Eötvös Loránd Tudományegyetem
Természettudományi Kar

Blázsik Zoltán

Lefogó ponthalmazok véges projektív terekben

Szakdolgozat

Matematikus MSc

Témavezető: Szőnyi Tamás, D.Sc.
Számítógéptudományi Tanszék

Budapest, 2014

Köszönetnyilvánítás

Ezúton szeretném megköszönni *Szőnyi Tamás* tanár úrnak az izgalmas közös gondolkozásokat, a problémafelvetést, valamint az építő megjegyzéseket és tanácsokat, amelyekkel jelentősen hozzájárult a szakdolgozat elkészítéséhez. Köszönöm szépen, hogy rendelkezésemre bocsátott számos cikket, és felhívta a figyelmemet több háttérinformációra, összefüggésre is, amelyek által nagyobb és pontosabb rálátásom lett a vizsgált kérdésekre. Nagyon hálás vagyok neki és *Kiss György* tanár úrnak amiatt is, hogy az egyetemi véges geometriával kapcsolatos órák keretén belül megismertették velem ezt a szép és érdekes ágát a matematikának.

Továbbá köszönöm a remek hangulatú véges geometria szeminárium minden előadójának és résztvevőjének a számomra új témákat és ötleteket, amelyekkel tovább bővítették az ismereteimet.

Végül szeretném megköszönni családomnak, menyasszonyomnak és barátaimnak, hogy szeretetükkel és türelmükkel segítettek és bátorítottak a szakdolgozat elkészítése és az egyetemi tanulmányaim teljes ideje alatt.

Tartalomjegyzék

Bevezetés

A véges geometriának a lefogó ponthalmazokkal foglalkozó része kifejezetten érdekes, igen sokat vizsgált terület, amelyben mégis szép számmal akadnak még megoldatlan, alapvető fontosságú kérdések is. A lefogó ponthalmazokra vonatkozó eredményeket, konstrukciókat és bizonyítási technikákat a matematika egyéb területein – mint például kódelméletben, gráfelméletben – is sikerrel lehet alkalmazni. A szakdolgozatom célja az, hogy a lefogó ponthalmazokkal kapcsolatos eddig ismert módszereket összefoglaljuk és mutassunk ezekre alkalmazásokat.

A szakdolgozat első fejezetében megismerkedünk a véges geometria alapvető fogalmaival, és bemutatunk néhány fontos eredményt, amiket a későbbiekben is használni fogunk majd. A második fejezetben a rengetegszer használható leszámlálási ötleteket (és ezek következményeit) mutatjuk be, majd az algebrát hívjuk segítségül és a Rédei-polinommal ismerkedünk meg, ami megkönnyíti a lefogó ponthalmaz illeszkedési struktúrájának leírását. A harmadik fejezetben kitekintünk magasabb dimenziós eredmények felé, és megemlítjük még a [4] cikkben használt levetítős módszert is.

Végül az utolsó fejezetben a [3] cikk eredményeit fogjuk q nem négyzet esetben ugyanazzal a gondolatmenettel bebizonyítani.

1. Véges geometriai alapok

A további szakaszokban a véges geometriának számos fogalmát és az ezek közötti összefüggéseket tárgyaljuk majd, ezért most definiálni fogjuk ezen objektumokat és néhány alapvető észrevételt is beidézünk. Ebben a részben az [1]-es könyvre fogunk támaszkodni. A zárójelben szereplő szám pedig mindig az [1]-es könyvbeli helyet jelöli. Az idézett állítások többségét bizonyítás nélkül közöljük majd, amennyiben az állítás vagy a bizonyítása kifejezetten fontos számunkra, akkor a bizonyítást is leírjuk, néha pedig rövid magyarázatot fogunk adni.

1.1. Definíció (1.1.) A $\Pi = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ hármast, ahol $\mathcal{P}$ és $\mathcal{L}$ két diszjunkt halmaz, $\mathrm{I} \subseteq \mathcal{P} \times \mathcal{L}$ pedig egy illeszkedésnek nevezett reláció, *projektív síknak* nevezünk, ha kielégíti a következő négy axiómát:

P1. $\mathcal{P}$ bármely két különböző eleméhez pontosan egy olyan eleme van $\mathcal{L}$-nek, amely mindkettővel relációban áll.

P2. $\mathcal{L}$ bármely két különböző eleméhez pontosan egy olyan eleme van $\mathcal{P}$-nek, amely mindkettővel relációban áll.

P3. $\mathcal{L}$ minden eleme legalább három különböző $\mathcal{P}$-beli elemmel áll relációban.

P4. $\mathcal{P}$ minden eleme legalább három különböző $\mathcal{L}$-beli elemmel áll relációban.

A továbbiakban a fenti absztrakt $\mathcal{P}$ és $\mathcal{L}$ helyett rendre a geometriából származó *pontok* és *egyenesek* fogalmát fogjuk használni.

1.2. Definíció (1.5.) A $\Pi' = (\mathcal{P}', \mathcal{L}', \mathrm{I}')$ projektív sík a $\Pi = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ projektív síknak *részsíkja*, ha $\mathcal{P}' \subseteq \mathcal{P}$, $\mathcal{L}' \subseteq \mathcal{L}$, és I' a $\mathcal{P}' \times \mathcal{L}'$ halmazon megegyezik I-vel (vagyis egy részsíkbeli pont pontosan akkor illeszkedik egy részsíkbeli egyenesre, ha az eredeti síkon is illeszkednek).

1.3. Tétel (1.7.) Ha a Π projektív síknak van olyan egyenese, amelyre pontosan $n+1$ pont illeszkedik, akkor

1. Π minden egyenesén $n + 1$ pont van,
2. Π minden pontján $n + 1$ egyenes halad keresztül,
3. Π összesen $n^2 + n + 1$ pontot és ugyanennyi egyenest tartalmaz.

Ez a megfigyelés könnyen adódik az axiómákból, ugyanakkor ez biztosítja a következő fogalom jóldefiniáltságát.

1.4. Definíció (1.8.) A Π *projektív sík rendje n*, ha Π-nek van olyan egyenese, amelyen $n+1$ pont van.

Az eddigiekben a projektív síkokat definiáltuk, azonban a későbbi fejezetekben magasabb dimenziós projektív tereket is használunk majd, így most ezek precíz definíciója következik.

1.5. Definíció (4.1.) Legyen S véges halmaz, amelynek adott néhány kitüntetett részhalmaza, melyek mindegyikéhez hozzá van rendelve egy $-1 \leq d \leq n$ egész szám. Az S halmazt n-dimenziós *véges projektív térnek*, a kitüntetett részhalmazokat pedig S *d-dimenziós altereinek* nevezzük, ha ezek a részhamazok kielégítik a következő axiómákat:

1. Minden $-1 \leq d \leq n$ egész szám esetén létezik legalább egy d-dimenziós altér, továbbá
   - egyértelműen létezik (-1)-dimenziós altér, az $\emptyset$;
   - egyértelműen létezik n-dimenziós altér, S;
   - a 0-dimenziós alterek megegyeznek S egyelemű részhalmazaival.
2. Ha egy r-dimenziós altér része egy s-dimenziós altérnek, akkor $r \leq s$, és ha $r = s$, akkor a két altér megegyezik.
3. Alterek metszete altér.
4. Ha valamely r-dimenziós altér és egy s-dimenziós altér metszete m-dimenziós altér, a mindkettőt tartalmazó összes altér metszete pedig t-dimenziós altér, 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.

Természetesen ugyanúgy, ahogy az 1.2 után is megjegyeztük, az absztrakt projektív tér esetén is a geometriában használatos elnevezéseket fogjuk használni. Vegyük észre, hogy ha az 1.1 definícióban szereplő $\mathcal{L}$ halmaz minden l elemét helyettesítjük $\mathcal{P}$ azon részhalmazával, amely az l-re illeszkedő $P \in \mathcal{P}$ elemekből áll, akkor éppen a 2-dimenziós projektív tér definícióját kapjuk.

A továbbiakban GF(q) jelölje a q elemű véges testet, ahol $q = p^h$ prímhatvány (vagyis a *karakterisztika* p).

1.6. Definíció (4.2. Példa) Legyen V_{n+1} a GF(q) test feletti $(n+1)$-dimenziós vektortér. Legyen S a V_{n+1} egydimenziós altereinek halmaza, a kitüntetett részhalmazok pedig legyenek V_{n+1} alterei és az $\emptyset$. A V_{n+1} egy $(k+1)$-dimenziós alterének megfelelő S-beli részhalmaz dimenziója legyen k, az $\emptyset$ dimenziója pedig legyen -1. Ezt a teret *n-dimenziós Galois-térnek* nevezzük, és PG(n, q)-val jelöljük.

1.7. Tétel (4.5.) Minden legalább 3-dimenziós véges projektív tér izomorf valamely PG(n, q) térrel.

A PG(n, q) projektív tér kombinatorikus tulajdonságainak leírásához bevezetünk néhány jelölést (szintén az [1] szerint). Legyen $\Theta(r) = \frac{q^{r+1}-1}{q-1}$ és $[r, s] = \prod_{i=r}^{s}(q^i - 1)$, amennyiben $r \leq s$. Megjegyezzük, hogy szokványosabb az $\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdot\ldots\cdot(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdot\ldots\cdot(q-1)}$ jelölés, ami az n-dimenziós vektortér k-dimenziós altereinek számát jelöli, ha $k \leq n$.

1.8. Tétel (4.6.) A PG(n, q) projektív tér altereire igazak az alábbiak:

1. a tér pontjainak száma $\Theta(n)$;
2. a tér m-dimenziós altereinek száma $\begin{bmatrix} n \\ m \end{bmatrix}_q = \frac{[n-m+1, n+1]}{[1, m+1]}$, ha $0 \leq m \leq n-1$;
3. a tér egy adott k-dimenziós alterét tartalmazó m-dimenziós altereinek száma $\frac{[m-k+1, n-k]}{[1, n-m]}$, ha $0 \leq k \leq m \leq n-1$.

Most pedig térjünk rá a szakdolgozat legfontosabb fogalmára, a *lefogó ponthalmazra*. A továbbiakban Π_q-val egy tetszőleges q-adrendű projektív síkot fogunk jelölni.

1.9. Definíció (6.21.) A Π_q projektív sík valamely B ponthalmaza *lefogó ponthalmaz*, ha minden egyenes metszi B-t.

1.10. Lemma (6.22.) A q-adrendű Π_q projektív sík bármely B lefogó ponthalmaza legalább $q+1$ pontból áll. Ha a B lefogó ponthalmaz elemszáma $q+1$, akkor a B pontjai egy egyenest alkotnak (azt mondjuk, hogy a B egy egyenes).

Bizonyítás: Egy $P \notin B$ ponton át pontosan $(q+1)$ egyenes halad át, amelyek mindegyike tartalmaz B-beli pontot (és két ilyen egyenesnek P-n kívül nincs más közös pontja), így $|B| \geq q+1$. Továbbá, ha $|B| = q+1$, akkor tekintsünk két különböző B-beli pont által meghatározott e egyenest. Indirekt tegyük fel, hogy a B-beli pontok nem pontosan az e egyenes pontjai. Így vehetünk egy e-re illeszkedő nem B-beli P pontot. Erre a P pontra az előző gondolatot felhasználva azt látjuk, hogy a P-n átmenő e-től különböző egyenesekre kell legalább egy-egy B-beli pontnak esnie, az e-n pedig tudjuk, hogy legalább két B-beli pont is volt, tehát ellentmondást kapnánk a $|B| = q+1$-es feltevéssel. Következésképp $B = e$. □

1.11. Definíció (6.23.) Olyan lefogó ponthalmazt, amely nem tartalmaz teljes egyenest, *blokkoló halmaznak* nevezünk. A blokkoló halmazt *minimálisnak* mondjuk, ha tartalmazásra nézve az.

Figyeljük meg, hogy a blokkoló halmaz pontosan akkor minimális, ha bármely pontján át van a halmazt „érintő” egyenes, vagyis olyan egyenes, amely csak ezt az egy pontját tartalmazza a blokkoló halmaznak. Megfigyelhető, hogy $q = 2$ esetén nincsen blokkoló halmaz (*Neumann* és *Morgenstern* észrevétele). Általában viszont három nem egy ponton átmenő egyenes uniójából elhagyva az egyenesek metszéspontjait egy $3(q-1)$ méretű minimális lefogó ponthalmazt kapunk; vagy két egyenesről egy-egy pontot törölve és a törölt pontok által meghatározott egyenes egy tetszőleges pontját választva egy $2q-1$ méretű minimális lefogó ponthalmazt kapunk.

1.12. Lemma (6.24.) A Π_q q-adrendű projektív sík B blokkoló ponthalmazát minden egyenes legfeljebb $|B| - q$ pontban metszi.

Bizonyítás: Tekintsünk egy tetszőleges L egyenest és rajta egy P nem B-beli pontot (ilyen létezik, mert B blokkoló ponthalmaz). Ezen a ponton át az L egyenesen kívül még pontosan q egyenes halad át, amelyeket $B \setminus L$-beli páronként különböző pontokkal kell lefogni, tehát $|B \setminus L| \geq q$, vagyis $|B \cap L| \leq |B| - q$. □

1.13. Tétel (Bruck, 6.25.) Ha a Π_q q-adrendű projektív síknak van s-edrendű S részsíkja, akkor $q = s^2$ vagy $q \geq s^2 + s$. A $q = s^2$ esetben az s-edrendű részsík blokkoló ponthalmaz.

Bizonyítás: Legyen t olyan egyenes, amely a részsíkot egyetlen P pontban metszi. Ilyen van, hisz a részsík egy pontján keresztül Π_q-ban $q+1$ egyenes megy át, amelyekből csak $s+1$ egyenese a részsíknak. Ezt a t érintőt az S P-n át nem menő egyenesei páronként különböző pontokban metszik, mert a részsík két egyenese a részsík valamely pontjában metszi egymást. Eszerint $q \geq s^2$. Ha $q = s^2$, akkor az S-et érintő egyenesek száma $(s^2 + s + 1)(s^2 - s)$, hiszen minden ponton át $q + 1 = s^2 + 1$ egyenes megy Π_q-ban, amelyből $s+1$ lesz egyenese a részsíknak, azaz a többi $s^2 - s$ érintő. S egyeneseinek száma s^2+s+1, e kettő együtt pontosan $s^4 + s^2 + 1 = q^2 + q + 1$ egyenes. Azt kaptuk tehát, hogy minden egyenes metszi S-et, azaz S blokkoló halmaz. Ha $q \neq s^2$, akkor ugyanez a számolás adja, hogy lesz olyan egyenes, amely nem metszi S-et. Ekkor viszont S egyenesei ezt az egyenest páronként különböző pontokban metszik, azaz valóban $q + 1 \geq s^2 + s + 1$. □

1.14. Definíció (6.26.) A Π_q q-adrendű projektív sík $\sqrt{q}$-adrendű részsíkját *Baer-részsík*-nak nevezzük.

Már itt is szeretnénk kiemelni, hogy Baer-részsík tehát csak akkor létezhet, ha q négyzet (vagyis h páros).

A lefogó ponthalmazok fogalmát többféle természetes módon is általánosíthatjuk. Vizsgálhatunk n-dimenziós projektív terekben ($n \geq 3$) olyan ponthalmazokat, amelyek valamely $0 < k < n$-re az összes k-dimenziós alteret metszik. Ugyanakkor érdekes lehet olyan ponthalmazok vizsgálata is a projektív síkokban, amelyek azzal a tulajdonsággal rendelkeznek, hogy a projektív sík bármely egyenesét legalább t pontban metszik (és van olyan egyenes, amelyet pontosan t pontban metszenek). Ezeket az általánosításokat kombinálhatjuk is.

1.15. Definíció (7.2.) q-adrendű projektív sík valamely B részhalmazát *t-szeresen lefogó ponthalmaznak* nevezzük, ha B-t minden egyenes legalább t pontban metszi, és van olyan egyenes, amely pontosan t pontban metszi B-t.

1.16. Definíció ([2]) A $\mathrm{PG}(n, q)$ projektív tér valamely B részhalmazát *$(n-k)$-lefogó ponthalmaznak* nevezzük, ahol $0 < k < n$, ha B a $\mathrm{PG}(n, q)$ bármely k-dimenziós alterét metszi.

Tehát a két fogalom közös általánosítása:

1.17. Definíció ([2]) A $\mathrm{PG}(n, q)$ projektív tér valamely B részhalmazát *t-szeresen $(n - k)$-lefogó ponthalmaznak* nevezzük, ahol $0 < k < n$, ha B-t a $\mathrm{PG}(n, q)$ bármely k-dimenziós altere legalább t pontban metszi, és van olyan k-dimenziós altér, amely pontosan t pontban metszi B-t.

1.18. Állítás (7.4.) q-adrendű projektív sík bármely B t-szeresen lefogó ponthalmazának mérete legalább $t(q + 1)$.

Bizonyítás: Hasonlóan az 1.10 bizonyításához, ha tekintünk egy $P \notin B$ pontot, akkor a rajta átmenő $q + 1$ egyenes mindegyikét le kell fognunk legalább t-szer, és ezen egyeneseknek nincsen P-n kívül más közös pontjuk, tehát $|B| \geq t(q + 1)$. □

Számos a lefogó ponthalmazokat jellemző olyan eredmény ismert, ami az *ív* fogalmával könnyen megfogalmazható, így most definiáljuk az ezen eredmények kimondásához szükséges fogalmakat.

1.19. Definíció (6.1.) Projektív sík olyan ponthalmazát, amelynek nincs három egy egyenesen fekvő pontja, *ívnek* nevezzük. Ha az ív k pontú, akkor k-ívről beszélünk. Az ívet *teljesnek* mondjuk, ha tartalmazásra nézve maximális, azaz nem része $(k + 1)$-ívnek.

1.20. Definíció (6.2.) A sík valamely egyenese az adott k-ívre nézve *szelő*, *érintő*, illetve *külső* egyenes, ha a k-ívvel rendre 2,1, illetve 0 közös pontja van.

1.21. Tétel (Bose, 6.3.) q-adrendű sík bármely k-ívére $k \leq q + 2$ teljesül. Ha q páratlan, akkor $k \leq q + 1$ is igaz.

Bizonyítás: (vázlat) Válasszuk ki az ív egy tetszőleges P pontját. Ezen a ponton $q + 1$ egyenes halad át, amelyek mindegyikén legfeljebb egy másik pontja lehet az ívnek, tehát $k \leq 1 + (q + 1)$. Ha viszont $k = q + 2$, akkor megmutatható, hogy az ívnek páros sok pontjának kell lennie, tehát q páros. □

1.22. Állítás (Lunelli, Sce, 6.4.) q-adrendű sík k-íve nem lehet teljes, ha $q \geq \frac{k(k-1)}{2}$.

Bizonyítás: Ha a k-ív teljes, akkor az ívre nézve szelő egyenesek a sík minden pontját lefedik. Mivel ehhez (az 1.10 duális változata miatt) legalább $q + 1$ egyenes kell, ezért $\binom{k}{2} \geq q + 1$. □

1.23. Definíció (6.5.) *Oválisnak* olyan ívet nevezünk, amelynek minden pontjában pontosan egyetlen érintő egyenese van. *Hiperoválisnak* az olyan íveket nevezzük, amelyeknek nincs érintő egyenesük.

Mivel tetszőleges k-ív minden pontján pontosan $k - 1$ szelő, és így $t = q + 2 - k$ érintő egyenes megy át, így a q-adrendű síkok oválisai éppen a $(q + 1)$-ívek, a hiperoválisok pedig a $(q + 2)$-ívek.

1.24. Állítás (6.6.) $\mathrm{PG}(2, q)$-ban léteznek oválisok. Ha q páros, akkor hiperoválisok is vannak.

1.25. Állítás (6.7.) Páros rendű síkon a $(q+1)$-ívek nem teljesek.

1.26. Tétel (6.19.) PG$(2,q)$-ban, ha $q>4$ négyzet, akkor léteznek teljes $(q-\sqrt{q}+1)$-ívek.

Az 1.22 bizonyítása során az is adódott, hogy a teljes ívek szelő egyenesei lefogó ponthalmazt alkotnak a projektív sík duális síkjában. Ebből az észrevételből kapjuk a következő állítást.

1.27. Következmény (6.33.) Ha $q=p$ prím, akkor PG$(2,q)$ legkisebb teljes íve legalább $\sqrt{3q}$ pontú.

Bizonyítás: Könnyű látni, hogy az állítás előtti megjegyzésben említett lefogó ponthalmaz nem tartalmazhat egyenest, mert az az eredetiben azt jelentené, hogy van olyan pont, amin átmenő minden egyenes szelő. Tehát $\binom{k}{2} \geq \frac{3(p+1)}{2}$. □

1.28. Tétel (Blokhuis, 6.34.) Legyen $q=p^n$, $n\geq 2$. Ekkor PG$(2,q)$ blokkoló ponthalmazai legalább $q+\sqrt{q}+1$ pontúak, ha n páros, és legalább $q+\sqrt{pq}+1$ pontúak, ha n páratlan.

Most pedig a többszörösen lefogó ponthalmazokat fogjuk tovább jellemezni a (k,n)-ívek segítségével.

1.29. Definíció (7.1.) q-adrendű projektív (vagy affin) sík K részhalmazát (k,n)-*ívnek* nevezzük, ha $|K|=k$, K-t minden egyenes legfeljebb n pontban metszi, és van olyan egyenes, amely pontosan n pontban metszi K-t.

Az 1.15 definícióval összevetve az iméntit azt láthatjuk, hogy ez a két fogalom egymás komplementuma, ha $n+t=q+1$.

1.30. Állítás (Barlotti, 7.3.) q-adrendű sík bármely (k,n)-ívének méretére

$$k \leq nq-q+n$$

teljesül, és egyenlőség esetén n osztója q-nak.

Bizonyítás: Az előző megjegyzés miatt $t=q+1-n$ mellett a két fogalom egymás komplementuma, vagyis felhasználva az 1.18 eredményét azt kapjuk, hogy tetszőleges K (k,n)-ív méretére:

$$|K| \leq q^2 + q + 1 - t(q+1) = q^2 + q + 1 - (q+1-n)(q+1) = nq - q + n.$$

Egyenlőség esetén minden olyan egyenes, ami metszi K-t pontosan n pontban kell messe. Tehát K pontjainak számát osztja n, ahonnan $n|q$. □

2. Kombinatorikus észrevételek és a Rédei-féle hézagos polinomos módszer

Most pedig térjünk rá – továbbra is az [1] könyvet követve – a PG(2, q) lefogó ponthalmazainak tulajdonságait jellemző állításokra, amelyek többsége a méretre vonatkozó becslés lesz. Ezen becslések kombinatorikus leszámlálásokkal igazolhatóak, és némelyek élesek abban az értelemben, hogy a becslésbeli egyenlőség esetén konstruálható a feltételeknek megfelelő lefogó ponthalmaz. Ezek után pedig a fejezet további részében megismerkedünk – [6] alapján – a *Rédei*-féle hézagos polinomok módszerével.

2.1. Tétel (Bruen, Pelikán, 6.27.) q-adrendű projektív sík blokkoló halmazai legalább $q + \sqrt{q} + 1$ pontúak. Ha egyenlőség van, akkor a blokkoló halmaz pontjai Baer-részsíkot alkotnak.

Bizonyítás: Jelöljük a blokkoló halmazt B-vel. Sorojuk fel a sík egyeneseit: $L_1, L_2, \ldots, L_{q^2+q+1}$, és legyen $n_i = |L_i \cap B|$, ahol $1 \leq i \leq q^2 + q + 1$. Kettős leszámlálást fogunk alkalmazni a B-beli pont és rajta átmenő egyenes párokra, valamint a B-beli pontpár és rajtuk átmenő egyenes párokra. Ezekből kapjuk, hogy

$$\sum_{i=1}^{q^2+q+1} n_i = |B|(q+1) \qquad ; \qquad \sum_{i=1}^{q^2+q+1} n_i(n_i-1) = |B|(|B|-1).$$

Az 1.12 miatt tudjuk, hogy $1 \leq n_i \leq |B| - q$, ezt felhasználva:

$$|B|(|B|-1) = \sum_{i=1}^{q^2+q+1} n_i(n_i-1) \leq (|B|-q)\cdot\left(\sum_{i=1}^{q^2+q+1}(n_i-1)\right) = (|B|-q)\cdot(|B|(q+1)-(q^2+q+1)).$$

Az egyenlőtlenség megoldásával adódik az állítás. Az egyenlőség feltétele az, hogy minden n_i vagy 1 vagy $|B| - q$ legyen, és ekkor a B-t metsző egyenesek $\sqrt{q}$-adrendű részsíkot alkotnak, hiszen bármely két ponton át egy egyenes megy, $|B| = q + \sqrt{q} + 1$ és így $|B| - q = \sqrt{q} + 1$, tehát az egyenesek $\sqrt{q} + 1$ pontúak. Ebből következik, hogy minden pont foka is $\sqrt{q} + 1$, azaz bármely két egyenes metszi egymást. Mivel két egyenes nem fedheti le B-t, így B valóban teljesíti a projektív sík axiomáit. □

2.2. Tétel (Ball, 7.9.) Legyen B t-szeresen lefogó ponthalmaz AG(2, q)-ban. Legyen $e(t)$ az a maximális kitevő, amelyre $p^{e(t)}$ osztja t-t. Ekkor $|B| \geq (t + 1)q - p^{e(t)}$.

Ebből a tételből egyrészt következik egy felső becslés az $\mathrm{AG}(2,q)$-beli K (k,n)-ív méretére, másrészt egy alsó becslés a $\mathrm{PG}(2,q)$ t-szeresen lefogó olyan ponthalmazára, ami tartalmaz egyenest.

2.3. Következmény (7.10.) Legyen K (k,n)-ív $\mathrm{AG}(2,q)$-ban. Legyen e az a maximális kitevő, amelyre p^e osztja n-et. Ekkor $|K| \leq (n-1)q + p^e$.

Bizonyítás: Legyen B a K komplementere $\mathrm{AG}(2,q)$-ra nézve. Ez $t = (q-n)$ mellett t-szeresen lefogó ponthalmaz lesz, innen az előző 2.2 tételből adódik az eredmény. □

Lunelli és *Sce* azt sejtette, hogy a $\mathrm{PG}(2,q)$ bármely (k,n)-ívére $k \leq (n-1)q+1$ teljesül, azonban ez általában nem igaz (*Hill* és *Mason* mutattak ellenpéldát diszjunkt Baer-részsíkok uniójaként). Például egyetlen Baer-részsík komplementere $k = q^2 - \sqrt{q}$ pontú $n = q$ paraméterű (k,n)-ív, és erre nem teljesül a Lunelli-Sce sejtés. Továbbá t darab Baer-részsík komplementerére nem fog teljesülni a Lunelli-Sce sejtés, ha $t < \frac{q+1}{\sqrt{q}+2}$. Ugyanis t darab Baer-részsík komplementere $k = q^2+q+1-t(q+\sqrt{q}+1)$ pontú és $n = q+1-t$ paramétreű (k,n)-ív, ahol $k > (n-1)q+1$. Így:

$$(q+1-t)(q-1)+1 < q^2+q+1-t(q+\sqrt{q}+1)$$

$$q^2-tq+t < q^2+q+1-tq-t\sqrt{q}-t$$

$$t(\sqrt{q}+2) < q+1 \qquad \Longrightarrow \qquad t < \frac{q+1}{\sqrt{q}+2}.$$

Ha azonban n és q relatív prímek, és van a (k,n)-ívet nem metsző egyenes, akkor a 2.3 miatt igaz a Lunelli-Sce sejtés.

2.4. Következmény (7.20.) Ha $\mathrm{PG}(2,q)$ valamely S t-szeresen lefogó ponthalmaza tartalmaz egyenest, akkor $|S| \geq (t+1)q - t + 2$.

Bizonyítás: Kihagyva az egyenest, egy $\mathrm{AG}(2,q)$-beli $(t-1)$-szeresen lefogó ponthalmazt kapunk. Innen a 2.2 szerint készen vagyunk. □

Az 1.30 miatt a maximális ívek az $(nq-q+n,n)$-ívek lehetnek. Ilyenek megkonstruálhatóak páros rendű síkokon feltéve, hogy $n|q$.

2.5. Tétel (Denniston, 7.14.) Páros q-ra minden $n|q$-ra létezik $(nq-q+n,n)$-ív $\mathrm{PG}(2,q)$-ban (sőt $\mathrm{AG}(2,q)$-ban is).

Nagyon érdekes ezen állítás tudatában, hogy ha a projektív sík rendje páratlan, akkor egészen más a helyzet.

2.6. Tétel (Ball, Blokhuis, Mazzocca, 7.15.) Páratlan q-ra PG$(2, q)$-ban nincsenek $(nq - q + n, n)$-ívek, $1 < n < q$.

Itt megjegyezzük, hogy az $n = 3$ esetet korábban *Cossu* illetve *Thas* elintézte. Sőt az előzőnél tételnél többet is tudunk:

2.7. Tétel (7.16.) Ha n osztja q-t, és $n \leq \frac{q}{4}$, akkor PG$(2, q)$ bármely (k, n)-ívére $k \leq nq - q + \frac{2n}{3}$.

2.8. Tétel (Ball, Blokhuis, [11]) Legyen B egy $(nq - q + n - \varepsilon, n)$-ív PG$(2, q)$-ban, ahol $n|q$ teljesül. Ekkor:

1. q páros esetben: ha $\varepsilon < \frac{n}{2}$ és $\frac{q}{n} > 2$ vagy $\varepsilon < 0{,}381 \cdot n$ és $\frac{q}{n} = 2$, akkor B egyértelműen kiterjeszthető egy $nq - q + n$ pontú maximális ívvé;

2. q páratlan esetben: ha $\frac{q}{n} > 2$, akkor $\varepsilon > \frac{n}{2}$ és ha $\frac{q}{n} = 3$, akkor $\varepsilon > 0{,}476 \cdot n$.

Ezen tételek bizonyításai és ezen kérdéskör további információi a [10], [11] cikkekben megtalálhatóak.

Most pedig térjünk rá egy algebrai technika ismertetésére: a *hézagos polinomok elméletének* vizsgálatára. A következőkben a [6] összefoglaló cikket fogjuk követni. A hézagos polinomok elmélete a szegedi Rédei Lászlótól származik, aki azt az 1970-ben német nyelven megjelent *Lückenhafte Polynome über endlichen Körpern* című könyvében [8] tette közzé. A szakdolgozat témája miatt itt a precíz algebrai háttérről nem fogunk szólni (ezeknek az olvasó utána tud nézni a [6] 2. szakaszában), helyette a módszer véges geometriai alkalmazásai közül mutatunk be párat.

Mindenekelőtt azonban a módszer tárgyalásához szükséges algebrai fogalmakat átismételjük. Korábban már bevezettük a $q = p^h$ elemű véges test fogalmát, aminek karakterisztikája tehát p. A véges testek fölött a szokásos módon definiálhatunk polinomokat és a polinomok között műveleteket. Egy F test feletti egyváltozós polinomok halmazát $F[X]$-el jelöljük, az $f(X) = \sum_{i=0}^{n} a_i X^i$ polinom *foka* $\deg(f) = n$, ha az a_n főegyüttható nem nulla az F testben. Tekintsük az n-edfokú $0 \neq f(X) = \sum_{i=0}^{n} a_i X^i$ polinomot és ennek segítségével képezzük a $g(X) = f(X) - a_n X^n$ polinomot. Nevezzük a g polinom fokát az

f polinom *második fokának*, és következőképpen jelöljük $\deg(g) = \deg2(f)$. A $\deg(f) - \deg2(f)$ értéket az f polinom *esésének* nevezzük (ez természetesen mindig legalább 1). A polinomot pedig *hézagosnak* mondjuk, ha az esése elég nagy (ez tehát csak egy szemléletes fogalom, az esés értéke tételről tételre változhat).

Az F test feletti polinomot *reducibilisnek* nevezzük, ha felbomlik két alacsonyabb fokú polinom szorzatára. A polinom *teljesen reducibilis*, ha F felett lineáris (elsőfokú) faktorokra bomlik. A polinomokat *formálisan deriválni* is fogjuk, vagyis az $f(X) = \sum_{i=0}^{n} a_i X^i$ polinom formális deriváltja az $f'(X) = \sum_{i=0}^{n-1}(i+1)a_{i+1}X^i$ polinom (természetesen $(i+1)a_i$ az F test azon eleme, amelyet az a_i elem $(i+1)$ példányának összeadásával kapunk). Ezzel a definícióval a deriválás jól megszokott szabályai érvényben fognak maradni. Vegyük észre, hogy véges test felett előfordulhat az, hogy egy nem-konstans polinom deriváltja 0, azonban itt teljesül az, hogy ha egy polinom deriváltja 0, akkor a polinom minden tagjának kitevője p-vel (a karakterisztikával) osztható kell legyen, vagyis a polinom X^p-nek is polinomja.

Lássuk a Rédei által [8]-ben vizsgált legfontosabb két kérdést. Legyen $F = \mathrm{GF}(q)$, ahol $q = p^n$, p prím.

I. Probléma. Legyen $d|(q-1)$ $(d > 1)$ rögzített. Meghatározandók azon 1 főegyütthatós, X-szel nem osztható $f(X) \in F[X]$ polinomok, melyek teljesen reducibilisek, nincs többszörös faktoruk, és amelyekre

$$\deg(f) = \frac{q-1}{d} \qquad ; \qquad \deg2(f) \leq \frac{q-1}{d^2}.$$

II. Probléma. Melyek azok az 1 főegyütthatós $f(X) \in F[X]$ polinomok, amelyek nem polinomjai X^p-nek, teljesen reducibilisek, és amelyekre

$$\deg(f) = q \qquad ; \qquad \deg2(f) \leq \frac{q+1}{2}.$$

Az algebrai háttért nem kívánjuk tárgyalni, ezért a teljesség igénye nélkül beidézünk néhány állítást, amelyek hézagos polinomokra vonatkoznak és szorosan kapcsolódnak a fenti két problémához.

2.9. Állítás ([8] Par. 10, [6] 2. Állítás) Legyen $f(X) = X^q + g(X)$ teljesen reducibilis és tegyük fel, hogy $f'(X) \neq 0$. Ekkor $\deg(g) \geq \frac{q+1}{2}$, vagy $f(X) = X^q - X$.

Bizonyítás: Mivel $f'(X) \neq 0$, így $g(X)$ nem lehet konstans polinom. Tekintsük a $g(X)+X$ polinomot. Mivel $f(X) = (X^q - X) + (g(X) + X)$ és az $(X^q - X)$-nek minden testelem (egyszeres) gyöke, így f minden gyöke a $(g(X)+X)$-nek is gyöke. Szemléletesen azt szeretnénk belátni, hogy f-nek sok különböző gyöke van. Ez a teljes reducibilitás miatt akkor lehet, ha nincs sok többszörös gyöke, így a többszörös gyökök számát szeretnénk korlátozni. Legyen $F(X)$ az a polinom, amely f minden gyökét pontosan egyszeres multiplicitással tartalmazza, azaz legyen $F(X)$ az $f(X)$ és az $X^q - X$ legnagyobb közös osztója. Ekkor a fentiek miatt $F(X)$ osztja $(g(X)+X)$-et is. Másrészt viszont az $\frac{f(X)}{F(X)}$ polinom gyökei pontosan az f többszörös gyökei, mégpedig eggyel kisebb multiplicitással, mint f-ben, így az is teljesül, hogy az $\frac{f(X)}{F(X)}$ polinom osztja $f'(X)$-et. Mivel $f(X) = X^q + g(X)$, így $f'(X) = g'(X)$, vagyis az $\frac{f(X)}{F(X)}$ polinom osztja $g'(X)$-et. Ebből viszont felhasználva, hogy $F(X)|(g(X)+X)$ azt kapjuk, hogy $f(X)$ osztja a $(g(X)+X)g'(X)$-et.

Mivel $f'(X) \neq 0$ és $g(X)$ nem konstans, így $g'(X)$ sem a nullapolinom. Ha $g(X)+X$ a nullapolinom, akkor $f(X) = X^q - X$, különben pedig $\deg(f) \leq \deg(g) + \deg(g') \leq$ $\leq 2 \cdot \deg(g) - 1$. Vagyis $q \leq 2 \cdot \deg(g) - 1$, amiből $\deg(g) \geq \frac{q+1}{2}$ következik. □

Ez az állítás motiválja a **II. Probléma** feltevését az f második fokára. A most következő két tétel pedig a problémák feltételeinek enyhítése esetén mond valamit:

2.10. Tétel (Blokhuis, [9]) Legyen $f(X)$ teljesen reducibilis $\mathrm{GF}(p)$ felett (p prím), és tegyük fel, hogy $f(X) = X^p g(X) + h(X)$, valamint hogy g és h relatív prímek. Ha $f(X) \neq$ $\neq a(X^p - X)$ és $f(X) \neq aX^p + b$, akkor g és h közül legalább az egyiknek a foka legalább $\frac{p+1}{2}$.

Bizonyítás: A bizonyítás során szeretnénk az előző 2.9 állítást használni, ezért megmutatjuk, hogy feltehető az, hogy $f'(X) \neq 0$. Ellenkező esetben ugyanis vagy az $f(X) =$ $= aX^p + b$ esetben vagyunk, vagy g és h valamelyikének foka legalább p lenne.

Jelölje a továbbiakban $e(X)$, illetve $t(X)$ az $f(X)$ egyszeres, illetve többszörös gyökeihez tartozó gyöktényezők szorzatát. A 2.9 bizonyításában már megállapítottuk, hogy $e(X)$ az $f(X)$ és az $X^q - X$ polinomok legnagyobb közös osztója, míg $t(X)$ az $f(X)$ és az $f'(X)$ legnagyobb közös osztója.

Most azonban tudjuk, hogy $e(X)$ osztja $X^p - X$-et is, így mivel $f(X) = X^p g(X) + h(X)$ azt kapjuk, hogy $e(X)$ osztja $Xg(X)+h(X)$-et is, ami azért lesz fontos, hiszen ennek a foka jóval kisebb, mint $f(X)$-é volt. Vegyük észre, hogy $Xg(X)+h(X)$ nem lehet a nullapolinom, mert a $g(X)$ és $h(X)$ relatív prímsége miatt ez csak akkor fordulhatna elő, ha $g(X)$ konstans polinom, ekkor viszont $f(X) = a(X^p - X)$.

Most találunk $t(X)$-hez is egy olyan kis fokú polinomot, amelyet $t(X)$ oszt. Azt tudjuk, hogy $t(X)$ osztja $f(X)$-et és $f'(X)$-et, amely polinomok legnagyobb fokú tagját kiejtve a következő adódik: $t(X)$ osztja az $f(X)g'(X) - f'(X)g(X) = h(X)g'(X) - h'(X)g(X)$ polinomot. Vegyük észre, hogy ez a polinom sem lehet a nullapolinom, hiszen a $g(X)$ és $h(X)$ relatív prímségéből most az adódna, hogy $g'(X) = 0$ és $h'(X) = 0$, ekkor viszont $f'(X) = 0$ lenne, amit az elején kizártunk. Tehát

$$f(X) \mid e(X)t(X) \mid \Big(Xg(X) + h(X)\Big)\Big(h(X)g'(X) - h'(X)g(X)\Big),$$

ahol a jobboldali polinom nem a nullapolinom, így van értelme a fokszámok összehasonlításának. Különböztessünk meg 3 esetet aszerint, hogy $g(X)$ és $h(X)$ fokai hogy viszonyulnak egymáshoz. A nagyobbik fokszámot jelölje k. Ha $\deg(g) = \deg(h)$, akkor $f(X)$ foka $p + k$, az $Xg(X) + h(X)$ foka $k + 1$, a $h(X)g'(X) - h'(X)g(X)$ foka pedig $2k - 2$ (mivel a főtag kiesik). Ebből $p + k \leq k + 1 + 2k - 2$, tehát tényleg $k \geq \frac{p+1}{2}$. Ha $\deg(g)$ a nagyobb, akkor ugyanezek érvényesek (sőt $\deg(h(X)g'(X) - h'(X)g(X)) \leq 2k - 2$), vagyis ekkor is $k \geq \frac{p+1}{2}$. Végül, ha $\deg(h)$ a nagyobb és $\deg(g) = s \leq k - 1$, akkor az $Xg(X) + h(X)$ foka legfeljebb k és $\deg(h(X)g'(X) - h'(X)g(X)) \leq k + s - 1$ és $\deg(f) = p + s$, ahonnan szintén $k \geq \frac{p+1}{2}$ adódik. □

Ha pedig általában prímhatvány rendű test feletti polinomokat vizsgálunk, akkor ez adódik:

2.11. Tétel (Blokhuis, [9]) Legyen $q = p^n$, $f(X)$ teljesen reducibilis GF(q) felett, és tegyük fel, hogy $f(X) = X^q g(X) + h(X)$, valamint hogy g és h relatív prímek. Ha $f(X) \neq a(X^q - X)$ és $f(X) \neq aX^q + b$, akkor g és h közül legalább az egyiknek a foka legalább $p^{\left[\frac{n+1}{2}\right]}$.

Térjünk rá a véges geometriai kapcsolat vizsgálatára. Ehhez legyen K egy q elemű véges test, $f : K \to K$ pedig egy függvény (polinom). Az $\{(x, f(x)) \ : \ x \in K\}$ pontok halmazát az f *grafikonjának* nevezzük a K-ra épített AG$(2, q)$ affin síkon. Azt mondjuk, hogy egy (m) irányt (m meredekséget) az f grafikonja *meghatároz*, ha találunk a grafikonon két olyan pontot, melyek összekötő egyenese m meredekségű. Rédei azt a kérdést válaszolta meg, hogy egy függvény legalább hány irányt határoz meg. Később Lovász és Schrijver ([7]) észrevették, hogy az nem lényeges, hogy egy függvény grafikonjáról beszélünk. Legyen ugyanis U tetszőleges q pontú halmaz az AG$(2, q)$ affin síkon és tegyük fel, hogy U nem határoz meg minden irányt. Ekkor válasszunk egy – az U által nem meghatározott – irányt az Y-tengely irányának (a „függőlegesnek"). Mivel ez az irány nem meghatározott volt, így minden függőleges egyenesen legfeljebb egy U-beli pont van, azonban $|U| = q$, így minden függőleges egyenesen pontosan egy U-beli pont van. Ezután tetszőlegesen választva az X-tengelyt az $(x,0)$ pontok esetén x-hez a rajtuk átmenő függőleges egyenesen levő U-beli pont második koordinátáját rendelve U épp egy függvény grafikonjaként adódik.

Legyen tehát $U = \{(a_i, b_i) \ : \ i = 0, \ldots, q-1\}$. Ha U függvény grafikonja, az pontosan azt jelenti, hogy az a_i elemek a test összes elemének egy permutációját adják. Tekintsük a következő polinomot:

$$H(X,Y) = \prod_{i=0}^{q-1}(X + a_i Y - b_i).$$

Ezt a kétváltozós polinomot az U *Rédei-polinomjának* nevezzük (ha a $H(X,Y)$ polinomot az y rögzítésével X polinomjaként akarjuk tekinteni, akkor $H_y(X)$-ként írjuk majd). A H polinomot úgy alkottuk meg, hogy az Y és X egy egyenes meredekségét és tengelymetszetét akarja jelölni, míg a pont X, Y koordinátáinak szerepét az a_i, b_i játsza. Az alábbi lemma a $H(X,Y)$ polinom egy szép tulajdonságára hívja fel a figyelmet:

2.12. Lemma ([1] 6.29.) Legyen $H(X,Y)$ az U Rédei-polinomja, $m \in \mathrm{GF}(q)$. Ekkor az $X = b$ pontosan akkor r-szeres gyöke $H(X,m)$-nek, ha az $Y = mX + b$ egyenes r pontban metszi U-t.

Bizonyítás: A Rédei-polinomban minden $(a_i, b_i) \in U$ ponthoz egy lineáris tényező tartozik. Mivel $b + a_i m - b_i = 0$ pontosan akkor, ha az $Y = mX + b$ egyenes átmegy az (a_i, b_i) ponton, az $X = b$ érték annyiszoros gyök lesz, ahány lineáris tényező eltűnik (a_i, b_i)-ben, azaz ahány pontja van U-nak az $Y = mX + b$ egyenesen. □

Továbbá ez a polinom érzékeny arra, hogy valamely y meredekséget meghatároz-e U, ahogy azt a következő lemma is mutatja.

2.13. Lemma ([6] 8. Lemma) Ha az $(y) \neq (\infty)$ irányt U nem határozza meg, akkor erre az y-ra $H_y(X) = X^q - X$.

Bizonyítás: Egy $\prod(X + a_i y - b_i)$ polinom akkor lesz $X^q - X$, ha a $(-a_i y + b_i)$ elemek páronként különbözőek, és így kiadják a test összes elemét. Vizsgáljuk meg, hogy mikor lesz $a_i y - b_i = a_j y - b_j$ valamely $i \neq j$-re! Ekkor $y = \frac{b_i - b_j}{a_i - a_j}$ adódik, ami éppen azt jelenti, hogy az (a_i, b_i) és (a_j, b_j) pontokon átmenő egyenes meredeksége y ($a_i = a_j$ esetén $b_i = b_j$ következik, ami nem lehetséges $|U| = q$ miatt). □

A 2.9 és az iménti lemma segítségével pedig levezethető a következő tétel.

2.14. Tétel (Rédei, Megyesi, [6] 9. Tétel) Legyen U az AG$(2, p)$ (p prím) affin sík olyan p pontú részhalmaza, amely nem egyenes. Ekkor U legalább $\frac{p+3}{2}$ irányt határoz meg. Más szóval, ha U legfeljebb $\frac{p+1}{2}$ irányt határoz meg, akkor szükségképpen egyenes.

Bizonyítás: Legyen $U = \{(a_i, b_i) \ : \ i = 0, \dots, p-1\}$ és tegyük fel, hogy a (∞) irányt meghatározza U. Tekintsük az U Rédei-polinomját, amelyet az X hatványai szerint csoportosítva is felírhatunk:

$$H(X,Y) = \prod_{i=0}^{p-1}(X + a_iY - b_i) = \sum_{j=0}^{p} h_j(Y)X^{p-j}.$$

Itt $h_0(Y) \equiv 1$, általában pedig a $h_j(Y)$ polinom foka legfeljebb j. Jelölje n az U által nem meghatározott Y irányok számát. Ilyen y-okra a 2.13 szerint $H(X,y) = X^p - X$, így ilyenkor $h_1(y), \dots, h_{p-2}(y) = 0$. Mivel ilyen y-ból n darab van, ezért ha a h_i polinom foka kisebb, mint n, akkor az n gyököt látva megállapíthatjuk, hogy $h_i(Y) \equiv 0$. Így a $h_1, \dots, h_{n-1}$ polinomok azonosan nullák.

Most tekintsük a $H(X,Y)$-t egy meghatározott iránynak megfelelő y-ra, mint X polinomját. Ekkor $H(X,y)$ főtagja X^p, míg a második fok ilyen y-ra is legfeljebb $p-n$. Összevetve ezt a 2.9 állítással azt kapjuk, hogy $p - n \geq \frac{p+1}{2}$, azaz $n \leq \frac{p-1}{2}$. Ez viszont azt jelenti, hogy a meghatározott irányok száma legalább $\frac{p+3}{2}$. □

A 2.10 és a 2.12 alapján a következő becslést kaphatjuk a PG$(2, p)$-beli blokkoló halmazok méretére p prím esetben.

2.15. Tétel (Blokhuis, 6.32.) PG$(2, p)$ (p prím) blokkoló halmazai legalább $\frac{3(p+1)}{2}$ pontot tartalmaznak.

Bizonyítás: Most is tekintsünk egy U halmazt, ami most a B ($p + k$) pontú blokkoló halmaz affin része legyen. Legyen $U = \{(a_i, b_i) \ : \ i = 0, \dots, p+s-1\}$, míg a B ideális pontjai legyenek a $(\infty), (y_1), \dots, (y_{k-1-s})$ pontok. Feltehető, hogy B tartalmazásra nézve minimális és hogy B az ideális egyenest legalább két pontban metszi.

Először a 2.14 bizonyításához hasonlóan vizsgáljuk meg a nem meghatározott irányok esetén a Rédei-polinomot. Legyen (y) valamely nem B-beli pont. Az y meredekségű egyeneseket B affin részének kell lefognia, azaz minden ilyen y-ra minden y meredekségű egyenest metsz U. A 2.12 miatt $(y) \notin B$ esetén $H(X,y)$ osztható $(X^p - X)$-el. Ez azt jelenti, hogy ilyen y-okra $H(X, y)$ nem tartalmaz X^p és X^{s+1} közötti tagokat. Így a 2.14 bizonyításához hasonlóan adódik, hogy $h_{s+1}(Y), \dots, h_{p-2}(Y)$ polinomok eltűnnek minden $y \neq y_r$-re. Ilyen y-ból pedig $p+1+s-k$ darab van, tehát $h_j(Y)$ polinomok azonosan nullák ($j \leq p+s-k$), mivel $\deg(h_j) \leq j$.

Most pedig tekintsük (a 2.14 tételhez hasonlóan) $H(X, y)$ polinomot valamely $y = y_r$ esetén ($r = 1, \dots, k-1-s$). Az $X^{p-1}, \dots, X^k$ tagok ekkor is hiányoznak majd, vagyis ilyen $y = y_r$-re:

$$H(X, y_r) = X^p g(X) + h(X), \qquad \deg(g) = s, \quad \deg(h) \leq k-1.$$

Ez majdnem a 2.10 tételbeli szituáció, mivel $H(X, y_r)$ teljesen reducibilis, a bajt tehát csak az okozhatja, ha g és h nem relatív prímek. Ha leosztunk e két polinom legnagyobb közös osztójával, akkor csak annyi változik, hogy olyan $X^p g_1(X) + h_1(X)$ polinomot kapunk, ahol $\deg(g_1) \leq s$ és $\deg(h_1) \leq k-1$. Mivel $k-1 \geq s$, így a 2.10 alapján $k-1 \geq \frac{p+1}{2}$, vagyis $|B| \geq \frac{3(p+1)}{2}$.

Meg kell még gondolnunk, hogy a 2.10 tételben kizárt esetek most sem fordulhatnak elő. Ha polinomunk $aX^p + b = (aX+b)^p$ lenne, akkor az azt jelentené, hogy az y_r meredekségű $\left(\frac{-b}{a}\right)$ tengelymetszetű egyenes teljes egészében B-ben van, ami nem lehetséges. Ha pedig $H(X, y_r)$ osztható lenne $(X^p - X)$-el, akkor az (y_r) ideális pontot elhagyhatnánk B-ből és továbbra is blokkoló halmazt kapnánk, ami ellentmondana B tartalmazásra nézve minimális választásával. □

A fejezet zárásaként bizonyítás nélkül következzen két becslés a lefogó ponthalmaz méretére vonatkozóan prímrendű síkon, amelyeket a Rédei-polinom segítségével lehetne bebizonyítani.

2.16. Tétel (7.21.) Legyen B t-szeresen lefogó ponthalmaz $PG(2, q)$-ban, ahol $q = p$ prím. Ekkor $|B| \geq \max\{tq + \frac{q+3}{2}, tq + t\}$.

A fenti tétel némileg erősíthető:

2.17. Tétel (Ball, 7.22.) Ha $q = p$ prím, B t-szeresen lefogó ponthalmaz $PG(2, q)$-ban, $t \leq \frac{q+1}{2}$, akkor $|B| \geq tq + t + \frac{q+1}{2}$.

Az iménti tétel éles is, ha $t = \frac{q+1}{2}$, ekkor ugyanis a kúpszeletekre nézve külső pontok a kúpszelet pontjaival együtt t-szeresen lefogó ponthalmazt alkotnak. Megjegyezzük, hogy általában a $q = p^h$ prímhatvány esetben az ismert eredmények megtalálhatóak a [10] cikkben.

3. További eredmények és módszerek

3.1. Magasabb dimenziós eredmények

Most az [5] könyvfejezetének második szakaszából fogunk bizonyítások nélkül beidézni néhány ismert lefogó ponthalmazokra vonatkozó eredményt magasabb dimenziós projektív terekben. Magasabb dimenziós konstrukciókról itt most nem fogunk szólni, azonban aki ezek iránt érdeklődik az utánaolvashat az [5] harmadik szakaszában.

3.1. Definíció ([5] Definition 1.2.) Egy B lefogó ponthalmazt nevezzünk *d-valódinak* (angolul *d-proper*), ha d-dimenziós (ami annyit jelent, hogy a B által generált altér d-dimenziós) és nem tartalmaz olyan lefogó ponthalmazt, aminek dimenziója $d-1$. Jelölje a legkisebb d-valódi lefogó ponthalmaz méretét $f_d(q)$. Legyen továbbá $r_d(q) = f_d(q) - (q+1)$.

3.2. Definíció ([5]) Legyen B egy ponthalmaz $\mathrm{PG}(n,q)$-ban, V pedig egy olyan altér, amelyre teljesül, hogy $V \cap \langle B \rangle = \emptyset$. Ekkor VB-vel jelöljük a V csúcsú és B alapú *kúpot*, amely a V-nek és a $\langle V, X \rangle$ altereknek uniója, ahol $X \in B$ (ha $B = \emptyset$, akkor a VB kúp maga V).

3.3. Tétel (Bose, Burton, [5] Theorem 2.1.) $\mathrm{PG}(n,q)$-ban egy k-lefogó halmaz mérete legalább $\Theta(k) = \frac{q^{k+1}-1}{q-1}$. Ha egyenlőség teljesül, akkor a lefogó ponthalmaz egy k-dimenziós altér.

3.4. Tétel (Heim, [5] Theorem 2.7.) Legyen B egy nem-triviális k-lefogó halmaz $\mathrm{PG}(n,q)$-ban, $n > k$, $q > 2$. Ekkor $|B| \geq \Theta(k) + q^{k-1} r_2(q)$. Amennyiben egyenlőség teljesülne, akkor B egy VB^* kúp, ahol V egy $(k-2)$-dimenziós altér, és B^* egy síkbeli lefogó ponthalmaz, amely mérete épp $q + 1 + r_2(q) = f_2(q)$.

3.5. Tétel (Bokler, [5] Theorem 2.11.) A legkisebb minimális k-lefogó ponthalmazok $\mathrm{PG}(n,q)$-ban (q négyzet, $q \neq 4$) olyan kúpok, amelyek csúcsának dimenziója $k-1-s$ és alapja egy Baer-részgeometria $\mathrm{PG}(2s, \sqrt{q})$, ahol $s = \min\{k, n-k\}$.

3.6. Tétel (Bokler, [5] Theorem 2.12.) Legyen B minimális k-lefogó ponthalmaz $\mathrm{PG}(n,q)$-ban ($q > 2$). Tegyük fel, hogy egy n' egész számra teljesül, hogy $k \leq n' \leq 2k$ és $|B| \leq \Theta(k) + \Theta(n'-k-1) r_2(q) q^{2k-n'}$. Ekkor B dimenziója legfeljebb n'. Ha egyenlőség teljesül, akkor a B méretére vonatkozó becslésben is egyenlőségnek kell teljesülnie, sőt B struktúrája is leírható.

3.2. Levetítős módszer

Ebben a részben egy – az eddigi módszerektől: leszámlálás, hézagos polinom vizsgálata jelentősen eltérő – újabb technikát fogunk röviden ismertetni, méghozzá a *levetítős módszert*. Az utolsó fejezetben sokszor használjuk majd a [4] cikk egy állítását (itt a 4.3), amelynek a [4]-beli bizonyítása folyamán a szerzők többször is alkalmazzák ezt a gondolatot. A módszer lényege, hogy a lefogó ponthalmaznak egy alkalmasan megválasztott pontból egy megfelelő síkra való levetített képéből pontos következtetéseket tudjunk levonni a lefogó ponthalmaz struktúrájáról. Most a módszert csupán szemléltetni szeretnénk, ezért a [4] cikk negyedik fejezetében szereplő egyik bizonyítás levetítős gondolatmenetét közöljük vázlatosan.

A következő lemmában szereplő B legyen s-szeresen lefogó ponthalmaz PG$(3,q)$-ban ($q \geq 661$), amire teljesül, hogy $|B| = sq + c - \frac{(s-1)(s-2)}{2} < sq + q^{\frac{2}{3}} - \frac{(s-1)(s-2)}{2}$, ahol $s < < \min\{c_p q^{\frac{1}{6}}, \frac{q^{\frac{1}{4}}}{2}\}$ és $c < q^{\frac{2}{3}}$.

3.7. Lemma ([4] Lemma 4.4.) Tegyük fel, hogy α a PG$(3,q)$ egy olyan síkja, ami a B-t úgy metszi, hogy a metszet tartalmaz egy S-el jelölt egyenest vagy Baer-részsíkot. Legyen $r_1, \ldots, r_{s-1}$ az S-nek $s-1$ pontja. Ekkor $(B \setminus S) \cup \{r_1, \ldots, r_{s-1}\}$ egy $(s-1)$-szeresen lefogó halmaz.

Bizonyítás: (vázlat) Ha $\alpha \cap B$ tartalmaz egy S egyenest, akkor az állítás azonnal teljesül. Tehát feltehetjük, hogy $\alpha \cap B$ tartalmaz egy S Baer-részsíkot.

Tekintsünk egy $\beta \neq \alpha$ síkot PG$(3,q)$-ban. Ha $\beta \cap \alpha$ egy érintő egyenese S-nek, akkor S kitörlése után is még lesz legalább $s-1$ B-beli pont β-ban. Ha pedig $\beta \cap \alpha$ egy $(\sqrt{q}+1)$-szelő S-hez (S Baer-részsík, ezért ez a két eset lehetséges), akkor a következőt tehetjük:

Tegyük fel, hogy β legfeljebb $s-2$ olyan pontját tartalmazza B-nek, ami nem tartozik bele $S \cap \alpha \cap \beta$-ba is. Rögzítsünk egy $r \in \beta \setminus \alpha$ pontot, ami nem esik B-be. Vetítsük le B-t az r pontból az α síkra!

Ekkor a fentiek miatt legalább $(\sqrt{q}+3-s)$ darab $\alpha \cap S$-beli pont lesz egyszeres pont a B'-vel jelölt vetületben.

1. Tegyük fel, hogy az összes $S \cap \alpha \cap \beta$-beli egyszeres ponthoz található olyan rajtuk átmenő egyenese α-nak, ami teljesen B'-be esik. Ekkor létezik legalább $\frac{2+\sqrt{q}}{2}$ különböző teljesen B'-be eső egyenes. Ezeken az egyeneseken összesen legalább $\frac{(2+\sqrt{q})(q+1)}{2} - \frac{\sqrt{q}(\sqrt{q}+2)}{8}$ pont van, ez viszont ellentmond annak, hogy $|B'| < q^{\frac{1}{6}}q + q^{\frac{2}{3}}$.

2. Most tegyük fel, hogy létezik olyan $r_1 \in S \cap \alpha \cap \beta$ egyszeres pont, amin át nincsen teljesen B'-be eső egyenes. Megmutatjuk, hogy létezik egy r_1-en áthaladó s-szelő B'-höz. Ezt úgy igazolhatjuk, hogy indirekt feltéve, hogy minden r_1-en átmenő egyenes még tartalmaz legalább s egyéb vetületi pontot, leszámlálással (használva, hogy $s < q^{\frac{1}{6}}$) ellentmondásba ütközünk.

   Ezek után már alkalmazhatjuk a [4] cikkbeli *Theorem 3.2*-t és a *Lemma 3.3*-at, amelyek együttesen azt fejezik ki, hogy ez esetben r_1 egy „*hosszú*" egyenesekből álló egyértelmű duális Baer-részegyenesen van rajta (ahol a *hosszú* alatt azt értjük, hogy legalább $\sqrt{q} + s$ B-beli pontot tartalmaz). Ráadásul belátható, hogy ez a duális Baer-részegyenes egybeesik az S-nek az r_1-en átmenő duális Baer-részegyenesével (hasonlóan működik a bizonyítás, mint a [4] cikk *Lemma 3.9*-ében). Így $\beta \cap \alpha$ is tartalmaz legalább $\sqrt{q} + s$ pontot, emiatt pedig β tartalmaz legalább $s - 1$ darab pontot $B \setminus S$-ből. Ahhoz pedig, hogy α-t is biztosan legalább $s - 1$ pontban messük hozzáadunk $B \setminus S$-hez még legfeljebb $s - 1$ darab α-beli pontot. □

4. Többszörös $(n-k)$-lefogó halmazok nem négyzetrendű projektív terekben

A [3] cikk a minimális többszörös $(n-k)$-lefogó ponthalmazokat karakterizálja bizonyos feltételek mellett abban az esetben, ha a többdimenziós projektív tér rendje négyzetszám. Mi azt vettük észre, hogy a [3] cikkben szereplő gondolatmenet lényegében ugyanúgy fog működni akkor is, ha a projektív tér rendje nem négyzetszám. Nagyon fontos megemlítenünk a nem négyzet és a négyzet eset közötti lényeges különbséget, miszerint a nem négyzet esetben Baer-részgeometriák nem léteznek. Így a [3] cikkben szereplő összes Baer-részgeometriákra vonatkozó (főleg) technikai állításokat teljesen átugorjuk majd. Ebben a fejezetben tehát végig fogjuk követni a [3] cikk által mutatott utat és karakterizáljuk a minimális t-szeresen $(n-k)$-lefogó ponthalmazokat q nem négyzet esetben.

Először beidézünk néhány állítást, amiket többször fogunk alkalmazni a karakterizáció bizonyítása során.

4.1. Tétel ([2] Theorem 5.3., [3] Theorem 2.1.) Legyen B minimális, t-szeresen $(n-k)$-lefogó ponthalmaz PG(n,q)-ban ($n \geq 2$), hogy $|B| = tq^{n-k} + t + k'$, ahol $t + k' \leq \frac{q^{n-k}-1}{2}$. Tegyük fel, hogy $q = p^h$, p prím, $h \geq 1$ és hogy B minden k-dimenziós alteret t (mod p^e) pontban metsz, ahol e a lehető legnagyobb, amire ez még teljesül. Jelölje $E = p^e$. Ha $2t < E$, akkor:

$$tq^{n-k} + \frac{q^{n-k}}{E+1} - 1 \leq |B| \leq tq^{n-k} + \frac{2tq^{n-k}}{E}.$$

4.2. Tétel ([2] Corollary 5.4., [3] Theorem 2.2) Legyen B t-szeresen $(n-k)$-lefogó ponthalmaz PG(n,q)-ban. Tegyük fel, hogy $q = p^h$, p prím, $h \geq 1$ és hogy B minden k-dimenziós alteret t (mod p^e) pontban metsz, ahol e a lehető legnagyobb, amire ez még teljesül. Jelölje $E = p^e$-t. Ha $\max\{2t,4\} < E$, akkor:

$$|B| \leq tq^{n-k} + \frac{2tq^{n-k}}{E} \qquad \text{vagy} \qquad |B| \geq Eq^{n-k} + t.$$

4.3. Tétel ([4] Theorem 5.9., [3] Theorem 3.1) Legyen B t-szeresen 1-lefogó halmaz PG(n,q)-ban, $q = p^h$, p prím, $q \geq 661$, $n \geq 3$. Tegyük fel, hogy $|B| < tq + c_p q^{\frac{2}{3}}$, ahol $c_2 = c_3 = 2^{-\frac{1}{3}}$, $c_p = 1$ $p > 3$ esetén, és $t < \frac{1}{2}c_p q^{\frac{1}{6}}$. Ekkor B tartalmazza t darab páronként diszjunkt egyenes vagy Baer-részsík unióját.

A továbbiakban az állításokat már bizonyítani is fogjuk, ugyanis a [3] cikkben ettől a ponttól kezdve a B t-szeresen $(n-k)$-lefogó ponthalmazról felteszik, hogy bármely k-dimenziós alteret nemcsak, hogy legalább t pontban, hanem $t \pmod{\sqrt{q}}$ pontban metsz, ahol q (a projektív tér rendje) négyzetszám. Mi viszont most a q nem négyzet esettel foglalkozunk, ezért minden olyan helyen, ahol az eredeti cikkben $\sqrt{q}$-s modulust használnak, ott mi $\sqrt{pq}$-s modulust fogunk használni.

A most következő lemmához tegyük fel B-ről, hogy minimális, t-szeresen $(n-k)$-lefogó $\mathrm{PG}(n,q)$-ban, ahol $q = p^h$, p prím, $q \geq 661$, $n \geq 3$ és B minden k-dimenziós alteret $t \pmod{\sqrt{pq}}$ pontban metsz. Tegyük fel továbbá, hogy $|B| < tq^{n-k} + c_p q^{n-k-\frac{1}{3}}$, ahol $c_2 = c_3 = 2^{-\frac{1}{3}}$ és $c_p = 1$ $p > 3$, és $t < \frac{1}{2} c_p q^{\frac{1}{6}}$.

Vegyük észre, hogy a 4.2-es tételt nemcsak p^e-re alkalmazhatjuk, hanem tetszőleges kisebb E-re is, amire $t \pmod{E}$ teljesül, hiszen ekkor csak kevésbé éles becslést kapunk a lefogó ponthalmaz méretére. Ezért a továbbiakban legyen $E = \sqrt{pq}$.

4.4. Lemma ([3] Lemma 3.2) Ha Π egy $(k+1)$-dimenziós altér, ami B-t egy **nem** minimális t-szeres 1-lefogóban metszi, akkor

$$|\Pi \cap B| \geq qE + t.$$

Bizonyítás: Mivel $\Pi \cap B$ minden Π-be eső k-dimenziós alteret $t \pmod{E}$ pontban metsz (tehát a $\Pi \cap B$ a Π-ben egy speciális 1-lefogó), így a 4.2 miatt, mivel $2t < E$ és így $\max\{2t,4\} < E$:

$$|\Pi \cap B| \leq tq + \frac{2tq}{E} \qquad \text{vagy} \qquad |\Pi \cap B| \geq qE + t.$$

Indirekt tegyük fel, hogy $|\Pi \cap B| \leq tq + \frac{2tq}{E} = tq + 2t\sqrt{\frac{q}{p}}$, vagyis a $2t < c_p q^{\frac{1}{6}}$ feltevés miatt: $|\Pi \cap B| \leq tq + 2t\sqrt{\frac{q}{p}} < tq + c_p q^{\frac{1}{6}}\sqrt{q} < tq + c_p q^{\frac{1}{6}+\frac{1}{2}} = tq + c_p q^{\frac{2}{3}}$. Ez azt jelenti, hogy alkalmazhatjuk a 4.3 tételt, ahonnan kapjuk, hogy $\Pi \cap B$ tartalmaz t páronként diszjunkt egyenest (mivel q nem négyzet, így Baer-részsíkokról nem beszélhetünk). Viszont $\Pi \cap B$ nem minimális 1-lefogó Π-ben, így azokat a pontjait $\Pi \cap B$-nek, amiket ez a t egyenes meghatároz nevezzük el S_1-nek, a további pontjait pedig S_2-nek.

Tekintsük S_2-nek egy tetszőleges r pontját. Ekkor létezik Π-ben egy r-re illeszkedő L egyenest, ami B-t csak r-ben metszi, mivel a Π altéren belül $q^k + q^{k-1} + \cdots + q + 1$ darab egyenes van, ami r-re illeszkedik, és $|\Pi \cap B| \leq tq + \frac{2tq}{E} < q^k + q^{k-1} + \cdots + q + 1$.

Ugyanezzel a skatulya-elves gondolattal találhatunk olyan Π_2 2-dimenziós alteret, ami L-et tartalmazza, és nem tartalmaz r-en kívül más B-beli pontot, majd egy Π_3 3-dimenziósat, ami tartalmazza Π_2-t és nem tartalmaz újabb B-beli pontot… végül találhatunk olyan Π_{k-1} $(k-1)$-dimenziós alteret, ami tartalmazza az eddigieket és még mindig csak egyetlen B-beli pontja van, az r.

Π-ben pontosan $(q + 1)$ darab k-dimenziós altér van, ami magában foglalja a Π_{k-1}-et. Ezen k-dimenziós alterek S_1-et pont $t \pmod{E}$ pontban metszik, ugyanis a Π-beli k-dimenziós alterek az S_1 egyeneseit rendre egy-egy pontban metszik. A B ponthalmaz $(n - k)$-lefogósága miatt viszont ezek a k-dimenziós alterek B-t is $t \pmod{E}$ pontban metszik, ahonnan következik, hogy tetszőleges ilyen k-dimenziós altér még tartalmaz r-en kívül legalább $(E - 1)$ pontot S_2-ből. Ezért:

$$|\Pi \cap B| \geq 1 + (q + 1)(E - 1) + t(q + 1).$$

Viszont tudjuk ($h = 2l-1$ mellett), hogy $|\Pi \cap B| \leq tq + 2t\sqrt{\frac{q}{p}} = tq + 2tp^{l-1} < tq + p^{2l-1}$, mert $2t < E = \sqrt{pq} = p^l$. Fent pedig azt kaptuk, hogy $|\Pi \cap B| \geq tq + t - q + (q+1)\sqrt{pq} =$ $= tq + t - p^{2l-1} + (p^{3l-1} + p^l)$, így:

$$p^{2l} \geq 2p^{2l-1} \geq p^{3l-1} + p^l + t$$

Ami pedig ellentmondás. Tehát bebizonyítottuk, hogy $|\Pi \cap B| \geq qE + t$. $\square$

Most egy darabig tételezzük fel B-ről, hogy egy minimális, t-szeresen **2-lefogó** halmaz $\mathrm{PG}(n, q)$-ban, ami minden $(n-2)$-dimenziós alteret $t \pmod{\sqrt{pq}}$ pontban metsz, ahol $q = p^h$, $h = 2l - 1$, így $\sqrt{pq} = E = p^l$. Tegyük fel továbbá, hogy:

$$|B| \leq tq^2 + \frac{2tq^2}{E} < tq^2 + c_p q^{\frac{5}{3}},$$

ahol $q > 661$ és $t < \frac{1}{2} c_p q^{\frac{1}{6}}$.

A $t \pmod{E}$ feltétel miatt minden $(n-1)$-dimenziós Π altérre a 4.2 és a 4.4 miatt:

$$|\Pi \cap B| \leq tq + \frac{2tq}{E} \qquad \text{vagy} \qquad |\Pi \cap B| \geq qE + t$$

teljesül. A fejezet hátralevő részében a 4.4 bizonyításában már megismert leszámlálási ötletet fogjuk többször alkalmazni, és a következő állítás is kulcsfontosságúnak fog bizonyulni. Most azt szeretnénk megmutatni, hogy a B t-szeresen 2-lefogó ponthalmazunk t darab páronként diszjunkt sík uniójaként áll elő. Ehhez először igazoljuk, hogy egy nem teljesen B-beli egyenes (aminek nem az összes pontja B-beli) kifejezetten kevés B-beli pontot tartalmaz. Ezután belátjuk, hogy a B-beli pontokon egészen sok teljesen B-beli egyenes halad át, amiből végül arra a következtetésre fogunk jutni, hogy B-nek tartalmaznia kell teljes síkot, ahonnan t szerinti indukcióval készen leszünk.

4.5. Lemma ([3] Lemma 4.2.) Legyen L egy egyenes $\mathrm{PG}(n, q)$-ban, ami nincs teljesen B-ben, ekkor $|L \cap B| \leq t$.

<u>**Bizonyítás:**</u> A 4.4 bizonyításában már használt ötlet miatt létezik olyan Π_{n-3} $(n-3)$-dimenziós altér, ami L-et tartalmazza, de nem tartalmaz B-be eső pontot az L esetleges pontjain kívül (vagyis $B \cap \Pi_{n-3} \subseteq L$).

Ekkor található Π_{n-3}-hoz olyan Π_{n-2} $(n-2)$-dimenziós altér, ami tartalmazza Π_{n-3}-at, és $|(\Pi_{n-2} \setminus \Pi_{n-3}) \cap B| \leq t$, mivel egy adott $(n-3)$-dimenziós altéren át $(q^2 + q + 1)$ darab $(n-2)$-dimenziós altér van és most a feltevés miatt $|B| \leq tq^2 + \frac{2tq^2}{E} < tq^2 + c_p q^{\frac{5}{3}}$. Hasonlóan létezik olyan Π_{n-1} $(n-1)$-dimenziós altér, ami tartalmazza Π_{n-2}-t és $|(\Pi_{n-1} \setminus \Pi_{n-2}) \cap B| \leq tq + \frac{2tq}{E}$. Ekkor viszont (mivel L-ben legfeljebb q darab B-beli pont van)

$$|\Pi_{n-1} \cap B| \leq q + t + tq + \frac{2tq}{E} < p^{2l-1} + t + \frac{p^{3l-1}}{2} + p^{2l-1} < p^{3l-1} + t = qE + t$$

teljesül a feltevések miatt. Így alkalmazva a 4.2 eredményét következik, hogy $|\Pi_{n-1} \cap B| \leq$ $\leq tq + \frac{2tq}{E}$, ami viszont kisebb, mint $tq + c_p q^{\frac{2}{3}}$, így a 4.3 miatt $\Pi_{n-1} \cap B$-ben van t páronként diszjunkt egyenes (mivel most nincsen Baer-részsík). Ekkor a 4.4 miatt a metszet nem lehet nem minimális lefogó (akkor legalább $qE + t$ pontjának kellene lennie), tehát a metszet minimális lefogó. Vagyis a metszet pontosan ezen t darab páronként diszjunkt egyenes uniója.

Mivel L benne van Π_{n-1}-ben, de nincsen teljesen B-ben, ezért nem lehet ezen egyenesek egyike sem. Mivel minden másik egyenest legfeljebb 1 pontban metsz, ezért L-nek legfeljebb t pontja esik B-be. □

4.6. Lemma ([3] Lemma 4.3.) PG(n, q)-nak minden Π hipersíkja B-t t darab páronként diszjunkt egyenes uniójában vagy legalább $qE + t$ pontban metszi.

Bizonyítás: Ha $\Pi \cap B$-nek nincsen legalább $qE + t$ pontja, akkor a 4.2 miatt legfeljebb $tq + \frac{2tq}{E}$ pontja van, vagyis a 4.3 miatt tartalmazza t darab páronként diszjunkt egyenes unióját. A 4.4 miatt azonban a metszetnek minimálisnak kell lennie, következésképp $\Pi \cap$ $\cap B$ épp a t darab páronként diszjunkt egyenesnek az uniója. □

4.7. Következmény ([3]) Tetszőleges Π hipersíkra $|\Pi \cap B| \geq t(q + 1)$.

Bizonyítás: Ehhez elegendő igazolni, hogy $qE + t \geq t(q + 1)$, ami a $t < \frac{1}{2} c_p q^{\frac{1}{6}}$ feltétel miatt teljesül. □

Most megmutatjuk, hogy feltehető, hogy minden B-beli ponton sok teljesen B-beli egyenes halad át. Ehhez tekintsünk egy $(n - 2)$-dimenziós Δ alteret, ami t különböző pontban metszi B-t. A fenti 4.7 miatt tudjuk, hogy a Δ-n átmenő $(q + 1)$ hipersík mindegyike legalább $t(q + 1)$ pontban metszi B-t. Ha elhagyjuk B-ből a $(q + 1) \cdot tq$ különböző pontot (hiszen hipersíkonként legalább tq új B-beli pontot találunk), akkor

$$|B| - (q + 1)tq \leq tq^2 + \frac{2tq^2}{E} - tq^2 - tq = \frac{2tq^2}{E} - tq$$

felső becslést kapjuk a méretre. Ha egy Δ-n átmenő hipersík legalább $(qE + t)$ pontot tartalmaz B-ből, akkor az elhagyás után is még marad legalább $qE + t - t(q + 1) = qE -$ $- tq$ pont, ami a jobboldalba még beleszámít. Így pedig felső becslést kaphatunk az ilyen hipersíkok számára:

$$\frac{\frac{2tq^2}{E} - tq}{qE - tq} \le \frac{\frac{2tq^2}{E}}{qE - tq}.$$

A jobboldal viszont legfeljebb $2t$, hiszen

$$\frac{\frac{2tq^2}{E}}{qE - tq} \le 2t$$

$$2tq^2 \le 2tE(qE - tq) = 2tqE^2 - 2t^2qE = 2tq^2p - 2t^2qE \iff tE \le q(p-1) = E^2 - q,$$

ami t választása miatt teljesül.

Így pedig a további legalább $(q+1) - 2t$ darab Δ-n áthaladó hipersík a 4.6 miatt t páronként diszjunkt egyenes uniójában metszi B-t. Ebből adódik, hogy minden $\Delta \cap B$-beli ponton legalább $(q+1) - 2t$ teljesen B-beli egyenes halad át.

Mivel B minimális, ezért feltehető, hogy minden B-beli ponton legalább $(q+1) - 2t$ darab teljesen B-beli egyenes halad át.

4.8. Lemma ([3] Lemma 4.5.) Ha B-nek minden pontja legalább $(q+1)-2t$ teljesen B-beli egyenesen van rajta, akkor B tartalmaz egy teljes síkot.

Bizonyítás: Tekintsünk egy $(n-2)$-dimenziós Δ alteret, ami B-t pontosan t pontban metszi. Ekkor a fentiek miatt létezik legalább $(q+1) - 2t$ hipersík, ami tartalmazza Δ-t és amelyek B-vel vett metszete éppen t darab páronként diszjunkt egyenes uniója.

Legyen Π egy ilyen hipersík, és jelölje ezt a t egyenest $L_1, L_2, \ldots, L_t$. Legyen $r \in B \backslash \Pi$. Ez az r pont is legalább $(q+1) - 2t$ teljesen B-beli egyenesen van rajta. Ezen egyenesek bármelyike Π-t legalább egy, $B \cap \Pi = \cup_{i=1}^{t} L_i$-beli pontban metszik. Így a skatulya-elv miatt létezik olyan j, hogy L_j-t legalább $\frac{(q+1)-2t}{t}$ teljesen B-beli r-et tartalmazó egyenes metszi.

Tekintsük a $P := \langle r; L_j \rangle$ generált síkot. Ez a P sík B-t legalább $\frac{(q+1)-2t}{t}$ r-en átmenő B-beli egyenesben metszi, így minden r-re nem illeszkedő egyenes P-ben már legalább $\frac{(q+1)-2t}{t}$ B-beli pontot tartalmaz. Ha egy ilyen egyenes nincsen teljesen B-ben, akkor a 4.5 miatt legfeljebb t közös pontja lehet B-vel. Azonban $\frac{(q+1)-2t}{t} > t$ teljesül, ezért minden P-beli r-re nem illeszkedő egyenes teljesen B-beli. Ebből következik, hogy az egész P teljesen B-be esik, vagyis B tartalmaz egy teljes síkot. □

Ekkor $(B \setminus P)$ egy $(t-1)$-szeresen 2-lefogó halmaz, ami minden $(n-2)$-dimenziós alteret $t-1 \pmod{E}$ pontban metsz, ugyanis a P sík minden $(n-2)$-dimenziós alteret $1 \pmod{q}$ és így persze $1 \pmod{E}$ pontban metsz. Tehát a fenti megfigyelésekből indukcióval adódik a következő tétel.

4.9. Tétel ([3] Theorem 4.6.) Legyen B olyan minimális, t-szeresen 2-lefogó halmaz $\mathrm{PG}(n,q)$-ban, hogy $|B| \leq tq^2 + \frac{2tq^2}{E} < tq^2 + c_p q^{\frac{5}{3}}$ és tegyük fel, hogy bármely $(n-2)$-dimenziós alteret $t \pmod{\sqrt{pq}}$ pontban metsz. Tegyük fel továbbá, hogy $q \geq 661$, és $t < \frac{1}{2} c_p q^{\frac{1}{6}}$. Ekkor B t darab páronként diszjunkt sík uniója.

Az előző néhány oldalon szereplő eredmények alapján indukcióval szeretnénk igazolni hasonló jellegű állítást általában $(n-k)$-lefogó ponthalmazokra. Így megfogalmazzuk az indukciós hipotézisünket.

Indukciós hipotézis: Minden $1 \le j \le n-k-1$-re legyen B_j minimális t-szeresen $(n-k-j)$-lefogó halmaz $\mathrm{PG}(n,q)$-ban és legyen q nem négyzet, $q \ge 661$, $t < \frac{1}{2}c_p q^{\frac{1}{6}}$. Tegyük fel, hogy $|B_j| \le tq^{n-k-j} + \frac{2tq^{n-k-j}}{E} < tq^{n-k-j} + c_p q^{n-k-j-\frac{1}{3}}$, és hogy minden $(k+j)$-dimenziós alteret $t \pmod{\sqrt{pq}}$ pontban metsz. Ekkor B_j t darab páronként diszjunkt $\mathrm{PG}(n-k-j,q)$ uniója.

A továbbiakban legyen B minimális t-szeresen $(n-k)$-lefogó halmaz $\mathrm{PG}(n,q)$-ban, legyen q nem négyzet, $q \ge 661$, $t < \frac{1}{2}c_p q^{\frac{1}{6}}$, amelyre: $|B| \le tq^{n-k} + \frac{2tq^{n-k}}{E} < tq^{n-k} + c_p q^{n-k-\frac{1}{3}}$, és ami minden k-dimenziós alteret $t \pmod{\sqrt{pq}}$ pontban metsz (jelölje $E = \sqrt{pq}$).

4.10. Lemma ([3] Lemma 5.1.) $\mathrm{PG}(n,q)$-nak minden Π $(k+1)$-dimenziós altere B-t t darab páronként diszjunkt egyenes uniójában vagy legalább $qE+t$ pontban metszi.

Bizonyítás: Ugyanúgy, mint a 4.6 esetén. □

4.11. Lemma ([3] Lemma 5.2.) Legyen L egy nem teljesen B-beli egyenes $\mathrm{PG}(n,q)$-ban. Ekkor $|L \cap B| \le t$.

Bizonyítás: A 4.4 lemmában is használt szokásos leszámlálási ötlet miatt találhatunk olyan Π_{k-1} $(k-1)$-dimenziós alteret, amire $L \subseteq \Pi_{k-1}$ és $(\Pi_{k-1} \cap B) = L \cap B$, tehát L-en kívül más B-beli pontot nem tartalmaz. Továbbá a 4.5 bizonyításához hasonlóan létezik olyan Π_k k-dimenziós altér, amire $\Pi_{k-1} \subseteq \Pi_k$ és $((\Pi_k \setminus \Pi_{k-1}) \cap B) \le t$. Tehát $|\Pi_k \cap B| \le q+t$ adódik, hiszen $|L \cap B| \le q$, mert L nincsen teljesen B-ben.

Az indukciós hipotézis miatt a legkisebb t-szeres 1-lefogó halmaz, ami egy $(k+1)$-dimenziós altér B-vel vett metszeteként előáll: épp t darab páronként diszjunkt egyenes uniója. Tehát minden $(k+1)$-dimenziós altér Π_k-n keresztül legalább $(q+1)t-(q+t) = (t-1)q$ új pontját tartalmazza B-nek. Így legfeljebb $tq^{n-k} + \frac{2tq^{n-k}}{E} - (t-1)q(q^{n-k-1} + q^{n-k-2} + \cdots + q + 1)$ ezektől is különböző B-beli pont lehet.

Ha egy Π_{k+1} $(k+1)$-dimenziós altér $(\Pi_k \subseteq \Pi_{k+1})$ legalább $qE+t$ pontot tartalmaz B-ből, akkor ez még tartalmaz legalább $qE-q$ egyéb pontot $B \setminus \Pi_k$-ból. Mivel $(q^{n-k-1} + \cdots + q + 1)(qE-q) > tq^{n-k} + \frac{2tq^{n-k}}{E} - (t-1)q(q^{n-k-1} + \cdots + q + 1)$, így létezik legalább egy olyan

$(k+1)$-dimenziós Π_{k+1} altér, ami tartalmazza a Π_k alteret és aminek legfeljebb $tq + \frac{2tq}{E}$ pontja van B-ből. Következésképp ez a $(\Pi_{k+1} \cap B)$ egy minimális t-szeres 1-lefogó Π_{k+1}-ben, így a 4.4 miatt t darab páronként diszjunkt egyenes uniója. L pedig ezen egyenesek bármelyikével legfeljebb 1 metszéspontot létesít, ezért $|L \cap B| \leq t$. □

Ezután már igazolhatjuk a következő, kissé meglepően hangzó állítást.

4.12. Lemma ([3] Lemma 5.3.) Legyenek L_0, L_1 B-beli egyenesek, amelyek metszéspontja r. Ekkor $\langle L_0, L_1 \rangle \subseteq B$.

Bizonyítás: Tekintsük az $S := \langle L_0, L_1 \rangle$ síkot. Nyilvánvaló, hogy $|S \cap B| \leq q^2 + q + 1$. A 4.4 lemmabeli okoskodás miatt létezik olyan $(k-1)$-dimenziós Π_{k-1} altér, hogy $S \subseteq \Pi_{k-1}$ és $\Pi_{k-1} \cap B = S \cap B$.

Mivel $|B| < tq^{n-k} + q^{n-k-\frac{1}{3}}$ és Π_{k-1}-en át éppen $q^{n-k} + \cdots + q + 1$ darab k-dimenziós altér halad át, így létezik olyan Π_k k-dimenziós altér, ami tartalmazza Π_{k-1}-et és $|(\Pi_k \setminus \Pi_{k-1}) \cap \cap B| \leq t$. Hasonlóan mivel $|B| \leq tq^{n-k} + \frac{2tq^{n-k}}{E}$, így létezik Π_{k+1} $(k+1)$-dimenziós altér, ami tartalmazza Π_k-t és amire $|(\Pi_{k+1} \setminus \Pi_k) \cap B| \leq tq + \frac{2tq}{E}$. Így pedig $|B \cap \Pi_{k+1}| \leq (q^2 + q + 1) + + \left(tq + \frac{2tq}{E}\right) + t$.

Tekintsük az összes $(q^{n-k-2} + \cdots + q + 1)$ darab $(k+2)$-dimenziós alteret, ami Π_{k+1}-et tartalmazza. A fentiekben is használt skatulya-elves megfontolásokhoz hasonlóan kapjuk, hogy létezik $\Pi_{k+2} \supseteq \Pi_{k+1}$, amire $|(\Pi_{k+2} \setminus \Pi_{k+1}) \cap B| \leq tq^2 + \frac{2tq^2}{E}$, így pedig az előzővel együtt a következő felső becslés adódik: $|\Pi_{k+2} \cap B| \leq (t+2)q^2$.

Ugyanakkor a 4.2 és a 4.4 miatt tudjuk, hogy $|\Pi_{k+2} \cap B| \leq tq^2 + \frac{2tq^2}{E}$ vagy $|\Pi_{k+2} \cap \cap B| \geq q^2 E + t$, így a fenti számolásból látszik, hogy csak az első eset fordulhat elő. Most használva a 4.9 tételt azt kapjuk, hogy $\Pi_{k+2} \cap B$ t darab páronként diszjunkt sík uniója. Viszont mivel L_0 és L_1 metszik egymást $(\Pi_{k+2} \cap B)$-ben, ezért $S = \langle L_0, L_1 \rangle \subseteq B$. □

Most pedig működtetni fogjuk az indukciót. Legyen $r \in B$ és $\Delta_k \cong \mathrm{PG}(k, q)$ olyan, ami tartalmazza r-et és $|\Delta_k \cap B| = t$. A fenti megfontolásokat használva ismét adódik, hogy található olyan Δ_{k+1} (k+1)-dimenziós altér Δ_k-n át, amire $|(\Delta_{k+1} \setminus \Delta_k) \cap B| \leq tq + \frac{2tq}{E}$, vagyis a 4.10 miatt ez a metszet éppen t darab páronként diszjunkt egyenes uniója, tehát $|\Delta_{k+1} \cap B| = t(q+1) = tq + t$. Ugyanezt a skatulya-elves gondolatot használva egészen Δ_{n-2}-ig tudunk egymásba skatulyázott altereket találni, amelyek nem nagyon metszenek B-be, ami azt jelenti, hogy $|\Delta_{k+i} \cap B| \leq tq^i + \frac{2tq^i}{E}$.

Viszont az indukciós hipotézis miatt $(\Delta_{n-2} \cap B)$ t páronként diszjunkt $\mathrm{PG}(n-k-2, q)$ uniója, tehát $|\Delta_{n-2} \cap B| = t(q^{n-k-2} + q^{n-k-3} + \cdots + q + 1)$. A 4.2 miatt léteznek olyan H_1 és H_2 hipersíkok (a szokásos leszámlálási ötletet használva nemcsak az adódik, hogy nem lehet az összes nagyon B-be metsző, hanem az sem lehet, hogy egy híján a többi nagyon B-be belemetsző), amelyek tartalmazzák Δ_{n-2}-t és legfeljebb $|H_i \cap B| \leq tq^{n-k-1} + \frac{2tq^{n-k-1}}{E}$ pontját tartalmazzák B-nek. Így az indukciós hipotézist használva kapjuk, hogy ezen két hipersíknak a B-vel vett metszete t darab páronként diszjunkt $\mathrm{PG}(n-k-1, q)$ uniója.

Legyen tehát Π_1 és Π_2 $(n-k-1)$-dimenziós a fent megtalált teljesen B-beli alterek egy-egy példánya H_i-ben. Vagyis $\Pi_j \subseteq H_j \cap B$, $j = 1{,}2$ és tegyük fel, hogy $(\Pi_1 \cap \Delta_{n-2}) =$ $= (\Pi_2 \cap \Delta_{n-2}) =: \Pi$, ahol Π egy $(n-k-2)$-dimenziós altér. Ekkor legyen $\sigma := \langle \Pi_1, \Pi_2 \rangle$ generált altér, ami az előzőek miatt egy $(n-k)$-dimenziós altér. Ekkor σ teljesen B-be esik, ugyanis ha rögzítünk egy $s \in \sigma \setminus (\Pi_1 \cup \Pi_2)$ pontot, és tekintünk egy $r \in \Pi$ pontot, valamint egy rajtuk áthaladó R síkot, akkor mivel Π_j hipersíkja σ-nak, így $(\Pi_j \cap R)$ egy-egy egyenes (L_1, L_2), amik átmennek r-en. Így a 4.12 miatt $\langle L_1, L_2 \rangle = R \subseteq B$, viszont $s \in R$, így $s \in B$. Így a fentieket tetszőleges s-re alkalmazva azt kapjuk, hogy $\sigma \subseteq B$.

Most pedig használva a $t \pmod{E}$ feltételt kapjuk, hogy $B \setminus \Pi_{n-k}$ egy $(t-1)$-szeresen $(n-k)$-lefogó $\mathrm{PG}(n, q)$-ban, ami minden k-dimenziós alteret $(t-1) \pmod{E}$ pontban metsz. Így adódik a következő tétel:

4.13. Tétel ([3] Theorem 5.8.) Legyen B olyan minimális t-szeresen $(n-k)$-lefogó $\mathrm{PG}(n, q)$-ban, ami minden k-dimenziós alteret $t \pmod{\sqrt{pq}}$ pontban metsz. Tegyük fel, hogy $|B| \leq$ $\leq tq^{n-k} + \frac{2tq^{n-k}}{E} < tq^{n-k} + c_p q^{n-k-\frac{1}{3}}$, ahol $q \geq 661$, $t < \frac{1}{2} c_p q^{\frac{1}{6}}$. Ekkor B t darab páronként diszjunkt $\mathrm{PG}(n-k, q)$ uniója.

Bizonyítás: Legyen Δ_{n-2} egy $(n-2)$-dimenziós altér, ami B-t legfeljebb $tq^{n-k-2} + \frac{2tq^{n-k-2}}{E}$ pontban metszi. Ekkor a fentiek miatt található olyan $B_0 \subseteq B$ egyszeres $(n-k)$-lefogó halmaz, amire $B \setminus B_0$ egy $(t-1)$-szeres $(n-k)$-lefogó halmaz, ami minden k-dimenziós alteret $(t-1) \pmod{E}$ pontban metsz. Innen t szerinti indukcióval készen vagyunk. □

A karakterizációhoz még hozzátartozik, hogy megjegyezzük, hogy páronként diszjunkt $\mathrm{PG}(n-k, q)$-k uniója csak akkor fér el egymás mellett, ha $k > \frac{n}{2}$.

Hivatkozások

[1] Kiss György, Szőnyi Tamás, *Véges geometriák*, POLYGON KÖNYVTÁR, Szeged, (2001)

[2] S. Ferret, L. Storme, P. Sziklai, Zs. Weiner, *A t* mod *p result on weighted multiple $(n-k)$-blocking sets in* $\mathrm{PG}(n,q)$, Innovations in Incidence Geometry, **6-7** (2009), 169-188.

[3] S. Ferret, L. Storme, P. Sziklai, Zs. Weiner, *A characterization of multiple $(n-k)$-blocking sets in projective spaces of square order*, Adv. Geom., **14** (2012), 739-756.

[4] J. Barát, L. Storme, *Multiple blocking sets in* $\mathrm{PG}(n,q)$, *$n \geq 3$*, Des. Codes Cryptogr., **33** (2004), 5-21.

[5] A. Blokhuis, P. Sziklai, T. Szőnyi, *Blocking sets in projective spaces*, Chapter 3 in J. De Beute, L. Storme: Current research topics in Galois geometry, Nova Science Publishers, Inc., (2010), 57-80.

[6] Szőnyi Tamás, *A hézagos polinomok Rédei-féle elméletének néhány újabb alkalmazása*, POLYGON V. évf., Szeged, **2** (1994), 49-78.

[7] L. Lovász, A. Schrijver, *Remarks on a theorem of Rédei*, Studia Scient. Math. Hungary, **16** (1981), 449-454.

[8] L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, Birkhäuser Verlag, Basel, (1970)

[9] A. Blokhuis, *On the size of a blocking set in* $\mathrm{PG}(2,q)$, Combinatorica, **14** (1994), 111-114.

[10] J.W.P. Hirschfeld, L. Storme, *The packing problem in statistics, coding theory and finite projective spaces*, in Finite Geometries, Developments of Mathematics, Kluwer, (2001), 201-246.

[11] S. Ball, A. Blokhuis, *On the incompleteness of (k,n)-arcs in Desarguesian planes of order q where n divides q*, Geom. Dedicata, **74** (1999), 325-332.