

pachpp_312_25

Polinom módszer az additív kombinatorikában

Pach Péter Pál

Doktori értekezés tézisei

Budapest, 2025.

1. Bevezetés

Az elmúlt néhány évtizedben a polinom módszer egy hatékony és sokrétűen alkalmazható eszközzé vált, amely számos fontos nyitott probléma megoldásához is elvezetett, mint például Dvir bizonyítása [35] a Kakeya-sejtés véges testek feletti változatára, Guth és Katz eredménye [65] Erdős különböző távolságokra vonatkozó problémájával kapcsolatban, vagy a „süveghalmaz-probléma” („cap set problem”) megoldása [31, 41]. A süveghalmaz-probléma arra a kérdésre keresi a választ, hogy mekkora az $\mathbb{F}_3^n$ vektortér legnagyobb olyan részhalmaza, amely nem tartalmaz három pontot egy egyenesen, vagy ezzel ekvivalensen: nem tartalmaz három hosszú (nemkonstans) számtani sorozatot. A kérdés az évek során egy fontos, központi problémává vált, amelynek megoldásától azt várták, hogy számos más probléma megoldásához is elvezethet (és később valóban el is vezetett) a kombinatorikában, a számelméletben, sőt, a matematika más területein is.

Bár a süveghalmaz-probléma erősen sugallta, hogy esetében a polinom módszer alkalmazható lehet, hiszen az a feltétel, hogy x , y és z számtani sorozatot alkotnak, egyszerűen kifejezhető az $x - 2y + z = 0$ egyenlettel, hosszú évekig szinte minden eredményt Fourier-analitikus technikák segítségével értek el. Jegyezzük meg, hogy amikor a problémát $\mathbb{F}_3$ felett vizsgáljuk, az $x - 2y + z$ egyenlet szimmetrikus a változóknak, mivel ebben az esetben az egyenlet az $x + y + z = 0$ alakot ölti.

Az 1990-es és a 2000-es években a polinom módszer segítségével igazolt eredmények többsége Alon kombinatorikus nullhelytételére [2] épült, azonban a süveghalmaz-probléma esetében egy új változatra volt szükség. Nagyon röviden, a fő ötlet hipermátrixok egy újfajta rangjának bevezetése volt (bár ez a rang csak implicit módon jelent meg az eredeti cikkünkben [31]), amelyre szintén teljesül, hogy egy diagonális hipermátrix rangja a főátlóján lévő nemnulla elemek száma. Ha egy A halmaz csak triviális (konstans) három hosszúságú számtani sorozatokat tartalmaz, akkor a három hosszú számtani sorozatok „karakterisztikus függvénye” ($A \times A \times A$ -ra megszorítva) egy diagonális tenzor, így ennek a tenzornak a rangját felülről becsülve az A halmaz méretére vonatkozó felső korlátot kapunk.

Bár az Alon-Jaeger-Tarsi sejtés közelmúltbeli megoldásában [90] (és az eredményeken tovább javító [91] cikkben) szintén a polinom módszer egy új változatát alkalmaztuk, ennek jellege egészen más, mint a korábban említett változaté: csoportgyűrű-azonosságok közötti összefüggésekre épül. A polinomok a szerző néhány aritmetikai Ramsey-elméleti munkájában [74, 80, 92] is meghatározó szerepet játszanak, de ezek az ötletek és módszerek is eléggé eltérő jellegűek.

Ezért a szerző úgy döntött, hogy jelen értekezésben a fent említett (Croot-Lev-Pach) polinom módszert ismerteti, amelyet először a $\mathbb{Z}_m^n$ csoportokban számtani sorozatot nem tartalmazó halmazok maximális lehetséges méretének becslésére használtunk, tárgyaljuk az ismert legjobb becsléseket rögzített hosszúságú számtani sorozatokat elkerülő halmazok maximális méretére vonatkozóan, végül bemutatjuk a technika néhány további alkalmazását.

Az értekezés első, bevezető fejezete után a 2. fejezet tartalmazza számtani sorozatokkal kapcsolatos eredményeket, melyek bizonyítása módszer és szűkebb témakör alapján a 3-6. fejezetekben található, a tézisfüzetben jelezzük melyik bizonyítás pontosan hol szerepel. A 7. fejezetben további alkalmazásokat tárgyalunk.

A fejezetek és állítások számozása az angol nyelvű értekezés számozását követi.

1.1. Roth problémája három hosszú számtani sorozatokról

1953-ban K. F. Roth [106] bebizonyította, hogy az $[n] := \{1, 2, \dots, n\}$ halmaz legnagyobb olyan részhalmazának mérete, amely nem tartalmaz $x, x + d, x + 2d$ három elemű számtani sorozatot $o(n)$. A bizonyítása (azt megfelelően értelmezve) $O(n/\log \log \log n)$ kvantitatív korlátot is ad. Ez természetes módon elvezet a következő kérdéshez:

Roth problémája. Mekkora a legnagyobb olyan $S \subseteq [n]$ részhalmaz mérete, amely nem tartalmaz három elemű számtani sorozatot?

A legtöbb előrelépés ennél a problémánál Roth ötletére épül, és úgynevezett „sűrűségnövelő érvelést” használ. Az ötlet lényege, hogy ha feltételezzük, hogy az $S \subseteq [n]$ halmazban nincs három hosszúságú számtani sorozat, és $|S| = \alpha n$, ahol $n > N_0(\alpha)$, akkor meg lehet mutatni, hogy létezik egy olyan

$$P := \{a, a + d, a + 2d, \dots, a + kd\} \subseteq [n]$$

számtani sorozat, aminek hosszára $k > n^{1/2-o(1)}$ teljesül, továbbá

$$|S \cap P| \geq \alpha(1 + c\alpha)|P|$$

bizonyos $c > 0$ konstans mellett. Eltolással és átskálázással tehát egy három hosszúságú számtani sorozatot nem tartalmazó $S' \subseteq [n']$ halmazt kapunk valamely $|n'| > n^{1/2-o(1)}$ mellett, úgy, hogy $|S'| \geq \alpha(1 + c\alpha)|n'|$. Ezt ismételve (az $N_0(\alpha)$ korlát felett maradva) végül ellentmondáshoz jutunk, ha $\alpha > c'/\log \log n$, mert ha α ilyen nagy, akkor az egyik S'' halmaznak már 1 sűrűségűnek kellene lennie, úgy, hogy közben nem tartalmaz három hosszú számtani sorozatot. Ha tehát az eredeti S halmaz nem tartalmaz három hosszú számtani sorozatot, akkor $|S| \ll n/\log \log n$.

Az ötlet további finomításaival nagyobb sűrűségnövelés is elérhető iterációnként (az intervallum hosszához viszonyítva) [68, 116], ami $|S| < n(\log n)^{-\delta}$ alakú korlátot ad bizonyos $0 < \delta < 1/2$ esetén. A sűrűségnövelést részsorozatok helyett (mint Roth módszerében) úgynevezett Bohr-szomszédságokon végezve, Bourgain [18] még erősebb, $|S| \ll n\sqrt{\frac{\log \log n}{\log n}}$ alakú becslést kapott. Ezután Bourgain [19] és Sanders [110, 111] további munkáikban a korlátot $|S| < n(\log n)^{-1+o(1)}$ -re javították. Ha ezt a korlátot még egy kicsit sikerül javítani (a -1 -et $(-1 - \varepsilon)$ -ra

csökkentve), a következő híres sejtés [47] megoldását nyerjük a $k = 3$ speciális esetben, ami Szemerédi tételének [115] általánosítása:

Erdős-Turán sejtés k hosszú számtani sorozatokról. Ha az A , pozitív egész számokból álló halmazra $\sum_{a \in A} 1/a = \infty$, akkor minden $2 \leq k$ -ra az A halmaz tartalmaz k hosszú számtani sorozatot.

A legjobb kvantitatív korlátot az általános esetben (tetszőleges k érték mellett) Leng, Sah és Sawhney [76] igazolták, akik nemrég bizonyították, hogy minden $k \geq 5$ esetén létezik egy bizonyos $c_k > 0$ konstans, melyre $[n]$ legnagyobb, k hosszú számtani sorozatot nem tartalmazó S részhalmazának méretére

$$|S| \ll n \exp(-(\log \log n)^{c_k}).$$

Ez a becslés javít a Gowers-féle korlátokon [58], miszerint $|S| \ll n(\log \log n)^{-2^{-2^{k+9}}}$. A $k = 4$ esetben Green és Tao [62, 63] az $|S| \ll n(\log n)^{-c}$ becslést adták bizonyos $0 < c < 1$ mellett.

Bloom és Sisask [15] voltak, akik a fenti sejtést $k = 3$ -ra először bizonyították, Bateman és Katz [9] munkájára építve, megmutatva, hogy $n > N_0$ esetén a legnagyobb, három hosszú számtani sorozatot nem tartalmazó $S \subseteq [n]$ halmaz méretére $|S| < n(\log n)^{-1-\varepsilon}$ (valamilyen expliciten megadható $\varepsilon > 0$ mellett). Ezután Kelley és Meka [73] egy jelentős áttörést elérve ezt tovább javították az

$$|S| < n \exp(-c(\log n)^{1/12})$$

becslésre, amit Bloom és Sisask [17] továbbfejlesztett, így kapjuk az

$$|S| < n \exp(-c'(\log n)^{1/9})$$

korlátot.

Ezek a felső becslések már nem állnak messze a lehető legjobbaktól, mivel Behrend [10] munkája óta ismert, hogy létezik olyan három hosszú számtani sorozatot nem tartalmazó $S \subseteq [n]$ halmaz, amelyre

$$|S| > n \exp(-(2\sqrt{\log 4} + o(1))\sqrt{\log n}).$$

Ezt Elkin [40] javította egy kicsi, de végtelenhez tartó tényezővel, majd nemrégiben Elsholtz, Hunter, Proske és Sauermann [44] további jelentős javulást elérve igazolták, hogy

$$|S| > n \exp(-(C + o(1))\sqrt{\log n}),$$

ahol $C = 2\sqrt{\log(24/7)} \log 2 < 2\sqrt{\log 4}$.

1.2. Véges testek feletti változatok

Mint láttuk, Roth eredeti megközelítésében a fő nehézség az volt, hogy kellően nagy sűrűségnövelést sikerüljön elérni. Meshulam [83] azt vizsgálta, hogy az érvelés mit ad abban az esetben, ha egész számok helyett az $\mathbb{F}_p^n$ vektortér részhalmazait vizsgáljuk. A $p = 3$ eset *sűveghalmaz-probléma* (*cap set problem*) néven ismert.

Meshulam az általános esetben ($\mathbb{F}_p^n$ esetén) ahelyett, hogy egy számtani sorozatban érne el sűrűségnövekedést minden egyes iterációnál (amint az Roth érvelésében volt), a $t + V$ affin alterekben kap sűrűségnövekedést, ahol $\dim(V) = n - 1$. Mivel ezek az affin alterek p^{n-1} méretűek, a sűrűségnövelő lépés többször alkalmazható, mintha az S halmaz elemeit egész számokból álló $[N]$ intervallumokból választanánk $N \approx p^n$ mellett. Továbbá, az egész érvelés elegánsabb és egyszerűbb, mint az egész számok esetében, miközben a nehézségek nagy részét továbbra is tartalmazza. Valójában ez igaz több másik additív kombinatorikai problémára [60, 95] is. Így gyakran célszerű lehet egy $\mathbb{Z}$ feletti probléma megoldásához először megnézni, hogy mit tudunk bizonyítani a probléma $\mathbb{F}_p^n$ feletti változatára.

Meshulam végül bebizonyította, hogy a legnagyobb olyan $S \subseteq \mathbb{F}_p^n$ részhalmaza, amely nem tartalmaz három hosszú számtani sorozatot (vagyis az $x - 2y + z = 0$ egyenlet megoldását) valamely $c_p > 0$ konstans mellett teljesül, hogy

$$|S| < \frac{c_p p^n}{n}.$$

Meshulam bizonyítása Fourier-analitikus módszereket használ, de Lev [78] kidolgozott egy tisztán kombinatorikus megközelítést is ugyanezen korlátok eléréséhez.

Fontos kihívásnak tartották Meshulam becslésének jelentős erősítését, Terry Tao [118] például egyszer úgy hivatkozott arra a kérdésre, hogy megértsük mekkora lehet $\mathbb{F}_3^n$ három hosszú számtani sorozatot nem tartalmazó részhalmaza, mint „talán a kedvenc nyitott kérdése”.

Bateman és Katz voltak az elsők, akik jelentős előrelépést értek el ilyen irányban, bebizonyítva, hogy létezik olyan $\varepsilon > 0$ konstans, hogy a $p = 3$ esetben $|S| \ll 3^n/n^{1+\varepsilon}$. Ezután Ellenberg és Gijswijt [41], a mi munkánkra [31] építve algebrai módszerekkel bebizonyították, hogy minden $p \geq 3$ prímszám esetén létezik olyan $\delta_p > 0$ konstans, hogy $|S| \ll (p - \delta_p)^n$. A módszer további algebrai általánosításait, átfogalmazásait dolgozta ki Tao, Sawin [112, 119] és Petrov [96].

Nemrégiben Kelley és Meka [73] kifejlesztettek egy kombinatorikus módszert (amelynek egyik összetevője [30]) ennél gyengébb, de más kombinatorikus és Fourier-analitikus megközelítésekénél még mindig sokkal erősebb korlátok bizonyítására, elérve az $|S| \ll 2^{-\kappa_p n^{1/9}} p^n$ becslést.

Edel [36] a $p = 3$ esetben olyan S halmazt konstruált, amely nem tartalmaz három hosszú számtani sorozatot és a méretére $|S| > (2,217389)^n$. Ezt először Tyrrell [121] cikkében $|S| > (2,218)^n$ -re javította, majd Romera-Paredes és sztsai [105] cikkükben nagy nyelvi modellek segítségével $|S| > (2,2202)^n$ becslést igazoltak, végül Naslund [87] eredménye szerint $|S| > (2,2208)^n$. Nemrégiben Elsholtz,

Hunter, Proske és Sauermann [44] általános alsó korlátot ért el tetszőleges $p \geq 3$ prímszámra, igazolva az $|S| > (cp)^n$ becslést valamilyen $c > 1/2$ konstans esetén.

1.3. Jelölések

Az értekezésben (és jelen tézisfüzetben is) a $\ll, \gg$ illetve O és Ω jelöléseket pozitív mennyiségekre a szokásos módon alkalmazzuk, vagyis $X \gg Y$, $Y \ll X$, $X = \Omega(Y)$ és $Y = O(X)$ mind azt jelenti, hogy $X \geq cY$, valamilyen $c > 0$ abszolút konstans mellett. Ha mind az $X \ll Y$, mind az $Y \ll X$ feltétel teljesül, akkor azt írjuk, hogy $X = \Theta(Y)$. Ha a c konstans függ egy t mennyiségtől, akkor az $X \ll_t Y$, $Y = O_t(X)$ jelöléseket alkalmazzuk, és így tovább. Használjuk a Landau-féle o jelölést is.

Az $x, y \in \mathbb{F}_q^n$ vektorok (standard) skaláris szorzatát $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$ jelöli. A skaláris szorzatot röviden xy -nak írjuk, ahol ez nem okozhat félreértést.

Használjuk az $[n] := \{1, 2, \dots, n\}$ jelölést és a Kronecker-delta függvényt is a következőképpen.

$$\delta_{x,y} = \delta_x(y) = \delta(x, y) = \begin{cases} 1 & \text{ha } x = y \\ 0 & \text{ha } x \neq y \end{cases}$$

A $\mathbb{Z}_m^n = (\mathbb{Z}/m\mathbb{Z})^n$ csoportban (nemtriviális) k hosszúságú számtani sorozat alatt egy $a, a+d, \dots, a+(k-1)d$ ($a, d \in \mathbb{Z}_m^n$) különböző elemekből álló k hosszú számtani sorozatot értünk, és a rövidség kedvéért k -AP-nek nevezzük (a számtani sorozat angol rövidítését használva, hogy az értekezésben használttal azonos legyen a jelölés). A k hosszú (nemtriviális) számtani sorozatot nem tartalmazó halmazokat k -AP-mentesnek nevezzük. A $\mathbb{Z}_m^n$ csoport legnagyobb k -AP-mentes részhalmazának méretét $r_k(\mathbb{Z}_m^n)$ -nel, az $\{1, 2, \dots, n\}$ halmaz legnagyobb k -AP-mentes részhalmazának méretét pedig $r_k(n)$ -nel jelöljük.

Az értekezésben $\mathbb{F}_2^n$ lineáris és affin altérivel is dolgozunk. Ha L egy d -dimenziós lineáris altér, akkor a rövidség kedvéért azt mondjuk, hogy L egy d -altér. A $v_1, \dots, v_k$ vektorokat tartalmazó legkisebb lineáris altér (vagyis az általuk generált lineáris altér) jelölése $\langle v_1, \dots, v_k \rangle$.

Hasonlóképpen, ha L egy d -dimenziós affin altér, akkor azt mondjuk, hogy L egy affin d -altér, és a legkisebb affin altér jelölése, amely tartalmazza a $v_1, \dots, v_k$ vektorokat (vagyis az általuk generált affin altér) $\langle v_1, \dots, v_k \rangle_{aff}$.

Egy $A \subseteq \mathbb{Z}_m^n$ részhalmazra az $A + A = \{a + a' : a, a' \in A\}$ jelölést használjuk az összeghalmazra és az $A \hat{+} A = \{a + a' : a, a' \in A, a \neq a'\}$ jelölést a megszorított összeghalmazra.

2. Számítási sorozatot nem tartalmazó halmazok

A 2. fejezetben $\mathbb{Z}_m^n$ alakú csoportok számítási sorozatot nem tartalmazó részhalmazainak méretére vonatkozó eredményeket tárgyalunk. A fejezet eredményeinek bemutatása során a [43, 45, 93, 94] cikkeket követjük.

Nagy érdeklődés övezi a $\mathbb{Z}_m^n$ csoport számítási sorozatot nem tartalmazó halmazainak vizsgálatát, különösen az $m = 3$ és 4 esetekben. (Megjegyezzük, hogy a páratlan és páros m esetek kissé eltérőek, és mivel az $m = 2$ eset triviális, a két legkisebb érdekes eset az $m = 3$ és az $m = 4$.) Ha $m = 3, 4, 5$, akkor az a tulajdonság, hogy „nincs 3 hosszúságú számítási sorozat modulo m ” ekvivalens annak megkövetelésével, hogy „nincs 3 pont egy egyenesen”. Az utóbbi tulajdonság *süveg* vagy *süveghalmaz* (*cap* vagy *cap set*) néven ismert. A számítási sorozatot nem tartalmazó halmazok és a süvegek iránti nagy érdeklődés ellenére nem sok szakirodalom szól $\mathbb{Z}_m^n$ számítási sorozatot nem tartalmazó halmazairól általános $m > 3$ és általános k hosszúságú sorozatok esetében. Továbbá nagyon kevés explicit értéket ismerünk az ilyen halmazok maximális méretére vonatkozóan. Bár a szorosan kapcsolódó véges geometria területén kiterjedt szakirodalom áll rendelkezésre, additív kombinatorikai nézőpontból mindössze Tao és Vu könyvének egy feladatát, valamint Lin és Wolf egy cikkét tudjuk említeni.

Ebben a fejezetben különböző esetekre vonatkozó alsó és felső korlátokat tárgyalunk, és $m = 4$ esetben pontos értékeket adunk meg, amelyek nagyságrendileg összevethetők az $m = 3$ -ra ismert pontos értékekkel.

Az 1. fejezetben már említettük Meshulam [83] eredményét, mely szerint $r_3(\mathbb{Z}_m^n) = O(\frac{m^n}{n})$ teljesül $m \geq 3$ páratlan értékeire, ezt Lev [77] kiterjesztette $m \geq 4$ páros értékekre is. Ennek további erősítését Sanders [109] érte el, megmutatva, hogy

$$r_3(\mathbb{Z}_4^n) = O\left(\frac{4^n}{n \log^c n}\right)$$

teljesül valamilyen pozitív c esetén. Green és Tao [61] cikkükben azt írták, hogy $c = 2^{-22}$ megfelelő választás.

Croot, Lev és a szerző [31] egy exponenciálisan kisebb korlátot bizonyított egy teljesen új megközelítés segítségével: Fourier-analitikus módszerek helyett a polinom módszer egy új változatát kidolgozva.

Jelölje H a bináris entrópiafüggvényt, azaz legyen

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

ahol $\log_2 x$ az x szám 2 alapú logaritmus. Legyen

$$\gamma := \max \left\{ \frac{1}{2} (H(0,5 - \varepsilon) + H(2\varepsilon)) : 0 < \varepsilon < 0,25 \right\} \approx 0,926.$$

2.1. Tétel (Croot-Lev-Pach [31]). *Ha $n \geq 1$ és az $A \subseteq \mathbb{Z}_4^n$ halmaz 3AP-mentes, akkor $|A| \leq 4^{\gamma n}$, ahol $4^\gamma \approx 3,61$.*

Megjegyezzük, hogy ez az exponenciális javítás a 2.1. Tételben az első volt az ilyen jellegű problémák körében.

Egy $G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \dots \oplus \mathbb{Z}_{m_k}$ csoport esetén, ahol $m_1 \mid m_2 \mid \dots \mid m_k$, jelöljük $\text{rk}_4(G)$ -vel az olyan $i \in [1, k]$ indexek számát, amelyekre $4 \mid m_i$. Mivel $n := \text{rk}_4(G)$ mellett a G csoport $4^{-n}|G|$ darab $\mathbb{Z}_4^n$ -nel izomorf mellékosztály uniója, így a 2.1. Tétel közvetlen következményeként az alábbi általánosítást kapjuk:

2.2. Következmény (Croot-Lev-Pach [31]). *Ha A egy G véges Abel-csoport 3AP-mentes részhalmaza, akkor $n := \text{rk}_4(G)$ mellett $|A| \leq 4^{-(1-\gamma)n}|G|$.*

A [31] cikkünkben kidolgozott új módszert használva Ellenberg és Gijswijt [41] az $r_3(\mathbb{Z}_3^n) \leq 2,756^n$ becslést igazolták. Megjegyezzük, hogy ezek a kérdések a mátrixszorzás bonyolultságának vizsgálatához is kapcsolódnak [5, 14].

A 3AP-mentes halmazok maximális lehetséges méretére vonatkozó alsó korlátokat a $G = \mathbb{Z}_3^n$ csoportban szintén részletesen vizsgálták. Ismert, hogy van olyan $S \subseteq G$ halmaz, amelyre $|S| > 2,2208^n = |G|^\beta$, ahol $\beta = \frac{\log 2,2208}{\log 3} \approx 0,72625$.

Sanders [109] az alábbi alsó korlátot bizonyította az $m = 4$ esetben: létezik 3AP-mentes $S \subseteq G = \mathbb{Z}_4^n$ halmaz, amelyre

$$|S| \gg |G|^{2/3} \approx 2,519^n.$$

Ez az eredmény abból következik, hogy $\mathbb{Z}_4^3$ -ban található egy 16 méretű konstrukció, amire a szorzatkonstrukciót alkalmazva a fenti aszimptotikus becslést nyerjük, hiszen $\sqrt[3]{16} = 2,519\dots$

Az alábbiakban egy jobb alsó korlátot adunk $r_3(\mathbb{Z}_4^n)$ -re. A konstrukcióban bizonyos minimális távolsággal rendelkező bináris kódokat használunk. Jelölje $A(m, d)$ az $\mathbb{F}_2^m$ vektortéren vett, legalább d minimális távolsággal rendelkező (esetleg nemlineáris) kódok közül a lehető legnagyobb méretét. Megjegyezzük, hogy $A(m, 1) = 2^m$ (minden vektor kiválasztható) és $A(m, 2) = 2^{m-1}$ (minden páros Hamming-súlyú vektor kiválasztható). Az alábbi két linken maximális kódok pontos értékeit vagy korlátjait tartalmazó táblázatok találhatók:

<https://www.win.tue.nl/~aeb/codes/binary-1.html>

és <http://www.codetables.de/>

A következő korlátot bizonyítjuk:

2.3. Tétel (Elsholtz-Pach [45]). *Ha $n > 1$, akkor*

$$r_3(\mathbb{Z}_4^n) \geq \max_{0 \leq t \leq n} \sum_{i=t+1}^n \binom{n}{i} A(i, i-t).$$

Ennek az eredménynek a következményeként egy elég jó alsó korlátot nyerünk $r_3(\mathbb{Z}_4^n)$ -re:

2.4. Következmény (Elsholtz-Pach [45]).

$$r_3(\mathbb{Z}_4^n) \gg \frac{3^n}{\sqrt{n}},$$

ami azt jelenti, hogy létezik olyan $3AP$ -mentes $S \subseteq \mathbb{Z}_4^n$ halmaz, melyre

$$|S| \gg 4^{0,7924n}.$$

Az alábbiakban felsoroljuk a kapott alsó becsléseket azokban az esetekben, amikor a dimenzió legfeljebb 10:

2.5. Következmény (Elsholtz-Pach [45]).

$$2 \leq r_3(\mathbb{Z}_4^1), \quad 6 \leq r_3(\mathbb{Z}_4^2), \quad 16 \leq r_3(\mathbb{Z}_4^3), \quad 42 \leq r_3(\mathbb{Z}_4^4), \quad 124 \leq r_3(\mathbb{Z}_4^5),$$

$$344 \leq r_3(\mathbb{Z}_4^6), \quad 960 \leq r_3(\mathbb{Z}_4^7), \quad 2832 \leq r_3(\mathbb{Z}_4^8), \quad 7880 \leq r_3(\mathbb{Z}_4^9), \quad 22232 \leq r_3(\mathbb{Z}_4^{10}).$$

A $\mathbb{Z}_3^n$ csoport esetén a [41] cikk korlátját Jiang [71] javította egy $\sqrt{n}$ faktorial, így a következő ismert:

$$2,2208 \dots^n \ll r_3(\mathbb{Z}_3^n) \leq 2,755 \dots^n / \sqrt{n}, \quad [87, 41, 71]$$

$$3^n / \sqrt{n} \ll r_3(\mathbb{Z}_4^n) \leq 3,61 \dots^n, \quad [45, 31],$$

ha pedig $p \geq 3$ prímszám, akkor valamilyen pozitív δ_p konstans esetén

$$r_3(\mathbb{Z}_p^n) \leq (p - \delta_p)^n \quad [41].$$

A módszer valójában az

$$r_3(\mathbb{Z}_p^n) \leq (J(p)p)^n \quad [14]$$

korlátot eredményezi, ahol

$$J(p) = \frac{1}{p} \min_{0 < t < 1} \frac{1 - t^p}{(1 - t) t^{(p-1)/3}}. \quad (1)$$

Továbbá ismert, hogy $J(s)$ csökkenő és $\lim_{s \rightarrow \infty} J(s) = 0,8414 \dots$ (lásd [14] cikk (4.11) egyenletét).

2.6. Megjegyzés. Mivel $J(s)$ csökkenő és $J(3) \leq 0,9184$, ezért tetszőleges $m \geq 3$ egész számra a következő becslést kapjuk (lásd pl. [14] vagy [97]):

$$r_3(\mathbb{Z}_m^n) \leq (0,9184m)^n. \quad (2)$$

Prímhatvány m -ek esetén a prím eset olyan triviális következményeinél, mint például $r_3(\mathbb{Z}_9^n) \leq 3^n r_3(\mathbb{Z}_3^n)$, erősebb becsléseket is adtak már. A módszert páratlan prímhatványokra megfelelően alkalmazva [14, 96, 114] az

$$r_3(\mathbb{Z}_m^n) \leq (mJ(m))^n$$

korlátot kapjuk. Például a triviális $r_3(\mathbb{Z}_9^n) \leq 3^n r_3(\mathbb{Z}_3^n) \leq 8,268^n$ becslés helyett ezzel az eredménnyel $r_3(\mathbb{Z}_9^n) \leq 7,847^n$ -re javul a korlát.

A technikailag nehezebb páros esetben $m = 2^3 = 8$ esetén szintén történt javítás. Az $r_3(\mathbb{Z}_8^n)$ mennyiség értékére $r_3(\mathbb{Z}_4^n)$ becslése alapján kapott triviális következmény az alábbi:

$$r_3(\mathbb{Z}_8^n) \leq 2^n r_3(\mathbb{Z}_4^n) \leq 7,222^n,$$

azonban Petrov és Pohoata [97] be tudták bizonyítani, hogy az erősebb $r_3(\mathbb{Z}_8^n) \leq 7,09^n$ korlát is érvényes.

Könnyű belátni, hogy az $(r_3(\mathbb{Z}_m^n))^{1/n}$ sorozat konvergál egy bizonyos $\alpha_{3,m}$ határértékhez (ha rögzített m mellett $n \rightarrow \infty$). Mindez abból a megfigyelésből látható, hogy a szorzatkonstrukció segítségével kis dimenziókban talált konstrukciókat fel lehet fűjni. Ha ugyanis A egy 3AP-mentes halmaz n -dimenzióban, akkor az $\underbrace{A \times A \times \dots \times A}_t$ direkt szorzat szintén 3AP-mentes tn -dimenzióban.

Mivel $\alpha_{3,m} < m$, azt mondhatjuk, hogy a $\mathbb{Z}_m^n$ csoport 3AP-mentes halmazai *exponenciálisan kicsik*, ha $m \geq 3$. A [94] cikket megelőzően hosszabb számtani sorozatok esetén nem volt ismert *egyetlen* $4 \leq k \leq m$ esetén sem, hogy $r_k(\mathbb{Z}_m^n)$ szintén exponenciálisan kicsi vagy $(m-o(1))^n$ nagyságrendű (ha $n \rightarrow \infty$). Az 5. fejezetben bebizonyítjuk, hogy amikor $6 \mid m$ és $k \in \{4, 5, 6\}$, akkor $r_k(\mathbb{Z}_m^n)$ exponenciálisan kicsi, speciálisan

$$r_6(\mathbb{Z}_6^n) \leq 5,709^n.$$

Úgy tűnhetne, hogy ezt az állítást akár úgy is meg lehet fogalmazni, hogy $\lim(r_6(\mathbb{Z}_6^n))^{1/n} \leq 5,709$, azonban némileg meglepő módon nem tudjuk bizonyítani, hogy $r_6(\mathbb{Z}_6^n)^{1/n}$ konvergál. A konvergencia azért nem adódik automatikusan, mert a szorzatkonstrukció nem működik teljes általánosságban.

Ha $k = 3$ vagy ha m prímszám, akkor az $\underbrace{A \times A \times \dots \times A}_t$ t -szeres direkt szorzat nem tartalmaz k -AP-t, ha A maga k -AP-mentes, azonban általános k és m esetén ez nem igaz, amit a $k = 6, m = 6$ esettel illusztrálunk. Az 1-dimenziós esetben világos, hogy $r_6(\mathbb{Z}_6) = 5$, és például az $A = \{0, 1, 2, 3, 4\}$ halmaz 6AP-mentes. Ha az $A \times A = \{0, 1, 2, 3, 4\} \times \{0, 1, 2, 3, 4\}$ halmazt vesszük, akkor a $\mathbb{Z}_6^2$ csoport egy 25 elemű részhalmazát kapjuk, amely a következő 6AP-t tartalmazza:

$$(0, 0), (2, 3), (4, 0), (0, 3), (2, 0), (4, 3).$$

Bár a szorzatkonstrukció nem alkalmazható, $r_6(\mathbb{Z}_6^2)$ értékére így is $25 = 5^2$ adódik, azonban megmutatjuk, hogy $r_6(\mathbb{Z}_6^3) < 125 = (r_6(\mathbb{Z}_6))^3$.

A következő korlátokat bizonyítjuk:

2.7. Tétel (Pach-Palincza [94]). *Kis dimenziókban a következők teljesülnek:*

$$r_6(\mathbb{Z}_6^1) = 5, \quad r_6(\mathbb{Z}_6^2) = 25, \quad 117 \leq r_6(\mathbb{Z}_6^3) \leq 124.$$

2.8. Tétel (Pach-Palincza [94]). *6AP-mentes halmazok esetén a következő eredményeket kapjuk:*

$$4,44^n \leq 2^n r_3(\mathbb{Z}_3^n) \leq r_6(\mathbb{Z}_6^n) \leq 5,709^n,$$

ha n elegendően nagy.

Ha $6 \mid m$, akkor a $\mathbb{Z}_6^n$ csoport $\mathbb{Z}_m^n$ egy részcsoporthja, és mind az $(m/6)^n$ mel-
lékosztályban használva a 2.8. Tétel korlátját az alábbi következményt kapjuk:

2.9. Következmény (Pach-Palincza [94]). *Ha $6 \mid m$ és $k \in \{4, 5, 6\}$, akkor*

$$r_k(\mathbb{Z}_m^n) \leq (0,948m)^n,$$

ha n elegendően nagy.

Végül egy másik felső korlátot is adunk $r_6(\mathbb{Z}_6^n)$ -ra $r_3(\mathbb{Z}_3^n)$ függvényében.

2.10. Tétel (Pach-Palincza [94]). *6AP-mentes halmazok esetén a következő becslést kapjuk:*

$$r_6(\mathbb{Z}_6^n) \leq 2^{n+1} \sqrt{3^n r_3(\mathbb{Z}_3^n)}.$$

Megjegyezzük, hogy az $r_3(\mathbb{Z}_3^n) \leq 2,756^n$ korlátot használva a 2.10. Tétel az $r_6(\mathbb{Z}_6^n) \leq 5,75^n$ becslést adja, ami rosszabb, mint a 2.8. Tételben szereplő. Ha azonban $r_3(\mathbb{Z}_3^n) \leq 2,69^n$, akkor a 2.10. Tétel jobb becslést ad, mint a 2.8. Tétel.

Megemlítjük, hogy bár a módszer bármely $\mathbb{F}_q$ véges test esetén alkalmazható $q = p^\alpha$ mellett, azonban mivel $r_3(\mathbb{F}_q^n) = r_3(\mathbb{F}_p^{\alpha n})$, a releváns esetek azok, amikor q prímszám. (Az $\mathbb{F}_{p^\alpha}$ -ra való alkalmazásból adódó felső korlát rosszabb, mint amit $\mathbb{F}_p$ mellett kapunk.)

Csak nagyon kevés explicit érték ismert. Az $m = 3$ esetben süvegek pontos értékéről a következők ismertek:

$$r_3(\mathbb{Z}_3^1) = 2, r_3(\mathbb{Z}_3^2) = 4, r_3(\mathbb{Z}_3^3) = 9, r_3(\mathbb{Z}_3^4) = 20, r_3(\mathbb{Z}_3^5) = 45, r_3(\mathbb{Z}_3^6) = 112.$$

Megjegyezzük, hogy a 4-dimenziós eset a SET kártyajátéknak felel meg. A 6-dimenziós eredmény szerzője (Potechin [100]) és az 5-dimenziós esetben karakterizált maximális süveg szerzői [39] említették, hogy számítógépes segítséget használtak. Edel arról tájékoztatott minket, hogy a [39] cikkhez szükséges számítási idő néhány hét volt.

A pontos értékeket a $\mathbb{Z}_4^n$ csoport 3AP-mentes részhalmazai esetén 5-dimenzióig, 4AP-mentes halmazok esetén pedig 4-dimenzióig határozzuk meg:

2.11. Tétel (Elsholtz-Pach [45]). *3AP-mentes halmazok esetén a következő eredmények teljesülnek:*

$$r_3(\mathbb{Z}_4^1) = 2, r_3(\mathbb{Z}_4^2) = 6, r_3(\mathbb{Z}_4^3) = 16, r_3(\mathbb{Z}_4^4) = 42, r_3(\mathbb{Z}_4^5) = 124.$$

2.12. Tétel (Elsholtz-Pach [45]). *4AP-mentes halmazok esetén a következő eredmények teljesülnek:*

$$r_4(\mathbb{Z}_4^1) = 3, r_4(\mathbb{Z}_4^2) = 10, r_4(\mathbb{Z}_4^3) = 36, r_4(\mathbb{Z}_4^4) = 128.$$

Mint már említettük, ismert, hogy az ilyen típusú eredményeket fel lehet fűjni magasabb dimenziókba is, és így aszimptotikus becsléseket nyerünk a szorzatkonstrukcióval:

2.13. Lemma. *Legyen q egy prímszám.*

a) *Ha $S_1 \subseteq \mathbb{Z}_q^{n_1}$ és $S_2 \subseteq \mathbb{Z}_q^{n_2}$ k -AP-mentes halmazok, akkor $S_1 \times S_2 \subset \mathbb{Z}_q^{n_1+n_2}$ szintén k -AP-mentes, következésképpen:*

$$r_k(\mathbb{Z}_q^{n_1+n_2}) \geq r_k(\mathbb{Z}_q^{n_1}) r_k(\mathbb{Z}_q^{n_2}).$$

b) *Az a) rész ismételt alkalmazásával kapjuk a következő becslést:*

$$r_k(\mathbb{Z}_q^{nt}) \geq (r_k(\mathbb{Z}_q^n))^t.$$

A legnagyobb ismert pontos értékek, $r_3(\mathbb{Z}_4^5) = 124$ és $r_4(\mathbb{Z}_4^4) = 128$, felfűzéséből az alábbi becsléseket kapjuk:

2.14. Következmény.

$$r_3(\mathbb{Z}_4^n) \gg 2,622^n, \quad r_4(\mathbb{Z}_4^n) \gg 3,363^n.$$

Az első eredmény lényegesen gyengébb, mint a 2.4. Következmény míg a második a jelenleg ismert legerősebb becslés.

A 2.13. Lemmából adódik a következő állítás:

2.15. Állítás. *Legyen $q \geq k \geq 3$, ahol a q prímszám és k rögzítettek. Ekkor az*

$$\alpha_{k,q} := \lim_{n \rightarrow \infty} (r_k(\mathbb{Z}_q^n))^{1/n}$$

határérték létezik.

A későbbiekben ismerttetett 2.16. és 2.17. Tételekből következik, hogy

$$\left\lceil \frac{m+1}{2} \right\rceil \leq \alpha_{k,m} \leq m.$$

$k = 3$ esetén többet is tudunk: $\alpha_{3,p} \leq J(p)p$, amikor $m = p$ egy páratlan prímszám, és $J(p)$ értéke (1) alapján lett definiálva.

Tao és Vu [120, Exercise 10.1.3] megfigyelik (Behrend konstrukciója alapján), hogy $\mathbb{Z}_m^n$ -ben létezik olyan 3AP-mentes halmaz, amelynek a mérete legalább $\frac{[m/2]^n}{m^2 n^2} \cdot 1$.

Lin és Wolf [79] a következőket bizonyította: ha m egy prímszám és $k \leq m$, akkor

$$r_k(\mathbb{Z}_m^n) \geq (m^{2(k-1)} + m^{k-1} - 1)^{\frac{n}{2k}} \approx m^{\frac{(k-1)n}{k}}.$$

A fenti alsó korláton javító általános eredményeink a következők:

¹Úgy tűnik, hogy a nevezőt valószínűleg $m^2 n$ -nek szánták (a mi jelöléseinkkel).

2.16. Tétel (Elsholtz-Pach [45]). *Legyen $m \geq 5$ páratlan szám, ekkor létezik olyan $C_m > 0$ konstans, hogy*

$$r_3(\mathbb{Z}_m^n) \geq \frac{C_m}{\sqrt{n}} \left(\frac{m+1}{2} \right)^n.$$

Továbbá, a

$$\sigma_m = \sqrt{\frac{1}{2880} (m^4 + 4m^3 - 14m^2 - 36m + 45)}$$

jelöléssel $C_m = \frac{1}{3\sqrt{3}\sigma_m}$ megfelelő. Végtelenhez tartó páratlan m esetén ezzel a választással aszimptotikusan $C_m \sim \frac{8\sqrt{5}}{\sqrt{3}m^2}$ érvényes.

Az $m = 5$ eset javít a süvegek aszimptotikus alsó korlátján, a részleteket lásd a 2.1 alfejezetben.

A legfontosabb ötlet ismét az, hogy kerüljük a szorzatkonstrukciót, és eggyel több számjegyet használunk, mint amit Tao és Vu [120, Exercise 10.1.3.] használt, néhány extra megkötéssel, amelyek a kapott becslésen nem rontanak sokat (ha m állandó és n növekszik).

2.17. Tétel (Elsholtz-Pach [45]). *Legyen $m \geq 4$ páros szám, ekkor létezik olyan $C_m > 0$ konstans, hogy*

$$r_3(\mathbb{Z}_m^n) \geq \frac{C_m}{\sqrt{n}} \left(\frac{m+2}{2} \right)^n.$$

Továbbá, a

$$\sigma_m = \sqrt{\frac{m^4 + 8m^3 + 4m^2 - 48m}{2880}}$$

jelöléssel $C_m = \frac{1}{3\sqrt{3}\sigma_m}$ megfelelő. Végtelenhez tartó páros m esetén ezzel a választással aszimptotikusan $C_m \sim \frac{8\sqrt{5}}{\sqrt{3}m^2}$ érvényes.

(Ennek az eredménynek egy változata az $m = 8$ speciális esetben szerepel a [97] cikkben is, és azt megelőzően [45] egy előzményében is. Petrov és Pohoata [97] cikke a felső korlát javítására koncentrál.)

Mint az Behrend konstrukciójából jól ismert, jó okok szólnak a rendelkezésre álló számjegyek számának felére való korlátozása mellett. A fenti esetekben a számjegyek felénél egy elemmel többet használunk. Páros m -ek esetén ezen felül még a $0\frac{m}{2}0$ típusú sorozatokat is alaposan meg kell vizsgálnunk. Az alábbi példákban még tovább megyünk, és megjegyezzük, hogy azok a számtani sorozatok, amelyek a modulo m redukciót használják, elég sok külön figyelmet igényelnek. (Például az $r_4(\mathbb{Z}_{11}^n)$ esetben figyelnünk kell az 1, 6, 0, 5 típusú sorozatokra is modulo 11).

2.18. Tétel (Elsholtz-Pach [45]). *A következő becslés érvényes:*

$$r_4(\mathbb{Z}_{11}^n) \gg \frac{7^n}{n^3}.$$

(A 3-as kitevő csökkentésére nem tettünk kísérletet.) Összehasonlításképpen Lin és Wolf [79] alsó korlátja $6,04^n$.

Az egyes esetek külön-külön vizsgálata segítségével m és k más konkrét értékeire is hasonló eredményeket kaphatunk. Két további esetet mutatunk, ahol ezeket az ötleteket általánosítjuk a következő végtelen családokra: $m = p^s$, $k = p^{s-1} + 1$ (illetve $k = p^{s-2} + 1$), ahol p prímszám. Mejegyezzük, hogy ebben az esetben a felhasznált számjegyeket úgy választjuk, hogy azok nem egymást követőek, hanem kihasználjuk a csoport algebrai szerkezetét. Számos hasznos tulajdonság megmarad: sok számtani sorozat kizárható Salem-Spencer „azonos gyakoriság tulajdonság” ötletével, és a „minden elem különböző” feltételt (nemtriviális számtani sorozatok) használva.

2.19. Tétel (Elsholtz-Pach [45]). *Legyen $m = p^s$ egy valódi prímszám: $s \geq 2$. Legyen $k = p^{s-1} + 1$. Ekkor léteznek olyan C_m és $c_m \leq m/2$ pozitív konstansok, hogy a következő becslés érvényes:*

$$r_k(\mathbb{Z}_m^n) \geq C_m \frac{(m - p + 1)^n}{n^{c_m}}.$$

2.20. Következmény (Elsholtz-Pach [45]). *Léteznek olyan C_m és $c_m \leq m/2$ pozitív konstansok, hogy a következő becslések érvényesek:*

$$r_3(\mathbb{Z}_4^n) \geq C_4 \frac{3^n}{n^{c_4}},$$

$$r_5(\mathbb{Z}_8^n) \geq C_8 \frac{7^n}{n^{c_8}},$$

$$r_{10}(\mathbb{Z}_{27}^n) \geq C_{27} \frac{25^n}{n^{c_{27}}},$$

$$r_{26}(\mathbb{Z}_{125}^n) \geq C_{125} \frac{121^n}{n^{c_{125}}},$$

$$r_{102}(\mathbb{Z}_{101^2}^n) \geq C_{10201} \frac{10101^n}{n^{c_{10201}}}.$$

2.21. Tétel (Elsholtz-Pach [45]). *Legyen $m = p^s$ egy valódi prímszám, melyre $s \geq 3$. Legyen $k = p^{s-2} + 1$. Ekkor léteznek olyan C_m és $c_m \leq m/2$ pozitív konstansok, hogy a következő becslés teljesül:*

$$r_k(\mathbb{Z}_m^n) \geq C_m \frac{(m - 2p^2 + 2p)^n}{n^{c_m}}.$$

Ha $p = 2$, akkor ez bizonyosan nem éles: a 2.17. Tétel szerint $m = 8, k = 3$ esetén 5 számjegyet is használhatunk 4 helyett.

2.22. Következmény (Elsholtz-Pach [45]). *Léteznek olyan C_m és $c_m \leq m/2$ pozitív konstansok, hogy a következő becslések érvényesek:*

$$\begin{aligned} r_{p+1}(\mathbb{Z}_{p^3}^n) &\geq C_{p+1} \frac{(p^3 - 2p^2 + 2p)^n}{n^{c_{p+1}}}, \\ r_4(\mathbb{Z}_{27}^n) &\geq C_{27} \frac{15^n}{n^{c_{27}}}, \\ r_{82}(\mathbb{Z}_{729}^n) &\geq C_{729} \frac{717^n}{n^{c_{729}}}, \\ r_6(\mathbb{Z}_{125}^n) &\geq C_{125} \frac{85^n}{n^{c_{125}}}, \\ r_{26}(\mathbb{Z}_{625}^n) &\geq C_{625} \frac{585^n}{n^{c_{625}}}. \end{aligned}$$

Korábbi ilyen típusú eredményekről nincs tudomásunk.

Az $r_3(\mathbb{Z}_4^n)$ mennyiség becsléséhez a probléma egy ekvivalens átfogalmazását használjuk, amelyet a 4.1 alfejezetben mutatunk be. Azt mondjuk, hogy egy $A(x) \subseteq \mathbb{F}_2^n$ ($x \in \mathbb{F}_2^n$) halmazrendszer kielégíti a $(*)$ tulajdonságot, ha az alábbi következtetés érvényes:

$$\forall x \in \mathbb{F}_2^n \ (y \in x + A(x) \hat{+} A(x) \implies A(y) = \emptyset). \quad (*)$$

(Megjegyezzük, hogy $A(x) = \emptyset$ esetén $x + A(x) \hat{+} A(x) := \emptyset$.) A 4.1. Lemmában megmutatjuk, hogy a $(*)$ tulajdonságot kielégítő halmazrendszert alkotó részhalmazok legnagyobb lehetséges összmérete pontosan $r_3(\mathbb{Z}_4^n)$. Ezért a $(*)$ tulajdonságot kielégítő $\{A(x) : x \in \mathbb{F}_2^n\}$ halmazrendszerek maximális összméretének becslése az eredeti kérdésünkkel ekvivalens probléma.

Mint kiderül, nagyon hasznos, amikor át tudunk térni arra az esetre, amikor a nemüres $A(x)$ részhalmazok mind (lineáris) alterek. Nem tudjuk, hogy ez magasabb dimenzióban is megoldható-e, de az alacsony dimenziós esetekben hatékony módszernek bizonyult.

Ebben az esetben 3^n felső korlátot igazolunk, ami elég közel van az általános $r_3(\mathbb{Z}_4^n) \gg 3^n/\sqrt{n}$ alsó korláthoz.

2.23. Tétel (Elsholtz-Pach [45]). *Ha az $A(x)$ ($x \in \mathbb{Z}_2^n$) halmazrendszer kielégíti a $(*)$ tulajdonságot és minden nemüres $A(x)$ részhalmaz lineáris altér, akkor*

$$\sum_{x \in \mathbb{F}_2^n} |A(x)| \leq 3^n.$$

Megjegyezzük, hogy $n = 1$ esetén bármely 2 elemű részhalmaz 3AP-mentes részhalmazt alkot $\mathbb{Z}_4^n$ -ben. Ha $n \in \{2, 3, 4\}$, akkor az extrémális konstrukció egyértelmű a következő értelemben:

2.24. Tétel (Elsholtz-Pach [45]). *Legyen $n \in \{2, 3, 4\}$. Ha az $\{A(x) : x \in \mathbb{F}_2^n\}$ és $\{A'(x) : x \in \mathbb{F}_2^n\}$ halmazrendszerek összmérete $r_3(\mathbb{Z}_4^n)$ és kielégítik a $(*)$ tulajdonságot, akkor létezik egy invertálható $\varphi : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ affin lineáris transzformáció és léteznek olyan $c(x) \in \mathbb{Z}_2^n$ vektorok ($x \in \mathbb{Z}_2^n$), hogy $A'(x) = A(\varphi(x)) + c(x)$ minden $x \in \mathbb{Z}_2^n$ esetén.*

2.1. Süvegek

Egy süveg az $AG(n, q)$ affin térben egy olyan halmaz $\mathbb{F}_q^n$ -ben, amelynek nincs három pontja egy egyenesen. Itt tehát $m = q$ prímhatvány, és olyan halmazokat vizsgálunk, amelyeknek nincs három pontja egy egyenesen $\mathbb{Z}_m^n$ -ben. Ha $m = q$ egy prímszám, akkor $\mathbb{Z}_m^n$ és $AG(n, q)$ süvegei megegyeznek. A „nincs három pont egy egyenesen” feltétel kifejezhető $ax + by + cz = 0$ típusú lineáris egyenletekkel (ahol $a + b + c = 0$). Amint az alábbiakban látjuk, ha $m = 3$ vagy $m = 5$, akkor elég, ha csak a három hosszú számtani sorozatokra figyelünk ($x - 2y + z = 0$ egyenlet). Az $m = 4$ eset nem felel meg az affin süvegeknek, hiszen $\mathbb{Z}_4 \neq \mathbb{F}_4$, de $\mathbb{Z}_m^n$ -ben $m = 3, 4, 5$ esetén ha három pont egy egyenesre esik, akkor mindig számtani sorozatot alkot.

Magas dimenzióban a legjobb alsó korlátokat eredményező konstrukciókat Edels [36] a legjobb 6-dimenziós süveg segítségével adta a szorzatkonstrukciót használva. Prím m esetén, ez $r_3(\mathbb{Z}_m^n) \geq m^{n(\log_m(m^4+m^2-1))/6}$ alsó korlátot ad (ez Lin és Wolf [79] konstrukciója is), és ez körülbelül $2/3$ kitevőt ad aszimptotikusan.

Ha $m = 5$, akkor ez $5^{0,6705n} \approx 2,9421^n$ méretű konstrukciót ad. Ezzel szemben, a fenti 2.16. Tétel alsó korlátja $C_5 3^n / \sqrt{n} \approx 5^{0,6826n}$. Elképzelhető, hogy a konstrukcióban a C_5 konstans a 2.3. Tételben szereplő $m = 4$ esethez hasonlóan javítható. Mindenesetre ez az első javítás $AG(n, m)$ affin süvegeinek méretére, ha $m = q \geq 5$.

2.2. Egyenesmentes halmazok

A véges geometria és az extrémális kombinatorika határterületén számos olyan problémát tanulmányoznak, amelyek az affin vagy projektív terek olyan maximális méretű részhalmazainak megtalálására irányulnak, amelyek bizonyos konfigurációkat elkerülnek. Például a korábban tárgyalt süveghalmaz-probléma esetében $\mathbb{F}_3^n$ -ben a 3 hosszú számtani sorozatok ugyanazok, mint az affin egyenesek, így a 3AP-mentes halmazok megegyeznek az egyenesmentes halmazokkal.

Természetes kérdés, hogy az $\mathbb{F}_q$ feletti n -dimenziós affin tér legnagyobb egyenesmentes részhalmaza mekkora lehet.

Mivel abban az esetben, ha p prímszám, az $\mathbb{F}_p^n$ csoport p hosszú számtani sorozatai éppen az n -dimenziós affin térben lévő egyeneseknek felelnek meg, ezért ebben az esetben $r_p(\mathbb{F}_p^n)$ értékét keressük.

Az általános esetben meglepően kevés eredmény ismert $r_p(\mathbb{F}_p^n)$ -re vonatkozóan. A triviális alsó korlát $r_p(\mathbb{F}_p^n) \geq (p-1)^n$, amelyet egy $p-1$ oldalhosszúságú hiperkocka segítségével érhetünk el. Jamison [70], valamint Brouwer és Schrijver [20] egymástól függetlenül bebizonyították, hogy ez éles $n = 2$ esetén. Eggyel nagyobb dimenzióban, $n = 3$ -ra, a javítás ehhez a konstrukcióhoz képest egyetlen ponttal nagyobb halmaz megadása volt, amit Zare egy mathoverflow számban [124] írt le. A következő alsó korlátokat bizonyítjuk:

2.25. Tétel (Elsholtz-Führer-Füredi-Kovács-Pach-Simon-Velich [43]).

Legyen $p \geq 5$ prímszám, ekkor

$$r_p(\mathbb{F}_p^3) \geq (p-1)^3 + p - 2\sqrt{p} = p^3 - 3p^2 + 4p - 2\sqrt{p} - 1.$$

Ez a becslés néhány speciális esetben tovább javítható.

2.26. Tétel (Elsholtz-Führer-Füredi-Kovács-Pach-Simon-Velich [43]).

Legyen p egy prímszám, amelyre $p \equiv 7 \pmod{24}$, ekkor

$$r_p(\mathbb{F}_p^3) \geq (p-1)^3 + (p-1) = p^3 - 3p^2 + 4p - 2.$$

Továbbá $r_7(\mathbb{F}_7^3) \geq 225$.

Aleksanyan és Papikian [1] a triviális $r_p(\mathbb{F}_p^n) \leq p^n - \frac{p^n-1}{p-1}$ felső korlátot adta, amely arra az észrevételre épül, hogy egy rögzített ponton átmenő összes egyenesből legalább egy pontot el kell hagyni. Speciálisan, $r_p(\mathbb{F}_p^3) \leq p^3 - p^2 - p - 1$. Az erősebb $r_p(\mathbb{F}_p^n) \leq p^n - 2p^{n-1} + 1$ és $r_p(\mathbb{F}_p^3) \leq p^3 - 2p^2 + 1$ korlátok Sziklai [117, Proposition 4.1] eredménye alapján kaphatók meg (lásd még [7], [13]). A következő új korlátot igazoljuk:

2.27. Tétel (Elsholtz-Führer-Füredi-Kovács-Pach-Simon-Velich [43]).

Legyen $p \geq 3$ egy prímszám, $k \in \{3, 4, \dots, p\}$ és $n \in \mathbb{N}$. Ekkor

$$r_k(\mathbb{F}_p^{n+1}) \leq \frac{2(p^{n+1} - 1)r_k(\mathbb{F}_p^n) + p^n - \sqrt{4(p^{n+1} - 1)r_k(\mathbb{F}_p^n)(p^n - r_k(\mathbb{F}_p^n)) + p^{2n}}}{2p^n}.$$

A háromdimenziós eset az alábbi következményt adja.

2.28. Következmény (Elsholtz-Führer-Füredi-Kovács-Pach-Simon-Velich [43]).

Legyen $p \geq 3$ egy prímszám, ekkor

$$r_p(\mathbb{F}_p^3) \leq \frac{2p^5 - 4p^4 + 2p^3 - p^2 + 4p - 2 - \sqrt{8p^6 - 20p^5 + 17p^4 - 12p^3 + 20p^2 - 16p + 4}}{2p^2},$$

speciálisan,

$$r_p(\mathbb{F}_p^3) \leq p^3 - 2p^2 - (\sqrt{2} - 1)p + 2.$$

Frankl és sztsai [56] napraforgómentes halmazokat használva az $r_p(\mathbb{F}_p^{2p}) \geq p(p-1)^{2p-1}$ alsó korlátot adták.

Találtunk egy 70 pontból álló 5AP-mentes halmazt $\mathbb{F}_5^3$ -ban, és megmutattuk a következő felső korlátokat kis prímszámokra:

2.29. Tétel (Elsholtz-Führer-Füredi-Kovács-Pach-Simon-Velich [43]).

$$r_5(\mathbb{F}_5^3) < 74.$$

2.30. Tétel (Elsholtz-Führer-Füredi-Kovács-Pach-Simon-Velich [43]).

$$r_7(\mathbb{F}_7^3) < 243.$$

A 2.13. Lemma szerint két egyenesmentes halmaz $S_1 \times S_2$ szorzatával ($S_1 \subseteq \mathbb{F}_p^{n_1}$, $S_2 \subseteq \mathbb{F}_p^{n_2}$) egy magasabb, $(n_1 + n_2)$ -dimenziós egyenesmentes halmazt kaphatunk. Ez a konstrukció az $|S_1|^{1/n_1}$ alsó korlátot adja $\alpha_p = \lim_{n \rightarrow \infty} (r_p(\mathbb{F}_p^n))^{1/n}$ értékére, és így az $(|S_1|^{1/n_1} - o(1))^n$ aszimptotikus alsó korlátot $r_p(\mathbb{F}_p^n)$ -re (lásd még pl. [33], [93]). A legerősebb ismert alsó korlát általános p esetén Frankl és sztsai [56] következő eredménye:

$$\alpha_p \geq p^{1/2p} (p-1)^{(2p-1)/2p},$$

azonban kis prímszámok esetén az új háromdimenziós alsó becsléseink, $r_5(\mathbb{F}_5^3) \geq 70$ és $r_7(\mathbb{F}_7^3) \geq 225$, jobb alsó korlátokat adnak: nevezetesen $\alpha_5 \geq 4,121$ és $\alpha_7 \geq 6,082$.

A következő alsó korlátot is igazoljuk tetszőleges dimenzióra:

2.31. Tétel (Elsholtz-Führer-Füredi-Kovács-Pach-Simon-Velich [43]).

Legyen $p \geq 3$ prímszám, ekkor $r_p(\mathbb{F}_p^n) \geq (p-1)^n + \frac{n-2}{2}(p-1)(p-2)^{n-3}$.

3. Az aszimptotikus alsó becslések bizonyítása

Ez a fejezet az aszimptotikus alsó becslések bizonyítását tartalmazza. Nevezetesen, a 2.4. Következmenyt, a 2.15. Állítást, a 2.16., 2.17., 2.18., 2.19. és 2.21. Tételeket bizonyítjuk ebben a fejezetben. A bizonyítások Salem-Spencer ötletére (különböző koordináták előfordulása gyakoriságának rögzítése), illetve Behrend-típusú konstrukciókra épülnek. Utóbbiak esetében egyszerűbb valószínűségi becsléseket (mint például a Csebisev-egyenlőtlenség) is felhasználunk. A 2.15. Állítás egy közismert észrevétel, ennek bizonyítását a teljesség kedvéért ismertetjük, illetve azért, hogy az állítás kimondásával hangsúlyozzuk a q prímszám feltétel szükségességét. (Amint említettük, modulo 6 például nem ismert az analóg állítás 6 hosszú számtani sorozatok esetén.)

4. Számtani sorozatot nem tartalmazó halmazok a $\mathbb{Z}_4^n$ csoportban

Ebben a fejezetben az $r_3(\mathbb{Z}_4^n)$ és $r_4(\mathbb{Z}_4^n)$ mennyiségekre adunk korlátokat. Az $r_3(\mathbb{Z}_4^n) \leq 3,611^n$ felső korlát bizonyításához Croot, Lev és a szerző [31] a polinom módszer egy új változatát dolgozta ki. Az értekezés ezen fejezetében a [31] cikk bizonyítását követjük, de kissé más módon mutatjuk azt be. A $\mathbb{Z}_4^n$ csoport szerkezetéből adódóan, ha a, b, c egy három hosszú számtani sorozat, akkor $c - a = 2(b - a)$ -nak az involúciók által generált részcsoporthoz kell lennie, vagyis a $\{0, 2\}^n \cong \mathbb{F}_2^n$ részcsoporthoz. (Megjegyezzük, hogy ez a részcsoporthoz egyszerre a

képe és a magja a $g \mapsto 2g$ ($g \in \mathbb{Z}_4^n$) endomorfizmusnak.) Így természetes, hogy az $r_3(\mathbb{Z}_4^n)$ érték meghatározásának problémáját átfogalmazzuk egy bizonyos feltételt kielégítő $\mathbb{F}_2^n$ -beli halmazok rendszerére vonatkozó extrémális problémává. Bár ez az átfogalmazás nem játszik döntő szerepet a bizonyításunkban, úgy gondoljuk, hogy hasznos lehet explicit módon kimondani, mivel a [31] cikkben csak implicit módon használtuk.

4.1. 3AP-mentesség halmazrendszeres átfogalmazása

Ebben a fejezetben $r_3(\mathbb{Z}_4^n)$ meghatározásának egy „halmazrendszeres megfogalmazását” adjuk, alkalmazásként egy újabb bizonyítást adunk a 2.4. Következmenyre, majd bizonyítjuk a 2.23. Tételt.

Azt mondjuk, hogy egy $A(x) \subseteq \mathbb{F}_2^n$ ($x \in \mathbb{F}_2^n$) halmazrendszer kielégíti a $(*)$ tulajdonságot, ha az alábbi következtetés teljesül:

$$\forall x \in \mathbb{F}_2^n \ (y \in x + A(x) \hat{+} A(x) \implies A(y) = \emptyset). \quad (*)$$

Jelölje $r'_3(n)$ a $\sum_{x \in \mathbb{F}_2^n} |A(x)|$ összeg maximális lehetséges értékét, ha az $\{A(x) : x \in \mathbb{F}_2^n\}$ halmazrendszer kielégíti a $(*)$ tulajdonságot.

A 4.1. Lemma bizonyítása megmutatja, hogy a $(*)$ tulajdonság éppen azt a feltételt fejezi ki, hogy a „megfelelő” $A \subseteq \mathbb{Z}_4^n$ halmaz 3AP-mentes:

4.1. Lemma. *Minden $n \geq 1$ esetén $r_3(\mathbb{Z}_4^n) = r'_3(n)$.*

A 2.23. Tétel arról a speciális esetről szól, amikor a nemüres $A(x)$ részhalmazok mind alterek. Ez egyrészt heurisztikusan egy érdekes esetnek tűnik, hiszen a $(*)$ tulajdonság egy rögzített x -re annál több üres $A(y)$ létezését követeli meg, minél nagyobb az $A(x) \hat{+} A(x)$ megszorított összeghalmaz, márpedig az alterek összeghalmaza kicsi. Másrészt, az alacsony dimenziós esetekben az derül ki, hogy amikor $\sum |A(x)|$ értéke nagy, akkor a legtöbb nemüres $A(x)$ részhalmaz valóban altér. A bizonyításunk egy lineáris algebrai ötletet, bizonyos tenszorszorzatok lineáris függetlenségét használja.

4.2. 4AP-mentesség halmazrendszeres átfogalmazása

Egy hasonló átfogalmazás adható a 4AP-mentességre is. Azt mondjuk, hogy részhalmazok egy $A(x) \subseteq \mathbb{F}_2^n$ ($x \in \mathbb{F}_2^n$) rendszere kielégíti a $(**)$ tulajdonságot, ha az alább következtetés érvényes:

$$\forall x, y \in \mathbb{F}_2^n \ (x + y \in (A(x) + A(x)) \cap (A(y) + A(y)) \implies x = y) \quad (**)$$

Jelölje $r'_4(n)$ a $\sum_{x \in \mathbb{F}_2^n} |A(x)|$ összeg maximális lehetséges méretét, ha az $\{A(x) : x \in \mathbb{F}_2^n\}$ halmazrendszer kielégíti a $(**)$ tulajdonságot.

4.2. Lemma. *Minden $n \geq 1$ esetén $r_4(\mathbb{Z}_4^n) = r'_4(n)$.*

4.3. Alsó becslés $r_3(\mathbb{Z}_4^n)$ értékére

Ez a rövid alfejezet a 2.3. Tétel bizonyítását tartalmazza. A konstrukcióban megfelelően választott részhalmazokon veszünk bináris kódokat bizonyos minimális távolsággal.

4.4. Felső becslés $r_3(\mathbb{Z}_4^n)$ értékére

Ez az alfejezet tartalmazza az értekezés legfontosabb eredményének, nevezetesen, az $r_3(\mathbb{Z}_4^n) \leq 3,611$ becslésnek a bizonyítását. Ez volt az első exponenciális javítás hasonló problémáknál, és az ennek igazolásához kidolgozott módszerünk – a polinom módszer egy új változata – számos más problémánál is hatékonynak bizonyult, a szűkebb, additív kombinatorikai terület mellett a számelmélet, geometria, algebra és a számítástudomány területén is.

A bizonyítás során polinomokkal dolgozunk. Egy többváltozós monom foka a kitevők összege, egy többváltozás polinom foka pedig az őt alkotó monomok fokainak maximuma. A polinom *multilineáris* ha minden egyes változóban lineáris.

A 2.1. Tétel bizonyítása a következő lemmán alapul.

4.3. Lemma. *Tegyük fel, hogy $n \geq 1$ és $d \geq 0$ egész számok, P egy n -változós multilineáris polinom egy $\mathbb{F}$ test felett, amelynek foka legfeljebb d , és $A \subseteq \mathbb{F}^n$ egy olyan halmaz, melyre*

$$|A| > 2 \sum_{0 \leq i \leq d/2} \binom{n}{i}.$$

Ha minden $a, b \in A$, $a \neq b$ esetén $P(a - b) = 0$, akkor $P(0) = 0$.

4.4. Megjegyzés. *A multilinearitási feltétel például cserélhető arra, hogy P minden egyes változóban korlátozott fokú. Jelölje $f_\delta(n, d)$ az olyan $x_1^{i_1} \dots x_n^{i_n}$ monomok számát, amelyekre $0 \leq i_1, \dots, i_n \leq \delta$ és $i_1 + \dots + i_n \leq d$. Ha P -ben egyetlen változó foka sem haladja meg a δ értéket, és a (teljes) fokszám legfeljebb d , akkor $|A| > 2f_\delta(n, \lfloor d/2 \rfloor)$ és $P(a - b) = 0$ ($a, b \in A$, $a \neq b$) mellett $P(0) = 0$. Továbbá, ha például $\delta = d$, vagy $\delta = |\mathbb{F}| - 1$ véges $\mathbb{F}$ esetén, akkor a változók fokára vonatkozó feltételt teljesen el is hagyhatjuk.*

4.5. Megjegyzés. *Az $|A|$ -ra vonatkozó alsó korlát nem gyengíthető jelentősen a következő példa szerint. Legyen $\mathbb{F} = \mathbb{F}_2$ és $P(x) \in \mathbb{F}_2[x_1, \dots, x_n]$ a legfeljebb d fokú multilineáris monomok összege, azaz $P(x) := \sum_{\substack{I \subseteq [n], \\ |I| \leq d}} x^I$, ahol $x^I = \prod_{i \in I} x_i$. Legyen*

$A \subseteq \mathbb{F}_2^n$ azon vektorok halmaza, amelyek legfeljebb $d/2$ darab 1-est tartalmaznak, ekkor $|A| = \sum_{0 \leq i \leq d/2} \binom{n}{i}$. Ugyanakkor $A \hat{+} A$ -ban minden vektor legfeljebb d darab 1-est tartalmaz, így a binomiális tétel szerint P eltűnik $A \hat{+} A$ -n, de $P(0) = 1 \neq 0$.

A 4.3. Lemmát és a halmazrendszeres átfogalmazást használva a következő állításon keresztül kapjuk a 2.1. Tétel bizonyítását. Az állítás arról szól, hogy a

(*) feltétel teljesülése esetén az $A(x)$ halmazok közül nem lehet *túl sok nagyon nagy*:

4.6. Állítás. *Tegyük fel, hogy $n \geq 1$ és az $A(x) \subseteq \mathbb{F}_2^n$ ($x \in \mathbb{F}_2^n$) halmazrendszer kielégíti a (*) tulajdonságot. Legyen $0 < \varepsilon < 0,25$ és*

$$B := \{x : |A(x)| \geq 2^{nH(0,5-\varepsilon)+1}\}.$$

Ekkor $|B| < 2^{nH(2\varepsilon)}$.

Az eredmény igazolása után megmutatjuk, hogy a lemma milyen alakot ölt, ha $\mathbb{Z}_4^n$ helyett $\mathbb{F}_3^n$ -ben (vagy más páratlan prímhatvány elemű test feletti vektortérben) vizsgáljuk a problémát, illetve, hogy a lemma alkalmazása hogyan alakul ebben a kontextusban. Ez utóbbi rész Ellenberg és Gijswijt [41] eredményének a cikkükben szereplőtől kicsit eltérő bemutatása.

4.5. A $\mathbb{Z}_4^n$ csoport 3AP-mentes részhalmazai, ha $n \leq 5$

Ebben a rövid alfejezetben az alacsony dimenziós pontos értékek meghatározása során alkalmazott stratégiánkat mutatjuk be.

4.6. A 2.11. Tétel bizonyítása $n \leq 4$ -re és a 2.24. Tétel bizonyítása

Ebben az alfejezetben a probléma halmazrendszeres átfogalmazását használva meghatározzuk $r_3(\mathbb{Z}_4^n)$ értékét a 4-dimenziós esetig, és az extrémális konstrukció (megfelelő értelemben vett) unicitását is igazoljuk.

4.7. Az $r_3(\mathbb{Z}_4^5) = 124$ állítás bizonyítása

Ebben az alfejezetben a 2.11. Tétel $n = 5$ esetét bizonyítjuk. Az ilyen jellegű problémákhoz hasonlóan a pontos érték meghatározása nagyon hamar nagyon nehézé válik. Ilyen típusú kérdésként említhetnénk például a Ramsey-számok, vagy közelebbi példaként, az $r_3(\mathbb{F}_3^n)$ mennyiség pontos értékének meghatározását. Utóbbi $n = 6$ -ig ismert, ott az extrémális halmaz 112 elemű egy 729 méretű csoportban, míg itt 124 elemű egy 1024 elemű csoportban. A pontos érték meghatározásához itt is a probléma halmazrendszeres átfogalmazását vizsgálva, több, kombinatorikus ötlet segítségével és esetszétválasztással jutunk el. Az ötletek részben leszámlálási jellegűek, részben lineáris algebraiak (amikor már tudjuk bizonyos részhalmazokról, hogy alterek). A kapott állítás egyrészt mutatja, hogy a 2.3. Tételben adott alsó becslésünk $n \leq 5$ -ig éles, valamint azt gondoljuk, hogy a bizonyítás során használt, időnként ad hoc jellegű ötletek között lehet olyan, amit megfelelően általánosítva alkalmazható lehet a jövőben hasonló problémáknál aszimptotikus becslések igazolásához is.

4.8. A $\mathbb{Z}_4^n$ csoport 4AP-mentes részhalmazai

Ebben az alfejezetben a 2.12. Tételt bizonyítjuk, a probléma halmazrendszeres átfogalmazását és lineáris algebrai ötleteket használva. Azért tartjuk érdekesnek $r_4(\mathbb{Z}_4^n)$ vizsgálatát, mert $\mathbb{Z}_4$ speciális szerkezete – ami 3 hosszú sorozatoknál inkább kisebb (technikai jellegű) nehézségeket okoz – 4 hosszú sorozatok esetén segíthet. Lehetségesnek tartjuk, hogy $r_4(\mathbb{Z}_4^n)$ esetében a felső becslésben egy exponenciális javítást elérni könnyebb, mint például $r_4(\mathbb{F}_5^n)$ esetében.

5. Számítási sorozatot nem tartalmazó halmazok a $\mathbb{Z}_6^n$ csoportban

Ebben a fejezetben a $\mathbb{Z}_6^n$ csoportban vizsgáljuk, hogy mekkora lehet egy k -AP-mentes halmaz, és belátjuk, hogy a válasz $k = 6$ -ra is exponenciálisan kicsi, legfeljebb $5,709^n$. A módszer ugyanakkor nagyon használja $\mathbb{Z}_6$ speciális szerkezetét, és így $\mathbb{Z}_m^n$ -re csak $6 \mid m$ esetén terjeszthetők ki eredményeink. A fejezet a [94] cikkre épül.

5.1. Halmazrendszeres átfogalmazás

Ebben az alfejezetben megadjuk $r_k(\mathbb{Z}_6^n)$ meghatározásának halmazrendszeres átfogalmazását minden $k \in \{3, 4, 5, 6\}$ mellett.

Azt mondjuk, hogy az $A(r) \subseteq \mathbb{Z}_3^n$ ($r \in \mathbb{Z}_2^n$) halmazrendszer kielégíti a

- $(*)_3$ feltételt, ha $A(r') \cup A(r'')$ 3AP-mentes minden $r', r'' \in \mathbb{Z}_2^n$ esetén,
- $(*)_4$ feltételt, ha nem lehet két különböző $r', r'' \in \mathbb{Z}_2^n$ indexet és egy a, b, c számtani sorozatot választani $\mathbb{Z}_3^n$ -ben úgy, hogy $a, b \in A(r')$ és $a, c \in A(r'')$,
- $(*)_5$ feltételt, ha nem lehet két különböző $r', r'' \in \mathbb{Z}_2^n$ indexet és egy a, b, c számtani sorozatot választani $\mathbb{Z}_3^n$ -ben úgy, hogy $a, b, c \in A(r')$ és $a, b \in A(r'')$,
- $(*)_6$ feltételt, ha $A(r') \cap A(r'')$ bármely $r', r'' \in \mathbb{Z}_2^n$ indexekre 3AP-mentes.

Megjegyezzük, hogy ebben az átfogalmazásban $\mathbb{Z}_2^n$ csak egy indexhalmaz, a struktúrája nem játszik szerepet.

A következő állítás $r_k(\mathbb{Z}_6^n)$ meghatározásának halmazrendszeres megfogalmazásait adja.

5.1. Állítás. *Legyen $k \in \{3, 4, 5, 6\}$. A legnagyobb összméretű olyan $A(r) \subseteq \mathbb{Z}_3^n$ ($r \in \mathbb{Z}_2^n$) halmazrendszer összmérete, melyre teljesül a $(*)_k$ tulajdonság $r_k(\mathbb{Z}_6^n)$.*

Megemlítjük, hogy $\mathbb{Z}_6$ felett a 3AP-mentes halmazok vizsgálata ekvivalens a kérdés $\mathbb{Z}_3$ feletti vizsgálatával:

5.2. Állítás. *3AP-mentes részhalmazokra következő összefüggés érvényes:*

$$r_3(\mathbb{Z}_6^n) = 2^n r_3(\mathbb{Z}_3^n).$$

Általánosabban is, $r_3(\mathbb{Z}_m^n)$ vizsgálata $m \equiv 2 \pmod{4}$ esetén a páratlan esettel ekvivalens:

5.3. Állítás. *Ha $m = 4M + 2$ valamely M egész számra, akkor*

$$r_3(\mathbb{Z}_m^n) = 2^n r_3(\mathbb{Z}_{m/2}^n).$$

5.2. Bizonyítások

Ebben az alfejezetben a 2.7., 2.8. és 2.10. Tételeket bizonyítjuk. Az $r_6(\mathbb{Z}_6^n)$ érték meghatározásának halmazrendszeres megfogalmazásánál az kap fontos szerepet, hogy ha $\mathbb{Z}_3^n$ egy részhalmaza kellően nagy, akkor nagyon sok 3AP-t tartalmaz.

5.3. Megjegyzések

Ebben az alfejezetben néhány általános megjegyzés mellett a kapott eredmény egy lehetséges alkalmazását mutatjuk be 3 hosszú geometriai sorozatot nem tartalmazó halmazokra.

6. Egyenesmentes halmazokra vonatkozó eredmények bizonyítása

Ebben a fejezetben egyenesmentes halmazokra vonatkozó eredményeinket – melyeket a 2.2. alfejezetben mutattunk be – igazoljuk. A fejezet a [43] cikkekre épül.

6.1. A felső becslések bizonyítása

A 2.27. Tétel, a 2.28. Következmény, a 2.29. és 2.30. Tételek bizonyítását tartalmazza ez az alfejezet.

6.2. Az alsó becslések bizonyítása

A 2.31., 2.25. és 2.26. Tételeket bizonyítjuk ebben az alfejezetben.

7. A szeletrangmódszer alkalmazásai

Ebben a fejezetben először az úgynevezett *szeletrangmódszert* (*slice rank method*) mutatjuk be. Ez a Croot, Lev és a szerző [31] által kidolgozott polinom módszer Tao által adott szimmetrikus változata. A szeletrangmódszer bemutatását lásd [119, 112] blogbejegyzésekben.

7.1. A szeletrangmódszer

Legyenek $A_1, \dots, A_k$ véges halmazok, $\mathbb{F}$ pedig egy test. Azt mondjuk, hogy

$$h : A_1 \times \dots \times A_k \rightarrow \mathbb{F}$$

szeletrangja 1, ha

$$h(x_1, \dots, x_k) = f(x_i)g(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_k)$$

bizonyos $1 \leq i \leq k$ esetén. Az $F : A_1 \times \dots \times A_k \rightarrow \mathbb{F}$ szeletrangja, amelyet slice-rank(F)-fel jelölünk, a legkisebb olyan r , hogy $F = \sum_{i=1}^r h_i$, ahol a h_i függvények szeletrangja 1. Megjegyezzük, hogy $k = 2$ esetén a szeletrang egybeesik a szokásos mátrixranggal.

A következő lemmát [119] többször is alkalmazni fogjuk:

7.1. Lemma. *Legyen A egy véges halmaz, és legyen $F : \underbrace{A \times \dots \times A}_k \rightarrow \mathbb{F}$ egy diagonális tenzor, amely tehát csak a diagonálisán vesz fel nemnulla értékeket, azaz,*

$$F(x_1, \dots, x_k) = \sum_{a \in A} c_a \delta_a(x_1) \dots \delta_a(x_k),$$

$$\text{ahol } c_a \neq 0 \text{ } (a \in A) \text{ és } \delta_a(x) = \begin{cases} 1 & x = a \\ 0 & x \neq a \end{cases}.$$

Ekkor

$$\text{slice-rank}(F) = |A|.$$

Ezt úgy fogjuk bizonyos feltételeknek eleget tevő halmazok méretének korlátozására használni, hogy találunk egy F diagonális tenzort, majd ezután elegendő lesz F szeletrangját felülről becsülni.

7.2. Derékszögmentes halmazok

Olyan problémákat vizsgálunk, amelyek bizonyos geometriai konfigurációkat elkerülő halmazok lehető legnagyobb méretének meghatározására vonatkoznak. Kérdéseink egy része kódelméleti problémákhoz kapcsolódik.

Legyen q egy páratlan prímszám, n pedig egy pozitív egész szám. Egy derékszög $\mathbb{F}_q^n$ -ben egy olyan $x, y, z \in \mathbb{F}_q^n$ hármas, amelynek elemei különbözők és

$$\langle x - z, y - z \rangle = 0,$$

ahol $\langle \cdot, \cdot \rangle$ a standard skaláris szorzatot jelöli.

Jelölje $R(n, q)$ az $\mathbb{F}_q^n$ tér legnagyobb olyan részhalmazának méretét, amely nem tartalmaz derékszöget.

Bennett [11] bebizonyította, hogy

$$R(n, q) \ll q^{\frac{n+2}{3}}.$$

Ge és Shangguan [57] a szeletrangmódszerrel javították ezt a korlátot rögzített q és nagy n esetén, nevezetesen, megmutatták, hogy

$$R(n, q) \leq \binom{n+q}{q-1} + 3,$$

vagyis rögzített q esetén az $R(n, q)$ mennyiség n -ben polinomiális. Megemlíteték, hogy a standard ortonormált bázis az $R(n, q) \geq n$ alsó korlátot adja és azt sejtették, hogy a felső korlátjuk aszimptotikusan pontos (rögzített q esetén):

7.2. Sejtés (Ge-Shangguan, [57]). *Bármely rögzített q prímszám esetén*

$$R(n, q) = \Theta(n^{q-1}).$$

Naslund [86] tovább javította az $R(n, q)$ felső korlátját, megmutatva, hogy

$$R(n, q) \leq \binom{n+q}{q-1} + 2 - \binom{n+q}{q-3}.$$

Megmutatjuk, hogy minden páratlan q prímszám esetén valójában $R(n, q) \ll n^{q-2}$, ami megcáfolja a 7.2. Sejtést:

7.3. Tétel (Bursics-Matolcsi-Pach-Schrettner [22]). *Legyen q egy páratlan prímszám. Ha egy $A \subseteq \mathbb{F}_q^n$ halmaz nem tartalmaz derékszöget, azaz három különböző vektort, melyekre $\langle x-z, y-z \rangle = 0$, akkor*

$$|A| \leq 2(q-1)q \binom{n+q-2}{q-2} + 2q.$$

Naslund a derékszög konfiguráció egy általánosított változatát is vizsgálta. Azt mondjuk, hogy az $x_0, x_1, \dots, x_k$ vektorok k -derékszöget alkotnak, ha különbözők, és $x_1 - x_0, \dots, x_k - x_0$ egy ortogonális vektor- k -ast alkotnak, azaz $\langle x_i - x_0, x_j - x_0 \rangle = 0$ minden $1 \leq i < j \leq k$ esetén. (Speciálisan, a 2-derékszög egy derékszög.) Naslund bebizonyította, hogy ha k egész szám és $q = p^r$ páratlan prímszám $p > k$ mellett, akkor ha egy $A \subseteq \mathbb{F}_q^n$ részhalmazra

$$|A| > \binom{n + (k-1)q}{(k-1)(q-1)}, \quad (3)$$

akkor A tartalmaz k -derékszöget.

Ennél a problémánál a következő alsó korlátot adjuk:

7.4. Tétel (Bursics-Matolcsi-Pach-Schretnner [22]). *Legyen q egy páratlan prím-szám és $2 \leq k$ egy egész szám. Létezik olyan $A \subseteq \mathbb{F}_q^n$ részhalmaz, melyre*

$$|A| \geq (1 - o(1)) \cdot \binom{n}{\lceil \frac{k-1}{k} k \lfloor \frac{k}{2k-1} q \rfloor \rceil} / \binom{\lfloor \frac{k}{2k-1} q \rfloor}{\lceil \frac{k-1}{k} k \lfloor \frac{k}{2k-1} q \rfloor \rceil}$$

és A nem tartalmaz egyetlen k -derékszöget sem, azaz nem tartalmaz olyan $x_0, x_1, \dots, x_k$ vektorokat, hogy

$$\langle x_i - x_0, x_j - x_0 \rangle = 0$$

minden $1 \leq i < j \leq k$ esetén.

A $k = 2$ speciális esetben a 7.4. Tétel a következő alsó korlátot adja $R(n, q)$ -ra:

7.5. Következmény (Bursics-Matolcsi-Pach-Schretnner [22]). *Legyen q egy páratlan prímszám. Létezik olyan $A \subset \mathbb{F}_q^n$ halmaz, melyre*

$$|A| \geq (1 - o(1)) \cdot \binom{n}{\lceil \frac{1}{2} \lfloor \frac{2}{3} q \rfloor \rceil} / \binom{\lfloor \frac{2}{3} q \rfloor}{\lceil \frac{1}{2} \lfloor \frac{2}{3} q \rfloor \rceil}$$

és A nem tartalmaz derékszöget, azaz nem lehet olyan $x, y, z \in A$ különböző vektorokat választani, hogy $\langle y - x, z - x \rangle = 0$.

Vagyis $R(n, q) \gg n^{\lfloor \frac{q-1}{3} \rfloor}$. Megjegyezzük, hogy ebben a korlátban a kitevő a $q/3$ -hoz legközelebbi egész szám.

Ezen problémák motiválták, hogy a következő kérdést is vizsgáljuk: Mekkora lehet egy $A \subseteq \mathbb{F}_q^n$ halmaz, ha nem tartalmaz olyan háromszöget, amely csupa-derékszögű, azaz nincsenek olyan $x, y, z \in A$ különböző vektorok, amelyekre

$$\langle x - y, y - z \rangle = \langle y - z, z - x \rangle = \langle z - x, x - y \rangle = 0?$$

A szeletrangmódszerrel a következő felső korlátot adjuk:

7.6. Tétel (Bursics-Matolcsi-Pach-Schretnner [22]). *Legyen q egy páratlan prímszám. Ha $A \subseteq \mathbb{F}_q^n$ nem tartalmaz csupa-derékszögű háromszöget, azaz olyan x, y, z különböző vektorokat, hogy*

$$\langle x - y, y - z \rangle = \langle y - z, z - x \rangle = \langle z - x, x - y \rangle = 0,$$

akkor

$$|A| \leq \binom{n+2q-2}{2q-2} + \binom{n+2q-3}{2q-3} + 2 \left(\binom{n+q-1}{q-1} + \binom{n+q-2}{q-2} \right).$$

Egy kapcsolódó kérdésnél az alábbiakat bizonyítjuk:

7.7. Tétel (Bursics-Matolcsi-Pach-Schretnner [22]). *Legyen q egy páratlan prím-szám. Legyen $S(n, q)$ az $\mathbb{F}_q^n$ tér legnagyobb olyan halmazának mérete, amely nem tartalmaz olyan x, y különböző vektorokat, hogy $\langle x - y, x - y \rangle = 0$. A következők teljesülnek:*

$$\binom{n}{q-1} \leq S(n, q) \leq \binom{n+q}{q-1} - \binom{n+q-2}{q-3}.$$

Továbbá, ha $n \not\equiv -2 \pmod{q}$ vagy $q \equiv 1 \pmod{4}$, akkor

$$S(n, q) \geq \binom{n}{q-1} + \binom{n}{q-2}.$$

A $q = 3$ speciális esetben tovább javíthatjuk a 7.7. Tétel alsó korlátját, ha feltételezzük, hogy az n szám 3-mal osztva 2 maradékot ad. Tudunk ugyanis konstruálni egy a feltételeknek megfelelő, $\binom{n+3}{2} - 1$ méretű halmazt, ami egyben az általános felső korlátunk. Végtelen sok esetben tehát a pontos válasz a következő:

7.8. Tétel (Bursics-Matolcsi-Pach-Schretnner [22]). *Ha $n \equiv 2 \pmod{3}$, akkor*

$$S(n, 3) = \binom{n+3}{2} - 1.$$

Ez a kérdés kapcsolódik egy kódelméleti problémához is, amelynél a következőket bizonyítjuk:

7.9. Tétel (Bursics-Matolcsi-Pach-Schretnner [22]). *Legyen q egy páratlan prím-szám. Legyen $T(n, q)$ az $\{a, b\}^n$ legnagyobb olyan részhalmazának mérete, amelyben nincs két olyan vektor, amelyek Hamming-távolsága osztható q -val. Ekkor a következő korlátok érvényesek:*

$$\begin{aligned} T(n, q) &\leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0} && \text{tetszőleges } n\text{-re,} \\ T(n, q) &\leq \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0} && \text{ha } n \equiv 0 \pmod{q}, \\ T(n, q) &\geq \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0} && \text{tetszőleges } n\text{-re,} \\ T(n, q) &\geq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0} && \text{ha } n \equiv -1 \pmod{q}. \end{aligned}$$

Tehát a 7.9. Tétel $n \equiv 0$ és $-1 \pmod{q}$ esetén megadja a pontos értéket.

Megjegyezzük, hogy a 7.9. Tételből az általános felső korlát Delsarte [34] egy klasszikus eredménye. Később különböző bizonyításokat adtak rá Frankl [55, Theorem 1.6], illetve Babai és sztsai [6]. Megjegyezzük, hogy Delsarte korlátja kapcsolatban áll a híres Ray-Chaudhuri-Wilson [102] tétellel, amely szerint egy n elemű halmaz k részhalmaza közül legfeljebb $\binom{n}{s}$ darab választható ki úgy, hogy legfeljebb s féle lehetséges mérete legyen a metszeteknek. Valójában ez az eredmény volt Delsarte motivációja a probléma vizsgálatára.

Ebben a dolgozatban a prím esetet vizsgáljuk, az állításnak egy újabb bizonyítását adjuk, és egy általános alsó korlátot igazolunk. Továbbá megmutatjuk, hogy mind az alsó, mind a felső korlát végtelen sok esetben éles.

7.3. Bizonyítások

Ebben az alfejezetben az utolsó fejezetben szereplő állításokat bizonyítjuk: a 7.3., 7.4., 7.6., 7.7., 7.8. és 7.9. Tételeket.

Hivatkozások

- [1] A. Aleksanyan and M. Papikian, On Blocking Sets of Affine Spaces, (1999) arXiv: 9910084
- [2] N. Alon, Combinatorial Nullstellensatz, Combinatorics, Probability and Computing 8 (1999) 7–29.
- [3] N. Alon and M. Dubiner, Zero-sum sets of prescribed size, in: „Combinatorics, Paul Erdős is Eighty”, Bolyai Society, Mathematical Studies, Keszthely, Hungary (1993) 33–50.
- [4] N. Alon and M. Dubiner, A lattice point problem and additive number theory, Combinatorica 15 (1995) 301–309.
- [5] N. Alon, A. Shpilka, C. Umans, On sunflowers and matrix multiplication, Comput. Complexity 22 (2013) no. 2, 219–243.
- [6] L. Babai, H. Snevily, R. M. Wilson, A new proof of several inequalities on codes and sets, Journal of Combinatorial Theory, Series A 71 (1) (1995) 146–153.
- [7] S. Ball, The polynomial method in Galois geometries (2009) <https://web.mat.upc.edu/simeon.michael.ball/polynomialmethod.pdf>
- [8] E. Bannai and E. Bannai, An upper bound for the cardinality of an s -distance subset in real Euclidean space, Combinatorica, 1 (2) (1981) 99–102.
- [9] M. Bateman and N. H. Katz, New bounds on cap sets, J. Amer. Math. Soc. 25 (2012) no. 2, 585–613.
- [10] F. A. Behrend, On sets of integers which contain no three terms in arithmetical progression, Proc. Natl. Acad. Sci. USA 32 (1946) 331–332.
- [11] M. Bennett, Occurrence of right angles in vector spaces over finite fields, European Journal of Combinatorics 70 (2018) 155–163.
- [12] J. Bierbrauer and Y. Edel, Large caps in small spaces, Des. Codes Cryptogr. 23 (2001) no. 2, 197–212.
- [13] A. Bishnoi, J. D’haeseleer, D. Gijswijt, A. Potukuchi, Blocking sets, minimal codes and trifferent codes, arXiv:2301.09457
- [14] J. Blasiak, T. Church, H. Cohn, J. Grochow, E. Naslund, W. Sawin, C. Umans, On cap sets and the group-theoretic approach to matrix multiplication, Discrete Anal. (2017) Paper No. 3, 27 pp.

- [15] T. Bloom and O. Sisask, Breaking the logarithmic barrier in Roth’s theorem on arithmetic progressions, arXiv:2007.03528
- [16] T. Bloom and O. Sisask, The Kelley–Meka bounds for sets free of three-term arithmetic progressions, arXiv:2302.07211
- [17] T. Bloom and O. Sisask, An improvement to the Kelley-Meka bounds on three-term arithmetic progressions, arXiv:2309.02353
- [18] J. Bourgain, On triples in arithmetic progression, *Geom. Funct. Anal.* 9 (5) (1999) 968–984.
- [19] J. Bourgain, Roth’s theorem on progressions revisited, *J. Anal. Math.* 104 (2008) 155–192.
- [20] A. E. Brouwer and A. Schrijver, The blocking number of an affine space, *J. Combinatorial Theory Ser. A* 24.2 (1978) 251–253.
- [21] T. C. Brown and J. P. Buhler, A density version of a geometric Ramsey theorem, *J. Combin. Theory Ser. A* 25 (1982) 20–34.
- [22] B. Bursics, D. Matolcsi, P.P. Pach, J. Schrejtner, Avoiding right angles and certain Hamming distances, *Linear Algebra and its Applications* 677 (2023) 71–87.
- [23] A. R. Calderbank and P. C. Fishburn, Maximal three-independent subsets of $\{0,1,2\}^n$, *Des. Codes Cryptogr.* 4 (1994) no. 3, 203–211.
- [24] P. J. Cameron, Sum-free sets of a square, manuscript, available at <http://www.maths.qmul.ac.uk/~pjc/odds/sfsq.pdf>
- [25] A. K. Chandra, On the solution of Moser’s problem in four dimensions, *Canad. Math. Bull.* 16 (1973) 507–511.
- [26] V. Chvátal, Remarks on a problem of Moser, *Canad. Math. Bull.* 15 (1972) 19–21.
- [27] V. Chvátal, Edmonds polytopes and a hierarchy of combinatorial problems, *Discrete Math.* 4 (1973) 305–337. Reprinted: *Discrete Math.* 306 (2006) 886–904.
- [28] D. Coppersmith and S. Winograd, Matrix multiplication via arithmetic progressions, *STOC ’87* (Proceedings of the nineteenth annual ACM symposium on Theory of computing) Pages 1–6, also: *Journal of Symbolic Computation* 9 no. 3 (1990) 251–280.
- [29] E. Croot, The minimal number of three-term arithmetic progressions modulo a prime converges to a limit, *Canad. Math. Bull.* 51 (2008) no. 1, 47–56.

- [30] E. Croot and O. Sisask, A probabilistic technique for finding almost-periods of convolutions, *Geom. Funct. Anal.* 20 (2010) 1367–1396.
- [31] E. Croot, V.F. Lev, P.P. Pach, Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small, *Ann. of Math.* (2) 185 (2017) no. 1, 331–337.
- [32] E. Croot, V.F. Lev, P.P. Pach, Past and future of the cap set problem, submitted (conference paper, International Congress of Basic Science, Beijing) (2024)
- [33] B. L. Davis and D. MacLagan, The card game SET, *Math. Intelligencer* 25 (2003) no. 3, 33–40.
- [34] P. Delsarte, Four Fundamental Parameters of a Code and Their Combinatorial Significance, *Information and Control* 23 (1973) 407–438.
- [35] Z. Dvir: On the size of Kakeya sets in finite fields, *Journal of the American Mathematical Society* 22.4 (2008) pp. 1093–1097.
- [36] Y. Edel, Extensions of generalized product caps, *Des. Codes Cryptography* 31 (2004) 5–14.
- [37] Y. Edel, Sequences in abelian groups G of odd order without zero-sum subsequences of length $\exp(G)$, *Des. Codes Cryptogr.* 47 (2008) no. 1-3, 125–134.
- [38] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin, L. Rackham, Zero-sum problems in finite abelian groups and affine caps, *Q. J. Math.* 58 (2007) no. 2, 159–186.
- [39] Y. Edel, S. Ferret, I. Landjev, L. Storme, The classification of the largest caps in $AG(5, 3)$, *J. Combin. Theory Ser. A* 99 (2002) 95–110.
- [40] M. Elkin, An Improved Construction of Progression-Free Sets, *Israeli J. Math.* 184 (2011) 93–128.
- [41] J. S. Ellenberg and D. Gijswijt, On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression, *Ann. of Math.* (2) 185 (2017) no. 1, 339–343.
- [42] C. Elsholtz, Lower bounds for multidimensional zero sums, *Combinatorica* 24 (2004) no. 3, 351–358.
- [43] C. Elsholtz, J. Führer, E. Füredi, B. Kovács, P. P. Pach, D. G. Simon, N. Velich, Maximal line-free sets in $\mathbb{F}_p^n$, *Periodica Mathematica Hungarica*, to appear
- [44] C. Elsholtz, Z. Hunter, L. Proske, L. Sauermann, Improving Behrend’s construction: Sets without arithmetic progressions in integers and over finite fields, [arXiv:2406.12290](https://arxiv.org/abs/2406.12290)

- [45] C. Elsholtz and P. P. Pach, Des. Codes Cryptography 88 (2020) 2133–2170.
- [46] C. Elsholtz and L. Rackham, Maximal sum-free sets of integer lattice grids, J. Lond. Math. Soc. (2) 95 (2017) no. 2, 353–372.
- [47] P. Erdős, Problems in number theory and combinatorics, Proceedings of the Sixth Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1976), Congress. Numer., XVIII, pages 35–58. Utilitas Math., Winnipeg, Man. (1977)
- [48] P. Erdős, A. Ginzburg, A. Ziv, Theorem in the additive number theory, Bull. Res. Council Israel F (10) (1961) 41–43.
- [49] P. Erdős, Problems and results on combinatorial number theory, in: A survey of Combinatorial Theory, J.N Srivastava et al., eds, North Holland (1973) 117–138.
- [50] P. Erdős and Z. Füredi, The greatest angle among n points in the d -dimensional Euclidean space, In Combinatorial mathematics (Marseille-Luminy, 1981), volume 75 of NorthHolland Math. Stud., pages 275–283. North-Holland, Amsterdam (1983)
- [51] P. Erdős, P. Frankl, Z. Füredi, Families of finite sets in which no set is covered by the union of two others, Journal of Combinatorial Theory, Series A 33 (2) (1982) 158–166.
- [52] P. Erdős and P. Turán, On some sequences of integers, J. London Math. Soc. 11 (1936) 261–264.
- [53] K. J. Falconer, On a problem of Erdős on fractal combinatorial geometry, J. Combin. Theory Ser. A, 59(1) (1992) 142–148.
- [54] J. Fox and L. M. Lovász, A tight bound for Green’s arithmetic triangle removal lemma in vector spaces, Adv. Math. 321 (2017) 287–297.
- [55] P. Frankl, Orthogonal vectors in the n -dimensional cube and codes with missing distances, Combinatorica 6 (3) (1986) 279–285.
- [56] P. Frankl, R. L. Graham, V. Rödl, On subsets of abelian groups with no 3-term arithmetic progression, J. Comb. Theory, Ser. A 45(1) (1987) 157–161.
- [57] G. Ge and C. Shangguan, Maximum subsets of $\mathbb{F}_q^n$ containing no right angles, J. Algebr. Comb. (2019) <https://doi.org/10.1007/s10801-019-00908-4>
- [58] W. T. Gowers, A new proof of Szemerédi’s theorem, Geom. Funct. Anal. 11 (3) (2001) 465–588.

- [59] W. T. Gowers, Generalizations of Fourier analysis, and how to apply them, *Bull. Amer. Math. Soc.* 54 (2017) 1–44.
- [60] B. J. Green, Finite field models in additive combinatorics, *Surveys in Combinatorics 2005*, London Math. Soc. Lecture Note Ser., vol. 327, Cambridge University Press (2005) pp. 1–27.
- [61] B. Green and T. Tao, New bounds for Szemerédi’s theorem. I. Progressions of length 4 in finite field geometries. *Proc. Lond. Math. Soc.* (3) 98 (2009), no. 2, 365–392.
and correction: New bounds for Szemerédi’s theorem, Ia: Progressions of length 4 in finite field geometries revisited, 16 pages, arXiv:1205.1330
- [62] B. Green and T. Tao, New bounds for Szemerédi’s theorem. II. A new bound for $r_4(N)$, *Analytic number theory*, Cambridge Univ. Press, Cambridge (2009) pp. 180–204.
- [63] B. Green and T. Tao, New bounds for Szemerédi’s theorem, III: a polylogarithmic bound for $r_4(N)$, *Mathematika* 63 (2017) 944–1040.
- [64] J. A. Grochow, New applications of the polynomial method: The cap set conjecture and beyond, *Bulletin of the American Mathematical Society* 56 (2019) no. 1, 29–64.
- [65] L. Guth and N. H. Katz, On the Erdős distinct distances problem in the plane, *Annals of Mathematics* 181 (1) (2015) 155–190.
- [66] A. W. Hales and R. I. Jewett, Regularity and positional games, *Trans. Amer. Math. Soc.* 106 (1963) 222–229.
- [67] V. Harangi, T. Keleti, G. Kiss, P. Maga, A. Máthé, P. Mattila, B. Strenner, How large dimension guarantees a given angle?, *Monatsh. Math.*, 171(2):169–187 (2013)
- [68] D. R. Heath-Brown, Integer sets containing no arithmetic progressions, *J. London Math. Soc.* 35 (1987) 385–394.
- [69] G. Hegedüs, A new exponential upper bound for the Erdős-Ginzburg-Ziv constant, arXiv:1712.00228
- [70] R. E. Jamison, Covering finite fields with cosets of subspaces, *J. Combinatorial Theory Ser. A* 22.3 (1977) 253–266.
- [71] Z. Jiang, Improved explicit upper bounds for the Cap Set Problem, arXiv:2103.06481

- [72] G. Kalai, Webblog, 7th February 2009,
<http://gilkalai.wordpress.com/2009/02/07/frankl-rodls-theorem-and-variations-on-the-cap-set-problem-a-recent-research-project-with-roy-meshulam-a/>
- [73] Z. Kelley and R. Meka, Strong bounds for 3-Progressions, 2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS), 933–973.
- [74] J. Kim, H. Liu, P. P. Pach, Optimal polynomial Schur’s theorem, submitted arXiv:2404.00794
- [75] J. Komlós, solution to problem P.170 by Leo Moser, *Canad. Math. Bull.* vol. 15 (1972) 312–313.
- [76] J. Leng, A. Sah, M. Sawhney, Improved bounds for Szemerédi’s theorem, arXiv:2402.17995
- [77] V. F. Lev, Progression-free sets in finite abelian groups, *J. Number Theory* 104 (2004) 162–169.
- [78] V. Lev, Character-free approach to progression-free sets, *Finite Fields Their Appl.* 18 (2012) 378–383.
- [79] Y. Lin and J. Wolf, Subsets of $\mathbb{F}_q^n$ containing no k -term progressions, *European J. Combin.*, 31(5) (2010) 1398–1403.
- [80] H. Liu, P. P. Pach, C. Sándor, Polynomial Schur’s Theorem, *Combinatorica* (2) (2022) 1357–1384.
- [81] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland (1977)
- [82] N. McNew, On sets of integers which contain no three terms in geometric progression, *Mathematics of Computation* 84 (2015) 2893–2910.
- [83] R. Meshulam, On subsets of finite abelian groups with no 3-term arithmetic progressions, *J. Comb. Theory, Ser. A* 71 (1995) 168–172.
- [84] L. Moser, Problem P.170 in *Canad. Math. Bull.* 13 (1970) 268
- [85] E. Naslund, Exponential Bounds for the Erdős-Ginzburg-Ziv constant, *J. Combin. Theory Ser. A* 174 (2020) 105185, 19 pp.
- [86] E. Naslund, The partition rank of a tensor and k -right corners in $\mathbb{F}_q^n$, *Journal of Combinatorial Theory, Series A* 174 (2020) 105190
- [87] E. Naslund, Lower bounds for the Shannon Capacity of Hypergraphs, manuscript (2024)

- [88] E. Naslund and W. Sawin, Upper bounds for sunflower-free sets, *Forum Math. Sigma* 5 (2017) e15
- [89] L. Newcombe, MSc Thesis, Royal Holloway (2008)
- [90] J. Nagy and P. P. Pach, The Alon-Jaeger-Tarsi conjecture via group ring identities, *Journal of the Eur. Math. Soc.*, to appear
- [91] J. Nagy, P. P. Pach, I. Tomon, Additive bases, coset covers, and non-vanishing linear maps, *arXiv:2111.13658*
- [92] P. P. Pach, Monochromatic solutions to the equation $x + y = z^2$ in the interval $[N, cN^4]$, *Bulletin of the London Mathematical Society* 50 (6) (2018) 1113–1116.
- [93] P. P. Pach: Bounds on the size of progression-free sets in $\mathbb{Z}_m^n$, *Unif. Distrib. Theory* 17 (2022) no.1, 1–10.
- [94] P. P. Pach and R. Palincza, Sets avoiding six-term arithmetic progressions in $\mathbb{Z}_6^n$ are exponentially small, *SIAM Journal on Discrete Mathematics* 36 (2) (2022) 1135–1142.
- [95] S. Peluse, Finite field models in arithmetic combinatorics – twenty years on, *arXiv:2312.08100*
- [96] F. Petrov, Combinatorial Results Implied by Many Zero Divisors in a Group Ring, *Funct. Anal. Appl.* 58 (2024) 80–89.
- [97] F. Petrov and C. Pohoata, Improved Bounds for Progression-Free Sets in C_8^n , *Israel J. Math.* 236 (2020) no. 1, 345–363.
- [98] D. H. J. Polymath, Density Hales-Jewett and Moser numbers, in: *An irregular mind*, 689–753, *Bolyai Soc. Math. Stud.* 21 János Bolyai Math. Soc., Budapest (2010)
- [99] C. Pohoata, O. Roche-Newton, Four-term progression free sets with three-term progressions in all large subsets, *Random Structure & Algorithms* 60 (4) (2022) 749–770.
- [100] A. Potechin, Maximal caps in $AG(6, 3)$. *Des. Codes Cryptogr.* 46 (2008) no. 3, 243–259.
- [101] R. A. Rankin, Representations of a number as the sum of a large number of squares. *Proc. Roy. Soc. Edinburgh Sect. A* 65 1960/1961, 318–331.
- [102] D. K. Ray-Chaudhuri and R. M. Wilson, On t -designs, *Osaka J. Math.* 12 (1975) 737–744.

- [103] C. Reiher, On Kemnitz' conjecture concerning lattice-points in the plane, *The Ramanujan Journal* 13 (2007) 333–337.
- [104] J. Riddell, A lattice point problem related to sets containing no ℓ -term arithmetic progression, *Canad Math. Bull.* 14 (1971) 535–538.
- [105] B. Romera-Paredes, M. Barekatin, A. Novikov, M. Balog, M. Kumar, E. Dupont, F. Ruiz, J. Ellenberg, P. Wang, O. Fawzi, P. Kohli, A. Fawzi, Mathematical discoveries from program search with large language models, *Nature* 625 (2023) 468–475.
- [106] K. F. Roth, On certain sets of integers, *J. Lond. Math. Soc.* (2) 28 (1) (1953) 104–109.
- [107] V. Rödl, On a Packing and Covering Problem, *European Journal of Combinatorics* 6 (1) (1985) 69–78.
- [108] R. Salem and D. C. Spencer, On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. Sci. U. S. A.* 28 (1942) 561–563.
- [109] T. Sanders, Roth's theorem in $\mathbb{Z}_4^n$. *Anal. PDE* 2 (2009) no. 2, 211–234.
- [110] T. Sanders, On Roth's theorem on progressions, *Ann. of Math.* (2) 174 (1) (2011) 619–636.
- [111] T. Sanders, On certain other sets of integers, *J. Anal. Math.* 116 (2012) 53–82.
- [112] W. Sawin and T. Tao, Notes on the slice rank of tensors, <https://terrytao.wordpress.com/2016/08/24/notes-on-the-slice-rank-of-tensors/> (2016)
- [113] C. E. Shannon, The zero-Error capacity of a noisy channel, *IRE Trans. Inform. Theory.* 2. (1956) 8–19.
- [114] D. Speyer, <https://sbseminar.wordpress.com/2016/07/08/bounds-for-sum-free-sets-inprime-power-cyclic-groups-three-ways/>
- [115] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression. *Acta Arith.* 27 (1975) 199–245.
- [116] E. Szemerédi, Integer sets containing no arithmetic progressions, *Acta Math. Hungar.* 56 (1990) 155–158.
- [117] P. Sziklai, Nuclei of pointsets in $PG(n, q)$, In: vol. 174. 1-3. *Combinatorics* (Rome and Montesilvano, 1994) (1997) 323–327.

- [118] T. Tao, Webblog, 23rd February 2007
<http://terrytao.wordpress.com/2007/02/23/open-question-best-bounds-for-cap-sets/>
Open question: best bounds for cap sets
- [119] 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> (2016)
- [120] T. Tao and V. Vu, Additive Combinatorics, Cambridge University Press (2006)
- [121] F. Tyrrell, New lower bounds for cap sets, Discrete Anal. (2023) Paper No. 20, 18pp.
- [122] V. Vassilevska Williams, Multiplying matrices faster than Coppersmith-Winograd, STOC'12–Proceedings of the 2012 ACM Symposium on Theory of Computing, 887–898, ACM, New York (2012)
- [123] J. Wolf, Finite field models in arithmetic combinatorics—ten years on, Finite Fields Appl. 32 (2015) 233–274.
- [124] D. Zare, <https://mathoverflow.net/q/229442>