Eötvös Loránd Tudományegyetem

Természettudományi Kar

Kiss Tibor

A SET játék, és ami mögötte van

BSc alkalmazott matematikus szakdolgozat

Témavezető:

Károlyi Gyula

Algebra és Számelmélet Tanszék

Budapest, 2018

Köszönetnyilvánítás

Szeretnék köszönetet mondani témavezetőmnek, Károlyi Gyulának, aki a konzultációk során sokat segített tudásom elmélyítésében a témával kapcsolatosan, illetve hasznos tanácsaival, megjegyzéseivel is rengeteg segítséget nyújtott abban, hogy a dolgozatom minél jobb legyen. Köszönöm a családomnak, barátaimnak és külön köszönöm Toma Zsófiának, hogy végig támogattak, a legnehezebb pillanataimban is mellettem voltak, és erőt adtak ahhoz, hogy ez a dolgozat elkészülhessen. Illetve köszönöm még középiskolai matematikatanáromnak, Molnár Juditnak, akinek áldozatos munkája nélkül valószínűleg most nem matematikával foglalkoznék.

Tartalomjegyzék

1. fejezet

Bevezetés

A SET napjaink egyik legnépszerűbb társasjátéka, ami nem is csoda, hiszen minden megvan benne, ami egy jó társasjátékhoz kell. A szabályok egyszerűek, könnyen érthetőek, a játékmenet gyors, pörgős, a játék akárhány fővel izgalmas és szórakoztató tud lenni, emellett pedig folyamatos koncentrációt és gondolkodást igényel a játékostól a siker érdekében. A SET azonban nemcsak a játék közben biztat gondolkodásra, hiszen a játék matematikai háttere rendkívül gazdag és érdekes. Magam is szeretem a SET-et, gyakran szoktam játszani, illetve az én érdeklődésem is felkeltette a játék struktúrájának matematikája, ezért választottam ezt a témát szakdolgozatomhoz.

Dolgozatomban először megismerkedünk magával a SET játékkal, majd néhány alapvető kombinatorikus tulajdonságát látjuk be a játéknak. Ezután bemutatjuk a SET kapcsolatát a véges testekkel és az affin geometriával, ebből ekvivalens tulajdonságokat adunk arra, hogy mikor alkotnak a kártyák SET-et, megismerkedünk a cap set-problémával, és megmutatjuk a SET-re a legnagyobb cap set méretét. Ezt követően számtani sorozatot nem tartalmazó halmazok méretével fogunk foglalkozni, előbb megismerjük Croot, Lev és Pach úttörő eredményét $\mathbb{Z}_4^n$-re a polinom-módszer segítségével, majd Ellenberg és Gijswijt eredményét az előbbi módszert felhasználva páratlan prím elemszámú testekre. A dolgozat végén pedig megismerkedünk Naslund és Sawin napraforgómentes halmazrendszerekre vonatkozó felső becslésével is.

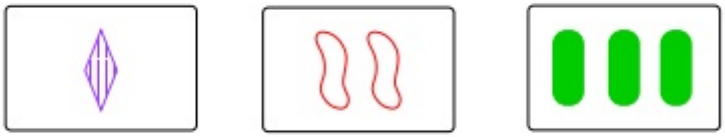
2. fejezet

A SET játék

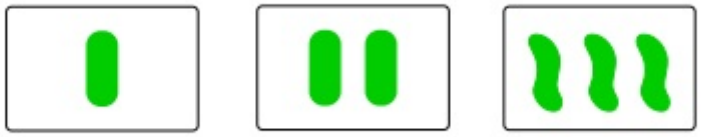
A játékot Marsha Jean Falco genetikus alkotta meg 1974-ben, mialatt német juhászkutyákon végzett kutatást az epilepszia örökletességével kapcsolatban. Hogy az egyes kutyák genetikai tulajdonságait könnyen össze tudja hasonlítani, az adatokat kártyákra jegyezte föl. Azonban bizonyos adatok sok állat esetében megegyeznek, ezért ezeket az adatokat szimbólumokkal helyettesítette. Miközben kollégáinak szemléltette a kombinációk közötti összefüggéseket, Falco felismerte, hogy remek szórakozás a különböző kombinációkat keresgélni a kártyák között, és ez adta a SET alapötletét. A játékot családja és a barátai segítségével az évek során folyamatosan fejlesztette, és a SET végül 1990-ben került piacra [1].

2.1. A SET szabályai

A játékot 2 vagy több játékos játszhatja. A kártyák mindegyike egy-egy ábrát tartalmaz szimbólumokkal. Minden kártya esetében 4 tulajdonságot veszünk figyelembe: a szimbólumok számát, színét, alakját, illetve kitöltöttségét, mindegyik esetében három lehetőség van. A kártyán lehet 1, 2 vagy 3 szimbólum, a szín lehet piros, zöld vagy kék, az alakja lehet rombusz, hullámos vagy ovális, a kitöltöttség pedig lehet teli, csíkozott vagy üres.



2.1. ábra. SET [5]



2.2. ábra. Nem SET [5]

Az asztalra lehelyezünk 12 kártyát, és a játék célja az, hogy a játékosok a asztalon lévő kártyákban minél hamarabb SET-et találjanak. SET-et három olyan kártya alkothat, amelyek a fent felsorolt tulajdonságok mindegyikére megegyeznek, vagy páronként különböznek. Például a 2.1 ábrán látható kártyák SET-et alkotnak, hiszen a lapok mind a négy tulajdonság esetén különböznek. A 2.2 ábrán látható kártyák viszont nem alkotnak SET-et, mivel kettő ovális, és egy hullámos kártya van.

A játék során aki SET-et talál, az elveheti az azt alkotó kártyákat, majd a pakliból három újabb kártya kerül ezek helyére. Ha a lent lévő 12 lapban nincs SET, akkor további 3 kártyát fordítunk fel, ekkor viszont SET esetén nem pótoljuk ki 15-re a lapok számát, hanem a megmaradó 12 kártyával folytatjuk a játékot. A játék akkor ér véget, ha elfogy a pakli, és az asztalon maradó kártyák közül már semelyik három nem alkot SET-et. A játékot az a játékos nyeri, aki a legtöbb SET-et találta.

2.2. A SET kombinatorikus tulajdonságai

Először vizsgáljuk meg a játék néhány alapvető tulajdonságát kombinatorikai eszközök segítségével.

Hány kártya van összesen?

4 tulajdonság van, és ezek mindegyike háromféle lehet, így $3^4 = 81$ kártya van a pakliban.

Hány SET van összesen?

Könnyen meggondolható, hogy ha véletlenszerűen kiválasztunk két kártyát, akkor ezekhez egyértelműen létezik egy olyan kártya, amellyel SET-et alkotnak. Ha a két kártya megegyezik egy tulajdonságban, akkor a harmadiknak is egyeznie kell az előző kettővel az adott tulajdonságnak, ha pedig különböznek, akkor a harmadiknak is különböznie kell az előző kettőtől. Ez egyben azt is jelenti, hogy bármely két kártya egyértelműen meghatároz egy SET-et, hiszen két lap ismeretében meghatározható a harmadik is. A pakliból két kártyát $\binom{81}{2} = 3240$-féleképpen tudunk kiválasztani, ezek mind meghatároznak egy-egy SET-et, azonban ekkor minden SET-et háromszor számoltunk, így összesen $\frac{3240}{3} = 1080$ SET van.

Egy lap hány SET-ben van benne?

Ha egy adott laphoz kiválasztunk egy másikat, akkor abból már egyértelműen következik, hogy melyik lap hiányzik még a SET-hez. Egy adott lap mellé 80 lapból tudunk választani, viszont ekkor minden SET-et kétszer veszünk, azaz $\frac{80}{2} = 40$ különböző SET-ben van benne egy lap.

Előfordulhat-e, hogy egy lap sem marad a játék végén?

Bár nem gyakran fordul elő ilyen eset, de lehetséges. Ehhez elég azt belátni, hogy az összes lapot feloszthatjuk diszjunkt SET-ek uniójára. Rendezzük például hármasokba a kártyákat úgy, hogy egy ilyen hármasba az azonos színű, kitöltöttségű és alakú kártyák kerüljenek. Nyilván ekkor ezek a hármasok mind különböző SET-eket fognak alkotni, és az összes kártyánkat felhasználtuk ehhez az elrendezéshez.

Előfordulhat-e, hogy három lap marad a játék végén?

Erre a kérdésre a 2.3.3 állításban adunk választ.

2.3. A SET és az affin terek kapcsolata

Mielőtt az előbbi kérdést megválaszolnánk, megmutatjuk miként reprezentálhatjuk a SET lapjait egy véges test feletti vektortér elemeiként. Ehhez először a véges testekkel, illetve azok felépítésével kell foglalkoznunk.

Egy H halmaz, mint tudjuk, akkor lesz test, ha értelmezve van rajta két művelet, egy összeadás és egy szorzás, az összeadásra H, a szorzásra pedig $H \setminus \{0\}$ Abel-csoportot alkot, illetve az összeadás disztributív a szorzásra nézve.

Ha $|H|$ véges, akkor beszélhetünk véges testről. A véges testek esetében érdemes megjegyezni, hogy minden véges test prímhatvány elemszámú, azaz ha K egy véges test, akkor létezik p prím, és $n \in \mathbb{N}$, hogy $|K| = p^n$, illetve minden q prímhatványhoz izomorfia erejéig pontosan egy véges test létezik.

Érdemes még beszélni arról, hogy az egyes műveletekre milyen a csoportstruktúrája a testnek, legyen az elemszám $q = p^n$. Ha a test prím elemszámú (azaz $n = 1$), akkor az additív csoport a modulo p maradékosztályok csoportja, ha pedig $n > 1$, akkor az additív csoport izomorf a p elemű test fölötti n dimenziós vektortér additív csoportjával. Multiplikatív szempontból pedig a nemnulla elemek ciklikus csoportot alkotnak, azaz létezik generátorelem, amelynek a hatványaiként minden további elem előáll, és a generátorelem rendje ekkor nyilván $q - 1$ [2].

A $q = p^n$ elemszámú véges testet $\mathbb{F}_q$-val jelöljük, az $\mathbb{F}_q$ fölötti n dimenziós vektorteret pedig $\mathbb{F}_q^n$-nel.

Először azt mutatjuk meg, hogyan írhatóak föl a SET lapjai a három elemű test fölötti négy dimenziós vektortér elemeiként, utána pedig azt, hogy ha három kártya SET-et alkot, az milyen összefüggést jelent a nekik megfelelő vektorok között.

2.3.1. Állítás. *A SET kártyái bijektíven megfeleltethetőek $\mathbb{F}_3^4$ elemeinek.*

Bizonyítás. A kártyákat 4 tulajdonság szerint kategorizáljuk, és mindegyik tulajdonság esetén 3 változat lehetséges. Az egyes változatoknak minden tulajdonság esetén feleltessük meg a $0, 1, 2$ számokat például a következő módon:

Szín: 0-piros, 1-zöld, 2-kék

Alak: 0-ovális, 1-hullámos, 2-rombusz

Kitöltöttség: 0-üres, 1-csíkozott, 2-teli

Szám: 0-három, 1-egy, 2-kettő

Ennek megfelelően minden kártyához hozzárendelhetünk egy 4-dimenziós vektort, amelyben mindegyik helyen $0, 1$ vagy 2 szerepel, és a számok azt mutatják, hogy a kártya milyen rendre szín, alak, kitöltöttség és számosság szempontjából. Például ahhoz a kártyához, amin egy darab kék csíkozott ovális forma van a $(2, 0, 1, 1)$ vektort rendeljük hozzá. Nyilván ezek a vektorok $\mathbb{F}_3^4$-beliek lesznek, már csak azt kell belátni, hogy ez a hozzárendelés tényleg bijektív. Az injektivitás könnyen belátható, mivel egy adott laphoz tartozó vektor a lap tartalmának kódolása, így két különböző lapnak nem lehet ugyanaz a képe. A megfeleltetés pedig visszafelé is működik, $\mathbb{F}_3^4$ bármely eleméről egyértelműen meghatározhatjuk, hogy melyik laphoz tartozik, tehát ez tényleg egy bijekció. □

2.3.2. Állítás. *Három kártya SET-et alkot akkor és csak akkor, ha a nekik megfelelő vektorok összege a nullvektor.*

Bizonyítás. Ha három kártya SET-et alkot, az azt jelenti, hogy az egyes tulajdonságokban vagy mindhárom lap megegyezik, vagy mindhárom különbözik. Ennek megfelelően a hozzájuk tartozó vektorokra is igaz, hogy a koordinátáikban rendre ugyanúgy mindhárom megegyezik, vagy mindhárom különbözik. Ha egy adott helyen különbözőek a koordináták, akkor ezek összege $0 + 1 + 2 = 0$ lesz. Ha egy helyen megegyeznek a koordináták, akkor szintén 0 lesz az összegük, mivel $\mathbb{F}_3$ feletti vektortérben vagyunk. Tehát a három vektor összege tényleg a nullvektor, ezzel az egyik irányt beláttuk.

A másik irányhoz elég azt belátni, hogy $\mathbb{F}_3$-ban három szám összege csak akkor lehet 0, ha mindhárom szám megegyezik, vagy mindhárom különbözik. Azt már beláttuk, hogy ezekben az esetekben tényleg 0 az összeg, tehát tegyük fel, hogy van három számunk, amely az előző feltételek egyikének sem felel meg, azaz tegyük fel, hogy létezik két különböző $a_1, a_2 \in \mathbb{F}_3$ szám, hogy $2a_1 + a_2 = 0$. Ez viszont nem lehetséges, hiszen azt már tudjuk, hogy három egyforma szám összege mindig 0, így a 0 helyére $3a_1$-et írva azt kapjuk, hogy

$a_1 - a_2 = 0$, ami azt jelenti, hogy $a_1 = a_2$, viszont a feltételünk az volt, hogy ez a két szám különböző. Tehát tényleg csak három egyforma vagy három különböző szám összege lehet 0, így pedig ha három vektor összege a nullvektor, akkor a hozzájuk tartozó kártyák SET-et alkotnak, így a másik irányt is sikeresen bizonyítottuk. □

Most térjünk vissza az előző szekció végén feltett kérdésre, azaz hogy maradhat-e három lap a játék végén az asztalon, és adjunk rá választ a SET előbbiekben bemutatott tulajdonságainak segítségével.

2.3.3. Állítás. *A SET játék végén nem maradhat pontosan* 3 *kártya az asztalon.*

Bizonyítás. Ha az összes kártyára vesszük a vektorok összegét, akkor a nullvektort kapjuk, hiszen az egyes tulajdonságok változatai egyenlően oszlanak el, azaz mindháromból 27-27 van. Amennyiben pontosan 3 kártya van az asztalon, akkor a többi kártya már különböző SET-ek részeként kikerült a játékból. A 2.3.2 állítás alapján tudjuk, hogy ekkor mindegyik SET esetében a vektorok összege a nullvektor, így az összes SET vektorait összeadva is a nullvektort kapjuk meg. Ennélfogva a lent lévő három lap vektorait összeadva is a nullvektort kapjuk, tehát ezek SET-et alkotnak. □

A SET és $\mathbb{F}_3^4$ kapcsolatát már beláttuk, ennek segítségével pedig azt is bemutatjuk, hogy a SET hogyan reprezentálható négydimenziós affin térként. Ehhez először definiálnunk kell, mit is értünk affin tér alatt.

2.3.4. Definíció. Legyen F egy test, V egy F feletti vektortér, X pedig pontok egy halmaza. Legyen Φ egy $X \times X$-ból V-be történő leképezés, amelyre igaz, hogy

1) tetszőleges $a \in X$ esetén a $\Phi\colon X \to V$, $\Phi_a(b) = \Phi(a, b)$ leképezés bijektív,

2) bármilyen $a, b, c \in X$ pontokra $\Phi(a, b) + \Phi(b, c) = \Phi(a, c)$.

Ekkor a Φ leképezést affin struktúrának, a (X, V, Φ) hármast pedig affin térnek nevezzük.

Egy adott V vektortér esetén például a természetes affin struktúra, hogy V-beli helyvektorok végpontjai alkotják a ponthalmazt, és két vektorhoz a különbségvektorukat rendeljük hozzá, azaz ebben az esetben $\Phi(x, y) = \mathbf{x} - \mathbf{y}$. Ekkor ha egy adott $\mathbf{w} \in V$-re vesszük Φ_w-t, akkor minden $\mathbf{x} \in V$-re a $\mathbf{w}$-től való eltérést kapjuk, tehát itt a definíciónál fogva nincs egy kitüntetett kezdőpont, mint például az origó a vektortér esetén.

2.3.5. Definíció. Legyen adott egy (X, V, Φ) affin tér, legyen $Y \subset X$ egy részhalmaz, illetve jelöljük $\widetilde{\Phi}$-vel Φ megszorítását $Y \times Y$-re. Ha létezik olyan $W \subset V$ lineáris altere V-nek, amellyel $(Y, W, \widetilde{\Phi})$ affin teret alkot, akkor Y-t affin altérnek nevezzük X-ben.

Egy V vektortér természetes affin struktúrájánál az affin altereket pontosan V lineáris alterei és ezek eltoltjai alkotják [3].

A természetes affin struktúra segítségével $\mathbb{F}_3^4$-ből is létrehozhatunk egy 4 dimenziós affin teret $\mathbb{F}_3$ fölött. A vektortér esetében már láthattuk, hogy a SET-et alkotó elemek között a vektorokra nézve milyen szép összefüggés áll fönn, az affin tér esetén pedig hasonlóan érdekes összefüggés figyelhető meg.

2.3.6. Állítás. *Három pont akkor és csak akkor alkot SET-et, ha kollineárisak az $\mathbb{F}_3^4$-hez tartozó affin térben.*

Bizonyítás. Az affin alterekről tudjuk, hogy a valódi alterek, és azok eltoltjai alkotják. $\mathbb{F}_3^4$ esetében az egydimenziós alterek háromeleműek: az $\mathbf{a} \in \mathbb{F}_3^4$ vektor által generált altérben a $\mathbf{0}, \mathbf{a}, \mathbf{2a}$ vektorok vannak benne. Tehát ha három pont kollineáris az affin térben, az azt jelenti, hogy ezek felírhatóak úgy, mint $b, a+b, 2a+b$, ahol $a, b \in \mathbb{F}_3^4$ különböző pontok az affin térben. Látható azonban, hogy $b+(a+b)+(2a+b) = 3a+3b = 0$, így a 2.3.2 állítás alapján ezek a pontok SET-et alkotnak. Tehát ha három pont kollineáris, akkor SET-et alkotnak.

Most bizonyítjuk a másik irányt is, ehhez vegyünk három pontot, amelyek SET-et alkotnak, jelöljük ezeket a, b, c-vel. Vonjuk ki mindháromból a-t, és vegyük az így kapott három elemet, azaz a $0, b-a, c-a$ hármast. Ezek szintén SET-et alkotnak, hiszen ugyanazt az elemet vontuk ki mindháromból, tehát továbbra is érvényes rájuk, hogy a megfelelő koordinátáik megegyeznek vagy különböznek. Mivel ez a hármas SET-et alkot, ezért teljesülnie kell, hogy $c-a = 2(b-a)$, a 2.3.2 állítás miatt. Viszont ez azt jelenti, hogy $0, b-a, c-a$ elemek egydimenziós alteret alkotnak $\mathbb{F}_3^4$-ben, az a, b, c hármas pedig ennek az altérnek az a-val való lineáris eltoltja. Így az a, b, c pontok az affin térben egy egyenesen vannak. □

Az egyik gyakran felmerülő kérdés a SET-tel kapcsolatban, hogy mennyi kártyát lehet legfeljebb úgy lerakni, hogy ne legyen köztük SET. Az triviális, hogy legalább 16 lap lerakható úgy, hogy ne legyen benne SET, hiszen minden tulajdonságból két változatot kiválasztva, és ezekből minden lehetséges kombinációt előállítva kapunk $2^4 = 16$ lapot, amelyekben nincs SET. Az előző állításban belátott összefüggés alapján pedig ez a kérdés ekvivalens azzal, hogy legfeljebb hány pont választható ki az $\mathbb{F}_3^4$ affin térben, hogy semelyik három ne legyen egy egyenesen. Erre a kérdésre a választ Pellegrino adta meg 1971-ben [4], még a játék létezése előtt.

A probléma természetesen kiterjeszthető általánosan is az $\mathbb{F}_3^n$ affin terekre, azaz azt keressük, hogy mekkora a legnagyobb olyan $\mathbb{F}_3^n$-beli részhalmaz mérete, amely nem tartalmaz egyenest. Ez az általános kérdés az $\mathbb{F}_3^n$-ekre a cap set-probléma, amellyel az elmúlt évtizedek során számos matematikus foglalkozott. 2016-ban Ellenberg és Gijswijt mutatta meg, hogy a legnagyobb egyenesmentes halmaz mérete legfeljebb $O(2{,}756^n)$ [8], ezzel az eredménnyel a 3.2 szakaszban fogunk bővebben foglalkozni.

Mielőtt belátnánk, hogy mekkora a legnagyobb egyenesmentes halmaz $\mathbb{F}_3^4$-ben, szükségünk van a legnagyobb ilyen halmazok méretére a kisebb dimenziókban.

2.3.7. Állítás. *$\mathbb{F}_3^2$-ben a legnagyobb egyenesmentes halmaz 4 pontból áll.*

Bizonyítás. Könnyen látható, hogy van négyelemű egyenesmentes halmaz, vegyük csak egyszerűen $\{0,1\}^2$ elemeit. Tegyük fel, hogy van ötelemű ilyen halmaz is. Az öt pontból semelyik három nem lehet egy egyenesen, viszont tudjuk, hogy bármely két pont meghatároz egy egyenest, így ez az öt pont 10 különböző egyenest kell meghatározzon. Kiszámolható, hogy $\mathbb{F}_3^2$-ben összesen 12 különböző egyenes van, ezeket 4 darab három elemű csoportba oszthatjuk úgy, hogy az egy csoportba tartozó egyenesek párhuzamosak. Ez azt jelenti, hogy az öt pontunk által meghatározott egyenesek között kell, hogy legyen 3 párhuzamos, azaz van három pontpár, amelyek párhuzamos egyeneseket határoznak meg. Viszont csak 5 pontunk van, tehát van olyan pont, amely két egyenesen is rajta kell legyen. Ekkor van két egyenesünk, amelyek párhuzamosak, és van közös pontjuk, tehát ez a két egyenes egybeesik, vagyis a halmazunk mégis tartalmaz egyenest. □

2.3.8. Állítás. *$\mathbb{F}_3^3$-ban a legnagyobb egyenesmentes halmaz 9 pontból áll.*

Bizonyítás. [[5] alapján] Mutassuk meg először, hogy $\mathbb{F}_3^3$-ban 9 elemű egyenesmentes halmaz. Vegyük a

$$H = \{(0,0,0),(0,0,2),(0,2,0),(0,2,2),(1,1,1),(2,0,1),(2,1,0),(2,1,2),(2,2,1)\}$$

halmazt, ez 9 elemű, és semelyik 3 pont sem kollineáris.

Tegyük fel, hogy létezik 10 elemű egyenesmentes halmaz. $\mathbb{F}_3^3$ felbontható 3 párhuzamos sík uniójára. 2.3.7 alapján egyik sík sem tartalmazhatja 4-nél több pontját a halmaznak, így a legkevesebb pontot tartalmazó síkon kettő vagy három pont van rajta. Jelöljük a legkevesebb pontot tartalmazó síkot H-val, nyilván az előbbiek alapján legalább hét olyan pontja van a halmaznak, ami nincs rajta H-n.

Legyen a és b két pontja a halmaznak, ami rajta van H-n. 4 olyan síkja van $\mathbb{F}_3^3$-nak, mely tartalmazza a-t és b-t is, legyenek ezek H, M_1, M_2 és M_3. Mivel van legalább hét olyan pontja a halmaznak, amelyek nem H-beliek, így ezek a pontok az M_1, M_2, M_3 valamelyikén vannak rajta. A skatulyaelv szerint viszont ekkor lesz olyan M_i sík, ami a hétből három pontot is tartalmaz, azaz összesen legalább öt pontját tartalmazza a halmazunknak, tehát a halmazunk mégis tartalmaz egyenest. □

A 2, illetve 3 dimenzióban alkalmazott egyszerű módszerek sajnos 4 dimenzióra már nem elég jók, ezért egy másfajta megközelítésre van szükség. A bizonyításhoz szükség lesz a következő állításra.

2.3.9. Állítás. *Legyen $n > k \geq 0$. Ha adott egy k-dimenziós affin altér $\mathbb{F}_3^n$-ben, akkor azoknak a hipersíkoknak a száma, amelyek tartalmazzák ezt az alteret*

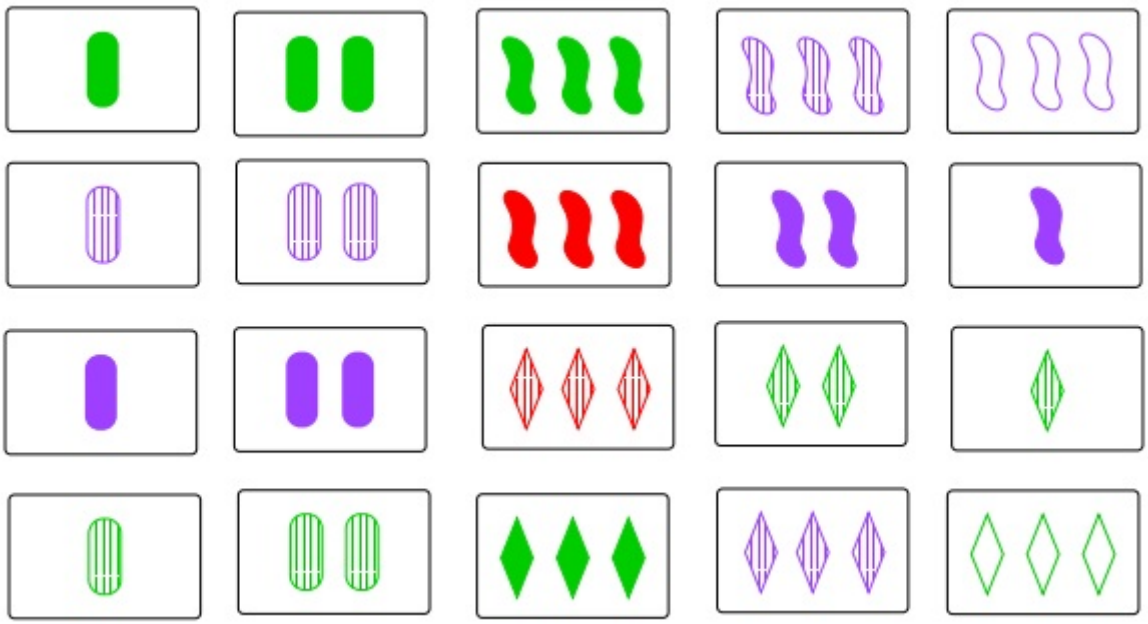
$$\frac{3^{n-k}-1}{2}.$$

Bizonyítás. [[5] alapján] Legyen K egy k-dimenziós altér, amely tartalmazza az origót. Ha vesszük az

$$\mathbb{F}_3^n \to \mathbb{F}_3^n / K \cong \mathbb{F}_3^{n-k}$$

leképezést, akkor azt láthatjuk, hogy bijekció képezhető $\mathbb{F}_3^n$ K-t tartalmazó hipersíkjai, és $\mathbb{F}_3^{n-k}$ origót tartalmazó hipersíkjai között.

Minden, az origót tartalmazó hipersíkot meghatároz egy nemnulla normálvektor, és minden hipersíkot pontosan két normálvektor határoz meg, tehát feleannyi hipersík van, mint nemnulla vektor. Mivel a nemnulla vektorok száma $3^{n-k} - 1$, így összesen $\frac{3^{n-k}-1}{2}$ hipersík tartalmazza az origót. □



2.3. ábra. 20 kártya SET nélkül [5]

2.3.10. Állítás. *$\mathbb{F}_3^4$-ben a maximális egyenesmentes halmaz* 20 *pontból áll.*

Bizonyítás. [[5] alapján] A 2.3 ábrán láthatunk 20 lapot, amelyek között nincs SET, tehát ezzel megmutattuk, hogy van 20 elemű egyenesmentes halmaz. Tegyük fel, hogy létezik 21 elemű egyenesmentes halmaz, jelöljük ezt C-vel. Ha a terünket felbontjuk 3 diszjunkt hipersík uniójára, akkor jelöljük x_{ijk}-val azoknak a felbontásoknak a számát, ahol az egyes hipersíkok C-nek pontosan i, j, illetve k elemét tartalmazzák. 2.3.8 alapján tudjuk, hogy a maximális egyenesmentes halmaz $\mathbb{F}_3^3$-ban 9 pontból áll, ezért összesen 7 különböző i, j, k hármas jelenhet meg a hipersíkokra bontásnál:

$$\{9,9,3\},\{9,8,4\},\{9,7,5\},\{9,6,6\},\{8,8,5\},\{8,7,6\},\{7,7,7\}$$

$\mathbb{F}_3^4$-et pontosan 40-féleképpen tudjuk hipersíkokra bontani, mivel az origó ennyi különböző egyenesen van rajta, ezáltal ennyiféleképpen tudunk normálvektort választani a hipersíkokhoz. Ez azt jelenti, hogy

$$x_{993}+x_{984}+x_{975}+x_{966}+x_{885}+x_{876}+x_{777}=40 \tag{2.1}$$

Ahhoz, hogy egy másik egyenletet is kapjunk az x_{ijk}-kra, számoljuk össze azt, hogy egy tetszőlegesen kiválasztott C-beli pontpárt hány különböző hipersík tartalmaz. 2.3.9 alapján tudjuk, hogy egy adott pontpárt mindig 13 különböző hipersík tartalmaz, és $\binom{21}{2}$-féleképpen választhatunk ki egy tetszőleges pontpárt C-ből, így összesen $13\cdot\binom{21}{2}=2730$ ilyen hipersíkunk van. C különböző felbontásaira az egy hipersíkba eső ponthalmazokra összesen

$$\left[\binom{9}{2}+\binom{9}{2}+\binom{3}{2}\right]x_{993}+\cdots+\left[\binom{7}{2}+\binom{7}{2}+\binom{7}{2}\right]x_{777}.$$

ilyen hipersík van, és ebből meg is kapjuk a második egyenletünket:

$$75x_{993}+70x_{984}+67x_{975}+66x_{966}+66x_{885}+64x_{876}+63_{777}=2730. \tag{2.2}$$

Még egy egyenletet kaphatunk, ha most azt számoljuk meg, hogy egy tetszőlegesen kiválasztott $x,y,z\in C$ ponthármast hány különböző hipersík tartalmaz. Fontos megjegyezni, hogy ezek a ponthármasok nem lehetnek kollineárisak, hiszen C-ről feltettük, hogy egyenesmentes. 2.3.9 alapján tudjuk, hogy egy adott nem kollineáris számhármast 4 különböző hipersík tartalmaz, így azt kapjuk, hogy $4\cdot\binom{21}{3}=5320$ ilyen hipersík van. A második egyenletnél már látott leszámlálást alkalmazva azt kapjuk, hogy

$$169x_{993}+144x_{984}+129x_{975}+124x_{966}+122x_{885}+111x_{876}+105x_{777}=5320. \tag{2.3}$$

Van három egyenletünk, hét változóval, tehát végtelen sok megoldás létezik, viszont szerencsére minket csak a nemnegatív egész megoldások érdekelnek. Ha 2.1 693-szorosát hozzáadjuk 2.3 háromszorosához, és ebből kivonjuk 2.2 hatszorosát, akkor azt kapjuk, hogy

$$5x_{984}+8x_{975}+9x_{966}+3x_{885}+2x_{876}=0.$$

Ennek az egyetlen nemnegatív megoldása, hogy $x_{984}=x_{975}=x_{966}=x_{885}=x_{876}=0$. Viszont ha a 2.2 egyenletből kivonjuk 2.1 63-szorosát,

$$12x_{993} + 7x_{984} + 4x_{975} + 3x_{966} + 3x_{885} + x_{876} = 210.$$

Ebből következik, hogy $12x_{993} = 210$, ez viszont ellentmond annak, hogy x_{993} egész. □

Fontos megemlíteni, hogy ezeknek az eredményeknek a segítségével egyre jobb alsó becslést adhatunk meg a legnagyobb egyenesmentes halmaz méretére $\mathbb{F}_3^n$-ben nagyobb n-ekre. 2^n triviális alsó korlát a legnagyobb cap set méretére n dimenzióban, hiszen ha vesszük a $\{0,1\}^n$ halmazt, akkor nyilván ebben nincs egyenes, azonban láthattuk, hogy ez a becslés csak 2 dimenzióban pontos, magasabb dimenziókra már nem. Olyan módon viszont javítható az alsó becslés, ha egy adott k dimenzióra kapott maximális érték k-adik gyökének n-edik hatványával becsülünk alulról, például a mi eseteinkben $(\sqrt[3]{9})^n = 2{,}08^n$-nel, illetve $(\sqrt[4]{20})^n = 2{,}115^n$-nel. A jelenleg ismert legjobb alsó becslés nagy n-ekre $2{,}217^n$, ezt a becslést Edel adta [6].

2.4. Számtani sorozatok a SET-ben

2.4.1. Definíció. Legyen G egy Abel-csoport, $n \geq 3$ egész, és legyenek $a_1, \ldots, a_n$ számok olyanok, hogy $a_i \in G$ minden $1 \leq i \leq n$ esetén, és $a_i \neq a_j$, ha $i \neq j$.

Ekkor az $a_1, \ldots, a_n$ számok számtani sorozatot alkotnak G-ben, ha minden $2 \leq i \leq n-1$ esetén teljesül, hogy $a_{i-1} + a_{i+1} = a_i + a_i$.

Ha a sorozatunk k elemből áll, akkor azt k hosszú sorozatnak nevezzük. A dolgozat további részében főként három hosszú számtani sorozatokkal fogunk foglalkozni.

2.4.2. Állítás. *Három kártya SET-et alkot akkor és csak akkor, ha a nekik megfelelő $\mathbb{F}_3^4$-beli elemek számtani sorozatot alkotnak.*

Bizonyítás. Az állítást a 2.3.2 állítás segítségével fogjuk belátni.

Jelöljük a SET-et alkotó kártyáknak megfelelő elemeket c_1, c_2, c_3-mal. Tudjuk, hogy $c_1 + c_2 + c_3 = 0$, ebből pedig $c_1 + c_3 = -c_2$. Mivel a három elemű test fölött vagyunk, ezért $-c_2 = 2c_2$, ez pedig azt jelenti, hogy c_1, c_2 és c_3 számtani sorozatot alkotnak.

A másik irány is hasonlóan látható be, c_1, c_2, c_3 számtani sorozatot alkotnak, azaz $c_1 + c_3 = 2c_2$. Adjunk hozzá mindkét oldalhoz c_2-t, így $c_1 + c_2 + c_3 = 3c_2 = 0$, azaz c_1, c_2 és c_3 SET-et alkot. □

A számtani sorozatokkal újabb ekvivalens tulajdonságot kaptunk arra, hogy három kártya mikor alkot SET-et, és így összességében azt is beláttuk, hogy $\mathbb{F}_3^4$-en ekvivalensek azok a tulajdonságok, hogy három pont kollineáris, három pont számtani sorozatot alkot, illetve hogy három pont összege az origó. Ez nem csak 4 dimenzióban áll fönn, könnyen belátható,

hogy ezek a tulajdonságok ekvivalensek lesznek $\mathbb{F}_3^n$-re bármilyen n esetén. Ez általános n-re is ugyanúgy bizonyítható, ahogy a 2.3.6 és a 2.4.2 állítások esetén 4 dimenzióra beláttuk.

3. fejezet

Három hosszú számtani sorozatot nem tartalmazó halmazok

Azt már a 2.3.10 állításban beláttuk, hogy $\mathbb{F}_3^4$-ben legfeljebb 20 lehet az elemszáma egy olyan halmaznak, amely nem tartalmaz egyenest, és ezáltal három hosszú számtani sorozatot sem. Fölvetődik azonban a kérdés, hogy mekkora lehet a maximális elemszáma egy számtani sorozatot nem tartalmazó halmaznak, illetve mekkora az az elemszám, amely fölött egy részhalmaz biztosan tartalmaz számtani sorozatot, ha magasabb dimenziókra tekintjük ezt a problémát, vagy akár ha más prím elemszámú testek esetét vizsgáljuk.

Roth mutatta meg először, hogy ha egy $A \subseteq \{1, 2, \ldots, N\}$ halmaz nem tartalmaz három elemet, amelyek számtani sorozatot alkotnak, akkor $|A| = o(N)$, kicsit pontosabban $|A| = O(N/\log\log N)$, és azóta a számtani sorozatot nem tartalmazó halmazok maximális méretének becslése az additív kombinatorika egyik központi problémájává vált. Könnyen látható, hogy Roth problémája gyakorlatilag ekvivalens azzal, mintha a $\mathbb{Z}_N$ ciklikus csoportban próbálnánk becsülni a legnagyobb, számtani sorozatoktól mentes részhalmaz méretét. Így érdemes vizsgálni a kérdést más Abel-csoportok esetén is.

Páratlan rendű Abel-csoportokra először Brown és Buhler látta be, hogy a legnagyobb ilyen részhalmaz egy G csoport esetén $o(|G|)$ nagyságú, majd Meshulam megmutatta, hogy $\mathbb{Z}_m^n$-re a legnagyobb sorozatmentes részhalmaz mérete legfeljebb $2m^n/n$. Bateman és Katz pedig bebizonyították, hogy $\mathbb{Z}_3^n$-re a felső korlát $O(3^n/n^{1+\epsilon})$, ahol $\epsilon > 0$ abszolút konstans.

A páros rendű Abel-csoportokkal csak az utóbbi években kezdtek el foglalkozni, $\mathbb{Z}_4^n$-re Sanders bizonyította, hogy a legnagyobb számtani sorozatot nem tartalmazó részhalmaz mérete $O(4^n/n(\log n)^\epsilon)$, ahol $\epsilon > 0$ abszolút konstans. Ezt az eredményt sikerült 2016-ban áttörést jelentő módon javítani: Croot, Lev és Pach eredménye [7] szerint $\mathbb{Z}_4^n$-re a legnagyobb számtani sorozatot nem tartalmazó részhalmaz mérete kisebb, mint $3{,}62^n$.

Módszerük alapvető jelentősége, hogy a korábbi becslésekhez használt Fourier-analízis és sűrűségnövelő módszer helyett teljesen más megközelítést alkalmazva, a polinom-módszert használták tételük bizonyításához. A polinom-módszer lényege, hogy úgy próbálunk becslést, korlátot adni halmazok elemszámára, hogy megmutatjuk, hogy létezik olyan nemnulla polinom, amely eltűnik az adott halmazon, és ekkor ennek a polinomnak a lehetséges legnagyobb foka egy felső becslést ad a halmaz méretére. A cikk hatására több hasonlóan fontos eredmény született: Ellenberg és Gijswijt az általuk alkalmazott módszert felhasználva mutatta meg, hogy bármely páratlan q prímre $\mathbb{F}_q^n$-ben a legnagyobb számtani sorozatot nem tartalmazó részhalmaz mérete $O(c^n)$, ahol $c < q$ [8], illetve Naslund és Sawin a módszer közvetlen alkalmazásával oldotta meg az Erdős-Szemerédi-féle napraforgó-sejtést [10].

Ebben a fejezetben először Croot, Lev és Pach tételével fogunk foglalkozni, majd Ellenberg és Gijswijt tételét fogjuk belátni páratlan prím elemszámú testekre, illetve megmutatjuk, hogy $\mathbb{F}_3^n$ esetén mekkora a felső korlát a számtani sorozatot nem tartalmazó halmazok méretére. A fejezethez az eredeti cikkek mellett Pach Péter Pál cikkét [9] is felhasználtam, amely e két eredményt foglalja össze.

3.1. Croot, Lev és Pach tétele

A bizonyítás alapja, és a módszer alapötlete a következő lemma:

3.1.1. Lemma. *Legyenek $n \geq 1$ és $d \geq 0$ egészek, P egy n-változós legfeljebb d-edfokú multilineáris polinom $\mathbb{F}$ test felett, $A \subset \mathbb{F}^n$ pedig egy halmaz, amire teljesül, hogy $|A| > 2\sum_{i=0}^{\lfloor \frac{d}{2} \rfloor} \binom{n}{i}$. Ha $P(a-b) = 0$ teljesül bármilyen $a, b \in A \quad (a \neq b)$ esetén, akkor $P(0) = 0$.*

Bizonyítás. [[7], [9] alapján] Tekintsük a $P(a-b)$-t úgy, mint egy $2n$-változós polinomot, a_i, b_i változókkal. Mivel P $\mathbb{F}$ feletti polinom, így ennek megfelelően ez is $\mathbb{F}$ feletti lesz, illetve mivel P-nek a foka legfeljebb d, így ez is legfeljebb d-edfokú lehet.

Csoportosítsuk a monomokat oly módon, hogy először vesszük azokat, amelyekben az a_i-kből legfeljebb $\frac{d}{2}$ van, és ezeket aszerint rendezzük, hogy mely a_i-k szerepelnek bennük pontosan. Az előző feltétel miatt nyilván a többi monomban b_i-kből van legfeljebb $\frac{d}{2}$, és ezeket is aszerint csoportosítjuk, hogy mely b_i-k jelennek meg az adott tagban. Például legyen $n = 4$ és $d = 3$, a polinomunk pedig $P(x) = x_1x_3x_4 + x_1x_2 + x_2x_4 + x_3 + 1$. Ekkor $P(a-b) = (a_1-b_1)(a_3-b_3)(a_4-b_4) + (a_1-b_1)(a_2-b_2) + (a_2-b_2)(a_4-b_4) + (a_3-b_3) + 1$. Ha erre elvégezzük a csoportosítást, azt kapjuk, hogy

$$P(a-b) = 1 \cdot (-b_1b_3b_4 + b_1b_2 + b_2b_4 - b_3 + 1) + a_1(b_3b_4 - b_2) + a_2(-b_1 - b_4) +$$
$$+a_3(b_1b_4 + 1) + a_4(b_1b_3 - b_2) + (a_1a_3a_4 + a_1a_2 + a_2a_4) \cdot 1 + (-a_3a_4)b_1 +$$
$$+0 \cdot b_2 + (-a_1a_4)b_3 + (-a_1a_3)b_4.$$

Az előállításra gondolhatunk úgy is, mintha a polinomot egy a-tól, és egy b-től függő vektor skaláris szorzataként adnánk meg:

$$P(a-b) = u(a)v(b),$$

ahol $u(a)$ és $v(b)$ a következők:

$$u(a) = \{1, a_1, a_2, a_3, a_4, a_1a_3a_4 + a_1a_2 + a_2a_4, -a_3a_4, 0, -a_1a_4, -a_1a_3\}$$
$$v(b) = \{-b_1b_3b_4 + b_1b_2 + b_2b_4 - b_3 + 1, b_3b_4 - b_2, -b_1 - b_4, b_1b_4 + 1, b_1b_3 - b_2, 1, b_1, b_2, b_3, b_4\}$$

Az általános esetben az $u(a)$ vektor első része csak az a_i-kből előálló, legfeljebb $\frac{d}{2}$-fokú monomokból fog állni, és a $v(b)$ vektor második része is hasonlóan a b_i-kből kialakítható maximum $\frac{d}{2}$-fokú monomokat tartalmazza, $u(a)$ második része és $v(b)$ első része pedig a megfelelő monomokhoz rendelt, $\frac{d}{2}$-nél magasabb fokúakból álló csoportokat.

Az általános esetben a $P(a-b) = u(a)v(b)$ felírásból a fentiek alapján adódik, hogy $u(a)$ és $v(b)$ $\mathbb{F}^{2m}$-beliek, ahol $m = \sum_{i=0}^{\lfloor \frac{d}{2} \rfloor} \binom{n}{i}$, hiszen akár az a_i-k, akár a b_i-k esetén ennyi különböző n-változós, minden változóban legfeljebb elsőfokú, legfeljebb $\frac{d}{2}$-fokú monom létezik.

Tegyük föl, hogy nem igaz az állítás, azaz $\forall a, b \in A$ $(a \neq b)$ esetén $P(a-b) = 0$, de $P(0) \neq 0$. A $P(a-b) = u(a)v(b)$ felbontást tekintve, ez azt jelenti, hogy az $u(a)$ és $v(b)$ vektorok akkor és csak akkor merőlegesek, ha $a \neq b$. Ebből az következik, hogy az $u(a)$ vektorok lineárisan függetlenek, hiszen ha $\exists a_0$, ami esetén $u(a_0)$ lineárisan függ a többi $u(a)$ vektortól, azaz $u(a_0) = \sum_{a \in A, a \neq a_0} \alpha_a u(a)$, és létezik $a \in A$, amire $\alpha_a \neq 0$, akkor ezt az egészet a $v(a_0)$ vektorral felszorozva skalárisan a bal oldalon valamilyen nullától különböző érték lesz, míg a jobb oldalon nullát kapunk. Mivel $u(a) \in \mathbb{F}^{2m}$ bármely $a \in A$ esetén, és ezek az $u(a)$-k lineárisan független rendszert alkotnak, ezért az $\{u(a) \colon a \in A\}$ halmaz elemszáma legfeljebb $2m$ lehet, ebből pedig az is következik, hogy $|A| \leq 2m$. Azonban A-t úgy definiáltuk, hogy $2m$-nél több elemű, azaz ellentmondásra jutottunk. $\square$

Ha $\mathbb{Z}_4^n$-ben vesszük az elemek involúcióit, azaz minden $g \in \mathbb{Z}_4^n$ esetén vesszük $2g$-t, az involúciók az $F = \{0, 2\}^n$ részcsoportot alkotják $\mathbb{Z}_4^n$-ben, és F izomorf az $\mathbb{F}_2^n$ vektortérrel. Tekintsük $\mathbb{Z}_4^n$ F szerinti mellékosztályait, ezek mindegyike reprezentálható egy $\{0, 1\}^n$ vektor segítségével. Ha van egy A halmazunk, amely nem tartalmaz három elemű számtani

sorozatot, az azt jelenti, hogy nem léteznek olyan, páronként különböző $a, b, c \in \mathbb{Z}_4^n$ elemek, amelyek az $a + c = 2b$ egyenletet kielégítik. Az, hogy a b elem melyik mellékosztályban van, egyértelműen meghatározza, hogy mi lesz a $2b$ értéke, illetve tudjuk, hogy $2b \in F$. Ez pedig azt jelenti, hogy a és c egy mellékosztályban vannak, hiszen $a + c \in F$.

A következő állításunkhoz bevezetjük a bináris entrópia fügvényt, amelyet H-val jelölünk:

$$H(x) = -x \log_2 x - (1 - x) \log_2(1 - x), \quad x \in (0, 1).$$

A bináris entrópia függvényt alapvetően az információelméletben alkalmazzák a Bernoulli-folyamat entrópiájának mérésére, magyarán ha van egy X Bernoulli-eloszlású változónk, ahol $P(X = 1) = p$, akkor $H(p)$ adja meg annak a mértékét, hogy mennyire bizonytalan az X kimenetele. Ennek megfelelően ha $p = 0$ vagy $p = 1$, azaz a kimenetel biztos, akkor H értéke 0, ha pedig $p = \frac{1}{2}$, vagyis mindkét kimenetelnek ugyanakkora az esélye, akkor veszi fel H a maximumát, $H(\frac{1}{2}) = 1$ [11].

A bináris entrópia függvény segítségével a következő módon adhatunk becslést a binomiális együtthatók összegére:

$$\sum_{i=0}^{z} \binom{n}{i} < 2^{nH(z/n)}. \tag{3.1}$$

3.1.2. Állítás. *Tegyük fel, hogy $n \geq 1$ és $A \subseteq \mathbb{Z}_4^n$ nem tartalmaz számtani sorozatot. Ekkor minden $0 < \epsilon < \frac{1}{4}$ esetén azoknak az F szerinti mellékosztályoknak a száma, amelyek legalább $2^{nH(1/2-\epsilon)+1}$ A-beli elemet tartalmaznak, legfeljebb $2^{nH(2\epsilon)}$.*

Bizonyítás. [[7] alapján] Legyen $\mathcal{R}$ azoknak az F szerinti mellékosztályoknak a halmaza, amelyek legalább $2^{nH(1/2-\epsilon)+1}$ A-beli elemet tartalmaznak, és minden $R \in \mathcal{R}$ esetén legyen $A_R = A \cap R$, azaz az egyazon R mellékosztályba tartozó A-beli elemek halmaza. Ekkor $\bigcup_{R \in \mathcal{R}} A_R \subseteq A$, ahol az unió nyilván diszjunkt, hiszen egy elem csak egy mellékosztályhoz tartozhat, és az R-ekre vonatkozó feltétel miatt $|A_R| \geq 2^{nH(1/2-\epsilon)+1}$ minden $R \in \mathcal{R}$ esetén.

Vezessük be az alábbi nem teljesen sztenderd jelöléseket, ha $S \subseteq \mathbb{Z}_4^n$, legyen

$$2 \cdot S \colon = \{s + s^* \colon s, s^* \in S, s \neq s^*\}, \quad 2 * S \colon = \{2s \colon s \in S\}.$$

Ekkor vegyük a következő halmazokat:

$$B \colon = \bigcup_{R \in \mathcal{R}} (2 \cdot A_R) \subseteq F, \quad C \colon = \bigcup_{R \in \mathcal{R}} (2 * R) \subseteq F.$$

Mivel A nem tartalmaz három elemű számtani sorozatot, ezért B és C diszjunktak kell legyenek, hiszen ha valamilyen $r \in R$ esetén $2r \in A_R$, akkor minden $a \in r + F$ esetén

$2a = 2r \in 2 \cdot A_R \subseteq A$. Továbbá minden $R \in \mathcal{R}$ esetén a $2 * R$ halmaz egyelemű, és ezek a halmazok különböző R-ekre páronként különbözőek, így $|\mathcal{R}| = |C|$

Legyen $d = n - \lceil 2\epsilon n \rceil$, ekkor 3.1 segítségével a következőt kapjuk:

$$2\sum_{i=0}^{d/2} \binom{n}{i} \leq 2^{nH(1/2-\epsilon)+1} \leq |A_R|, \quad R \in \mathcal{R}. \tag{3.2}$$

Legyen $\overline{C} := F \setminus C$, és tegyük fel, hogy $|\mathcal{R}| \geq 2^{nH(2\epsilon)}$, vagyis hogy az állításunk nem teljesül. Ekkor a 3.1 becslést használva:

$$\sum_{i=0}^{d} \binom{n}{i} = 2^n - \sum_{i=0}^{\lceil 2\epsilon n \rceil - 1} \binom{n}{i} > 2^n - 2^{nH(2\epsilon)} \geq 2^n - |\mathcal{R}| = 2^n - |C| = |\overline{C}|.$$

Mivel $\mathbb{F}_2$ elemei idempotensek, ezért minden $\mathbb{F}_2$ feletti n-változós polinomhoz létezik olyan $\mathbb{F}_2$ feletti n-változós multilineáris polinom, hogy a két polinom polinomfüggvényei megegyeznek. A bizonyítás szempontjából a polinomokhoz tartozó polinomfüggvények a lényegesek, ebből kifolyólag a továbbiakban csak a multilineáris polinomokkal fogunk foglalkozni $\mathbb{F}_2$ felett.

A $\mathbb{F}_2$ feletti n-változós legfeljebb d-fokú multilineáris polinomok vektorterének dimenziója $\sum_{i=0}^{d} \binom{n}{i}$, illetve az összes $\mathbb{F}_2$ feletti n-változós multilineáris polinom vektorterének dimenziója megegyezik az $\mathbb{F}_2^n$-ből $\mathbb{F}_2$-be képező függvények vektorterének dimenziójával, és ebből következik, hogy minden nemnulla polinom megfeleltethető egy nemnulla függvénynek.

Ha tekintjük az F és $\mathbb{F}_2$ közötti izomorfizmust, és a B és C halmazokra úgy tekintünk, mint $\mathbb{F}_2$ részhalmazaira, azt láthatjuk, hogy az összes $\mathbb{F}_2$ feletti n-változós multilineáris polinomfüggvény vektorterének dimenziója meghaladja a $\overline{C}$-ből $\mathbb{F}_2$-be képező függvények vektorterének dimenzióját. Így ha minden polinomfüggvényhez hozzárendeljük a megfelelő függvényt, akkor lesz olyan függvény, amelyet több polinomfüggvényhez is hozzá kell rendelnünk. Emiatt létezik olyan nemnulla n-változós, legfeljebb d-fokú, multilineáris $P \in \mathbb{F}_2[x_1, \ldots, x_n]$ polinom, ami eltűnik $\overline{C}$-n. P nyilván a $B \subseteq \overline{C}$ halmazon is eltűnik, és ennélfogva $2 \cdot A_R$-en is minden $R \in \mathcal{R}$ esetén. Ha rögzítünk egy $r \in R$ elemet, akkor a $P(2r + x)$ polinom eltűnik a $2 \cdot (A_R - r)$ halmazokon, minden $R \in \mathcal{R}$ esetén. A 3.2 alapján alkalmazhatjuk a 3.1.1 lemmát, így $P(2r) = 0$ teljesül bármilyen r-re, ez pedig azt jelenti, hogy a P eltűnik a $2 * R$ halmazokon minden $R \in \mathcal{R}$ mellékosztályra. Ebből pedig az következik, hogy P az egész C-n eltűnik. A P polinom tehát eltűnik mind $\overline{C}$-n, mind C-n, azaz P $\mathbb{F}_2^n$ minden elemén eltűnik, így P csak a nullpolinom lehet, ami ellentmondás, hiszen feltettük P-ről, hogy egy nemnulla polinom. Mivel ellentmondásra jutottunk, ez azt jelenti, hogy $|\mathcal{R}| < 2^{nH(2\epsilon)}$, és ezzel igazoltuk az állítást. $\square$

3.1.3. Tétel. *Ha $n \geq 1$ és $A \subseteq \mathbb{Z}_4^n$ nem tartalmaz három hosszú számtani sorozatot, és*

$$\gamma \colon = \max\left\{\frac{1}{2}(H(\frac{1}{2}-\epsilon)+H(2\epsilon))\colon 0<\epsilon<\frac{1}{4}\right\} \approx 0{,}926,$$

akkor $|A| < 4^{\gamma n} \approx 3{,}62^n$.

Bizonyítás. [[7] alapján] Minden $x \geq 0$-ra jelölje $N(x)$ azon F szerinti mellékosztályok számát, amelyek legalább x A-beli elemet tartalmaznak. Mivel a mellékosztályok 2^n eleműek, ezért $N(x) = 0$, ha $x > 2^n$. Legyen R egy F szerinti mellékosztály, és legyen $N_R(x)$ olyan függvény, hogy minden $x \geq 0$-ra $N_R(x) = 1$, ha R legalább x A-beli elemet tartalmaz, és $N_R(x) = 0$ egyébként. Ha egy R mellékosztály pontosan k A-beli elemet tartalmaz, akkor nyilván $N_R(x) = 1$ a $[0, k]$ intervallumon, és mindenhol máshol $N_R(x) = 0$, ez pedig azt jelenti, hogy ha integráljuk $N_R(x)$-et a $[0, 2^n]$ intervallumon, akkor az integrál értékeként k-t kapjuk. Könnyen látható, hogy minden R mellékosztályt tekintve $N(x)$ előáll az $N_R(x)$-ek összegeként, tehát $N(x)$ integráljának értéke egy adott intervallumra szintén előáll az $N_R(x)$-ek ugyanazon intervallumon vett integráljainak összegeként. Tudjuk, hogy A tetszőleges eleme pontosan egy F szerinti mellékosztályban lehet benne, így az A halmaz elemszámát megadhatjuk úgy, mint

$$|A| = \int_0^{2^{n+1}} N(x)dx. \tag{3.3}$$

Ezután kettébontjuk az integrálunkat, és külön becsüljük az értékét a $[0, 2^{nH(1/4)+1}]$ és a $[2^{nH(1/4)+1}, 2^{n+1}]$ intervallumokon.

Mivel 2^n mellékosztály van, ezért $N(x) \leq 2^n$, illetve $H(1/4) + 1 < 2\gamma$ és így

$$\int_0^{2^{nH(1/4)+1}} N(x)dx \leq 2^{n(H(1/4)+1)+1} < 2 \cdot 4^{\gamma n}. \tag{3.4}$$

A másik résznél helyettesítéses integrálást alkalmazunk, ott az $x = 2^{nH(1/2-\epsilon)+1}$ helyettesítéssel azt kapjuk, hogy

$$\int_{2^{nH(1/4)+1}}^{2^{n+1}} N(x)dx = n \int_0^{1/4} 2^{nH(1/2-\epsilon)+1} N(2^{nH(1/2-\epsilon)+1}) \log\frac{1/2+\epsilon}{1/2-\epsilon} d\epsilon. \tag{3.5}$$

Alkalmazzuk a 3.1.2 állítást, és ennek segítségével adjunk becslést a helyettesítéssel kapott integrálra:

$$2n \int_0^{1/4} 2^{n(H(1/2-\epsilon)+H(2\epsilon)} \log \frac{1/2+\epsilon}{1/2-\epsilon} d\epsilon \leq 2n \cdot 4^{\gamma n} \int_0^{1/4} \log \frac{1/2+\epsilon}{1/2-\epsilon} d\epsilon < n \cdot 4^{\gamma n}. \tag{3.6}$$

Ha a 3.4 és a 3.6 becslések eredményeit összegezzük, azt kapjuk, hogy $|A| < (n+2)4^{\gamma n}$. Már csak egy lépés van hátra, azt belátni azt, hogy az egyenlőtlenség az $(n+2)$-es szorzó nélkül is igaz. Ehhez az A halmaz önmagával vett direktszorzatait fogjuk felhasználni: $k \geq 1$-re az $A \times \ldots \times A \subseteq \mathbb{Z}_4^{kn}$ halmaz nem tartalmaz három hosszú számtani sorozatot, és a fenti lépéseket elvégezve azt kapjuk, hogy

$$|A|^k < (kn+2)4^{\gamma kn}.$$

Vonjunk k-dik gyököt mindkét oldalból, így visszakapjuk az $|A|$-t és a $4^{\gamma n}$-t, $\sqrt[k]{kn+2}$ pedig 1-hez tart, ha k-val tartunk a végtelenbe, így láthatjuk, hogy a szorzó elhagyható, és ezzel a tételt igazoltuk. □

Egyszerű analízisbeli módszerrel megmutatható, hogy $\gamma \approx 0{,}926$: ha deriváljuk a $H(\frac{1}{2} - \epsilon) + H(2\epsilon)$ kifejezést ($H(x)$ deriváltja $-\log_2 \frac{x}{1-x}$ [11]), akkor azt kapjuk, hogy

$$\log_2 \frac{\frac{1}{2}-\epsilon}{\frac{1}{2}+\epsilon} - 2\log_2 \frac{2\epsilon}{1-2\epsilon} = \log_2 \frac{(\frac{1}{2}-\epsilon)(1-2\epsilon)^2}{(\frac{1}{2}+\epsilon)4\epsilon^2}.$$

Nyilván ez akkor lesz 0, ha a tört értéke 1, vagyis ha a számláló és a nevező egyenlőek. Ha egyenlővé tesszük a számlálót és a nevezőt, és egy oldalra rendezünk, akkor a következő harmadfokú egyenletet kapjuk ϵ-ra:

$$2\epsilon^3 - \epsilon^2 + \frac{3}{4}\epsilon - \frac{1}{8} = 0.$$

Ennek egy valós megoldása van, $x_0 \approx 0{,}1983$, és ha ezt az x_0-t behelyettesítjük a maximumon belüli kifejezésbe, akkor a kifejezés értéke körülbelül 0,926 lesz.

3.2. Ellenberg és Gijswijt tétele

A $\mathbb{Z}_4^n$ esetre sikeresen beláttuk, hogy van 4-nél kisebb konstans, amelynek az n-edik hatványa felső korlátot ad a legnagyobb számtani sorozatot nem tartalmazó halmaz méretére, most pedig térjünk vissza a véges testekhez, és mutassuk meg, hogy itt is létezik ilyen konstans $\mathbb{F}_q^n$-hez minden q páratlan prím esetén.

Legyen $\mathbb{F}_q$ egy véges test, és legyen $n \geq 1$. Jelölje M_n azoknak az n-változós monomoknak a halmazát, amelyek foka legfeljebb $q-1$ minden változóra, és legyen S_n az M_n elemei által feszített, $\mathbb{F}_q$ feletti vektortér.

Bármely $d \in \{0, \ldots, 2n\}$ számra legyen M_n^d a legfeljebb d-fokú M_n-beli monomok halmaza, S_n^d pedig S_n-nek az altere, amelyet M_n^d elemei meghatároznak. Jelöljük az S_n^d vektortér dimenzióját m_d-vel, illetve a továbbiakban legfeljebb d-fokú polinomként utalunk S_n^d elemeire.

3.2.1. Állítás. *Legyen $\mathbb{F}_q$ egy véges test, és $A \subseteq \mathbb{F}_q^n$. Legyenek továbbá α, β, γ olyan $\mathbb{F}_q$-beli elemek, amelyekre $\alpha + \beta + \gamma = 0$. Tegyük fel, hogy a $P \in S_n^d$ polinomra minden $a, b \in A \quad (a \neq b)$ pár esetén teljesül, hogy $P(\alpha a + \beta b) = 0$. Ekkor azon $a \in A$ elemek száma, amelyekre $P(-\gamma a) \neq 0$, legfeljebb $2m_{d/2}$.*

Észrevehető, hogy ez az állítás hasonlít a 3.1.1 lemmához, illetve majd látjuk, hogy az állítás bizonyításában is lényegében hasonló lépéseket használunk fel, hiszen a 3.1.1 lemma gyakorlatilag azt az esetét látja be az állításnak, ha $\alpha = 1, \beta = -1$ és $\gamma = 0$. A $\gamma = 0$ esetre itt is azt kapjuk, hogy $P(0) = 0$, ha $|A| > 2m_{d/2}$ azonban itt lényeges lesz, hogy a P polinomunk egy nagyobb halmazon tűnjön el.

Bizonyítás. [[8] alapján] Bármilyen $P \in S_n^d$ felírható M_n^d-beli monomok lineáris kombinációjaként, így

$$P(\alpha a + \beta b) = \sum_{m,m' \in M_n^d : deg(mm') \leq d} c_{m,m'} m(x) m'(y).$$

A fenti felírásban mindegyik tag esetén m és m' közül legalább az egyik foka legfeljebb $\frac{d}{2}$. Ez alapján a következő felírás adható meg, nem feltétlen egyértelműen:

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

ahol F_m és G_m a megfelelő monomokhoz tartozó polinomjai y-nak, illetve x-nek.

Legyen B egy $|A| \times |A|$-as mátrix, amelynek az a, b helyén az áll, hogy

$$B_{ab} = P(\alpha a + \beta b) = \sum_{m \in M_n^{d/2}} m(a) F_m(b) + \sum_{m \in M_n^{d/2}} G_m(a) m(b).$$

Egy adott $m \in M_n^{d/2}$ elemre legyen a B_{mF_m} mátrix olyan, hogy az a, b helyen $m(a)F_m(b)$ áll, illetve a $B_{G_m m}$ az a mátrix, ahol az a, b helyen $G_m(a)m(b)$ szerepel. Ekkor B felírható úgy, mint

$$B = \sum_{m \in M_n^{d/2}} B_{mF_m} + \sum_{m \in M_n^{d/2}} B_{G_m m}.$$

Mind a B_{mF_m}, mind a $B_{G_m m}$ mátrixok előállnak egy oszlop- és egy sorvektor szorzataként, tehát ezeknek a mátrixoknak a rangja 1. Így beláttuk, hogy B előáll $2m_{d/2}$ 1-rangú mátrix összegeként, azaz B rangja legfeljebb $2m_{d/2}$ lehet.

A feltételünk alapján a B diagonális mátrix kell legyen, így a B rangjára adott felső becslés miatt a főátlóban legfeljebb $2m_{d/2}$ nemnulla elem szerepelhet. Ezzel beláttuk az állításunkat. □

3.2.2. Tétel. *Legyenek α, β, γ olyan $\mathbb{F}_q$-beli elemek, hogy $\alpha+\beta+\gamma = 0$ és $\gamma \neq 0$, illetve legyen $A \subseteq \mathbb{F}_q^n$ olyan, hogy az*

$$\alpha a_1 + \beta a_2 + \gamma a_3 = 0$$

egyenlethez nem létezik olyan $(a_1, a_2, a_3) \in A^3$ számhármas, amely megoldja azt, kivéve a triviális $a_1 = a_2 = a_3$ megoldást.

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

Bizonyítás. [[8] alapján] Legyen $d \in \{0, \ldots, (q-1)n\}$ egész. Legyen $V \subset S_n^d$ azoknak a polinomoknak az altere, amelyek eltűnnek a $-\gamma A$ komplementerén. Mivel $-\gamma A$ komplementerének elemszáma $q^n - |A|$, így V dimenziója legfeljebb $m_d - q^n + |A|$ lehet. Jelöljük $\mathcal{S}(A)$-val azoknak az $\mathbb{F}_q^n$-beli elemeknek a halmazát, amelyek felírhatók $\alpha a_1 + \beta a_2$ alakban úgy, hogy $a_1, a_2 \in A$ és $a_1 \neq a_2$. Ekkor az A-ra vonatkozó feltétel miatt $-\gamma A$ és $\mathcal{S}(A)$ diszjunktak, vagyis ha egy P polinom eltűnik a $-\gamma A$ komplementerén, akkor az értelemszerűen $\mathcal{S}(A)$-n is eltűnik. Azt pedig már a 3.2.1 állításban beláttuk, hogy $P(-\gamma a)$ legfeljebb $2m_{d/2}$ A-beli elem esetén vesz fel nemnulla értéket bármely $P \in V$ polinomra.

Tekintsük V elemeit úgy, mint $\mathbb{F}_q^n$-ból $\mathbb{F}_q$-ba képező függvényeket, legyen $P \in V$ maximális tartójú, és jelöljük Σ-val P tartóját, azaz $\Sigma := \mathbb{F}_q^n \setminus \{a \in \mathbb{F}_q^n : \exists \delta \quad \forall x \in B(a,\delta) \quad P(x) = 0\}$. Tudjuk, hogy $|\Sigma| \geq \dim V$, mert másképp létezne olyan nemnulla $Q \in V$, ami eltűnik a Σ halmazon, és ekkor a $P+Q$ függvény tartója tartalmazná Σ-t, ellentmondva annak, hogy P maximális tartójú.

P tartójáról tudjuk, hogy részhalmaza a $-\gamma A$ halmaznak, és a 3.2.1 állításnak köszönhetően ezáltal azt is tudjuk, hogy $|\Sigma| \leq 2m_{d/2}$, és így $\dim V \leq 2m_{d/2}$. Ebből azt kapjuk, hogy

$$m_d - q^n + |A| \leq 2m_{d/2},$$

azaz

$$|A| \leq 2m_{d/2} + (q^n - m_d).$$

Vegyük észre, hogy $q^n - m_d$ azoknak az n-változós monomoknak a száma, amelyek minden változójukban legfeljebb $q-1$-fokúak, de a fokuk magasabb, mint d. Bijekciót képezhetünk

ezen monomok, és azon monomok között, amelyek foka kisebb $(q-1)n-d$-nél a következőképpen: legyen $\tilde{m} = x_1^{q-1}x_2^{q-1}\dots x_n^{q-1}$, illetve legyen m d-nél magasabb fokú, ekkor m-hez az $m' = \frac{\tilde{m}}{m}$ monomot rendeljük hozzá, ennek a foka pedig tényleg kisebb lesz, mint $(q-1)n-d$. Azoknak a monomoknak a száma, amelyek foka kisebb, mint $(q-1)n-d$, nyilván legfeljebb $m_{(q-1)n-d}$.

Legyen $d = 2(q-1)n/3$, ekkor

$$|A| \leq m_{(q-1)n/3} + (q^n - m_{2(q-1)n/3}) \leq 3m_{(q-1)n/3},$$

ezzel a tételt beláttuk. $\square$

Sikerült bizonyítanunk, hogy $|A|$ felülről becsülhető a legfeljebb $\frac{(q-1)n}{3}$-fokú, minden változóban legfeljebb $q-1$-fokú monomok számának háromszorosával, mostmár csak azt kell ebből belátnunk, hogy minden q-hoz létezik olyan $c < q$ konstans, hogy $|A| < c^n$, ha A nem tartalmaz három hosszú számtani sorozatot.

Mivel q^n az összes M_n-beli monom száma, így annak a valószínűsége, hogy M_n-ből véletlenszerűen kiválasztva egy monomot, az legfeljebb d-fokú lesz, pontosan $\frac{m_d}{q^n}$. Ezt kicsit tovább gondolva: legyenek $X_1, X_2, \dots, X_n$ független, azonos eloszlású valószínűségi változók, hogy minden $1 \leq i \leq n$-re és minden $0 \leq k \leq q-1$-re $P(X_i = k) = \frac{1}{q}$. Ekkor annak a valószínűsége, hogy $X_1 + X_2 + \ldots + X_n \leq d$, szintén $\frac{m_d}{q^n}$, hiszen ha véletlenszerűen választunk egy monomot M_n-ből, az ekvivalens azzal, hogy az egyes változók fokait véletlenszerűen választjuk ki a $\{0, 1, \dots, q-1\}$ halmazból, az X_i valószínűségi változók pedig pontosan ezt reprezentálják, és a monom pontosan akkor lesz legfeljebb d-fokú, ha a fokok összege legfeljebb d.

Tekintsük ekkor $d = \frac{(q-1)n}{3}$-at, ahogyan az előbb láthattuk, $\frac{m_{(q-1)n/3}}{q^n}$ annak a valószínűsége, hogy $X_1 + X_2 + \ldots + X_n \leq \frac{(q-1)n}{3}$. Ezt az egyenlőtlenséget megfelelően átalakítva, és alkalmazva a centrális határeloszlás tételt azt láthatjuk, hogy $\frac{m_{(q-1)n/3}}{q^n}$ a 0-hoz tart, ha n-nel tartunk a végtelenbe, és azt fogjuk belátni, hogy exponenciálisan kicsi is.

A becsléshez szükségünk lesz a Markov-egyenlőtlenségre. A Markov-egyenlőtlenség azt mondja ki, hogy ha X egy nemnegatív valószínűségi változó, és $c > 0$, akkor

$$P(X \geq c) \leq \frac{E[X]}{c}.$$

Ennek a segítségével szeretnénk becsülni $\frac{m_d}{q^n}$ értékét, azonban ahhoz, hogy használhassuk a Markov-egyenlőtlenséget, fel kell szoroznunk az $X_1 + X_2 + \ldots + X_n \leq d$ egyenlőtlenséget egy θ negatív valós számmal. Így azt kapjuk:

$$\frac{m_d}{q^n} = P(\theta(X_1 + X_2 + \ldots + X_n) \geq \theta d).$$

Átalakítjuk az egyenlőtlenséget olyan módon, hogy mindkét oldal esetén vesszük a kompozíciójukat e^x-szel, majd alkalmazzuk a Markov-egyenlőtlenséget:

$$P(\exp(\theta(X_1 + X_2 + \ldots + X_n)) \geq \exp(\theta d)) \leq \frac{E[\prod_{i=1}^{n} \exp(\theta X_i)]}{\exp(\theta d)}.$$

Mivel az X_i-k függetlenek, így az $\exp(\theta X_i)$ függvények szorzatának a várható értéke egyenlő a várható értékek szorzatával, ebből pedig az jön ki, hogy

$$\left(\frac{E[\exp(\theta X_1)]}{\exp(\theta d/n)}\right)^n = \left(\frac{(1 + e^\theta + \ldots + e^{(q-1)\theta})/q}{e^{\theta d/n}}\right)^n.$$

Tehát ez azt jelenti, hogy úgy kaphatunk $\frac{m_d}{q^n}$-re egy alsó korlátot, ha megkeressük a

$$\frac{(1 + e^\theta + \ldots + e^{(q-1)\theta})/q}{e^{\theta d/n}}$$

függvény minimumát a $\theta < 0$ értékekre [12].

Helyettesítsünk be $d = \frac{(q-1)n}{3}$-at az előbb kapott kifejezésbe, és jelöljük az így kapott függvényt f_q-val:

$$f_q(\theta) = \frac{(1 + e^\theta + \ldots + e^{(q-1)\theta})/q}{e^{\theta(q-1)/3}},$$

és ennek a minimumát akarjuk megtalálni adott q-ra. Ha vesszük f_q-nak a logaritmusát, majd deriváljuk azt θ szerint, azt kapjuk, hogy

$$\log'(f_q(\theta)) = \frac{\sum_{k=0}^{q-1} k \cdot e^{k\theta}}{\sum_{j=0}^{q-1} e^{j\theta}} - \frac{q-1}{3}.$$

Arra vagyunk kíváncsiak, hogy ez hol lesz 0, ennek megfelelően ha ezt egyenlővé tesszük 0-val, és átrendezzük, akkor a következő egyenletet kapjuk e^θ-ra:

$$P_q(e^\theta) = \sum_{k=0}^{q-1} (3k - q + 1)(e^\theta)^k = 0.$$

Nyilván az így meghatározott P_q polinom gyökei lesznek e^θ lehetséges értékei, de egyelőre nem tudjuk, hogy biztosan lesz-e olyan z gyöke P_q-nak, hogy $0 < z < 1$, azaz amihez

létezik olyan $\theta < 0$, hogy $z = e^\theta$. Annak bizonyítására, hogy ilyen gyök létezik, a Bolzano-Darboux-tételt fogjuk alkalmazni. A Bolzano-Darboux-tétel azt mondja ki, hogy ha adott egy $f\colon [a,b] \to \mathbb{R}$ folytonos függvény, és $f(a) \neq f(b)$, akkor minden $f(a)$ és $f(b)$ közötti y értékhez létezik olyan $x \in [a,b]$, hogy $f(x) = y$. P_q-ról tudjuk, hogy folytonos, így alkalmazzuk a tételt $a = 0$ és $b = 1$ mellett P_q-ra. Kiszámolható, hogy $P_q(0) = -q + 1$, és $P_q(1) = \frac{q(q-1)}{2}$, tehát $P_q(0)$ értéke negatív és $P_q(1)$ értéke pozitív, azaz létezik olyan $z \in [0,1]$, amire $P_q(z) = 0$, vagyis minden q-ra létezik megfelelő z gyöke a P_q polinomnak.

Így azt már beláttuk, hogy létezik $\theta < 0$, amire $\log'(f_q(\theta)) = 0$. Azt viszont még be kell látnunk, hogy $\min\limits_{\theta<0} f_q(\theta) < 1$, mivel erre szükség van, hogy megmutassuk, tényleg létezik $c < q$ konstans, amire $|A| = O(c^n)$. Tudjuk, hogy mind $f_q(\theta)$, mind $\log'(f_q(\theta))$ folytonos $(-\infty, 0)$-n, és azt is tudjuk, hogy hová tart $\log'(f_q(\theta))$, ha θ a végtelenbe tart, vagy ha θ balról tart 0 felé:

$$\lim_{\theta\to-\infty} \log'(f_q(\theta)) = \lim_{\theta\to-\infty} \frac{\sum\limits_{k=0}^{q-1} k \cdot e^{k\theta}}{\sum\limits_{j=0}^{q-1} e^{j\theta}} - \frac{q-1}{3} = -\frac{q-1}{3},$$

$$\lim_{\theta\to0-} \log'(f_q(\theta)) = \log'(f_q(0)) = \frac{\sum\limits_{k=0}^{q-1} k}{q} = \frac{q-1}{2}.$$

Mivel $\log'(f_q)$ határértéke $-\infty$-ben negatív, és az értéke 0-ban pozitív, illetve folytonos a $(-\infty, 0)$ intervallumon, így van olyan zérushely, ahol a függvény előjelet kell váltson, és azon a helyen f_q-nak lokális minimumhelye van. Ha több ilyen zérushely is van, ahol $\log'(f_q)$ előjelet vált, akkor válasszuk ki a 0-hoz legközelebbit, és jelöljük ezt θ_0-val. Mivel ez az utolsó zérushely, ahol $\log'(f_q)$ előjelet vált, így $\log'(f_q(\theta)) \geq 0$ minden $\theta \in (\theta_0, 0)$-ra, és f_q-nak lokális minimumhelye van θ_0-ban. $\log'(f_q)$ folytonossága miatt 0-nak van olyan $\delta > 0$ sugarú bal oldali környezete, hogy $|\log'(f_q(0)) - \log'(f_q(x))| < \frac{q-1}{2}$ minden $x \in (-\delta, 0)$-re, azaz minden $x \in (-\delta, 0)$-re $\log'(f_q(x)) > 0$. Tehát $\log(f_q)$ szigorúan monoton nő $(-\delta, 0)$-n, így minden $x \in (-\delta, 0)$-re $\log(f_q(x)) < \log(f_q(0)) = 0$.

Tegyük föl, hogy $f_q(\theta_0) \geq 1$, vagyis $\log(f_q(\theta_0)) \geq 0$. A fentiek alapján nyilván $\theta_0 \notin (-\delta, 0)$, így $\theta_0 \leq \delta$. Válasszunk ki egy tetszőleges x-et $(-\delta, 0)$-ból, és alkalmazzuk a Lagrange-középértéktételt $\log(f_q(\theta))$-n θ_0-ra és x-re. Eszerint létezik olyan $y \in (\theta_0, x)$, hogy

$$\log'(f_q(y)) = \frac{\log(f_q(\theta_0)) - \log(f_q(x))}{\theta_0 - x}.$$

Azonban ennek a törtnek a számlálója és a nevezője különböző előjelű, azaz $\log'(f_q(y))$ negatív lesz. Ez viszont ellentmondás, hiszen θ_0-t úgy választottuk, hogy $\log'(f_q(\theta)) \geq 0$

minden $\theta \in (\theta_0, 0)$-ra, tehát $f_q(\theta_0) < 1$, és ebből következően $\min_{\theta<0} f_q(\theta) < 1$ is teljesül. Azt nem tudjuk, hogy f_q tényleg a θ_0-ban veszi-e fel minimumát, azonban a célunk nem az volt, hogy megtaláljuk, hol van a minimuma a függvénynek, hanem hogy belássuk, hogy a minimum értéke egynél kisebb.

Jelöljük az $f_q(\theta)$ minimumát γ-val. Ekkor

$$\frac{m_{(q-1)n/3}}{q^n} \leq \gamma^n,$$

és ebből

$$m_{(q-1)n/3} \leq (\gamma q)^n = c^n,$$

ahol $c < q$, mivel $\gamma < 1$. A 3.2.2 tétel alapján pedig ekkor $|A| \leq O(c^n)$.

3.2.3. Következmény. Legyen $A \subseteq \mathbb{F}_3^n$ olyan, hogy A nem tartalmaz három hosszú számtani sorozatot. Ekkor $|A| = O(2{,}756^n)$

Bizonyítás. Ha $q = 3$, akkor $P_3(e^\theta) = 4(e^\theta)^2 + e^\theta - 2$, ennek egyetlen olyan z gyöke van, amire $z \in [0, 1]$, ez pedig $z = \frac{\sqrt{33}-1}{8}$. Ennek a logaritmusát visszahelyettesítve f_3-ba megkapjuk a minimumot, ami körülbelül 0,918. Ebből pedig már adódik az $m_{2n/3} \leq 3^n \cdot 0{,}918^n = 2{,}756^n$ becslés, és így 3.2.2 alapján $|A| = O(2{,}756^n)$. □

Az előző fejezet végén láthattuk, hogy különböző $a_1, a_2, a_3 \in \mathbb{F}_3^n$ pontok esetén a_1, a_2, a_3 kollineáris akkor és csak akkor, ha a_1, a_2, a_3 számtani sorozatot alkotnak. Tehát a $q = 3$-ra kapott felső korlát egyben a cap set-probléma megoldása is.

4. fejezet

Napraforgómentes halmazrendszerek

4.1. Naslund és Sawin tétele

Az előző fejezetben már említést tettünk Naslund és Sawin eredményéről [10] az Erdős-Szemerédi napraforgó-sejtéssel kapcsolatban, amelyet a Croot, Lev és Pach által használt módszer alkalmazásával értek el. Ebben a fejezetben azt fogjuk belátni, hogy ha adott egy $\{1, \dots, n\}$ részhalmazaiból álló napraforgómentes halmazrendszer, akkor létezik $c < 2$ konstans, hogy a halmazrendszer elemszáma felülről becsülhető c^n-nel.

Ehhez először definiáljuk, hogy mik a napraforgók, illetve kimondjuk az Erdős-Szemerédi sejtést.

4.1.1. Definíció. Legyenek $H_1, H_2, \dots, H_k$ halmazok. Ha $H_i \cap H_j$ azonos minden $1 \leq i < j \leq k$-ra, akkor a H_i-k k-napraforgót alkotnak.

Egy halmazrendszerre azt mondjuk, hogy k-napraforgómentes, ha semelyik k eleme sem alkot k-napraforgót, ha pedig $k = 3$, akkor egyszerűen azt mondjuk, hogy napraforgómentes.

Az Erdős-Szemerédi napraforgósejtés szerint, ha S egy k-napraforgómentes halmazrendszere $\{1, \dots, n\}$ részhalmazainak, akkor

$$|S| < c_k^n,$$

ahol $c_k < 2$ egy csak k-tól függő konstans.

Jelölje $F_k(n)$ a legnagyobb k-napraforgómentes $\mathcal{F}$ halmazrendszer méretét, amely $\{1, \dots, n\}$ részhalmazaiból áll, és legyen

$$\mu_k^S = \limsup_{n \to \infty} F_k(n)^{1/n}$$

az Erdős-Szemerédi k-napraforgómentes kapacitás. Nyilván $\mu_k^S \leq 2$, hiszen $\{1, \ldots, n\}$ összes részhalmazának száma 2^n, viszont a sejtés szerint minden $k \geq 3$-ra $\mu_k^S < 2$. Mi csak a $k = 3$ esetre fogjuk belátni, hogy a kapacitás tényleg kisebb 2-nél.

4.1.2. Definíció. Legyen $k \geq 2$, A egy véges halmaz, és $\mathbb{F}$ egy test. Az $\Phi\colon A^k \to \mathbb{F}$ függvény rangja a legkisebb r pozitív egész, hogy Φ felírható r darab

$$(x_1, \ldots, x_k) \mapsto f(x_i)g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$$

alakú függvény lineáris kombinációjaként, ahol $i \in \{1, \ldots, k\}$, $f\colon A \to \mathbb{F}$, és $g\colon A^{k-1} \to \mathbb{F}$.

A $\Phi\colon A^k \to \mathbb{F}$ függvény rangja felülről becsülhető $|A|^k$-val, tehát a megadott feltételek mellett mindig létezik.

Legyen $T\colon A \times A \times A \to \mathbb{R}$ háromváltozós függvény, amely akkor és csak akkor nem nulla, ha $x = y = z$, vagy ha x, y, z napraforgót alkot. Nyilván ha A napraforgómentes, akkor $T(x, y, z)$ nem nulla akkor és csak akkor, ha $x = y = z$. Ahhoz, hogy belássuk, hogy létezik $c < 2$ konstans, amire $\mu_3^S \leq c$, korlátot kell adnunk $T(x, y, z)$ rangjára, ezt pedig a következő lemma segítségével tehetjük meg.

4.1.3. Lemma. *Legyenek $k \geq 2$, A egy véges halmaz, $\mathbb{F}$ egy test, és minden $a \in A$-ra $c_a \in \mathbb{F}$ együtthatók, illetve jelölje rögzített $a \in A$-ra $\delta_a(x)$ a Kronecker-delta függvényt. Ekkor az*

$$(x_1, \ldots, x_k) \mapsto \sum_{a \in A} c_a \delta_a(x_1) \ldots \delta_a(x_k) \tag{4.1}$$

függvény rangja egyenlő a nemnulla c_a-k számával.

A lemmát csak a $k = 3$ esetre fogjuk alkalmazni, hiszen $T(x, y, z)$ háromváltozós, azonban a lemmát indukcióval bizonyítjuk a $k > 2$ esetekre, így általánosan minden $k \geq 2$-re be fogjuk látni.

Bizonyítás. [[13] alapján] Indukcióval bizonyítunk k-ra, ennek megfelelően először a $k = 2$ esetet nézzük. Két változóra az egyrangú függvények $(x_1, x_2) \mapsto f(x_1)g(x_2)$ alakban jelennek meg. Ha veszünk egy v_f oszlopvektort, amiben az $f(x)$ értékek szerepelnek minden $x \in A$-ra, illetve egy v_g sorvektort, amiben a $g(y)$ értékek szerepelnek minden $y \in A$-ra, és az elemek sorrendje, ahogy a függvényértéküket vesszük, megegyezik mindkét vektorra, akkor a $v_f \cdot v_g$ szorzat egy olyan $|A| \times |A|$-as M mátrixot ad, hogy $m_{xy} = f(x)g(y)$ minden $x, y \in A$-ra. Nyilván az M mátrix rangja ekkor 1, hiszen előáll egy sorvektor és egy oszlopvektor szorzataként. Ha egy Φ kétváltozós függvény rangja l, az azt jelenti, hogy l darab ilyen $f(x)g(y)$ egyrangú függvény lineáris kombinációjaként áll elő. Ha Φ-re veszünk egy

olyan B mátrixot, hogy $b_{xy} = \Phi(x, y)$, akkor azt láthatjuk, hogy B előáll azoknak az M mátrixoknak a lineáris kombinációjaként, amelyeket azok az egyrangú függvények generálnak, amelyek lineáris kombinációjaként Φ előáll. Viszont az M mátrixok mindegyikének egy a rangja, így a B rangja legfeljebb l lehet.

Ha a 4.1 függvényre vesszük azt a B mátrixot, hogy $b_{xy} = \sum_{a \in A} c_a \delta_a(x_1)\delta_a(x_2)$, akkor B egy diagonális mátrix lesz és nyilván ekkor B rangja megegyezik a nemnulla c_a-k számával, így $k = 2$-re tényleg igaz a lemma.

Tegyük fel, hogy $(k-1)$-re már beláttuk, hogy teljesül a lemma, és így lássuk be, hogy $k > 2$ esetén is teljesülni fog. Mivel a 4.1 jobb oldalán lévő összeadandók egyrangú függvények, így a rangja legfeljebb a nemnulla c_a-k számával lehet egyenlő, tehát elég azt belátni, hogy a rang ennél nem lehet kisebb. Elhagyva azokat az $a \in A$ elemeket, amelyekre $c_a = 0$, az általánosság elvesztése nélkül feltehetjük, hogy egyik c_a sem nulla. Tegyük fel, hogy 4.1 rangja legfeljebb $|A| - 1$, ekkor azt kapjuk, hogy

$$\sum_{a \in A} c_a \delta_a(x_1) \dots \delta_a(x_k) = \sum_{i=1}^{k} \sum_{\alpha \in I_i} f_{i,\alpha}(x_i) g_{i,\alpha}(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_k), \tag{4.2}$$

ahol $I_1, \dots, I_k$ olyan halmazok, amelyek számosságainak összege legfeljebb $|A| - 1$, és $f_{i,\alpha} \colon A \to \mathbb{F}$, $g_{i,\alpha} \colon A^{k-1} \to \mathbb{F}$ függvények.

Tekintsük azoknak a $h \colon A \to \mathbb{F}$ függvényeknek a terét, amelyek ortogonálisak minden $f_{k,\alpha}, \alpha \in I_k$ függvényre olyan értelemben, hogy

$$\sum_{x \in A} f_{k,\alpha}(x) h(x) = 0$$

minden $\alpha \in I_k$-ra. A h függvények vektorterének d dimenziója legalább $|A| - |I_k|$. Ennek a vektortérnek egy bázisa egy $(d \times |A|)$-as teljesrangú koordinátamátrixot generál, ami azt jelenti, hogy létezik $(d \times d)$-es nemszinguláris minor, és így van olyan h függvény, ami sehol sem tűnik el egy $A' \subset A$ legalább $|A| - |I_k|$ elemszámú halmazon. Ha felszorozzuk a 4.2 egyenletet $h(x_k)$-val, és x_k szerint összegzünk, akkor azt kapjuk, hogy

$$\sum_{a \in A} c_a h(a) \delta_a(x_1) \dots \delta_a(x_{k-1}) = \sum_{i=1}^{k-1} \sum_{\alpha \in I_i} f_{i,\alpha}(x_i) \widetilde{g}_{i,\alpha}(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{k-1}),$$

ahol $\widetilde{g}_{i,\alpha}(x_1, \dots, x_{k-1}) = \sum_{x_k \in A} g_{i,\alpha}(x_1, \dots, x_k) h(x_k)$.

A jobb oldal rangja legfeljebb $|A| - 1 - |I_k|$, hiszen az összeadandók, mind egyrangú függvények, míg a bal oldal rangja legalább $|A| - |I_k|$ kell legyen, így ellentmondásra jutottunk. □

Érdemes megjegyezni, hogy Tao ennek a lemmának a segítségével új bizonyítást adott Ellenberg és Gijswijt tételére is.

$T(x,y,z)$-t felírhatjuk a 4.1.3 lemmában látható módon $c_a = T(a,a,a)$ együtthatókkal, ha A napraforgómentes. Ekkor a lemma alapján $T(x,y,z)$ rangja $|A|$ lesz, hiszen bármely $a \in A$ esetén $c_a = T(a,a,a) \neq 0$.

Ha vesszük az $\{1,\dots,n\}$ egy részhalmazát, az egyértelműen megfeleltethető egy $\{0,1\}^n$-beli vektornak úgy, hogy az i-edik helyen 1 áll, ha i eleme az adott részhalmaznak, és 0 egyébként. Tehát ha $\{1,\dots,n\}$ részhalmazainak egy napraforgómentes rendszeréhez vesszük azt az $S \subset \{0,1\}^n$ halmazt, amely a részhalmazoknak megfelelő vektorokat tartalmazza, akkor bármely három különböző $x,y,z \in S$ vektorhoz létezik olyan $1 \leq i \leq n$, hogy az x_i, y_i, z_i számok közül pontosan kettő értéke 1.

Továbbá, ha van egy olyan napraforgómentes halmazrendszerünk $\{1,\dots,n\}$ részhalmazaiból, hogy a halmazrendszernek nincs két olyan eleme, hogy az egyik valódi részhalmaza a másiknak, akkor az ebből kapott $S \subset \{0,1\}^n$ halmazon bármely $x,y,z \in S$ vektorok esetén, ha nem mind egyenlőek, akkor létezik $1 \leq i \leq n$, hogy az x_i, y_i, z_i számok közül pontosan kettő értéke 1. Ez azért lesz igaz, mert az egyetlen új eset, ha két vektor egyenlő, és a harmadik különböző (például $x = y$ és z különböző), és mivel $x \neq z$, így x nem részhalmaza z-nek, tehát van olyan i, ahol $x_i = y_i = 1$, és $z_i = 0$.

4.1.4. Tétel. *Legyen $\mathcal{F}$ egy napraforgómentes halmazrendszere $\{1,\dots,n\}$ részhalmazainak. Ekkor*

$$|\mathcal{F}| \leq 3(n+1)\sum_{k=0}^{n/3}\binom{n}{k},$$

és ebből

$$\mu_3^S \leq \frac{3}{2^{2/3}} \approx 1{,}89.$$

Bizonyítás. [[10] alapján] Vegyük az $\mathcal{F}$-nek megfelelő $S \subset \{0,1\}^n$ halmazt, és jelölje S_l minden $l \in \{0,\dots,n\}$-re azoknak az S-beli vektoroknak a halmazát, amelyekben pontosan l darab egyes van, azaz $S = \bigcup_{l=0}^{n} S_l$. Ekkor minden l-re S_l napraforgómentes halmazrendszer, és S_l-nek nincs két olyan eleme, hogy az egyik valódi részhalmaza lenne a másiknak, így ha $x,y,z \in S_l$ vektorokra nincs olyan i, hogy pontosan két vektorban egyes áll az i-edik helyen, akkor $x = y = z$. Vegyük az $x,y,z \in \{0,1\}^n$ vektorokra azt a $T\colon \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \to \mathbb{R}$ függvényt, amely úgy áll elő, hogy

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

A $T(x,y,z)$ függvény pontosan azokon az (x,y,z) hármasokon nem nulla, amelyekre nincs olyan i, hogy $\{x_i,y_i,z_i\}=\{1,1,0\}$. Ha T-t megszorítjuk $S_l\times S_l\times S_l$-re, akkor pedig $T(x,y,z)$ nem nulla akkor és csak akkor, ha $x=y=z$, így a 4.1.3 lemma alapján T rangja legalább $|S_l|$. Ha kibontjuk T szorzatalakját, akkor $T(x,y,z)$ előáll a következő, x-re, y-ra és z-re vett monomok szorzatainak lineáris kombinációjaként:

$$x_1^{i_1}\dots x_n^{i_n}y_1^{j_1}\dots y_n^{j_n}z_1^{k_1}\dots z_n^{k_n},$$

ahol $i_1,\dots i_n,j_1,\dots,j_n,k_1,\dots,k_n\in\{0,1\}$, és

$$\sum_{r=1}^{n}i_r+\sum_{r=1}^{n}j_r+\sum_{r=1}^{n}k_r\le n.$$

Minden ilyen szorzat esetén $\sum i_r,\sum j_r,\sum k_r$ közül legalább az egyik legfeljebb $\frac{n}{3}$ lehet. Minden tag esetén válasszuk ki $x_1^{i_1}\dots x_n^{i_n},y_1^{j_1}\dots y_n^{j_n}$, és $z_1^{k_1}\dots z_n^{k_n}$ közül az egyiket, amelyik esetén a fokszám legfeljebb $\frac{n}{3}$. Alakítsuk át T kibontását oly módon, hogy minden kiválasztott monom esetén vesszük azokat a tagokat, amelyekben az adott monomot emeltük ki, ekkor nyilván ezeknek a tagoknak az összege felírható szorzatként, ahol az egyik tényező az adott monom (amiről tudjuk, hogy egy változó függvénye), a másik tényező pedig a tagok másik két változótól függő részeinek összege. Tehát T-t felbontottuk olyan szorzatok összegére, ahol az első tényező egy változótól függ, a második pedig a másik két változótól, így T rangja legfeljebb annyi lehet, ahány monomot kiválasztottunk, általánosan pedig úgy tudunk felső becslést adni T rangjára, ha megnézzük, legfeljebb hány monomot választhatunk ki. Minden monom n-változós, az egyes változókban legfeljebb 1-fokú, összesen legfeljebb $\frac{n}{3}$ fokú, ezeknek a száma összesen $\sum\limits_{k\le n/3}\binom{n}{k}$. Ha mindhárom változó esetén vesszük ezeket a monomokat, azt kapjuk, hogy

$$|S_l|\le 3\sum_{k=0}^{n/3}\binom{n}{k},$$

ebből pedig

$$|S|\le\sum_{l=0}^{n}|S_l|\le 3(n+1)\sum_{k=0}^{n/3}\binom{n}{k}.$$

Még a μ_3^S-re vonatkozó felső becslést kell megmutatnunk, ehhez a Croot-Lev-Pach-tételnél alkalmazott 3.1 becslést fogjuk felhasználni:

$$\mu_3^S \leq \limsup_{n\to\infty} \left(3(n+1)\sum_{k=0}^{n/3}\binom{n}{k}\right)^{1/n} \leq 1\cdot 1\cdot 2^{H(1/3)} = \frac{3}{2^{2/3}}.$$

Ezzel a tételt igazoltuk. □

Ellenberg és Gijswijt cap setek méretére adott felső becslését felhasználva is megadható olyan $c < 2$, amelyre $\mu_3^S \leq c$. Legyen $A_n \subset \mathbb{F}_3^n$ a legnagyobb cap set n dimenzióban, és legyen $C = \limsup_{n\to\infty} |A_n|^{1/n}$, 3.2.3 miatt nyilván $C \leq 2{,}756$. A következő tételben C segítségével fogunk felső becslést adni μ_3^S-re.

4.1.5. Tétel. *Ha μ_3^S az Erdős-Szemerédi napraforgómentes kapacitás, és C a fent definiált konstans, akkor $\mu_3^S \leq \sqrt{1+C}$.*

Bizonyítás. [[10] alapján] Úgy fogunk becslést adni a legnagyobb napraforgómentes halmazra $\{0,1\}^{2n}$-ben, hogy minden vektort a négy különböző $\{0,1\}^2$-beli vektor segítségével írunk fel:

$$u_0 = \begin{bmatrix}0\\0\end{bmatrix}, u_1 = \begin{bmatrix}1\\0\end{bmatrix}, u_2 = \begin{bmatrix}0\\1\end{bmatrix}, u_3 = \begin{bmatrix}1\\1\end{bmatrix}.$$

Minden $S \subset \{0,1\}^{2n}$ megfeleltethető egy $\widetilde{S} \subset \{0,1,2,3\}$ halmaznak olyan módon, hogy $\widetilde{S}$ elemeiben az $i \in \{0,1,2,3\}$ számokat kicseréljük az u_i vektorokra.

Minden $x \in \{0,1\}^n$-re vegyük a következő halmazt:

$$\widetilde{S}_x = \left\{v \in \widetilde{S} \colon v_i = 3 \Leftrightarrow x_i = 1\right\}.$$

Legyen $w(x) = \sum_{x=1}^{n} x_i$, azaz az egyesek száma x-ben. $\widetilde{S}_x$ elemeit tekinthetjük úgy is, mint $\{0,1,2\}^{n-w(x)} = \mathbb{F}_3^{n-w(x)}$-beli elemeket, elhagyva azokat az i koordinátákat, ahol $x_i = 1$. Ha három $\widetilde{S}_x$-beli elem számtani sorozatot alkot $\mathbb{F}_3^{n-w(x)}$-ben, akkor minden koordinátában vagy egyformák, vagy a $0,1,2$ értékeket veszik fel valamilyen sorrendben. Ekkor a megfelelő S-beli vektorra is igaz lesz, hogy minden helyen vagy megegyeznek, vagy az u_0, u_1, u_2 vektorok jelennek meg valamilyen sorrendben. Mivel u_0, u_1 és u_2 napraforgót alkotnak, így ekkor ez a három S-beli vektor is napraforgót alkot. Tehát ha S napraforgómentes, akkor $\widetilde{S}_x$ cap set kell, hogy legyen $\mathbb{F}_3^{n-w(x)}$-ben, így

$$|\widetilde{S}_x| \leq C^{n-w(x)}.$$

Az $\widetilde{S}_x$ halmazok diszjunkt felbontását adják $\widetilde{S}$-nek, hiszen minden vektor szerepel valamelyik $\widetilde{S}_x$-ben, és egy vektor sem szerepelhet különböző x_1, x_2 vektorokra $\widetilde{S}_{x_1}$-ben és $\widetilde{S}_{x_2}$-ben

is, hiszen az azt jelentené, hogy x_1 és x_2 ugyanazokban a koordinátákban lesznek egyenlőek eggyel, ebből pedig az következik, hogy $x_1 = x_2$. Ennek köszönhetően

$$|S| \leq \sum_{x \in \{0,1\}^n} C^{n-w(x)} = \sum_{k=0}^{n} \binom{n}{k} C^k = (1+C)^n,$$

ebből pedig adódik, hogy $\mu_3^S \leq \sqrt{1+C}$. $\square$

Ha behelyettesítjük C helyére a 2,756-ot, akkor $\sqrt{3{,}756} \approx 1{,}938$-at kapunk felső becslésként μ_3^S értékére. Ez gyengébb tehát, mint a 4.1.4 tételben kapott becslés, azonban ennek az értéke a cap setek méretére adott felső becsléstől függ, így ha a jövőben sikerül erősebb felső becslést adni a legnagyobb cap set méretére, akkor az egyúttal ezt a becslést is erősebbé teheti.

Irodalomjegyzék

[1] https://www.setgame.com/founder-inventor

[2] Freud Róbert: Lineáris algebra. ELTE Eötvös Kiadó, 2006

[3] Moussong Gábor: Geometria. Typotex Kiadó, 2014

[4] G. Pellegrino. Sul massimo ordine delle calotte in $S_{4,3}$. Matematiche (Catania), 25, 149–157 (1971)

[5] B. L. Davis, D. Maclagan: The card game SET. The Mathematical Intelligencer, Vol. 25, Issue 3, 33-40 (2003)

[6] Y. Edel: Extensions of generalized product caps, Designs, Codes and Cryptography 31, No. 1, 5-14 (2004)

[7] E. Croot, V. Lev, P. P. Pach: Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small. Annals of Mathematics Vol. 185, 331-337 (2017)

[8] J. Ellenberg, D. Gijswijt: On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression. Annals of Mathematics Vol. 185, 339-343 (2017)

[9] Pach Péter Pál: Számtani sorozatot nem tartalmazó halmazok. Matematikai Lapok, 22. évfolyam 1. szám (2016)

[10] E. Naslund, W. F. Savin: Upper bounds for sunflower-free sets. Forum Mathematics Sigma Vol. 5, e15 (2017)

[11] Wikipedia. https://en.wikipedia.org/wiki/Binary_entropy_function

[12] D. Austin: Game. SET. Polynomial. http://www.ams.org/publicoutreach/feature-column/fc-2016-08

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