

EÖTVÖS LORÁND TUDOMÁNYEGYETEM
TERMÉSZETTUDOMÁNYI KAR

Mikulás Zsófia

ÁLTALÁNOSÍTOTT ÍVEK VÉGES
TEREKBEN

SZAKDOLGOZAT

Matematikus MSc

Témavezető:

Dr. Kiss György, habilitált egyetemi docens

Geometriai Tanszék



Budapest, 2025.

Ezúton is szeretnék köszönetet mondani témavezetőmnek, Kiss Györgynek, akinek az óráin sokat tanultam a véges geometriákról, melynek nyomán megszilárdult bennem a gondolat, hogy szívesen foglalkoznék a témakörrel mélyebben is. Köszönöm a tartalmas konzultációkat, ahol értékes megjegyzéseivel, észrevételeivel és javaslataival segítette helyes irányba terelni a gondolataimat. Külön hálás vagyok azért is, hogy mindig mindent alaposan átnézett már a dolgozat korai vázlaiban is.

Köszönöm az oktatóimnak, akik átadott tudásukkal, egy-egy témakör szépségére rámutatva, formálták a matematika iránti lelkesedésemet, többnyire pozitív irányba mozdítva azt. Köszönettel tartozom Szőnyi Tamásnak, aki a kódelméleti előadásai mellett, készségesen segített a blokkoló halmazokkal kapcsolatos kérdéseim megválaszolásában is.

Meleg szívvel gondolok a családomra, a barátaimra, és a Bolyai Kollégium közösségére, akik támogatásukkal és a mindennapjaim szebbé tételével segítették a tanulmányaim elvégzését, így e dolgozat létrejöttét is. Külön szeretném kiemelni régi barátomat, Annát, akinek támogatása ennyi év után is töretlen, továbbá a szobatársaimat, akik hősiezen tolerálták a gyakran változó bioritmusomat.

Végezetül, egy kedves barátom nyomására, kénytelen vagyok megosztani a vizsgaidőszakaim mélypontjának egyik melléktermékét.

- Melyik a legerősebb mátrix?

- ...?

- Az egységmátrix, mert az helyben hagyja az összes többi.

Áttekintés

A dolgozat témája, a véges terekben vizsgált általánosított ívek elmélete, a véges geometria egyik kiemelten aktív kutatási területe. Az íveket először véges síkokon definiálták, mint olyan ponthalmazok, melyek elemei között nincs három kollineáris. A diplomamunka során ennek a fogalomnak egy szokásos általánosítását jártuk körbe.

Az n -dimenziós véges térbeli (k, r) -ív olyan ponthalmaz, amely bármely hipersíkot legfeljebb r pontban metsz. Ezek a struktúrák nemcsak tisztán geometriai szempontból érdekesek, hanem szoros kapcsolatot mutatnak kódelméleti fogalmakkal, különösen $r = n$ esetben, ahol az ívek azonosíthatók a maximális minimális távolságú (MDS) kódokkal. A diplomamunka fő célja a (k, r) -ívek szerkezeti tulajdonságainak, teljességi feltételeinek és méretbeli korlátainak vizsgálata volt.

A dolgozat felépítése a következő:

Az *1. fejezetben* bevezetem a véges tereket, a kapcsolódó fogalmakat, valamint ezek legfontosabb tulajdonságait. Ezt követően ismertetem a síkbeli ívek fogalmát, majd bemutatok két lehetséges általánosítást, köztük a dolgozat fő témáját képező $PG(n, q)$ -beli (k, r) -íveket. A fejezet a blokkoló halmazok tárgyalásával zárul, külön figyelmet fordítva a síkbeli ívekkel való kapcsolatukra. A fejezetben, és így a dolgozat során is, elsősorban *Kiss és Szőnyi: Véges geometriák* [12] című könyvének terminológiájához igazodom.

A *2. fejezetben* bemutatom a síkbeli (k, r) -ívekre vonatkozó klasszikus eredményeket, majd Barlotti tételének általánosítása révén felső korlátot adok a $PG(n, q)$ -beli (k, r) -ívek méretére. Végül ismertetem a kódelméleti szempontból kiemelten fontos $PG(n, q)$ -beli (k, n) -ívekre vonatkozó eredményeket, külön figyelmet szentelve Segre nevezetes sejtésének, amely szerint $n < q - 2$ esetén $k \leq q + 1$.

Miután a $PG(n, q)$ -beli (k, n) -íveket, különösen $n = 3$ esetén már alaposan tanulmányozták, a diplomamunka során a $PG(3, q)$ -beli $(k, 4)$ -ívek vizsgálatára tértünk ki. A *3. fejezetben* az ezekre az ívekre vonatkozó megfigyeléseket mutatom be. A fejezet első részében a síkok és az ívek lehetséges metszeteit vizsgálom, és bemutatok egy később hasznosnak bizonyuló összefüggést: az ív mérete és a 4 pontban metsző síkok száma egyértelműen meghatározza az $i \in \{0, 1, 2, 3\}$ pontban metsző síkok számát. Törekedtünk arra, hogy minél többféle módszert, lehetséges kapcsolódó fogalmat és azokra vonatkozó ered-

ményt felhasználjunk, a fejezet következő részében az ezek segítségével kapott korlátokat tárgyalom.

A diplomamunka során cél volt, hogy az elméleti korlátok felállítása mellett, konkrét nagyméretű $(k, 4)$ -ívekből is következtetéseket vonjunk le. *Python* kód segítségével kis prímrendű terekben kerestünk ilyen íveket, a 3. fejezet második felében ezt mutatom be. Végül nem sikerült azon túlmutató hipotézist felállítani, hogy valószínűleg sokkal kisebb felső korlát is teljesül annál, ami a dolgozatban szerepel, azonban felfigyeltünk a $q = 5$ rendű $(12, 5)$ -ívek szabályosságára, ennek a struktúráját részben külön vizsgálom.

A dolgozat zárásaként, a 4. fejezetben bevezetem az algebrai kódelmélet legfontosabb fogalmait, valamint bemutatom a lineáris kódok szoros kapcsolatát az általánosított ívekkel. Végül Ball és Hirschfeld 2005-ös cikkének ([4]) mintájára néhány eredményt is mutatok a 3. fejezetben leírtak felhasználásaként.

Tartalomjegyzék

1. Szükséges előismeretek	1
1.1. Affin és projektív véges terek	1
1.2. Ívek véges síkon, magasabb dimenziós általánosítás	7
1.3. Blokkoló halmazok	10
2. Általánosított ívek mérete	15
2.1. Projektív síkon	15
2.2. Magasabb dimenzióban	16
2.3. A $PG(n, q)$ -beli (k, n) -ívek	20
3. Teljes $(k, 4)$-ívek $PG(3, q)$-ban	22
3.1. Szelősíkok száma	23
3.2. Ívek mérete	26
3.3. $(k, 4)$ -ívek keresése	31
3.4. Teljes $(12, 4)$ -ívek $PG(3, 5)$ -ben	33
4. Lineáris kódok és a véges projektív tér kapcsolata	37
4.1. Lineáris kódok	37
4.2. Lineáris kódok és az általánosított ívek kapcsolata	42
Irodalomjegyzék	47
A. $PG(3, q)$-ban talált $(k, 4)$-ívek	48

1. fejezet

Szükséges előismeretek

Elöljáróban tekintsük át röviden a szükséges alapfogalmakat és azok néhány egyszerű tulajdonságát. Ezek nagy része elhangzott az egyetemi tanulmányaim során BSc-s vagy MSc-s órákon is, és megtalálható Kiss György és Szőnyi Tamás Véges geometriák című könyvében ([12]).

1.1. Affin és projektív véges terek

1.1.1. Definíció. Legyenek $\mathcal{P}$ és $\mathcal{E}$ diszjunkt halmazok, és nevezzük az elemeiket rendre *pontoknak*, illetve *egyeneseknek*. Továbbá legyen az $I \subset \mathcal{P} \times \mathcal{E}$ *illeszkedésnek* nevezett reláció. Ekkor a $\Pi = (\mathcal{P}, \mathcal{E}, I)$ hármast *projektív síknak* nevezzük, ha teljesíti a következő axiómákat:

1. Bármely két különböző pont egyértelműen meghatároz egy egyenest, vagyis $\forall P_1, P_2 \in \mathcal{P}$ -hez $\exists! e \in \mathcal{E}$, hogy $P_1 \text{ I } e$ és $P_2 \text{ I } e$.
2. Bármely két különböző egyenes pontosan egy pontban metszi egymást, vagyis $\forall e_1 \neq e_2 \in \mathcal{E}$ -hez $\exists! P \in \mathcal{P}$, hogy $e_1 \text{ I } P$ és $e_2 \text{ I } P$.
3. Minden egyenesen legalább 3 pont van, vagyis $\mathcal{E}$ bármely eleme legalább két különböző $\mathcal{P}$ -beli elemmel áll relációban.
4. Minden ponton át legalább 3 egyenes halad át, vagyis $\mathcal{P}$ bármely eleme legalább három különböző $\mathcal{E}$ -beli elemmel áll relációban.

1.1.2. Tétel. *Ha a Π projektív síknak van olyan egyenese, amelyre pontosan $q + 1$ pont illeszkedik, akkor minden egyenesén $q + 1$ pont van, minden pontjára $q + 1$ egyenes illeszkedik, és a sík összesen $q^2 + q + 1$ pontot és ugyanennyi egyenest tartalmaz.*

Ha egy $(\mathcal{P}, \mathcal{E}, I)$ projektív sík egyik egyenesét és a rajta lévő összes pontot elhagyjuk, a következő fogalom axiómáit teljesítő struktúrához jutunk:

1.1.3. Definíció. Az $\mathcal{A} = (\mathcal{P}', \mathcal{E}', I')$ hármast, ahol $\mathcal{P}'$ (pontok) és $\mathcal{E}'$ (egyenesek) diszjunkt halmazok, az $I' \subset \mathcal{P}' \times \mathcal{E}'$ illeszkedési reláció, *affin síknak* nevezzük, ha teljesíti a következő axiómákat:

1. Bármely két különböző pont egyértelműen meghatároz egy egyenest, vagyis $\forall P_1, P_2 \in \mathcal{P}'$ -hez $\exists! e \in \mathcal{E}'$, hogy $P_1 I' e$ és $P_2 I' e$.
2. Bármely egyeneshez egy rajta nem lévő ponton át pontosan egy *párhuzamos* egyenes van, vagyis ha $P \in \mathcal{P}'$ és $e_1 \in \mathcal{E}'$ nem állnak relációban, akkor $\exists! e_2 \in \mathcal{E}'$, hogy $P I' e_2$, de $\nexists P' \in \mathcal{P}'$, hogy $e_2 I' P' I' e_1$.
3. Minden egyenesen legalább 2 pont van, vagyis $\mathcal{E}'$ bármely eleme legalább két különböző $\mathcal{P}'$ -beli elemmel áll relációban.
4. Minden ponton át legalább 3 egyenes halad át, vagyis $\mathcal{P}'$ bármely eleme legalább három különböző $\mathcal{E}'$ -beli elemmel áll relációban.

Az eljárás visszafelé is működik, affin síkból is tudunk projektív síkot konstruálni egy egyenes hozzáadásával, amelynek a pontjai a párhuzamossággal definiált osztályoknak felelek meg.

1.1.4. Tétel. Ha az $\mathcal{A}$ affin síknak van olyan egyenese, amelyre pontosan q pont illeszkedik, akkor minden egyenesén q pont van, minden pontjára $q + 1$ egyenes illeszkedik, és a sík összesen q^2 pontot és $q^2 + q$ egyenest tartalmaz.

A 1.1.2. illetve a 1.1.4. tételekben szereplő q értéket a Π projektív, illetve az $\mathcal{A}$ affin sík *rendjének* nevezzük.

1.1.5. Definíció. Az $\mathcal{S}$ véges halmaz néhány kitüntetett részhalmazához rendeljünk hozzá egy $-1 \leq d \leq n$ egész számot. Ekkor az $\mathcal{S}$ egy n -dimenziós projektív tér, a kitüntetett részhalmazai pedig a d -dimenziós *altér*ei, ha teljesítik a következő axiómákat:

1. $\forall -1 \leq d \leq n$ -re létezik legalább egy d -dimenziós altér, valamint
 - $\exists!$ (-1) -dimenziós altér, az $\emptyset$,
 - $\exists!$ n -dimenziós altér, az $\mathcal{S}$,
 - a 0 -dimenziós altérek pontosan az egyelemű részhalmazai $\mathcal{S}$ -nek;
2. ha $A \subset B$, ahol $\dim A = r$, $\dim B = s$, akkor $r \leq s$, valamint $r = s$ esetén $A = B$,

3. alterek metszete altér,

4. ha $A \cap B = C$, ahol $\dim A = r$, $\dim B = s$, $\dim C = m$, és az A -t és B -t is tartalmazó összes altér metszete t -dimenziós, akkor $r + s = m + t$,

5. az 1-dimenziós alterek mindegyike $q + 1 \geq 3$ elemből áll.

A 0-, 1-, 2- és az $(n - 1)$ -dimenziós altereket rendre *pontoknak*, *egyeneseknek*, *síkoknak* és *hipersíkoknak* nevezzük.

1.1.6. Definíció. Az $\mathcal{S}$ projektív tér *duális terének* nevezzük azt az $\mathcal{S}^*$ projektív teret, melynek k -dimenziós alterei megfelelnek az $\mathcal{S}$ $(n - k - 1)$ -dimenziós altereinek, valamint az illeszkedés a következő:

$$S_k^* \subset S_\ell^* \text{ az } \mathcal{S}^* \text{-ben} \iff S_k \supset S_\ell \text{ az } \mathcal{S} \text{-ben.}$$

1.1.7. Tétel (Dualitási elv). *Ha egy $\mathbf{T}$ tétel alterekről és illeszkedésről szól, akkor a duális tétel is teljesül.*

A projektív tér 4. axiómájából azonnal következik, hogy $\forall n$ -re bármely egyenes és azt nem tartalmazó hipersík metszete egy pont, bármely két különböző hipersík metszete egy $(n - 2)$ -dimenziós altér, valamint két különböző pont egyértelműen meghatároz egy egyenest.

Vegyük az $\mathbb{F}_q$, q elemű véges test feletti $(n + 1)$ -dimenziós V_{n+1} vektorteret. Legyen $\mathcal{S}$ a V_{n+1} 1-dimenziós altereinek halmaza, a kitüntetett részhalmazok pedig V_{n+1} alterei és az $\emptyset$. A V_{n+1} egy $(k + 1)$ -dimenziós alterének megfelelő $\mathcal{S}$ -beli részhalmazhoz rendeljük hozzá a k dimenzióértéket, az $\emptyset$ -hoz pedig a (-1) -et.

Meggondolható, hogy ez projektív teret definiál, ezt *n-dimenziós Galois-térnek*, a q -t a projektív tér *rendjének* nevezzük, és $PG(n, q)$ -val jelöljük. Belátható, hogy pontosan akkor létezik q elemű véges test, ha $q = p^r$ valamely p prím és r pozitív egész számra, valamint az is, hogy minden legalább 3-dimenziós véges projektív tér izomorf valamely $PG(n, q)$ térrel, tehát testtel koordinátázható. Ehhez definiáljuk a $\mathbb{F}_q^{n+1} \setminus \{\mathbf{0}\}$ elemein a következő $\sim$ ekvivalenciarelációt:

$$(v_0, v_1, \dots, v_n) \sim (w_0, w_1, \dots, w_n), \text{ ha } \exists \lambda \in \mathbb{F}_q \setminus \{0\}, \text{ hogy } w_i = \lambda v_i \ \forall i \in \{0, 1, \dots, n\}.$$

Ekkor az ekvivalenciaosztályok természetes módon megfeleltethetők a V_{n+1} 1-dimenziós altereinek. A dolgozat során a $PG(n, q)$ következő *homogén koordinátázását* fogom használni: a pontok az $\mathbb{F}_q^{n+1} \setminus \{\mathbf{0}\}$ ekvivalenciaosztályainak azon $[v] = (v_0, v_1, \dots, v_n)$ reprezentánsai lesznek, melyekre $v_0 \in \{0, 1\}$. A továbbiakban a $(v_0 : v_1 : \dots : v_n)$ jelölést használjuk, és a $v_0 = 0$ esetben ideális pontokról beszélünk.

1.1.8. *Megjegyzés.* Ugyanúgy, ahogy síkban, a $PG(n, q)$ projektív térből valamely hipersík és a rajta lévő pontok illetve alterek elhagyásával előállíthatjuk az $AG(n, q)$ *affin teret*. A koordinátázás könnyen kezelhetőségének érdekében az ideális hipersíkot és annak pontjait, tehát a $[v] = (0 : v_1 : \dots : v_n)$ koordinátájú pontokat és az $[1 : 0 : \dots : 0]$ síkot hagyjuk el.

Természetesen az affin tereket is lehet axiomatikusan definiálni, de itt most az egyszerűség kedvéért ezzel a származtatással definiáljuk.

Egy *ponthalmaz által generált altérben* azok a pontok helyezkednek el, melyek reprezentáló vektorai előállíthatók a generáló ponthalmaz vektorainak lineáris kombinációjaként. Vagyis a $PG(n, q)$ térben bármely $2 \leq k \leq n$ db ponthoz létezik legalább egy olyan $(k-1)$ -dimenziós altér, amely mind a k pontot tartalmazza. Amennyiben pontosan egy ilyen altér van, nem létezik mindegyiket tartalmazó $(k-2)$ -dimenziós altér, és a pontokat *általános helyzetűeknek* hívjuk. Továbbá tehát a $\mathbf{p}_1, \mathbf{p}_2, \dots, \mathbf{p}_k$ reprezentálóvektorú pontok pontosan akkor helyezkednek el egy $(k-2) \geq l$ -dimenziós altérben, ha bármely $(l+2)$ elemű $\mathbf{p}_{i_1}, \mathbf{p}_{i_2}, \dots, \mathbf{p}_{i_{l+2}}$ részhalmaza lineárisan összefüggő, vagyis $\exists(\lambda_1, \lambda_2, \dots, \lambda_{l+2}) \in \mathbb{F}_q^{l+1} \setminus \{\mathbf{0}\}$, hogy $\sum_{j=1}^{l+2} \lambda_j \mathbf{p}_{i_j} = \mathbf{0}$. Ebből következik, hogy bármely l -dimenziós alteret meghatározza $l+1$ általános helyzetű pontja.

1.1.9. Állítás. A $PG(n, q)$ -beli páronként különböző $P_1 = (p_{10} : p_{11} : \dots : p_{1n}), P_2 = (p_{20} : p_{21} : \dots : p_{2n}), \dots, P_n = (p_{n0} : p_{n1} : \dots : p_{nn})$ pontok pontosan akkor helyezkednek el egy hipersíkon, ha lineárisan függetlenek, azaz

$$\begin{vmatrix} p_{10} & p_{11} & \cdots & p_{1n} \\ p_{20} & p_{21} & \cdots & p_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n0} & p_{n1} & \cdots & p_{nn} \end{vmatrix} = 0.$$

Tehát homogén koordinátákat rendelhetünk a hipersíkokhoz is. A $\mathbf{p}_1, \mathbf{p}_2, \dots, \mathbf{p}_n$ vektorú általános helyzetű pontokhoz rendeljük hozzá azt a $\mathbf{h} \in \mathbb{F}_q^{n+1}$ normált vektort, amelyre $\sum_{i=1}^n h_i(\mathbf{p}_j)_i = 0$. Ennek az egyenletrendszernek skalárszoros erejéig pontosan egy megoldása lesz, hiszen n független egyenlet és $n+1$ ismeretlen van. Könnyen ellenőrizhető, hogy pontosan azon $\mathbf{v}$ koordinátavektorú pontokat tartalmazza a generált hipersík, amelyek szintén teljesítik a $\sum_{i=1}^n h_i v_i = 0$ egyenlőséget. A hipersíkokra a $[h_0 : h_1 : \dots : h_n]$ jelölést használjuk, és a $[1 : 0 : \dots : 0]$ -hoz tartozót *ideális hipersíknak* nevezzük.

Az egyenesekhez is hozzárendelhetők úgynevezett *Plücker-koordináták*, mégpedig a $P = (p_0 : p_1 : \dots : p_n) \neq Q = (q_0 : q_1 : \dots : q_n)$ pontokat összekötő egyeneshez a $l_{ij} = p_i q_j - p_j q_i$ ($i < j$), $\binom{n+1}{2}$ hosszúságú vektor. Meggondolható, hogy nem számít, hogyan választjuk ki a két pontot, valamint ezek homogén koordináták is, tehát egy Plücker-koordinátavektor és annak nem nulla skaláris többszöröse ugyanazt az egyenest határozza

meg. Azonban nem minden $\binom{n+1}{2}$ hosszúságú vektor rendelhető egyeneshez $PG(n, q)$ -ban, $n = 3$ -dimenzióban például a következőket mondhatjuk.

1.1.10. Állítás. A $\mathbf{0} \neq (\ell_{ij})_{0 \leq i < j \leq 3}$ vektor a $PG(3, q)$ egy egyenesének Plücker-koordináta vektora pontosan akkor, ha

$$\ell_{01}\ell_{23} + \ell_{02}\ell_{31} + \ell_{03}\ell_{12} = 0.$$

1.1.11. Lemma. A $PG(3, q)$ tér $\mathbf{0} \neq \ell = (\ell_{ij})_{0 \leq i < j \leq 3}$ és $\mathbf{0} \neq \ell' = (\ell'_{ij})_{0 \leq i < j \leq 3}$ egyenesei-nek pontosan akkor van közös pontja, ha

$$\ell_{01}\ell'_{23} + \ell_{02}\ell'_{31} + \ell_{03}\ell'_{12} + \ell'_{01}\ell_{23} + \ell'_{02}\ell_{31} + \ell'_{03}\ell_{12} = 0.$$

1.1.12. Állítás. A $PG(n, q)$ projektív térben

1. a k -dimenziós alterek száma $\begin{bmatrix} n+1 \\ k+1 \end{bmatrix}_q$,

2. adott d -dimenziós altéren keresztüli k -dimenziós alterek száma $\begin{bmatrix} n-d \\ k-d \end{bmatrix}_q$,

ahol

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{\prod_{i=0}^{k-1} (q^n - q^i)}{\prod_{j=0}^{k-1} (q^k - q^j)}.$$

1.1.13. Definíció. Két ponthalmaz a $PG(n, q)$ -ban projektíven ekvivalens, ha V_{n+1} -ben lineáris transzformációval egymásba vihetők.

1.1.14. Definíció. Legyen

$$Q(\mathbf{x}) = \sum_{i,j=0}^n a_{ij}x_i x_j$$

kvadratikus alak. A $PG(n, q)$ térben azon pontok halmazát, melyek koordinátái kielégítik a $Q(\mathbf{x}) = 0$ egyenletet, a Q -hoz tartozó másodrendű varietásnak nevezzük. Síkban a *másodrendű görbe*, térben a *másodrendű felület*, magasabb dimenzióban a *másodrendű hiperfelület* kifejezéseket használjuk.

Egy varietás *szinguláris*, ha a koordináta-rendszer változtatásával elérhető, hogy a hozzá tartozó alak eggyel kevesebb változót tartalmazzon. Ha ez nem tehető meg, akkor a varietás *nemszinguláris*.

Belátható, hogy ha q páratlan, egy másodrendű varietás pontosan akkor szinguláris, ha a varietáshoz tartozó alak mátrixa szinguláris.

1.1.15. Tétel. Nemszinguláris másodrendű varietáshoz tartozó kvadratikus alak a $PG(n, q)$ térben páratlan q esetén az alábbi kanonikus alak egyikére hozható:

1. Ha n páros, akkor $Q_n(\mathbf{x}) = \sum_{i=0}^n x_i^2$ (parabolikus kvádrika, ha $n > 2$, és kúpszelet $n = 2$ -re).
2. Ha n páratlan, akkor $Q_n(\mathbf{x}) = \sum_{i=0}^n x_i^2$ (hiperbolikus kvádrika), vagy $Q_n(\mathbf{x}) = \sum_{i=0}^{n-1} x_i^2 + \alpha x_n^2$ (elliptikus kvádrika), ahol α rögzített nemnégyzet elem.

A következő tétel páros q esetén is igaz:

1.1.16. Tétel. Nemszinguláris másodrendű varietáshoz tartozó kvadratikus alak a $PG(n, q)$ térben az alábbi kanonikus alak egyikére hozható:

1. Ha n páros, akkor $Q_n(\mathbf{x}) = x_0^2 + x_1x_2 + \cdots + x_{n-1}x_n$ (parabolikus kvádrika, ha $n > 2$, és kúpszelet $n = 2$ -re).
2. Ha n páratlan, akkor $Q_n(\mathbf{x}) = x_0x_1 + x_2x_3 + \cdots + x_{n-1}x_n$ (hiperbolikus kvádrika), vagy $Q_n(\mathbf{x}) = f(x_0, x_1) + x_2x_3 + \cdots + x_{n-1}x_n$ (elliptikus kvádrika), ahol f irreducibilis homogén másodfokú polinom.

1.1.17. Tétel. A $PG(n, q)$ térben

1. parabolikus kvádrikán $\frac{q^n-1}{q-1}$,
2. elliptikus kvádrikán $\frac{(q^{\frac{n+1}{2}}+1)(q^{\frac{n-1}{2}}-1)}{q-1}$,
3. hiperbolikus kvádrikán $\frac{(q^{\frac{n+1}{2}}-1)(q^{\frac{n-1}{2}}+1)}{q-1}$ pont van.

Végezetül vezessünk be egy az affin síkkal szoros kapcsolatban álló struktúrát.

1.1.18. Definíció. Legyenek $\mathcal{P}$ és $\mathcal{K}$ diszjunkt halmazok, melyek elemeit rendre *pontoknak*, illetve *köröknek* nevezzük. Legyen továbbá az $I \subset \mathcal{P} \times \mathcal{K}$ illeszkedésnek nevezett reláció.

Az $\mathcal{M} = (\mathcal{P}, \mathcal{K}, I)$ hármast *Möbius-síknak* nevezzük, ha kielégíti a következő axiómákat:

1. $\mathcal{P}$ bármely három különböző eleméhez pontosan egy olyan eleme van $\mathcal{K}$ -nak, amely mindhárommal relációban áll.
2. Minden $(P_1, P_2, k) \in (\mathcal{P} \times \mathcal{P} \times \mathcal{K})$ olyan hármashoz, melyre $P_1 \not I k \not I P_2$, $\exists! k' \in \mathcal{K}$, melyre $P_1 \not I k' \not I P_2$ és $|k' \cap k| = 1$.

3. $\mathcal{P}$ -nek létezik négy különböző eleme, melyekhez nincs olyan $\mathcal{K}$ -beli elem, amely mindegyikkel relációban áll.

1.1.19. Tétel. *Ha egy véges Möbius-síknak van olyan köre, melyre $q + 1$ pont illeszkedik, akkor a síkon összesen $q^2 + 1$ pont és $q(q^2 + 1)$ kör van, valamint minden körön $q + 1$ pont helyezkedik el és minden pontjára $q(q + 1)$ kör illeszkedik.*

Ezt a q értéket a Möbius-sík *rendjének* nevezzük.

1.1.20. Definíció. Legyen P az $\mathcal{M} = (\mathcal{P}, \mathcal{K}, I)$ Möbius-sík egy rögzített pontja, $\mathcal{K}_P \subset \mathcal{K}$ pedig a sík P -n átmenő köreinek halmaza. Ekkor az $\mathcal{M}_P = (\mathcal{P} \setminus \{P\}, \mathcal{K}_P, I)$ hármast a Möbius-sík P -szerinti *derivált síkjának* nevezzük.

Az axiómák ellenőrzésével könnyen adódik, hogy:

1.1.21. Lemma. *A fent definiált $\mathcal{M}_P = (\mathcal{P} \setminus \{P\}, \mathcal{K}_P, I)$ affin sík, amelynek rendje megegyezik a Möbius-sík rendjével.*

1.2. Ívek véges síkon, magasabb dimenziós általánosítás

1.2.1. Definíció. Az affin vagy projektív sík azon k méretű ponthalmazait, melyeknek nincs 3 kollineáris pontja, *k-íveknek* nevezzük. Amennyiben tartalmazásra nézve maximális, az ív *teljes*.

1.2.2. Tétel (Bose). *q -adrendű projektív sík bármely k -ívére*

$$k \leq \begin{cases} q + 1, & \text{ha } q \text{ páratlan,} \\ q + 2, & \text{ha } q \text{ páros} \end{cases}$$

1.2.3. Állítás. *A $PG(2, q)$ -beli*

$$\mathcal{K} = \{(1 : t : t^2) : t \in \mathbb{F}_q\} \cup \{(0 : 0 : 1)\}$$

ponthalmaz $(q + 1)$ -ívet alkot.

Ha q páros, a $\mathcal{K} \cup \{(0 : 1 : 0)\}$ ponthalmaz egy $(q + 2)$ -ív.

Bizonyítás. Világos, hogy $|\mathcal{K}| = |\mathbb{F}_q| + 1$. Még azt kell belátni, hogy $\mathcal{K}$ semelyik három pontja nem kollineáris. Ehhez használjuk az 1.1.9. állítást.

1. A három pont egyike az ideális $\{(0 : 0 : 1)\}$ pont. Ekkor

$$\begin{vmatrix} 1 & t_1 & t_1^2 \\ 1 & t_2 & t_2^2 \\ 0 & 0 & 1 \end{vmatrix} = t_2 - t_1 \neq 0, \text{ hiszen } t_1, t_2 \in \mathbb{F}_q \text{ különbözők.}$$

2. A három pont egyike sem az ideális pont. Ekkor meggondolható, hogy

$$\begin{vmatrix} 1 & t_1 & t_1^2 \\ 1 & t_2 & t_2^2 \\ 1 & t_3 & t_3^2 \end{vmatrix} = (t_1 - t_2)(t_2 - t_3)(t_3 - t_1) \neq 0, \text{ hiszen } t_1, t_2, t_3 \in \mathbb{F}_q \text{ különbözők.}$$

Páros q esetén ezen felül még a $(0 : 1 : 0)$ -t tartamazó ponthármasok kollinearitását kell ellenőriznünk.

1. A másik két pont egyike az ideális $\{(0 : 0 : 1)\}$ pont. Ekkor

$$\begin{vmatrix} 1 & t_1 & t_1^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} = 1 \neq 0.$$

2. A másik két pont egyike sem az ideális pont. Ekkor

$$\begin{vmatrix} 1 & t_1 & t_1^2 \\ 1 & t_2 & t_2^2 \\ 0 & 1 & 0 \end{vmatrix} = t_1^2 - t_2^2 = (t_1 - t_2)^2 \neq 0, \text{ hiszen } q = 2^h \text{ és } t_1, t_2 \in \mathbb{F}_q \text{ különbözők.}$$

□

Tehát Bose tétele testtel koordinátázható síkon éles. Belátható, hogy páros q esetén nem csak az állításban szereplő $\mathcal{K}$, de bármely $(q+1)$ -ív kiegészíthető $(q+2)$ -ívvé, vagyis a $(q+1)$ -ívek nem lehetnek teljesek.

1.2.4. Tétel (Segre). *Páratlan rendű $PG(2, q)$ sík esetén minden $(q+1)$ -ív másodrendű görbe.*

Az ív fogalma többféleképpen kiterjeszthető, lássunk rá két példát:

1.2.5. Definíció. A $PG(n, q)$ és $AG(n, q)$ véges terekben azon ponthalmazokat, melyeknek nincs három kollineáris pontja, *süvegnek* nevezzük. Egy süveg *teljes*, ha nem része nagyobb süvegnek.

1.2.6. Állítás. *$PG(3, 2)$ -ben a maximális méretű teljes süvegek pontosan a 8 pontú beágyazott $AG(3, 2)$ affin terek (a projektív térbeli síkok komplementerei).*

1.2.7. Állítás. *A $PG(3, q)$ térben $q > 2$ esetén a legnagyobb teljes süveg mérete $q^2 + 1$. Továbbá ezeket a tér minden síkja metszi és a süveg bármely pontján pontosan egy érintősík halad át.*

A tér elliptikus másodrendű felületei $q^2 + 1$ pontú süvegek.

1.2.8. *Megjegyzés.* Vegyük a süveg egy P pontján keresztüli érintősíkját és rajta egy egyenest. Ekkor ezen az egy pontban metsző egyenesen átmenő további q sík mindegyikén a süvegnek legfeljebb q pontja lehet P -n kívül, hiszen bármely síknak P -n keresztül további q egyenese van, amelyeken legfeljebb egy-egy további pontja lehet a süvegnek. Tehát $q^2 + 1$ pontú süveg esetén a pontjain keresztül a nem érintősíkok $q + 1$ pontban metszenek.

1.2.9. Tétel (Barlotti, Panella). *A $PG(3, q)$ páratlan rendű térben pontosan a tér elliptikus másodrendű felületei a $q^2 + 1$ pontú süvegek.*

1.2.10. Állítás. *$PG(3, q)$ tér $q^2 + 1$ méretű süvegei Möbius-síkot definiálnak, ahol a sík pontjai a süveg pontjainak, körei a süveg nem egypontú síkmetszeteinek felelnek meg.*

Bizonyítás. A Möbius-sík definíciójában szereplő axiómákat ellenőrizzük.

Definícióból adódóan a süveg bármely három pontja általános helyzetű, egyértelműen meghatároz egy (nem egypontban metsző) síkot, így az 1. axióma teljesül.

Az 1.2.8. alapján a süveg P_1, P_2 pontjaihoz és a Π ($q + 1$) pontban metsző síkhoz, melyre $P_1 \in \Pi$, $P_2 \notin \Pi$, egyértelműen létezik $P_1, P_2 \in \Pi'$ sík, melyre $\Pi \cap \Pi'$ -n nincs további pontja a süvegnek. Hiszen bármely két sík metszete egyenes, a P_1 -en keresztül pontosan egy olyan egyenes van, amelyen a süvegnek nincs további pontja, és bármely pont és rajta nem áthaladó egyenes egyértelműen meghatároz egy síkot. Így teljesül a 2. axióma is.

A 3. axióma teljesülése $q > 2$ esetén nyilvánvaló. □

Ebből és az 1.2.7.-ből persze adódik a következő állítás.

1.2.11. Állítás. *$PG(3, q)$ tér bármely elliptikus kvádrikája Möbius-síkot definiál, ahol a sík pontjai a kvádrika pontjainak, a sík körei pedig a kvádrika nem egypontú síkmetszeteinek felelnek meg.*

Bár ez a fogalom is hasznos lesz számunkra, a dolgozatban elsősorban az ív következő általánosításával fogunk foglalkozni:

1.2.12. Definíció. A $PG(n, q)$ és $AG(n, q)$ véges terekben $r \geq n$ esetén (k, r) -íveknek nevezzük azokat az Ω ponthalmazokat, melyekre teljesül, hogy $|\Omega| = k$ és semelyik $r + 1$ pontja nem esik egy hipersíkra.

A szakirodalomban több helyen a (k, r) -ívek definíciója azt is megköveteli, hogy létezen olyan Π hipersík, melyre $|\Omega \cap \Pi| = r$. Ez nyilván csak annyit változtat a fogalmon, hogy emiatt a $(k, r - 1)$ -ívek halmazát nem tekintjük részhalmazának a (k, r) -ívekének. Itt ezt most nem tesszük fel, viszont vegyük észre, hogy a következő fogalomból következik ez a tulajdonság is (fordítva viszont nem).

1.2.13. Definíció. Egy (k, r) -ív *teljes*, ha nincs olyan $(k + 1, r)$ -ív, amely tartalmazza.

Jelölje $m_r(n, q)$ azt a legnagyobb k értéket, amelyre létezik (k, r) -ív $PG(n, q)$ -ban.

Ez az érték nyilvánvalóan létezik és véges, hiszen $PG(n, q)$ -nak véges sok pontja van, illetve ekkor az ívről azt is tudjuk, hogy teljes.

1.2.14. Definíció. Nevezzük az Ω ív *s-szelőinek* a $PG(n, q)$ azon Π altereit, melyekre $|\Omega \cap \Pi| = s$. Az $s = 0$ esetben használjuk az *elkerülő* altér kifejezést.

Természetesen (k, r) -ívben a hipersíkok, így minden altér is legfeljebb r -szelő. A továbbiakban, amennyiben nem jelöljük külön az altér dimenzióját, s -szelő alatt hipersíkot értünk.

Most lássunk egy nevezetes példát $PG(n, q)$ -beli (k, r) -ívekre.

1.2.15. Definíció. $PG(n, q)$ -ban a következő ponthalmazt *momentumgörbének* nevezzük:

$$\mathcal{C}_n = \{(1 : t : t^2 : \dots : t^n) : t \in \mathbb{F}_q\} \cup \{(0 : 0 : \dots : 1)\}.$$

Ez pont a 1.2.3. állításban bemutatott $(q + 1)$ -ív magasabb dimenziós általánosítása. A síkbeli változathoz hasonlóan belátható, hogy amennyiben $q \geq n$, a $PG(n, q)$ bármely hipersíkja legfeljebb n pontját tartalmazza a $\mathcal{C}_n$ momentumgörbének.

1.2.16. Állítás. $PG(n, q)$ -ban a $\mathcal{C}_n$ momentumgörbe pontjai $(q + 1, n)$ -ívet alkotnak.

1.3. Blokkoló halmazok

Vegyük észre, hogy egy $PG(n, q)$ -beli teljes (k, r) -ív r -szelő hipersíkjai lefedik a tér összes pontját. Hiszen ha lenne olyan pont, amin keresztül nincs r -szelő, azt hozzávéve továbbra sem sérülne az a feltétel, hogy bármely hipersíkon legfeljebb r pontja van az ívnek, ez viszont ellentmondana a teljességnek.

Tekintsük az ívet a duális téren. Ekkor olyan hipersíkhalmazt kapunk, amelyre teljesül, hogy a duális tér bármely pontján legfeljebb r halad át közülük. Továbbá az előző megfigyelés alapján, az ív r -szelői a duális térben olyan ponthalmazt alkotnak, amely minden hipersíkot metsz. Természetes tehát, hogy az általános ívek vizsgálatakor körüljárjuk az alábbi fogalmat is.

1.3.1. Definíció. Az n -dimenziós projektív vagy affin tér valamely $\mathcal{B}$ ponthalmazát *b-blokkoló halmaznak* nevezzük, ha $\mathcal{B}$ -nek minden $(n - b)$ -dimenziós altere legalább egy pontját tartalmazza. Az 1-blokkoló halmazt szokás simán *blokkoló halmaznak* nevezni.

A $\mathcal{B}$ *minimális b-blokkoló halmaz*, ha tartalmazásra nézve az.

Például, ha a $PG(2, q)$ síkon vesszük egy egyenesnek a $q+1$ pontját, az egy $\mathcal{B}$ minimális 1-blokkoló halmazt alkot. Valóban, mivel bármely két különböző egyenesnek pontosan egy metszéspontja van, így minden egyenesen lesz $\mathcal{B}$ -beli pont, és ha $\mathcal{B}$ -nek elhagynánk egy pontját, az azon átmenő, $\mathcal{B}$ -től különböző egyenesek nem metszenék az új halmazt.

Belátható, hogy $PG(2, q)$ -ben nincs ennél kisebb $\mathcal{B}$ blokkoló halmaz. Ehhez azt kell észrevenni, hogy egy nem $\mathcal{B}$ -beli ponton átmenő minden egyenest legalább egy pontban kell metszenie $\mathcal{B}$ -nek. Az is meggondolható, hogy $PG(2, q)$ bármely $q+1$ pontú blokkoló halmaza egyenes.

A síkbeli eredmény magasabb dimenziós általánosítása is teljesül.

1.3.2. Állítás. $PG(n, q)$ egy b -dimenziós altere a legkisebb méretű minimális b -blokkoló halmaz.

1.3.3. Definíció. A $\mathcal{B}$ b -blokkoló halmaz *triviális*, ha tartalmazza egy b -dimenziós alter minden pontját.

A projektív tér definíciójából adódóan, a $PG(n, q)$ hipersíkjai adott $PG(n-1, q)$ -val izomorf hipersíkot $(n-2)$ -dimenziós altérben, vagyis $PG(n-1, q)$ -beli hipersíkban metsz. Tehát ha egy hipersíkon vesszük annak egy 1-blokkoló halmazát, az a teljes térben is 1-blokkoló halmaz lesz. Ennél még többet is tudunk mondani.

1.3.4. Állítás. A $PG(n, q)$ egy alterének b -blokkoló halmaza szintén b -blokkoló halmaz a teljes n -dimenziós térben.

Az állítás megfordítása nem igaz minden esetben, azonban ha veszünk egy b -blokkoló halmazt, annak egy hipersíkkal vett metszete $(b-1)$ -blokkoló halmazt alkot a hipersíkon.

1.3.5. Definíció. A $\mathcal{B}$ blokkoló halmaz d -dimenziós, ha $\mathcal{B}$ pontjai d -dimenziós alteret generálnak. A $d=2$ esetben a *síkbeli* blokkoló halmaz elnevezést használjuk.

1.3.6. Definíció. A $\mathcal{B}$ d -dimenziós *valódi* blokkoló halmaz, ha d -dimenziós és nem tartalmaz $(d-1)$ -dimenziós blokkoló halmazt.

A d -dimenziós valódi blokkoló halmazok méretének minimumát $f_d(q)$ -val jelöljük. Használjuk továbbá az $r_d(q) = f_d(q) - (q+1)$ jelölést.

$PG(2, q)$ -ban már láttunk egy $q+1$ méretű triviális blokkoló halmazt. Kézenfekvő kérdés, hogy a nemtriviális blokkoló halmazok mérete mennyivel tér el ettől.

1.3.7. Tétel (Bruen, Pelikán). $PG(2, q)$ -beli nemtriviális blokkoló halmaz mérete

$$f_2(q) \geq q + \sqrt{q} + 1, \text{ vagy másképp, } r_2(q) \geq \sqrt{q},$$

egyenlőség esetén a blokkoló halmaz egy $\sqrt{q}$ -rendű, úgynevezett Baer-részsík.

Prímrendű sík esetén ennél még többet is tudunk mondani.

1.3.8. Tétel (Blokhuis). *A prímrendű $PG(2, q)$ sík nemtriviális blokkoló halmazainak méretére $f_2(q) \geq \frac{3(q+1)}{2}$ teljesül (tehát $r_2(q) \geq \frac{(q+1)}{2}$).*

Bruen és Pelikán tétele általános esetben is javítható.

1.3.9. Tétel (Blokhuis). *Legyen p prím, $q = p^{2h+1}$, $h \geq 1$. Ekkor a $PG(2, q)$ síkon*

$$f_2(q) \geq q + \sqrt{pq} + 1, \text{ vagy másképp, } r_2(q) \geq \sqrt{pq}.$$

Tekintsük át, mit mondhatunk magasabb dimenzióban. Ezek nagyrészt a síkbeli állítások általánosításaként jelennek meg, emiatt a síkbeli blokkoló halmazok mérete szoros kapcsolatban áll velük.

1.3.10. Tétel (Heim). *Nem-triviális $PG(n, q)$ -beli blokkoló halmaz mérete legalább $f_2(q)$, egyenlőség esetén a blokkoló halmaz síkbeli.*

1.3.11. Tétel (Heim). *$q > 3$ esetén $f_{e+1}(q) > f_e(q)$, ha $f_e(q) \leq 2q$, és $f_3(q) \geq f_2(q) + 2$.*

1.3.12. Tétel (Heim). *Legyen $\mathcal{B}$ nem-triviális b -blokkoló halmaz $PG(n, q)$ -ban, $n > b$ és $q > 2$. Ekkor $|\mathcal{B}| \geq \begin{bmatrix} b+1 \\ 1 \end{bmatrix}_q + q^{b-1}r_2(q)$. Egyenlőség esetén $\mathcal{B}$ egy $\mathcal{V}\mathcal{B}^*$ kúp, ahol $\mathcal{V}$ egy $(b-2)$ -dimenziós altér, $\mathcal{B}^*$ pedig egy $q+1+r_2(q)$ pontú síkbeli blokkoló halmaz.*

1.3.13. Tétel (Huber). *Ha $\mathcal{B}$ nem-triviális b -blokkoló halmaz $PG(n, q)$ -ban $q > 5$, $b \geq s-1$ és nem tartalmaz s -dimenziós alteret, akkor $|\mathcal{B}| \geq \begin{bmatrix} b+1 \\ 1 \end{bmatrix}_q + \sqrt{q}(q^{b-1} + \dots + q^{s-1})$. Egyenlőség pontosan akkor van, ha $\mathcal{B}$ úgynevezett Baer-kúp, amelynek csúcsa egy $(s-2)$ -dimenziós altér, alapja pedig egy $2(b-s+1)$ -dimenziós altér Baer-résztere.*

Térjünk vissza a (k, r) -ívekre, pontosabban azok duálisára. Az ív r -szelőinek duális megfigyeléseink szerint blokkoló halmazt alkotnak, így az r -szelők számára alsó korlátot tudunk adni. És mivel az r -szelők száma és a (k, r) -ív mérete összefügg, ezzel az ív méretére vonatkozó következtetést is tudunk levonni. Lássunk erre egy síkbeli példát.

1.3.14. Állítás. *A páratlan prímrendű $PG(2, q)$ sík legkisebb teljes $(k, 2)$ -ívének mérete*

$$k > \sqrt{3q}.$$

Bizonyítás. A teljes ív 2-szelő egyenesei $\binom{k}{2}$ pontú blokkoló halmazt alkotnak a duális síkon. Ez ráadásul nemtriviális, hiszen ha az lenne, akkor az eredeti síkon lenne olyan pont, amin átmenő minden egyenes 2-szelő, így legalább $1 + (q+1)$ pontja lenne, ami Bose (1.2.2.) tétele alapján nem lehetséges. Ekkor használhatjuk a 1.3.8. tételt, amivel

$$\binom{k}{2} \geq \frac{3(q+1)}{2}.$$

□

1.3.15. Állítás. A $PG(2, q)$ sík legkisebb teljes $(k, 2)$ -ívének mérete $q = p^{2h+1}$, $h \geq 1$ esetén

$$k > \sqrt{2p^{h+1}(p^h + 1)},$$

$q = p^{2h}$, $h \geq 1$ esetén pedig

$$k > \sqrt{2p^h(p^h + 1)}.$$

Ezek az előzőhöz hasonlóan, a 1.3.9. és 1.3.7. eredményeket felhasználva láthatók be. Magasabb dimenzióban később fogunk látni hasonló korlátot.

1.3.16. Definíció. A projektív vagy affin n -dimenziós tér valamely $\mathcal{B}$ ponthalmazát t -szeresen b -blokkoló halmaznak nevezzük, ha $\mathcal{B}$ -nek minden $(n - b)$ -dimenziós altere legalább t pontját tartalmazza.

A $\mathcal{B}$ minimális t -szeresen b -blokkoló halmaz, ha tartalmazásra nézve az.

A definíciókból azonnal látható, hogy $r + t = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q$ esetben a (k, r) -ív és a t -szeresen blokkoló halmaz fogalmak egymás komplementerei, sőt minimális t -szeresen blokkoló halmaz komplementere teljes (k, r) -ív.

1.3.17. Megjegyzés. Az $n = 2$ esetben a t -szeresen blokkoló halmazokat t -szeresen lefogó halmazoknak is nevezzük.

A t -szeresen blokkoló ponthalmazok mérete lényegesen eltérhet azonos dimenziójú affin és projektív terekben. Ezt most csak síkbeli példákon érzékeltetjük, mivel a későbbiekben csak ezeket fogjuk használni.

A projektív síkon már körüljártuk az 1-szeresen lefogó halmazok méretét, lássuk ennek affin verzióját. Az első észrevétel, hogy a projektív síkkal ellentétben $AG(2, q)$ -ben egy egyenes pontjai nem alkotnak lefogó ponthalmazt, hiszen a vele párhuzamos egyenesek egyikével nincs közös pontja. A megfigyelésből adódik az ötlet, hogy ennek "kijavítására" az egyenes pontjai mellé, válasszunk minden vele párhuzamos egyenesen egy-egy pontot. Világos, hogy ennek a ponthalmaznak már minden affin síkbeli egyenessel lesz közös pontja. Sőt, meglepő módon az így kapott $2q - 1$ pontú lefogó ponthalmaznál nem is tudunk kisebbet megadni.

1.3.18. Tétel (Jamison, Brouwer, Schrijver). A $\mathcal{B}$ 1-szeresen lefogó ponthalmaz méretére $AG(2, q)$ -ban $|\mathcal{B}| \geq 2q - 1$ teljesül.

Térjünk át a $t > 1$, t -szeresen lefogó ponthalmazok méretére. Ha a síkon választunk egy pontot, amelyet nem tartalmaz a $\mathcal{B}$ lefogó ponthalmazunk, akkor a rajta átmenő egyenesek mindegyikének $\mathcal{B}$ -t legalább t pontban kell metszenie. Ebből megkaptuk a következő eredményt.

1.3.19. Állítás. Minden t -szeresen lefogó ponthalmaznak $PG(2, q)$ -ban legalább $t(q + 1)$ pontja, míg $AG(2, q)$ -ban legalább tq pontja van.

A t -szeresen lefogó ponthalmazok minimális mérete ennél valamivel nagyobb, nézzünk erre néhány eredményt.

1.3.20. Tétel (Blokhuis, Ball). A $\mathcal{B}$ t -szeresen lefogó ponthalmaz mérete $AG(2, q)$ -ban, ahol $q = p^h$ valamely p prímre, és $(t, q) = p^{e(t)}$, $|\mathcal{B}| \geq (t + 1)q - p^{e(t)}$.

Felhasználva, hogy az affin és projektív síkot egy egyenes hozzá- vagy elvételével alakíthatunk egymásból:

1.3.21. Következmény. Legyen $q = p^h$ valamely p prímre, és $(t - 1, q) = p^{e(t-1)}$. Ha a $PG(2, q)$ projektív sík valamely $\mathcal{B}$ t -szeresen lefogó ponthalmaza tartalmaz teljes egyenest, akkor $|\mathcal{B}| \geq tq - p^{e(t-1)} + q + 1 \geq (t + 1)q - t + 2$.

1.3.22. Tétel (Ball). Ha q páratlan prím, $\mathcal{B}$ t -szeresen lefogó ponthalmaz $PG(2, q)$ -ban, akkor $|\mathcal{B}| \geq \max\{tq + \frac{q+3}{2}, tq + t\}$.

Ha továbbá $t \leq \frac{q+1}{2}$, akkor $|\mathcal{B}| \geq tq + t + \frac{q+1}{2} \geq tq + 2t$.

1.3.23. Megjegyzés. Ball tétele $t = \frac{q+1}{2}$ esetben éles. Ekkor ugyanis egy kúpszelet valamint az ún. külső pontjai együttesen t -szeresen lefogó ponthalmazt alkotnak.

2. fejezet

Általánosított ívek mérete

2.1. Projektív síkon

Tekintsük át, mit tudunk a $PG(2, q)$ -beli (k, r) -ívek méretére vonatkozóan. Ekkor, mivel minden egyenesen (hipersíkon) pontosan $q+1$ pont helyezkedik el, valamint bármely két különböző pontnak van közös egyenese, $r \geq q+1$ esetben a teljes projektív sík, míg $r = 1$ esetben egyetlen pont lenne a legnagyobb méretű (k, r) -ív. Ezen triviális esetek kizárása érdekében a továbbiakban feltesszük, hogy $1 < r < q+1$.

Az ív egy pontján átmenő egyeneseken elhelyezkedő pontok számának vizsgálatával egyszerűen megkapható a következő korlát:

2.1.1. Tétel (Barlotti). $m_r(2, q) \leq 1 + (q+1)(r-1) = (r-1)q + r$, és egyenlőség esetén r osztója q -nak.

Az állítás második feléhez azt kell észrevenni, hogy egyenlőség esetén minden egyenes pontosan r vagy 0 pontban metszi az ívet. Ezután már csak egy nem ívbeli ponton átmenő egyeneseken lévő pontokat kell összeszámolni (amik persze lefedik a teljes síkot). Erre a 2.2. részben egy általánosabb esetre vonatkozó bizonyítást is mutatunk.

2.1.2. Tétel (Ball, Blokhuis, Mazzocca, [3]). *Páratlan rendű $PG(2, q)$ síkban $1 < r < q$ esetén nincsenek $((r-1)q + r, r)$ -ívek.*

2.1.3. Tétel (Denniston). *Páros q -ra minden $r|q$ -ra létezik $((r-1)q + r, r)$ -ív $PG(2, q)$ -ban, sőt $AG(2, q)$ -ban.*

2.1.4. Tétel. *Ha $r|q$ és $r \leq \frac{q}{4}$, akkor $PG(2, q)$ bármely (k, r) -ívére $k \leq (r-1)q + \frac{2r}{3}$ teljesül.*

Összességében a legjobb, amit általánosan mondhatunk a $PG(2, q)$ -beli (k, r) -ívek méretére vonatkozóan:

2.1.5. Tétel. Ha $q = p^h$, és $p^e = (r, q)$, akkor

$$k \leq \begin{cases} (r-1)q + \lfloor \frac{r^2-1}{q} \rfloor, & \text{ha nincs elkerülő egyenes ([4]),} \\ (r-1)q + p^e, & \text{ha van elkerülő egyenes ([1]).} \end{cases}$$

2.1.6. Tétel (Weiner, [16]). Egy $PG(2, q)$ -beli (k, p^e) -ívre, ahol $q = p^h$, $p \geq 2$ és $p^e \leq \frac{1}{2}\sqrt{q}$, teljesül, hogy

$$k \leq (p^e - 1)q + p^e - \frac{1}{4}\sqrt{q}.$$

2.2. Magasabb dimenzióban

A továbbiakban tegyük fel, hogy $n \geq 3$, valamint, hogy $n \leq r < \sum_{i=0}^{n-1} q^i$. Mivel bármely hipersíkon pontosan $\sum_{i=0}^{n-1} q^i$ pont helyezkedik el, illetve bármely legfeljebb n különböző ponthoz van olyan hipersík, amely tartalmazza őket, $r \geq \sum_{i=0}^{n-1} q^i$ esetben a legnagyobb ív a teljes $PG(n, q)$, míg $r \leq n-1$ esetben r pont lenne a legnagyobb méretű (k, r) -ív.

Ekkor a 2.1.1. tétel általánosítható magasabb dimenzióban is. A gondolatmenet egy az egyben átvihető annyi különbséggel, hogy az egyenesek helyett az ív olyan hipersíkokkal vett metszetének méretét vizsgáljuk, amelyek metszete egy $(n-2)$ -dimenziós altér, és amik így a metszeten kívül a tér minden pontját pontosan egyszer fedik.

2.2.1. Állítás. $PG(n, q)$ -ban $m_r(n, q) \leq (r - n + 1)q + r$. Egyenlőség esetén bármely n pont legalább $(n-1)$ -dimenziós alteret feszít.

Bizonyítás. Legyen Ω egy $PG(n, q)$ -beli teljes (k, r) -ív. Legyen továbbá Π_{n-2} a tér olyan $(n-2)$ -dimenziós altere, amelyen a legtöbb Ω -beli pont van, és $d := |\Pi_{n-2} \cap \Omega|$. Ekkor az ezen átmenő hipersíkok mindegyikén legfeljebb $(r-d)$ további pontja lehet Ω -nak.

Továbbá vegyük észre, hogy $d \geq n-1$, hiszen az ív teljessége miatt van olyan hipersík, amely r -szelő ($r \geq n$), és ezen a hipersíkon $n-1$ pontját kiválasztva az ívnek, azok egy legfeljebb $(n-2)$ -dimenziós alteret feszítenek.

Ezzel, és az adott altéren átmenő adott dimenziós alterek számára vonatkozó (2) azonosságot felhasználva megkapjuk a kívánt felső korlátot. $\square$

2.2.2. Megjegyzés. Ha $d = |\Pi_{n-2} \cap \Omega| > n-1$ teljesül egy teljes ívre, akkor az ív mérete $k \leq (q+1)(r-d) + d = (r-d)q + r$. Nyilván $d \leq r$. Ebből következik az is, hogy ha egy $PG(n, q)$ -beli (k, r) -ívre teljesül, hogy $k > (r-d)q + r$, akkor bármely $(n-2)$ -dimenziós hipersíkra $|\Pi_{n-2} \cap \Omega| < d$.

Az egyenlőség esetét most csak q prím esetén vizsgáljuk. Bár a későbbiekben enélkül is ki fog derülni, hogy egyenlőség alig pár esetben állhat fenn, azért lássuk be a következő segédállítást:

2.2.3. Állítás. *Legyen q prím, valamint $r > k_1 > k_2 > \dots > k_m \geq 0$ a hipersíkok és az ív metszetének lehetséges méretei. Ekkor, ha $m_r(n, q) = (r - n + 1)q + r$ teljesül, az $(r - k_m)$, $(r - k_i)$, $(k_i - k_m)$ ($\forall i \in \{1, \dots, m - 1\}$) mindegyike q -val osztható, valamint $n - 2 \geq k_1$, így $q \leq r$ és ha az $[r - n + 2, r]$ intervallumban nincs q -val osztható szám, az ívnek csak r -szelői lehetnek.*

Bizonyítás. Az előző bizonyítás alapján egyenlőség esetén az $(n - 2)$ -dimenziós altérben elhelyezkedő ívpontok számának maximuma $d = n - 1$, valamint ha egy $(n - 2)$ -dimenziós altér $(n - 1)$ -szelő, az azon átmenő $q + 1$ hipersík mindegyike r -szelő lesz.

Ugyanakkor emiatt, ha egy hipersík legfeljebb $(r - 1)$ -szelő, akkor annak bármely $(n - 2)$ -dimenziós altere legfeljebb $(n - 2)$ -szelő. Tehát ekkor a hipersík is legfeljebb $(n - 2)$ -szelője lehet az ívnek, hiszen $n - 1$ pont által kifeszített altér legfeljebb $(n - 2)$ -dimenziós.

Jelölje k_1 az ív második legnagyobb, $(n - 2)$ -dimenziós $\Pi_{n-2}^{k_1}$ altérrel vett metszetének méretét. Vegyük észre, hogy ezt az alteret tartalmazza egy hipersík, amin pontosan ez a k_1 darab ívpont van. Hiszen $\Pi_{n-2}^{k_1}$ -n keresztül kell lennie r -nél kevesebb ívpontot tartalmazó hipersíknak (különben legalább $rq - qk_1 + r > rq - q(n - 1) + r$ méretű lenne az ív), valamint ezeken nem lehetnek további pontok, mivel ekkor a hipersíkon $k_1 < k \leq n - 2$ pont lenne, ami ellentmond k_1 definíciójának. Ebből az is látszik, hogy bármely $\Pi_{n-2}^{k_1}$ -n keresztüli hipersík k_1 - vagy r -szelő.

Jelölje $s_r \leq q$ a $\Pi_{n-2}^{k_1}$ -t tartalmazó r -szelő hipersíkok számát ($s_r \geq 1$, különben csak k_1 pontja lehetne az ívnek). Ekkor az ív pontjainak száma $(r - n + 1)q + r = k_1 + (r - k_1)s_r$, vagyis $(r - n + 1)q = (s_r - 1)(r - k_1)$, tehát $(s_r - 1) < q$, és $r - n + 1 \geq 1$ miatt $q | r - k_1$.

A továbbiakat rekurzióval tudjuk belátni. Tegyük fel, hogy $\forall i < l$ -re beláttuk, hogy $q | r - k_i$. Vegyünk egy k_l -szelő $\Pi_{n-1}^{k_l}$ hipersíkot, amire $k_{l-1} > k_l$, és $\nexists j : k_{l-1} > k_j > k_l$, hogy van az ívet k_j pontban metsző hipersík. Ekkor van olyan $(n - 2)$ -dimenziós $\Pi_{n-2}^{k_l}$ altere a hipersíknak, ami tartalmazza a metszéspontokat. Ezen keresztül az r -szelő, illetve k_i -szelő ($k_i > k_l$) hipersíkok száma rendre s_r, s_i , a többi (≥ 1) hipersíkon pedig pontosan k_l ívpont van. Tehát

$$(r - n + 1)q + r = k_l + (r - k_l)s_r + \sum_{i=1}^{l-1} (k_i - k_l)s_i,$$

amiből

$$q(r - n + 1) = \left(s_r - 1 + \sum_{i=1}^{l-1} s_i \right) (r - k_l) - \sum_{i=1}^{l-1} s_i (r - k_i),$$

és mivel $\left(s_r - 1 + \sum_{i=1}^{l-1} s_i\right) < q$, következik, hogy $q|(r - k_l)$.

Ha a hipersíkok és az ív metszetének méretének minimuma $k_m \geq 0$, akkor persze átírható $q|(r - k_m) - (r - k_i) = k_i - k_m \ \forall i \in \{1, \dots, m-1\}$ alakra. $\square$

Tehát ha van az ívet elkerülő hipersík, akkor r is, valamint bármely hipersík ívvel vett metszetének mérete is osztható q -val.

Vegyük észre, hogy a bizonyítás során erősen kihasználtuk, hogy az $(n-2)$ -dimenziós altereken lévő pontok vagy maximális $d = n-1$ számúak, vagy tartalmazza őket $(n-3)$ -dimenziós altér. Így $d > n-1$ esetben az $m_r(n, q) = (r-d)q + r$ egyenlőség nem kezelhető ilyen egyszerűen.

2.2.4. Megjegyzés. $q|k_i - k_{i+1} > 0 \ \forall i$ -ből persze az is adódik, hogy $n-2 \geq (m-1)q$, és így az $n=2$ esetben $1 \geq m$, tehát $q|r$, amit az 2.1.1. síkokra vonatkozó állítással összevetve megkapjuk, hogy prímrendű síkon egyenlőség esetén $r = q$. Ez azt jelenti, hogy az ív komplementere egy $q^2 + q + 1 - ((q-1)q + q) = q + 1$ méretű blokkoló halmaz, amely 1.3.2. alapján egy egyenes. Tehát az ív pont a $PG(2, q)$ -ba beágyazott affin sík.

2.2.5. Megjegyzés. $n=3$ esetén $1 \geq k_1$, $1 \geq (m-1)q$, tehát vagy minden hipersík r és 1 pontban metszi az ívet, vagy r és 0 pontban, vagyis $q|r-1$ vagy $q|r$. Tehát projektív 3-dimenziós térben (k, r) -ívre $q \geq r+1$ prím esetén $k < (r-2)q + r$.

2.2.6. Állítás. *Ha a $PG(n, q)$ -beli (k, r) -ívnek egy P pontjára teljesül, hogy a rajta átmenő hipersíkokon bármely $m \leq n$ pont általános helyzetű, akkor az ívet ebből a P pontjából levetítve egy, a pontot nem tartalmazó hipersíkjára, egy $PG(n-1, q)$ -beli $(k-1, r-1)$ -ívet kapunk.*

Ha a P ponton átmenő hipersíkok r -, s_i -szelők voltak, akkor a vetület szelői $(r-1)$ -, (s_i-1) -szelők lesznek.

Bizonyítás. Mivel n -dimenziós projektív térben két pont egyértelműen meghatároz egy egyenest, és bármely egyenes és azt nem tartalmazó hipersík metszete egy pont, a vetítés injektív az ívre nézve. Így a vetítés után $k-1$ különböző pontunk lesz. Továbbá mivel minden egyenesen legfeljebb 2 pontja van az ívnek, a vetítés bijektív is az ívre nézve.

A vetítés után, a hipersík egy adott l -dimenziós H_l alterén pont a $PG(n, q)$ -beli, $\langle H_l, P \rangle$ generált $(l+1)$ -dimenziós altéren elhelyezkedő, nem P ívpontjai lesznek, speciálisan a $PG(n-1, q)$ tér $(n-2)$ -dimenziós hipersíkjai az kapott ívnek legfeljebb $r-1$ pontja van. $\square$

2.2.7. Megjegyzés. Ha a 2.2.1. állításban $d = n-1$, akkor bármely $m \leq n$ pont is általános helyzetű, hiszen tegyük fel, hogy van olyan $m \leq n$ pont amelyek által generált altér

legfeljebb $m - 2$ -dimenziós. Ekkor hozzávéve további $n - m - 2$ pontját az ívnek, azok egy legfeljebb $(n - 2)$ -dimenziós alteret generálnának, amiben így legalább n pont lenne.

2.2.8. Következmény. *Ha $PG(n, q)$ -ban van olyan $(m_r(n, q), r)$ -ív, amelynek létezik P pontja, amin átmenő hipersíkok bármely $(n - 2)$ dimenziós altere legfeljebb $(n - 1)$ pontban metszi az ívet, akkor $m_r(n, q) \leq m_{r-1}(n - 1, q) + 1$, ha $n \geq 3$.*

Egyenlőség akkor állhat fenn, ha ebből a P pontból vetítve egy azt nem tartalmazó hipersíkra, $(m_{r-1}(n - 1, q) - 1, r - 1)$ -ívet kapunk.

2.2.9. Megjegyzés. A vetítés utáni $(k - 1, r - 1)$ -ívnek legfeljebb $(n - 2)$ pontja lesz egy $(n - 3)$ -dimenziós alterén, hiszen tegyük fel, hogy lesz olyan $(n - 3)$ -dimenziós altér, amin van $n - 1$ pont. Ezek a pontok ekkor eredetileg egy $(n - 2)$ -dimenziós alteret feszítettek, hiszen $PG(n, q)$ minden P -átmenő alterén, legfeljebb $(n - 1)$ pont általános helyzetű volt. Viszont a vetítés miatt a $PG(n - 1, q)$ tér ezen $(n - 3)$ -dimenziós alterének ősképe egy P -n keresztüli $(n - 2)$ -dimenziós altér, amin így P -vel együtt legalább n pont lenne.

2.2.10. Következmény. *Ha $PG(n, q)$ -ban van olyan $(m_r(n, q), r)$ -ív, amelynek létezik pontja, amin átmenő hipersíkok bármely $(n - 2)$ -dimenziós altere legfeljebb $(n - 1)$ pontban metszi az ívet, akkor $m_r(n, q) \leq m_{r-n+s}(s, q) + n - s$, $\forall n \geq s \geq 2$.*

Speciálisan $m_r(n, q) \leq m_{r-n+2}(2, q) + n - 2$, tehát felhasználva a 2.1.1., 2.1.2., 2.2.3. állításokat, valamint hogy $n \leq r$, az alábbi kapjuk:

2.2.11. Következmény. *Ha $n \geq 3$, a $PG(n, q)$ -beli maximális (k, r) -ívek méretére*

$$m_r(n, q) \leq (r - n + 1)q + r$$

teljesül, egyenlőség esetén pedig $(r - n + 2)|q$.

Amennyiben q prím, akkor egyenlőség esetén $r - n + 2 = q$, továbbá ha $q \geq n - 2$ is teljesül, az ívnek csak r -, $(n - 2)$ -, és 0 -szelői lehetnek.

Ha q páratlan és $r - n + 2 < q$ teljesül, akkor nem állhat fenn egyenlőség.

2.2.12. Állítás. *Ha a $PG(n, q)$ -beli teljes (k, r) -ívre $k > (r - n)q + r$, akkor*

$$k - r \leq \begin{cases} q^2, & \text{ha } q \text{ páros,} \\ q^2 - q, & \text{ha } q \text{ páratlan.} \end{cases}$$

Bizonyítás. A 2.2.2. megjegyzés alapján a $k > (r - n)q + r$ esetben bármely $(n - 2)$ -dimenziós altéren legfeljebb $n - 1$ pont van. A teljesség miatt vehetjük az ív egy r -szelőjét, ami így egy $PG(n - 1, q)$ -beli $(r, n - 1)$ -ívben fogja metszeni az ívet. Ekkor az ívnek 2.2.7.

alapján bármely $((n-1)-2)$ -dimenziós alterén legfeljebb $(n-1)-1$ pontja van. Tehát alkalmazhatjuk a 2.2.10. következményt, amiből

$$r \leq m_{n-1}(n-1, q) \leq m_2(2, q) + n - 3.$$

Alkalmazva Bose tételét (1.2.2.), q paritásától függően az $r-n+1 \leq q$ illetve az $r-n+2 \leq q$ egyenlőtlenséget kapjuk, amivel a 2.2.11. állításból következik a kívánt egyenlőtlenség. $\square$

2.2.13. *Megjegyzés.* Tehát ha $((r-n)q+r)$ -nél nagyobb méretű ívet szeretnénk találni, $r-n+1 \leq q$ is feltehető.

2.2.14. *Megjegyzés.* A 2.2.7. megjegyzés alapján, minden $PG(n, q)$ -beli (k, r) -ív, melyre $k > (r-n)q+r$, része egy süvegnek. Hiszen ha lenne három kollineáris pontja, akkor ezekhez $(n-3)$ pontot hozzávéve, azok egy legfeljebb $(n-2)$ -dimenziós alteret feszítenének, tehát $d \geq n$, vagyis $k \leq (r-n)q+r$ teljesülne.

2.3. A $PG(n, q)$ -beli (k, n) -ívek

A $PG(n, q)$ -beli (k, n) -ívek szoros kapcsolatban állnak bizonyos kódelméletben fontos objektumokkal, így ezeket már széles körben tanulmányozták. Lássunk néhány eredményt ezekről az ívekről.

Először is, vegyük észre, hogy a 2.2.11. állításból következően

$$m_n(n, q) \leq q + n,$$

egyenlőség esetén q páros.

Ennél azonban jelentősen erősebb felső korlátok is teljesülnek.

2.3.1. Tétel (Ball, De Beule). *A $PG(n, q)$ -beli (k, n) -ívek méretére teljesül, hogy*

- *ha $q = p^h$ és $n \leq 2p-3$, akkor $k \leq q+1$,*
- *ha q páratlan és $n \leq \frac{1}{4}\sqrt{q} + \frac{9}{4}$, akkor $k \leq q+1$.*

2.3.2. Állítás. *A $PG(3, q)$ $(k, 3)$ -ívei $q > 2$ esetén legfeljebb $q+1$ pontúak.*

Észrevehetjük, hogy az állítás páratlan q -ra azonnal következik az előző tételből, hiszen ekkor $p \geq 3$, vagyis $n = 3 \leq 2p-3$.

2.3.3. *Megjegyzés.* Az 1.1.9. felhasználásával belátható, hogy $PG(3, 2)$ -ben az öt alappont, tehát a $(0:0:0:1)$, $(0:0:1:0)$, $(0:1:0:0)$, $(1:0:0:0)$, $(1:1:1:1)$, egy $(5, 3)$ -ívet alkot, hiszen bármely négy vektorból alkotott mátrix determinánsa 1 lesz. Ennél nagyobb méretűt nem is tudunk megadni, hiszen ez pont eléri a $q+n$ felső korlátot (ebben az esetben $q = 2$, $n = 3$).

Az 1.2.16. állításban már láttuk, hogy a $PG(n, q)$ térben a $\mathcal{C}_n$ momentumgörbe pontjai $(q+1, n)$ -ívet alkotnak, vagyis az előző állítás éles korlátot ad. Nevezetes, Segre-től származó sejtés, hogy ha $n < q-2$, akkor $q+1$ -nél nagyobb méretű (k, n) -ívek nincsenek.

2.3.4. Tétel (Segre). $PG(3, q)$ -ban páratlan $q > 7$ esetén bármely $(q+1, 3)$ -ív projektív ekvivalens a momentumgörbével.

$PG(3, q)$ -ben $q = 2^h$ esetén nem igaz, hogy a $(q+1, n)$ -ívek mind ekvivalensek lennének a momentumgörbével. Ezeket az íveket Casse és Glynn karakterizálták 1982-ben ([9]), valamint megmutatták a következőt is:

2.3.5. Tétel (Casse, Glynn, [8]). Ha $q \geq 8$ páros, akkor $PG(4, q)$ -ban bármely $(k, 4)$ -ív mérete $k \leq q+1$, és egyenlőség esetén az ív projektív ekvivalens a momentumgörbével.

2.3.6. Tétel (Storme, J.Thas, [14]). Legyen $n \geq 4$, $q \geq (2n - \frac{11}{2})^2$ páros. Ekkor a $PG(n, q)$ térben a legnagyobb (k, n) -ívre $k \leq (q+1)$ teljesül. Továbbá, ha $q > (2n - \frac{7}{2})^2$, akkor minden $(q+1, n)$ -ív projektív ekvivalens $\mathcal{C}_n$ -nel.

2.3.7. Tétel (J.Thas). Legyen $n \geq 2$, $q \geq n+3$, és tegyük fel, hogy $PG(n, q)$ -ban minden $(q+1, n)$ -ív projektív ekvivalens $\mathcal{C}_n$ -nel. Ekkor $PG(q-1-n, q)$ -ban is minden $(q+1, n)$ -ív projektív ekvivalens $\mathcal{C}_{q-1-n}$ -nel.

Speciálisan, $PG(q-2, q)$ -ban léteznek $(q+2, q-2)$ -ívek.

3. fejezet

Teljes $(k, 4)$ -ívek $PG(3, q)$ -ban

Láttuk, hogy a $PG(n, q)$ -beli (k, n) -íveket, kifejezetten $n = 3$ esetén, már mélyrehatóan tanulmányozták, így kézenfekvő következő lépésként, a diplomamunka során főleg a $PG(3, q)$ -beli $(k, 4)$ -ívekre koncentráltunk. Egyrészt próbáltunk minél nagyobb ilyen íveket találni kis q prím értékekre, másrészt igyekeztünk ezek segítségével megsejteni méretre vonatkozó általánosabb korlátokat, valamint olyan általános q -ra megadható szabályos struktúrát találni, amely $(k, 4)$ -ívet alkot.

Mindenekelőtt tegyünk egy hasznos megfigyelést, idézzük fel a 2.2.2. megjegyzést a $PG(3, q)$ -beli $(k, 4)$ -ívekre vonatkoztatva.

3.0.1. Állítás. *A $PG(3, q)$ -ban, ha egy $(k, 4)$ -ívnek van három kollineáris pontja, akkor $k \leq q + 4$.*

Bizonyítás. Legyen Ω egy $(k, 4)$ -ív, amelynek P_1, P_2, P_3 egymástól különböző pontjai az e egyenesre illeszkednek. Ekkor valamennyi e -t tartalmazó síkon legfeljebb egy további pontja lehet Ω -nak. Tudjuk, hogy bármely egyenesen keresztül pontosan $q + 1$ különböző sík megy át, ezzel megkaptuk, hogy $|\Omega| \leq 3 + q + 1$. $\square$

Ha az ívnek nincs három kollineáris pontja, akkor használhatjuk a 2.2.1. állítás eredményét. Lássunk most erre egy másik tanulságos bizonyítást is.

3.0.2. Állítás. *$PG(3, q)$ térben a $(k, 4)$ -ívek maximális méretére teljesül, hogy*

$$m_4(3, q) \leq 2q + 4.$$

Bizonyítás. Vegyük észre, hogy ha egy (nem teljes) $(k, 4)$ -ív legalább 3-szelő síkjai lefedik a $PG(3, q)$ tér összes egyenesét, akkor bármely két pont hozzávételével keletkezik olyan sík, amelyen legalább 5 pont van. Valóban, tegyük fel, hogy a P_1, P_2 pont hozzávételével még nincs legalább 5 pontos sík. Ez azt jelentené, hogy az általuk meghatározott egyenesen keresztül minden síkon legfeljebb 2 pont lehetett, ami ellentmond a lefedettségnek.

Tegyük fel, hogy a $(k, 4)$ -ívnek van olyan i -szelő egyenese, amely nincs lefedve 3- vagy 4-szelővel ($i \leq 2$). Ekkor a rajta átmenő síkok mindegyikén legfeljebb $2 - i$ pontja lehet az ívnek, vagyis $k \leq (q + 1)(2 - i) \leq 2q + 2$. Az előző észrevételt felhasználva ekkor viszont megkaptuk, hogy ha $k = 2q + 3$, akkor legfeljebb egy pont vehető már csak az ívhez, amiből megkaptuk az állítást. $\square$

Bár a szakdolgozati munka során ezzel nem foglalkoztunk, ebből az is látszik, hogy az egyeneseket lefogó síkhalmazokra vonatkozó eredmények felhasználásával is lehetne következtetéseket levonni $PG(3, q)$ -beli általánosított ívek méretével kapcsolatban.

Az utóbbi tétel jól mutatja, hogy a $(k, 4)$ -ívek maximális méretének vizsgálata során azzal az esettel érdemes foglalkozni, amikor az ívnek bármely három pontja általános helyzetű.

3.1. Szelősíkok száma

Először néhány kombinatorikai megfigyelést teszünk abban az esetben, amikor a $PG(3, q)$ -beli Ω teljes $(k, 4)$ -ívnek nincs három kollineáris pontja.

Jelöljük $\mathcal{S}_i$ -vel a $PG(3, q)$ síkjainak azon halmazát, melyek pontosan i pontban metszik a Ω ívet (i -szelők), továbbá egy adott $A \subseteq \Omega$ részhalmazra $\mathcal{S}_i^A$ -val azokat az i -szelő síkokat, melyek tartalmazznak minden A -belit.

Világos, hogy ha $P, Q \in \Omega$ különböző pontok, akkor

$$|\mathcal{S}_0| + |\mathcal{S}_1| + |\mathcal{S}_2| + |\mathcal{S}_3| + |\mathcal{S}_4| = q^3 + q^2 + q + 1, \quad (3.1)$$

$$|\mathcal{S}_1^P| + |\mathcal{S}_2^P| + |\mathcal{S}_3^P| + |\mathcal{S}_4^P| = q^2 + q + 1, \quad (3.2)$$

$$|\mathcal{S}_2^{\{P, Q\}}| + |\mathcal{S}_3^{\{P, Q\}}| + |\mathcal{S}_4^{\{P, Q\}}| = q + 1. \quad (3.3)$$

Valamint ha veszünk egy e egyenest, akkor az ív rajta lévő $\Omega \cap e$ pontjain kívüli $(k - |\Omega \cap e|)$ pontja az e -n átmenő szelőkön helyezkedik el, mindegyik pontosan az egyiken, továbbá az i -szelőkön pontosan $i - |\Omega \cap e|$ pont van. Tehát

$$k - |\Omega \cap e| = \sum_{i=|\Omega \cap e|+1}^4 (i - |\Omega \cap e|) \cdot |\mathcal{S}_i^e|. \quad (3.4)$$

Vizsgáljuk meg, mi történik, ha adott $P \in \Omega$ ponton átmenő síkokat a rajta átmenő 2-szelő egyenesek segítségével számoljuk meg. Ekkor minden síkot pontosan annyszor számoltunk, ahány P -n keresztüli 2-szelő egyenes van rajta:

$$\sum_{Q \in \Omega \setminus P} |\mathcal{S}_4^{\{P, Q\}}| = 3|\mathcal{S}_4^P|, \quad \sum_{Q \in \Omega \setminus P} |\mathcal{S}_3^{\{P, Q\}}| = 2|\mathcal{S}_3^P|, \quad \sum_{Q \in \Omega \setminus P} |\mathcal{S}_2^{\{P, Q\}}| = |\mathcal{S}_2^P|. \quad (3.5)$$

Hasonlóan, amennyiben a tér síkjait az egyes pontokon átmenő síkok segítségével számoljuk meg, a következő összefüggéseket kapjuk:

$$\sum_{P \in \Omega} |\mathcal{S}_4^P| = 4|\mathcal{S}_4|, \sum_{P \in \Omega} |\mathcal{S}_3^P| = 3|\mathcal{S}_3|, \sum_{P \in \Omega} |\mathcal{S}_2^P| = 2|\mathcal{S}_2|, \sum_{P \in \Omega} |\mathcal{S}_1^P| = |\mathcal{S}_1|. \quad (3.6)$$

Ezeket felhasználva megkaphatjuk a következő állítást:

3.1.1. Állítás. *A $PG(3, q)$ -beli Ω $(k, 4)$ -ívek adott P pontján átmenő i -szelősíkjainak száma meghatározható a ponton átmenő 4-szelők számából, a következő összefüggésekkel:*

- $|\mathcal{S}_3^P| = \binom{k-1}{2} - 3|\mathcal{S}_4^P|,$
- $|\mathcal{S}_2^P| = (k-1)(q+3-k) + 3|\mathcal{S}_4^P|,$
- $|\mathcal{S}_1^P| = q^2 + q + 1 - (k-1)(q+1) + \binom{k-1}{2} - |\mathcal{S}_4^P|.$

Bizonyítás. A 3-szelőkre vonatkozó összefüggéshez azt kell meggondolni, hogy ha a P ponthoz választunk két különböző pontot, akkor azok egy 3- vagy 4-szelőt fognak meghatározni. Ily módon minden P -n keresztüli 3-szelőt pontosan egyszer, a 4-szelőket pedig pontosan $\binom{3}{2} = 3$ -szor kapjuk meg.

A (3.5) egyenleteket összeadva és a (3.3) azonosságot felhasználva, majd behelyettesítve az $|\mathcal{S}_3^P| = \binom{k-1}{2} - 3|\mathcal{S}_4^P|$ egyenlőséget kapjuk, hogy

$$(k-1)(q+1) = 3|\mathcal{S}_4^P| + 2|\mathcal{S}_3^P| + |\mathcal{S}_2^P| = 2\binom{k-1}{2} - 3|\mathcal{S}_4^P| + |\mathcal{S}_2^P|.$$

Ezt átrendezve, megkapjuk a 2-szelőkre vonatkozó összefüggést.

Ezután a (3.2) egyenletet, valamint az előbbi azonosságot felhasználva kapjuk, hogy

$$q^2 + q + 1 = |\mathcal{S}_1^P| + (k-1)(q+1) - 2\binom{k-1}{2} + 3|\mathcal{S}_4^P| + \binom{k-1}{2} - 3|\mathcal{S}_4^P| + |\mathcal{S}_4^P|,$$

ami átrendezve pont az 1-szelőkre vonatkozó egyenlőség. □

3.1.2. Állítás. *A $PG(3, q)$ -beli Ω $(k, 4)$ -ívek szelősíkjainak száma egyértelműen meghatározható a 4-szelők számából, pontosabban, a következő összefüggések teljesülnek:*

- $|\mathcal{S}_3| = \binom{k}{3} - 4|\mathcal{S}_4|,$
- $|\mathcal{S}_2| = \binom{k}{2}(q+3-k) + 6|\mathcal{S}_4|,$
- $|\mathcal{S}_1| = k(q^2 + q + 1 - (k-1)(q+1) + \binom{k-1}{2}) - 4|\mathcal{S}_4|,$
- $|\mathcal{S}_0| = q^3 + q^2 + q + 1 - k(q^2 + q + 1) + \binom{k}{2}(q+1) - \binom{k}{3} + |\mathcal{S}_4|.$

Bizonyítás. Ha vesszük az összes lehetséges ponthármas Ω -ból és a rájuk illeszkedő síkokat, akkor megkapjuk az összes 3-és 4-szelő síkot, az előbbieket egy, az utóbbiak mind-egyikét pontosan négy hármas esetén, tehát

$$|\mathcal{S}_3| + 4|\mathcal{S}_4| = \binom{k}{3}.$$

Felhasználva az előző, 3.1.1. állítást egyenleteit, azokat $\forall P \in \Omega$ -ra összegezve, majd a (3.6) azonosságokat behelyettesítve megkapjuk a 2- és 1-szelőkre vonatkozó egyenlőségeket is.

$$\begin{aligned} \sum_{P \in \Omega} |\mathcal{S}_1^P| &= k \left(q^2 + q + 1 - (k-1)(q+1) + \binom{k-1}{2} \right) - \sum_{P \in \Omega} |\mathcal{S}_4^P|, \\ |\mathcal{S}_1| &= k \left(q^2 + q + 1 - (k-1)(q+1) + \binom{k-1}{2} \right) - 4|\mathcal{S}_4|. \end{aligned}$$

Valamint

$$2|\mathcal{S}_2| = \sum_{P \in \Omega} |\mathcal{S}_2^P| = k(k-1)(q+1) - 2k \binom{k-1}{2} + 3 \sum_{P \in \Omega} |\mathcal{S}_4^P|,$$

tehát

$$|\mathcal{S}_2| = \frac{k(k-1)(q+1)}{2} - k \binom{k-1}{2} + 6|\mathcal{S}_4|.$$

Ezután a fentieket és a (3.1)-et felhasználva, megkapjuk az elkerülő síkok állításban szereplő számát. $\square$

3.1.3. Állítás. *Legyen $P \in \Omega$, és a $A \notin \Omega$ olyan pont, amely nincs rajta az ív pontjai által meghatározott egyenesek egyikén sem. Ekkor*

- $|\mathcal{S}_2^{PA}| + 2|\mathcal{S}_3^{PA}| + 3|\mathcal{S}_4^{PA}| = k-1,$
- $|\mathcal{S}_2^A| + 3|\mathcal{S}_3^A| + 6|\mathcal{S}_4^A| = \binom{k}{2}.$

Bizonyítás. A PA egy 1-szelő egyenesen átmenő szelősíkok segítségével a pontokat megszámlálva, a (3.4) azonosság alapján megkapjuk az állítás első felét.

Ha a A pont mellé választunk két tetszőleges ívbéli pontot, azzal meghatároztunk egy legalább 2-szelő síkot A -n keresztül. Ekkor minden i -szelőt ($i \geq 2$) pontosan $\binom{i}{2}$ pontpár esetén számoltunk, így kapjuk a második azonosságot.

Az állítás második fele az elsőből is megkapható, hiszen ha $\forall P \in \Omega$ -ra felírjuk, majd a k egyenletet összegezzük, az i -szelők ($i \geq 2$) mindegyikét pontosan i -szer kapjuk meg. Tehát a

$$2|\mathcal{S}_2^Q| + 3 \cdot 2 \cdot |\mathcal{S}_3^Q| + 4 \cdot 3 \cdot |\mathcal{S}_4^Q| = k(k-1)$$

egyenlethez jutunk. $\square$

3.1.4. Állítás. Legyen az Ω egy $PG(3, q)$ -beli $(k, 4)$ -ív, ahol $k \geq q + 5$. Ekkor

$$\frac{k(k-1)(k-q-3)}{12} \leq |\mathcal{S}_4| \text{ és } \forall P \in \Omega\text{-ra } \frac{(k-1)(k-q-3)}{3} \leq |\mathcal{S}_4^P|.$$

Speciálisan $|\mathcal{S}_4^P| \geq \frac{2}{3}(q+4)$ és $|\mathcal{S}_4| \geq \frac{(q+5)(q+4)}{6}$.

Bizonyítás. A 3.0.1. állítás alapján az ívnek nincs három kollineáris pontja, tehát tetszőleges $Q \in \Omega \setminus P$ pontra $k-2 = |\mathcal{S}_3^{PQ}| + 2|\mathcal{S}_4^{PQ}| \leq q+1 + |\mathcal{S}_4^{PQ}|$. Ezt megfelelően átrendezve, majd összegezve a P -től különböző ívpontokra, a (3.5) alapján kapjuk, hogy

$$k(k-q-3) \leq \sum_{Q \in \Omega \setminus P} |\mathcal{S}_4^{\{P, Q\}}| = 3|\mathcal{S}_4^P|,$$

majd a (3.6)-tal, hogy

$$k(k-q-3) \leq 3 \sum_{P \in \Omega} |\mathcal{S}_4^P| = 12|\mathcal{S}_4|.$$

□

3.2. Ívek mérete

Először vizsgáljuk meg a $q = 2$ esetet. Ekkor a 2.2.1. állításból következik, hogy $k \leq 8$, és egyenlőség esetén az ívnek nincs 3 kollineáris pontja, vagyis süveg. Ekkor viszont az 1.2.6. állítást felhasználva azt kapjuk, hogy a $(8, 4)$ -ívek $PG(3, 2)$ -ben pontosan a projektív térbe beágyazott $AG(3, 2)$ maximális süvegek, hiszen $AG(3, 2)$ minden síkján pontosan 4 pont van.

A továbbiakban csak $q \geq 3$ esettel foglalkozunk. A 2.2.3. és 2.2.11. állítások speciális eseteként megkaphatjuk az alábbiakat.

3.2.1. Állítás. Ha $q \neq 3$, akkor $m_4(3, q) \leq 2q + 3$.

Ha $q = 3$, akkor $m_4(3, q) \leq 2q + 4$, egyenlőség esetén az ívnek csak 4- és 1-szelői vannak.

3.2.2. Megjegyzés. Feltéve, hogy nincs három kollineáris pontja az ívnek, az állítás második fele a 3.1.1. felhasználásával is azonnal következik. Eszerint az ív bármely P pontjára $0 \leq |\mathcal{S}_3^P| + |\mathcal{S}_2^P| = (k-1)\frac{(2q+4-k)}{2}$, vagyis $k \leq 2q+4$ teljesül, és a $k = 2q+4$ esetben nincsenek 3- és 2-szelők.

Vegyük észre, hogy $q = 3$ -ra fennáll az állításbeli egyenlőség, sőt az $(m_4(3, 3), 4)$ -ívek pont a $PG(3, 3)$ tér elliptikus kvádrikái. Hiszen ha $m_4(3, 3) > q+4 = 7$, akkor a 2.2.14. megjegyzés alapján az ív része egy süvegnek, így legfeljebb $q^2 + 1 = 10$ pontja lehet. Mivel az 1.2.8. szerint, $q^2 + 1$ pontú süvegnek bármely sík legfeljebb $q+1 = 4$ pontját

tartalmazza, $(10, 4)$ -ív is. Az 1.2.9. alapján $q = 3$ -ra a maximális süvegek pont az elliptikus kvádrikák, és ezzel az 1.2.10. alapján azt is megkaptuk, hogy $PG(3, q)$ -ban a maximális méretű $(k, 4)$ -ívek pontjai Möbius-síkot alkotnak.

A fejezet elején megállapítottuk, hogy azt az esetet érdemes vizsgálni, amikor az ívnek nincs három kollineáris pontja. Ez valójában a 2.2.8. speciális esete.

3.2.3. Állítás. $PG(3, q)$ -ban, ha egy $(k, 4)$ -ívnek nincs három kollineáris pontja, akkor $k \leq m_3(2, q) + 1$

Továbbá, vegyük észre, hogy teljesülnek a 2.2.6. állítás feltételei is. Eszerint, ha a $PG(3, q)$ -beli $(k, 4)$ -ívnek nincs három kollineáris pontja, akkor az ívet egy P pontjából levetítve valamelyik, a pontot nem tartalmazó síkra, egy $PG(2, q)$ -beli $(k - 1, 3)$ -ívet kapunk.

Tekintsük át, milyen következtetésekre juthatunk ezekből, és a 2.1. részben bemutatott síkbeli ívekre vonatkozó eredményekből.

3.2.4. Következmény. (2.1.4) Ha $3|q$ és $12 \leq q$, akkor $PG(3, q)$ bármely $(k, 4)$ -ívére $k \leq 2q + 3$ teljesül.

Vegyük észre, hogy a 3.2.1. állításnál ez nem mond jobbat.

3.2.5. Következmény. (2.1.6) Egy $PG(3, q)$ -beli $(k, 3)$ -ívre, ahol $q = 3^h$, $36 \leq q$:

$$k \leq 2q + 4 - \frac{1}{4}\sqrt{q}.$$

3.2.6. Következmény. (2.1.5) $PG(3, q)$ bármely $(k, 4)$ -ívére

$$k \leq \begin{cases} 2q + \lfloor \frac{8}{q} \rfloor + 1, & \text{ha van olyan pontja az ívnek, amelynek nincs 1-szelő síkja} \\ 2q + s + 1, & \text{ha van olyan pontja az ívnek, amelynek van 1-szelő síkja,} \end{cases}$$

ahol $s = (3, q)$, tehát 1 és 3 értéket vehet fel.

Ezekből és a 3.2.1. állításból a következő korlátokhoz jutunk:

3.2.7. Következmény. $PG(3, q)$ bármely $(k, 4)$ -ívére, ahol $q \geq 3$ és $n_q = \lfloor \frac{8}{q} \rfloor + 1$,

$$k \leq \begin{cases} 2q + 1, & \text{ha } q > 8 \text{ és van olyan pontja az ívnek, amelynek nincs 1-szelő síkja} \\ 2q + 2, & \text{ha } 3 \nmid q > 8 \text{ és az ív minden pontjának van 1-szelő síkja} \\ 2q + 3, & \text{ha } 3|q > 8 \text{ és az ív minden pontjának van 1-szelő síkja} \\ 2q + n_q, & \text{ha } 3 \nmid q \leq 8 \text{ és van olyan pontja az ívnek, amelynek nincs 1-szelő síkja} \\ 2q + 2, & \text{ha } 3 \nmid q \leq 8 \text{ és van olyan pontja az ívnek, amelynek van 1-szelő síkja} \\ 2q + 3, & \text{ha } q = 3 \text{ és van olyan pontja az ívnek, amelynek nincs 1-szelő síkja} \\ 2q + 4, & \text{ha } q = 3 \text{ és az ív minden pontjának van 1-szelő síkja.} \end{cases}$$

Ezek a korlátok $q \in \{3, 5\}$ esetén élesek, $PG(3, 3)$ -ban már láttuk, hogy létezik $(10, 4)$ -ív, illetve $PG(3, 5)$ -ban a $(12, 4)$ -ívre később látunk példát.

A 3.1. rész alapján néhány további, ennél jobb felső korlátot tudunk mondani.

3.2.8. Állítás. *Ha az $\Omega(k, 4)$ -ívnek $\exists P \in \Omega$ pontja, amelyre $|S_1^P| = 0$, akkor $q \leq 3$.*

Bizonyítás. Használjuk a 3.1.1. állítást. Eszerint $|S_1^P| = 0$ esetben

$$|S_4^P| = q^2 + q + 1 - (k - 1)(q + 1) + \binom{k - 1}{2},$$

tehát

$$|S_3^P| = \binom{k-1}{2} - 3(q^2 + q + 1 - (k - 1)(q + 1) + \binom{k-1}{2}) = -3q^2 + 3q(k - 2) - (k - 2)(k - 4).$$

Mivel a 3-szelők száma nemnegatív, $0 \leq -3q^2 + 3q(k - 2) - (k - 2)(k - 4)$, ami a következő alakra hozható:

$$9(2q + 2 - k)^2 + 3(k - 6)^2 \leq 16.$$

Figyelembe véve, hogy q és k nemnegatív egész számok, azt kapjuk, hogy $k \in \{4, 5, 6, 7, 8\}$, továbbá a $|2q + 2 - k| = 0$, vagy a $|2q + 2 - k| = 1$ egyenlőségnek teljesülnie kell. Az előbbi esetben $q \in \{1, 2, 3\}$, az utóbbi esetben pedig $q \in \{1, 2, 3\}$ értékek teljesítik a feltételeket. $\square$

3.2.9. Állítás. *Ha $3 \nmid q \geq 4$, akkor $k \leq 2q + 2$.*

Bizonyítás. Az előző állítás szerint $q \geq 4$ esetén az ív bármely P pontjára teljesül, hogy $|S_1^P| \geq 1$, vagyis az ívet egy pontjából levétítve a projektív síkra, azon lesz elkerülő egyenes. Ekkor a kapott $(k - 1, 3)$ -ív komplementere a $PG(2, q)$ síkon egy olyan $\mathcal{B}$, $(q + 1) - 3 = (q - 2)$ -szeresen blokkoló halmaz lesz, amely tartalmaz egyenest.

Így az 1.3.21. állítás alapján

$$|\mathcal{B}| \geq (q - 2)q - p^e + q + 1$$

teljesül, ahol $p^e = (q, q - 3)$. Világos, hogy $3 \nmid q \geq 4$ esetén $p^e = 1$, tehát megkaptuk, hogy

$$k - 1 = q^2 + q + 1 - |\mathcal{B}| \leq 2q + 1.$$

$\square$

3.2.10. Megjegyzés. Az előző számolás $q = 3^h$, $h \geq 2$ esetben $k \leq 2q + 3$ -at ad, hiszen ekkor $p^e = (q, q - 3) = 3$.

3.2.11. Következmény. $PG(3, q)$ bármely $(k, 4)$ -ívére, ahol $q \geq 3$

$$k \leq \begin{cases} 2q + 2, & \text{ha } 3 \nmid q \geq 4, \\ 2q + 4 - \frac{1}{4}\sqrt{q}, & \text{ha } 3^h = q \geq 36, \\ 10, & \text{ha } q = 3, \\ 2q + 3, & \text{ha } q \in \{9, 27\}, \end{cases}$$

továbbá a $q = 3$, $k = 10$ esetben az ív minden pontjának van 1-szelő síkja.

3.2.12. Megjegyzés. A $3^h = q \geq 36$ feltétel valójában azt jelenti, hogy $q = 3^h$ és $h \geq 4$, tehát $2q + 4 - \frac{1}{4}\sqrt{q} \leq 2q + 4 - \frac{9}{4}$, vagyis mivel az ívek mérete egész szám, $k \leq 2q + 1$ teljesül.

Ezzel a 2.2.10. állítás speciális eseteként kapunk egy magasabb dimenzióbeli korlátot is. Az állítás az $s = 3, r = n + 1$ értékekkel a $m_{n+1}(n, q) \leq m_4(3, q) + n - 3$ összefüggést adja, amelyre alkalmazhatjuk a 3.2.11. következményt.

3.2.13. Következmény. A $PG(n, q)$ -beli $(k, n + 1)$ -ívek esetében teljesül, hogy

$$k \leq \begin{cases} 2q + n - 1, & \text{ha } 3 \nmid q \geq 4, \\ 2q + n + 1 - \frac{1}{4}\sqrt{q}, & \text{ha } 3^h = q \geq 36, \\ n + 7, & \text{ha } q = 3. \\ 2q + n, & \text{ha } q \in \{9, 27\}, \end{cases}$$

A 2.2.11. ennél valamivel gyengébbet mond, mégpedig, hogy $m_{n+1}(n, q) \leq 2q + n + 1$ és egyenlőség esetén $3|q$.

3.2.14. Állítás. $PG(3, q)$ -ban $q > 2$ esetén $m_4(3, q) \geq m_3(3, q) + 1 = q + 2$

Bizonyítás. A $(k, 3)$ -ívhez hozzávéve egy pontot minden síkon legfeljebb 4 pontja lesz az ívnek, így $(k + 1, 4)$ -ívet kapunk.

Láttuk, hogy a $\mathcal{C}_3$ momentumgörbe $(q + 1, 3)$ -ívet alkot $PG(3, q)$ -ban, így ehhez még egy pontot hozzávéve $(q + 2, 4)$ -ívet kapunk. $\square$

Ahogy azt az 1.3. részben már megállapítottuk, a $PG(3, q)$ -beli $\Omega(k, 4)$ -ívhez tartozó $\mathcal{S}_4$ halmaz a duális térben blokkoló halmazt határoz meg. Vegyük észre, hogy $q > 3$ esetben ez nem lehet triviális. Ellenkező esetben a duális téren a blokkoló halmaz tartalmazna egyenest, így az eredeti $PG(3, q)$ -ban lenne olyan egyenes amelyen át minden sík 4-szelő. Ekkor viszont $2 + 2(q + 1)$, $1 + 3(q + 1)$, vagy $4(q + 1)$ pontja lenne az ívnek attól függően, hogy az egyenes 2, 1 vagy 0 pontban metszi. Ez viszont ellentmond az fentebbi megállapításoknak.

Tehát alkalmazhatjuk az 1.3.12. tételt, amely alapján

$$|\mathcal{S}_4| \geq \begin{bmatrix} 2 \\ 1 \end{bmatrix}_q + r_2(q) = q + 1 + r_2(q),$$

vagyis felhasználva, amit $r_2(q)$ -ről tudunk, megkapjuk, hogy

$$|\mathcal{S}_4| \geq \begin{cases} q + 1 + \frac{q+1}{2}, & \text{ha } q \text{ prím,} \\ q + 1 + \sqrt{pq}, & \text{ha } q = p^{2h+1}, h \geq 1, p \text{ prím,} \\ q + 1 + \sqrt{q}, & \text{ha } q = p^{2h}, h \geq 1, p \text{ prím.} \end{cases} \quad (3.7)$$

3.2.15. Állítás. *$PG(3, q)$ -ban a legkisebb méretű teljes $(k, 4)$ -ív mérete, melynek nincs három kollineáris pontja,*

$$k > \begin{cases} \sqrt[3]{36(q+1)}, & \text{ha } q \text{ prím,} \\ \sqrt[3]{24p^{h+1}(p^h+1)}, & \text{ha } q = p^{2h+1}, h \geq 1, p \text{ prím,} \\ \sqrt[3]{24p^h(p^h+1)}, & \text{ha } q = p^{2h}, h \geq 1, p \text{ prím.} \end{cases}$$

Bizonyítás. Használjuk, hogy

$$\binom{k}{3} = |\mathcal{S}_3| + 4|\mathcal{S}_4| \geq 4|\mathcal{S}_4|,$$

majd alkalmazzuk a (3.7) egyenlőtlenségeket, illetve felhasználjuk, hogy $\frac{k^3}{6} > \binom{k}{3}$. $\square$

Továbbá, mivel az $\mathcal{S}_4$ duálisa által definiált blokkolóhalmaz nem tartalmaz síkot sem (hiszen egyenest sem), $q \geq 5$ -re alkalmazhatjuk az 1.3.13. tételt is. Eszerint

$$|\mathcal{S}_4| \geq \begin{bmatrix} 2 \\ 1 \end{bmatrix}_q + \sqrt{q}(1+q) = (q+1)(\sqrt{q}+1), \quad (3.8)$$

amivel lényegesen jobb alsó korlátot tudunk mondani.

3.2.16. Állítás. *$PG(3, q)$ -ban a legkisebb méretű teljes $(k, 4)$ -ív mérete, melynek nincs három kollineáris pontja,*

$$k > \sqrt[3]{24(q+1)(\sqrt{q}+1)}.$$

Bizonyítás. Az előző állításhoz hasonlóan, ezúttal a (3.8) egyenlőtlenség felhasználásával, azt kapjuk, hogy

$$\binom{k}{3} = |\mathcal{S}_3| + 4|\mathcal{S}_4| \geq 4|\mathcal{S}_4| \geq 4(q+1)(\sqrt{q}+1),$$

amiből következik az állítás. $\square$

3.3. $(k, 4)$ -ívek keresése

Láttuk, hogy $PG(3, q)$ -ban a $(k, 4)$ -ívek $q \geq 4$ esetén legfeljebb $2q+2$ pontúak lehetnek. Ennél jobb felső korlátot általános esetben nem sikerült találni, viszont kíváncsiak voltunk, vajon mennyire éles, ezért megpróbáltunk minél nagyobb méretű íveket találni. Ehhez *Python* programkódot írtam, ami a megfelelő projektív tér pontjainak generálása után, speciális ponthalmazok segítségével, random pontok mohón hozzávételével keresett íveket.

A keresés során a két fő irány meglévő speciális ponthalmazok kiegészítése, valamint más speciális halmazokból pontok kiválasztása volt.

Elevenítsük fel a 2.2.14. megjegyzést. Eszerint $PG(3, q)$ -ban minden $k > q + 4$ méretű $(k, 4)$ -ív része egy süvegnek, így ha legalább ekkorát szeretnénk találni, az elemeit érdemes egy maximális méretű süveg, például elliptikus kvádrika pontjai közül kiválasztani. Fontos azonban, hogy nem minden süveg egészíthető ki maximális méretűvé, léteznek a maximálisnál kisebb méretű teljes süvegek is, azaz vannak olyan ívek, amiket így nem találhatunk meg. Viszont most a cél nem a maximális, hanem egy minél nagyobb méretű $(k, 4)$ -ív megtalálása volt, így első irányként elliptikus kvádrika pontjaiból indultunk ki. Ez főleg nagyobb q értékekre bizonyult hasznosnak, mivel így a $q^3 + q^2 + q + 1$ pont helyett csak $q^2 + 1$ pontot kellett figyelembe venni, ami már $q = 7$ -nél jelentősen csökkentette a futásidőt.

3.3.1. Állítás. *Ha a $PG(3, q)$ -beli $(k, 4)$ -ív része egy $\mathcal{K}$ elliptikus kvádríkának, akkor*

$$k \leq 2q + 1 + p^{e(t)},$$

ahol $q = p^h$ és $p^{e(t)} = (4, q)$.

Bizonyítás. Az 1.2.10. és 1.2.11. állításokban láttuk, hogy a $q^2 + 1$ méretű süvegek, így $\mathcal{K}$ pontjai is, Möbius-síkot definiálnak, ahol a sík köreinek a $\mathcal{K}$ nem egy pontú síkmetszetei (tehát amin a süvegnek pontosan $q + 1$ pontja helyezkedik el) felelnek meg.

Ekkor a Möbius-síkon a $(k, 4)$ -ívnek megfelelő pontokra teljesül, hogy a sík bármely körén legfeljebb 4 helyezkedik el közülük. Tehát minden $(k, 4)$ -ívet megkaphatunk úgy, hogy a Möbius-síknak elhagyjuk néhány pontját, mindegyik köréről legalább $q + 1 - 4 = q - 3$ -at. Ez egy $(q - 3)$ -szorosan lefogó $\mathcal{B}$ ponthalmazt jelent.

Emlékezzünk vissza, hogy deriválási eljárással (1.1.21.), a Möbius-síkból affin síkot nyerhetünk. Ehhez válasszuk a síknak egy $P \notin \mathcal{B}$ pontját. Vegyük észre, hogy ekkor a $\mathcal{B}$ ponthalmaz képe az affin síkon is $(q - 3)$ -szorosan lefogó, hiszen az affin sík minden egyenese egy P -n keresztüli körnek felelt meg a Möbius-síkon, és ezek mindegyikén legalább $q - 3$ pontja van $\mathcal{B}$ -nek.

Felhasználva az affin t -szeresen lefogó pontthalmazokra vonatkozó 1.3.20. eredményt, azt kapjuk, hogy

$$|\mathcal{B}| \geq (q-2)q - p^{e(t)},$$

tehát a Möbius-síkon legalább ennyi pontot kell elhagynunk, hogy a megfeleltetett pontok a kvádrikán $(k, 4)$ -ívet alkossanak. Azaz

$$k \leq q^2 + 1 - ((q-2)q - p^{e(t)}) = 2q + 1 + p^{e(t)}.$$

□

3.3.2. Megjegyzés. Vegyük észre, hogy egy, az $AG(2, q)$ affin síkon talált $(q-3)$ -szorosan lefogó pontthalmaz nem feltétlenül alkot a Möbius-síkon is $(q-3)$ -szorosan lefogó pontthalmazt. Hiszen csak a deriválás P centrumára illeszkedő körök jelennek meg az affin síkon, csak ezekről tudjuk biztosan, hogy a visszaemelés után $(q-3)$ -szorosan le lesznek fogva. És előfordulhat, hogy bármely visszaemelésnél a többi kör valamelyikére $(q-3)$ -nál kevesebb pontja kerül az affin lefogó pontthalmaz képének.

A másik fő irány a momentumgörbe kiegészítése volt, ennek pontjaihoz próbáltunk pontokat úgy hozzávenni, hogy azokkal ne keletkezzen 5-szelő sík. Mint azt korábban láttuk, $PG(3, q)$ -ban $q > 2$ esetén a $\mathcal{C}_3$ momentumgörbe maximális méretű $(k, 3)$ -ívet határoz meg, páratlan $q > 7$ esetén pedig minden maximális méretű $(k, 3)$ -ív projektív ekvivalens $\mathcal{C}_3$ -mal.

Ha egy $(k, 4)$ -ívből egyesével elvesszük a pontokat, akkor előbb-utóbb egy $(k', 3)$ -ívhez jutunk. Így ha visszafelé nézzük a folyamatot, akkor érdemes egy minél nagyobb $(k', 3)$ -ívet felvenni kezdésként, remélve, hogy elég nagy $(k, 4)$ -ívből tudunk úgy elvenni pontokat, hogy végül ehhez a pontthalmazhoz jussunk. Persze általában nem teljesül, hogy $(k, 4)$ -ívnek el lehet távolítani $k - (q+1)$ pontját úgy, hogy a megmaradtak $\mathcal{C}_3$ momentumgörbét alkossanak. Viszont a keresést nagyban gyorsította, sőt a $q \in \{5, 13, 17\}$ esetekben talált legalább akkora méretűt, mint más módszerekkel.

Érzékelhető, hogy a fentebbi módszerekkel viszonylag speciális típusú $(k, 4)$ -íveket tudunk csak találni, így, bár sokkal időigényesebb volt, ezek felhasználása nélkül is csináltam pár futtatást. Ezeknél az alkalmaknál is figyelembe vettem, hogy az ív mérete $3 \nmid q \geq 4$ esetén legfeljebb $2q+2$ lehet (tehát amint talált ekkorát, megszakítottam a programot), illetve mivel $q+4$ méretűnél nagyobbakat szerettünk volna találni, azt is kihasználtam, hogy minden pont hozzávételekor az eddigiek, és az általa meghatározott egyenesek pontjai kiszórhatók a potenciálisan még hozzávehető pontok halmazából.

A futtatások során talált legnagyobb $PG(3, q)$ -beli $(k, 4)$ -ívek méretét az alábbi táblázat mutatja, a talált ívek pontjainak koordinátái pedig a A. függelékben található. Megfigyelhető, hogy ahogy q értéke nő, egyre jobban eltér a talált legnagyobb méret a $2q+2$ határtól.

q	2q+2	Kvádrikán	$\mathcal{C}_3$ -mal	Speciális halmaz nélkül
5	12	10	12	12
7	16	13	13	14
11	24	15	16	18
13	28	16	18	17
17	36	19	21	20

3.4. Teljes $(12, 4)$ -ívek $PG(3, 5)$ -ben

A 3.2.9. állítás alapján tudjuk, hogy $m_4(3, 5) \leq 12$, és ahogy az a fentebbi táblázatban látható, találtunk is ekkora íveket. A kapott ívek vizsgálata során feltűnt, hogy mind-egyikre teljesül, hogy az ív minden egyes pontján pontosan 16 darab 4-szelő sík halad át. Ebből arra következtettünk, hogy valószínűleg valamilyen szabályos struktúrát alkotnak. Megpróbáltuk meghatározni ezt a struktúrát. Ehhez vizsgáltuk, hogy egy pontjából egy síkra vetítve hogy helyezkednek el egymáshoz képest a pontok.

Először is, vegyük észre, hogy a $P \in \Omega$ pontból az Π síkra vetítve minden $\mathcal{S}_i^P$ -beli sík képe egy olyan egyenes lesz, amelyre pontosan i darab Ω -beli pont képe illeszkedik. Jelöljük $\mathcal{E}_{i-1}$ -gyel az $(i-1)$ -szelő egyeneseket, vagyis $\mathcal{S}_i^P$ képhalmazát.

Ekkor a talált ív esetén, mivel $|\mathcal{E}_{i-1}| = |\mathcal{S}_i^P|$, $|\mathcal{E}_3| = |\mathcal{S}_4^P| = 16$, a 3.1. rész alapján kiszámolható, hogy $|\mathcal{E}_0| = |\mathcal{S}_1^P| = 4$, $|\mathcal{E}_1| = |\mathcal{S}_2^P| = 4$, $|\mathcal{E}_2| = |\mathcal{S}_3^P| = 7$. Ezek alapján a következőt mondhatjuk:

3.4.1. Állítás. *A pontok vetületeit $Q_1, Q_2, Q_3, Q_4, P_1, \dots, P_7$ -tel jelölve teljesül, hogy $|\mathcal{E}_1^{Q_i}| = 1$, $|\mathcal{E}_3^{Q_i}| = 5$ és $|\mathcal{E}_2^{P_i}| = 2$, $|\mathcal{E}_3^{P_i}| = 4$.*

Bizonyítás. Mivel $PG(2, 5)$ -ben az egy ponton átmenő 6 egyenes lefedi a teljes síkot (tehát mind a 11 vetített ívpontot is), ha vesszük a Q képpontot, akkor a

$$\sum_{i=1}^3 (i-1)|\mathcal{E}_i^Q| = |\mathcal{E}_2^Q| + 2|\mathcal{E}_3^Q| = 10, \text{ valamint az } |\mathcal{E}_1^Q| + |\mathcal{E}_2^Q| + |\mathcal{E}_3^Q| = 6$$

egyenlőségek segítségével könnyen kiszámolható, hogy kétféle típusú pontja van az ívünknek, amelyre $|\mathcal{E}_1^Q| = 1$, $|\mathcal{E}_3^Q| = 5$, illetve amelyre $|\mathcal{E}_2^Q| = 2$, $|\mathcal{E}_3^Q| = 4$.

Mivel $\sum_Q |\mathcal{E}_1^Q| = |\mathcal{E}_1| = 4$, az előbbiből pontosan négy, tehát az utóbbiból hét van. $\square$

3.4.2. Állítás. *A Q_1, Q_2, Q_3, Q_4 pontok általános helyzetűek.*

Bizonyítás. Indirekten tegyük fel, hogy a Q_1, Q_2, Q_3 pontok kollineárisak. Vegyük észre, hogy ekkor

$$\left| \bigcup_{i=1}^4 \mathcal{E}_3^{Q_i} \right| = \sum_{i=1}^4 |\mathcal{E}_3^{Q_i}| - 2|\mathcal{E}_3^{\{Q_1, Q_2, Q_3\}}| - \sum_{i=1}^3 |\mathcal{E}_3^{\{Q_i, Q_4\}}| = 4 \cdot 5 - 2 \cdot 1 - 3 = 15.$$

Ekkor, mivel Q_i -kon keresztül nincs 2-szelő, a $P_1P_2P_3$, P_1Q_1 , P_1Q_2 , P_1Q_3 egyenesek páronként különböző 3-szelők. Ugyanakkor P_1Q_4 is 3-szelő, tehát ez egybeesik valamelyik korábban felsorolt egyenessel. Feltehetjük, hogy a P_1, Q_1, Q_4 pontok a kollineárisak. Ugyanezt végiggondolhatjuk a P_2, P_3 pontokon áthaladó egyenesek esetében is, így megkapjuk, hogy a P_2, Q_2, Q_4 és a P_3, Q_3, Q_4 pontok is kollineárisak. Vegyük észre, hogy ezzel meghatároztuk az összes P_i, Q_j, Q_l ($j \neq l$) kollineáris ponthármaszt. Ugyanakkor az is világos lett, hogy a P_4, P_5, P_6, P_7 általános helyzetű pontok által meghatározott hat egyenes közül kettő a Q_4 -ben metszi egymást, tehát

$$\bigcup_{i=4}^7 \bigcup_{i \neq j=4}^7 |\mathcal{E}_3^{\{P_i, P_j\}}| \leq 4.$$

Azonban a P_4, P_5, P_6, P_7 pontokon áthaladó 3-szelőket számolva ellentmondásra jutunk:

$$\begin{aligned} 4 \cdot 4 &= \sum_{i=4}^7 |\mathcal{E}_3^{P_i}| = \sum_{l=1}^4 \sum_{j=1}^3 \sum_{i=4}^7 |\mathcal{E}_3^{\{P_i, P_j, Q_l\}}| + 2 \sum_{i=4}^6 \sum_{j>i}^7 |\mathcal{E}_3^{\{P_i, P_j\}}| \\ 16 &= \sum_{l=1}^3 \sum_{l \neq j=1}^3 \sum_{i=4}^7 |\mathcal{E}_3^{\{P_i, P_j, Q_l\}}| + 2 \sum_{i=4}^6 \sum_{j>i}^7 |\mathcal{E}_3^{\{P_i, P_j\}}| \leq 2 \cdot 3 + 2 \cdot 4 = 14. \end{aligned}$$

□

Ekkor, az előző állítás alapján

$$\left| \bigcup_{i=1}^4 \mathcal{E}_3^{Q_i} \right| = \sum_{i=1}^4 |\mathcal{E}_3^{Q_i}| - \sum_{i=1}^3 \sum_{j=i+1}^4 |\mathcal{E}_3^{\{Q_i, Q_j\}}| = 4 \cdot 5 - \binom{4}{2} = 14,$$

ami azt jelenti, hogy pontosan két olyan egyenes van a síkon, amelyen a P -típusú pontok száma három.

3.4.3. Állítás. *Ez a két egyenes öt képpontot fed le, tehát P -típusú pontban metszik egymást.*

Bizonyítás. Tegyük fel, hogy a két egyenes a P_1, P_2, P_3 és P_4, P_5, P_6 pontokat tartalmazza. Ekkor mind a négy, P_7 ponton áthaladó 3-szelőn van Q -típusú pont. Tehát azoknak a 3-szelőknek a száma, amik a P_7 és a Q -típusú pontok közül legalább kettőn átmennek, $\binom{4}{2} + 4 = 10$. Ugyanakkor, azoknak a 3-szelőknek a száma, amik a $P_1, \dots, P_6$ pontok közül tartalmaznak legalább kettőt, $3 \cdot 3 + 2 = 8$. Ezzel minden 3-szelőt pontosan egyszer megszámoltunk, amivel ellentmondásra jutottunk, hiszen $|\mathcal{E}_3| \neq 10 + 8$. □

Az általánosság megsértése nélkül feltehetjük, hogy a P_1 ponton átmenő egyenesek rendre a $\{Q_1, Q_2\}$, $\{Q_3, Q_4\}$, $\{P_2, P_3\}$, $\{P_4, P_5\}$, P_6 , P_7 pontokon mennek át.

3.4.4. Következmény. *A P_6, P_7 pontok 3-szelőin pontosan egy Q -típusú pont van. A P_2, P_3, P_4, P_5 pontok 3-szelői közül, egy a fentebb meghatározott P_1 -en áthaladó, a többi három között pedig pontosan egy olyan van, amely két Q -típusún halad át.*

Legyen $\mathcal{E}_0 = \{e_1, e_2, e_3, e_4\}$. Vegyük az $e_1, e_2 \in \mathcal{E}_0$ különböző egyeneseket, valamint legyen $A = e_1 \cap e_2$. Ekkor az A ponton keresztüli maradék négy egyenes megy át a 11 vetületpontra, mindegyik legfeljebb hármon. Ez csak úgy lehet, ha $|\mathcal{E}_0^A| = 2$, $|\mathcal{E}_2^A| = 1$, $|\mathcal{E}_3^A| = 3$, vagyis az elkerülő egyenesek általános helyzetűek.

Legyenek az elkerülő egyenesek metszéspontjai által meghatározott pontok az $A_1, A_2, B_1, B_2, C_1, C_2$, ahol az azonos betűvel jelölteknek nincs közös 0-szelőjük.

3.4.5. Állítás. *A_1A_2, B_1B_2, C_1C_2 "átlós" egyenesek közül pontosan kettő 3-szelő, a harmadik pedig 2-szelő.*

Bizonyítás. Vegyük észre, hogy a $A_1, A_2, B_1, B_2, C_1, C_2$ pontok bármely nem átlós 3-szelője az öt nem tartalmazó átlós egyeneseket vetületpontokban metszi, hiszen az elkerülő egyenesek három különböző pontban metszik a nem átlós és a nem 0-szelőket.

Tegyük fel, hogy mindegyik 3-szelő. Ekkor ezeken már ki van jelölve két-két pont, ami rajta van 0-szelőn, tehát nem lehet vetületpont. Ekkor az átlós egyenesek által meghatározott metszéspontok közül legalább kettő vetületpont (különben lenne olyan, amin a két metszéspont se, tehát összesen négy pontja nem vetületpont, így legfeljebb 2-szelő lehetne). Feltehetjük, hogy $A_1A_2 \cap C_1C_2 = A_3$, $B_1B_2 \cap C_1C_2 = B_3$ vetületpontok. Legyen a C_1C_2 harmadik vetületpontja C_3 , a harmadik nem vetületpontja pedig D . Mivel A_1, A_2, B_1, B_2 pontok nem átlós 3-szelői vetületpontban metszik C_1C_2 -t és az azonos betűjelűek különbözőben, ezért ezek 2-szelői mind a D ponton haladnak át.

Tehát arra jutottunk, hogy $|\mathcal{E}_2^D| = 4$, $|\mathcal{E}_3^D| = 1$, ezek összesen $2 \cdot 4 + 3 = 11$ vetületpontot fednek le, vagyis $|\mathcal{E}_0^D| = 1$. Ez viszont nem lehetséges, hiszen összesen négy 0-szelő van, és egyik sem megy át D -n a definíciója miatt. Tehát az átlós egyenesek között van 2-szelő.

Tegyük fel, hogy az A_1A_2 egy 2-szelő. Ekkor az A_1 -en átmenő három 3-szelő mindegyike a B_1B_2 és C_1C_2 egyeneseket vetületpontokban metszik, hiszen mindegyiket 3 különböző pontban metszik a 0-szelők, így B_1B_2, C_1C_2 egyeneseken van legalább 3 vetületpont. Ezzel beláttuk az állítást. $\square$

Konstruáljuk meg a vetületet a fentebbi jelöléseket használva. Feltehetjük, hogy $C_1 = (0 : 0 : 1)$, $C_2 = (0 : 1 : 0)$, $A_1 = (1 : 0 : 0)$, $A_2 = (1 : 1 : 1)$. Ebből $B_1 = (1 : 1 : 0)$, $B_2 = (1 : 0 : 1)$, valamint az A_1, A_2 pontok 3-szelőin lévő vetületpontok egyértelműek, ezek koordinátái: $(0 : 1 : 2)$, $(0 : 1 : 3)$, $(0 : 1 : 4)$, $(1 : 2 : 3)$, $(1 : 2 : 4)$, $(1 : 3 : 2)$, $(1 : 3 : 4)$, $(1 : 4 : 2)$, $(1 : 4 : 3)$. Ugyanakkor így megkaptuk az ezen az egyeneseken lévő nem vetületpontokat is, amik a 0-szelők pontjaival együtt a következők: $(0 : 0 : 1)$,

$(0 : 1 : 0), (0 : 1 : 1), (1 : 0 : 0), (1 : 0 : 1), (1 : 0 : 2), (1 : 0 : 3), (1 : 0 : 4), (1 : 1 : 0),$
 $(1 : 1 : 1), (1 : 1 : 2), (1 : 1 : 3), (1 : 1 : 4), (1 : 2 : 0), (1 : 2 : 1), (1 : 3 : 0), (1 : 3 : 1),$
 $(1 : 4 : 0), (1 : 4 : 1).$ Vegyük észre, hogy az $[1 : 1 : 2], [1 : 2 : 1], [1 : 2 : 3], [1 : 3 : 2]$
egyenesek minden pontjáról tudjuk, vetületpont-e, vagy sem, sőt mindegyik 1-szelő. Végül
vegyük észre, hogy a $[0 : 1 : 4]$ egyenesnek a $(0 : 1 : 1), (1 : 0 : 0), (1 : 1 : 1), (1 : 3 : 3)$
pontjairól tudjuk, hogy nem vetületpont, tehát az $(1 : 2 : 2), (1 : 4 : 4)$ pontjai biztosan
vetületpontok, hiszen ez az egyenes nem lehet sem 1-, sem 0-szelő, mert azokat már mind
ismerjük.

Tehát a $(12, 4)$ -ív bármely pontjából, egy azt elkerülő síkra vetítve a $Q_1 = (0 : 1 : 2),$
 $Q_2 = (0 : 1 : 3), Q_3 = (1 : 2 : 4), Q_4 = (1 : 4 : 2), P_1 = (0 : 1 : 4), P_2 = (1 : 2 : 3),$
 $P_3 = (1 : 3 : 2), P_4 = (1 : 3 : 4), P_5 = (1 : 4 : 3), P_6 = (1 : 2 : 2), P_7 = (1 : 4 : 4)$
ponthalmazzal projektív ekvivalens halmazt kapunk.

4. fejezet

Lineáris kódok és a véges projektív tér kapcsolata

Végül lássunk egy alkalmazást, miért is érdemes az általánosított ívek méretével és struktúrájával foglalkozni, külön figyelmet fordítva a $PG(3, q)$ -beli $(k, 4)$ -ívek esetére.

A kódelméleti fogalmak bevezetésénél itt eltérünk a szokásos jelölésektől, mivel azok egy részét már használtuk az előzőekben.

4.1. Lineáris kódok

Az algebrai kódelmélet egyik központi problémája, hogy hogyan lehet megbízhatóan továbbítani egy üzenetet olyan csatornán keresztül, amely zajos, tehát előfordulhat, hogy az üzenet torzul, mire célba ér, például rövidülhet, hozzáadódhatnak plusz karakterek, vagy a meglévők megváltozhatnak. Mi most azzal az esettel foglalkozunk, amikor csak az utóbbi történhet meg. Ennek kezelésére az üzenetet úgynevezett redundáns formában kódoljuk, vagyis kiegészítjük úgy, hogy az üzenet fogadója visszanyerhesse az esetleg sérülten érkezett üzenetből is a szükséges információkat.

Erre egy gyakori példa a számítógépeknél használt $0 - 1$ bináris kódok esetében az ún. *paritásellenőrző bit*, amely az üzenet végére illeszt egy 0 vagy 1 értékű bitet, aszerint, hogy az eredeti üzenetben páros, vagy páratlan darab 1 -es szerepelt.

Az üzenet feladója tehát egy m hosszúságú üzenetből kiindulva képez egy $m < n$ hosszúságú $\mathbf{w}$ üzenetet, amely az eredetinek egy valamilyen redundáns kódolása. Ez az üzenet a zajos csatornán átérve, torzított $\mathbf{w}' = \mathbf{w} + \mathbf{e}$ üzenetként érkezik meg. A küldő és a fogadó fél előzetesen megegyeznek abban, milyen kódolást használnak, így a fogadó ismeri az összes hibátlan üzenetet. A *dekódolás* során megkeresi azt a $\mathbf{w}''$ kódolt üzenetet, amelyből a legkevesebb módosítással kapható $\mathbf{w}'$, hiszen ez lesz a legvalószínűbb eredeti

üzenet. Ezt *minimális távolság szerinti dekódolásnak* nevezzük. Ha több ilyen $\mathbf{w}''$ kódszó is van, a dekódolást eredménytelennek tekintjük.

Vegyük az $\mathbb{F}_q$, q elemű véges test feletti k -dimenziós $\mathbb{F}_q^k$ vektorteret, majd tekintsük az *üzeneteket* a vektortér egy-egy elemének.

4.1.1. Definíció. Az $\mathbb{F}_q^k$ vektortér egy C részhalmazát *kódnak*, a részhalmazban elhelyezkedő vektorokat *kódszavaknak*, az k -t pedig a kód *hosszának* nevezzük.

Amennyiben a kiválasztott részhalmaz egy altere $\mathbb{F}_q^k$ -nak, C *lineáris kód*. Ekkor az alter dimenzióját a kód *dimenziójának* nevezzük.

Egy C kód *nem-degenerált*, ha $\nexists i$, amelyre $\forall \mathbf{v} \in C$ esetén $\mathbf{v}_i = 0$.

4.1.2. Definíció. Két kód *ekvivalens*, ha koordináták permutációjával megkapható egyik a másiból. Lineáris kódok esetén, egy koordináta nemnulla testelemmel való végigszorozása is ekvivalens kódot ad.

A továbbiakban csak lineáris kódokkal foglalkozunk.

A C lineáris kód az $\mathbb{F}_q^k$ egy m -dimenziós altere, így hozzárendelhetők valamilyen $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m$ bázisvektorok.

4.1.3. Definíció. A C lineáris kód $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m$ bázisvektoraiból, mint sorvektorokból alkotott $m \times k$ méretű $\mathbf{G}$ mátrixot a C kód *generátormátrixának* nevezzük.

Ekkor a kód kódszavainak halmaza $C = \{\mathbf{v} : \exists \mathbf{a} \in \mathbb{F}_q^m, \text{ melyre } \mathbf{v} = \mathbf{a}\mathbf{G}\}$.

4.1.4. Definíció. Legyen $\mathbf{v}, \mathbf{w} \in \mathbb{F}_q^k$ a vektortér két különböző eleme. A két vektor *Hamming-távolságán* az eltérő koordinátáik számát értjük:

$$d_H(\mathbf{v}, \mathbf{w}) = |\{i : \mathbf{v}_i \neq \mathbf{w}_i\}|.$$

4.1.5. Állítás. A *Hamming-távolság metrika* az $\mathbb{F}_q^k$ térben.

Az $(\mathbb{F}_q^k, d_H)$ metrikus teret *Hamming-térnek* nevezzük. Definiálhatjuk a $\mathbf{v}$ kódszó körüli t sugarú *Hamming-gömböt*:

$$B_t(\mathbf{v}) = \{\mathbf{w} \in C, \text{ melyre } d_H(\mathbf{v}, \mathbf{w}) \leq t\}.$$

4.1.6. Definíció. A C kód *minimális távolsága* az a d érték, amelyre igaz, hogy bármely két kódszó legalább d koordinátájában különbözik egymástól, vagyis

$$d = \min\{d_H(\mathbf{v}, \mathbf{w}) : \mathbf{v}, \mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}.$$

4.1.7. Definíció. Egy $\mathbf{v} \in \mathbb{F}_q^k$ vektor *súlya* a nemnulla koordinátáinak száma, tehát

$$w(\mathbf{v}) = d_H(\mathbf{v}, \mathbf{0}) = |\{i : \mathbf{v}_i \neq 0\}|.$$

4.1.8. Állítás. *Lineáris kódok esetén a minimális távolság a kódszavak minimális súlyával egyezik meg:*

$$d = \min\{w(\mathbf{v}) : \mathbf{v} \in C\}.$$

4.1.9. Definíció. Ha a C lineáris kód az $\mathbb{F}_q^k$ egy m -dimenziós altere, és d a minimális távolsága, akkor $[k, m, d]_q$ kódnak nevezzük.

A $\mathbf{v} = (v_1, \dots, v_k)$ és $\mathbf{w} = (w_1, \dots, w_k)$ vektorok skaláris szorzata legyen a szokásos módon

$$\langle \mathbf{v}, \mathbf{w} \rangle = \sum_{i=1}^k v_i w_i.$$

4.1.10. Definíció. A $C^\perp = \{\mathbf{x} \in \mathbb{F}_q^k : \langle \mathbf{x}, \mathbf{w} \rangle = 0 \ \forall \mathbf{w} \in C\}$ halmazt a C kód *duálisának*, a duális kód H generátormátrixát pedig a C kód *ellenőrző mátrixának* nevezzük.

Könnyen ellenőrizhető, hogy egy $[k, m, d]_q$ kód duálisa $[k, k - m, d']_q$ kód, alkalmas d' értékkel.

Világos, hogy a H sorai ortogonálisak a kódszavakra, vagyis a C kód megadható a következőképpen is: $C = \{\mathbf{v} \in \mathbb{F}_q^k : \mathbf{v}H^T = \mathbf{0}\}$.

Fontos észrevétel, hogy tetszőleges C lineáris kód esetén a H ellenőrző mátrixból ki tudjuk olvasni C minimális távolságát.

4.1.11. Állítás. *A C kód minimális távolsága pontosan akkor d , ha ellenőrző mátrixának bármely $(d - 1)$ oszlopa független, de van d olyan oszlop, amelyek lineárisan összefüggők.*

Ez amiatt teljesül, mert egy kód d súlyú vektora éppen d oszlopra ad meg lineáris összefüggést.

4.1.12. Tétel (Griesmer korlát). *Bármely $[k, m, d]_q$ kódra teljesül, hogy*

$$k \geq \sum_{i=0}^{m-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

4.1.13. Tétel (Singleton-korlát). *Ha C egy $[k, m, d]_q$ kód, akkor $d \leq k - m + 1$.*

Ez alapján látható, hogy adott hosszúságú kód esetén minél több kódszót szeretnénk, a minimális távolság annál kisebb kell, hogy legyen.

Ha a tételben egyenlőség teljesül, a C -t *MDS kódnak* nevezzük. Azonban nem minden k, m, q értékre létezik $[k, m, k - m + 1]_q$ kód, ezt később látni fogjuk.

MDS sejtés (Segre). *Ha $m \leq q$, akkor a $[k, m, k - m + 1]_q$ MDS kódoknak a hossza legfeljebb $q + 1$, az $m = 3$ és $m = q - 1$ kivételes esetektől eltekintve, amikor $q = 2^h$ esetén $q + 2$ lehet.*

A sejtést általános esetben még nem igazolták, azonban néhány plusz feltétel mellett már belátták, hogy teljesül. Ezek közül néhány:

4.1.14. Tétel. *Ha az alábbiak valamelyike fennáll, akkor a $[k, m, k - m + 1]_q$ MDS kód hosszára $k \leq q + 1$ teljesül.*

- $m < \frac{\sqrt{q}}{4}$, ha q páratlan; $m < \sqrt{q}$, ha q páros, [Segre, 1967]
- $m < \sqrt{pq}$, ahol $q = p^{2h+1}$, [Vloach, 1991]
- $m < \frac{\sqrt{q}}{2}$, ahol $q = p^{2h}$, $p > 5$ prím, [Hirschfeld–Korchmáros, 1996]
- $m < q$, ahol $q \neq 2$ prím, [Ball, 2010]
- $m < 2\sqrt{q}$, ahol $q = p^2$, p prím. [Ball–De Beule, 2011]

A minimális távolság szerinti dekódolás során, a kapott $\mathbf{w}'$ üzenet alapján a fogadó azt a $\mathbf{w}''$ kódszót választja a C halmazból, amelyre $d_H(\mathbf{w}', \mathbf{w}'')$ a lehető legkisebb, tehát a d érték, vagyis a kód minimális távolsága a kód hibajavító képességét jellemzi. Minél több helyen különböznek egymástól a kódszavak, annál több helyen kell a kódnak megváltoznia, hogy a vevő ne tudja biztosan felismerni az eredeti üzenetet. Ez jól mutatja az MDS kódok hasznosságát.

4.1.15. Definíció. Egy C kód t -hibadetektáló, ha $\forall \mathbf{w} \in C$ és $\forall \mathbf{e} \in \mathbb{F}_q^k$, ahol $0 < w(\mathbf{e}) \leq t$, teljesül, hogy $\mathbf{w} + \mathbf{e} \notin C$. Azaz ha a kapott $\mathbf{w}'$ üzenet legfeljebb t helyen tér el az eredetitől, akkor nem lehet kódszó.

4.1.16. Állítás. A $C [k, m, d]_q$ kód t -hibadetektáló pontosan akkor, ha $d \geq t + 1$.

4.1.17. Definíció. A C kód t -hibajavító, ha a minimális távolság szerinti dekódolás bármely kódszóban előforduló, legfeljebb t hiba esetén sikeres, az eredeti $\mathbf{w}$ üzenet visszanyerhető.

4.1.18. Állítás. Egy d minimális távolságú C kód legfeljebb $\lfloor \frac{d-1}{2} \rfloor$ hibát tud kijavítani. Pontosán akkor t -hibajavító, ha $d \geq 2t + 1$.

A t -hibajavító tulajdonságot úgy is megfogalmazhatjuk, hogy a kódszavak köré írt t sugarú gömbök diszjunktak.

4.1.19. Tétel (Hamming-korlát). *Ha a C (nem feltétlenül lineáris) kód t -hibajavító, akkor*

$$|C| \cdot \sum_{i=0}^t \binom{k}{i} (q-1)^i \leq q^k.$$

Ha C egy $[k, m, d]_q$ kód, akkor persze $|C| = q^m$.

4.1.20. Definíció. Egy kód *perfekt*, ha az előbbi tételben egyenlőség teljesül, vagyis bármely kódszó köré írt t sugarú Hamming-gömb nem tartalmaz más kódszót, illetve az összes gömb együttesen lefedi az $\mathbb{F}_q^k$ teret.

Tekintsük a lehető legegyszerűbb példát perfekt kódokra.

4.1.21. Definíció. A $[k, 1, k]_q$ *ismétlés-kód* az az egydimenziós lineáris kód, amit az $(1, 1, \dots, 1)$ vektor generál.

Az ismétlés-kód $\lfloor \frac{k}{2} \rfloor$ hibát képes javítani, és páratlan k esetén *perfekt*. Az ismétlés-kódokat, és az egy kódszóból álló kódokat *triviális kódoknak* nevezzük.

Most tekintsünk egy nemtriviális példát is perfekt kódokra.

4.1.22. Definíció. Legyen $k = \frac{q^m - 1}{q - 1}$. A $[k, k - m, d]_q$ *Hamming-kód* olyan kód, amelynek ellenőrző mátrixának oszlopai az $\mathbb{F}_q^m$ tér azon nemnulla vektorai, amelyek nem skalárszorosai egymásnak.

Tehát az ellenőrző mátrixának oszlopai megfeleltethetők a $PG(m - 1, q)$ projektív tér pontjainak.

A legegyszerűbb példa a $q = 2, m = 3$. Ekkor a $[7, 4, d]_2$ Hamming-kód ellenőrző mátrixa:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

A 4.1.11. állítás segítségével megfigyelhető, hogy a Hamming-kódok 3 minimális súlyúak ($d=3$), így 1-hibajavítók, továbbá ellenőrizhető, hogy *perfekt* kódok.

4.1.23. Állítás. *Nem létezik nemtriviális, bináris, 2-hibajavító perfekt kód.*

A lineáris perfekt kódok teljes osztályozása ismert, az alábbiakban felsoroljuk az összes további ilyen kódot.

Az $\mathbb{F}_2$ test felett az $x^{23} - 1$ polinom három irreducibilis tényező szorzatára bontható:

$$x^{23} - 1 = (x - 1)p(x)q(x),$$

ahol

$$p(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1, \quad q(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1.$$

4.1.24. Definíció. A fenti 11 fokú polinomok bármelyikének legfeljebb 22 fokú többszörösei egy $[23, 12, 7]_2$ kódot alkotnak, a *bináris Golay-kódot*, amit G_{23} -mal jelölünk.

Legyen S_5 az az 5×5 -ös mátrix, amelynek i, j elemét a Legendre-szimbólummal definiáljuk:

$$(S_5)_{i,j} = \left(\frac{i-j}{5} \right), \quad \text{azaz} \quad S = \begin{bmatrix} 0 & 1 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ -1 & 1 & 0 & 1 & -1 \\ -1 & -1 & 1 & 0 & 1 \\ 1 & -1 & -1 & 1 & 0 \end{bmatrix}.$$

Erre teljesül, hogy $S_5 S_5^T = 5I_5 - J_5$, ahol J_n az $n \times n$ -es csupa 1-es mátrix.

Legyen

$$G_{11} = \left[I_6 \left| \begin{array}{ccc} 1 & \cdots & 1 \\ S_5 & & \end{array} \right. \right].$$

4.1.25. Definíció. A G_{11} generátormátrixú $[11, 6, 5]_3$ lineáris kódot *ternér Golay-kódnak* nevezzük és $\mathcal{G}_{11}$ -gyel jelöljük.

A $\mathcal{G}_{23}$ és $\mathcal{G}_{11}$ kódokról belátható, hogy rendre 3- és 2-hibajavító perfekt kódok.

4.1.26. Tétel (Tietäväinen, van Lint). *Nem triviális lineáris perfekt kód, amely legalább két hibát javít csak a bináris vagy ternér Golay-kód lehet.*

A 4.1.19. korlát gömbös átfogalmazásából jól látszik, hogy a perfekt kódok a lehető legjobb kódok, azonban sajnos ezekből kevés van, főleg, ha az is igény, hogy legalább 2-hibajavító is legyen, ezért érdemes más szempontok alapján "jó"-nak ítélt kódokat használni, például a már említett maximális értékű minimális súlyú *MDS* kódokat.

4.2. Lineáris kódok és az általánosított ívek kapcsolata

Vegyük az $\mathbb{F}_q$, q elemű véges test feletti k -dimenziós $\mathbb{F}_q^k$ vektorteret. Legyenek a C lineáris, nem-degenerált $[k, n+1, d]_q$ kód bázisvektorai, tehát a kód $\mathbf{G}$ generátormátrixának sorai $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{n+1}$.

Legyenek az $\mathbf{u}_i$ ($i \in \{1, 2, \dots, k\}$) vektorok a $\mathbf{G}$ mátrix $(n+1)$ -dimenziós oszlopvektorai, tehát:

$$(\mathbf{u}_i)_j = (\mathbf{v}_j)_i.$$

Ekkor, mivel $\forall \mathbf{a} \in \mathbb{F}_q^{n+1}$ vektorra $\mathbf{a}\mathbf{G} = \sum_{j=1}^{n+1} a_j \mathbf{v}_j \in C$ súlya legalább d , azaz legfeljebb $(k-d)$ koordinátája nulla, $\forall i \in \{1, 2, \dots, k\}$ -ra az alábbi egyenletnek legfeljebb $(k-d)$ megoldása lehet:

$$\sum_{j=1}^{n+1} a_j (\mathbf{v}_j)_i = 0.$$

Tehát a $\sum_{j=1}^{n+1} a_j(\mathbf{u}_i)_j = 0$ egyenletnek legfeljebb $(k-d)$ megoldása lesz.

Az 1.1. részben láttuk alapján az $\mathbf{u}_i$ vektorokat tekinthetjük, mint a $PG(n, q)$ projektív tér egy-egy pontját, és $\forall \mathbf{a} \in \mathbb{F}_q^{n+1}$ vektorra a $\sum_{j=1}^{n+1} a_j \mathbf{x}_j = 0$ egyenleteket pedig mint a hipersíkjaikat. Ekkor a fenti észrevételek alapján az $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k$ vektorok által meghatározott pontok közül bármely hipersíkon legfeljebb $(k-d)$ helyezkedik el, vagyis egy $(k, k-d)$ -ívet definiálnak a $PG(n, q)$ térben.

4.2.1. Állítás. *Egy $PG(n, q)$ -beli (k, r) -ív ekvivalens egy lineáris $[k, n+1, k-r]_q$ kóddal, amely generátormátrixának bármely két $\mathbf{u}_i \neq \mathbf{u}_j$ ($i \neq j$) oszlopa lineárisan független, vagyis $\langle \mathbf{u}_i \rangle \neq \langle \mathbf{u}_j \rangle$.*

Tehát, ha van egy nagy méretű teljes (k, r) -ívünk $PG(n, q)$ -ban, akkor egyúttal van egy n hosszú kódunk, amiben sok, pontosabban q^k darab kódszó van, és a minimális távolsága $k-r$. Az állításból adódóan az általánosított ívekre kapott eredmények kódelméleti eredményeket adnak, és ugyanígy, ha van egy kódelméleti eredményünk, az az ívekre lefordítva is teljesülni fog.

4.2.2. Megjegyzés. Az MDS-kódok pont a $PG(n, q)$ -beli (k, n) -íveknek felelnek meg, hiszen ezek az ívek a $[k, n+1, k-n]_q$ -kódokkal ekvivalensek, amik így $m = n+1$, $d = k-n$ értékeket behelyettesítve, egyenlőséggel teljesítik a Singleton-korlátot.

A megfigyelésből látszik, hogy adott q , k és m értékekre pontosan akkor létezik $[k, m, k-m+1]_q$ MDS kód, ha $n = m-1$ -re $PG(n, q)$ -ban létezik (k, n) -ív.

Vegyük észre, hogy a 4.1.14. eredmények alapján a következő korlátot kapjuk (k, n) -ívek méretére vonatkozóan.

4.2.3. Állítás. *Ha az alábbiak valamelyike fennáll, akkor a $PG(n, q)$ térben a (k, n) -ívek méretére $k \leq q+1$ teljesül.*

- $n < \frac{\sqrt{q}}{4} - 1$, ha q páratlan; $n < \sqrt{q} - 1$, ha q páros,
- $n < \sqrt{pq} - 1$, ahol $q = p^{2h+1}$,
- $n < \frac{\sqrt{q}}{2} - 1$, ahol $q = p^{2h}$, $p > 5$ prím,
- $n < q - 1$, ahol $q \neq 2$ prím,
- $n < 2\sqrt{q} - 1$, ahol $q = p^2$, p prím.

Jegyezzük meg, hogy az MDS sejtést (4.1.) Segre eredetileg ívekre fogalmazta meg, ezt már kimondtuk a 2.3. részben is.

A 4.2.1. megfeleltetéssel, és a Griesmer korlát (4.1.12.) felhasználásával megkapható, hogy a $PG(n, q)$ -beli (k, r) ívekre teljesül, hogy

$$k \geq \sum_{i=0}^n \left\lceil \frac{k-r}{q^i} \right\rceil.$$

Feltéve, hogy $(r-n)q + r < k$, a 2.2.12. állítás szerint $k-r \leq q^2$ is teljesül, így

$$k \geq k-r + \left\lceil \frac{k-r}{q} \right\rceil + n-1,$$

amiből következik, hogy

$$k \leq (r-n+1)q + r,$$

amit a 2.2.1. állításban is láttunk már.

Végül a ([4]) cikk mintájára, most tekintsünk egy $PG(3, q)$ -beli $(k, 4)$ -ívek méretéből következő kódelméleti állítást.

4.2.4. Állítás. *Ha $3 \nmid q \geq 4$ vagy $3^h = q \geq 36$, $k-d = n+1$, akkor a $[k, n+1, d]_q$ kódra $q < d$ esetén teljesül, hogy*

$$d + \left\lceil \frac{d}{q-1} \right\rceil + \sum_{i=2}^n \left\lceil \frac{d}{q^i} \right\rceil \leq k. \quad (4.1)$$

Bizonyítás. Legyen $r = n+1$. Ekkor a $PG(n, q)$ -beli (k, r) -ívekre a 2.2.12. állítás alapján $k-r \leq q^2$ teljesül, mivel $q < d$, és így $(r-n)q + r < k$.

A 3.2.13. következmény alapján, a $PG(n, q)$ -beli (k, r) -ívekre, ahol $3^h = q \geq 36$ vagy $3 \nmid q \geq 4$ teljesül, az ív mérete

$$k \leq 2q + n - 1.$$

Ez az $r-n+1 = 2$, $r = k-d$ behelyettesítésekkel és némi átrendezéssel a következő alakra hozható:

$$d + (n-1)(q-1) \leq (k-d)(q-1).$$

Ha ezt $(q-1)$ -gyel végigosztjuk, átrendezzük, és használjuk, hogy $d = k-r \leq q^2$:

$$d + \frac{d}{q-1} + \sum_{i=2}^n \left\lceil \frac{d}{q^i} \right\rceil = d + \frac{d}{q-1} + n-1 \leq k,$$

valamint észrevevessük, hogy egész számok közötti egyenlőtlenséget vizsgálunk, megkapjuk, hogy bármely $[k, n+1, d]_q$ kódra, ahol $d = k - (n+1)$ és a generátormátrixában nincs két azonos oszlop, teljesül a (4.1) azonosság.

Ha a $[k, n+1, d]_q$ kód minimális távolsága $d = k - (n+1)$, és a generátormátrixában van két azonos oszlop, akkor feltehetjük, hogy az első két oszlopvektor az $(1, 0, \dots, 0)^T$. Ekkor az első sort és ezt a két oszlopot törölve, egy $[k-2, n, d]_q$ kód generátormátrixát kapjuk, ami így teljesíti a Griesmer korlátból adódó egyenlőtlenséget:

$$k-2 \geq \sum_{i=0}^{n-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

Erre használva, hogy $k-r \leq q^2 < q^n$ ($n > 2$), illetve hogy $\left\lceil \frac{d}{q} \right\rceil + 1 \geq \left\lceil \frac{d}{q-1} \right\rceil$, ismét a (4.1) azonossághoz jutunk. $\square$

4.2.5. *Megjegyzés.* A $PG(n, q)$ -beli $(k, n+1)$ -íveknek megfelelő $[k, n+1, d]_q$ kódok $(\frac{k-n}{2})$ -hibajavítók, és $(k-n)$ -hibadetektálók.

4.2.6. *Megjegyzés.* Ha a $[k, n+1, d]_q$ kódra $d = k - n - 1$ helyett $d = k - n$ teljesülne, *MDS* kód lenne, tehát a $PG(n, q)$ -beli $(k, n+1)$ -ívekből, tehát speciálisan a $PG(3, q)$ -beli $(k, 4)$ -ívekből kapott lineáris kódok csak eggyel térnek el ezektől a maximális értékű minimális súllyal rendelkező kódoktól.

Irodalomjegyzék

- [1] S. Ball. “On Nuclei and Blocking Sets in Desarguesian Spaces”. *Journal of Combinatorial Theory, Series A* 85.2 (1999), 232–236. old. DOI: <https://doi.org/10.1006/jcta.1998.2903>. URL: <https://www.sciencedirect.com/science/article/pii/S009731659892903X>.
- [2] S. Ball és J. De Beule. “On sets of vectors of a finite vector space in which every subset of basis size is a basis Π^* ”. *Designs, Codes and Cryptography* 65.1 (2012), 5–14. old.
- [3] S. Ball, A. Blokhuis és F. Mazzocca. “Maximal arcs in desarguesian planes of odd order do not exist”. *Combinatorica* 17 (1997), 31–41. old. DOI: <https://doi.org/10.1007/BF01196129>.
- [4] S. Ball és J.W.P. Hirschfeld. “Bounds on (n, r) -arcs and their application to linear codes”. *Finite Fields and Their Applications* 11.3 (2005). Ten Year Anniversary Edition!, 326–336. old. DOI: <https://doi.org/10.1016/j.ffa.2005.04.002>. URL: <https://www.sciencedirect.com/science/article/pii/S1071579705000250>.
- [5] D. Bartoli és tsai. “On planes through points off the twisted cubic in $PG(3, q)$ and multiple covering codes”. *Finite Fields Appl.* 67 (2020).
- [6] A. Blokhuis, Sziklai P. és Szőnyi T. “Blocking sets in projective spaces”. *Current Research Topics in Galois Geometry, Mathematics Research Developments* (2011), 63–86. old.
- [7] M. Braun, A. Kohnert és A. Wassermann. “Construction of (n, r) -arcs in $PG(2, q)$ ”. *Innovations in Incidence Geometry: Algebraic, Topological and Combinatorial* 1.1 (2005), 133–141. old.
- [8] L.R.A Casse és D.G Glynn. “On the uniqueness of $(q + 1)_4$ -arcs of $PG(4, q)$, $q = 2^h$, $h \geq 3$ ”. *Discrete Mathematics* 48.2 (1984), 173–186. old. DOI: [https://doi.org/10.1016/0012-365X\(84\)90180-8](https://doi.org/10.1016/0012-365X(84)90180-8). URL: <https://www.sciencedirect.com/science/article/pii/0012365X84901808>.

- [9] L.R.A Casse és D.G Glynn. “The solution to Beniamino Segre’s problem $I_{r,q}$, $r = 3$, $q = 2^h$ ”. *Geometriae Dedicata* 13 (1982), 157–163. old. DOI: 10.1007/BF00147659.
- [10] A. Davydov, S. Marcugini és F. Pambianco. “Orbits of Lines for a Twisted Cubic in $PG(3, q)$ ”. *Mediterranean Journal of Mathematics* 20 (2023). DOI: 10.1007/s00009-023-02279-4.
- [11] Kiss Gy. és Szőnyi T. *Finite Geometries*. 2019. DOI: 10.1201/9781315120072.
- [12] Kiss Gy. és Szőnyi T. *Véges geometriák*. Polygon, Szeged, 2001.
- [13] F. Pavese. “On 4-general sets in finite projective spaces”. *Journal of Algebraic Combinatorics* 61 (2025). DOI: 10.1007/s10801-025-01383-w.
- [14] L. Storme és J.A. Thas. “Complete k -arcs in $PG(n, q)$, q even”. *Discrete Mathematics* 106-107 (1992), 455–469. old. DOI: [https://doi.org/10.1016/0012-365X\(92\)90576-2](https://doi.org/10.1016/0012-365X(92)90576-2). URL: <https://www.sciencedirect.com/science/article/pii/0012365X92905762>.
- [15] G. Tallini. “On caps of kind s in a Galois r -dimensional space”. *Acta Arithmetica* 7 (1961), 19–28. old. URL: <https://api.semanticscholar.org/CorpusID:117018322>.
- [16] Weiner Zs. “On (k, p^e) -arcs in Desarguesian planes”. *Finite Fields and Their Applications* 10.3 (2004), 390–404. old. DOI: <https://doi.org/10.1016/j.ffa.2003.09.007>. URL: <https://www.sciencedirect.com/science/article/pii/S1071579704000048>.

A. függelék

$PG(3, q)$ -ban talált $(k, 4)$ -ívek

A.1. táblázat: $(k, 4)$ -ívek $PG(3, q)$ térbeli elliptikus kvádrikán

q	k	A $(k, 4)$ -ív pontjai
5	10	(1: 1: 0: 3), (1: 3: 0: 0), (0: 1: 1: 3), (1: 1: 1: 4), (0: 1: 4: 3), (1: 1: 0: 2), (1: 0: 4: 2), (0: 1: 4: 2), (1: 4: 1: 4), (0: 1: 2: 0)
7	13	(1: 6: 3: 6), (1: 1: 3: 6), (1: 4: 6: 6), (1: 0: 6: 2), (0: 0: 1: 3), (0: 0: 1: 4), (0: 1: 0: 3), (0: 1: 0: 4), (1: 0: 0: 3), (1: 1: 0: 2), (1: 2: 2: 2), (1: 4: 1: 6), (1: 5: 5: 2)
11	15	(1: 8: 4: 6), (1: 7: 5: 9), (1: 0: 0: 3), (1: 1: 5: 1), (0: 0: 1: 3), (0: 0: 1: 8), (0: 1: 0: 3), (0: 1: 0: 8), (1: 0: 0: 8), (1: 1: 1: 4), (1: 2: 2: 9), (1: 2: 9: 9), (1: 3: 1: 0), (1: 3: 10: 0), (1: 8: 2: 7)
13	16	(1: 10: 6: 5), (1: 4: 11: 6), (1: 10: 12: 2), (1: 2: 9: 6), (1: 4: 2: 6), (1: 10: 12: 11), (1: 3: 3: 12), (1: 1: 3: 11), (1: 10: 7: 8), (1: 11: 1: 1), (1: 3: 6: 5), (0: 1: 8: 0), (1: 0: 8: 0), (1: 6: 3: 5), (1: 0: 6: 2), (1: 1: 11: 1)
17	19	(1: 7: 1: 0), (1: 3: 16: 3), (1: 3: 6: 13), (1: 7: 15: 2), (0: 1: 2: 1), (0: 1: 2: 16), (0: 1: 3: 6), (0: 1: 3: 11), (1: 0: 2: 1), (1: 0: 2: 16), (1: 0: 3: 11), (1: 0: 4: 0), (1: 1: 1: 2), (1: 1: 2: 5), (1: 1: 14: 3), (1: 1: 16: 2), (1: 2: 10: 2), (1: 3: 15: 9), (1: 8: 7: 13)

A.2. táblázat: $(k, 4)$ -ívek $PG(3, q)$ térbeli $\mathcal{C}_3$ kiegészítésével

q	k	A $(k, 4)$ -ív pontjai
5	12	(0: 0: 0: 1), (1: 0: 0: 0), (1: 1: 1: 1), (1: 2: 4: 3), (1: 3: 4: 2), (1: 4: 1: 4), (0: 1: 2: 1), (1: 3: 3: 0), (1: 1: 3: 2), (0: 1: 4: 4), (1: 4: 0: 0), (0: 1: 0: 2)
7	13	(0: 0: 0: 1), (1: 0: 0: 0), (1: 1: 1: 1), (1: 2: 4: 1), (1: 3: 2: 6), (1: 4: 2: 1), (1: 5: 4: 6), (1: 6: 1: 6), (1: 3: 5: 2), (1: 2: 5: 6), (0: 1: 3: 3), (1: 0: 6: 5), (1: 2: 0: 0)
11	16	(0: 0: 0: 1), (1: 0: 0: 0), (1: 1: 1: 1), (1: 2: 4: 8), (1: 3: 9: 5), (1: 4: 5: 9), (1: 5: 3: 4), (1: 6: 3: 7), (1: 7: 5: 2), (1: 8: 9: 6), (1: 9: 4: 3), (1: 10: 1: 10), (1: 9: 9: 0), (1: 1: 5: 4), (1: 9: 3: 9), (0: 1: 9: 2)
13	18	(0: 0: 0: 1), (1: 0: 0: 0), (1: 1: 1: 1), (1: 2: 4: 8), (1: 3: 9: 1), (1: 4: 3: 12), (1: 5: 12: 8), (1: 6: 10: 8), (1: 7: 10: 5), (1: 8: 12: 5), (1: 9: 3: 1), (1: 10: 9: 12), (1: 11: 4: 5), (1: 12: 1: 12), (1: 5: 1: 7), (1: 1: 10: 6), (1: 0: 12: 8), (1: 2: 9: 4)
17	21	(0: 0: 0: 1), (1: 0: 0: 0), (1: 1: 1: 1), (1: 2: 4: 8), (1: 3: 9: 10), (1: 4: 16: 13), (1: 5: 8: 6), (1: 6: 2: 12), (1: 7: 15: 3), (1: 8: 13: 2), (1: 9: 13: 15), (1: 10: 15: 14), (1: 11: 2: 5), (1: 12: 8: 11), (1: 13: 16: 4), (1: 14: 9: 7), (1: 15: 4: 9), (1: 16: 1: 16), (1: 12: 10: 2), (0: 1: 9: 15), (1: 14: 11: 2)

A.3. táblázat: $(k, 4)$ -ívek $PG(3, q)$ térben, speciális ponthalmaz nélkül

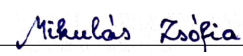
q	k	A $(k, 4)$ -ív pontjai
5	12	(1: 1: 0: 3), (1: 3: 0: 0), (0: 1: 1: 3), (1: 1: 1: 4), (0: 1: 4: 3), (1: 1: 0: 2), (1: 0: 4: 2), (0: 1: 4: 2), (1: 4: 1: 4), (0: 1: 2: 0), (1: 1: 2: 3), (1: 0: 0: 4)
7	14	(0: 1: 1: 3), (0: 1: 4: 3), (1: 0: 0: 0), (1: 0: 1: 0), (1: 0: 2: 5), (1: 0: 3: 5), (1: 1: 2: 6), (1: 2: 1: 5), (1: 2: 2: 1), (1: 2: 2: 3), (1: 2: 4: 2), (1: 4: 0: 2), (1: 4: 0: 6), (1: 4: 6: 4)
11	18	(1: 5: 5: 6), (1: 1: 10: 8), (1: 7: 6: 10), (1: 5: 1: 7), (1: 6: 10: 2), (1: 4: 6: 9), (1: 10: 8: 6), (1: 7: 5: 1), (1: 10: 3: 6), (1: 8: 4: 8), (1: 1: 3: 1), (1: 3: 6: 7), (1: 3: 4: 6), (1: 1: 10: 3), (1: 2: 7: 2), (1: 8: 3: 7), (1: 5: 10: 7), (1: 5: 6: 5)
13	17	(1: 12: 9: 1), (1: 7: 12: 0), (1: 1: 9: 0), (1: 5: 7: 4), (1: 5: 6: 7), (1: 1: 12: 2), (1: 0: 1: 4), (1: 9: 3: 4), (1: 2: 7: 4), (1: 12: 8: 11), (0: 1: 5: 7), (1: 1: 7: 5), (1: 9: 9: 10), (1: 4: 10: 7), (1: 1: 5: 0), (1: 8: 1: 11), (1: 8: 9: 2)
17	20	(1: 6: 16: 8), (1: 11: 10: 16), (1: 8: 5: 11), (1: 14: 0: 2), (1: 10: 1: 14), (1: 14: 13: 4), (1: 9: 10: 14), (1: 1: 16: 1), (0: 1: 16: 1), (1: 3: 6: 6), (1: 7: 3: 7), (0: 1: 6: 6), (1: 15: 5: 7), (1: 0: 9: 6), (1: 13: 0: 5), (1: 10: 0: 1), (1: 1: 7: 13), (1: 10: 12: 5), (1: 5: 4: 3), (1: 14: 11: 1)

Alulírott Mikulás Zsófia nyilatkozom, hogy szakdolgozatom elkészítése során az alább felsorolt feladatok elvégzésére a megadott MI alapú eszközöket alkalmaztam:

Feladat	Felhasznált eszköz	Felhasználás helye	Megjegyzés
Táblázat készítése	GPT-4o	3.3. alfejezet, Függelék, MI nyilatkozat	
LaTeX-kódolási kérdések	GPT-4o	Teljes dolgozat	Matematikai jelölések megfelelő megjelenítése
Python-kódolási kérdések	Claude 3.5 Sonnet	3.3. alfejezet, Függelék	Kód javítása, megfelelő parancsok megtalálása

A felsoroltakon túl más MI alapú eszközt nem használtam.

Budapest, 2025. június 1.


Aláírás