. □

Mivel

$$|\{b+c\in A : b\in B\ c\in C\}| = \sum_{c\in C} r_{A-B}(c)$$

ezért

$$|\{b+c\in A : b\in B\ c\in C\}| - \frac{|A||B||C|}{|G|} = \sum_{c\in C}\Big(r_{A-B}(c) - \frac{|A||B|}{|G|}\Big) \leq$$

használva a Cauchy egyenlőtlenséget

$$\leq \sqrt{|C|}\sqrt{\sum_{c\in C}\Big(r_{A-B}(c) - \frac{|A||B|}{|G|}\Big)^2} \leq \sqrt{|C|}\sqrt{\sum_{x\in G}\Big(r_{A-B}(c) - \frac{|A||B|}{|G|}\Big)^2} \leq$$

a lemmát használva

$$\leq \sqrt{|C|}\sqrt{|B|(|A|-1) + |B|^2\frac{|G|-|A|^2}{|G|}} = \sqrt{|C||B|}\sqrt{|A| - 1 + |B|\frac{|G|-|A|^2}{|G|}}.$$

Így

$$|\{b+c \in A : b \in B\ c \in C\}| - \frac{|A||B||C|}{|G|} <$$

$$< \sqrt{|C||B|}\sqrt{\sqrt{|G|-\Delta}+|B|\frac{\Delta}{|G|}} \leq \sqrt{|B||C|}\cdot \sqrt[4]{|G|}\sqrt{1+\frac{\Delta}{\sqrt{|G|}}},$$

($|B| \leq |G|$). $\square$

A fenti "additív incidencia tétel" segítségünkre lesz, hogy a 11.1.3 tétel speciális esetét igazoljuk (amikor $d=2$):

11.2.2. Tétel. *Legyenek $\mathcal{P}$ és $\mathcal{L}$ pontok és egyenesek halmazai $\mathbb{F}_p \times \mathbb{F}_p-$ben. Ekkor*

$$|\{(p,l) \in \mathcal{P}\times\mathcal{L}\ :\ p \in l\}| \leq \frac{|\mathcal{P}||\mathcal{L}|}{p} + Cp^{1/2}(|\mathcal{P}||\mathcal{L}|)^{1/2},$$

ahol $C>0$ konstans.

(Itt C nagyobb lesz, mint 1, ám az alkalmazásokat ez lényegesen nem érinti).

Bizonyítás:
Egy lemmára itt is szükségünk lesz:

17. Lemma. *Legyen g az $\mathbb{F}_p^*$ multiplikatív csoport egy generátora és legyen*

$$A = \{(x, g^x) : x \in \mathbb{F}_p^*\} = \{(ind_g y, y) : y \in \mathbb{F}_p^*\}.$$

Ekkor A Sidon halmaz.

A lemma bizonyítása:
Legyen $(x_1, g^{x_1}) - (x_2, g^{x_2}) = (z_1, z_2)$. Ha $z_1 = 0$, akkor $x_1 = x_2$, és így $(x_1, g^{x_1}) = (x_2, g^{x_2})$. Tehát $z_1 \neq 0$, így $x_1 = x_2 + z_1$, amiből

$$g^{x_2+z_1} - g^{x_2} = g^{x_2}(g^{z_1}-1) = z_2,$$

azaz, ha (z_1, z_2) adott, $g^{z_1}-1 \neq 0$, tehát

$$g^{x_2} = \frac{z_2}{g^{z_1}-1} \quad \Rightarrow \quad x_2 = ind_g\Big(\frac{z_2}{g^{z_1}-1}\Big),$$

amiből, $x_1 = x_2 + z_1$ miatt x_1 is egyértelműen adódik. □

Legyen $|\mathcal{P}| = N,\ |\mathcal{L}| = M$, és legyen $\mathcal{P} = \{(p_k, q_k) : k = 1, 2, \ldots, N\}$, valamint $\mathcal{L} = \{y = a_i x + b_i : i = 1, 2, \ldots, M\}$ $\mathbb{F}_p \times \mathbb{F}_p$ pontjainak és egyeneseinek a halmaza.

Álljon B halmaz a $B := \{(ind_g a_i, -b_i) : i = 1, 2, \ldots, M\}$ C pedig legyen $C := \{(ind_g p_j, q_j) : j = 1, 2, \ldots, N\}$ és $A = \{(ind_g y, y) : y \in \mathbb{F}_p^*\}$.

$$B + C = \{(ind_g a_i p_j, q_j - b_i) : i = 1, 2, \ldots, M\ j = 1, 2, \ldots, N\},$$

és $B + C-$beli elem pontosan akkor van az A halmazban, ha

$$a_i p_j = q_j - b_i \ \Leftrightarrow\ q_j = a_i p_j + b_i,$$

azaz a pont illeszkedik egy egyenesre. A 11.2.1 tétel miatt így

$$|\{(p, l) \in \mathcal{P} \times \mathcal{L}\ :\ p \in l\}| = |\{b + c \in A : b \in B\ c \in C\}| <$$

$$< \frac{|A||B||C|}{|G|} + \sqrt{3}\sqrt{|B||C|} \cdot \sqrt[4]{|G|} < \frac{|B||C|}{p} + \sqrt{3}\sqrt{|B||C|} \cdot \sqrt{p} =$$

$$= \frac{|\mathcal{P}||\mathcal{L}|}{p} + \sqrt{3} p^{1/2} (|\mathcal{P}||\mathcal{L}|)^{1/2}.$$

□

11.3. Gráf spektrum technika

Egy $G(V, E)$ gráfon egy véges V csúcshalmazú, irányítatlan, többszörös élt nem tartalmazó, esetleg hurokélt tartalmazó E élhalmazú struktúrát értünk.

$G-$hez hozzárendelhetjük – kölcsönösen egyértelműen – az $n \times n$ négyzetes $M\ adjacencia$ mátrixát, ahol n a G véges gráf pontjainak a száma, így: az $i-$edik sor $j-$edik elemét $M_{ij}-$vel jelölve e mátrixban $M_{ij} = 1$, ha az $i-$edik pont $j-$vel össze van kötve, azaz $(i, j) \in E$, máskülönben $M_{ij} = 0$.

M nyilván szimmetrikus mátrix, azaz bármely i, j esetén $M_{ij} = M_{ji}$.

Most röviden összefoglaljuk azokat a fogalmakat és tételeket a lineáris algebra területéről, amelyekre a továbbiakban szükségünk lesz. A bizonyítások egyes lépéseit feladatként tűzzük ki.

Legyen M egy tetszőleges $n \times n$ négyzetes mátrix, $\lambda \in \mathbb{C}$ komplex szám, $\overrightarrow{v}$ egy nem nulla vektor.

11.3.1. Sajátérték, sajátvektor

Az

$$M\overrightarrow{v} = \lambda\overrightarrow{v}$$

egyenletet kielégítő λ-t az M *sajátértékének,* $\overrightarrow{v}-$t M *sajátvektorának* nevezzük.

λ-t a

$$\det(M - \lambda I) = 0$$

egyenlet megoldásai adják, ahol I az $n \times n-$es egységmátrix.

11.3.1. Tétel. *Legyen M a G gráf adjacencia mátrixa. Ekkor M minden sajátértéke valós.*

Tulajdonképpen elég lett volna azt írni, hogy a mátrix *szimmetrikus* t.i. az adjacencia mátrixnak csak ezt a tulajdonságát fogjuk használni.

Bizonyítás: Legyen $z = a + ib$ komplex szám konjugáltja $z^* = a - ib$. Definiáljuk $\overrightarrow{u}$ és $\overrightarrow{v}$ vektor skaláris szorzatát így

$$\overrightarrow{u} \cdot \overrightarrow{v} := \sum_{i=1}^{n} u_i^* v_i,$$

ahol u_i, v_i a két vektor $i-$edik koordinátáját jelöli. Legyen λ egy sajátérték, $\overrightarrow{v}$ sajátvektora $M-$nek. Nyilván elég igazolni, hogy $\lambda = \lambda^*$.

1. Feladat: Bizonyítsuk be, hogy $(\overrightarrow{u} \cdot \overrightarrow{v})^* = \overrightarrow{v} \cdot \overrightarrow{u}$, továbbá, hogy $\overrightarrow{u} \cdot \overrightarrow{u} = |\overrightarrow{u}|^2$.

Most

$$(M\overrightarrow{v}) \cdot \overrightarrow{v} = \sum_{i=1}^{n}\sum_{j=1}^{n} M_{ij}^* u_j^* u_i =$$

$$= \sum_{j=1}^{n}\sum_{i=1}^{n} M_{ji} u_i u_j^* = \overrightarrow{v} \cdot (M\overrightarrow{v})$$

mivel $M_{ij}^* = M_{ji}$ a szimmetria miatt és mivel valós számról van szó.

Végül

$$(M\overrightarrow{v}) \cdot \overrightarrow{v} = \lambda^* |\overrightarrow{v}|^2 =$$

$$= \overrightarrow{v} \cdot (M\overrightarrow{v}) = \lambda |\overrightarrow{v}|^2$$

és mivel a sajátvektor nem nulla, következik, hogy $\lambda^* = \lambda$, azaz λ valós. □

Definició: Egy λ sajátérték *algebrai multiplicitásán* azt értjük, hogy λ a $\det(M - \lambda I) = 0$ egyenletnek hányszoros gyöke.

Geometriai multiplicitásán pedig, hogy a $\lambda-$hoz tartozó sajátaltérnek mekkora a dimenziója.

Bizonyítás nélkül közöljük, hogy

11.3.2. Tétel. *Bármely M mátrix esetén, ha λ egy sajátértéke, akkor geometriai multiplicitása legfeljebb az algebrai multiplicitással egyenlő.*

Végül

11.3.3. Tétel. *Ha M egy szimmetrikus mátrix, $\lambda_1 \neq \lambda_2$ két sajátértéke, a sajátaltereik merőlegesek egymásra.*

Bizonyítás: Legyen $\overrightarrow{u_1}, \overrightarrow{u_2}$ a két valós sajátértékhez tartozó egy-egy sajátvektor. Az M szimmetriájából, valamint abból, hogy a két sajátérték valós következik, hogy

$$(M\overrightarrow{u_1}) \cdot \overrightarrow{u_2} = \overrightarrow{u_1} \cdot (M\overrightarrow{u_2}).$$

Mivel

$$(M\overrightarrow{u_1}) \cdot \overrightarrow{u_2} = \lambda_1 \overrightarrow{u_1} \cdot \overrightarrow{u_2},$$

továbbá

$$\overrightarrow{u_1} \cdot (M\overrightarrow{u_2}) = \lambda_2 \overrightarrow{u_1} \cdot \overrightarrow{u_2}$$

következik, hogy

$$(\lambda_1 - \lambda_2)\overrightarrow{u_1} \cdot \overrightarrow{u_2} = 0.$$

De $\lambda_1 - \lambda_2 \neq 0$, amiből viszont következik, hogy

$$\overrightarrow{u_1} \cdot \overrightarrow{u_2} = 0,$$

azaz a két sajátvektor merőleges egymásra és így a két sajátaltér is merőleges egymásra. □

Jegyezzük meg, a Gram-Schmidt ortogonalizációs eljárás miatt a sajáltérben is van egy ortogonális bázis (azaz olyan bázis melyben bármely két különböző elem merőlegesegymásra).

A fenti tételeket összevetve kapjuk (tekintve, hogy páronként merőleges vektorrendszer lineárisan független).

11.3.4. Tétel. *Ha M egy szimmetrikus mátrix, akkor a normált sajátvektoraik egy ortonormált bázist alkotnak.*

2. Feladat: Legyen M egy adjacencia mátrix. Bizonyítsuk be, hogy M_{ij}^2 az $i-$edik pontot a $j-$edik ponttal összekötő 2 hosszúságú utak számát adja meg.

3. Feladat: Legyen S és T a G gráf ponthalmazának két nem üres részhalmaza. Legyen $\overrightarrow{v_S}, \overrightarrow{v_T}$ két n dimenziós vektor, ahol a $\overrightarrow{v_S}$ $i-$edik koordinátája 1, ha $i \in S$, és 0, ha $i \notin S$. Hasonlóan definiáljuk a $\overrightarrow{v_T}$ vektort. Bizonyítsuk be, hogy

$$\overrightarrow{v_S} M \overrightarrow{v_T} = e(S,T).$$

11.3.2. Reguláris gráfokra vonatkozó tételek

A következőkben egy fontos állítást bizonyítunk (amit az irodalomban "Expander Mixing Lemma"-nak neveznek)

11.3.5. Tétel. *Legyen G egy n pontú d-reguláris gráf. Legyenek a sajátértékei $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. Legyen $\lambda = \lambda(G) = \max\{|\lambda_2|, |\lambda_n|\}$. Ekkor bármely $S, T \subseteq V$ halmazokra*

$$\left| e(S,T) - \frac{d}{n}|S||T| \right| \leq \lambda \sqrt{|S||T|}.$$

A tételnek egy fontos értelmezése a következő: minden pontból d él indul ki, tehát ha véletlenszerűen indítunk egy élt egy adott i pontból a j pontba ennek $\approx \frac{d}{n}$ a valószínűsége. Így egy S és egy T ponthalmaz között várhatóan

$\frac{d}{n}|S||T|$ él fut. Tehát a tényleges $e(S,T)$ él és a "várható" $\frac{d}{n}|S||T|$ között "kicsi" a különbség, ha $\lambda\sqrt{|S||T|}$ kicsi, tehát ha λ kicsi.

Röviden, ha egy G gráf olyan, melynek adjacencia mátrixában a második legnagyobb sajátérték "kicsi", akkor a gráf olyan, mintha egy véletlen gráf lenne.

4. Feladat: Legyen G egy n pontú d reguláris gráf. Ekkor adjacencia mátrixának legnagyobb sajátértéke éppen d, $\overrightarrow{e_1}$ normált sajátvektorának minden koordinátája $\frac{1}{\sqrt{n}}$.

A 4. feladat szerint tehát ha nagy a hézag a legnagyobb és abszolútértékben rákövetkező legnagyobb sajátérétk között, akkor a gráf olyan, mintha egy véletlen gráf lenne.

A 11.3.5 tétel bizonyítása:

Jelölje a sajátvektorok alkotta ortonormált bázist $\{\overrightarrow{e_i}\}_{i=1}^{n}$.

Vegyük az $S,T \subseteq V$ halmazokat, és tekintsük az általuk definiált karakterisztikus vektorokat (azaz $\overrightarrow{v_S}$ $i-$edik koordinátája 1, ha $i \in S$, és 0, ha $i \notin S$, hasonlóan a $\overrightarrow{v_T}$ vektorra). Írjuk fel a két vektort a sajátvektorok alkotta ortonormált bázisban:

$$\overrightarrow{v_S} = \sum_i \alpha_i \overrightarrow{e_i} \quad \overrightarrow{v_T} = \sum_j \beta_j \overrightarrow{e_j}$$

A 3. feladat szerint és használva, hogy $\overrightarrow{e_j}-$k sajátvektorok

$$e(S,T) = \overrightarrow{v_S} M \overrightarrow{v_T} = \Big(\sum_i \alpha_i \overrightarrow{e_i}\Big) M \Big(\sum_j \beta_j \overrightarrow{e_j}\Big) = \Big(\sum_i \alpha_i \overrightarrow{e_i}\Big)\Big(\sum_j \beta_j \lambda_j \overrightarrow{e_j}\Big) =$$

ami az ortonormáltság miatt

$$= \sum_i \lambda_i \alpha_i \beta_i.$$

A 4. feladat szerint $\alpha_1 = \overrightarrow{v_S} \cdot \overrightarrow{e_1} = \frac{|S|}{\sqrt{n}}$, és $\beta_1 = \overrightarrow{v_T} \cdot \overrightarrow{e_1} = \frac{|T|}{\sqrt{n}}$, ezért azt kapjuk, hogy

$$e(S,T) = \frac{d}{n}|S||T| + \sum_{i=2}^{n} \lambda_i \alpha_i \beta_i.$$

Így

$$\left|e(S,T) - \frac{d}{n}|S||T|\right| \leq \sum_{i=2}^{n} |\lambda_i \alpha_i \beta_i| \leq \lambda \sum_{i=2}^{n} |\alpha_i \beta_i|$$

A Cauchy egyenlőtlenség miatt

$$\sum_{i=2}^{n} |\alpha_i \beta_i| \leq \sqrt{\sum_{i=2}^{n} \alpha_i^2 \sum_{i=2}^{n} \beta_i^2} \leq |\overrightarrow{v_S}||\overrightarrow{v_T}| = |S||T|.$$

Azaz

$$\left|e(S,T) - \frac{d}{n}|S||T|\right| \leq \lambda\sqrt{|S||T|}$$

amit éppen bizonyítani kívántunk. □

Álljon végül itt bizonyítás nélkül két állítás, ami teszteli, hogy a második sajátérték kisebb, mint a legnagyobb (d), továbbá, hogy minden további sajátérték abszolút értéke is kisebb, mint d, azaz az alábbi két feltételt kell ellenőrizni, ha az expander mixing lemmát "jól" akarjuk alkalmazni.

11.3.6. Tétel. *1. A legnagyobb sajátérték $\lambda_1 = d$ egyszeres érték, azaz $\lambda_2 < \lambda_1$ pontosan akkor, ha a G gráf összefüggő.*

2. Bármely $i \neq 1$ esetén $|\lambda_i| < d$, ha G nem páros gráf.

Megoldások

1. A definíció közvetlen következménye

2. Mivel M egy szimmetrikus mátrix, ezért úgy tekinthetünk M^2 elemeire, mint az M két sorvektorának a skaláris szorzatára. E sorvektorok 0-kból és 1-esekből áll; tehát ha az $i-$edik sor és a $j-$edik sorban a $k-$adik helyen 1 járul hozzá a skaláris szorzathoz, akkor mind az i, mind a j a $k-$adik ponttal össze van kötve. Röviden i, k, j egy két hosszúságú út.

3. Az $M\overrightarrow{v_T}$ vektor $i-$edik koordinátáját úgy kapjuk meg, hogy M $i-$edik sorát $\overrightarrow{v_T}-$vel saklárisan összeszorozzuk. Megint két $0-1$ koordinátájú vektort szorzunk össze, ahol annyi összeadandó ($1-$es) keletkezik ahány él fut

az $i-$ből a T halmazba. Így ha most $\overrightarrow{v_S}$ vektort az $M\overrightarrow{v_T}$ vektorral összeszorozzuk, éppen az $e(S,T)$ élek számát kapjuk.

4. $M-$ben minden sorban pontosan d darab $1-$es szerepel (G d-reguláris). Így a csupa 1 koordinátájú vektor nyilván sajátvektor d sajátértékkel. Ezt normálva nyilván azt a vektort kapjuk, amelynek minden koordinátája $\frac{1}{\sqrt{n}}$.

Azt kell tehát megmutatnunk, hogy d a legnagyobb sajátérték.

Legyen $\overrightarrow{v}$ sajátvektor λ sajátértékkel. A d regularitás miatt nyilván a $j-$edik koordinátára

$$\sum_{k=1}^{d} v_{jk} = \lambda v_j, \quad j = 1, \ldots, n,$$

$n-$re összegezve és a háromszög egyenlőtlenség miatt

$$|\lambda| \sum_{j=1}^{n} |v_j| = \sum_{j=1}^{n} \Big| \sum_{k=1}^{d} v_{jk} \Big| \leq \sum_{j=1}^{n} \sum_{k=1}^{d} |v_{jk}| = d \sum_{j=1}^{n} |v_j|,$$

így $|\lambda| \leq d$ (mivel $\overrightarrow{v}$ nem nulla vektor).

11.3.3. A gráfspektrum technika néhány alkalmazása

11.3.7. Tétel. *Legyen $A \subseteq \mathbb{F}_p^*$. Ekkor*

$$|A+A||A \cdot A| \gg \min\left\{ p|A|, \frac{|A|^4}{p} \right\}.$$

Erre a tételre több, különböző módszer segítségével kapunk bizonyítást. Ebben a paragrafusban a gráfspektrum technikát használjuk.

Bizonyítás:

Egy ú.n. összeg-szorzat gráfot fogunk elsőként definiálni: legyen $A \subseteq \mathbb{F}_p$, $G(V,E)$ gráf ponthalmaza legyen $V := \mathbb{F}_p^* \times \mathbb{F}_p$ és két pontot $(a,b),(c,d) \in V$ pontosan akkor kötünk össze, ha $ac = b + d$.

A $G(V,E)$ $(p-1)$-reguláris, hiszen fixálva (a,b)-t egy adott $c \in \mathbb{F}_p^*$ egyértelműen meghatározza d-t. A gráf nem páros (valóban pl. $p > 2$ esetén a $(2,2)$ pontban hurokél van) és mint látni fogjuk bármely két különböző pont között kettő hosszúságú út vezet. Ebből adódóan, $\lambda < d = p - 1$.

Most megmutatjuk, hogy ha a két pont koordinátáira $a \neq c$ és $b \neq d$ akkor e két pontnak van egyértelmű közös szomszédja, ha $a = c$ vagy $b = d$, akkor nincs közös szomszéd.

Legyen (x, y) az $(a, b), (c, d)$ pontok közös szomszédja. Ekkor a definícióból következőleg

$$x = \frac{b-d}{a-c} \quad y = a\frac{b-d}{a-c} - b$$

ha $a \neq c$ és $b \neq d$.

Jegyezzük meg, hogy ha $a = c$ és $b = d$ (a két pont azonos) akkor $p - 1$ "közös szomszéd" van (épp az (a, b) pont foka).

Írjuk M^2 mátrixot

$$M^2 = J + (p-2)I - E$$

formába, ahol J a csupa 1-es mátrix, I pedig az egységmátrix.

(Ez a felírás k paraméterű projektív síkok esetében nagyon hasonló; itt még egy E hiba mátrixszal egészül ki e felírás).

Az E is egy $d = 2p - 3$-reguláris adjacencia mátrix.

Mint láttuk M^2_{ij} az i és j pontok között menő 2 hosszúságú utak száma. Mint megjegyeztük M^2 átlójában $p - 1$-ek állnak. Tekintsük most az (a, b) sorát. Ez 1-eseket, egy helyen $p - 1$-et és nullákat tartalmaz. 0-t, ha az oszlop (a, d)-alakú, $p - 1$ lehetőség ($b \neq d$) és amikor (c, b) alakú $p - 1$ $a \neq c$ lehetőségből, azaz $p - 2$ helyen. Tehát $2p - 3$ nulla van minden sorban, egy esetben $p - 1$, a többi elem 1. Ezért az E mátrix $(2p - 3)$-reguláris.

Legyen $\lambda \neq d$ és legyen $\overrightarrow{v}$ a hozzá tartozó sajátvektor. Mivel $M^2 = J+(p-2)I-E$, ezért $\overrightarrow{v}$ is sajátvektora E-nek. Mivel E $(2p-3)$-reguláris azt kapjuk, hogy minden sajátértéke legfeljebb $2p-3$. Mivel $\overrightarrow{v}$ egy $(1, 1, \ldots, 1)^t$ vektortól különböző sajátvektor, ezért $J\overrightarrow{v} = \overrightarrow{0}$ és így

$$\lambda^2\overrightarrow{v} = J\overrightarrow{v} + (p-2)\overrightarrow{v} - E\overrightarrow{v} = (p-2)\overrightarrow{v} - E\overrightarrow{v}.$$

Ez azt jelenti, hogy $(\lambda^2 - (p-2))\overrightarrow{v} = E\overrightarrow{v}$, azaz $\overrightarrow{v}$ E-nek is sajátvektora. Ezért

$$\lambda^2 \leq (p-2) + (2p-3) < 3p,$$

vagyis $\lambda < \sqrt{3p}$.

Most használni fogjuk a 11.3.5 tételt, amihez definiáljuk az S és T halmazokat

Legyen $(x,-a) \in S = AA \times (-A)$, $(b^{-1},y) \in T = A^{-1} \times (A+A)$. Nyilván $x = ab$ esetén $y = a + c$

$$(ab)b^{-1} = -a + (a+c)(= a)$$

megoldás. Tehát

$$e(S,T) \geq |A|^3.$$

Továbbá a 11.3.5 tétel miatt

$$|A|^3 \leq e(S,T) \leq \frac{p-1}{p(p-1)}|S||T| + \sqrt{3p|S||T|} =$$

$$= \frac{|AA||A+A||A|^2}{p} + \sqrt{3p|AA||A+A||A|^2},$$

ezért

$$|A|^3 \leq \frac{2|AA||A+A||A|^2}{p} \quad \Leftrightarrow \quad \frac{p}{2}|A| \leq 2|AA||A+A|,$$

vagy

$$|A|^3 \leq 2\sqrt{3p|AA||A+A||A|^2} \quad \Leftrightarrow \quad \frac{|A|^4}{12p} \leq |AA||A+A| \quad \square$$

3. Megjegyzés. *Valójában felmerülhet, hogy miért $M^2 = J + (p-2)I - E$ alakban írtuk fel M^2-et. Mint említettük J azt hivatott szolgálni, hogy a csupa 1 sajátvektortól (és így d legnagyobb sajátértéktől) különböző sajátvektorra (és így sajátértékre) következtethessünk. A két utolsó tagot $(p-2)I - E$ egybe is írhattuk volna; azonban $(p-2)I$ leválasztásával E már tényleg egy $0-1$ szimmetrikus adjacencia mátrixot fog jelenteni.*

Egy másik hasonló állítást is igazolunk a gráfspektrum módszerrel.

11.3.8. Tétel. *Legyen $A, B, C \subseteq \mathbb{F}_p$. Ekkor*

$$|A + (B-C)^2| \gg \min\left\{p, \frac{|A||B||C|}{p}\right\}.$$

Bizonyítás:

Definiáljuk $G(V,E)$ gráfot: $V = \mathbb{F}_p \times \mathbb{F}_p$, $(a,b),(c,d) \in V$ pontokat pontosan akkor kötjük össze, ha $a + c = (b+d)^2$.

Fixáljuk (a,b)-t. A d változót p-féleképpen tudjuk megválasztani; c egyértelműen adódik. Azaz gráfunk p-reguláris.

Legyen (x,y) az $(a,b);(c,d)$ pontok közös szomszédja. Ekkor

$$a+x=(b+y)^2; \quad \text{és} \quad c+x=(d+y)^2$$

teljesül. Ha $b=d$, akkor nyilván $a=c$, azaz ilyenkor (a,b) pont szomszégairól van szó, M^2 főátlójában tehát p áll.

Amennyiben $a=c$, akkor az előbb említett $b=d$ következik, vagy $b+y=-d-y$, amiből azt kapjuk, hogy (a,b) és (a,d) közös szomszédja $((b-d)^2/4-a,-(b+d)/2)$. A többi esetben pedig

$$y=\frac{1}{2}\Big[\frac{a-c}{b-d}-b-d\Big];\ x=(b+y)^2-a.$$

Így M^2 mátrix (a,b)-edik sorában az átlóbeli elem p, a többi oszlopban 1-es áll, kivéve, ha a második koordináta b, ekkor ott 0. $M^2=J+(p-1)I-E$, ezért E egy $(p-1)$ reguláris mátrix. Könnyen látható, hogy G összefüggő és $(1,1);(-1;-1);(2^{-1}+1;2^{-1})$ háromszög; G nem páros gráf. Hasonlóan, ahogy az előbb

$$\lambda^2\le(p-1)+(p-1) \quad \Rightarrow \quad \lambda\le\sqrt{2(p-1)}.$$

Legyen $D=A+(B-C)^2$ és legyen $S=D\times B$, $T=(-A)\times(-C)$. Nyilván ha $(d,b)\in S$, $(-a,-c)\in T$ akkor $d-a=(b-c)^2$ azaz az $d=a+(b-c)^2$ egyenletnek legalább $|A||B||C|$ megoldása van. Az "Expander Mixing Lemma" miatt, használva, hogy $\lambda<\sqrt{2p}$

$$|A||B||C|=J\le e(S,T)\le\frac{|A||B||C||D|}{p}+\sqrt{2p|A||B||C||D|}.$$

Ha a jobb oldalon az első tag nagyobb, mint a második, akkor $|A+(B-C)^2|\gg p$. Ellenkező esetben $|A+(B-C)^2|\gg\frac{|A||B||C|}{p}$ $\square$

A paragrafus utolsó tételében megmutatjuk, hogy az ú.n. Additív illeszkedési tétel (11.2.1 tétel kicsit módosítva) levezethető a gráfspektrum technikával is.

11.3.9. Tétel. *Legyen Z egy véges additív csoport, $|Z|\equiv 1 \pmod 2$. Legyen S egy Sidon halmaz. Legyen $\Delta:=|Z|-|S|^2>0$. Ekkor*

$$|\{b+c\in S: b\in B\ c\in C\}|=\frac{|S||B||C|}{|Z|}+\alpha\sqrt{|B||C|}\cdot\sqrt[4]{|Z|},$$

$ahol\ \alpha \leq \sqrt{1+\frac{\Delta}{\sqrt{|Z|}}}$.

(Mint már megjegyeztük az első bizonyításnál, itt is olyan csoportoknál érdekes, ahol $|Z| - |A|^2 = o(|Z|)$)

A (kicsit módosított) 11.2.1 tétel második bizonyítása:

Definiáljuk $G(V,E)$-t: legyen $V(G) = Z$ és $a, b \in Z$ pontokat kössük össze pontosan akkor, ha $a + b \in S$.

Igazolnunk kell, hogy $G(V,E)$

(a) egy $|S|$ reguláris,

(b) nem páros és hogy

(c) összefüggő.

(a) Adott $a \in Z$ elem szomszédainak az $S - a$ halmaza.

(b) A gráf az (x,y,z) háromszöget tartalmazza; $x + y = s_1,\ x + z = s_2, y + z = s_3$; $s_1, s_2, s_3 \in S$ másként $x = \frac{s_1+s_2-s_3}{2};\ y = \frac{s_1-s_2+s_3}{2};\ z = \frac{-s_1+s_2+s_3}{2}$.

(Jegyezzük meg, hogy $|2Z| = |\{2z : z \in Z\}| = |Z|$ – azaz nincs $2z = 2z'; z \neq z'$ pár. Ellenkező esetben $2|ord|Z|$ lenne ellentmondásként. Azaz bármely $z \in Z$-beli elemre létezik $z/2$).

(c) Legyen a és b két pont. Megmutatjuk, hogy létezik közöttük egy legfeljebb négy hosszúságú út. Tekintsük a szomszédait: ez az $S-a$ halmaz. Továbbá ezen pontok szomszédait (ezek a-ból 2-hosszúsággal elérhető pontok). Ezen másodszomszédok mind különbözőek, ellenkező esetben lenne a gráfban C_4, négy hosszúságú kör, ami ellentmond annak, hogy S Sidon sorozat. Ezen pontok halmazának elemszáma $|S|(|S|-1)$. Most tekintsük a b-ből kettő hosszúságú úttal elérhető pontok halmazát. Az a-ból 2 hosszúsággal elérhető pontok halmaza nem lehet diszjunkt a b-ből 2 hosszúsággal elérhető pontok halmazától, u.i. $2|S|(|S|-1) > |Z|$ (ehhez pl. elég, hogy a Sidon halmaz elemszáma $> \sqrt{|Z|/2}$ legyen).

Legyen M a $G(V,E)$ adjacencia mátrixa. Írjuk (mint előbb) $M^2 = J + (|S|-1)I - E$. Most megmutatjuk, hogy E d'-reguláris és $d' \leq |Z| - |S|(|S|-1)$, amiből

$$\lambda(G) \leq \sqrt{2(1+\Delta)}\sqrt[4]{|Z|}.$$

Valóban, az M^2 egy sorában az átlóban $|S|$ áll (a G-beli elemek fokszáma). Könnyű látni, hogy i és j pontoknak pontosan akkor van közös szomszédja, ha $i - j \in S - S$. Ezért $|Z| - |S|(|S| - 1)$ elem 0, a többi (nem átlóbeli) 1; tehát E gráf $[|Z| - |S|(|S| - 1)]$-reguláris.

Most a $\lambda(G) \leq \sqrt{2(1 + \Delta)}\sqrt[4]{|Z|}$ becslést az "Expander Mixing Lemma"-ba beírva kapjuk a tétel állítását. □

12. fejezet

Additív-Multiplikatív kombinatorika véges testekben

A címben említettekre később visszatérünk (ott diszkrét Fourier analízis segítségével nyerünk eredményeket), most egy kombinatorikus ötletet felhasználó tételt mutatunk be.

12.0.1. Tétel. *Legyen $A, B \subseteq \mathbb{F}_p$ két halmaz. Ekkor létezik $\alpha_0 \in \mathbb{F}_p^*$, hogy*

$$|A \pm \alpha_0 B| \geq \frac{|A||B| \cdot p}{p + |A||B|}.$$

Bizonyítás:

Jelölje $R_\alpha(m) = |\{(a,b) : m = a + \alpha b; a \in A, b \in B\}|$ és $Q_\alpha(m) = |\{(a,b) : m = a - \alpha b; a \in A, b \in B\}|$, ahol $\alpha \in \mathbb{F}_p^*$. Most kiszámítjuk az $R_\alpha(m)$ reprezentációs függvény második momentumát:

Elsőként

$$\sum_{a \neq a'} \sum_{\alpha} R_\alpha^2(m) \leq |A|^2 |B|^2,$$

mivel, $R_\alpha^2(m)$-ben $a + \alpha b = a' + \alpha b'$ esetén $a \neq a' \Leftrightarrow b \neq b'$, így

$$\alpha = \frac{a - a'}{b' - b}$$

és egy (a, a', b, b') négyeshez egy α tartozik. Ha most $a = a'$ (és így $b = b'$) akkor

$$\sum_{a=a';b=b'} \sum_{\alpha} R_\alpha^2(m) \leq p \cdot |A||B|.$$

A második momentum így

$$\sum_m \sum_\alpha R_\alpha^2(m) \le |A|^2|B|^2 + p \cdot |A||B|,$$

amiből átlagolással kapjuk, hogy van olyan $\alpha_0 \in \mathbb{F}_p^*$, hogy

$$\sum_m R_{\alpha_0}^2(m) \le \frac{|A|^2|B|^2}{p} + |A||B|.$$

Most a Cauchy egyenlőtlenséget használva

$$|A|^2|B|^2 = \Big(\sum_m R_{\alpha_0}(m)\Big)^2 = \Big(\sum_m Q_{\alpha_0}(m)\Big)^2 \le |A \pm \alpha_0 B| \cdot \sum_m R_{\alpha_0}^2(m) \le$$

$$\le |A \pm \alpha_0 B|\Big(\frac{|A|^2|B|^2}{p} + |A||B|\Big),$$

amiből következik, hogy

$$\frac{|A||B| \cdot p}{p + |A||B|} \le |A \pm \alpha_0 B|. \quad \square$$

2. Következmény. *Legyen $A \subseteq \mathbb{F}_p$. Van olyan $\alpha_0 \in \mathbb{F}_p^*$, hogy*

$$|A \pm \alpha_0 A| \ge \min \frac{1}{2}\{|A|^2, p\}.$$

Valóban, van olyan $\alpha_0 \in \mathbb{F}_p^*$, hogy

$$|A \pm \alpha_0 A| \ge \frac{|A|^2 \cdot p}{p + |A|^2}.$$

Ha $|A|^2 > p$, akkor

$$\frac{|A|^2 \cdot p}{p + |A|^2} > \frac{p}{2},$$

ha $|A|^2 \le p$, akkor

$$\frac{|A|^2 \cdot p}{p + |A|^2} \ge \frac{|A|^2}{2}. \quad \square$$

E tétel másik következménye a következő összeg-szorzat bázis tétel:

12.0.2. Tétel. *Legyen $A, B \subseteq \mathbb{F}_p$ két olyan halmaz, melyre $|A||B| > 2p$. Ekkor*

$$8AB = \mathbb{F}_p.$$

Bizonyítás:

Legyen $B_1 : \{b \in B : -b \in B\}$ és $B_2 = B \setminus B_1$. Ekkor vagy $|A||B_1| > p$ vagy $|A||B_2| > p$.

Ha $|A||B_2| > p$, akkor az előző tétel miatt

$$|A + \alpha_0 B_2| \geq \frac{|A||B_2| \cdot p}{p + |A||B_2|} > \frac{p}{2}.$$

Ekkor azonban

$$| - A - \alpha_0 B_2| > \frac{p}{2}.$$

is teljesül. A skatulya-elv miatt tehát létezik a_1, a_2, b_1, b_2 úgy, hogy

$$a_1 + \alpha_0 b_1 = -a_2 - \alpha_0 b_2$$

és mivel $B_2 \cap -B_2 = \emptyset$, azt kapjuk, hogy

$$\alpha_0 = -\frac{a_1 + a_2}{b_1 + b_2}.$$

Viszont

$$\frac{p}{2} < |A - \alpha_0 B_2| = |A + \frac{a_1 + a_2}{b_1 + b_2} B_2|$$

is teljesül, amiből

$$\frac{p}{2} < |A(b_1 + b_2) + (a_1 + a_2)B_2|.$$

Mint láttuk, ha egy csoportban $U, V \subseteq G$, $|U| + |V| > |G|$, akkor $U + V = G$. Ezért azt kapjuk, hogy

$$8AB_2 \supseteq A(b_1 + b_2) + (a_1 + a_2)B_2 + A(b_1 + b_2) + (a_1 + a_2)B_2 = \mathbb{F}_p,$$

azaz $8AB_2$ lefedi $\mathbb{F}_p$-t.

Ha $|A||B_1| > p$ és nyilván $|A + \alpha_0 B_1| \leq p$, így

$$|A + \alpha_0 B_1| \leq |A||B_1|,$$

amiből az következik, hogy $A + \alpha_0 B_1$ elemei nem mind különbözőek, azaz létezik a_1, a_2, b_1, b_2 úgy, hogy

$$a_1 + \alpha_0 b_1 = a_2 + \alpha_0 b_2 \;\Leftrightarrow\; \alpha_0 = \frac{a_1 - a_2}{b_2 - b_1}.$$

Mivel

$$\frac{p}{2} < |A + \alpha_0 B_1| = |A + \frac{a_1 - a_2}{b_1 - b_2} B_1|,$$

így mivel $B_1 = -B_1$, létezik $-b_1' = b_1$ kapjuk, hogy

$$\frac{p}{2} < |A(b_2 - b_1) + (a_1 - a_2)B_1| = |Ab_2 + Ab_1' + a_1 B + (-a_2)(-B_1)|$$

és ezért

$$8AB_1 \supseteq Ab_2 + Ab_1' + a_1 B + a_2 B_1 + Ab_2 + Ab_1' + a_1 B + a_2 B_1 = \mathbb{F}_p.$$

A két esetet összevetve tehát kapjuk, hogy

$$8AB = \mathbb{F}_p. \quad \square$$

Megjegyzés:
Érdekes Waring típusú kérdést lehet feltenni prímtestekben. Az előző tétel speciális esete az, amikor $A = B = H < \mathbb{F}_p^*$, azaz H az $\mathbb{F}_p^*$-nek egy multiplikatív részcsoportja. Ekkor nyilván $AB = HH = H$. Be lehet bizonyítani (lásd a Feladatokat), hogy H elemei k-adik hatványok. Tehát kapjuk a következő

Következmény:
Legyen $H = \{x^k : x \in \mathbb{F}_p^*\}$. Ha $|H| > \sqrt{2p}$, akkor H 8-adrendű bázis, azaz $8H = \mathbb{F}_p$.

Megjegyeznénk továbbá, hogy egy érdekes kérdés lenne, hogy egy H multiplikatív részcsoport mikor lesz másodrendű bázis. Mint láttuk a kvadratikus maradékok azok (I. fejezet 1. feladat). A későbbiekben más módszerrel megmutatjuk, hogy $|H| > p^{1/2+\varepsilon}$ feltételből már következik ez.

12.0.3. Tétel. *Tegyük fel, hogy $A \subseteq \mathbb{F}_p$. Ekkor*

$$|3A^2 - 3A^2| > \frac{1}{2} \min\{|A|^2, p\}.$$

Bizonyítás:

Az előző tételben láttuk, hogy $|A+\alpha A| = |A|^2$ pontosan akkor teljesül, ha $\alpha \notin \frac{A-A}{A-A}$.

Tegyük fel először, hogy $\frac{A-A}{A-A} \neq \mathbb{F}_p$.

Ekkor van négy olyan $A-$beli elem, amelyre $\frac{a_1-a_2}{a_3-a_4}+1 \notin \frac{A-A}{A-A}$. Az előbbiek miatt tehát

$$\left|A+\left(\frac{a_1-a_2}{a_3-a_4}+1\right)A\right| = |A|^2,$$

ami ekvivalens azzal, hogy

$$|3A^2-3A^2| \geq |A(a_3-a_4)+(a_1-a_2)A+(a_3-a_4)A| = |A|^2.$$

Most tegyük fel, hogy $\frac{A-A}{A-A} = \mathbb{F}_p$.

Mivel valamely α_0 mellett

$$|A+\alpha_0 A| \geq \min \frac{1}{2}\{|A|^2, p\},$$

továbbá valamely négy $A-$beli elemre, $\frac{a_1-a_2}{a_3-a_4} = \alpha_0$, így

$$\left|A+\frac{a_1-a_2}{a_3-a_4}A\right| \geq \min \frac{1}{2}\{|A|^2, p\},$$

ami ekvivalens azzal, hogy

$$|A(a_3-a_4)+(a_1-a_2)A| \geq \min \frac{1}{2}\{|A|^2, p\}.$$

Mivel

$$3A^2-3A^2 \supseteq 2A^2-2A^2 \supseteq A(a_3-a_4)+(a_1-a_2)A,$$

amiből következik az állítás. □

Következmény: *Tegyük fel, hogy $A \subseteq \mathbb{F}_p$, és hogy valamely $\beta > 0$ mellett $|A| > p^\beta$. Ekkor van olyan $k = k(\beta)$, hogy*

$$|kA^k - kA^k| = \mathbb{F}_p.$$

Bizonyítás:

Ha A helyére $3A^2 - 3A^2$ halmazt írjuk, akkor $3(3A^2 - 3A^2)^2 - 3(3A^2 - 3A^2)^2 = sA^4 - sA^4$ alakú lesz és így

$$|sA^4 - sA^4| > \frac{1}{2}\min\{|3A^2 - 3A^2|^2, p\} > \frac{1}{2}\min\{|A|^4, p\}.$$

Ezt az eljárást ismételve lesz olyan $n = \max\{m, t\}$, hogy

$$|nA^n - nA^n| > |mA^t - mA^t| > \frac{p}{2}.$$

Az "$|X| > |G|/2 \Rightarrow X + X = G$" feladatot használva $k = 2n$ mellett

$$|kA^k - kA^k| = \mathbb{F}_p. \quad \square$$

A harmadik fejezetben láttuk, hogy az ú.n. *energia* a reprezentációs függvény második momentuma (ami kapcsolatba hozható az összeg-, szorzathalmaz stb. elemszámával). Ebben a pontban prímtestekben vizsgáljuk a multiplikatív energiát. Ha $A, B \subseteq \mathbb{F}_p$, akkor $E_\times(A, B) := \{(a, a', b, b') : ab = a'b'\}$. Ha $A = B$, akkor $E_\times(A, B) := E_\times(A) = \sum_x r^2(x)$, ahol $r(x) = \{(a, a') : aa' = x\}$.

A következő tételben becslést kapunk a multiplikatív energiára.

12.0.4. Tétel. *Ha $A \subseteq \mathbb{F}_p$, akkor van olyan $C > 0$, hogy*

$$E_\times(A)^4 < C(|A + A|^9|A|^2 + \frac{1}{p}|A|^5|A + A|^8)\log^4(|A|).$$

Bizonyítás:
A multiplikatív energia nyilván

$$E_\times(A) = \sum_x r^2(x) = \sum_{a,b\in A} |aA \cap bA|,$$

hiszen az utóbbi összegben is azokat az a, a', b, b' négyeseket számláljuk le, amelyekre $aa' = bb'$. Ekkor létezik olyan $b_0 \in A$, hogy

$$\sum_{a\in A} |aA \cap b_0A| \geq \frac{E_\times(A)}{|A|}. \ (**)$$

Az $\sum_{a\in A}|aA\cap b_0A|$ összeget rendezzük értékeinek növekvő sorrendjébe és skálázzuk a 2 hatványai szerint, azaz $\log_2|A|$ csoportba osztjuk úgy, hogy az egyes csoportokon belül $2^k\le|aA\cap b_0A|\le 2^{k+1}$ teljesül. Ekkor van olyan $1\le N\le|A|$, $A_1\subseteq A$, hogy

$$N\le|aA\cap b_0A|\le 2N$$

teljesül az $a\in A_1$ elemekre. Így $(**)$ miatt

$$\frac{E_\times(A)}{|A|}\le 2N|A_1|\log_2|A|.$$

Két esetet különböztetünk meg:

1.
$$\frac{A_1-A_1}{A_1-A_1}=\mathbb{F}_p.$$

Ekkor van olyan $\alpha\in\mathbb{F}_p^*$, és $a_1,a_2,a_3,a_4\in A_1$ amelyre

$$\alpha=\frac{a_1-a_2}{a_3-a_4},$$

és

$$|\{(x_1,x_2,x_3,x_4)\in A_1^4:\alpha=\frac{x_1-x_2}{x_3-x_4}\}|\le\frac{|A_1|^4}{p}.$$

Vegyük észre, hogy most

$$|\{(x_1,x_2,x_3,x_4)\in A_1^4:\alpha=\frac{x_1-x_2}{x_3-x_4}\}|=E_+(A_1,\alpha A_1),$$

hiszen átrendezve az egyenletet épp a megoldás-négyesek számát kapjuk.

Ekkor

$$|(a_3-a_4)A_1+(a_1-a_2)A_1|=|A_1+\alpha A_1|.$$

Ha most $\rho(x)=|\{a+a'\alpha:a,a'\in A_1\}|$, akkor a szokásos módon (használva a Cauchy egyenlőtlenséget) azt kapjuk, hogy

$$|A_1|^2|\alpha A_1|^2=\big(\sum_x\rho(x)\big)^2\le|A_1+\alpha A_1|\sum_x\rho(x)^2=|A_1+\alpha A_1|E_+(A_1,\alpha A_1).$$

Mint láttuk

$$p\le\frac{|A_1|^4}{E_+(A_1,\alpha A_1)}=\frac{|A_1|^2|\alpha A_1|^2}{E_+(A_1,\alpha A_1)},$$

így a Plünnecke-Ruzsa egyenlőtlenséget használva

$$p \leq \frac{|A_1|^2|\alpha A_1|^2}{E_+(A_1, \alpha A_1)} \leq |A_1 + \alpha A_1| \leq |a_3A_1 - a_4A_1 + a_1A_1 - a_2A_1| \leq$$

$$\leq \frac{\prod_{i=1}^4 |a_iA + (-1)^{i+1}b_0A|}{|A|^3}$$

Most a páros $i-$kre használva a háromszög-egyenlőtlenséget, páratlan $i-$kre pedig a Plünnecke-Ruzsa egyenlőtlenséget azt kapjuk, hogy

$$|a_iA - b_0A| \leq \frac{|a_iA + (a_iA \cap b_0A)||(a_iA \cap b_0A) + b_0A|}{|a_iA \cap b_0A|} \leq$$

$$\leq \frac{|a_iA + a_iA||b_0A + b_0A|}{|a_iA \cap b_0A|} = \frac{|A + A||A + A|}{|a_iA \cap b_0A|} \leq \frac{|A + A||A + A|}{N}$$

mivel az a_i-ket az A_1 halmazból választottuk. Így

$$p \leq \frac{1}{|A|^3}\Big(\frac{|A + A|^2}{N}\Big)^4$$

Az N értékére tudjuk, hogy $\frac{E_\times(A)}{|A|} \leq 2N|A_1|\log_2|A|$, amit átrendezve és a fenti becslésbe beírva, kapjuk, hogy

$$E_\times(A)^4 < 16\frac{1}{p}|A|^5|A + A|^8\log^4|A|.$$

2. Második esetünkben tegyük fel, hogy

$$\frac{A_1 - A_1}{A_1 - A_1} \neq \mathbb{F}_p.$$

Ekkor az $\frac{A_1-A_1}{A_1-A_1}$ halmaz eltoltja nincs teljesen e halmazban, azaz van négy olyan elem, melyre $\alpha := \frac{a_1-a_2}{a_3-a_4} + 1 \notin \frac{A_1-A_1}{A_1-A_1}$. Most bármely $A_1' \subseteq A_1$ halmazra teljesül, hogy

$$|A_1' + \alpha A_1'| = |A_1'|^2.$$

Ekkor tehát

$$|A_1'|^2 = \Big|A_1' + \big(\frac{a_1 - a_2}{a_3 - a_4} + 1\big)A'\Big| \leq |A_1'(a_3 - a_4) + A_1'(a_1 - a_2) + A_1'(a_3 - a_4)|.$$

Legyen $X := (a_3 - a_4)A_1$. Az erősebb Plünnecke-Ruzsa tételből tudjuk, hogy létezik $X' = (a_3 - a_4)A_1' \subseteq X$, hogy $|X'| > |X|/2$, és

$$|X' + A_1'(a_1 - a_2) + A_1'(a_3 - a_4)| \leq \frac{|(a_3 - a_4)A_1 + X||(a_1 - a_2)A_1 + X|}{|X|},$$

ezzel az $A_1'-$vel az előbbi becslés tehát

$$|A_1'|^2 \leq \frac{|(a_3 - a_4)A_1 + X||(a_1 - a_2)A_1 + X|}{|X|} =$$

$$= \frac{|(a_3 - a_4)A_1 + (a_3 - a_4)A_1||(a_1 - a_2)A_1 + (a_3 - a_4)A_1|}{|(a_3 - a_4)A_1|}.$$

Az első esetnél a $|(a_1 - a_2)A_1 + (a_3 - a_4)A_1|$ kifejezésre használt becsléssel azt kapjuk tehát, hogy

$$|A_1|^2 \ll |A_1'|^2 \leq \frac{|A_1 + A_1|}{|A_1|} \frac{1}{|A|^3} \Big(\frac{|A + A|^2}{N} \Big)^4.$$

Végül használva a $\frac{E_\times(A)}{|A|} \leq 2N|A_1| \log_2 |A|$ becslést, azt kapjuk, hogy

$$|A_1|^3 |A|^3 \frac{E_\times(A)^4}{|A|^4 |A_1|^4 \log^4(|A|)} \ll |A + A|^9,$$

és így

$$E_\times(A)^4 \ll |A + A|^9 |A|^2. \quad \square$$

Feladatok

1. Bizonyítsuk be, hogy ha $H < \mathbb{F}_p^*$ egy multiplikatív részcsoport, akkor valamely $k \in \mathbb{N}$ számra $H = \{x^k : x \in \mathbb{F}_p^*\}$.

2. Bizonyítsuk be, hogy $|A + \alpha B| < |A||B|$ ($\alpha \in \mathbb{F}_p$) akkor és csak akkor, ha $\frac{A-A}{B-B} = \mathbb{F}_p$.

3. Bizonyítsuk be, hogy ha $X, X \subseteq \mathbb{F}_p$, $|Y| > 1$, és $\frac{X-X}{Y-Y} \neq \mathbb{F}_p$, akkor

$$|2XY - 2XY + Y^2 - Y^2| \geq |X||Y|.$$

Megoldás

1. Mivel $\mathbb{F}_p^*$ ciklilkus csoport, minden részcsoportja ciklikus. Tehát ha g egy generátora (primitív gyöke) $\mathbb{F}_p^*$-nek, akkor valamely m egészre $H = \{g^{mk} : k = 1, 2, \ldots, p-1\}$ alakú. Mivel $g^k : k = 1, 2, \ldots, p-1$ végigfut $\mathbb{F}_p^*$ elemein, ezért H elemei valóban $\{x^k : x \in \mathbb{F}_p^*\}$ alakúak.

2. Az $\alpha = 0$ elem nyilván benne van $\frac{A-A}{B-B}$ halmazban. Ha $\forall \alpha \in \mathbb{F}_p$; $|A + \alpha B| < |A||B|$, akkor és csak akkor (rögzítve egy $\alpha \neq 0$ elemet) ha az $a + \alpha b$ között van összeesés; azaz $a + \alpha b = a' + \alpha b'$ valamely a, a', b, b' elem négyesre. Más szóval

$$\alpha = \frac{a - a'}{b' - b},$$

ami másként írva

$$\frac{A - A}{B - B} = \mathbb{F}_p.$$

3. Mivel $\frac{X-X}{Y-Y} \neq \mathbb{F}_p$, így van négy olyan elem x_1, x_2, y_1, y_2 amelyekre teljesül, hogy

$$\frac{x_1 - x_2}{y_1 - y_2} + 1 \notin \frac{X - X}{Y - Y}.$$

Tekintsük a $\tau : X \times Y \mapsto 2XY - 2XY + Y^2 - Y^2$

$$\tau : \ (x, y) \mapsto (y_1 - y_2)x + (y_1 - y_2 + x_1 - x_2)y$$

leképezést. Bizonyítjuk, hogy injektív.

Valóban ha indirekt valamely $(x', y') \neq (x, y)$ párosra

$$(x', y') \mapsto (y_1 - y_2)x' + (y_1 - y_2 + x_1 - x_2)y'$$

akkor

$$(y_1 - y_2)x + (y_1 - y_2 + x_1 - x_2)y = (y_1 - y_2)x' + (y_1 - y_2 + x_1 - x_2)y'$$

teljesülne, így átrendezve azt kapnánk, hogy

$$\frac{x_1 - x_2}{y_1 - y_2} + 1 = \frac{x - x'}{y' - y} \in \frac{X - X}{Y - Y}$$

ami ellentmond az x_1, x_2, y_1, y_2 elemek választásának.

13. fejezet

Diszkrét Fourier analízis

13.1. Bevezető tételek; additív karakterek

Jelölje $\mathbb{Z}_n$ a $(\mathrm{mod}\ n)$ maradékosztályokat. Legyen

$$e_n(x) = e^{2\pi x i/n}.$$

Ahol nem okozhat félreértést az $e_n(x)$ kifejezésnél elhagyjuk az indexet és röviden $e(x)$-et írunk.

Legyenek f, g függvények amelyekre

$$f, g : \mathbb{Z}_n \to \mathbb{C}.$$

Az f Fourier transzformáltja

$$\widehat{f}(y) = \sum_{x \in \mathbb{Z}_n} f(x) \cdot e(xy).$$

A fenti összeget, ha az összegzés az egész csoportra vonatkozik, röviden $\sum_x f(x) \cdot e(xy)$ alakban használjuk.

Először egy egyszerű állítást mondunk ki:

13.1.1. Tétel. *Az exponenciális összegre*

$$\sum_x e(xy) = \begin{cases} n, & y = 0 \\ 0, & y \neq 0 \end{cases}$$

Továbbá

$$|1 - e^{2\pi i\alpha}| > \|2\pi\alpha\|.$$

Bizonyítás:

Valóban, ha $y = 0$, akkor n db 1-est adunk össze. Ha $y \neq 0$, akkor egy mértani sor az összeg, amelyik zárt képletben

$$\frac{e(ny) - 1}{e(y) - 1} = 0,$$

mivel $e(ny) = 1$.

Továbbá

$$|1 - e^{2\pi i\alpha}| = |e^{\pi i\alpha} - e^{-\pi i\alpha}| = 2|\sin(\pi\alpha)|.$$

Jelölje $\beta = \min\{\alpha, 1 - \alpha\}$. Így $2|\sin(\pi\alpha)| = 2|\sin(\pi\beta)| > |2\pi\beta| = \|2\pi\alpha\|$, ugyanis $\sin(\pi x)$ a $0 < x < 1/2$ intervallumon konkáv és így itt nagyobb, mint az $y = 2x$. $\square$

A következő tételt igen gyakran fogjuk használni:

13.1.2. Tétel (Plancherel formula).

$$\sum_x f(x)\overline{g(x)} = \frac{1}{n}\sum_y \widehat{f}(y)\overline{\widehat{g}(y)}.$$

Speciális esetben, ha $A \subseteq \mathbb{Z}_n$ és $A(x)$ az A halmaz indikátora, azaz

$$A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

akkor

$$\sum_r |\widehat{A}(r)|^2 = n\sum_x |A(x)|^2 = n \cdot |A|.$$

Továbbá

$$\frac{1}{n}\sum_r \widehat{f}(r)\overline{\widehat{g}(r-u)} = \sum_x f(x)\overline{g(x)}e(xu).$$

Ez $u = 0$ esetben pontosan a Plancherel.

Bizonyítás:
Az előző tételt alkalmazva,

$$\sum_y \widehat{f}(y)\overline{\widehat{g}(y)} = \sum_y \Big(\sum_x f(x) \cdot e(xy) \cdot \sum_z \overline{g(z)} \cdot e(-zy) \Big) =$$

$$= \sum_{x,z} \sum_y (f(x)\overline{g(z)}e((x-z)y)) = n \cdot \sum_x f(x)\overline{g(x)}.$$

$$\frac{1}{n}\sum_r \widehat{f}(r)\overline{\widehat{g}(r-u)} = \frac{1}{n}\sum_r \Big(\sum_x f(x)e(xr) \Big) \Big(\sum_y \overline{g(y)}e(-yr+yu) \Big) =$$

$$= \frac{1}{n}\sum_{x,y} f(x)\overline{g(y)}e(yu) \sum_r e(r(x-y)) = \frac{1}{n} \cdot n \sum_x f(x)\overline{g(x)}e(xu) =$$

$$= \sum_x f(x)\overline{g(x)}e(xu). \quad \square$$

Fontos lesz még az ú.n. Inverziós-formula:

13.1.3. Tétel.

$$f(x) = \frac{1}{n}\sum_y \widehat{f}(y) \cdot e(-xy).$$

Bizonyítás:

$$\frac{1}{n}\sum_y \widehat{f}(y) \cdot e(-xy) = \frac{1}{n}\sum_y \sum_z f(z) \cdot e(zy) \cdot e(-xy) =$$

$$= \frac{1}{n}\sum_z \sum_y f(z) \cdot e((z-x)y) = f(x). \quad \square$$

Additív kérdések esetén fontos a konvolúció:

I. Definiáljuk először a következő konvolúciót:

$$(f * g)(x) = \sum_y f(y)\overline{g(x-y)},$$

(Tehát ha f és g indikátorok, akkor $(f*g)(x) = r(x)$, az $x = a+b$ megoldásainak a számát méri.)

II. Legyen egy másik konvolúció

$$(f \circ g)(x) = \sum_y f(y)\overline{g(y-x)},$$

(Most tehát ha f és g indikátorok, akkor $(f \circ g)(x) = d(x)$, az $x = a-b$ megoldásainak a számát méri.)

Bizonyítjuk, hogy

13.1.4. Tétel. *1. Az első konvolúcióra:*

$$\widehat{(f*g)}(x) = \widehat{f}(x)\widehat{g}(x).$$

2. A másik konvolúcióra:

$$\widehat{(f \circ g)}(x) = \widehat{f}(x)\overline{\widehat{g}(x)}.$$

Bizonyítás:

$$\widehat{(f*g)}(r) = \sum_x f*g(x)e(rx) = \sum_x \Big(\sum_y f(y)g(x-y)\Big)e(rx) = *.$$

Legyen $z = x-y$, így $x = y+z$. Ha x végigfut $\mathbb{Z}_n$ elemein (és y fix), akkor z is.

Ekkor

$$* = \sum_{y,z} f(y)g(z)e(r(y+z)).$$

Másfelöl

$$\widehat{f}(r)\widehat{g}(r) = \sum_z f(z)e(rz) \cdot \sum_y g(y)e(ry) = \sum_{y,z} f(y)g(z)e(r(y+z)),$$

amit bizonyítani akartunk.

Teljesen hasonló a másik konvolúciós állításnak az igazolása. □

Feladatok

1. Tekintsük a Diszkrét Fourier transzformáltat egy véges test feletti vektortérben a következőképpen:

legyen $f : {\mathbb{F}_p}^n \mapsto \mathbb{C}$. Ekkor legyen

$$\widehat{f}(r) = \sum_x f(x)e(r^T x),$$

ahol $r, x \in {\mathbb{F}_p}^n$, r^T jelöli a transzponáltat és $r^T x$ a szokásos skalárszorzat.

Bizonyítsuk be, hogy a fenti tételek ${\mathbb{F}_p}^n$-ben is igazak!

2. Legyen $A(x)$ az $A \subseteq \mathbb{Z}_N$ indikátora. Bizonyítsuk be, hogy

$$\sum_r |\widehat{A}(r)|^4 = NE(A),$$

ahol $E(A) = E(A, A)$ az A halmaz additív energiája.

3. Legyen $A(x)$ az $A \subseteq \mathbb{Z}_N$ indikátora. Bizonyítsuk be, hogy

$$\sum_r |\widehat{A}(r)| \geq \sqrt{\frac{N^2|A|^3}{E(A)}}.$$

4. Bizonyítsuk be, hogy

$$\sum_r |\widehat{A}(r)|^{2k} = NE_k(A),$$

ahol $E_k(A)$ az A hamaz k-tagú additív energiája, azaz

$$E_k(A) = \{(a_1, \ldots, a_k, a'_1, \ldots, a'_k) : a_1 + \cdots + a_k = a'_1 + \cdots + a'_k\}.$$

5. Bizonyítsuk be, hogy

$$\frac{E_k(A)}{|A|^{2k}}$$

k monoton csökkenő függvénye.

6. Legyen $A \subseteq \mathbb{Z}_n$; és tegyük fel, hogy $|A| < \frac{\log n}{\log 3}$.

Ekkor van olyan $r \neq 0$, hogy

$$|\widehat{A(r)}| \geq \frac{|A|}{2}.$$

7. Legyen $R < \mathbb{F}_p^*$ egy multiplikatív részcsoport és legyen Q egy R-invariáns részhalmaz, azaz $Q \cdot R = Q$. Bizonyítsuk be, hogy bármely $\xi \neq 0$ elemre $|\widehat{R(\xi)}| \leq \sqrt{p|Q|/|R|}$.

Igazoljuk, hogy bármely $\xi \neq 0$ elemre $|\widehat{R(\xi)}| \leq \sqrt{p}$.

8. Bizonyítsuk be, hogy

$$\sum_{r=1}^{n} \sum_{x=k}^{k+h-1} e_n(rx) \ll n \log n.$$

9. Bizonyítsuk be a 10. fejezet 10.2.2 tételét. Azaz igazoljuk a következő állítást:

Legyen $A \subseteq [1, X]$ és legyen p olyan prím, mely $\leq \sqrt{X}$. Jelölje $E_p(A)$ a moduláris energiát, azaz mindazon (a_1, a_2, a_3, a_4) négyesek számát amelyekre $a_1 + a_2 \equiv a_3 + a_4 \pmod{p}$. Ekkor

$$\sum_{p \leq \sqrt{X}} p\Big(E_p(A) - \frac{|A|^4}{p}\Big) \leq 4XE(A).$$

10. Legyen $\{a_n\}_{n=1}^N \subseteq \mathbb{C}$ és $\widehat{A}(r) = \sum_n a_n e_N(rn)$. Bizonyítsuk be, hogy

$$\Big| \sum_{a \leq n \leq b} a_n - \frac{b-a}{N} \widehat{A}(0) \Big| \ll \log N \max_{r \neq 0} |\widehat{A}(r)|.$$

(*Ezt a feladatot a Kloosterman összegek c. részben egy érdekes becsléshez fogjuk felhasználni.*)

Megoldások

2. A definíciót használva

$$\sum_{r \in \mathbb{Z}_N} |\widehat{A}(r)|^4 = \sum_{r \in \mathbb{Z}_N} \sum_{x_1, x_2, x_3, x_4 \in A} e_N(r(x_1 + x_2 - x_3 - x_4)) =$$

$$= \sum_{x_1,x_2,x_3,x_4 \in A} \sum_{r \in \mathbb{Z}_N} e_N(r(x_1 + x_2 - x_3 - x_4)) =$$

$$= N|\{(x_1, x_2, x_3, x_4) \in A^4 : x_1 + x_2 = x_3 + x_4\}| = NE(A).$$

3. A Parseval azonosság miatt

$$N|A| = \sum_r |\widehat{A}(r)|^2 = \sum_r |\widehat{A}(r)|^{2/3} |\widehat{A}(r)|^{4/3} \leq$$

a Hölder egyenlőtlenség miatt

$$\leq \left(\sum_r |\widehat{A}(r)| \right)^{2/3} \left(\sum_r |\widehat{A}(r)|^4 \right)^{1/3} =$$

$$= \left(\sum_r |\widehat{A}(r)| \right)^{2/3} (NE(A))^{1/3}.$$

Átrendezve az állítást kapjuk.

5. Két bizonyítást is adunk rá:

I. Mivel

$$\sum_r |\widehat{A}(r)|^{2k} = NE_k(A),$$

ezért

$$NE_{k+1}(A) = \sum_r |\widehat{A}(r)|^{2k+2} \leq \max |\widehat{A}(r)|^2 \sum_r |\widehat{A}(r)|^{2k} =$$

$$= |A|^2 \sum_r |\widehat{A}(r)|^{2k} = |A|^2 NE_k(A).$$

Az egyenlőtlenség mindkét oldalát $N|A|^{2k+2}$–vel elosztva kapjuk az állítást.

II. Jelentse $r_k(n)$ az n k-tagú összegeként való előállítását. Ekkor

$$E_{k+1} = \sum_n r_{k+1}^2(n) = \sum_{a,a' \in A} \sum_n r_k(n) r_k(n + (a - a')),$$

mivel

$$a_1 + \cdots + a_k + a = a_1' + \cdots + a_k + a' \;\Leftrightarrow\; a_1 + \cdots + a_k = a_1' + \cdots + a_k + a' - a.$$

Így a Cauchy egyenlőtlenség miatt

$$E_{k+1} \le |A|^2 \sum_n r_k(n) r_k(n+(a-a')) \le |A|^2 \sqrt{\sum_n r_k^2(n)} \sqrt{\sum_n r_k^2(n+a-a')} =$$

$$|A|^2 \sum_n r_k^2(n) = |A|^2 E_k.$$

A bizonyítás innen ugyanaz, mint az előbb.

6. Legyen $\alpha_i = \frac{a_i}{n}$ és $\varepsilon = 1/3$.
Használjuk Dirichlet tételét, ami a skatuly-elv egyszerű következménye:
Legyenek $\alpha_1, \alpha_2, \dots, \alpha_k$ valós számok. Ekkor van olyan r, hogy

$$\|\alpha_i r\| < \varepsilon,$$

igaz $i = 1, 2, \dots, k$ esetén és ahol $1 \le r \le \left(\frac{1}{\varepsilon}\right)^k$.
Emiatt tehát van olyan r,

$$1 \le r \le 3^{\log n / \log 3} = n,$$

(azaz $r \in \mathbb{Z}_n;\ r \ne 0$,) hogy minden $1 \le i \le k$ esetén

$$\left\| r \frac{a_i}{n} \right\| < \frac{1}{3}.$$

Így

$$|\widehat{A(r)}| \ge \Re(\widehat{A(r)}) \ge |A| \cdot \cos(\pi/3) = \frac{|A|}{2}.$$

7. Megmutatjuk, hogy ha Q egy R-invariáns részhalmaz, azaz $Q \cdot R = Q$, akkor $|\widehat{R(\xi)}| \le \sqrt{p|Q|/|R|}$. Mivel R egy részcsoport, ezért $R \cdot R = R$ és ekkor a második állítás következik az elsőből. Először is belátjuk, hogy ha $\xi \ne 0$ és $r \in R$, akkor $\widehat{Q(\xi)} = \widehat{Q(r\xi)}$. Valóban a definíció miatt

$$\widehat{Q(r\xi)} = \sum_{q \in Q} e(r\xi \cdot q).$$

Ám amint q végigfut Q elemein – az invariancia miatt $r \cdot q$ is végigfut Q elemein.

$$\sum_{q \in Q} e(r\xi \cdot q) = \sum_{q' \in Q} e(\xi \cdot q') = \widehat{Q(\xi)}$$

Azt kaptuk tehát, hogy egy $\widehat{Q(\xi)}$ legalább $|R|-$szer fordul elő. Így használva a Parseval-egyenlőséget

$$|R||\widehat{Q(\xi)}|^2 \le \sum_{\zeta\neq 0} |\widehat{Q(\zeta)}|^2 = p|Q| - |Q|^2 < p|Q| \;\Rightarrow\; |\widehat{Q(\xi)}| < \sqrt{\frac{p|Q|}{|R|}}.$$

8.

$$\Big|\sum_{x=k}^{k+h-1} e_n(rx)\Big| = \Big|\sum_{y=0}^{h-1} e_n(ry)\Big| = \Big|\frac{e_n(hr)-1}{e_n(r)-1}\Big| \le \frac{2}{|e_n(r)-1|},$$

mivel $e_n(r)\neq 1$. Mint láttuk

$$\frac{2}{|e_n(r)-1|} \le \frac{n}{2\min\{r,n-r\}}.$$

Így

$$\sum_{r=1}^{n}\Big|\sum_{x=k}^{k+h-1} e_n(rx)\Big| \le \sum_{r=1}^{n}\frac{n}{2\min\{r,n-r\}} \le 2n\sum_{r=1}^{n}\frac{1}{2r} = O(n\log n).$$

9. Mint láttuk $E(A)=\sum_x r_A^2(x)$ és felhasználva az ortogonalitást

$$E_p(A) = \sum_{x,x'\le 2X;\ x\equiv x' \pmod p} r(x)r(x') = \frac{1}{p}\sum_{z\in\mathbb{F}_p}\Big|\sum_{x\le 2X} r(x)e_p(zx)\Big|^2$$

így

$$\sum_{p\le\sqrt{X}} pE_p(A) = \sum_{p\le\sqrt{X}}\sum_{z\in\mathbb{F}_p}\Big|\sum_{x\le 2X} r(x)e_p(zx)\Big|^2 =$$

$$= \sum_{p\le\sqrt{X}}\sum_{z\in\mathbb{F}_p^*}\Big|\sum_{x\le 2X} r(x)e_p(zx)\Big|^2 + \sum_{p\le\sqrt{X}} p\frac{|A|^4}{p}.$$

Jegyezzük meg, hogy $|\frac{z}{p}-\frac{z'}{p'}|\ge\frac{1}{pp'}\ge\frac{1}{X}$, így a nagy szíta (gyenge) alakját használva azt kapjuk, hogy

$$\sum_{p\le\sqrt{X}}\sum_{z\in\mathbb{F}_p^*}\Big|\sum_{x\le 2X} r(x)e_p(zx)\Big|^2 \le 4XE(A).$$

10. Legyen $I(x)$ az $[a,b]$ intervallum indikátor függvénye, és – csak a jelölésmód egységessége miatt – $A(x) = a_x$. Ekkor a Plancherel azonosság miatt

$$\sum_{a\le n\le b} a_n = \sum_x I(x)A(x) = \frac{1}{N}\sum_r \widehat{A}(r)\widehat{I}(r).$$

Leválasztva az $r = 0$ tagot és használva a háromszög egyenlőtlenséget és a 8. feladatot

$$\Big|\sum_{a\le n\le b} a_n - \frac{b-a}{N}\widehat{A}(0)\Big| \ll \frac{1}{N}\max_{r\neq 0}|\widehat{A}(r)||\sum_r \widehat{I}(r)| \ll (\log N)\max_{r\neq 0}|\widehat{A}(r)|.$$

Mivel $\widehat{A}(0)$ éppen $\sum_n a_n$, kapjuk a feladat állítását.

13.2. Additív és multiplikatív karakterek; Gauss összeg

Karaktereket véges abel csoportokon szokás úgy bevezetni mint a G csoport homomorfizmusát az egy abszolút értékű komplex számokra (egységkörre).

Ebben a részben egy egyszerűsített változatát vizsgáljuk (habár minden állítás és azok bizonyítása könnyen átvihetőek az általános esetre). Későbbiekben lényegében a prímtestbeli additív és multiplikatív karaktereket fogjuk tekinteni.

Tekintsük a $\mathbb{Z}_k$ additív csoportot.

Ezen ψ **additív karakter**, ha teljesíti a $\psi(x_1 + x_2) = \psi(x_1)\psi(x_2)$ azonosságot. Mint láttuk ezek a $n-$edik egységgyökök, tehát az $\psi_r(x) = e_k(rx)$ függvények. Ezzel a jelöléssel tehát $\psi_r(x) = \psi_1(rx)$.

$\mathbb{Z}_k-$beli **multiplikatív (vagy Dirichlet) karakteren** a $\chi : \mathbb{Z}_k \mapsto \mathbb{C}$ $\chi(a\cdot b) = \chi(a)\cdot\chi(b)$ leképezés és függvény egyenlet definiálja és megvan az a tulajdonsága, hogy k szerint periodikus; azaz ha az egészeken értelmezzük, akkor teljesül a $\chi(n+k) = \chi(n)$. Konvenció, hogy $\chi(0) = 0$ és hogy a főkarakterre $\chi_0(r) = 1$ telesül minden $r \in \mathbb{Z}_k$ maradékra.

Euler tétele miatt, és mivel könnyen ellenőrízhetően $\chi(1) = 1$ azt kapjuk, hogy

$$1 = \chi(n^{\varphi(k)}) = \chi(n)^{\varphi(k)},$$

azaz χ $\varphi(k)-$adik egységgyök. Látni fogjuk (lásd a FELADAT-ot), ha $d = (n,k) > 1$, akkor $\chi(n) = 0$. A χ_0 *főkaraktert* így definiálhatjuk:

$$\chi_0(n) = \begin{cases} 1 & ha\ (n,k) = 1 \\ 0 & ha\ (n,k) > 1 \end{cases}$$

A továbbiakban a legegyszerűbb $k = p$ prím esettel foglalkozunk.

Elevenítsük fel, hogy modulo p mi az index (vagy diszkrét logaritmus) fogalma; legyen g egy fix primitív gyök modulo p és legyen $a \in \mathbb{F}_p^*$. Ekkor a felírható $a = g^x : x \in \{1, 2, \ldots, p-1\}$ formában. Az index (diszkrét logaritmus) tehát $ind_g a = ind\ a := x$.

8. Definíció. *Legyen*

$$\chi_r(t) = \exp\Big(\frac{2\pi i r \operatorname{ind}_g(t)}{p-1}\Big),\ r = 0, \ldots, p-2.$$

2. Propozíció. *Legyen $\chi_r(t)$ a fent definiált függvény. Ekkor $\chi_r(t)$ multiplikatív karakter, azaz bármely t_1, t_2 párra*

$$\chi_r(t_1 t_2) = \chi_r(t_1)\chi_r(t_2).$$

4. Megjegyzés. *1. Könnyű látni, hogy $\{\chi_r(t)\}$ karakterek halmaza ciklikus csoportot alkot (ami nyilván $(\mathbb{F}_p^*, \cdot)$ csoporttal izomorf). Ezt duális (vagy Pontryagin) csoportnak nevezik.*

2. Ellenőrizhető, hogy minden multiplikatív karakter a fent definiált formában írható fel.

3. A definícióból rögtön következik, hogy minden k esetén

$$\chi_{kr}(t) = \chi_r^k(t) = \chi_r(t^k), \quad \chi_{r_1}(x)\chi_{r_2}(x) = \chi_{r_1+r_2}(x).$$

9. Definíció. *Legyen f tetszőleges $\mathbb{F}_p^*$-ból $\mathbb{C}$-be képező függvény. Ekkor egy rögzített χ karakter szerinti Fourier-transzformáltját a*

$$\widehat{f(u)} := \sum_{x \in \mathbb{F}_p^*} f(x)\chi_u(x)$$

azonossággal definiáljuk.

13.2.1. Tétel.

$$\sum_{u\in\mathbb{F}_p^*} |\widehat{f(u)}|^2 = (p-1)\sum_{x\in\mathbb{F}_p^*} |f(x)|^2$$

$$\sum_{u\in\mathbb{F}_p^*} \widehat{f(u)}\overline{\widehat{g(u)}} = (p-1)\sum_{x\in\mathbb{F}_p^*} f(x)\overline{g(x)}$$

és

$$f(x) = \frac{1}{p-1}\sum_{r\in\mathbb{F}_p^*} \widehat{f(u)}\overline{\chi_r(x)}.$$

E tétel bizonyítása hasonlóan történik mint az additív karakterekről szóló tétel bizonyítása.

Végül definiáljuk az ú.n. **Gauss összeget** $\mathbb{Z}_k$-n a következőképpen: Legyen χ egy multiplikatív karakter, ψ_n pedig egy additív karakter. Ekkor

$$G(\chi,\psi_n) := \sum_{x=1}^{k} \chi(x)\psi_n(x)$$

összeget nevezzük Gauss összegnek. (Itt tulajdonképpen $\psi_n(x)$ az $e_k(nx)$ karaktert jelenti. Az általánosabb jelölésmód annak szól, hogy a karaktereket tetszőleges véges kommutatív csoportokban is hasonló módon lehet definiálni.)

13.2.2. Tétel. *Bármely* $(n,k)=1$ *esetén* $G(\chi,\psi_n) = \overline{\chi(n)}G(\chi,\psi_1)$.

Bizonyítás:
Mivel $\chi(n)\overline{\chi(n)} = |\chi(n)|^2 = 1$, ezért

$$G(\chi,\psi_n) = \sum_{x=1}^{k} \chi(x)\psi_n(x) = \overline{\chi(n)}\sum_{x=1}^{k} \chi(x)\chi(n)\psi_n(x) =$$

$$= \overline{\chi(n)}\sum_{x=1}^{k} \chi(nx)\psi_n(x) = \overline{\chi(n)}\sum_{x=1}^{k} \chi(nx)\psi_1(nx) = \overline{\chi(n)}\sum_{y=1}^{k} \chi(y)\psi_1(y) =$$

$$\overline{\chi(n)}G(\chi,\psi_1)$$

felhasználva, hogy $\psi_r(x) = \psi_1(rx)$.

13.2.3. Tétel. *Bármely* $(n,k)=1$ *esetén* $|G(\chi,\psi_n)|=\sqrt{k}$, *ahol* $\chi\neq\chi_0$.

Bizonyítás:
Az előző tétel miatt elég az $n=1$ esetet megnézni.

$$|G(\chi,\psi_1)|^2=G(\chi,\psi_1)\overline{G(\chi,\psi_1)}=\Big(\sum_{x=1}^{k}\chi(x)\psi_1(x)\Big)\Big(\sum_{y=1}^{k}\overline{\chi(y)}\psi_1(y^{-1})\Big)=$$

$$=\sum_{x,y}\chi(x-y)\psi_1\Big(\frac{x}{y}\Big)$$

bevezetve a $\lambda=x/y$ új változót a fenti összeg a

$$\sum_{\lambda}\psi_1(\lambda)\sum_{y}\chi(\lambda(y-1))$$

alakba írható. Az ortogonalitás miatt csak a $\lambda=1$ esetén nem nulla az összeg, így

$$|G(\chi,\psi_1)|^2=\psi_(1)k=k.\quad\square$$

FELADAT

1. Legyen $\chi\neq\chi_0$ és legyen $d=(n,k)>1$. Bizonyítsuk be, hogy $\chi(n)=0$.

MEGOLDÁS

1. $k=k'd;\ n=n'd$, ahol $1<k'<k$, azaz k' nem periódusa $\chi-$nek: tehát van olyan a egész, melyre $\nu:=\chi(a+k')-\chi(a)\neq 0$. Így

$$\nu\chi(d)=\chi(ad+k)-\chi(ad)=\chi(ad)-\chi(ad)=0.$$

Mivel ν nem nulla, így $\chi(d)=0$ és így $\chi(d)\chi(n')=\chi(n)=0$.

13.3. Néhány egyszerű alkalmazás; alsó becslések a Fourier transzformáltakra

A 13.1 paragrafus feladatai közül kettő is ($3.$ és a $6.$) az $|\widehat{A}(r)|$ értékét becsülte alulról, bizonyos feltételek mellett.

A következő állítás "nagyobb hézaggal" rendelkező sorozatok esetén ad egy alsó becslést, ha még az r frekvenciát is korlátozzuk:

13.3.1. Tétel. *Legyen* $A \subseteq \mathbb{Z}_N,\ 2|M,\ 0 < L < N, \quad L > \left(\frac{N}{2M}\right)^2$, *és tegyük fel, hogy* $A \cap [-M, M) = \emptyset$. *Ekkor van olyan* $0 < |r| < L$, *hogy*

$$\max_{0<|r|<L} |\widehat{A}(r)| \geq c_{M,N}|A|$$

ahol $c_{M,N}$ *választható* $\left(\frac{M}{N} - \frac{N}{4ML}\right)$*−nek.*

Bizonyítás:

Legyen $|A| = t$.

Legyen $I = [-M/2, M/2)$, ekkor $I \circ I = [-M, M)$ és mivel $A \cap [-M, M) = \emptyset$ azt kapjuk, hogy

$$\sum_r \widehat{A}(r)|\widehat{I}(r)|^2 = 0.$$

Idézzük fel, hogy ha J egy $2M$ hosszúságú intervallum, akkor

$$|\widehat{I}(r)| \leq \min\left\{2M, \frac{N}{2|r|}\right\}.$$

A

$$\sum_r \widehat{A}(r)|\widehat{I}(r)|^2 = 0$$

feltételből és az $|\widehat{I}(r)|$ fenti becsléséből azt kapjuk a háromszög egyenlőtlenség segítségével, hogy

$$tM^2 = \widehat{A}(0)|\widehat{I}(0)|^2 \leq \sum_{r\neq 0} |\widehat{A}(r)||\widehat{I}(r)|^2 =$$

$$= \sum_{0<|r|<L} |\widehat{A}(r)||\widehat{I}(r)|^2 + \sum_{|r|\geq L} |\widehat{A}(r)||\widehat{I}(r)|^2 \leq$$

$$\leq \max_{0<|r|<L} |\widehat{A}(r)| \sum_r |\widehat{I}(r)|^2 + t \sum_{|r|\geq L} \frac{N^2}{4|r|^2} \leq$$

$$\leq \max_{0<|r|<L} |\widehat{A}(r)|NM + t\frac{N^2}{4}\frac{1}{L},$$

amiből

$$\max_{0<|r|<L} |\widehat{A}(r)| \geq |A| \left(\frac{M}{N} - \frac{N}{4ML} \right). \quad \square$$

A következő tétel a Sidon sorozatok elemszámára vonatkozó becslés harmadik bizonyítása::

13.3.2. Tétel. *Legyen $S \subseteq \{1, 2, \ldots, N\}$ egy Sidon sorozat, azaz $r_S(n) \leq 1$ bármely n-re. Ekkor*

$$|S| \leq \sqrt{N} + \sqrt[4]{N} + 1.$$

III. Bizonyítás:

Az n paramétert később határozzuk meg; legyen $I = \{1, 2, \ldots, n\}$ és tekintsük $\mathbb{Z}_{N+n}$-ben

$$T := \sum_{x \in \mathbb{Z}_{N+n}} I \circ I(x) S \circ S(x)$$

összeget. (Ez lényegében azt méri, hogy egy $s_i - s_j$ mikor esik egy $2n+1$ hosszú intervallumba).

Nyilván

$$T \leq n|S| + n^2,$$

ugyanis

$$T = I \circ I(0) S \circ S(0) + \sum_{x \neq 0, x \in \mathbb{Z}_{N+n}} I \circ I(x) S \circ S(x) \leq |I||S| + n^2,$$

mivel $S \circ S(x) \leq 1$, az $\sum I \circ I(x)$-ben az I-beli elempárokat számoljuk össze.

Továbbá az általánosított Plancherel formula miatt

$$T = \sum_{x \in \mathbb{Z}_{N+n}} I \circ I(x) S \circ S(x) = \frac{1}{N+n} \sum_r \widehat{I \circ I}(r) \widehat{S \circ S}(r) =$$

$$= \frac{1}{N+n}\sum_r |\widehat{I}(r)|^2|\widehat{S}(r)|^2 \geq \frac{1}{N+n}|\widehat{I}(0)|^2|\widehat{S}(0)|^2 = \frac{|S|^2n^2}{N+n}.$$

Így használjuk az $|S| := m$ jelölést

$$\frac{m^2n^2}{N+n} \leq nm + n^2$$

(v.ö. a 10.3.2 tétel kombinatorikus bizonyításaival) amit átrendezve és n-et $\lfloor N^{3/4} \rfloor$-nek választva kapjuk az állítást.

A következő tételben összefüggést találunk a korlátos k-tagú összeghalmaz és a halmaz Fourier transzformáltja között:

13.3.3. Tétel. *Legyen $A \subseteq \mathbb{Z}_N$; és tegyük fel, hogy létezik $K > 0$, hogy*

$$|hA| < K|A| < \frac{N}{2}.$$

Ekkor

$$\max_{r\neq 0} |\widehat{A}(r)| > \left(\frac{1}{4K}\right)^{\frac{1}{2h-2}} |A|$$
$$> \left(1 - \frac{\ln 4K}{2h-2}\right)|A|.$$

Bizonyítás:

$$\sum_{r=1}^{N} |\widehat{A}(r)|^h |\widehat{hA}(-r)| = |A|^h \cdot N,$$

használva az ortogonalitást. Ekkor mivel $|hA| < N/2$

$$= |A|^h \cdot N = \sum_{r\neq 0} |\widehat{A}(r)|^h |\widehat{hA}(-r)| + |\widehat{A}(0)|^h |\widehat{hA}(0)| =$$

$$= \sum_{r\neq 0} |\widehat{A}(r)|^h |\widehat{hA}(-r)| + |A|^h |hA|$$

kapjuk, hogy

$$|A|^h \cdot \frac{N}{2} \leq \sum_{r\neq 0} |\widehat{A}(r)|^h |\widehat{hA}(-r)|.$$

A Cauchy egyenlőtlenséget használva

$$|A|^h \cdot \frac{N}{2} \le \sum_{r\neq 0} |\widehat{A}(r)|^h |\widehat{hA}(-r)| \le$$

$$\le \max_{r\neq 0} |\widehat{A}(r)|^{h-1} \sum_{r\neq 0} |\widehat{A}(r)||\widehat{hA}(-r)| \le$$

$$\le \max_{r\neq 0} |\widehat{A}(r)|^{h-1} \big(\sum_{r\neq 0} |\widehat{A}(r)|^2\big)^{1/2} \big(\sum_{r\neq 0} |\widehat{hA}(-r)|^2\big)^{1/2} \le$$

$$\le \max_{r\neq 0} |\widehat{A}(r)|^{h-1} \cdot \sqrt{|A|N}\sqrt{|hA|N}.$$

Átrendezve

$$\max_{r\neq 0} |\widehat{A}(r)|^{h-1} \ge |A|^{h-1} \sqrt{\frac{|A|}{4|hA|}} > |A|^{h-1} \sqrt{\frac{1}{4K}},$$

amiből

$$\max_{r\neq 0} |\widehat{A}(r)| > \big(\frac{1}{4K}\big)^{\frac{1}{2h-2}} |A|.$$

A másik becslésnél az

$$M^{-x} = e^{-x\ln M} > 1 - x\ln M$$

összefüggést használtuk, így igaz a

$$\max_{r\neq 0} |\widehat{A}(r)| > \big(1 - \frac{\ln 4K}{2h-2}\big)|A|$$

is.

13.3.4. Tétel. *Legyen* $B, C \subseteq \mathbb{Z}_n$, $|B| = \beta n$, $|C| = \gamma n$. *Legyen* $A = \mathbb{Z}_n \setminus (B + C)$.

Ekkor bármely $S \subseteq A$

$$\max_{x\neq 0} |\widehat{S}(x)| \ge \sqrt{\beta\gamma}|S|.$$

Bizonyítás:
Használni fogjuk a halmaz indikátor függvényét:

$$A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

Ekkor

$$B * C(x) = r(x),$$

ahol $r(x)$ jelöli, hogy hányféleképpen írható fel $x = b + c$ alakban ($b \in B;\ c \in C$). Mivel $S \subseteq A$, $S(x)$ pontosan akkor 0, ha $B * C(x) = 1$, így

$$\sum_x S(x)(B * C(x)) = 0.$$

A Plancherel formula miatt

$$\sum_a S(x)(B * C(x)) = 0 \ \Leftrightarrow \ \sum_x \widehat{S}(x)\overline{(\widehat{B * C})(x)} = 0.$$

Mivel

$$(\widehat{B * C})(x) = \widehat{B}(x)\widehat{C}(x),$$

így

$$\sum_x \widehat{S}(x)\overline{(\widehat{B * C}(x))} = \sum_x \widehat{S}(x)\overline{\widehat{B}(x)\widehat{C}(x)} = 0.$$

Továbbá

$$\sum_x \widehat{S}(x)\overline{\widehat{B}(x)\widehat{C}(x)} = \widehat{S}(0)\widehat{B}(0)\widehat{C}(0) + \sum_{x \neq 0} \widehat{S}(x)\overline{\widehat{B}(x)\widehat{C}(x)} =$$

$$= |S||B||C| + \sum_{x \neq 0} \widehat{S}(x)\overline{\widehat{B}(x)\widehat{C}(x)} = 0.$$

A háromszög egyenlőtlenség miatt

$$|S||B||C| \leq \sum_{x \neq 0} |\widehat{S}(x)||\widehat{B}(x)||\widehat{C}(x)| \leq$$

$$\leq \sup_{x \neq 0} |\widehat{S}(x)| \sum_{x \neq 0} |\widehat{B}(x)||\widehat{C}(x)| \leq$$

és a Cauchy egyenlőtlenség miatt

$$\leq \sup_x |\widehat{S}(x)|(\sum_x |\widehat{B}(x)|^2)^{1/2}(\sum_x |\widehat{C}(x)|^2)^{1/2} = *.$$

A Parseval formula miatt

$$(\sum_x |\widehat{B}(x)|^2) = n\sum_x |B(x)|^2 = n|B|$$

és hasonlóan

$$(\sum_x |\widehat{C}(x)|^2) = n\sum_x |C(x)|^2 = n|C|.$$

Ezért

$$* = \sup_x |\widehat{S}(x)| n\sqrt{|B||C|} = \sup_x |\widehat{S}(x)| n^2\sqrt{\beta\gamma}.$$

Továbbá

$$|S||B||C| = |S|n^2\beta\gamma \leq \sup_x |\widehat{S}(x)| n^2\sqrt{\beta\gamma},$$

amiből

$$\sup_{x\neq 0} |\widehat{S}(x)| \geq \sqrt{\beta\gamma}|S|. \quad \square$$

A következő tételt szokás a diszkrét Fourier transzformáltakra vonatkozó "Határozatlansági reláció"-nak is nevezni.

13.3.5. Tétel. *Jelölje supp(u) egy u(x) $\mathbb{Z}_N-$beli függvény azon x−einek a halmazát, amelyre $u(x) \neq 0$.*

Ekkor

$$N \leq |supp(u)| \cdot |supp(\widehat{u})|.$$

Bizonyítás:

A Cauchy egyenlőtlenség és a Parseval formula miatt

$$\max_r |\widehat{u}(r)| \leq \sum_x |u(x)| \leq \sqrt{|\mathsf{supp}(u)|}\cdot\sqrt{\sum_x |u(x)|^2} = \sqrt{|\mathsf{supp}(u)|}\cdot\sqrt{\frac{1}{N}\sum_r |\widehat{u}(r)|^2} \leq$$

$$\leq \sqrt{|\mathsf{supp}(u)|}\cdot\sqrt{\frac{1}{N}\cdot|\mathsf{supp}(\widehat{u})|}\cdot\max_r |\widehat{u}(r)|,$$

így

$$N \leq |\mathsf{supp}(u)| \cdot |\mathsf{supp}(\widehat{u})|. \quad \square$$

13.4. Bilineáris exponenciális összeg becslése

Ebben a pontban két becslést fogunk bizonyítani az

$$S(r) = \sum_{x=1}^{N} \sum_{y=1}^{N} v(x)\varrho(y)e(xy)$$

ú.n. bilineáris exponenciális összegre ($e(\cdot) = e_N(\cdot)$), valamint a 11.1.8 tételre egy erősebb becslést, amennyiben $\alpha > \frac{4}{9}$.

Az első becslés Vinogradovtól származik:

13.4.1. Tétel. *Legyen $r \neq 0$, és*

$$S(r) = \sum_{x=1}^{N} \sum_{y=1}^{N} v(x)\varrho(y)e(rxy),$$

és legyen

$$\sum_{x=1}^{N} |v(x)|^2 = X; \ \sum_{x=y}^{N} |\varrho(y)|^2 = Y.$$

Ekkor

$$|S(r)| \leq \sqrt{X \cdot Y \cdot N}.$$

Bizonyítás:

$$S(r) = \sum_{x=1}^{N} \sum_{y=1}^{N} v(x)\varrho(y)e(rxy) = \sum_{x=1}^{N} v(x) \sum_{y=1}^{N} \varrho(y)e(rxy) =$$

$$= \sum_{x=1}^{N} v(x)\widehat{\varrho(rx)}.$$

A Cauchy egyenlőtlenség és a Parseval formula miatt

$$|S(r)|^2 = \left| \sum_{x=1}^{N} v(x)\widehat{\varrho(rx)} \right|^2 \leq \Big(\sum_{x=1}^{N} |v(x)|^2 \Big) \cdot \Big(\sum_{x=1}^{N} |\varrho(rx)|^2 \Big) \leq$$

$$\leq \Big(\sum_{x=1}^{N} |v(x)|^2 \Big) \cdot \Big(\sum_{x=1}^{N} |\varrho(x)|^2 \Big) = N \cdot X \cdot Y. \quad \square$$

3. Következmény. *Legyen* $A, B \subseteq \mathbb{Z}_N$ $r \neq 0$. *Ha*

$$S(r) = \sum_{x \in A} \sum_{y \in B} e(rxy),$$

akkor

$$|S(r)| \leq \sqrt{|A| \cdot |B| \cdot N}.$$

A másik becslés Bourgain-Garaev egy eredménye:

13.4.2. Tétel. *Legyen* $A, B \subseteq \mathbb{Z}_N$ $r \neq 0$. *Ha*

$$S(r) = \sum_{x \in A} \sum_{y \in B} e(rxy),$$

akkor

$$|S(r)|^8 \leq N \cdot |A|^4 \cdot |B|^4 E_+(A) E_+(B),$$

ahol E *az additív energia, azaz*

$$E_+(X) := \{(a, b, a', b') \in X^4 : a + b = a' + b'\}.$$

Bizonyítás:

Használjuk az exponenciális összeg kifejtését és a Cauchy egyenlőtlenséget:

$$|S(r)|^2 \leq |A| \sum_{y, y' \in B} \left| \sum_{x \in A} e(rx(y - y')) \right|.$$

Emeljük négyzetre és ismételjük meg az előzőt, csak most az A szerepében a $B \times B$ legyen. Továbbá legyen $d(z) = \{(y, y' \in B; z = y - y'\}$. Ekkor

$$|S(r)|^4 \leq |A|^2 |B|^2 \sum_{z \in \mathbb{Z}_N} d(z) \left| \sum_{x \in A} e(rxz) \right|^2.$$

Végül még egyszer a Cauchy egyenlőtlenséget alkalmazva

$$|S(r)|^8 \leq |A|^4 |B|^4 \sum_{z \in \mathbb{Z}_N} d^2(z) \sum_{z \in \mathbb{Z}_N} \left| \sum_{x \in A} e(rxz) \right|^4 =$$

$$= N \cdot |A|^4 \cdot |B|^4 E_+(A) E_+(B). \quad \square$$

5. Megjegyzés. *Egyszerű számítás mutatja, hogy a második becslés a kedvezőbb, ha*

$$E_+(A)E_+(B) < N^3,$$

ellenkező esetben pedig a Vinogradov becslés az élesebb.

Jegyezzük meg (könnyű bizonyítani), hogy

$$E_+(X) \leq |X|^3.$$

Így ha

$$|A||B| < N,$$

azaz ha a két halmaz együttvéve "kis" halmazok, akkor a második becslés az élesebb.

A következő tételben megmutatjuk, hogy erősebb becslés nyerhető a 11.1.8 tételre:

13.4.3. Tétel. *Legyen $A \subseteq \mathbb{F}_p$, $|A| = p^\alpha$. Ekkor*

$$|\mathbb{Z}_p - (A + AA)| \leq p^{3-3\alpha}.$$

Valóban egy egyszerű számítás mutatja, hogy e tétel $\alpha > \frac{4}{9}$ esetén erősebb.

Bizonyítás:

Jelölje röviden S az $A+AA$ halmazt. Ekkor $E(S)$ energia azon $(x, y, z, x', y', z') \in A^6$ hatosok számát számlálja, melyekre $xy + z = x'y' + z'$. $E(S)$ könnyen láthatóan a következőképpen számlálható le:

$$\begin{aligned} E(S) &= \frac{1}{p}\sum_{h=1}^{p}\Big|\sum_{x,y\in A} e_p(hxy)\Big|^2\Big|\sum_{z\in A} e_p(hz)\Big|^2 \\ &\leq \frac{|A|^6}{p} + \max_{1\leq h\leq p-1}\Big|\sum_{x,y\in A} e_p(hxy)\Big|^2 \times \frac{1}{p}\sum_{h=1}^{p-1}\Big|\sum_{z\in A} e_p(hz)\Big|^2 \\ &\leq \frac{|A|^6}{p} + \big(\sqrt{p|A|^2}\big)^2\Big(|A| - \frac{|A|^2}{p}\Big) = \frac{|A|^6}{p} + p|A|^3 - |A|^4, \end{aligned}$$

ahol a második egyenlőtlenségnél a $\max_{1\leq h\leq p-1}\Big|\sum_{x,y\in A} e_p(hxy)\Big|^2$-t a Vinogradov egyenlőtlenséggel becsültük, valamint a Parseval azonosságot használtuk.

Végül a szokásos Cauchy egyenlőtlenség miatt

$$|A+AA| \geq \frac{|A|^6}{E(S)} \geq p\left(1+\frac{p^2}{|A|^3}-\frac{p}{|A|^2}\right)^{-1} \geq p-\frac{p^3}{|A|^3}+\frac{p^2}{|A|^2}$$

amiből egyszerű átrendezéssel kapjuk a

$$p-|A+AA| < \frac{p^3}{|A|^3} = p^{3-3\alpha}$$

becslést. □

Összehasonlítva a 11.1.8 tétel becslésével

$$p^{3-3\alpha} < p^{2-3\alpha/4}$$

teljesül, amint $\alpha > \frac{4}{9}$.

A következő tétel az előbbi Vinogradov tétel multiplikatív karakterekre vonatkozó analogonja.

13.4.4. Tétel. *Legyen $A, B \in \mathbb{F}_p$, és $\chi \neq \chi_0$. Ekkor*

$$\left|\sum_{a\in A; b\in B} \chi(a+b)\right| \leq \sqrt{p|A||B|}\sqrt{1-\frac{|A|}{p}}\sqrt{1-\frac{|B|}{p}}.$$

Bizonyítás:

Jegyezzük meg a Gauss-összegre vonatkozóan, hogy $G(r) = \sum_x \chi^{-1}(x)e(rx)$, továbbá, hogy $r \neq 0$ esetén $|G(r)| = \sqrt{p}$.

Ha $r \neq 0$, akkor rx végigfut $\mathbb{F}_p$ elemein, így

$$G(r)\chi^{-1}(r) = \sum_x \chi^{-1}(x)\chi^{-1}(r)e(rx) = \sum_y \chi^{-1}(y)e(y) = G(1)$$

és ezért

$$\left|\sum_{a\in A; b\in B} \chi(a+b)\right| = \frac{1}{\sqrt{p}}\left|\sum_{a\in A; b\in B} G(a+b)\right| =$$

$$= \frac{1}{\sqrt{p}} \left| \sum_{a\in A; b\in B} \sum_{x\neq 0} \chi^{-1}(x) e((a+b)x) \right| = \frac{1}{\sqrt{p}} \left| \sum_{x\neq 0} \chi^{-1}(x) \sum_{a\in A} e(ax) \sum_{b\in B} e(bx) \right| \leq$$

$$\leq \frac{1}{\sqrt{p}} \sum_{x\neq 0} \left| \sum_{a\in A} e(ax) \right| \left| \sum_{b\in B} e(bx) \right| \leq$$

használva a Cauchy egyenlőtlenséget

$$\leq \frac{1}{\sqrt{p}} \left(\sum_{x\neq 0} \left| \sum_{a\in A} e(ax) \right|^2 \right)^{1/2} \left(\sum_{x\neq 0} \left| \sum_{b\in B} e(bx) \right|^2 \right)^{1/2} =$$

majd a Parseval formulát

$$= \frac{1}{\sqrt{p}} (p|A| - |A|^2)^{1/2} (p|B| - |B|^2)^{1/2} = \sqrt{p|A||B|} \sqrt{1 - \frac{|A|}{p}} \sqrt{1 - \frac{|B|}{p}}. \quad \square$$

A következő tételben az $\mathbb{F}_p^*$ multiplikatív csoport R részcsoportjának Fourier-transzformáltjára vonatkozó becsléssel foglalkozunk:

13.4.5. Tétel. *Legyen R az $\mathbb{F}_p^*$ egy R multiplikatív részcsoportja. Ekkor bármely $\xi \neq 0$ esetén*

$$(1) \quad |\widehat{R(\xi)}| < \sqrt{p}; \quad ha \quad p^{2/3} < |R|,$$

$$(2) \quad |\widehat{R(\xi)}| \ll p^{1/4} |R|^{3/8} \quad ha \quad p^{1/2} \leq |R| < p^{2/3},$$

$$(3) \quad |\widehat{R(\xi)}| \ll p^{1/8} |R|^{5/8} \quad ha \quad |R| < p^{1/2}.$$

Bizonyítás:
Az (1) a $13.$ fejezet $7.$ feladata.

A (2) bizonyításhoz a következő lemmára van szükség:

18. Lemma. *Legyen Q egy $R-$invariáns halmaz, azaz $Q = Q \cdot R$. Ekkor bármely $\xi \neq 0$ esetén*

$$|\widehat{Q(\xi)}| \leq |Q|^{3/4}|R|^{-1}(pE_+(R))^{1/4}.$$

Speciálisan, ha $Q = R$, akkor

$$|\widehat{R(\xi)}| \leq \frac{p^{1/4}E_+(R)^{1/4}}{|R|^{1/4}}.$$

A lemma bizonyítása:

Nyilván elég az első becslést igazolni. A Q az R mellékosztályainak az uniója; $Q = \cup_{i=1}^{T} x_i R$ valamely $\{x_i\}$ halmazzal, $T = |Q|/|R|$. Így a háromszög és a Hölder egyenlőtlenségek segítségével

$$|\widehat{Q(\xi)}| = \big|\sum_{i=1}^{T} \widehat{R(x_i\xi)}\big| \leq \sum_{i=1}^{T} \big|\widehat{R(x_i\xi)}\big| \leq T^{3/4}(\sum_{i=1}^{T} |\widehat{R(x_i\xi)}|^4)^{1/4} =$$

$$= |Q|^{3/4}|R|^{-1}(\sum_{i=1}^{T} |R||\widehat{R(x_i\xi)}|^4)^{1/4} = |Q|^{3/4}|R|^{-1}(\sum_{x\in\mathbb{F}_p^*} |\widehat{R(x)}|^4)^{1/4} =$$

felhasználva, hogy a mellékosztályokon $\widehat{R(\cdot)}$ ugyanazt az értéket veszik fel, továbbá, hogy így az utolsó zárójelben $p-$szer az additív energia van,

$$= |Q|^{3/4}|R|^{-1}(pE_+(R))^{1/4}.$$

A második és harmadik becsléshez bizonyítás nélkül használjuk a következő lemmát:

19. Lemma. *Legyen $R < \mathbb{F}_p^*$, és tegyük fel, hogy $|R| \ll p^{2/3}$. Ekkor*

$$E_+(R) \ll |R|^{5/2}.$$

(Jegyezzük meg, hogy ez erős eredmény, a triviális az $E_+(R) \ll |R|^3$).

Megint felhasználva, hogy a mellékosztályokon $\widehat{R(\cdot)}$ ugyanaz az érték,

$$|R|^2|\widehat{R(\xi)}|^2 = |\sum_{x,y\in R} e(xy\xi)|^2.$$

A 13.4.2 tételt $A = B = R$ halmazra alkalmazva és a fenti lemmából

$$|\sum_{x,y\in R} e(xy\xi)|^2 \leq p^{1/4}|R|^2E_+(R)^{1/2} \ll p^{1/4}|R|^{2+5/4}.$$

Ezt beírva az előbbi becslésbe és egyszerűsítve $|R|^2-$tel kapjuk a (3) becslést. □

13.5. Lineáris egyenletek megoldhatósága prímtestben

Már a 13.3 pontban láttunk alsó becsléseket a diszkrét Fourier transzformáltakra.

Legyen $A \subseteq \mathbb{F}_p$ és legyen $|A| = \gamma p$. Ha definiáljuk az

$$R := \{r : |\widehat{A}(r)| > \varrho|A|\}$$

halmazt, tehát azokat a frekvenciákat, ahol, a transzformált "nagy", egy egyszerű számolással kvantitatív becslést is kaphatunk R elemszámára. Valóban legyen $|A| = \gamma|A|$, ekkor a Parseval egyenlőtlenséget felhasználva

$$p|A| = \sum_r |\widehat{A}(r)|^2 \geq |R|\varrho^2|A|^2,$$

amiből $|R| < \varrho^{-2}\frac{1}{\gamma}$.

Ennél erősebb állítás Chang tétele, ami R szerkezetéről, lefedhetőségéről szól, és amit bizonyítás nélkül közlünk:

3. Propozíció. *Legyen $A \subseteq \mathbb{F}_p$ és legyen $|A| = \gamma p$ és $R := \{r : |\widehat{A}(r)| > \varrho|A|\}$. Ekkor R lefedhető egy*

$$P(Q) = \Big\{ \sum_{i=1}^{s} \varepsilon_i q_i : \varepsilon_i \in \{-1, 0, 1\} \Big\}$$

halmazzal, ahol $s = |Q| \leq 2\varrho^{-2} \log \frac{1}{\gamma}$.

Ez az állítás segítségünkre lesz abban, hogy lineáris egyenletek prímtestbeli megoldhatóságát megvizsgáljuk:

13.5.1. Tétel. *Tekintsük az*

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = b$$

egyenletet, ahol $b \neq 0$. Tegyük fel, hogy ennek a lineáris egyenletnek egy W halmazban nincs megoldása. Ekkor

$$\max |W| \leq \frac{p}{2^{s/6}},$$

ahol $s := \min\{|B| : P(B) \supseteq A\}$.

6. Megjegyzés. *Chang tétele nélkül csak a gyengébb*

$$\max|W| \le \frac{p}{\sqrt[3]{s}}$$

becslést kapnánk.

Bizonyítás:

Jelölje – szokásos módon – N a fenti lineáris egyenlet megoldásainak a számát és $|W| = \gamma p$. Ekkor

$$pN = \sum_{r=0}^{p-1} \widehat{W}(ra_1)\widehat{W}(ra_2)\cdots\widehat{W}(ra_k)e_p(-rb)$$

és mivel nincs megoldása az egyenletnek, ezért ez az összeg nulla. Ebből adódóan az $r = 0$ taghoz tartozó érték abszolútértéke egyenlő a többi tag abszolútértékével, ezért a háromszög egyenlőtlenséget használva kapjuk, hogy

$$|W|^k \le \sum_{r=1}^{p-1} |\widehat{W}(ra_1)||\widehat{W}(ra_2)|\cdots|\widehat{W}(ra_k)|$$

Legyen $\prod_{i=1}^{k} |\widehat{W}(r_0a_i)| = \max_{r\neq 0}\prod_{i=1}^{k}|\widehat{W}(ra_i)|$. Ekkor a fenti egyenlőtlenségből

$$|W|^k \le \prod_{i=1}^{k} |\widehat{W}(r_0a_i)|^{1-\frac{2}{k}} \sum_{r=1}^{p-1}\prod_{i=1}^{k}|\widehat{W}(ra_i)|^{2/k}.$$

Használjuk a Hölder egyenlőtlenséget az $r = \frac{2}{k}$ és $i = 1, 2, \ldots k$ esetén $p_i = 2$ paraméterekre

$$|W|^k \le \prod_{i=1}^{k} |\widehat{W}(r_0a_i)|^{1-\frac{2}{k}} \prod_{i=1}^{k}\Big(\sum_{r=1}^{p-1}|\widehat{W}(ra_i)|^2\Big)^{1/k} \le p|W|\prod_{i=1}^{k}|\widehat{W}(r_0a_i)|^{1-\frac{2}{k}}$$

felhasználva, hogy $|W| = \gamma p$ és átrendezve azt kapjuk, hogy

$$\gamma^{\frac{k}{k-2}}|W|^k \le \prod_{i=1}^{k}|\widehat{W}(r_0a_i)|.$$

Legyen $\delta > 0$ később meghatározandó paraméter. Most a "nagy" Fourier transzformáltakat egy R halmzba gyűjtjük

$$R := \{r_0 a_i : |\widehat{W}(r_0 a_i)| \geq \gamma^{\frac{\delta}{k}} |W|\}.$$

Az R halmaz méretére a fenti becslésből következtethetünk: mivel $|\widehat{W}(r_0 a_i)| \leq |W|$ mindig teljesül az R halmaz elemeire, így

$$\gamma^{\frac{k-2}{k}} |W|^k \leq \left(\gamma^{\frac{\delta}{k}} |W|\right)^{k-|R|} |W|^{|R|},$$

amiből $|R| > k - \frac{k}{\delta}$ és így

$$|r_0 A \setminus R| < \frac{k}{\delta}.$$

Most a 3. Propozíciót használjuk a $\varrho = \gamma^{\frac{\delta}{k-2}}$ paraméterrel. Ekkor azt kapjuk, hogy van olyan $\Gamma \subseteq \mathbb{F}_p$, melyre

$$|\Gamma| \leq 2\gamma^{-\delta/(k-2)} \log\left(\frac{1}{\gamma}\right),$$

és amelyre $P(\Gamma) \supseteq R$. Ehhez a Γ halmazhoz vegyük hozzá $r_0 A$ azon elemeit, amelyek nem tartoznak R-hez – jelöljük ezt a halmaz Γ'-vel – ekkor

$$P(\Gamma') \supseteq R \cup (r_0 A \setminus R) = r_0 A.$$

Chang tételéből és az $r_0 A \setminus R$ halmaz elemszámára vonatkozó becslésből

$$|\Gamma'| < 2\gamma^{-\delta/(k-2)} \log\left(\frac{1}{\gamma}\right) + \frac{k}{\delta}.$$

A δ paraméter függvényében a jobb oldalt minimalizálva kapjuk, hogy

$$|\Gamma'| \leq 6 \log\left(\frac{1}{\gamma}\right),$$

amiből kapjuk az állítást. □

13.6. Rudin tétel néhány következménye

Az előbbi paragrafusban Chang egy spektrál tételét használtuk. E tétel bizonyításában alapvető szerepet játszott Rudin egy tétele. Használjuk a következő jelöléseket itt: legyen G egy kommutatív csoport és $f : G \mapsto \mathbb{C}$. Legyen

$$\|f\|_{L^p_G} := \Big(\frac{1}{|G|}\sum_x |f(x)|^p\Big)^{1/p}; \quad \|f\|_{l^p_G} := \Big(\sum_r |f(r)|^p\Big)^{1/p}.$$

Egy Λ tetszőleges véges halmazt disszociatívnak nevezzük, ha a $\sum_{\lambda_i\in\Lambda}\varepsilon_i\lambda_i$ alakú elemek páronként különbözőek. Ezt úgy is megfogalmazhatjuk, hogy a

$$\sum_{\lambda_i\in\Lambda}\eta_i\lambda_i = 0$$

egyenlet $\eta_i \in \{-1, 0, 1\}$ mellett csak úgy teljesülhet, hogy minden $\eta_i = 0$. Ebből rögtön következik, hogy ha $A \subseteq G$ és Λ egy maximális disszociatív részhalmaza egy A véges halmaznak, akkor

$$\mathsf{Span}(\Lambda) := \Big\{\sum_{\lambda_i\in\Lambda}\eta_i\lambda_i\Big\} \supseteq A.$$

Ekkor

13.6.1. Tétel (Rudin). *Legyen G egy kommutatív csoport és $a_r \in \mathbb{C}$ jelöljön komplex számokat. Legyen Λ egy tetszőleges véges disszociatív halmaz. Ekkor bármely $2 \le p < \infty$ esetén*

$$\Big(\frac{1}{|G|}\sum_x(\sum_{r\in\Lambda}|a_re^{2\pi rx}|^p\Big)^{1/p} = O\Big(\sqrt{p}(\sum_{r\in\Lambda}|a_r|^2\Big)^{1/2}$$

Tehát a norma jelölésekkel, ha $f(x) := a_re^{2\pi rx}$, akkor igaz, hogy

$$\|f\|_{L^p_G} = O(\sqrt{p}\|f\|_{l^2_G}).$$

E tételt itt nem bizonyítjuk, hanem néhány szép következményét fogjuk igazolni. Elsőként egy "diszkrepancia" tételt:

13.6.2. Tétel. *Legyen $p \geq 2$ valós szám, t pozitív egész. Tegyük fel, hogy G egy kommutatív csoport, $A \subseteq G$ egy véges részhalmaza. Ekkor létezik olyan $A_1 \subseteq A$, amelynek bármely disszociatív részhalmaza legfeljebb t elemű. Ekkor*

$$\Big(\frac{1}{|G|}\sum_{r\in G}|\widehat{A}(r)-\widehat{A_1}(r)|^p\Big)^{1/p} = O\Big(\sqrt{\frac{p}{t}}|A|\Big).$$

Bizonyítás:

Válasszunk ki A-ból egy t elemű disszociatív részhalmazt. Ha ilyen nincs, akkor A_1 üres halmaznak választható; ekkor a bizonyítandó exponenciális összeg becslés éppen a Rudin tétel. Legyen $D_1 \subseteq A$ tehát egy t elemű disszociatív részhalmaz és folytassuk az eljárást: keressünk az $A \setminus D_1$ halmazban egy t elemű disszociatív részhalmazt. Legyen ez D_2. Ezt az ejárást legfeljebb $k = \lfloor |A|/t \rfloor$ lépésben folytathatjuk. Emiatt az $A \setminus \cup_{i=1}^{k} D_i := A_1$ halmaz definíció szerint olyan, amelynek bármely disszociatív részhalmaza legfeljebb t elemű. Így

$$\Big(\frac{1}{|G|}\sum_{r\in G}|\widehat{A}(r)-\widehat{A_1}(r)|^p\Big)^{1/p} = \Big(\frac{1}{|G|}\sum_{r\in G}|\sum_{i=1}^{k}\widehat{D_i}(r)|^p\Big)^{1/p}$$

amit – mivel az L_p normára igaz a háromszög egyenlőlenség – úgy becsülhetünk tovább, mint

$$\Big(\frac{1}{|G|}\sum_{r\in G}|\sum_{i=1}^{k}\widehat{D_i}(r)|^p\Big)^{1/p} \leq \sum_{i=1}^{k}\Big(\frac{1}{|G|}\sum_{r\in G}|\widehat{D_i}(r)|^p\Big)^{1/p}.$$

Rudin tétele miatt minden egyes $(\frac{1}{|G|}\sum_{r\in G}|\widehat{D_i}(r)|^p)^{1/p}$ tag felül becsülhető $O(\sqrt{pt})$-vel, így

$$\Big(\frac{1}{|G|}\sum_{r\in G}|\widehat{A}(r)-\widehat{A_1}(r)|^p\Big)^{1/p} = \sum_{i=1}^{k} O(\sqrt{pt}) = O\Big(\sqrt{\frac{p}{t}}|A|\Big). \ \square$$

Az alábbi tételben arra kapunk választ, hogy egy olyan halmazpárnak, amelynek "nagy" az additív energiája, milyen struktúrális tulajdonsága van. Emlékeztetnénk, hogy bármely $A, B \subseteq G$ esetén $E(A,B) \leq |A||B|^2$. "Nagy" itt azt jelenti, hogy $E(A,B) \geq c|A||B|^2$ valamely $0 < c \leq 1$ értékkel. (Megjegyeznénk, hogy itt a c függhet a halmazok elemszámától, tehát ez a "nagy" nem is feltétlenül nagy).

13.6.3. Tétel. *Legyen $A, B \subseteq G$ és tegyük fel, hogy $E(A,B) \geq c|A||B|^2$ valamely $0 < c \leq 1$ értékkel.Ekkor létezik egy $B_1 \subseteq B$ halmaz és egy $\Lambda \subseteq G$, melyre $Span(\Lambda) \supseteq B_1$, $|\Lambda| \ll (\log|A|)/c$ és erre az A, B_1 párra is nagy az additív energia, azaz*

$$E(A,B_1) \geq E(A,B)/40.$$

Bizonyítás:

Felhasználjuk a 13.6.2 tételt a $p = \log|A|$ és $t = (3\log|A|)/c$ választással. E tétel miatt létezik egy $B_1 \subseteq B$ halmaz, melynek minden disszociatív részhalmaza legfeljebb t elemű. Legyen $E(x) := B(x) - B_1(x)$. A 13.1 paragrafus 2. feladatánál láttuk, hogy az additív energia felírható exponenciális összegek segítségével:

$$NE(A,B) = \sum_r |\widehat{A}(r)|^2|\widehat{B}(r)|^2 = \sum_r |\widehat{A}(r)|^2(|\widehat{B}_1(r) + E(r)|^2) =$$

$$= \sum_r |\widehat{A}(r)|^2|\widehat{B}_1(r)|^2 + \sum_r |\widehat{A}(r)|^2|\widehat{E}(r)|^2 +$$

$$+ \sum_r |\widehat{A}(r)|^2\widehat{B}_1(r)\overline{\widehat{E}(r)} + \sum_r |\widehat{A}(r)|^2\overline{\widehat{B}_1(r)}\widehat{E}(r) = S_1 + S_2 + S_3 + S_4.$$

E négy összeg közül először az S_2-re alkalmazzuk a Hölder egyenlőtlenséget az $1 - 1/p$ és p paraméterekkel. Ekkor

$$S_2 = \sum_r |\widehat{A}(r)|^2|\widehat{E}(r)|^2 \leq \Big(\sum_r |\widehat{A}(r)|^{\frac{2p}{p-1}}\Big)^{\frac{p-1}{p}} \Big(\sum_r \widehat{E}(r)|^{2p}\Big)^{1/p}$$

Akkor tehát a $\Big(\sum_r \widehat{E}(r)|^{2p}\Big)^{1/p}$ tényezőre alkalmazhatjuk a 13.6.2 tételt. Így azt kapjuk, hogy

$$\Big(\sum_r |\widehat{E}(r)|^{2p}\Big)^{1/p} = \Big(\Big(\sum_r |\widehat{E}(r)|^{2p}\Big)^{1/2p}\Big)^2 \ll \frac{p}{t}|B|^2.$$

Most alakítsuk át

$$\Big(\sum_r |\widehat{A}(r)|^{\frac{2p}{p-1}}\Big)^{\frac{p-1}{p}} = \Big(\sum_r |\widehat{A}(r)|^{\frac{2p-2}{p-1}}|\widehat{A}(r)|^{\frac{2}{p-1}}\Big)^{\frac{p-1}{p}} \leq$$

$$\leq \Big(|A|^{\frac{2}{p-1}}\sum_r |\widehat{A}(r)|^2\Big)^{\frac{p-1}{p}} = N^{1-1/p}|A|^{1+1/p} < N|A|^{1+1/p}$$

felhasználva a Parseval egyenlőtlenséget. Így

$$S_2 = \sum_r |\widehat{A}(r)|^2 |\widehat{E}(r)|^2 \ll \frac{p}{t}|B|^2 N|A|^{1+1/p}.$$

Tehát a már említett $p = \log|A|$ és $t = (3\log|A|)/c$ választás mellett

$$S_2 \ll \frac{c}{2}N|A||B|^2 \leq NE(A,B)/2$$

teljesül. Ezért valamely $i = 1, 3, 4$-re teljesül, hogy $S_i \gg NE(A,B)$. Ha ez S_1, akkor ez maga az állítás. Mivel S_3 és S_4 szerepe szimmetrikus, tegyük fel, hogy $S_3 \gg NE(A,B)$. A Cauchy egyenlőtlenség miatt

$$N^2E^2(A,B) \ll$$

$$\ll \Big(\sum_r |\widehat{A}(r)|^2 \widehat{B}_1(r)\overline{\widehat{E}(r)}\Big)^2 \leq \Big(\sum_r (|\widehat{A}(r)||\widehat{B}_1(r)|)(|\widehat{A}(r)||\overline{\widehat{E}(r)}|)\Big)^2 \leq$$

$$\leq \Big(\sum_r (|\widehat{A}(r)|^2|\widehat{B}_1(r)|^2\Big)\Big(\sum_r |\widehat{A}(r)|^2|\widehat{E}(r)|^2\Big) = NE(A,B_1)S_2,$$

használva az S_2-re vonatkozó felső becslést, kapjuk a kívánt állítást. □

13.7. Összeg-szorzat egyenlet prímtestekben

Schur egy ismert állítása, hogy az $x^n+y^n \equiv z^n \pmod p$ "egyenletnek" létezik nem triviális megoldása, ha $p > [n!e]$. A bizonyítás – mai nyelven szólva – egy Ramsey típusú gráfelméleti tételből következik; egy elég nagy méretű $|G| > [n!e]+1$ gráf éleit n színnel színezve, e gráf tartalmaz egyszínű háromszöget.

A következő általánosabb tétel jóval hatékonyabb, és így egy lényegesen jobb becslést ad.

13.7.1. Tétel. *Legyen $A, B, C, D \subseteq \mathbb{F}_p$. Tegyük fel, hogy $|A||B||C||D| > p^3$, akkor az*

$$a + b = cd$$

egyenletnek van megoldása $\mathbb{F}_p^*-$ben.

Bizonyítás:
Jelentse N a fenti egyenlet megoldásszámát. Ekkor

$$N = \frac{1}{p} \sum_r \sum_{a,b,c,d} e(r(cd - a - b))$$

($a \in A; b \in B; c \in C; d \in D$.)
Elkülönítve az $r = 0$ tagot és használva a Vinogradov egyenlőtlenséget

$$N = \frac{|A||B||C||D|}{p} + \sum_{r \neq 0} \sum_{a,b,c,d} e(r(cd-a-b)) \geq \frac{|A||B||C||D|}{p} - \sqrt{p|C||D|} \sum_r |\widehat{A}(r)||\widehat{B}(r)|.$$

A Cauchy egyenlőtlenség és a Parseval egyenlőség miatt

$$\sum_r |\widehat{A}(r)||\widehat{B}(r)| \leq \left(\sum_r |\widehat{A}(r)|^2 \right)^{1/2} \left(\sum_r |\widehat{B}(r)|^2 \right)^{1/2} =$$

$$= p\sqrt{|A||B|}.$$

Ezért

$$N \geq \frac{|A||B||C||D|}{p} - \frac{1}{p}\sqrt{p|C||D|}p\sqrt{|A||B|} = \frac{|A||B||C||D|}{p} - \sqrt{p|A||B||C||D|}.$$

Így $N > 0$, ha $|A||B||C||D| > p^3$. $\square$

4. Következmény. *Ha $p > n^4$, akkor az $x^n + y^n \equiv z^n \pmod p$ egyenletnek létezik nem triviális megoldása.*

Valóban, az előző tétel miatt legyen $A = B = C = D = H = \{u^n : u \in \mathbb{F}_p\} < \mathbb{F}_p^*$ részcsoport.
Ekkor

$$|H| = \frac{p-1}{(n, p-1)}.$$

Tehát ha

$$\left(\frac{p-1}{(n,p-1)} \right)^4 > p^3,$$

akkor van megoldása az egyenletnek. Ha tehát

$$p > n^4 > \left(\frac{p-1}{(n,p-1)} \right)^4$$

akkor van megoldás ($p - 1 \sim p$ egyszerűsítéssel éltünk).

13.8. Waring típusú probléma prímtestekben

Mint láttuk (és többször használtuk is), ha $A, B \subseteq G$ véges csoport két részhalmazára teljesül, hogy $|A| + |B| > |G|$, akkor $A + B = G$. Ebből következik, hogy a kvadratikus maradékok $\cup\{0\}$ másodrendű bázist alkotnak. A $H =$kvadratikus maradékok $\mathbb{F}_p^*$ (multiplikatív) részcsoportját alkotják, így kérdezhető, hogy milyen $H = \{u^n : u \in \mathbb{F}_p\} < \mathbb{F}_p^*$ részcsoport lesz másodrendű bázis. Sokáig az volt az ismert legjobb eredmény, hogy ha $|H| > p^{3/4}$, akkor H másodrendű bázis. Erre két különböző megoldást is adunk.

13.8.1. Tétel. *Legyen $H < \mathbb{F}_p^*$, és $|H| > p^{3/4}$. Akkor bármely $a, b \in \mathbb{F}_p^*$ esetén*

$$aH + bH \supseteq \mathbb{F}_p^*.$$

Bizonyítás:
Tekintsük a következőt

$$\widehat{H}(ax)\widehat{H}(bx) = \sum_{h_1 \in H} e(ah_1x) \sum_{h_2 \in H} e(bh_2x) = \sum_{h_1,h_2 \in H} e((ah_1 + bh_2)x) =$$

$$= \sum_y r(y)e(yx) = \widehat{r}(x),$$

ahol

$$r(y) = \{(h_1, h_2) \in H^2 : ah_1 + bh_2 = y\}.$$

Így

$$\sum_{x \in \mathbb{F}_p^*} |\widehat{H}(ax)\widehat{H}(bx)|^2 = \sum_{x \in \mathbb{F}_p^*} |\widehat{r}(x)|^2 = p\sum_x r^2(x) - |\widehat{H}(0)|^4 = p\sum_x r^2(x) - |H|^4.$$

Több esetben használtuk a következő átalakítást: legyen $A \subseteq G$, legyen $r(x) = \{(a_1, a_2) \in A^2 : a_1 + a_2 = x\}$. Ekkor

$$|G|\sum_{x \in G} r^2(x) - |A|^4 = |G|\sum_{x \in G} \left(r(x) - \frac{|A|^2}{|G|}\right)^2.$$

Ezt használva

$$\sum_{x\in\mathbb{F}_p^*}|\widehat{H}(ax)\widehat{H}(bx)|^2 = p\sum_{x\in\mathbb{F}_p}\left(r(x)-\frac{|H|^2}{p}\right)^2.$$

Legyenek

$$H, x_1H, x_2H, \ldots, x_kH$$

a H szerinti mellékosztályok. Könnyű látni, hogy $\forall i$, és $\forall x, x' \in x_iH$ $r(x) = r(x')$. Továbbá a Parseval azonosság miatt

$$\sum_{x\in\mathbb{F}_p^*}|\widehat{H}(x)|^2 = \sum_{x\in\mathbb{F}_p}|\widehat{H}(x)|^2 - |H|^2 = p|H| - |H|^2.$$

Továbbá $\forall x, x' \in x_iH$, ha $x' = h_0x$, $h_0 \in H$,

$$\widehat{H}(x') = \sum_{h\in H}e(x'h) = \sum_{h\in H}e(xh_0h) = \sum_{h\in H}e(xh) = \widehat{H}(x),$$

ezért a mellékosztályok reprezentáló elemei szerint összeadva

$$p|H| - |H|^2 = \sum_{x\in\mathbb{F}_p^*}|\widehat{H}(x)|^2 = |H|\sum_{i=1}^{k}|\widehat{H}(x_i)|^2.$$

Ebből azt kapjuk, hogy $\forall x \in \mathbb{F}_p^*$

$$|\widehat{H}(x)|^2 \le p - |H|.$$

Mivel $r(x)$ azonos bármely mellékosztály elemein, ezért

$$p\sum_{x\in\mathbb{F}_p}\left(r(x)-\frac{|H|^2}{p}\right)^2 = p|H|\sum_{i=1}^{k}\left(r(x_i)-\frac{|H|^2}{p}\right)^2 = \sum_{x\in\mathbb{F}_p^*}|\widehat{H}(ax)\widehat{H}(bx)|^2 \le$$

$$\le \max_x|\widehat{H}(ax)|^2\sum_{x\in\mathbb{F}_p^*}|\widehat{H}(bx)|^2 \le (p-|H|)\sum_{x\in\mathbb{F}_p^*}|\widehat{H}(bx)|^2 =$$

$$= (p-|H|)(p|H|-|H|^2) = (p-|H|)^2|H|.$$

Így az előző második és utolsó tagjából

$$p\sum_{i=1}^{k}\left(r(x_i)-\frac{|H|^2}{p}\right)^2 \le (p-|H|)^2.$$

Ha most valamelyik mellékosztály elemei nem állnának elő, azaz $r(x_i) = 0$ lenne valamely $1 \leq i \leq k$ esetén, akkor

$$p\frac{|H|^4}{p^2} < (p - |H|)^2 < p^2$$

lenne és így

$$|H| < p^{3/4}$$

adódna ellentmondásként. □

A másik bizonyításban azt bizonyítjuk, hogy $H + H$ lefedi $\mathbb{F}_p$-t (nyilván itt is megmutathatnánk, hogy két tetszőleges H mellékosztálya is lefedi $\mathbb{F}_p$-t). Ezt a következő tételből vezetjük le:

13.8.2. Tétel. *Legyen* $H < \mathbb{F}_p^*$, $|H| > \sqrt{p}$. *Ekkor*

$$|H + H| \geq \frac{p}{1 + \frac{p^2}{|H|^3}}.$$

Valóban, használjuk a már többször említett feladatot multiplikatív formában: ha $A, B \subseteq G$, ahol G egy multiplikatív csoport és $|A| + |B| > |G|$, akkor $A \cdot B = G$.

Ha most $A = H + H$ és $B = H$, akkor $(H + H)H = H + H = G$, feltéve, hogy

$$\frac{p}{1 + \frac{p^2}{|H|^3}} + |H| > p,$$

ami teljesül, ha $|H| > p^{3/4}$. Ez adja tehát a második bizonyítást.

Bizonyítás:
Az additív energia

$$E_+(H) = \frac{1}{p}\sum_r |\widehat{H}(r)|^4 = \frac{1}{p}\sum_{a,b,c,d \in H}\sum_r e(r(a + b - c - d)) =$$

$$= \frac{|H|^4}{p} + \frac{1}{p}\sum_{a,b,c,d \in H}\sum_{r \neq 0} e(r(a + b - c - d)).$$

Lemma: *A H részcsoport $H(n)$ indikátorfüggvénye:*

$$H(n) = \frac{1}{d} \sum_{\chi:\chi^d=1} \chi(n),$$

ha $H = \{x^d : x \in \mathbb{F}_p^*\}$.

A bizonyítás egyszerű (ha n H-beli, akkor az összeg d, máskülönben 0). Ezért

$$\widehat{H}(r) = \sum_n H(n)e(rn) = \sum_n \frac{1}{d} \sum_{\chi:\chi^d=1} \chi(n)e(rn) =$$

$$= \frac{1}{d} \sum_{\chi:\chi^d=1} \overline{\chi}(r) \sum_n \chi(rn)e(rn).$$

Az összegben a $\sum_n \chi(rn)e(rn)$ egy Gauss-összeg, jelöljük $G(\chi)$-vel. Így

$$\widehat{H}(r) = \frac{1}{d} \sum_{\chi:\chi^d=1} \overline{\chi}(r)G(\chi).$$

Ezért $|\widehat{H}(r)| \leq \sqrt{p}$, mivel $|G(\chi)| \leq \sqrt{p}$ (és egyébként $\leq |H|$ minden esetben).

(Emlékezzünk, az előző bizonyításban Gauss-összegek említése nélkül is a $|\widehat{H}(x)|^2 \leq p - |H|$ becslést kaptuk).

Tehát

$$E_+(H) \leq \frac{|H|^4}{p} + \frac{1}{p} \sum_{r \neq 0} |\widehat{H}(r)|^4 \leq \frac{|H|^4}{p} + (\sqrt{p})^2 \frac{1}{p} \sum_{r \neq 0} |\widehat{H}(r)|^2 =$$

$$= \frac{|H|^4}{p} + p|H|.$$

Másfelől a Cauchy egyenlőtlenség miatt

$$\frac{|H|^4}{|H+H|} \leq E_+(H) \leq \frac{|H|^4}{p} + p|H|,$$

amiből átrendezéssel következik a tétel. □

A következő tétel egy reprezentációs kérdésre ad választ; egy szorzathalmaz mikor lesz harmadrendű bázis egy prímtestben.

13.8.3. Tétel. *Legyen $A \subseteq \mathbb{F}_p$ és tegyük fel, hogy $|A| > p^{3/4}$. Ekkor*

$$A \cdot A + A \cdot A + A \cdot A = \mathbb{F}_p.$$

Bizonyítás:

Nyilván elhagyhatjuk a 0 elemet, ha az benne van A-ban. Legyen $f(x) = \frac{1}{|A|} \sum_{y \in A} A(xy^{-1})$. Könnyű látni, hogy $f(x)$ pozitív vagy 0 aszerint, hogy $x \in AA$ vagy sem.

Írjuk fel f diszkrét Fourier transzformáltját $\widehat{f}(r) = \frac{1}{|A|} \sum_{y \in A} \widehat{A}(ry)$ és legyen $J_z := \frac{1}{p} \sum_r \widehat{f}(r)^3 e_p(-rz)$. A fent elmondottakból következik, hogy $z \in AA + AA + AA$, amennyiben $J_z > 0$.

Most a Cauchy egyenlőtlenség és a Parseval formula miatt

$$|\widehat{f}(r)| = \frac{1}{|A|} \sqrt{|A|} \sqrt{\sum_{y \in A} |\widehat{A}(ry)|^2} \leq$$

$$\leq \frac{1}{|A|} \sqrt{|A|} \sqrt{\sum_{y \in \mathbb{F}_p} |\widehat{A}(ry)|^2} = \sqrt{p}.$$

Ezt felhasználva J_z-t fogjuk becsülni: elkülönítve az $r = 0$ tagot

$$J_z = \frac{1}{p} \sum_r \widehat{f}(r)^3 e_p(-rz) = \frac{1}{p} \widehat{f}(0)^3 + \frac{1}{p} \sum_{r \neq 0} \widehat{f}(r)^3 e_p(-rz).$$

Itt $\widehat{f}(0) = \sum_x f(x) = |A|$, ezért

$$\Big| J_z - \frac{1}{p} |A|^3 \Big| \leq \Big| \frac{1}{p} \sum_{r \neq 0} \widehat{f}(r)^3 e_p(-rz) \Big| \leq$$

$$\leq \frac{1}{p} \sum_{r \neq 0} |\widehat{f}(r)^3| \leq \max_{r \neq 0} \frac{1}{p} |\widehat{f}(r)| \sum_{r \neq 0} |\widehat{f}(r)|^2 \leq \frac{1}{p} \sqrt{p} \Big(\sum_r |\widehat{f}(r)|^2 \Big) =$$

$$= \sqrt{p} \sum_x |f(x)|^2 \leq \sqrt{p} |A|.$$

megint a Parseval azonosságot, az $f(x) \leq 1$-et, és $\sum_x f(x) = |A|$ azonosságot használva. Átrendezve a becslést, azt kapjuk, hogy $J_z > 0$, ha $|A| > p^{3/4}$ bármely $z \in \mathbb{F}_p$ esetén. □

Most egy olyan tételt igazolunk, amelyben $\mathbb{F}_p^*$-beli részcsoportok eloszlását vizsgáljuk, megmutatva, hogy az csak a részcsoportok additív energiájától függ:

13.8.4. Tétel. *Legyen $H < \mathbb{F}_p^*$. Ekkor bármely $r \neq 0$ és $k \in \mathbb{N}$ esetén*

$$\left|\sum_{x\in H} e(rx)\right| \leq |H|^{1-1/k} p^{1/8k^2} \sqrt[4k^2]{E_{4k}(H)},$$

ahol $E_m(H) := \{(h_1, \dots, h_m, h'_1, \dots, h'_m\} : h_1 + \dots + h_m = h'_1 + \dots + h'_m\}$.

Bizonyítás: Lényegében azt használjuk ki, hogy $\forall y \in H$, $yH = H$.

$$S := \left|\sum_{x\in H} e(rx)\right| = \frac{1}{|H|} \sum_{y\in H} \left|\sum_{x\in H} e(rxy)\right|.$$

Most a Hölder egyenlőtlenséget az $\frac{1}{p} = 1 - \frac{1}{2k}$ és az $\frac{1}{q} = \frac{1}{2k}$ számokra használva

$$S \leq \frac{1}{|H|} \left(\sum_{y\in H} 1^{\frac{2k}{2k-1}}\right)^{1-\frac{1}{2k}} \left(\sum_{y\in H} \left|\sum_{x\in H} e(rxy)\right|^{2k}\right)^{\frac{1}{2k}} =$$

$$= |H|^{-\frac{1}{2k}} \left(\sum_{x_1,\dots,x_k,x'_1,\dots,x'_k,y} e(ry((x_1 + \dots + x_k) - (x'_1 + \dots + x_k)))\right)^{\frac{1}{2k}} \leq$$

és megint, ugyanazokkal a paraméterekkel a Hölder egyenlőtlenséget használva, csak most az összegzést a $2k$ számú x-re végezve és használva, hogy $\sum_{x_1,\dots,x_k,x'_1,\dots,x'_k\in H} 1 = |H|^{2k}$

$$\leq |H|^{-\frac{1}{2k}} \left(\sum_{x_1,\dots,x_k,x'_1,\dots,x'_k\in H} 1^{\frac{2k}{2k-1}}\right)^{(1-\frac{1}{2k})\frac{1}{2k}} \times$$

$$\left(\sum e(r((x_1 + \dots + x_k) - (x'_1 + \dots + x_k))((y_1 + \dots + y_k) - (y'_1 + \dots + y_k)))\right)^{\frac{1}{4k^2}} =$$

$$= |H|^{1-\frac{1}{k}} \times$$

$$\left(\sum e(r((x_1 + \dots + x_k) - (x'_1 + \dots + x_k))((y_1 + \dots + y_k) - (y'_1 + \dots + y_k)))\right)^{\frac{1}{4k^2}},$$

ahol $\sum = \sum_{x_1,\dots,x_k,x'_1,\dots,x'_k,y_1,\dots,y_k,y'_1,\dots,y'_k\in H}$. Tekintsük a

$$\sum e(r((x_1 + \dots + x_k) - (x'_1 + \dots + x_k))((y_1 + \dots + y_k) - (y'_1 + \dots + y_k)))$$

összeget. Legyen $z := (x_1 + \cdots + x_k) - (x'_1 + \cdots + x'_k)$ és $w = (y_1 + \cdots + y_k) - (y'_1 + \cdots + y_k)$. Ekkor a $R(z), R(w)$ reprezentációs függvényekkel felírva az összeget

$$\sum e(r((x_1 + \cdots + x_k) - (x'_1 + \cdots + x_k))((y_1 + \cdots + y_k) - (y'_1 + \cdots + y_k))) =$$

$$= \sum R(z)R(w)e(rzw).$$

Végül a Vinogradov egyenlőtlenséget használva

$$\sum R(z)R(w)e(rzw) \leq \sqrt{p \sum R^2(z) \sum R^2(w)}.$$

A $\sum R^2(z)$ azon $s_1, \ldots, s_k, s'_1, \ldots, s'_k, t_1, \ldots, t_k, t'_1, \ldots, t'_k$ $4k$-asokat számolja, amelyekre

$$(s_1 + \cdots + s_k) - (s'_1 + \cdots + s'_k) = (t_1 + \cdots + t_k) - (t'_1 + \cdots + t'_k),$$

amit átrendezve pozitív tagokra, éppen $E_{4k}(H)$-t kapjuk. Tehát

$$\sum e(r((x_1+\cdots+x_k)-(x'_1+\cdots+x_k))((y_1+\cdots+y_k)-(y'_1+\cdots+y_k))) \leq \sqrt{pE_{4k}(H)^2}.$$

Ezzel a becsléssel tehát

$$S \leq |H|^{1-\frac{1}{k}} \left(\sqrt{pE_{4k}(H)^2}\right)^{\frac{1}{4k^2}} = |H|^{1-1/k} p^{1/8k^2} \sqrt[4k^2]{E_{4k}(H)}. \quad \square$$

A következőkben egy speciális Waring típusú problémát tekintünk; megvizsgáljuk, hogy egy összeghalmaz milyen sokszor metsz bele a kvadratikus maradékok halmazába:

13.8.5. Tétel. *Legyen $A, B \subseteq \mathbb{F}_p$ és $k \in \mathbb{N}$. Jelölje $\mathcal{Q}$ a kvadratikus maradékok halmazát modulo p. Tegyük fel, hogy*

$$\frac{|A|}{|B|}(|B| - 2k + 1)^2 + |B| - 1 \geq p.$$

Ekkor létezik $q \in \mathcal{Q}$ melyre $r_{A,B}(q) \geq k$, más szóval létezik k számú $(a_i, b_i) \in A \times B;\ i = 1, 2, \ldots, k$ melyre

$$a_i + b_i = q;\ i = 1, 2, \ldots, k.$$

Bizonyítás:

Legyen χ egy kvadratikus karakter ($\chi(0)=0; \chi(x)=1$ ha x kvadratikus maradék és $\chi(x)=-1$ ha x kvadratikus nem-maradék) és legyen $a \in A$. Indirekt tegyük fel, hogy állításunk nem igaz. Elsőként belátjuk, hogy

$$\Big(\sum_{b\in B}\chi(a+b)\Big)^2 \geq (|B|-2k+1)^2.$$

Valóban $\chi(a+b)$ értékei között legfeljebb $k-1$ darab 1-es van, legfeljebb egy esetben 0, a többi -1.

20. Lemma. *Legyen $y \neq y'$, $y, y' \in \mathbb{F}_p$. Ekkor*

$$\sum_{x\in\mathbb{F}_p}\chi(x+y)\chi(x+y') = -1.$$

Bizonyítás:

Mivel $|\chi(x)|=1$, ($x\neq 0$), ezért azt kapjuk, hogy

$$\sum_{x\in\mathbb{F}_p}\chi(x+y)\chi(x+y') = \sum_{x\in\mathbb{F}_p}\chi\Big(\frac{x+y}{x+y'}\Big) = \sum_{x\in\mathbb{F}_p}\chi\Big(1+\frac{y-y'}{x+y'}\Big).$$

Továbbá vezessük be a $z = 1+\frac{y-y'}{x+y'}$ új változót, ekkor $x = \frac{y-y'z}{1-z}$, ezért amint x befutja $\mathbb{F}_p \setminus \{-y'\}$ elemeit, z is befutja $\mathbb{F}_p \setminus \{1\}$ elemeit.

Továbbá mivel $\sum_{x\in\mathbb{F}_p}\chi(x)=0$; és $\chi(1)=1$, adódik a lemma állítása. □

Most

$$\sum_{a\in A}\Big(\sum_{b\in B}\chi(a+b)\Big)^2 \leq \sum_{a\in\mathbb{F}_p}\Big(\sum_{b\in B}\chi(a+b)\Big)^2 =$$

$$= \sum_{a\in\mathbb{F}_p}|B| + \sum_{a\in\mathbb{F}_p}\sum_{b,b'\in B; b\neq b'}\chi(a+b)\chi(a+b') = p|B| - |B|(|B|-1)$$

használva a lemmát.

Végül összehasonlítva a $(\sum_{b\in B}\chi(a+b))^2$ összegre kapott alsó és felső becslést ellentmondásra jutunk a tétel feltételével. □

13.9. Kloosterman összeg, Weil tétel és következményei

Számos esetben olyan exponenciális összeggel van dolgunk, ahol a változó és annak multiplikatív inverze is szerepel (lásd az előző fejezet tételét).

Az ú.n. Kloosterman összeg a következő:

$$S(a,b,p) := \sum_{x \in \mathbb{F}_p^*} e(ax + bx^{-1}),$$

ahol $a, b \in \mathbb{F}_p^*$. Erre az összegre Kloostermannak a Lagrange tétel általánosításánál volt szüksége. A kérdés úgy hangzott; becsüljük meg az

$$\mathbb{R}(n) := \{n = ax^2 + by^2 + cz^2 + dw^2 : x, y, z, w \in \mathbb{Z}\}$$

($a, b, c, d \in \mathbb{N}$ fix) reprezentációs függvényt. Erre a Kloosterman összegre igaz, hogy

$$|S(a,b,p)| \leq 2\sqrt{p},$$

melyet először A. Weil igazolt (lásd később). Megjegyezzük, hogy összetett modulus esetén

$$|S(a,b,c)| = \left| \sum_{x \neq 0} \exp\left(\frac{ax + bx^{-1}}{c}\right) \right| \leq \tau(c)(a,b,c)^{1/2}\sqrt{c}$$

igaz.

A következő tételben egy gyengébb változatát igazoljuk a fenti becslésnek (amit eredetileg Kloosterman is igazolt):

13.9.1. Tétel.

$$|S(a,b,p)| \leq \sqrt[4]{3}p^{3/4}.$$

Bizonyítás:
Belátjuk, hogy $\forall m \in \mathbb{F}_p^*$

$$S(a,b,p) = S(a \cdot m, b \cdot \overline{m}, p),$$

ahol röviden $\overline{m} \in \mathbb{F}_p^*$ az az elem, melyre $m \cdot \overline{m} = 1$.

Ha x végigfut $\mathbb{F}_p^*$ elemein, akkor xm is végigfut ezeken az elemeken, így

$$S(a,b,p) = \sum_{x\in\mathbb{F}_p^*} e(a(mx) + b(\overline{mx})) = \sum_{x\in\mathbb{F}_p^*} e((am)x + (b\overline{m})\overline{x}) =$$

$$= S(a\cdot m, b\cdot \overline{m}, p).$$

Tekintsük most a

$$V := \sum_{a,b=0}^{p-1} |S(a,b,p)|^4$$

összeget. Az előbbiek miatt egy fix $|S(a,b,p)|^4$ a V összegben legalább $p-1$-szer szerepel, azaz

$$(p-1)\,|S(a,b,p)|^4 \le V.$$

Kifejtve V-t

$$V = \sum_{a,b=0}^{p-1} \sum_{n_1,n_2,n_3,n_4} e(a(n_1+n_2-n_3-n_4) + b(\overline{n_1}+\overline{n_2}-\overline{n_3}-\overline{n_4})) =$$

$$= \sum_{n_1,n_2,n_3,n_4} \sum_{a,b=0}^{p-1} e(aX+bY) = \sum_{n_1,n_2,n_3,n_4} \left(\sum_a e(aX)\right)\left(\sum_b e(bY)\right).$$

A $(\sum_a e(aX))$ tag vagy p vagy 0, hasonlóan a másik tag is p vagy 0. Ezért (az ortoganilitás miatt)

$$V = p^2\{(n_1,n_2,n_3,n_4) : p|n_1+n_2-n_3-n_4; p|\overline{n_1}+\overline{n_2}-\overline{n_3}-\overline{n_4}\}.$$

Ha

$$n_1+n_2 \equiv n_3+n_4 (mod p) \text{ és } \frac{1}{n_1}+\frac{1}{n_2} \equiv \frac{1}{n_3}+\frac{1}{n_4} \pmod p,$$

akkor

$$n_1n_2 \equiv n_3n_4 \pmod p$$

feltéve, hogy $n_1+n_2 \not\equiv 0 (mod p)$. Tehát az n_1, n_2 értéke egyértelműen meghatározza az n_3, n_4 értékét (permutáció erejéig). Így

$$V \le p^2 3(p-1)^2.$$

Tehát

$$(p-1)\,|S(a,b,p)|^4 \le V \le p^2 3(p-1)^2.$$

Ezt átrendezve a tétel állítását kapjuk. □

A következő fontos tétel Weiltől származik, amit bizonyítás nélkül közlünk:

13.9.2. Tétel. *Legyen a χ karakter rendje $d > 1$, f polinomnak m különböző gyöke és f nem teljes d-edik hatvány. Akkor*

$$\left| \sum_{x \in \mathbb{F}_p^*} \chi(f(x)) \right| \leq (m-1)\sqrt{p}.$$

E tételből levezetjük a következőt:

13.9.3. Tétel. *Legyen $\chi \neq \chi_0$, és legyen $b_1, b_2, \ldots, b_{2r} \in \mathbb{F}_p$, valamint $\exists i \neq j$, hogy $b_i \neq b_j$.*
Ekkor

$$\left| \sum_{x \in \mathbb{F}_p} \chi\left((x+b_1)(x+b_2)\ldots(x+b_r)\right) \overline{\chi}\left((x+b_{r+1})\ldots(x+b_{2r})\right) \right| \leq 2r\sqrt{p}.$$

Bizonyítás:

$$\chi\left((x+b_1)(x+b_2)\ldots(x+b_r)\right) \overline{\chi}\left((x+b_{r+1})\ldots(x+b_{2r})\right) = \chi(f(x)),$$

ahol a Fermat-tétel segítségével felírva

$$f(x) = \prod_{j=1}^{r}(x+b_j) \prod_{j=r+1}^{2r} (x+b_j)^{p-2}.$$

Tehát $f(x)$-nek van olyan gyöke, ami egyszeres, vagy $p-2$-szörös gyök. A karakter rendje $d > 1$, így $d|p-1$ és mivel $(1,d) = (p-2,d) = 1$, $f(x)$ nem teljes d-edik hatvány. □

Egy még általánosabb állítás is igaz (bizonyítás nélkül).

13.9.4. Tétel. *Legyenek $\chi_1, \chi_2, \ldots, \chi_m$ multiplikatív karakterek melyek közül legyen m_0 a triviális χ_0, továbbá legyenek $b_1, b_2, \ldots, b_m \in \mathbb{F}_p$ különböző elemek. Ekkor*

$$\left| \sum_{x \in \mathbb{F}_p} \chi_1(x+b_1)\chi_2(x+b_2)\ldots\chi_m(x+b_m) \right| \leq (m-m_0+1)\sqrt{p} + m_0 + 1.$$

E fenti tétel egy szép alkalmazása a következő állítás:

13.9.5. Tétel. *Legyenek $A, B \subseteq \mathbb{F}_p$ olyan halmazok, melyekre*

$$|A||B| > (3\sqrt{p}+1)^2.$$

Ekkor létezik $x, y \in \mathbb{F}_p$, melyekre

$$x+y \in A, \quad \text{és} \quad xy \in B.$$

Bizonyítás:

A bizonyításhoz fel fogjuk használni a multiplikatív karakterekre vonatkozó 13.2.1 tételt. Jelölje $f(x) = \sum_y A(x+y)B(xy)$, így

$$\widetilde{f}(r) = \sum_{x \in \mathbb{F}_p^*} f(x)\overline{\chi_r(x)} = \sum_{x,y \in \mathbb{F}_p^*} A(x+y)B(xy)\overline{\chi_r(x)}$$

és legyen $N := \{(x,y) : x+y \in A,\ xy \in B\}$. Célunk kimutatni, hogy N nem üres halmaz. Ekkor nyilván $N = \sum_x f(x) = \widetilde{f}(0)$. Vezessük be az $y = \lambda x$ változót, ekkor

$$\widetilde{f}(r) = \sum_{x,y \in \mathbb{F}_p^*} A(x(1+\lambda))B(\lambda x^2)\overline{\chi_r(x)}.$$

A 13.2.1 tétel inverziós formulája miatt

$$\widetilde{f}(r) = \frac{1}{(p-1)^2} \sum_{r_1, r_2} \widetilde{A}(r_1)\widetilde{B}(r_2) \sum_{\lambda, x} \chi_{r_1}(x(1+\lambda))\chi_{r_2}(\lambda x^2)\overline{\chi_r(x)}.$$

A karakterek multiplicitását, a $\chi_{r_2}(\lambda x^2) = \chi_{2r_2}(\lambda x)$, $\overline{\chi_r(x)} = \chi_{-r}(x)$ összefüggést, valamint hogy a karakterek is csoportot alkotnak kapjuk egyrészt, hogy

$$\sum_{r_1,r_2} \chi_{r_1}(x)\chi_{r_2}(x^2)\overline{\chi_r(x)} = \sum_{r_1} \chi_{r_1+2r_2-r}(x)$$

és ez utóbbi összeg $p-1$ akkor és csak akkor, ha $r_1 = r - 2r_2$, egyébként nulla.

Ezt felhasználva

$$\widetilde{f}(r) = \frac{1}{p-1}\sum_{r_2} \widetilde{A}(r-2r_2)\widetilde{B}(r_2)\sum_{\lambda} \chi_{r-2r_2}(1+\lambda)\chi_{r_2}(\lambda) =$$

elkülönítve az $r_2 = p-1$ értéket (és $\widetilde{X}(\cdot)$ $p-1$ szerinti periodicitása miatt)

$$\widetilde{f}(r) = \frac{1}{p-1}\widetilde{A}(r)|B|\sum_{\lambda} \chi_r(1+\lambda) +$$

$$+\frac{1}{p-1}\sum_{r_2\neq p-1} \widetilde{A}(r-2r_2)\widetilde{B}(r_2)\sum_{\lambda} \chi_{r-2r_2}(1+\lambda)\chi_{r_2}(\lambda).$$

Most a második tagra a 13.9.4 tételt $m=2$-re használva valamint a Cauchy egyenlőtlenség és a Parseval formula miatt

$$\Big|\frac{1}{p-1}\sum_{r_2\neq p-1} \widetilde{A}(r-2r_2)\widetilde{B}(r_2)\sum_{\lambda} \chi_{r-2r_2}(1+\lambda)\chi_{r_2}(\lambda)\Big| \leq$$

$$\leq \frac{1}{p-1}\Big(\sum_{r_2} |\widetilde{A}(r_2)|^2\Big)^{1/2}\Big|\Big(\sum_{r_2} |\widetilde{B}(r_2)|^2\Big)^{1/2} \cdot (3\sqrt{p}+1) =$$

$$\sqrt{|A||B|}(3\sqrt{p}+1).$$

Így

$$N = \widetilde{f}(0) \geq |A||B| - \sqrt{|A||B|}(3\sqrt{p}+1) > 0$$

feltéve, hogy

$$|A||B| > (3\sqrt{p}+1)^2. \quad \square$$

Feladatok

A "Bilineáris összegek" fejezetben két becslés szerepelt a nem triviális additív karakter összegre, (az $|A||B| < p$ és az $|A||B| \geq p$ méretétől függően) és egy tovább becslés a multiplikatív karakterösszegre, ugyancsak a "nagy halmazok" ($|A||B| \geq p$) esetére. Most kiegészítjük ez utóbbit az $|A||B| < p$ esetre.

1. Legyen $A, B \subseteq \mathbb{F}_p$, melyekre $0 < |A||B| < p$. Bizonyítsuk be, hogy ha $\chi \neq \chi_0$, akkor

$$S := \left| \sum_{a \in A; b \in B} \chi(a+b) \right| \leq |A|^{7/8} |B|^{7/8} p^{1/8}.$$

2. Bizonyítsuk be, hogy ha $A, B \subseteq \mathbb{F}_p$, akkor

$$\left| \sum_{a \in A; b \in B; a \neq b} e_p\left(\frac{1}{a-b}\right) \right| \leq 2\sqrt{p|A||B|}.$$

Megoldások

1. Használjuk a háromszög egyenlőtlenséget és a Hölder egyenlőtlenséget az $1/4 + 3/4 = 1$ választással:

$$S = \big| \sum_{a \in A; b \in B} \chi(a+b) \big| \leq |A|^{3/4} \left(\sum_{a \in A} \big| \sum_{b \in B} \chi(a+b) \big|^4 \right)^{1/4}.$$

Az $a-$ra való összegzést kiterjeszthejük az összes $r \in \mathbb{F}_p$ értékre (nem negatív tagú összegekről van szó) és kifejtük a $4-$dik hatványt

$$S \leq |A|^{3/4} \left(\sum_{b_1, b_2, b_3, b_4 \in B} \sum_{a \in \mathbb{F}_p a \neq b_i} \chi((a+b_1)(a+b_2)) \overline{\chi((a+b_3)(a+b_4))} \right)^{1/4}.$$

(Amikor $a = -b_i$ valamely b_i-vel, akkor $\chi(0) = 0$ miatt az a tag 0.)

Használva a fejezetben szereplő becslést a zárójelben levő összegre, kapjuk, hogy

$$S \leq |A|^{3/4} \left(|B|^4 \sqrt{p}\right)^{1/4} = |A|^{3/4}|B|p^{1/8}.$$

Az A és B szerepét felcserélve

$$S \leq |B|^{3/4}|A|p^{1/8}.$$

A két becslést összeszorozva és gyököt vonva kapjuk a feladat állítását.

2. Vegyük az

$$e_p\left(\frac{1}{a-b}\right) = \frac{1}{p}\sum_{x\in\mathbb{F}_p^*} e_p\left(\frac{1}{x}\right)\sum_{r\in\mathbb{F}_p} e_p(r(x-a+b))$$

azonosságot. Ekkor

$$\Big|\sum_{a\in A;b\in B;a\neq b} e_p\left(\frac{1}{a-b}\right)\Big| = \Big|\sum_{a\in A;b\in B;a\neq b}\frac{1}{p}\sum_{x\in\mathbb{F}_p^*} e_p\left(\frac{1}{x}\right)\sum_{r\in\mathbb{F}_p} e_p(r(x-a+b))\Big| \leq$$

$$\leq \frac{1}{p}\max_{r_0\neq 0}\Big|\sum_{x\in\mathbb{F}_p^*} e_p\left(\frac{1}{x}+r_0x\right)\Big|\Big|\sum_{r\in\mathbb{F}_p;a\in A;b\in B;a\neq b} e_p(-ra)e_p(rb)\Big| \leq$$

$$\leq \frac{1}{p}2\sqrt{p}\sqrt{\sum_{r\in\mathbb{F}_p^*}|\hat{A}(r)|^2}\sqrt{\sum_{r\in\mathbb{F}_p^*}|\hat{B}(r)|^2} = 2\sqrt{p|A||B|}$$

Használva a Kloosterman-összeg becslést, a Cauchy egyenlőtlenséget és a Parseval formulát.

13.10. Feltételes becslések prímtestekben

A legegyszerűbb ilyen feladat az ú.n. összeg-szorzat becslés. A következő tétel azonos a 11.3.7 tétellel, a bizonyításában itt exponenciális összeget hívunk segítségül.

13.10.1. Tétel. *Legyen $A \subseteq \mathbb{F}_p^*$. Ekkor*

$$|A+A||A\cdot A| \gg \min\left\{p|A|, \frac{|A|^4}{p}\right\}.$$

Bizonyítás:
Jelölje N az

$$x/a_1 + a_2 = y,$$

egyenlet megoldásainak a számát, ahol $x \in AA$, és $y \in A+A$. (Jegyezzük meg, hogy ez az ötlet hasonló ahhoz, amit a valós számokon vett összeg-szorzat problémánál használtunk. Ott is az $y = a(x-a')$ egyenletet vizsgáltuk, ahol $x \in A+A$ és $y \in AA$. Az egyenletet átrendezve a fentit kapjuk.)

Mivel bármely $a_1, a_2, a_3 \in A$ hármasra $x = a_1a_3, y = a_2 + a_3$ megoldása az egyenletnek, ezért

$$|A|^3 \leq N.$$

Továbbá a megoldások számát exponenciális összegként felírva

$$N = \frac{1}{p}\sum_{r\in\mathbb{F}_p}\sum_{x\in AA}\sum_{y\in A+A}\sum_{a_1,a_2\in A} e(r(x/a_1+a_2-y)).$$

Leválasztva az $r=0$ tagot, kapjuk, hogy

$$N = \frac{1}{p}|AA||A+A||A|^2 + \frac{1}{p}\sum_{r\neq 0}\sum_{x\in AA, a_1\in A} e(r(x\cdot a_1^{-1}))\sum_{y\in A+A, a_2\in A} e(r(a_2-y)).$$

Használjuk most a Vinogradov becslést a szorzatra és az utolsó két tagra a Cauchy egyenlőtlenséget és a Parseval-azonosságot

$$N \leq \frac{1}{p}|AA||A+A||A|^2 + \frac{1}{p}\max_{r\neq 0}\left|\sum_{x\in AA,a_1\in A} e(r(x\cdot a_1^{-1}))\right|\sum_{r\neq 0}\sum_{y\in A+A,a_2\in A} e(r(a_2-y)) \leq$$

$$\leq \frac{1}{p}|AA||A+A||A|^2 + \frac{1}{p}\sqrt{p|AA||A|}\sum_{r\in\mathbb{F}_p}\left|\sum_{a_2\in A} e(ra_2)\right|^2\sum_{r\in\mathbb{F}_p}\left|\sum_{y\in A+A} e(ry)\right|^2 =$$

$$= \frac{1}{p}|AA||A+A||A|^2 + \frac{1}{p}\sqrt{p^3|A|^2|AA||A+A|}$$

ahonnan átrendezéssel kapjuk a tételt $\square$.

7. Megjegyzés. *Az alábbiakban megmutatjuk, hogy a fenti tétel az* $|A| \gg p^{2/3}$ *esetén éles.*

Valóban az $|A| \gg p^{2/3}$ *esetén a tétel a* $\max\{|A+A|, |A\cdot A|\} \gg \sqrt{p|A|}$ *becslést adja.*

Legyen most $X = X_M := \{g^x : 1 \le x \le M\}$, g *egy primitív gyök* $\mathbb{F}_p^*-$*ben és legyen* $Y = Y_M := \{1, 2, \dots, M\}$. *Ekkor*

$$\{g^x : 1 \le x \le M\} \cap \{L+1, L+2, \dots, L+M\} = r_{X-Y}(L).$$

Mint láttuk

$$\sum_{L\in\mathbb{F}_p} r_{X-Y}(L) = M^2$$

így van olyan L, *hogy az*

$$A := \{g^x : 1 \le x \le M\} \cap \{L+1, L+2, \dots, L+M\}$$

halmazra $|A| \ge \frac{M^2}{p}$. *Erre az* A*-ra* $|A+A|, |A\cdot A| < 2M \le 2\sqrt{p|A|}$. □

Teljesen hasonló módon (az olvasóra bizva a bizonyítást) igazolható:

13.10.2. Tétel. *Legyen* $A, B, C \subseteq \mathbb{F}_p$, $0 \notin C$. *Ekkor*

$$|A+B||A\cdot C| \ge \min\left\{\frac{p|A|}{2}, \frac{|A|^2|B||C|}{4p}\right\}.$$

E tételek következménye:

13.10.3. Tétel. *Legyen* $H < \mathbb{F}_p^*$, *egy multiplikatív részcsoport. Ekkor*

$$|H+H| \ge \min\left\{\frac{p}{2}, \frac{|H|^3}{4p}\right\}.$$

Amiből a $|H| > 3p^{2/3}$ esetén teljesül, hogy $|H+H| > p/2$. Ekkor felhasználva az 1. fejezet 1./a feladatát – $|H+H| + |H+H| > p$ miatt – teljesül, hogy $H+H+H+H = \mathbb{F}_p$. (v.ö. a régebbi becslésekkel).

Egy további szép feltételes becslés a következő:

13.10.4. Tétel. *Legyen* $A, B, C, D \subseteq \mathbb{F}_p$, $0 \notin A, C$. *Legyen*

$$S = |A+B||C+D||B||D|.$$

a.) Ha $S < 4p^3$, *akkor*

$$|A+B||C+D||A \cdot C|^2 \geq \frac{|A|^2|B||C|^2|D|}{16p}.$$

b.) Ha $S \geq 4p^3$, *akkor*

$$|A+B||C+D||A \cdot C| \geq p|A||C|.$$

Úgy is fogalmazhatunk, hogy

$$|A+B||C+D||A \cdot C| \geq \min\left\{\frac{p}{2}|A \cdot C|, \frac{|A|^2|C|^2}{|A \cdot C|}, \frac{|B||D|}{4p}\right\}.$$

Bizonyítás:

Jelölje $r_{AC}(m)$ az $m = ac$ alakban való előállítási számát. Ekkor az átlagolás szerint van olyan m, hogy

$$r_{AC}(m) \geq \frac{|A||C|}{|AC|}.$$

Legyen

$$Z := \{(u,v) \in (A+B)\times(C+D); (b,d) \in B\times D : \text{ melyre } (u-b)(v-d) = m\}.$$

Az

$$(u-b)(v-d) = m$$

egyenletnek bármely $b \in B; d \in D$ esetén nyilván megoldása a

$$(u-b)(v-d) = ((a+b)-b)((c+d)-d) = m,$$

ezért a Z-beli egyenletnek a megoldásszáma

$$\geq |B||D|r_{AC}(m) \geq |B||D|\frac{|A||C|}{|AC|}.$$

Írjuk m-et $m = x \cdot y$ alakban, továbbá legyen $U = A + B; V = C + D$; és jelöljük u-val és v-vel az U és V elemeit, akkor a megoldásszám

$$J = \sum_{b,d,u,v} \sum_{m=x\cdot y} \frac{1}{p} \sum_{r\in\mathbb{F}_p} e(r(u-b-x)) \frac{1}{p} \sum_{t\in\mathbb{F}_p} e(t(v-d-y)).$$

A szokásos jelöléssel

$$J = \frac{1}{p^2} \sum_{r,t\in\mathbb{F}_p} \widehat{U}(r)\widehat{B}(-r)\widehat{V}(t)\widehat{D}(-t) \sum_{m=x\cdot y} e(-rx)e(-ty).$$

Az $r = t = 0$ esetben a fenti összegben – mivel $m = x \cdot y$ egyenletnek $p - 1$ megoldása van és $\widehat{X}(0) = |X|$ – ezért tehát az $r = t = 0$ taghoz tartozó érték

$$\frac{p-1}{p^2}|U||V||B||D|.$$

Ha $t = 0$ de $r \neq 0$, akkor az utolsó szumma $= -1$ (a teljes összeg $=0$, de hiányzik a 0 tag) tehát így az $r \neq 0$ tagokra összegezve a következőt kapjuk:

$$\frac{1}{p^2}|V||D| \left(\sum_{r\neq 0} \widehat{U}(r)\widehat{B}(r)(-1) \right).$$

Most

$$\sum_{r\neq 0} \widehat{U}(r)\widehat{B}(r)(-1) = (-1) \left(\sum_{r} \widehat{U}(r)\widehat{B}(r) - \widehat{U}(0)\widehat{B}(0) \right) =$$

$$= (-1) \left(\sum_{r} \widehat{U}(r)\widehat{B}(r) - |U||B| \right).$$

Használjuk a Plancherel formulát. Ekkor

$$\sum_{r} \widehat{U}(r)\widehat{B}(r) = p \sum_{x} U(x)B(x) = p|U \cap B|,$$

ezért a $t = 0$ de $r \neq 0$ esetén az összegünk

$$\frac{1}{p^2}|V||D|(|U||B| - p|U \cap B|) < \frac{1}{p^2}|V||D||U||B|$$

lesz. Hasonló a helyzet, ha $r = 0$ de $t \neq 0$.

Végül, amikor $r, t \neq 0$, akkor az utolsó tag egy Kloosterman összeg ami következő:

$$S(a, b, p) := \sum_{x \in \mathbb{F}_p^*} e(ax + bx^{-1}),$$

ahol $a, b \in \mathbb{F}_p^*$. Ezen összegre ismert az $|S(a, b, p)| \leq 2\sqrt{p}$ becslés.

Így az utolsó tag abszolút értékben legfeljebb $2\sqrt{p}$. Így ebben az esetben becsülhetünk így

$$\frac{2\sqrt{p}}{p^2} \sum_{r \neq 0} \left|\widehat{U}(r)\widehat{B}(r)\right| \sum_{t \neq 0} \left|\widehat{V}(r)\widehat{D}(r)\right|,$$

négyzetre emelve és használva a Cauchy egyenlőtlenséget

$$\frac{4}{p^3} \sum_r \left|\widehat{U}(r)\right|^2 \sum_r \left|\widehat{B}(r)\right| \sum_t \left|\widehat{V}(r)\right|^2 \sum_t \left|\widehat{D}(r)\right| =$$

$$= 4p|U||B||V||D|.$$

Összegezve a fentieket azt kapjuk, hogy

$$\frac{|A||B||C||D|}{|AC|} \leq \frac{p - 1 + 2}{p^2}|U||B||V||D| + 2\sqrt{p|U||B||V||D|}.$$

Ebből következik a tételbeli állítás □.

Egy további feltételes tétel a következő

13.10.5. Tétel. *Legyen $A, B, C, D \subseteq \mathbb{F}_p^*$. Ekkor*

$$|A + B||A/C||C + D| \geq \min\left\{\frac{|A|^2|C|^2|B||D|}{2p}, \frac{p}{2}|A||C|\right\}.$$

Bizonyítás:

Jelölje J azon $\{(u, b, m, v, d) \in (A + B) \times B \times (A/C) \times (C + D) \times D\}$ ötösök halmazának a számát, amelyekre

$$(u - b) = m(v - d).$$

Most bármely $a, b, c, d \in A \times B \times C \times D$ négyesre

$$(a + b - b) = (a/c)(c + d - d)$$

megoldása a fenti egyenletnek, így

$$J \geq |A||B||C||D|.$$

Másfelől exponenciális összegként felírva a megoldásszámot

$$J = \frac{1}{p} \sum_r \sum_{u,b,m,v,d} e(r(u - b - m(v - d))) = \frac{1}{p}|A + B||B||A/C||C + D||D| +$$

$$+\frac{1}{p} \sum_{r \neq 0} \sum_{u,b,m,v,d} e(r(u - b - m(v - d)))$$

Az $r \neq 0$ tagra a Vinogradov- és Cauchy egyenlőtlenségeket használva kapjuk, hogy

$$|A||B||C||D| \leq J \leq \frac{1}{p}|A + B||B||A/C||C + D||D| +$$

$$+\sqrt{p|A/C||C + D - D|} \cdot \frac{1}{p}\sqrt{p|A + B|p|B|}.$$

Innen átrendezéssel – felhasználva, hogy $|C + D - D| \leq |C + D||D|$ – adódik a tétel. □

A következő hasonló tétel Garaevtől származik:

13.10.6. Tétel. *Legyen* $A, B, C \subseteq \mathbb{F}_p^*$. *Ekkor*

$$|AB||(A + 1)C| \geq \min\left\{\frac{|A|^2|C||B|}{2p}, \frac{p}{2}|A|\right\}.$$

E tétel következménye:

5. Következmény.

$$|A(A+1)| \geq \min\left\{\sqrt{p|A|/2}, \frac{|A|^2}{2\sqrt{p}}\right\};$$

így, ha $|A| \gg p^{2/3}$, *akkor*

$$|A(A+1)| \gg \sqrt{p|A|},$$

azaz, ha

$$|A| > cp^{\frac{2}{2+\beta}},$$

$(c > 0,\ 0 < \beta < 1)$, *akkor az*

$$f(x,y) = xy + x$$

függvényre

$$|f(A,A)| > c'|A|^{1+\beta'}$$

$(c' = c'(c) > 0)$*; ahol* $\beta' = \frac{\beta}{2(\beta+2)}$. *Másszóval* f *függvény az adott méretű halmazokra egy expander.*

Bizonyítás:

A bizonyítás során szükségünk lesz a Vinogradov egyenlőtlenség multiplikatív karakterekre vonatkozó tételére az alábbi formában:

21. Lemma. *Legyen* $X, Y \subseteq \mathbb{F}_p^*$, $\chi \neq \chi_0$ *és* $k \in \mathbb{F}_p^*$ *egy tetszőleges elem. Ekkor*

$$S := \left|\sum_{x,y} \chi(xy+k)\right| \leq \sqrt{2p|X||Y|}.$$

A lemma bizonyításánál a 13.4.4. tétel bizonyításának az ötletét használjuk fel:

A Cauchy egyenlőtlenség miatt

$$S^2 \leq |X| \sum_x \sum_{y_1,y_2} \chi\Big(\frac{xy_1+k}{xy_2+k}\Big) = |X| \sum_x \sum_{y_1,y_2} \chi\Big(1 + \frac{x(y_1-y_2)}{xy_2+k}\Big).$$

Az x értékeit kiterjesztve az összes elemre, az $y_1 = y_2$ esetén e fenti összeg $\leq |X||Y|(p-1)$. Vezessük be a $z = 1 + \frac{x(y_1-y_2)}{xy_2+k}$ változót. Amint x befutja

az összes értéket, addig z is befutja az összes $z \neq 1$ értéket. Így, mint már láttuk

$$\Big|\sum_x \sum_{y_1,y_2} \chi\Big(1+\frac{x(y_1-y_2)}{xy_2+k}\Big)\Big| \leq |Y|^2 \leq |Y|p.$$

Tehát S^2-re kapjuk becslésként

$$S^2 \leq |X||Y|(p-1)+|Y|^2 \leq 2|X||Y|p. \quad \square$$

A tétel bizonyítása hasonló lesz az eddigiekhez. Jelölje J az

$$\frac{y}{x}\left(\frac{t}{z}-1\right)=1$$

egyenlet megoldásainak a számát, ahol $x \in AB$, $y \in B$, $z \in C$ és $t \in (A+1)C$. Ekkor minden a, b, c esetén

$$\frac{b}{ab}\left(\frac{(a+1)c}{c}-1\right)=1$$

megoldás, tehát

$$|A||B||C| \leq J.$$

A megoldásszámot multiplikatív karakterekkel felírva (ne feledjük, hogy $|\mathbb{F}_p^*| = p-1$)

$$J=\frac{1}{p-1}\sum_{\chi}\sum_{x,y,z,t}\chi(x^{-1}y(z^{-1}t-1))=\frac{|AB||B||C||(A+1)C|}{p}+$$

$$+\frac{1}{p-1}\sum_{\chi\neq\chi_0}\sum_{x,y,z,t}\chi(x^{-1}y(z^{-1}t-1)).$$

Most

$$\frac{1}{p-1}\sum_{\chi\neq\chi_0}\sum_{x,y,z,t}\chi(x^{-1}y(z^{-1}t-1)) \leq \frac{1}{p-1}\max\{\chi(z^{-1}t-1))\}\sum_{\chi\neq\chi_0}\sum_{x,y,z,t}\chi(x^{-1})\chi(y)$$

Mivel $\max\{\chi(z^{-1}t-1)) \leq \sqrt{p|C||(A+1)C|}$ a Vinogradov egyenlőtlenség miatt, továbbá alkalmazva a háromszög- és Cauchy egyenlőtlenségeket a

$\sum_{\chi=\chi_0}\sum_{x,y,z,t}\chi(x^{-1})\chi(y)$ tagra –kiterjesztve a χ_0-ra is és mivel $p/(p-1)<1$ kapjuk, hogy

$$|A||B||C| \leq J \leq \frac{|AB||B||C||(A+1)C|}{p}+$$

$$+\sqrt{p|C||(A+1)C||AB||B|},$$

amiből átrendezéssel a tétel adódik. □

13.10.7. Tétel. *Legyen $A,B,C\subseteq\mathbb{F}_p$, akkor a multiplikatív energiára kapjuk, hogy*

$$E_\times(A,B)\leq \max\left\{\frac{|A+C||B|}{|C|}p;\frac{|A||B|^2|A+C|}{p}\right\}$$

Bizonyítás
Tekintsük az

$$abb_1^{-1}+c=x \quad a\in A;\ b,b_1\in B;\ c\in C;\ x\in A+C$$

egyenlet megoldásait. Az olyan négyesre, melyre $ab=a_1b_1$ azt kapjuk, hogy $x=a_1+c$ megoldás. Tehát $J-$vel jelölve a megoldásszámot szabadon választhatjuk a négyeseket és $c-$t. Tehát $J\geq E_\times(A,B)|C|$. Másfelől exponenciális összeget véve:

$$J=\frac{1}{p}\sum_r\sum_{a,b,b_1,c,x}e(r(abb_1^{-1}+c-x)).$$

Az $r=0-$hoz tartozó értéket elkülönítve

$$J=\frac{|A||B|^2|C||A+C|}{p}+\frac{1}{p}\sum_{r\neq 0}\sum_{a,b,b_1,c,x}e(r(abb_1^{-1}+c-x)),$$

Legyen

$$W=\max_{r\neq 0}\Big|\sum_{a,b,b_1}e(rabb_1^{-1})\Big|.$$

Ekkor a Cauchy egyenlőtlenséget és a Parseval azonosságot felhasználva

$$J\leq\frac{|A||B|^2|C||A+C|}{p}+W\frac{1}{p}\sum_{r\neq 0}\sum_{a,b,b_1,c,x}e(r(c-x))\leq$$

$$\leq \frac{|A||B|^2|C||A+C|}{p} + W\sqrt{|C||A+C|}.$$

A W becsléséhez emeljünk négyzetre és megint felhasználva a Cauchy egyenlőtlenséget a következő becslést kapjuk

$$W^2 \leq |B| \sum_b \Big| \sum_{a,b_1} e_p(rabb_1^{-1})\Big|^2 \leq$$

$$\leq |B| \sum_{r\in\mathbb{F}_p} \Big| \sum_{a,b_1,a',b_1'} e_p(rb(ab_1^{-1} - a'b_1^{'-1}))\Big|.$$

A fenti szumma nulla, kivéve azokra a négyesekre, amelyekre $ab_1^{-1} - a'b_1^{'-1} = 0$, amelyek száma éppen $E_\times(A,B)$. Vagyis az ortogonalitás miatt

$$W^2 \leq |B|pE_\times(A,B).$$

E becslést felhasználva kapjuk a becslést. □

Feladat

1. Igazoljuk, hogy bármely $A, B, C \subseteq \mathbb{F}_p^*$ halmazokra

$$|A+B|\Big|\frac{1}{A} + C\Big| \gg \min\Big\{p|A|, \frac{|A|^2|B||C|}{p}\Big\}.$$

Megoldások

1. Kövessük az e fejezetben megismert utat: keressük az

$$\frac{1}{u-b} + c = y;\ u \in A+B;\ c \in C;\ y \in \frac{1}{A} + C$$

egyenlet megoldásait. Ha ebben az egyenletben u-t $a+b$-nek választjuk, nyilván kapunk egy megoldást. A megoldások számát N-nel jelölve, tehát $N \geq |A||B||C|$. Másrészt felírva N-re a szokásos exponenciális összeget

$$N = \frac{1}{p}\sum_{r\in\mathbb{F}_p}\sum_{u,c,y} e_p\Big(r(\frac{1}{u-b} + c - y)\Big).$$

Elkülönítve az $r = 0$ tagot és használva 13.9 pont 2. feladatát, (azaz, hogy $\max_{r\neq 0} |e_p(\frac{r}{u-b})| \ll \sqrt{p|A+B||B|}$) adódik az

$$|A||B||C| \leq N \ll \frac{1}{p}|A+B||B||C||1/A+C| + \sqrt{p|A+B||B||C||1/A+C|}$$

becslés, és ebből a feladat állítása.

13.11. Roth tétele véges test feletti vektortérben

Erdős és Turán nevezetes sejtése volt (a van der Waerden tétel kapcsán), hogy az egész számok egy pozitív felső sűrűségű részhalmazában mindig található egy nem triviális $a, a+d, a+2d, \ldots, a+kd;\ d \neq 0$ számtani sorozat. E sejtést – egy kicsit erősebb formában – a múlt század ötvenes éveiben $k = 2$ esetén K.F. Roth bizonyította be.

Ebben a részben megmutatjuk, hogy véges test feletti vektortérben – egy jóval erősebb formában, mint az egész számok halmazában – igaz az állítás. Jelölje röviden $\mathbb{F} := \mathbb{F}_p{}^n$, ahol p egy kettőnél nagyobb prímszám. Nyilván $|\mathbb{F}| = p^n := N$. Bizonyítjuk a következő tételt:

13.11.1. Tétel. *Ha $A \subseteq \mathbb{F}$ és*

$$|A| > (8 \log p)\frac{N}{\log N},$$

akkor A tartalmaz egy nem triviális háromtagú számtani sorozatot.

Bizonyítás:
Legyen $|A| = \alpha N$, és mondjuk azt, hogy A η-egyenletes, ha $\forall r \neq 0$, esetén

$$|\widehat{A}(r)| \leq \eta N.$$

22. Lemma. *Ha A η-egyenletes, akkor*

$$M := |\{(a,b,c) : a+b=2c\}| \geq (\alpha^3 - \alpha\cdot\eta)N^2.$$

6. Következmény. *Ha $(\alpha^3 - \alpha\cdot\eta)N^2 > \alpha N$, akkor $A-$ban van egy nem triviális háromtagú számtani sorozat. Ez teljesül ha*

$$\alpha^2 - \eta > \frac{1}{N},$$

így pl. ha $\eta = \frac{\alpha^2}{2}$, akkor $N > \frac{2}{\alpha^2}$ feltételt kell teljesíteni, amiről később kiderül, hogy igaz, ha N elég nagy.

A lemma bizonyítása: Az M megoldásszámot felírjuk a már ismert módon:

$$M = \frac{1}{N}\sum_r \widehat{A}^2(r)\widehat{A}(-2r) = \frac{1}{N}|A|^3 + \frac{1}{N}\sum_{r\neq 0}\widehat{A}^2(r)\widehat{A}(-2r) \geq$$

$$\geq \frac{1}{N}|A|^3 - \frac{1}{N}\max_{r\neq 0}|\widehat{A}(-2r)|\sum_{r\neq 0}|\widehat{A}^2(r)| \geq$$

az η-egyenletességet és a Parseval formulát felhasználva

$$\geq \alpha^3 N^2 - \eta N \alpha N = (\alpha^3 - \alpha\cdot\eta)N^2. \quad \square$$

Látható, hogy az η-egyenletesség (a paraméterek alkalmas beállításával) maga után vonja a háromtagú számtani sorozat létezését. A tétel hátralevő részében tehát olyan halmazokkal kell foglalkozni, amelyek nem egyenletesek.

Ha A nem η-egyenletes, akkor van olyan $r_0 \neq 0$, hogy

$$|\widehat{A}(r_0)| > \eta N.$$

Legyen $H := \langle r_0\rangle^{\perp}$, az r_0-ra merőleges altér $\mathbb{F}$-ben. Nyilván $|H| = p^{n-1}$.

Jelölje $H(x) = H + x$ mellékosztályt (a□n alteret) és legyen $h(x) = \frac{H(x)}{|H|}$.

23. Lemma. *Az $A * h(x)$ A-nak $H(x)$ beli sűrűsége, továbbá*

$$\max_x |A * h(x)| \geq \alpha + \frac{\eta}{2}.$$

A lemma bizonyítása:

Valóban

$$|A * h(x)| = \frac{1}{|H|}|\{(-h, a) : x = -h + a, \Leftrightarrow a = x + h \in H(x)\}|,$$

ami valóban A halmaz $H(x)$-beli sűrűsége.

Mivel $|H| = p^{n-1}$, ezért alkalmas i elemekre $i = 0, 1, \ldots p-1$

$$\bigcup_i H(i) = \mathbb{F}.$$

Most

$$\widehat{A}(r_0) = \sum_x A(x)e(r_0^T x) = \sum_{x\in\mathbb{F}, h\in H} \sum_{j=1}^{p} A(x)e(r_0^T(j+h)) =$$

mivel $r_0 \perp H$, így $r_0^T h = 0$,

$$= \sum_j |A \cap H(j)|e(r_0^T j) =$$

felhasználva, hogy $\sum_j e(r_0^T j) = 0$, ezért a fenti úgy is írható, mint

$$= \sum_j (|A \cap H(j)| - \alpha|H(j)|)e(r_0^T j) = \sum_j d_j e(r_0^T j),$$

ahol $d_j = (|A \cap H(j)| - \alpha|H(j)|)$. Mivel $|A| = \alpha N$, ezért $\sum_j d_j = 0$, továbbá

$$\sum |d_j| \geq |\widehat{A}(r_0)| \geq \eta N,$$

így

$$\sum_j (|d_j| + d_j) \geq \eta N.$$

Ezért az átlag miatt van olyan j, hogy

$$|d_j| + d_j \geq \frac{\eta N}{p} = \eta |H|$$

és így

$$d_j = |A \cap H(j)| - \alpha |H(j)| \geq \frac{\eta |H|}{2},$$

amiből

$$|A \cap H(j)| \geq \left(\alpha + \frac{\eta}{2}\right) |H|. \quad \square$$

Azaz: a sorozat vagy η-egyenletes valamilyen alkalmas η-ra, vagy van olyan a□n altér, ahol a halmaz sűrűbb, mint az eredeti vektortérben.

A bizonyítást egy iterációval folytatjuk:

Legyen

$$A_0 = A \qquad H_0 = \mathbb{F} \qquad \alpha_0 = \alpha.$$

Tegyük fel, hogy valamely $i \geq 0-$ra az $A_0, \ldots, A_i$ $H_0, \ldots, H_i$ halmazokat és $\alpha_0, \ldots, \alpha_i$ értékeket definiáltuk.

Most A_i **vagy** $\eta_i = \frac{\alpha_i^2}{2}$ egyenletes, **vagy** van egy $H_{i+1} < H_i$ altér (H_i-ben), és $x \in H_i$, melyekre

$$|A_i \cap (x + H_{i+1})| \geq \left(\alpha_i + \frac{\alpha_i^2}{2}\right) |H_{i+1}|.$$

Legyen

$$A_{i+1} := (A_i - x) \cap H_{i+1}; \quad \alpha_{i+1} := \alpha_i + \frac{\alpha_i^2}{2}.$$

Ekkor tehát

$$|A_{i+1}| \geq \alpha_{i+1} |H_{i+1}|.$$

Vegyük észre, hogy

$$\alpha_1 \geq \alpha + \frac{\alpha^2}{4} = \alpha(1 + \alpha/4); \quad \alpha_2 \geq \alpha(1 + \alpha/4) + \frac{\alpha^2 (1 + \alpha/4)^2}{4} \geq$$

$$\geq \alpha(1 + \alpha/4)^2.$$

Indukcióval belátható, hogy minden $k \geq 0$ esetén

$$\alpha_k \geq \alpha(1 + \alpha/4)^k.$$

Végül definiáljuk a $k_1, k_2, \ldots$ sorozatot így: Ha $k_1 > \frac{4}{\alpha}$, akkor $\alpha_{k_1} > 2\alpha$, ha $k_2 > \frac{4}{2\alpha}$, akkor $\alpha_{k_2} > 4\alpha$, így általában

$$k_t > \frac{4}{2^{t-1}\alpha} \Rightarrow \alpha_{k_t} > 2^t\alpha \geq 1,$$

ha $t > \log 1/\alpha$.

Az iteráció hossza

$$\frac{4}{\alpha} + \frac{4}{2\alpha} + \ldots \frac{4}{2^{t-1}\alpha} < \frac{4}{\alpha} \cdot 2 = \frac{8}{\alpha}.$$

Minden iterációs lépésben az új altér a régi altér elemszámának a p-ed része, tehát, hogy az iteráció működjön kell, hogy

$$N = p^n > p^{\frac{8}{\alpha}},$$

amiből

$$\alpha > \frac{8 \log p}{\log N}$$

azaz, ha α ilyen, akkor vagy a sűrűség 1, vagy az A egyenletes, bizonyítva az állítást. □

8. Megjegyzés. *A fenti becslésnél mostanában élesebb eredményeket is nyertek*

13.12. Számtani sorozatok összeghalmazokban

Szemerédi tétele után elég természetes kérdés, hogy vajon egy összeghalmazban milyen hosszú számtani sorozat lesz?

Erre vonatkozik a következő tétel:

13.12.1. Tétel. *Legyen $0 < \gamma < 1$, és legyen $A \subseteq \mathbb{Z}_N$, melyre $|A| = \gamma N$. Legyen $m \geq 3$, akkor az A $m-$szeres összeghalmaza tartalmaz "sok" $J-$tagú számtani sorozatokat, azaz léteznek*

$$\{a_i + d_i j\}_{j=0}^{J-1} \subseteq mA,$$

ahol $i = 1, 2, \ldots, \lfloor \gamma N/2 \rfloor$ és $J = c_1 N^{c_2}$.

Az állítás $m \geq 3$-tól igaz. A helyzet – mint lenni szokott – $m = 2$ esetén lényegesen más és annak bizonyítása is komplikáltabb.

Bizonyítás:

Most is exponenciális összeg segítségével történik a bizonyítás. Várható, hogy ott kell keresni a számtani sorozat elemeit, ahol a DFT értéke "nagy". Legyen tehát

$$U := \{r : |\widehat{A}(r)| > \delta N\},$$

ahol $0 < \delta < 1$ egy később meghatározandó konstans. Könnyű látni, hogy U-nak nincs sok eleme, csak a paraméterektől függ.

A Parseval formulát és U definícióját használva

$$|U| \cdot \delta^2 N^2 < \sum_r |\widehat{A}(r)|^2 = \gamma N^2,$$

amiből

$$|U| < \frac{\gamma}{\delta^2}.$$

Nyilván $0 \in U$, ha $\delta < \gamma$.

Ahogy már előbb is

$$R(y) = \sum_r (\widehat{A}(r))^m e(-ry)$$

megadja az N-szeresét annak, hogy az $y = a_1 + \cdots + a_m$ egyenletnek hány megoldása van.

Ezt az R függvényt két részre bontjuk; az egyikben azokra az r-ekre összegzünk, melyek U-ban vannak, a többiekre a másikban. Azaz legyen

$$R(y) = S(y) + T(y) = \sum_{r \in U} + \sum_{r \notin U}.$$

($S(y)$-ban keressük a számtani sorozat elemeit.)

Felső becsléseket adunk $|S(y)|$ és $|T(y)|$ értékeire:

$$|S(y)| \leq \sum_{r \in U} |\widehat{A}(r)|^m \leq |\widehat{A}(r)|^{m-2} \sum_r |\widehat{A}(r)|^2 \leq *$$

(láthatóan itt használjuk az $m \geq 3$ feltételt; ki tudtuk emelni az $m-2-$edik hatványt) használva, hogy $|\widehat{A}(r)| \leq |\widehat{A}(0)|$ és a Parseval formulát

$$* \leq |\widehat{A}(0)|^{m-2} \sum_r |\widehat{A}(r)^m|^2 = (\gamma N)^{m-2} \gamma N^2 = (\gamma N)^{m-1} N = (\gamma)^{m-1} N^m.$$

Továbbá

$$|T(y)| \leq \sum_{r \notin U} |\widehat{A}(r)|^m \leq |\widehat{A}(r)|^{m-2} \sum_r |\widehat{A}(r)|^2 \leq \delta^{m-2} \gamma N^m.$$

Az $S(y)$ "átlaga" az ortogonalitást felhasználva

$$\sum_y S(y) = \sum_{r \in U} |\widehat{A}(r)|^m \sum_y e(-ry) = |\widehat{A}(0)|^{m+1},$$

így

$$\sum_y S(y) = \gamma^m N^{m+1}.$$

Tekintsük azt a halmazt, melyekbe azokat az y-okat gyűjtjük, amelyekre $S(y)$ az "átlag" felénél nagyobb:

$$W := \left\{ y \in \mathbb{Z}_N : |S(y)| > \frac{\gamma^m N^m}{2} \right\}.$$

Mivel

$$\gamma^m N^{m+1} = \sum_y S(y) \leq \sum_{y \in W} |S(y)| + \sum_{y \notin W} |S(y)| \leq$$

használva az $|S(y)|-$ra kapott becslést

$$\leq |W| \gamma^{m-1} N^m + (N - |W|) \frac{\gamma^m N^m}{2},$$

amiből

$$\frac{\gamma N}{2} < |W|.$$

A keresett számtani sorozat első tagját $W-$ből választjuk. Tehát valamely $y \in W$, mellett keresünk egy

$$y, y+d, \ldots, y+Jd$$

számtani sorozatot. Ehhez választunk két olyan α, β paramétert, melyekre

$$\alpha + \beta = \frac{1}{2} \qquad |S(y) - S(y+jd)| < \alpha\gamma^m N^m \qquad |T(y+jd)| < \beta\gamma^m N^m$$

teljesül $j = 1, 2, \ldots, J$ esetén.

Keresnünk kell tehát jó $d-$t és "nagy" $J-$t.

Előtte azonban megmutatjuk, hogy e három feltétel már biztosítja $y, y+d, \ldots, y+Jd$ létezését.

Indirekten, ha valamely $0 \leq j \leq J$ esetén

$$0 = |R(y+jd)| = |S(y+jd) + T(y+jd)|$$

lenne, akkor

$$\beta\gamma^m N^m > |T(y+jd)| = |S(y+jd)| \geq$$

a háromszög egyenlőtlenség miatt

$$\geq |S(y)| - |S(y+jd) - S(y)| \geq \frac{\gamma^m N^m}{2} - \alpha\gamma^m N^m$$

adódna, amiből

$$\alpha + \beta > \frac{1}{2}$$

következne ellentmondásként.

A harmadik feltételt $|T(\cdot)|$-ra adott becslés miatt könnyű teljesíteni:

$$|T(y+jd)| \leq \gamma\delta^{m-2} N^m < \beta\gamma^m N^m$$

esetén igaz, azaz, ha δ értékére

$$\delta < (\beta\gamma^{m-1})^{\frac{1}{m-2}}.$$

A középső feltételhez a Dirichlet-től származó, (és mint már említettük a skatulya-elvvel könnyen igazolható) lemmára van szükségünk:

24. Lemma. *Legyen $t > 1$, $t \in \mathbb{N}$, $z_1, z_2, \ldots, z_k$ valós számok. Ekkor van olyan d, $1 \leq d \leq t^k$, hogy*

$$\|d \cdot z_i\| < \frac{1}{t},$$

ahol $\|x\| = \min\{x, 1-x\}$ $x-$hez legközelebb eső egésztől való távolsága.

Legyen

$$U' = U \setminus \{0\} = \{r_1, r_2, \ldots, r_u\}.$$

Ekkor nyilván

$$|S(y) - S(y+jd)| = |\sum_{r \in U} \widehat{A}(r)^m \left(e(-r(y+jd)) - e(-ry)\right)| =$$

$$= |\sum_{r \in U'} \widehat{A}(r)^m \left(e(-r(y+jd)) - e(-ry)\right)| \leq$$

$$\leq \sum_{r \in U'} |\widehat{A}(r)|^m |1 - e(rjd)| \leq \sum_{r \in U'} |\widehat{A}(r)|^m 2\pi \left\| \frac{rjd}{N} \right\|.$$

Mint láttuk $u \leq \gamma/\delta^2$. Alkalmazzuk a lemmát erre a halmazra $t = N^{\frac{1}{u}}$ mellett. Ekkor $d \leq t^u \leq N$, és bármely r_i-re

$$\left\| \frac{r_i d}{N} \right\| < \frac{1}{N^{\frac{1}{u}}}.$$

Ezért

$$|S(y) - S(y+jd)| \leq \sum_{r \in U'} |\widehat{A}(r)|^m 2\pi \left\| \frac{rjd}{N} \right\| \leq 2\pi \cdot j \cdot \frac{1}{N^{\frac{1}{u}}} \sum_{r \in U'} |\widehat{A}(r)|^m \leq$$

$$\leq 2\pi \cdot j \cdot \frac{1}{N^{\frac{1}{u}}} \gamma^{m-1} N^m.$$

Az $|S(y) - S(y+jd)|$-re szabott feltétel teljesül, ha

$$\leq 2\pi \cdot j \cdot \frac{1}{N^{\frac{1}{u}}} \gamma^{m-1} N^m < \alpha \gamma^m N^m.$$

Ez $j-$re a

$$j \leq \frac{\gamma}{2\pi} N^{\frac{1}{u}} = c_1 N^{c_2}$$

feltételt szabja (a konstansok a paraméterekből kiszámíthatók; $c_1 = c_1(\gamma)$, $c_2 = c_2(\gamma, m)$). $\square$

13.13. Prímtestbeli halmazok eloszlásáról

Ismeretes, hogy karakterösszegből következtethetünk halmazok eloszlásáról például véges testekben. Mint a 13.9 pontban láttuk a Weil becslés polinomok (bizonyos megszorítások mellett) értékeinek az eloszlásáról mond ki éles eredményt. Többváltozós polinomok ú.n. nem teljes összegére csak bizonyos konkrét polinomok mellett mondható ki néhány eredmény. A következőkben egy ilyen becslést mutatunk meg, amelyben az Additív Kombinatorika eszközeit használjuk.

13.13.1. Tétel. *Legyenek* $A, B \subseteq \mathbb{F}_p$, *melyekre* $|A|, |B| < \sqrt{p}$. *Ekkor van olyan* $\eta > 0$, *hogy bármely* $r \neq 0$ *esetén*

$$\Big| \sum_{x\in A; y\in B} e_p(r(xy + x^2y^2)) \Big| < p^{1-\eta}.$$

Bizonyítás:

Legyenek $f, g \in \mathbb{F}_p[x]$ tetszőleges nem konstans polinomok, és jelölje $E_{f,g}(A)$ az

$$\begin{cases} f(a_1) + f(a_2) + f(a_3) = f(a_4) + f(a_5) + f(a_6) \\ g(a_1) + g(a_2) + g(a_3) = g(a_4) + g(a_5) + g(a_6) \end{cases}$$

$a_i \in A;\ i = 1, 2, \ldots, 6$ megoldásainak a számát. Hasonlóan definiáljuk $E_{f,g}(B)-$t is.

25. Lemma (Exponenciális-összeg becslés többváltozós energiákkal). *Tekintsük az*

$$S := \Big| \sum_{x\in A; y\in B} e_p(f(x)f(y) + g(x)g(y)) \Big|$$

összeget.Ekkor

$$S \leq (|A||B|)^{2/3} \sqrt[9]{p}\, \sqrt[18]{E_{f,g}(A)E_{f,g}(B)}.$$

A lemma bizonyítása:

Használjuk a Hölder egyenlőtlenséget $2/3 + 1/3 = 1$ paraméterekkel. Így

$$|S| \leq (\sum_{x\in A} 1)^{2/3} \Big(\sum_{x\in A} \Big| \sum_{y\in B} e_p(f(x)f(y) + g(x)g(y)) \Big|^3 \Big)^{1/3},$$

$$|S|^3 \le |A|^2 \sum_{x\in A} \Big| \sum_{y_1,y_2,y_3\in B} e_p(f(x)(f(y_1)+f(y_2)+f(y_3))+g(x)(g(y_1)+g(y_2)+g(y_3))\Big|$$

Alkalmas u_x komplex paraméterekkel, melyekre $|u_x| = 1$, az abszolút értékektől megszabadulhatunk.

$$|S|^3 \le |A|^2 \sum_{x\in A} u_x \sum_{y_1,y_2,y_3\in B} e_p(f(x)(f(y_1)+f(y_2)+f(y_3))+g(x)(g(y_1)+g(y_2)+g(y_3)).$$

Jelölje

$$\alpha_1 := \alpha_{1,y_1,y_2,y_3} = f(y_1)+f(y_2)+f(y_3);\ \alpha_2 := \alpha_{2,y_1,y_2,y_3} = g(y_1)+g(y_2)+g(y_3)$$

értékeket és $m(\alpha_1,\alpha_2)$ az

$$\alpha_1 = f(y_1)+f(y_2)+f(y_3) \quad \alpha_2 = g(y_1)+g(y_2)+g(y_3)$$

egyenletrendszer megoldásainak a számát. Ezekkel a jelölésekkel és újra a Hölder egyenlőtlenséget $2/3, 1/3$ paraméterekkel használva

$$|S|^9 \le |A|^6|B|^6 \sum_{\alpha,\alpha_2\in\mathbb{F}_p} m(\alpha_1,\alpha_2)\Big|\sum_{x\in A} u_x e_p(\alpha_1 f(x)+\alpha_2 g(x))\Big|^3.$$

Végül használni fogjuk a Cauchy egyenlőtlenséget. Ehhez vegyük észre, hogy

$$\sum_{\alpha,\alpha_2\in\mathbb{F}_p} m^2(\alpha_1,\alpha_2) = E_{f,g}(B)$$

és az ortogonalitást felhasználva

$$\sum_{\alpha_1,\alpha_2\in\mathbb{F}_p} \Big(\Big|\sum_{x\in A} u_x e_p(\alpha_1 f(x)+\alpha_2 g(x))\Big|^3\Big)^2 \le p^2 E_{f,g}(A).$$

Így

$$|S|^{18} \le p^2|A|^{12}|B|^{12}E_{f,g}(A)E_{f,g}(B). \quad \square$$

Mivel $|A|, |B| < \sqrt{p}$, továbbá a lemmát az $f(x) = x;\ g(x) = x^2$ polinomokra használva és $E_{f,g}(A)$-t ($E_{f,g}(B)$-t) röviden $J(A)$-nak ($J(B)$-nek) írva kapjuk, hogy

$$S^{18} \ll p^{14} J(A)J(B).$$

Ha bizonyítjuk, hogy $J(A)$ ill. $J(B)$ értéke $\ll p^{2-\delta}$, akkor igazoltuk az állítást.

Jelölje $I(\lambda_1, \lambda_2)$ a

$$\begin{cases} \lambda_1 = a_1 + a_2 + a_3 \\ \lambda_2 = a_1a_2 + a_1a_3 + a_2a_3 \end{cases}$$

megoldásainak a számát. Ekkor egyszerű algebrai átalakítás miatt – t.i. $\lambda_1^2 - 2\lambda_2 = a_1^2 + a_2^2 + a_3^2$ – azt kapjuk, hogy $\sum_{\lambda_1,\lambda_2 \in \mathbb{F}_p} I^2(\lambda_1, \lambda_2) = J(A)$.

Bármely $\lambda_1, \lambda_2 \in \mathbb{F}_p$ párra $I(\lambda_1, \lambda_2) \ll |A|$. Valóban, rögzítsünk egy tetszőleges $z := a_3 \in A$ elemet. Ekkor

$$\begin{cases} \lambda_1 - z = a_1 + a_2 \\ \lambda_2 - z(\lambda_1 - z) = a_1a_2 \end{cases}$$

egyenletrendszert kapjuk, aminek a_1, a_2-ban legfeljebb két megoldása van. A következő "nívóhalmaz" lesz a pontok halmaza:

$$\mathcal{P}\{(\lambda_1, \lambda_2) : I(\lambda_1, \lambda_2) > p^{1/2-\varepsilon}\},$$

$$\mathcal{L} := \{y = (a_1 + a_2)x - (a_1^2 + a_1a_2 + a_2^2) : a_1, a_2 \in A\}$$

pedig az egyenesek halmaza. Az $\varepsilon > 0$ és később definiáljuk, kellően kis értékre. Célunk megmutatni, hogy $|\mathcal{P}| < p^{1/2-\varepsilon}$.

Valóban, ugyanis ekkor egyfelől

$$\sum_{\lambda_1,\lambda_2 \notin \mathcal{P}} I^2(\lambda_1, \lambda_2) < p^{1/2-\varepsilon} \sum_{\lambda_1,\lambda_2 \notin \mathcal{P}} I(\lambda_1, \lambda_2) \leq p^{1/2-\varepsilon}|A|^3 < p^{2-\varepsilon},$$

és így

$$J(A) \ll p^{2-\varepsilon} + \sum_{\lambda_1,\lambda_2 \in \mathcal{P}} I^2(\lambda_1, \lambda_2).$$

Tehát, mivel $I(\lambda_1, \lambda_2) \ll |A|$, ezért

$$\sum_{\lambda_1,\lambda_2 \in \mathcal{P}} I^2(\lambda_1, \lambda_2) \ll |\mathcal{P}||A|^2 \ll p^{2-\varepsilon}$$

így $J(A) \ll p^{2-\varepsilon}$ következik.

A $|\mathcal{P}| < p^{1/2-\varepsilon}$ becslést a Szemerédi-Trotter típusú 11.1.2 tételből vezetjük le.

Az egyenesek száma $|\mathcal{L}| = c|A|^2 \ll p;\ (c > 0)$, ugyanis bármely $a_1, a_2 \in A$ párra, ha

$$m = a_1 + a_2 \quad b = a_1^2 + a_1 a_2 + a_2^2,$$

akkor rögzített m, b párra legfeljebb két megoldást kapunk a_1, a_2-ben.

Továbbá $(\lambda_1, \lambda_2) = (x, y)$ egy pontja egy egyenesnek, pontosan akkor, ha $I(\lambda_1, \lambda_2) > 0$. Valóban, az egyenesek definíciója miatt

$$(a_1 + a_2)\lambda_1 - (a_1^2 + a_1 a_2 + a_2^2) =$$

$$= (a_1 + a_2)(a_1 + a_2 + a_3) - (a_1^2 + a_1 a_2 + a_2^2) = a_1 a_2 + a_1 a_3 + a_2 a_3 = \lambda_2.$$

Így az illeszkedések száma legalább $|\mathcal{P}|p^{1/2-\varepsilon}$.

Most

$$|\mathcal{P}|p^{1/2-\varepsilon} \leq \sum_{\lambda_1, \lambda_2 \in \mathcal{P}} I(\lambda_1, \lambda_2) \leq |A|^3 \leq p^{3/2},$$

így $|\mathcal{P}| \leq p^{1+\varepsilon}$. Mivel $|\mathcal{L}| = c|A|^2 \ll p$, így $|\mathcal{P}| + |\mathcal{L}| \ll p^{1+\varepsilon}$ és a 11.1.2 illeszkedési tétel miatt

$$(|\mathcal{L}| + |\mathcal{P}|)^{3/2-\gamma} \ll p^{3/2-\gamma/2}$$

ha $\varepsilon > 0$ elég kicsi a fix γ értékéhez képest. Összevetve ezt az illeszkedések $|\mathcal{P}|p^{1/2-\varepsilon}$ alsó becslésével, kapjuk, hogy

$$|\mathcal{P}| < p^{1/2-\gamma/2}$$

ha ε elég kicsi.

A $J(B)-$re a becslés hasonló. □

14. fejezet

Hilbert kockákról

A manapság ismert legrégebbi Ramsey-típusú eredményt D. Hilbert fogalmazta meg $1892-$ben egész együtthatós racionális törtfüggvények irreducibilitását vizsgálva (közel 25 évvel korábban, mint Schur nevezetes "$x + y = z$" tételét). Egy $m-$dimenziós a□n kocka – vagy Hilbert tiszteletére $m-$dimenziós Hilbert kocka – alatt a

$$H = H(a_0, a_1, a_2, \ldots, a_m) = \{a_0 + \sum_{i=1}^{m} \varepsilon_i a_i : \varepsilon_i \in \{0, 1\}\}$$

halmazt értjük. Az a_i elemeket a kocka éleinek szokás nevezni, H elemszámát a kocka méretének nevezzük. Nyilván $|H| \leq 2^m$.

Amennyiben $a_0 = 0$ akkor az $A' = \{a_1, a_2, \ldots, a_m\}$ halmazra az $FS(A') := \{\sum_{i=1}^{m} \varepsilon_i a_i : \varepsilon_i \in \{0, 1\}\}$ rövidebb jelölést használjuk.

Végtelen Hilbert kockát is definiálhatunk; ekkor az A halmaz végtelen, és nyilván ilyenkor csak véges összegeket tekintünk, azaz a fenti definícióhoz a szükséges $\sum_i \varepsilon_i < \infty$ feltételt kell hozzátennünk.

Hilbert nevezetes tétele 1892-ből így hangzik:

14.0.1. Tétel. *Legyenek m és r pozitív egészek. Ekkor a természetes számok bármely $r-$színezése esetén létezik olyan $H(a_0, a_1, a_2, \ldots, a_m)$ affin kocka, melynek elemei azonos színűek.*

1969−ben Szemerédi e fenti tétel e□ektív-sűrűségi változatát bizonyította be.

14.0.2. Tétel. *Legyen $A \subseteq \mathbb{N}$, melyre $\eta := \underline{d}(A) > 0$. Ekkor van olyan $\beta > 0$ valós szám, hogy bármely $n > n_0(\eta)$ esetén $A \cap [1, n]$ tartalmaz egy $\beta \log\log n$ dimenziójú Hilbert kockát.*

Bizonyítás:

Létezik olyan n_0 küszöbindex, melyre $n > n_0$ esetén az $[1, n]$ intervallum az A halmazból legalább $m_0 := \nu \cdot n$ elemet tartalmaz, ahol $\nu = \eta/2$ és $n > n_0$. E halmazból $\binom{m_0}{2}$ különbség képezhető, tehát van egy olyan d_1, amelyik legalább $h_1 := \frac{\binom{m_0}{2}}{n-1}$-szer szerepel. Legyen $A_1 = \{a \in A : a+d_1 \in A\}$. Erre a halmazra tehát

$$A_1 \subseteq A;\ d_1 + A_1 \subseteq A;\ \text{és } |A_1| \geq h_1.$$

Alkalmazzuk az előző gondolatmenetet az A_1 halmazra, kapva egy d_2 egészt, egy A_2 halmazt, melyre

$$A_2 \subseteq A_1;\ d_2 + A_2 \subseteq A_1 \subseteq A;\ \text{és } |A_2| \geq h_2,$$

ahol $h_2 = \frac{\binom{|A_1|}{2}}{n-1}$. Ezt az eljárást folytatva kapjuk általában a d_i egészt, egy A_i halmazt, melyre

$$A_i \subseteq A_{i-1};\ d_i + A_i \subseteq A_{i-1} \subseteq A;\ \text{és } |A_i| \geq h_i,$$

ahol $h_i = \frac{\binom{|A_{i-1}|}{2}}{n-1}$, feltéve, hogy $h_i \geq 1$. Legyen k az a legnagyobb index, amelyre még $h_k \geq 1$. Egyszerű számolással adódik, hogy ez a $k = \log\log n + C(\eta)$. Továbbá, hogy valamely $a \in A_k$

$$H(a, d_1, d_2, \ldots, d_k) \subseteq A$$

amint azt akartuk. □

14.1. Brown-Erdős-Freedman problémájáról

Az előző pontban "sűrű" sorozatokban vizsgáltuk nagy Hilbert kockák létezését. Ebben a paragrafusban T.C. Brown, Erdős és A. Freedman problémájához kapcsolódva nevezetes sorozatokban található Hilbert kockák dimenzióját vizsgáljuk. Jelölje $\mathcal{Q}$ a négyzetszámok sorozatát.

Az eredeti kérdés úgy hangzott, vajon a négyzetszámok halmaza tartalmaze tetszőleges dimenziójú Hilbert kockát. E kérdés nyitva maradt, számos számítógép által talált példa ismert csak. Például

$$H(5,2,6,96) = \{5,7,11,13,101,103,107,109\} \subset \mathcal{P},$$

$$H(1,15,48) = \{1,16,49,64\} \subset \mathcal{Q}.$$

E kérdést motiválhatta az az Euler óta ismert tény, hogy a négyzetszámok halmazában nincsen négytagú számtani sorozat. (Euler egy erősebb állítást fogalmazott meg; az $a(a+d)(a+2d)(a+3d) = x^2$ diofantikus egyenletnek $d \neq 0$ mellett nincs megoldása)

14.1.1. Tétel.

$$H_{\mathcal{Q}}(N) < 48\sqrt[3]{\log N}.$$

E tételt azóta többen javították; mégis ezt mutatjuk be, mert jól illusztrálja, hogyan lehet a 10. fejezet Gallagher-féle nagyobb szitát és az előző fejezetben használt diszkrét Fourier analízist alkalmazni.

Bizonyítás:

A tétel bizonyításához először e kérdés moduláris megfelelőjét vizsgáljuk. Jelölje $f(p)$ annak a legnagyobb $\mathcal{A} \subset \mathbb{Z}_p$ halmaznak a számosságát, melyre valamely $d \in \mathbb{Z}_p$ mellyett $H(d,\mathcal{A})$ négyzetes maradékok $\mathbb{Z}_p$-ben.

Bizonyítjuk, hogy

4. Propozíció. *Bármely $\varepsilon > 0$, ha $p > p_0(\varepsilon)$, akkor*

$$f(p) < 12\sqrt[4]{p}.$$

Bizonyítás nélkül megemlítjük Olson egy szép eredményét:

26. Lemma. *Legyen p prím és $a_1, a_2, \ldots, a_s$ olyan nem nulla maradékok modulo p melyekre $a_i \neq \pm a_j$, $i \neq j$. Ekkor*

$$|FS(a_1, a_2, \ldots, a_s)| \geq \frac{1}{2}\min\{p+3, s(s+1)\}.$$

E lemmából levezetjük ennek egy következményét:

7. Következmény. *Ha p prím és $R \subseteq \mathbb{Z}_p$, akkor*

$$|FS(R)| \geq \frac{1}{2}\min\{p+3, (|R|^2-1)/4\}.$$

A Következmény bizonyítása:

A $p = 2$ eset nyilvánvaló, tehát legyen $p > 2$. Legyen $A = \{a_1, a_2, \ldots, a_s\}$ az $R \cap [1, 2, \ldots, (p-1)/2]$ és az $R \cap [-1, -2, \ldots, -(p-1)/2]$ halmazok közül a nagyobbik. Ekkor nyilván $s = |A| \geq \frac{|R|-1}{2}$, és erre a halmazra teljesül, hogy $0 \notin A$, és $a_i \neq \pm a_j$, $i \neq j$. Így a 26. Lemma miatt

$$|FS(R)| \geq |FS(A)| \geq \frac{1}{2}\min\{p+3, s(s+1)\} \geq \frac{1}{2}\min\{p+3, (|R|^2-1)/4\}.$$

Mint a 13.2 pontban, a Gauss összeg a

$$G(h,p) = \sum_{x=0}^{p-1} e_p(hx^2)$$

kifejezés. Vezessük be a $G_0 = G(1,p)$ jelölést. A 13.2 pontban láttuk, hogy $|G_0| = \sqrt{p}$ és $|G(h,p)| = |G_0|$ esetén $h \neq 0$, továbbá, hogy $G(0,p) = p$..

Tegyük fel, hogy $d \in \mathbb{Z}_p$, $\mathcal{A} = \{a_1, a_2, \ldots, a_k\} \subseteq \mathbb{Z}_p$. A Hilbert kockát osszuk kétfelé;

$$B := d + FS(a_1, a_2, \ldots, a_{[k/2]}) \quad C := FS(a_{[k/2]+1}, \ldots, a_k),$$

így

$$B + C \subseteq H(d, a_1, a_2, \ldots, a_k) \tag{14.1}$$

és $B + C$ halmaz elemei négyzetes maradékok $\mathbb{Z}_p$-ben.

Ekkor a 7. Következmény miatt

$$\min\{|B|, |C|\} \geq \frac{1}{2}\min\{p+3, (\lfloor k/2 \rfloor^2 - 1)/4\}. \tag{14.2}$$

Legyen

$$T = \sum_{x=0}^{p-1} \Big(\sum_{b\in B} e_p(bx^2)\Big)\Big(\sum_{c\in C} e_p(cx^2)\Big).$$

Ekkor (14.1) miatt

$$|T| = \Big|\sum_{x=0}^{p-1}\sum_{b\in B}\sum_{c\in C} e_p((b+c)x^2)\Big)\Big| = \Big|\sum_{b\in B}\sum_{c\in C} G(b+c,p)\Big| \geq$$

$$\geq \Big|\sum_{b\in B}\sum_{c\in C} G_0\Big| - \sum_{b\in B}\sum_{c\in C}|G_0 - G(b+c,p)| = |B||C||G_0| - \sum_{b\in B; c\in C; p|b+c}|G_0 - G(0,p)| \geq$$

$$\geq |B||C|\sqrt{p} - 2\sum_{b\in B; c\in C; p|b+c} 1 \geq |B||C|\sqrt{p} - 2\min\{|B|,|C|\}. \qquad (14.3)$$

Most a $|T|$-re adunk felsőbecslést: A Cauchy egyenlőtlenség miatt

$$|T| = \sum_{x=0}^{p-1}\Big|\sum_{b\in B} e_p(bx^2)\Big|\Big|\sum_{c\in C} e_p(cx^2)\Big| \leq$$

$$\leq \Big(\sum_{x=0}^{p-1}\Big|\sum_{b\in B} e_p(bx^2)\Big|^2\Big)^{1/2}\Big(\sum_{x=0}^{p-1}\Big|\sum_{c\in C} e_p(cx^2)\Big|^2\Big)^{1/2}.$$

Amint x végigfut $0, 1 \ldots, p-1$ elemein addig x^2 minden négyzetes maradékot legfeljebb kétszer fut be. Ezért

$$|T| \leq \Big(2\sum_{y=0}^{p-1}\Big|\sum_{b\in B} e_p(by)\Big|^2\Big)^{1/2}\Big(2\sum_{y=0}^{p-1}\Big|\sum_{c\in C} e_p(cy)\Big|^2\Big)^{1/2} =$$

$$= 2\Big(\sum_{y=0}^{p-1}\Big|\sum_{b,b'\in B} e_p((b-b')y)\Big|^2\Big)^{1/2}\Big(\sum_{y=0}^{p-1}\Big|\sum_{c,c'\in B} e_p((c-c')y)\Big|^2\Big)^{1/2} =$$

$$= 2\sqrt{|B|p}\sqrt{|C|p} = 2p\sqrt{|B||C|}. \qquad (14.4)$$

(14.3)-ból és (14.4)-ből következik, hogy

$$|B||C|\sqrt{p} \leq 2p(\sqrt{|B||C|} + \min\{|B|,|C|\}) \leq 4p\sqrt{|B||C|}$$

ezért

$$\min\{|B|,|C|\} \leq \sqrt{|B||C|} \leq 4\sqrt{p}. \qquad (14.5)$$

(14.2) és (14.5) miatt

$$\min\Big\{\frac{p+3}{2}, \frac{\lfloor k/2\rfloor^2 - 1}{8}\Big\} \leq 4\sqrt{p}. \qquad (14.6)$$

Ha $p > 57$ akkor $\frac{p+3}{2} > 4\sqrt{p}$, és így (14.6)-ből következik, hogy

$$\lfloor k/2\rfloor^2 - 1 \leq 32\sqrt{p}$$

Tehát ha p elég nagy, akkor

$$k = |A| < 12\sqrt[4]{p}$$

ami bizonyítja az állítást.

A moduláris eset és Gallagher nagyobb szitája lesz a segítségünkre az eredeti állítás bizonyításában. Idézzük ezt most fel, mint egy lemmát:

27. Lemma. *Legyen $A \subseteq [1, N]$ egészek egy halmaza. Legyen $\mathcal{P}$ prímszámok egy véges hamaza és minden egyes prímre jelölje $\nu(p)$ azon maradékosztályok számát modulo p melyek tartalmaznak A elemeivel kongruens elemeket. Ekkor*

$$|A| \leq \frac{\sum_{p\in\mathcal{P}} \log p - \log n}{\sum_{p\in\mathcal{P}} \frac{\log p}{\nu(p)} - \log n}.$$

Ennek segítségével igazoljuk a következőt:

5. Propozíció. *Legyen $K > 0$, $0 < \eta < 1$, $p_0 > 0$, $\varepsilon > 0$ és legyen $C = (2K(1-\eta)^{1/(1-\eta)}$. Ekkor létezik egy $n_0 = n_0(K, \eta, p_0, \varepsilon)$ küszöbindex, melyre ha $n \in \mathbb{N}$, $n > n_0$, $A \subset \{1, 2, \ldots, n\}$ és U-val jelölve $U = C(\log n)^{1/(1-\eta)}$ mennyiséget teljesül, hogy*

$$\nu(p) < Kp^{\eta} \tag{14.7}$$

ahol p olyan prím, amelyik $p_0 < p \leq U$. Ekkor

$$|\mathcal{A}| < (C + \varepsilon)(\log n)^{\eta/(1-\eta)}. \tag{14.8}$$

Ez egy kissé technikai jellegű állítás, első olvasásra a bizonyítás ki is hagyható.

Bizonyítás:

Használjuk a 27. Lemmát a $\mathcal{P} = \{p : p \text{ prím};\ p_0 < p \leq U\}$ halmazra. Ekkor (14.7) és a prímszámtétel miatt, amennyiben $n \to \infty$, a nevező

$$\sum_{p\in\mathcal{P}} \frac{\log p}{\nu(p)} - \log n > \sum_{p_0<p\leq U} \frac{\log p}{Kp^{\eta}} - \log n =$$

$$= \Big(\frac{1}{K} + o(1)\Big) \sum_{n\leq U/\log U} \frac{\log n}{(n \log n)^{\eta}} - \log n =$$

$$= \Big(\frac{1}{K} + o(1)\Big) \int_2^{U/\log U} \frac{(\log x)^{1-\eta}}{x^\eta} - \log n =$$

$$= \Big(\frac{1}{K} + o(1)\Big) \frac{1}{1-\eta} U^{1-\eta} - \log n = \Big(\frac{1}{K(1-\eta)} + o(1)\Big) U^{1-\eta} \qquad (14.9)$$

ami tehát pozitív és így a szita alkalmazható.

Ugyancsak a prímszámtétel miatt a számláló

$$\sum_{p\in\mathcal{P}} \log p - \log n = \sum_{p_0<p\le U} \log p - \log n = (1+o(1))U - \log n = (1+o(1))U. \qquad (14.10)$$

Így (14.9) és (14.10) miatt

$$|\mathcal{A} \le (2K(1-\eta) + o(1))U^\eta = (C + o(1))(\log n)^{\eta/(1-\eta)}$$

amint azt állítottuk. □

Felhasználva a fenti propozíciót; tegyük fel, hogy van egy $H(d, a_1, a_2, \ldots, a_k)$ Hilbert $k-$kocka a $\mathcal{Q}\cap\{1, 2, \ldots, n\}$ halmazban. Ez azt jelenti, hogy bármely p prímszámra a $H(d, a_1, a_2, \ldots, a_k)$ elemei kvadratikus maradékok $\mathbb{Z}_p$-ben. Így a 4. propozíció miatt a különböző maradékosztályok ν száma $\nu(p) < 12\sqrt[4]{p}$. Használva a 5. propozíciót $K = 12;\ \eta = 1/4;\ \varepsilon = \frac{1}{100}$ mellett azt kapjuk, hogy ha n elég nagy, akkor

$$k < (C+\varepsilon)(\log n)^{\eta/(1-\eta)} = \Big(18^{4/3} + \frac{1}{100}\Big)(\log n)^{1/3} < 48\sqrt[3]{\log n}$$

bizonyítva az állítást. □

A fenti tétel párjaként kérdezhetjük, hogy vajon pl. a négyzetmentes számok milyen Hilbert kockát tartalmazhatnak. A következő tételben a "milyen" határozott értelmet fog nyerni.

14.1.2. Tétel. *Legyen B a természetes számok egy olyan sorozata, amelyre $\sum_{b\in B} \frac{1}{b}$ sor konvergens és elemei páronként relatív prímek. Legyen A azon természetes számok sorozata, mely számok egyik B-beli elemmel se oszthatóak. Ekkor A tartalmaz egy végtelen Hilbert kockát.*

8. Következmény. *Az S négyzetmentes számok sorozata tartalmaz végtelen Hilbert kockát.*

Valóban, legyen $B = \{p^2 : p \in \mathcal{P}\}$. Mivel $\sum_{p\in\mathcal{P}} \frac{1}{p^2}$ sor konvergens, és az A sorozat éppen a négyzetmentes számok, ezért a fenti tétel igazolja a következményt.

A 14.1.2 tétel bizonyítása:

Legyen $B = \{b_1 < b_2 < \dots\}$ és $\varepsilon > 0$ rögzített. Ekkor van olyan n_0, hogy $\sum_{i>n_0} \frac{1}{b_i} < \varepsilon$. Definiáljuk m-et a b-k szorzataként: $m = b_1 b_2 \dots b_{n_0}$.

Vegyünk egy $\{a_1 < a_2 < \dots < a_k\} \subseteq A$ véges halmazt és tekintsük az $a_i + mt$, $(i = 1, 2, \dots k)$ számtani sorozatokat, ahol t fusson $N-$ig. Megmutatjuk, hogy legfeljebb $\varepsilon k N$ elem nem tartozik az A halmazhoz. Legyen $a_i + mt$ $i = 1, 2, \dots k$ egy tetszőleges számtani sorozat, és tegyük fel, hogy egy x eleme nem tartozik A-hoz. Ekkor valamely b_j osztja x-et. Ennek a b_j-nek az indexe nem lehet az $1, 2, \dots, n_0$ egyike se, mert ellenkező esetben az $a_i - t$ is osztaná. Tehát $j > n_0$. Mivel $(m, b_j) = 1$, ezért a "kimaradó" elemek száma N-ig legfeljebb

$$\sum_{j>n_0} \left(1 + \frac{N}{b_j m}\right) \leq \sum_{b_j \leq N} 1 + \frac{N\varepsilon}{m} = \frac{N\varepsilon}{m} + o(N),$$

egyrészt felhasználva, hogy $\sum_{i>n_0} \frac{1}{b_i} < \varepsilon$, másrészt azon sorozat, melynek reciprok összege konvergens $o(N)$ elemet tartalmaz $N-$ig. (lásd a feladatot). Azaz $a_i + Nm$-ig $\frac{N\varepsilon}{m} Nm$ tag nem tartozik $A-$hoz, a k elemet véve így legfeljebb $k\varepsilon N$ elem nem tartozik az A halmazhoz.

Rekurzióval fogjuk definiálni a végtelen Hilbert kockát. Egy $H(x_0, d_1)$ nyilván található A-ban. Tegyük fel, hogy $H(x_0, d_1, \dots, d_k) \subseteq A$ teljesül valamilyen $k \geq 1$ index mellett, és tegyük fel, hogy $H(x_0, d_1, \dots, d_k) \subseteq \{a_1 < a_2 < \dots < a_k\} \subseteq A$. Legyen $0 < \varepsilon < \frac{1}{k a_k}$, és tekintsük az $a_i + mt$, $(i = 1, 2, \dots, k)$ számtani sorozatokat, ahol m az ε konstanshoz tartozó egész.

Az előbb elmondottak alapján így lesz $\frac{1}{\varepsilon} > k a_k$ egymást követő T index, hogy minden $i = 1, 2, \dots, k$ esetén az $a_i + tm, \dots, a_i + (t+T)m$ elemek mindegyike az A halmazban lesz benne. Legyen $d_{k+1} = t$. Mivel $H(x_0, d_1, \dots, d_k) \subseteq \{a_1 < a_2 < \dots < a_k\}$, és

$$H(x_0, d_1, \dots, d_{k+1}) = H(x_0, d_1, \dots, d_k) + \{0, d_{k+1}\},$$

ezért $H(x_0, d_1, \dots, d_k) + \{0, d_{k+1}\} \subseteq A$ is teljesülni fog, amint azt akartuk. □

Feladatok

1. Legyen $B \subseteq \mathbb{N}$ egy olyan sorozat, melyre $\sum_{b\in B} \frac{1}{b}$ sor konvergens. Ekkor a B sorozat nulla sűrűségű.

2. (T. Schoen)

a.) Legyen S egészek egy halmaza, és tegyük fel, hogy valamely x-re és $0 < \delta < 1$ számra

$$|S \cap (S + x)| \geq (1 - \delta)|S|.$$

Ekkor S tartalmaz egy $\lfloor \frac{1}{\delta} \rfloor$ hosszúságú x di□erenciájú számtani sorozatot.

b.) Tegyük fel, hogy A, B két véges, egészekből álló sorozat, valamely K-ra $|A + B| \leq K|A|$, továbbá B tartalmaz egy d dimenziós Hilbert kockát. Ekkor $A + B$-ben található egy legalább

$$\Big\lfloor \frac{d}{(e-1)\log K} \Big\rfloor$$

hosszú számtani sorozat, feltéve, ha $d \geq \log K$.

Megoldások

1. A feladattal ekvivalens a következő állítás: ha egy C sorozat felső sűrűsége pozitív, akkor az elemeiből képzett reciprok összeg divergens. Legyen tehát $x_1 < x_2 < \cdots < x_k < \ldots$ egy olyan sorozat, melyre létezik $\alpha > 0$, hogy $B(x_k) > \alpha x_k$ igaz, továbbá nyilván feltehetjük, hogy $x_k > x_{k-1}^2$ is teljesül. Ekkor elég nagy k értékre $B(x_k) - B(x_{k-1}) > \frac{\alpha}{2} x_k$. Így ettől a k-tól kezdve

$$\sum_{x_{k-1} \leq c < x_k; c\in C} \frac{1}{c} \geq \frac{\alpha}{2} x_k \cdot \frac{1}{x_k} = \frac{\alpha}{2},$$

Így a $\sum_{c\in C} \frac{1}{c}$ sor divergens.

2. a.) Tekintsük S-ben a legalább 2 hosszúságú, x di□erenciájú számtani sorozatokat. Legyen ezek hossza $k_1 \leq k_2 \leq \cdots \leq k_d$, és legyen $S' \subseteq S$ az ezekben található tagok uniója, Tegyük fel, hogy minden egyes számtani sorozat már nem bővíthető, azaz diszjunktak, és így $\sum_{i=1}^{d} k_i = |S'|$.

Ha $a < a + x < a + 2x < \cdots < a + k_i x$ egy ilyen számtani sorozat, akkor

$$a + x, a + 2x, \ldots, a + k_i x \in S \cap (S + x)$$

és így

$$\sum_{i=1}^{d}(k_i-1)=|S\cap(S+x)|\geq(1-\delta)|S|\geq(1-\delta)|S'|.$$

$\sum_{i=1}^{d}(k_i-1)=\sum_{i_1}^{d}k_i-d=|S'|-d$, ezért

$$\left\lfloor\frac{1}{\delta}\right\rfloor\leq\frac{|S'|}{d}.$$

Végül

$$|S'|=\sum_{i=1}^{d}k_i\leq d\max_i k_i,$$

amiből következik az állítás.

b.) Legyen $H(x_0,x_1,\ldots,x_d)\subseteq B$. Mint láttuk, $H(x_0,d_1,\ldots,d_k)=x_0+\{0,x_1\}+\{0,x_2\}+\ldots\{0,x_d\}$.

Továbbá $A+B\supseteq A+H$, ezért elég lesz $A+H$-ban keresni "hosszú" számtani sorozatot. Legyen $Y_0=A+x_0$, továbbá $i\geq 1$ esetén $Y_{i+1}=Y_i+\{0,x_{i+1}\}$. Nyilván

$$Y_0\subseteq Y_1\subseteq\cdots\subseteq A+B$$

és így

$$|A|\leq|Y_0|\leq|Y_1|\cdots\leq|A+B|\leq K|A|,$$

ezért létezni fog olyan i, melyre

$$|Y_{i+1}|=|Y_i+\{0,x_{i+1}\}|\leq K^{1/d}|Y_i|.$$

A logokai szita legegyszerűbb formájából tehát következik, hogy

$$|(Y_i+x_{i+1})\cap Y_i|\geq(2-K^{1/d})|Y_i|,$$

így az a.) pontban mondottak alapján Y_i-ben van egy

$$\left\lfloor\frac{1}{K^{1/d}-1}\right\rfloor$$

hosszú számtani sorozat.

$$K^{1/d}\leq 1+(e-1)\frac{\log K}{d}$$

(ami következik abból, hogy az $x=K^{1/d}$ választással az $1\leq x\leq e$ esetén az $f(x):=(e-1)\log x-x+1$ függvényre teljesül, hogy ebben a tartományban szigorúan konkáv, és $f(1)=f(e)=0$,)

15. fejezet

Additív kombinatorika a Heisenberg csoportban

Jelölje

$$\mathcal{H} = \{[x, y, z],\ x, y, z \in R\}$$

az ú.n. 3 dimenziós Heisenberg csoportot (R tetszőleges gyűrű) felett, ahol

$$[x, y, z] = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(R).$$

A $\mathcal{H}$ egy multiplikatív csoport, melyre igaz a

$$[x, y, z] \cdot [x', y', z'] = [x + x', y + y', z + z' + xy']. \tag{15.1}$$

műveleti szabály.

1. Legyen $A, B \subset R$; a

$$[A, B, 0] = \{[a, b, 0],\ a \in A,\ b \in B\}$$

halmazt nevezzük 2-kockának, hasonlóan definiáljuk az $[A, B, C]$ 3-kockát.

Könnyű belátni, hogy ha A és B véges halmazok, akkor

$$[A, B, 0]^2 \subset [2A, 2B, A \cdot B]$$

és ezért $\big|[A, B, 0]^2\big| \le \big|2A\big|\big|2B\big|\big|A \cdot B\big|$. Másfelől

$$\big|[A, B, 0]^2\big| \le |A|^2|B|^2.$$

A következőkben $R = \mathbf{K}$ testet fog jelölni (tipikusan $\mathbb{R}$ ill. az $\mathbb{F}_p$ lesz) és célunk a 2- és 3-kockák négyzeteire alsó becslést adni.

Jelölje $S = [A, A, 0]$, ($A \subset \mathbf{K}$) véges 2-kockát. Ekkor S bármely két $[a, b', 0]$ és $[a', b, 0]$ elemére

$$[a, b', 0] \cdot [a', b, 0] = [a + a', b + b', ab].$$

15.0.1. Tétel.

$$|S^2| \geq |S|^{3/2}.$$

Bizonyítás:

Valóban az $E_S^\times$ energia a

$$a_1 + a_1' = a_2 + a_2', \quad b_1 + b_1' = b_2 + b_2', \quad a_1 b_1 = a_2 b_2$$

nyolcas megoldásainak a száma lesz. Rögzítsük az a_1, a_1', a_2',valamint a b_1 és b_1' elemeket. Az első háromból $a_1 + a_1' = a_2 + a_2'$ miatt adódik a_2, $a_1 b_1 = a_2 b_2$-ből b_2, $b_1 + b_1' = b_2 + b_2'$-ből pedig b_2'. Azaz legfeljebb öt elemet váaszthatunk meg szabadon, ezért $E_S^\times \leq |A|^5$. Most a Cauchy egyenlőtlenség miatt

$$|S^2| \geq \frac{|S|^4}{E_S^\times}$$

amiből következik a tétel.

A továbbiakban e becslést fogjuk javítani.

15.0.2. Tétel. *Legyen $A \subset R$ véges halmaz és legyen $S = [A, A, 0]$. Ekkor*

$$|S^2| \geq |A|^2 \max(|A^2|, |2A|).$$

Bizonyítás:

Valóban, ha rögzítjük a $k = ab \in A^2$ szorzatot, akkor $S^2 \supseteq [a+A, b+A, k]$, ezért

$$|S^2| \geq |A^2||A|^2.$$

Továbbá $A_m := A \cap (m - A) \subseteq A$ azokból az a elemekből áll, melyekre $m - a \in A$. Így

$$S^2 = \bigcup_{m,n \in 2A} [m, n, A_m \cdot A_n].$$

Kapjuk, hogy

$$|S^2| = \sum_{m,n \in 2A} |A_m \cdot A_n| \geq \sum_{m,n \in 2A} |A_m| = |2A||A|^2.$$

E tétel következménye:

15.0.3. Tétel. *Legyen $A \subseteq \mathbb{F}_p$. Ekkor*

$$|S^2| \geq \min \left\{ p|S|^{3/2}, \frac{|S|^3}{4p} \right\}.$$

Bizonyítás:
Használhatjuk a 13.10.1 tétel

$$|2A||A^2| \geq \min \left\{ \frac{p|A|}{2}, \frac{|A|^4}{4p} \right\}.$$

becslését, amiböl az előző tételt felhasználva kapjuk az állítást.

15.0.4. Tétel. *Legyen $A \subset \mathbb{F}_p$ véges halmaz és legyen $S = [A, B, C]$. Ekkor*

$$|S^2| \geq |A|^2 \min \left\{ p|2A||2B|, \frac{|C|^4|A|^2|B|^2}{pE_+(C)} \right\},$$

ahol $E_+(C)$ a C halmaz additív energiája.

Bizonyítás:
Legyen $S = [A, B, C] = \{[a, b, c] : a \in A; b \in B; c \in C\} \subset H$. Ekkor S^2 előáll

$$S^2 = \bigcup_{x,y} [x, y, 2C + A_x \cdot B_y]$$

alakban, ahol $A_x = A \cap (x - A);\ B_y = B \cap (y - B)$.
Így

$$|S^2| = \sum_{x \in 2A, y \in 2B} |2C + A_x \cdot B_y|.$$

Legyen $N_{x,y}(t)$ $(a, b, c, c') \in A_x \times B_y \times C \times C$ négyesek száma, melyre

$$t = c + c' + ab.$$

A Cauchy egyenlőtlenség miatt

$$|2C + A_x \cdot B_y| \geq \frac{\Big(\sum_t N_{x,y}(t)\Big)^2}{\sum_t N_{x,y}(t)^2}.$$

A számlálót könnyű kiszámítani: $(|C|^2|A_x||B_y|)^2$.

A nevezőben azt számoljuk, hány olyan $8-$as van, melyre

$$c_1 + c_1' + a_1 b_1 = c_2 + c_2' + a_2 b_2.$$

Ezt exponenciális összeg segítségével:

$$\frac{1}{p}\sum_r |\widehat{C}(r)|^4 \Big| \sum_{a\in A_x, b\in B_y} e_p(rab)\Big|^2,$$

ahol $e_p(z) = \exp(2i\pi z/p)$ és $\widehat{C}(r) = \sum_x C(x) e_p(r\cdot x)$. Az $r = 0$ tagot elkülönítve, ez

$$\frac{|C|^4|A_x|^2|B_y|^2}{p}.$$

Az $r \neq 0$ tagokra használva a

$$\Big| \sum_{(a,b)\in A'\times B'} e_p(rab)\Big| \leq \sqrt{p|A'||B'|}$$

Vinogradov becslést, kapjuk, hogy

$$\frac{1}{p}\sum_{r\neq 0} |\widehat{C}(r)|^4 \Big| \sum_{a\in A_x, b\in B_y} e_p(rab)\Big|^2 \leq |C|^3 \Big(\sqrt{p|A_x||B_y|}\Big)^2$$

Így

$$|2C + A_x \cdot B_y| \gg \min\Big(p, \frac{|C||A_x||B_y|}{p}\Big)$$

továbbá mivel $\sum_x |A_x| = |A|^2$,

$$|S^2| \gg \min\Big(|2A||2B|p, \frac{|C||A|^2|B|^2}{p}\Big) \gg |S|^{1+\delta}$$

[1] N. Alon, Combinatorial Nullstellensatz, Combinatorics, Probability and Computing, Vol. 8 Issue 1-2, 1999 Pages 7-29

[2] N. Alon, M. B. Nathanson, I. Ruzsa, The Polynomial Method and Restricted Sums of Congruence Classes, Journal of Number Theory Volume 56, Issue 2, 1996, Pages 404-417

[3] L. Babai, N. Nikolov, L. Pyber, Product growth and mixing in finite groups, SODA: Proceedings of the nineteenth annual ACM-SIAM symposium on Discrete algorithms San Francisco, California, 2008, 248-257

[4] A. Balog and E. Szemerédi: A statistical theorem of set addition, Combinatorica 14 1994, 263-268.

[5] V. Bergelson, Sets of reccurence of $\mathbb{Z}^m$-actions and properties of sets of di□erences, *J. London Math. Soc.* (2) 31 1985, 295–304

[6] E. Croot, I. Z. Ruzsa and T. Schoen. Arithmetic progressions in sparse sumsets. In B. Landman et al., editor, Proc. Integers Conference 2005, p 157-64, Carrollton, Ga., USA. de Gruyter.

[7] P. Diaconis, K. Soundararajan and F. Xuancheng Shao: Carries, group theory, and additive combinatorics, Amer. Math. Monthly 121 2014, no. 8, 674-688.

[8] P. Erdős, A. Ginzburg and A. Ziv, Theorem in the additive number theory, Bull. Research Council Israel 10F 1961, 41-43.

[9] G. Freiman, H. Halberstam, I. Ruzsa, Integer sumsets containing long arithmetic progressions, JLMS (2), 46 1992, no 2, 193-201.

[10] Gowers, W. T., Quasirandom groups, Comb. Probab. Comp. 17 2008, 363-387

[11] A. Granville, B. Green, Additive Combinatorics, 2010 (kézirat)

[12] B. Green, Finite field models in additive combinatorics Surveys in Combinatorics 2005, London Math. Soc. Lecture Notes 327, 1-27

[13] D.R. Heath-Brown, Arithmetic applications of Kloosterman sums, NAW 5/1 nr. 4, 2000 p. 380-384

[14] N. Hegyvári, Symmetry sets, Approximate groups, Journal of Combinatorics and Number Theory, 2011, Volume 1, Number 3, pp. 1-6

[15] N. Hegyvári, Additive Structure of Di□erence Sets, seminar Advanced Courses in Mathematics CRM Barcelona, Thematic Seminars Chapter 4 p 253-265 2004

[16] N. Hegyvári, A. Sárközy, On Hilbert Cubes in Certain Sets, The Ramanujan J., 3, 1999, p. 303-314

[17] V. Lev, A. Sárközy: An Erdős-Fuchs type theorem for finite groups, Integers 11 2011, 487-494.

[18] L. Li, On a theorem of Schoen and Shkredov on sumsets of convex sets, arXiv preprint arXiv:1108.4382, 2011

[19] M. B. Nathanson, K. O'Bryant, B. Orosz, I. Ruzsa, and M. Silva, Binary linear forms over finite sets of integers, Acta Arith. 129 2007, 341-362

[20] P. Petridis, New proofs of Plünnecke-type estimates for product sets in groups, Combinatorica, 32, Issue 6, pp 721-733

[21] C. Pomerance, A. Sárközy, C.L. Stewart, On divisors of sums of integers, III, Pacific J. Math., 133 1988, 363-379

[22a] Ruzsa, I. Z. An analog of Freiman's theorem in groups. Asterisque, 258, 1999 323-326.

[22b] I. Z. Ruzsa: Cardinality questions about sumsets, in: Additive Combinatorics (Providence, RI, USA), CRM Proceedings and Lecture Notes, vol. 43, American Math. Soc., 2007, pp. 195–205.

[23] A. Sárközy, On squares in arithmetic progression, On squares in arithmetic progressions Annales Univ. Sci. Math. 25: pp. 267-272. 1982

[24] T. Schoen and I. Shkredov, Higher moments of convolutions, J. Number Theory 133 2013, no. 5, 1693-1737

[25] T. Schoen and I. Shkredov, On sumsets of convex sets, Comb. Prob. and Comp. Vol. 20, (5), pp 793-798

[26] I. D. Shkredov, On monochromatic solutions of some nonlinear equations in $\mathbb{Z}/p\mathbb{Z}$, Mathematical Notes 2010, Volume 88, Issue 3-4, pp 603-611

[27] I. D. Shkredov and S. Yekhanin, Sets with large additive energy and symmetric sets, Journal of Combinatorial Theory, Series A, Volume 118, Issue 3, 2011, pp 1086-1093

[28] Solymosi, J., Incidences and the spectra of graphs, seminar Advanced Courses in Mathematics CRM Barcelona, Thematic Seminars p 299-314

[29] Székely, L, Crossing numbers and hard Erdős problems in discrete geometry , Combin. Probab. Comput. 6 1997 p. 353-358.

[30] T. Tao, Hamidoune's Freiman-Kneser theorem for nonabelian groups, Tao webblog (https://terrytao.wordpress.com/2011/03/12/hamidounes-freiman-kneser-theorem-for-nonabelian-groups/)

[31] T. Tao, V.H. Vu, Additive combinatorics, p.526, Cambridge University Press, 2006

[32] L.A. Vinh: Graphs generated by Sidon sets and algebraic equations over finite fields, J. of Comb. Th., Ser B 103 (2013) 651-657

[33] L.A. Vinh: Szemerédi–Trotter type theorem and sum-product estimate in finite fields, *European J. Combin.* **32** (2011), 1177-1181.