Doktori értekezés tézisei

Kombinatorikus problémák a Galois-geometriákban

Szőnyi Tamás

Budapest, 1999.

1. Bevezetés

A véges geometriák a projektív tér axiomatizálásakor, szinte kuriózumként, mint véges modellek születtek meg a múlt században. Az 1940-es évektől kezdve tanulmányozták őket rendszeresen. Később csoportelméleti, illetve kombinatorikus szempontból is érdekeseknek bizonyultak, legújabban pedig a kódelméleti alkalmazások irányították a figyelmet a véges geometria bizonyos területeire. Számos olyan fontos csoport van, mely természetes módon szépen hat egy geometrián, vagy annak valamely részhalmazán. Kombinatorikai szempontból a véges geometriák, — szabályosságuk miatt — mint extremális problémák megoldásai fordultak elő. A geometriák közül a legszabályosabbak a testre épített terek, melyeket szoktak Galois-tereknek is nevezni.

A jelen dolgozatban 9 megjelent vagy közlésre elfogadott cikkemet gyűjtöttem össze a Galois-geometriák témaköréből. A Galois-geometriák a véges geometria egy az ötvenes években kialakult ága, mely véges terek kombinatorikusan definiált ponthalmazaival foglalkozik. A síkok illetve terek rendjét mindig q-val jelöljük, és csak a testre épített PG(n, q) Galois-terekkel foglalkozunk. Tipikus kérdések az alábbiak: mekkora lehet egy kombinatorikus tulajdonságokkal definiált PG(n, q)-beli ponthalmaz *maximális illetve minimális mérete*? Igen gyakran ilyen maximális vagy minimális méretet szolgáltat valamely klasszikus geometriai struktúra. Ilyenkor az a természetes kérdés, hogy a kombinatorikus tulajdonságok és az adott méret együtt *karakterizálják-e a klasszikus példát*. Ugyancsak jellegzetes kérdésfeltevés a maximális (minimális) méretű példák *stabilitása*: ha egy struktúra mérete közel maximális (vagy minimális), akkor vajon beágyazható-e maximális méretűbe (illetve tartalmaz-e minimális méretűt). A véges geométerek az ilyen stabilitási eredményeket *Segre típusú* tételeknek nevezik, mert ő látott be először ilyen jellegű tételeket Galois síkok íveire. Az *ívek* olyan PG$(2, q)$-beli ponthalmazok, melyeknek nem esik három pontjuk egy egyenesre. Igen gyakran az a helyzet, hogy a fentebb említett klasszikus struktúra valamely klasszikus geometriai objektum véges test feletti megfelelője (például kúpszelet, másodrendű felület, részsík, stb.). Máskor az extremális példát valamilyen algebrai módon lehet leírni (például a lefogó ponthalmazoknál a projektív háromszöget, vagy (k, n)-ívekre Denniston konstrukcióját kúpszeletsorból, stb.). Ennek megfelelően az alkalmazott módszerek is részben a klasszikus geometriából jönnek, részben kombinatorikai okoskodások, és igen gyakran algebrát (véges testek feletti polinomokat vagy görbéket) használnak. Ugyancsak tipikus jelenség, hogy pusztán kombinatorikus okoskodásokkal elég ritkán tudunk stabilitási tételeket bizonyítani.

A most vázolt kérdésfeltevésre a legjellemzőbb példa a *síkbeli ívek* elmélete. Először Bose meghatározta a legnagyobb ív méretét, majd Segre karakterizálta páratlan rendű síkokon a lehető legnagyobb íveket, mint kúpszeleteket (a kúpszeletet itt és a későbbiekben irreducibilis másodrendű görbe értelemben használjuk). Később stabilitási tétel is született (ugyancsak Segretől), mely szerint ha egy ív mérete legfeljebb $c\sqrt{q}$-val tér el (alkalmas c-re) a $(q+1)$-től, akkor az ív része kúpszeletnek (ha q páratlan). Ebben az elméletben a kúpszeletek a klasszikus példák, az algebrai módszer pedig görbék használata: a Menelaosz tétel általánosítása, majd a Weil becslés alkalmazása.

Hasonló a helyzet lefogó ponthalmazokra, csak itt a minimális méretű illetve ahhoz közeli lefogó ponthalmazok érdekesek. Ebben az esetben kombinatorikus okoskodásokkal könnyen látható, hogy a legkisebb méretű lefogó ponthalmaz egyenes kell legyen, így itt az igazi kérdés a stabilitási eredmény volt. Meglepő módon kombinatorikusan is be lehetett látni egy stabilitási tételt, mely Bruentől és Pelikántól származik. Ők azt mutatták meg, hogy ha egy lefogó ponthalmaz nem tartalmaz egyenest, akkor legalább annyi pontja van, mint egy $\sqrt{q}$-adrendű részsíknak, és ezek a Baer-részsíkok le is írják az extremális példákat. Kombinatorikusan megint nem lehetett ezt a tételt jelentősen megjavítani, ha a sík rendje nem volt négyzet. A javítás akkor sikerült, amikor Blokhuis hézagos polinomokat tudott alkalmazni a kérdés megválaszolására. Rédei 1970-ben megjelent *Hézagos polinomok véges testek felett* c. könyve volt az, amely a szükséges algebrai eszközöket kidolgozta ezen vizsgálatokhoz. Végül Blokhuis (1994) nevezetes dolgozatából kiderült, hogy prímrendű Galois-síkokon egyenest nem tartalmazó lefogó ponthalmaz legalább másfélszer akkora kell legyen, mint egy egyenes. Fontos megjegyezni, hogy egy speciális esetben ezt már Rédei könyvében megtalálhatjuk (Rédei–Megyesi tétel, 36. paragrafus).

A dolgozat három fejezetre tagolódik. Az első fejezet ívekkel, pontosabban azok magasabb dimenziós általánosításaival foglalkozik. (A fogalmakat ld. a 2.2 Definícióban). Itt a fő kérdés az, hogy magasabb dimenzióra hogyan lehet általánosítani a síkra megismert eredményeket. Az egyik irányban süvegekkel kapcsolatban becslést adunk a négy dimenziós tér legnagyobb süvegének méretére. Egy másik dolgozatunk ívekkel kapcsolatban Seroussi és Roth egy MDS kódokkal kapcsolatos kérdésére ad geometriai választ. Itt sikerült egy ív és egy momentumgörbe (azaz $\{(1, t, t^2, \ldots, t^{n-1}\} \cup \{(0, 0, \ldots, 0, 1)\})$ közös részének méretére olyan becslést adnunk (Leo Storme-val közösen), amely pontos, ha a dimenzió nem túl nagy q-hoz képest, sőt ezekben az esetekben egy stabilitási tételt is beláttunk.

A második és a harmadik fejezet (többszörösen) lefogó ponthalmazokkal és (k, n)-ívekkel foglalkozik. (A fogalmakat ld. a 3.2 Definícióban). A kilencvenes években két algebrai eljárás alakult ki ezen objektumok tanulmányozására, a hézagos polinomok illetve az algebrai görbék használata. A második fejezet a hézagos polinomos módszert mutatja be. A Blokhuis, Brouwer, Szőnyi [E] dolgozat volt az, amellyel ezen Rédei által kezdeményezett módszer új életre kelt (és egyben Blokhuis fentebb már említett eredményének is egy előfutára volt). A második dolgozat többszörösen lefogó ponthalmazokról szól. A fentebb említett Bruen–Pelikán tétel után talán meglepő, hogy többszörösen lefogó ponthalmazokra tisztán kombinatorikus eszközökkel nem ismert bizonyítás arra, hogy egy t-szeresen lefogó ponthalmaznak legalább annyi pontja van, mint t diszjunkt Baer-részsíknak. A Blokhuis, Storme, Szőnyi [F] dolgozat hézagos polinomok alkalmazásával és geometriai okoskodásokkal megintcsak egyszerre bizonyít stabilitási és karakterizációs tételt arra az esetre, ha t nem túl nagy q-hoz képest (és q négyzetszám).

Az utolsó fejezet algebrai görbéket használ lefogó ponthalmazokra és (k, n)-ívekre. Lényeges újdonság, hogy a görbéket a Rédei polinom közvetítésével rendeljük ponthalmazainkhoz, nem pedig a fentebb említett Segre-féle módon (Menelaosz-tétellel). Ezen a módon a p^2 rendű Galois síkokon a Baer-részsíkokra lehet stabilitási tételt mondani, azaz egy jelentős lépéssel túl lehet menni a Bruen–Pelikán féle eredményen. Pontosan azt bizonyítjuk, hogy PG$(2, p^2)$ egy sem egyenest, sem Baer-részsíkot nem tartalmazó lefogó ponthalmaza legalább másfélszer akkora, mint egy egyenes. Ugyancsak görbéket használó módszerrel (k, n)-ívekre is sikerült beágyazási tételt belátni.

Ezekről a módszerekről viszonylag részletesen a *Some applications of algebraic curves in finite geometry and combinatorics*, Surveys in Combinatorics 1997 (ed.: R. A. Bailey), *British*

Combinatorial Conference, London, 1997, LMS Lecture Note Series, 198–237 c. összefoglaló dolgozatomban lehet olvasni.

Végezetül néhány technikai megjegyzés: azoknál az általában régebbi eredményeknél, melyeket Hirschfeld *Projective Geometries over Finite Fields* c. [13] könyvének második kiadása is feldolgoz, csak az évszámot adtuk meg, teljes referenciát nem. A dolgozatban feldolgozott saját cikkek a tézisek végén találhatók, ezekre [A], [B], ... módon hivatkozunk. Az [A] dolgozatbeli [1] referenciát [A], ref.: [1] alakban idézzük.

A q elemű véges testet GF(q), a rá épített n dimenziós projektív teret PG(n, q), az affint AG(n, q) fogja jelölni. A terek alapvető geometriai, aritmetikai illetve algebrai tulajdonságait külön referencia nélkül felhasználjuk, és a klasszikus geometriából is ismert fogalmakat nem definiáljuk. Mindezek a [10, 11, 12, 13] könyvekben, valamint magyar nyelven Kárteszi Ferenc: *Bevezetés a véges geometriákba* című monográfiájában megtalálhatóak.

2. Ívek és süvegek Galois terekben

Leghamarabb az *ív* és az *ovális* fogalma alakult ki projektív síkokon, mint a kúpszeletek kombinatorikus általánosítása. Ezeket a fogalmakat Bose (1947) már a negyvenes években bevezette.

2.1. Definíció. *Egy Π_q q-adrendű projektív sík valamely $\mathcal{I}$ halmazát* ívnek *nevezzük, ha nincs három kollineáris pontja. Ha $|\mathcal{I}| = k$, akkor k-ívről is beszélünk. A $k = q + 1$ esetben az* ovális*, míg a $k = q + 2$ esetben a* hiperovális *elnevezést is használni fogjuk. Egy k-ív* teljes*, ha nincs benne $(k + 1)$-ívben, azaz ha tartalmazásra nézve maximális.*

Mint azt Bose (1947) megmutatta, egy k-ív méretére $k \leq q + 2$ mindig teljesül, és $k = q + 2$ csak akkor lehetséges, ha q páros. Galois síkokon az irreducibilis másodrendű görbék (kúpszeletek) mindig oválist adnak. Ha q páros, akkor a kúpszelet érintői egy ponton mennek át, ezt a — *magpont*nak nevezett — pontot hozzávéve a kúpszelet pontjaihoz hiperoválist kapunk. Ez az észrevétel Qvist-től (1952) származik.

A Galois-geometriák, vagy más szóval a testre épített síkok és terek elmélete akkor kapott igazán lendületet, amikor B. Segre 1955-ben belátta az alábbi alapvető eredményt.

Tétel. *(Segre (1955)) Páratlan q-ra* PG$(2, q)$*-ban minden ovális kúpszelet.*

Túl azon, hogy ez az eredmény meglepő, hiszen a klasszikus síkon nincs megfelelője, a bizonyításhoz kidolgozott módszer a „véges geometriai okoskodás" mintapéldája mind a mai napig. Ha a sík rendje páros, akkor a megfelelő állítás általában még úgy sem igaz, ha ovális helyett hiperoválist, kúpszelet helyett kúpszelet és magpontját mondunk. Több végtelen ovális-osztály is ismert, melyek ismertetésére most nem térünk ki. Ilyeneket maga Segre (1957), (1962) konstruált, majd később további példákat adott Glynn (1983), újabban pedig az oválisok és általánosított négyszögek kapcsolatát felhasználva több új osztályt talált Cherowitzo, Penttila, Pinneri, Royle, Payne és mások.

Ha a megfelelő fogalmakat és tételeket magasabb dimenzióra próbáljuk általánosítani, akkor már három dimenzióban is két természetes lehetőségünk van: vagy megtartjuk szó szerint, hogy „nincs három pont egy egyenesen", vagy pedig azt követeljük meg, hogy „nincs négy pont egy síkban". Így a *süveg*, illetve az *ív* fogalmához jutunk.

2.2. Definíció. *A* PG(n, q) *tér egy ponthalmazát* süveg*nek nevezzük, ha nincs három kollineáris pontja. Az* ív *olyan ponthalmaz, amelynek legalább* $n+1$ *pontja van és nincs* $n+1$ *pontja egy hipersíkban. A síkbeli esethez hasonlóan* k*-süvegről, illetve* k*-ívről beszélünk, ha a ponthalmaz* k *pontú. A süveg (illetve ív)* teljes*, ha tartalmazásra nézve maximális.*

Röviddel Segre fent említett síkbeli tételének megszületése után Barlotti (1955) és Panella (1955) kiterjesztették Segre tételét három dimenziós süvegekre.

Tétel. (Barlotti (1955), Panella (1955)) *Páratlan* q*-ra PG*$(3, q)$*-ban minden* (q^2+1)*-süveg elliptikus másodrendű felület.*

Az, hogy a legnagyobb süveg mérete (q^2+1), páratlan q-ra Bose síkbeli eredményéből könnyen következik, páros q-ra ($q > 2$) Qvist (1952) látta be. Itt tehát már nincs különbség a páros és a páratlan karakterisztika között. Annyi különbség azért megmarad, hogy páros q-ra vannak olyan (q^2+1)-süvegek, amelyek nem elliptikus másodrendű felületek (ezek a Suzuki–Tits ovoidok, melyek nem-négyzet q-ra léteznek). Barlotti (1965) azt a jelenséget is észrevette, hogy ha a süveg mérete nagyobb, mint q^2-q+6, akkor is igaz marad, hogy része kell legyen elliptikus másodrendű felületnek. Háromnál magasabb dimenzióban már nem tudjuk, hogy a legnagyobb méretű süvegnek hány pontja lehet. Barlotti (1965) azt is megmutatta, hogy három dimenziós beágyazási eredményéből a legnagyobb négy dimenziós süveg méretére felső becslés kapható. Mint azt később részletesen is említjük, ez a becslés elég messze van a sejtett igazságtól.

Maga B. Segre (1955) a másik irányban általánosította tételét. Megmutatta, hogy páratlan q-ra PG$(3, q)$ egy íve legfeljebb $q+1$ pontot tartalmaz, és egyenlőség pontosan akkor áll, ha az ív harmadrendű térgörbe (szokták momentumgörbének is nevezni), azaz projektíve ekvivalens az $\{(1, t, t^2, t^3) : t \in \mathrm{GF}(q)\} \cup \{(0, 0, 0, 1)\}$ halmazzal. Ha egy három dimenzióbeli ívet egy pontjából levetítünk egy síkra, akkor természetesen síkbeli ív keletkezik, csak a méret csökken eggyel. Így Segre a bizonyítás során azt is belátta, hogy páratlan q-ra PG$(2, q)$ q-ívei mindig kúpszelet részei. Páros q esetén itt is csökken a páros és páratlan karakterisztika közti különbség: Casse (1969) belátta, hogy páros q-ra is legfeljebb $q+1$ pontúak lehetnek PG$(3, q)$ ívei, azonban még itt is vannak a fenti harmadfokú térgörbétől különböző $(q+1)$-ívek. Azt is belátta, hogy a $(q+1)$-ívek hiperbolikus másodrendű felületen vannak. A három dimenziós $(q+1)$-íveket később Casse és Glynn (1982) teljesen leírta. Ezek az ívek az egyik Segre által talált oválís-osztállyal, a transzláció-oválisokkal vannak kapcsolatban. Négy dimenzióban azonban, ha q elég nagy, akkor már csak a momentumgörbék $(q+1)$-ívek. Természetes ötlet a magasabb dimenziós esetet visszavezetni — ismételt vetítésekkel — a síkbeli esetre, és aztán a síkbeli karakterizációt felhasználva leírni a magasabb dimenziós íveket. Ez az ötlet persze a síkbeli esetben nagyon pontos eredményt igényel. Ilyet a q páratlan esetben Segre tétele szolgáltat, a q páros esetben ez a kiinduló dimenzió négy lesz.

Ezen motiváció alapján már az ötvenes években megfogalmazódott a következő alapvető kérdés.

Kérdés. Milyen méretűek lehetnek $\mathrm{PG}(2, q)$ teljes ívei?

Ezt a kérdést teljesen általánosan is kezelhetjük, és így azt is magában foglalja, hogy például mekkorák $\mathrm{PG}(2, q)$ legkisebb teljes ívei, vagy hogy milyen intervallumokban vannak minden intervallumbeli méretre teljes ívek, stb. Erre a kérdésre most nem térünk ki, egy viszonylag részletes áttekintés [22]-ben található.

Az ívek és süvegek egy fontos alkalmazása kódelméletben van. Ennek megértéséhez definiáljuk a lineáris kódokat.

2.3. Definíció. *Legyen F a* $\mathrm{GF}(q)$ *test, $V = V_n$ pedig az erre épített n dimenziós vektortér. Két vektor* Hamming-távolsága *a különböző koordináták száma. Egy vektor* súlya *a nullvektortól való Hamming-távolsága. Az $x, y \in V$ Hamming-távolságát $d(x, y)$, $x \in V$ súlyát $w(x)$ jelöli. Ha C k-dimenziós altere V-nek, akkor C-t $[n, k]$-kódnak nevezik. Az altér egy bázisát $k \times n$-es mátrixba írva a kód egy* generátor-mátrixát *kapjuk. A C minimális súlya (vagy távolsága; lineáris kódokra ez a két dolog egybeesik) d, ha*

$$d = \min\{d(x, y) \ : \ x, y \in C, \ x \neq y\}.$$

Egy d minimális súlyú lineáris $[n, k]$-kódra az $[n, k, d]$-kód elnevezést szokás használni. A kód $e = [(d-1)/2]$ hibát képes javítani. Ha H olyan mátrix, melynek sorai ortogonálisak C elemeire (azaz $x \in C$ akkor és csak akkor, ha $xH^T = 0$), akkor H-t a C kód paritás-ellenőrző mátrix*ának nevezzük.*

A kódok, valamint bizonyos geometriai objektumok kapcsolatát az alábbi tény mutatja.

Állítás. A C kód minimális súlya d, ha a H paritás-ellenőrző mátrix bármely $d-1$ oszlopa független, de van olyan d oszlop, amely nem.

A triviális eseteket elkerülendő, tegyük fel, hogy H-nak nincs két összefüggő oszlopa. A fenti állítás alapján a C lineáris kód helyett tekinthetjük egy paritás-ellenőrző mátrixának oszlopait, mint egy alkalmas projektív tér pontjait. Ez a tér persze szintén $\mathrm{GF}(q)$ feletti, dimenziója $r = n - k - 1$, a szóbanforgó ponthalmaz mérete n. Ugyancsak azonnali következménye a fenti állításnak az ú. n. Singleton korlát, mely szerint $d \leq n - k + 1$. Nézzük meg, mikor lehet itt egyenlőség: az ilyen kódokat *MDS (maximum distance separable) kódok*nak nevezik. Ekkor H bármely $n - k$ oszlopa független, azaz az oszlopok halmaza n-ívet alkot $\mathrm{PG}(n - k - 1, q)$-ban. Hasonlóan, a süvegek olyan kódokkal állnak kapcsolatban, amelyeknek minimális súlya 4. Ha a süveg teljes, akkor a szóbanforgó kód fedési sugara 2 lesz. A legnagyobb süveg illetve ív elemszámának meghatározása kódelméleti szempontból azért érdekes, mert esetünkben a kód kodimenziója és minimális súlya adott, tehát minél hosszabb a kód, annál kevésbé redundáns. Ilyen kódokat többen vizsgáltak, lásd G. Cohen, I. Honkala, S. Lytsin, A. Lobstein [8] monográfiáját. A kódelméleti vonatkozásokra még visszatérünk.

Most a Segre tétel térbeli kiterjesztése kapcsán mi csak a második legnagyobb síkbeli ív méretére koncentrálunk. Még általánosabban, bevezethetjük az alábbi jelöléseket, és sík helyett tetszőleges dimenzióban kérdezhetjük, hogy mekkora a legnagyobb ív vagy süveg, valamint mekkora a második legnagyobb teljes ív vagy süveg mérete.

2.4. Definíció. *Jelölje $m_2(n,q)$ a* PG(n,q) *legnagyobb, $m_2'(n,q)$ pedig a második legnagyobb teljes süvegének méretét.*

Hasonlóan jelölje $m(n,q)$ a PG(n,q) *legnagyobb, $m'(n,q)$ a második legnagyobb teljes ívének méretét.*

Mivel a konkrét becsléseket nem használjuk, csak Segre eredeti eredményeit említjük.

Tétel. (1) *$m'(2,q) \leq q - \sqrt{q} + 1$, ha $q = 2^{2h}$ (*Segre (1967)*),*

(2) *$m'(2,q) \leq q - \frac{\sqrt{q}}{4} + \frac{7}{4}$, ha q páratlan (*Segre (1967)*).*

Ezeket az eredményeket Voloch, majd Hirschfeld és Korchmáros lényegesen megjavították a nyolcvanas, kilencvenes években. A másik irányban nagyon kevés ismert: Kestenband (1981), Ebert (1985), Fisher–Hirschfeld–Thas (1986), valamint Boros–Szőnyi (1986) példát adtak teljes $(q - \sqrt{q} + 1)$-ívekre, ha $q > 4$ négyzet. Azaz $m'(2,q) \geq q - \sqrt{q} + 1$, ha $q > 4$ négyzet, amiből az (1) alatti Segre-becslés élessége következik. A q nem-négyzet esetben az ismert példák mérete $q/2$ körül van.

Ezekhez a nevezetes ciklikus $(q - \sqrt{q} + 1)$-ívekhez csatlakozik az értekezés [D] dolgozata. A fenti $(q - \sqrt{q} + 1)$-ívek PG$(2,q)$ Singer-csoportjának alkalmas részcsoport-orbitjai. A [D] dolgozat egyrészt az eredetinél egyszerűbb bizonyítást ad arra, hogy ezek az orbitok ívek (a teljességet ezt tudva már nem nehéz belátni), másrészt szükséges és elégséges feltételt ad arra, hogy egy ilyen részcsoport-orbit ív legyen. Ennek segítségével azt is be tudtuk látni, hogy ha az orbit mérete kicsi, akkor a keletkező síkbeli ponthalmaz mindig ív. A módszer olyan, hogy automatikusan működik akárhány dimenzióra is, ilyenkor azonban egy aritmetikai feltétel is kell ahhoz, hogy a ciklikus részcsoport-orbitok süvegek legyenek. Végül jegyezzük meg, hogy Korchmárossal közös [16] dolgozatunkban a „kis" orbitok szerkezetét teljesen le tudtuk írni, valamint ezek segítségével a Fermat-görbe véges test feletti megoldásainak számát sikerült bizonyos esetekben pontosan meghatároznunk.

A jelen értekezés első két dolgozata a legnagyobb illetve második legnagyobb teljes süveg problémájához kapcsolódik: azt vizsgáltuk meg, hogy mekkora lehet $m_2'(3,q)$, ha ismerjük $m'(2,q)$ értékét. Ezután azt néztük meg, hogy $m'(2,q)$ illetve $m_2'(3,q)$ ismeretében hogyan lehet $m_2(4,q)$-ra becslést adni. Bizonyos értelemben a négy dimenziós tér kulcsszerepet játszik a legnagyobb süvegek vizsgálatában. A technikai értelemben azért, mert R. Hill (1978) egy eredménye becslést ad $m_2(n,q)$-ra $m_2(4,q)$ ismeretében:

$$m_2(n,q) \leq q^{n-4} m_2(4,q) - q^{n-4} - 2(q^{n-5} + \ldots + q + 1) + 1,$$

amúgy pedig azért, mert az $m_2(4,q)$-ra ismert legerősebb felső becslés nagyságrendje cq^3, a legjobb ismert süveg-konstrukció pedig csak Cq^2 méretű íveket szolgáltat. Érdekes, hogy Hill (1978) bizonyítása kódelméleti eszközöket használt. Újabban Veerecke adott Ph. D. értekezésében geometriai bizonyítást Hill becslésére. Fontos megemlítenünk, hogy a Hill-féle becslés nagyon gyenge eredményt ad, ha a dimenzió nagy. Erre az esetre Meshulam [17] belátta, hogy

$$m_2(n,q) \leq \frac{2}{n} q^n + \frac{2}{n-1} q^{n-1}.$$

Valójában Meshulam bizonyítása általánosabb a süvegek eseténél: azt mutatta meg hogy a p^s elemű elemi Abel csoportban egy olyan halmaz mérete, amely nem tartalmaz három tagú számtani sorozatot, legfeljebb $\frac{2}{s}p^s$ (igazából Meshulam eredménye még ennél is általánosabban Abel-csoportokra vonatkozik, de a teljes általánosságtól most eltekintünk.)

A mi eredményeink (a páros esetben Leo Storme-val, a páratlanban Nagy Gáborral közösen) az alábbiak.

2.5. Tétel. (Storme, Szőnyi [A], Thms. 2.7 és 3.1) *Ha* $q = 2^h$, $q \geq 64$*, akkor*

$$m_2^{'}(3, q) < q^2 - q + 2\sqrt{q} + 1.$$

Ugyanezen feltételek mellett

$$m_2(4, q) < q^3 - q^2 + 2q\sqrt{q} + 2q - 2\sqrt{q} + 1.$$

2.6. Tétel. (Nagy, Szőnyi [B], Thm. 1.1) *Ha* q *páratlan,* $M = \max\{m'(2, q), (5q + 19)/6\}$, *akkor*

$$m_2'(3, q) < qM + \frac{3}{4}(q + \frac{10}{3} - M)^2 - q - 1.$$

Ha $N = \max\{m_2'(3, q), (q^2 + 5q + 2)/2\}$ *és* q *továbbra is páratlan, akkor*

$$m_2(4, q) < qN + 2q^2.$$

Mindkét tétel bizonyítása geometriai és kombinatorikus okoskodásokra épít. A páros esetben a kombinatorikus, a páratlanban a geometriai (másodrendű felületsorok) érvelések dominálnak.

Érdemes áttekinteni a korábbi eredményeket is: páros q-ra Hirschfeld és Thas ([A], ref.: [6]) korábbi korlátja

$$m_2'(3, q) \leq q^2 - \frac{q}{2} - \frac{\sqrt{q}}{2} + 2$$

volt, páratlan q-ra Hirschfeld ([B], ref.: [4]) az

$$m_2'(3, q) \leq q^2 - \frac{1}{4}q^{3/2} + 2q$$

becslést látta be, ha $q \geq 67$. Ha figyelembe vesszük az $m_2'(2, q)$-ra ismert legjobb eredményeket, láthatjuk, hogy a 2.6 Tétel a korábban ismert eredménynél még akkor is jobb, ha q négyzet, a Storme-val közös korlát pedig nagyjából megduplázta a $(q^2 + 1)$-től való eltérésre adott korlátot

A teljesség kedvéért jegyezzük meg, hogy mindkét eredménynél egy kicsit jobb is ismert azóta. A páros esetben Ming Chu [7] belátta, hogy $m_2'(3, q) \leq q^2 - q + 5$ (ha $q \geq 8$), míg a páratlan esetben Storme, Thas és Veerecke [20] az

$$m_2(4, q) < (q + 1)(qM + \frac{3}{4}(q + \frac{10}{3} - M)^2 - q - 1 - M) + M$$

becslést látta be. Itt azonban érdemes megemlíteni, hogy $m'(2,q)$ becslése biztosan nem javítható, ha q négyzet, ugyanakkor az elképzelhető, hogy $m_2'(3,q)$ lényegesen kisebb q^2-nél még akkor is, ha q négyzet.

A Storme-val közös dolgozat azonban még egy fontos eredményt tartalmaz: megadtunk egy q-nál nagyobb nagyságrendű intervallumot, amelyben az esetleg létező nagy teljes süvegek mérete csak néhány, viszonylag rövid részintervallumban lehet. A részintervallumok alsó végpontja kb. $q^2 - q^{5/4}$. Ez az eredmény az egyetlen, amely azt jelzi, hogy valószínűleg páros q esetén is lényegesen javítható $m_2'(3,q)$ felső becslése.

2.7. Tétel. (Storme, Szőnyi [C], Thm. 2.6) *Ha a olyan egész szám, melyre*

$$2 \leq a \leq \frac{-2\sqrt{q}+3+\sqrt{16q\sqrt{q}+12q-44\sqrt{q}-7}}{4\sqrt{q}+2},$$

és

$$k \in \left[q^2-(a-1)q+a\sqrt{q}+2-a+\binom{a}{2}, q^2-(a-2)q-a^2\sqrt{q}\right],$$

akkor $\mathrm{PG}(3,q)$*-ban, (q páros, $q \geq 64$), nincs teljes k-süveg.*

Ívekre vonatkozóan ugyanehhez a kérdéskörhöz kapcsolódik, bár meglehetősen lazán, a harmadik (szintén Leo Storme-val közös) cikk. A kérdést itt, kódelméleti indíttatásból, Seroussi és Roth (1986) tette fel. Mint azt fentebb említettük, az MDS kódok íveknek felelnek meg. A leggyakrabban használt (a CD-k is ezt használják) MDS kódok az ú. n. *Reed–Solomon kódok*, melyek geometriailag a momentumgörbének, pontosabban annak egy részhalmazának, felelnek meg. Kérdésük az volt, hogy lehet-e úgy bővíteni ezeket a kódokat, hogy az MDS tulajdonság megmaradjon. Geometriailag ez a következőt jelenti.

Kérdés. *(Seroussi–Roth (1986))* Legyen C a $\{1,t,t^2,\ldots,t^n\} \cup \{0,0,0,\ldots,1)\}$ momentumgörbe, $K \neq C$ pedig egy ív. Milyen nagy lehet $|K \cap C|$?

Persze, ha $|K \cap C|$-re tudunk alsó becslést mondani, akkor egyben az $m'(n,q)$-ra is lesz egy alsó becslésünk. A kérdést meg is fordíthatjuk: vegyünk egy $P \notin C$ pontot és becsüljük meg, hogy C-ről hány pontot tudunk úgy választani, hogy azok P-vel együtt is ívet alkossanak. Ha $n=2$, akkor ez a kúpszelettől különböző teljes ívek egyik nevezetes, Segre-től és Lombardo–Radice-től származó konstrukciója. Síkban a helyzet nagyon egyszerű, tekintsük azon P-n átmenő egyeneseket, amelyek metszik C-t, és válasszunk egy-egy pontot ezeken az egyeneseken. Így persze olyan halmazt kapunk, amely P-vel együtt is ívet ad és mérete $(q+3)/2$ vagy $(q+1)/2$, ha q páratlan, $(q+2)/2$, ha q páros. Lényegében ugyanez az okoskodás adja, hogy ennél több pontot nem is választhatunk C-ről a síkban. Ebből az esetből kiindulva indukcióval magasabb dimenzióban is lehet felső becslést adni $|K \cap C|$-re. Lényegében ezt tette Seroussi és Roth (1986), valamint némileg általánosabban és direkt módon Blokhuis, Bruen és Thas (1990). Ők az alábbi eredményt látták be:

$$|K \cap C| < n + \left[\frac{q+1}{2}\right], \quad \text{ha } n \geq 3,$$

ahol [.] az egészrész függvény.

Az eredmény hátránya, hogy a becslés a dimenzió növelésével romlik, valamint hogy csupán az $n = 2$ (síkbeli) esetben éles. Ezen némileg javított Storme és Thas (1991) a háromdimenziós eset részletes vizsgálatával, de a korlát továbbra is $n + f(q)$ alakú maradt alkalmas $f(q)$-val, bár már három dimenzióra is éles volt. A Leo Storme-val közös cikkekben ezeken a hátrányokon sikerült segíteni, azaz korlátunk éles, ha a dimenzió legfeljebb $0.09q + 2.59$, és ilyen n-ekre korlátunk nem függ n-től. Sőt ha a dimenzió legfeljebb ekkora, akkor le is tudjuk írni azokat a halmazokat, amelyekre a $|K \cap C|$ érték maximális. Mindenképp érdekes, hogy ez azt is mutatja, hogy magasabb dimenzióban a Segre, Lombardo–Radice konstrukció lényegében egyértelmű, ha kb. $q/2$ méretű íveket kívánunk szerkeszteni. A jelen értekezésben csak a q páros esetről szóló cikket találhatjuk meg, hasonló eredmény igaz a q páratlan esetre is, lásd [21].

A most következő tételben legyen q_0 az a legkisebb egész, melyre $(1+\sqrt{3})r_3(n) < 0.01n$, ha $n > q_0$. Itt $r_3(n)$ az $\{1, 2, \ldots, n\}$ legnagyobb olyan részhalmazának méretét jelöli, amely nem tartalmaz három tagú számtani sorozatot.

2.8. Tétel. (Storme, Szőnyi [C], Thm. 4.2) *Tekintsük az $L = \{(1, t, \ldots, t^n)||t \in GF(q)^+\}$ momentumgörbét, ha $q = 2^h, q \geq q_0, n \geq 4$, és legyen K olyan $(k + 1)$-ív PG(n, q)-ban, amelynek L-lel k közös pontja van. Ekkor $k \leq \frac{q}{2} + 1$. Ha $k \geq 0.41(q + 1) + n - 2$, és $K \setminus L = \{r\}$, akkor r az L görbe valamely érintőjén kell legyen.*

Tegyük fel, hogy r a $(0, \ldots, 0, 1) \in L$ pontbeli érintőn van, azaz $r(0, \ldots, 0, 1, a_1)$. Ekkor létezik GF(q) *additív csoportjának olyan H kettő indexű részcsoportja, hogy $K \cap L$ pontjainak paraméterei H (vagy H komplementerének) elemei és esetleg a $(0, \ldots, 0, 1)$ pont. Ha $(0, \ldots, 0, 1) \in K$, akkor K teljes, ha nem, akkor a $(0, \ldots, 0, 1)$-beli érintő egy pontjának hozzávételével teljessé tehető.*

Talán érdemes a bizonyítást is vázolni: először három dimenzióban látjuk be az állításokat. r-ből vetítve ívünket, olyan síkbeli ívet kapunk, mely egy racionális harmadrendű görbén van. A harmadrendű görbe pontjain bevezethető egy csoportművelet, és ívünk ezen csoport egy olyan részhalmaza, melyre $a + a' + a'' \neq 0$, ha a, a', a'' páronként különbözőek. Ha részhalmazunk elég nagy, akkor más lehetőség nincs, mint hogy részhalmazunk egy kettő indexű részcsoport a harmadrendű görbe csoportjában (mely esetünkben vagy ciklikus vagy elemi Abel). A csoportos állítás bizonyítása a Kneser tételt, valamint Szemerédi (ill. igazán csak a három tagú számtani sorozatokra vonatkozó Roth) tételét használja. Egy ilyen kettő indexű részcsoport algebrailag könnyen parametrizálható, amiből kiderül, hogy a kapott térbeli ív teljes. Itt a bizonyítás a Weil-becslést használja algebrai görbék véges test feletti pontjainak számáról. Ugyanez az észrevétel használható négy dimenzióban is, majd a magasabb dimenziós eset vetítésekkel és elemi geometriai okoskodásokkal kapható. Jegyezzük meg, hogy ezen a módon a dimenzióra való (esetünkben $0.09q$-s) becslés valószínűleg tovább javítható, de sokkal több számolással, és a legjobb, amit ettől a módszertől várhatunk, az kb. $n \leq q/6$.

3. Hézagos polinomok, lefogó ponthalmazok és (k, n)-ívek

A további cikkek jórészt lefogó ponthalmazokkal, valamint (k, n)-ívekkel kapcsolatosak. Mindkét fogalom igazából a hatvanas években alakult ki, noha a lefogó ponthalmaz fogalma már Neumann és Morgenstern 1948-ban megjelent játékelméleti könyvében is megtalálható.

3.1. Definíció. *Egy Π_q q-adrendű projektív sík valamely ponthalmazát* lefogó ponthalmaz*nak nevezzük, ha minden egyenest metsz. Ha a lefogó ponthalmaz nem tartalmaz egyenest, akkor* blokkoló ponthalmaz *a neve. Egy lefogó ponthalmaz* minimális*, ha tartalmazásra nézve az. (Ez geometriailag azt jelenti, hogy minden pontjában van olyan egyenes, amely csak ebben a pontban metszi a halmazt.)*

3.2. Definíció. *Egy Π_q q-adrendű projektív sík valamely ponthalmaza (k, n)-ív, ha k pontja van, minden egyenes legfeljebb n pontban metszi, és van olyan egyenes, amely pontosan n-ben. Egy (k, n)-ív* teljes*, ha nem része $(k + 1, n)$-ívnek. Egy ponthalmaz* t-szeresen lefogó *ponthalmaz, ha minden egyenest legalább t pontban metsz, és van olyan egyenes, amit pontosan t-ben.*

Ennek megfelelően, ha $n+t = q+1$, akkor a (k, n)-ívek és a t-szeresen lefogó ponthalmazok egymás komplementumai. Szokásosan akkor használjuk a t-szeresen lefogó halmaz illetve a (k, n)-ív elnevezést, ha t illetve n kicsi q-hoz képest.

Mint a definícióból látható, a (k, n)-ív $n = 2$-re visszaadja a k-ív fogalmát, így az alábbi Barlottitól (1965) származó eredmény a Bose tétel közvetlen megfelelőjének tekinthető.

Tétel. (Barlotti (1965)) *(k, n)-ívre $k \leq qn - q + n$, és egyenlőség csak akkor állhat, ha n osztja q-t.*

PG$(2, q)$-ban minden $n|q$-ra vannak $(qn - q + n, n)$-ívek, ha q páros (Denniston (1969)). Nemrégen Ball, Blokhuis és Mazzocca [3] megmutatták, hogy páratlan q-ra PG$(2, q)$-ban semmilyen $1 < n < q$-ra nincsenek ilyen (k, n)-ívek.

Lefogó ponthalmazokra a helyzet némileg hasonló: triviális, hogy minden lefogó ponthalmaz legalább $q + 1$ pontot tartalmaz és egyenlőség csak akkor áll, ha a halmaz egyenes. Ha viszont a lefogó ponthalmaz nem tartalmaz egyenest, akkor Bruen (1968) és Pelikán belátták, hogy mérete legalább $q + \sqrt{q} + 1$ és egyenlőség csak a $\sqrt{q}$-adrendű (Baer-)részsíkokra áll. Az ő bizonyításuk kombinatorikus (azaz minden q-adrendű síkra érvényes). Abban az esetben, ha q nem négyzet, a becslést tisztán kombinatorikus úton nem sikerült lényegesen javítani. Hosszú ideig csak az affin síkokra vonatkozó Jamison (1977), Brouwer–Schrijver (1978) dolgozat volt az, amely polinomos módszerével reményt nyújtott arra, hogy a testre épített síkokra jóval többet lehet belátni, mint általában.

Tétel. (Jamison (1977), Brouwer–Schrijver (1978)) AG$(2, q)$ *tetszőleges lefogó ponthalmaza legalább $2q - 1$ pontból áll.*

Ezt az eredményt felhasználva Blokhuis–Brouwer ([G], ref.: [5]), valamint Bruen–Silverman ([G], ref.: [14]) megmutatták, hogy ha q nem négyzet, akkor PG$(2,q)$ egy blokkoló ponthalmaza legalább $q+\sqrt{2q}+1$ pontú. Érdemes kiemelni, hogy a bizonyítás egy része már Rédei László 1970-ben megjelent könyvében megtalálható.

Lefogó ponthalmazok egy nevezetes családja a *Rédei típusú* lefogó ponthalmazoké. Legyen U az AG$(2,q)$ affin sík egy q pontú részhalmaza. Azt mondjuk, hogy egy (m) irányt (m meredekséget) U *meghatároz*, ha találunk U-ban két olyan pontot, melyek összekötő egyenese m meredekségű. Ha U egy függvény grafikonja, akkor a meghatározott (m)-ek $m=(f(x)-f(y))/(x-y)$ alakúak. A Rédei [19] által megválaszolt kérdés a következő.

Kérdés. *(Rédei (1970))* Legalább hány irányt határoz meg egy függvény grafikonja (azaz a különbségi hányados legalább hány értéket vesz fel)?

Ha a meghatározott irányok halmaza D (és $|D|\le q$), akkor $U\cup D$ könnyen láthatóan (minimális) lefogó ponthalmaz. Megfordítva, ha B olyan minimális lefogó ponthalmaz, melyre valamely ℓ egyenesre $|B\setminus\ell|=q$, akkor az $U=B\setminus\ell$ által meghatározott irányok halmaza éppen $D=B\cap\ell$ lesz, azaz a fenti kérdés ekvivalens a Rédei típusú (minimális) lefogó ponthalmazok méretének alsó becslésével.

Jane Di Paola (1969) kisrendű síkok ($q\le 7$) vizsgálatával már a hatvanas években azt sejtette, hogy prímrendű Galois-síkok egyenest nem tartalmazó lefogó ponthalmazai legalább $3(q+1)/2$ pontúak. Ez a kérdés hosszú ideig megoldatlan volt, elsősorban amiatt, hogy nem voltak megfelelő módszerek. Di Paola sejtését nemrégiben Blokhuis [4] bizonyította, s módszere néhány más hasonló becslést is kiadott nem-négyzet rendű síkokra, így például azt, hogy $q=p^3$ esetben blokkoló halmaz mérete legalább p^3+p^2+1. Mindkét eredmény éles, $3(q+1)/2$ méretű blokkoló ponthalmazra példa az ú. n. *projektív háromszög* (mely Rédei típusú, a pontok egy háromszög oldalain vannak elosztva), a $q=p^3$ esetben pedig a GF(p^3)-ből GF(p)-be vezető *nyom (trace) függvény* grafikonjából származó Rédei típusú blokkoló ponthalmaz a példa. Mindkét konstrukció megtalálható Rédei könyvének 36. Paragrafusában.

Blokhuis módszere szerves folytatása Rédei hézagos polinomos módszereinek. Még pontosabban, az értekezésben szereplő [E] dolgozat az, mellyel újra elkezdődött a polinomok alkalmazása projektív síkok lefogó ponthalmazaira. (Noha a cikk jóval később jelent meg, az eredeti kézirat 1990-ből származik.)

Rédei László *Lacunary polynomials over finite fields* című könyve ugyan érezhetően hasznos algebrai módszereket tartalmazott, de a könyv terjedelme miatt nem volt teljesen világos, hogy a véges geometriai kérdésekkel pontosan milyen kapcsolatban álltak az algebraiak. Igazából a Blokhuis, Brouwer, Szőnyi [E] dolgozat egyik lényeges része éppen annak tisztázása volt, hogy a geometriai kérdésekhez Rédei könyvének mely részeit szükséges megérteni.

3.3. Tétel. (Blokhuis, Brouwer, Szőnyi [E], Thm. 1) *Legyen $U\subset AG(2,q)$ ($q=p^n$) q pontú ponthalmaz, D pedig az U által meghatározott irányok halmaza. Legyen $N:=|D|$. Legyen e ($0\le e\le n$) a legnagyobb olyan egész szám, amelyre minden m ($(m)\in D$) meredekségű egyenes U-t p^e-vel osztható számú pontban metszi. Ekkor az alábbiak egyike áll fenn:*

(i) $e=0$ *és* $(q+3)/2\le N\le q+1$,

(ii) $1 \le e < n/3$, *és* $2 + (q-1)/(p^e+1) \le N \le (q-1)/(p^e-1)$,

(iii) $e = n/3$ *és* $N = p^{2e} + 1$ *vagy* $N = p^{2e} + p^e + 1$.

(iv) $e = n/2$ *és* $N = p^e + 1$,

(v) $e = n$ *és* $N = 1$.

Továbbá $N \equiv 1 \pmod{p^e}$, *és* $(q, N) \ne (16, 7)$.

A bizonyítás a Rédei-polinom vizsgálatára, és hézagos polinomokra vonatkozó eredményekre épít.

3.4. Definíció. *Legyen* $U = \{(a_i, b_i) : i = 1, \ldots, N\}$ *az* AG$(2, q)$ *egy ponthalmaza. U Rédei polinomja a*

$$H(X,Y) := \prod_{i=1}^{N}(X + a_iY - b_i) = X^N + h_1(Y)X^{N-1} + \ldots + h_N(Y)$$

kétváltozós polinom, ahol h_j*-nek, mint* Y *polinomjának a foka legfeljebb* j *(*$j = 1, \ldots, N$*).*

A 3.3 tételben a $q = p$ esetre vonatkozó ((i) vagy (v) lehet csak) eredmény Rédei és Megyesi tétele (24. Tétel, 36 Paragrafus, Rédei könyvében). Két évtizedig ez volt az egyetlen általános jele annak, hogy Di Paola sejtése igaz lehet, hisz ez Rédei típusú lefogó ponthalmazokra bizonyítja a sejtést. Ezt egyszerűbben Lovász és Schrijver (1981) is belátták, sőt ők azt is megmutatták, hogy a $(p+3)/2$ irányt meghatározó ponthalmazok egyértelműek (a belőlük származó blokkoló ponthalmazt szokták *projektív háromszög*nek nevezni.) Az újdonság a Blokhuis, Brouwer, Szőnyi [E] dolgozatban kettős, egyrészt általában is tudjuk, hogy az (i) esetben $(q+3)/2 \le N$, ami a Rédei [19] könyvében szereplő 7. probléma egy részére ad választ, másrészt (ii)-ben az $e < n/3$ korlát jobb, mint a Rédeinél szereplő $e < n/2$. Úgy tűnik, hogy az $N \equiv 1 \pmod{p^e}$ észrevétel sem szerepel explicite Rédei könyvében. Ez tette lehetővé, hogy az $e = n/3$ esetben N lehetséges értékeit pontosan meghatározzuk. A $(q, N) \ne (16, 7)$ arra ad példát, hogy még az $N \equiv 1 \pmod{p^e}$ feltétel mellett sem áll elő a (ii)-beli intervallumok minden eleme meghatározott irányok számaként. Permutációs polinomokkal Evans, Greene és Niederreiter [9] is belátta (i)-t tőlünk függetlenül.

Fontos megjegyezni, hogy később Blokhuis, Ball, Brouwer, Storme és Szőnyi [6] karakterizálták az olyan ponthalmazokat, melyek kevesebb, mint $(q+3)/2$ irányt határoznak meg.

Tétel. (Blokhuis–Ball–Brouwer–Storme–Szőnyi (1999)) *Ha U kevesebb, mint* $(q+3)/2$ *irányt meghatározó q pontú halmaz, akkor a fenti 3.3 Tétel szerint minden egyenes* 1 *modulo* p^e *pontban metszi. Ha* $p^e > 3$ *(vagy* $p^e = 3$ *és* $N = q/3 + 1$*), akkor létezik egy* GF(p^e) *résztestе* GF(q)*-nak, melyre U egy* GF(p^e) *feletti altér eltoltja.*

Pontosabban, ha mondjuk $q = q_1^h$, akkor AG$(2, q)$-t tekinthetjük egy a GF(q_1) feletti $2h$ dimenziós vektortérnek. Ha még $0 \in U$, akkor U h-dimenziós altér.

Blokhuis lefogó ponthalmazokra vonatkozó eredményei (lásd [4]) után természetesnek tűnt többszörösen lefogó ponthalmazokat vizsgálni. Ezt Ball és Blokhuis ([G], ref.: [1]), majd

Ball [1] kezdte el, a kétszeresen illetve háromszorosan lefogó ponthalmazok tanulmányozásával. Az Aart Blokhuis-szal és Leo Storme-val közös cikkünkben az általános esetre vonatkozó eredményt láttunk be, ha t nem túl nagy.

3.5. Tétel. (Blokhuis, Storme, Szőnyi [F], Thm. 1.1) *Legyen B s-szeresen lefogó halmaz* $\mathrm{PG}(2,q)$*-ban, q nem prím, melyre $|B| = s(q+1)+c$. Legyen $c_2 = c_3 = 2^{-1/3}$ és $c_p = 1$, ha* $p > 3$.

1. *Ha $q = p^{2d+1}$ és $s < q/2 - c_p q^{2/3}$, akkor $c \geq c_p q^{2/3}$.*

2. *Ha $4 < q$ négyzet, $s < q^{1/4}/2$ és $c < c_p q^{2/3}$, akkor $c \geq s\sqrt{q}$ és B tartalmazza s diszjunkt Baer részsík egyesítését.*

3. *Ha $q = p^2$, $s < q^{1/4}/2$ és $c < p\lceil \frac{1}{4} + \sqrt{\frac{p+1}{2}} \rceil$, akkor $c \geq s\sqrt{q}$ és B tartalmazza s diszjunkt Baer részsík egyesítését.*

A $q = p$ prím esetben Ball ([1]) belátta, hogy $|B| \geq (s + \frac{1}{2}(q+1))$, ha $s \leq (q-1)/2$, $|B| \geq (s+1)q$, ha $s \geq (q+1)/2$. Ugyancsak ő (illetve Ball és Blokhuis) dolgozta ki azt, hogy a Rédei polinomból hogyan lehet ügyesen hézagos polinomot csinálni többszörösen lefogó ponthalmazra. Ezután egy a fenti lemmánál pontosabb hézagos polinomos állítást látunk be, majd az abból nyert lokális információt használva kombinatorikusan építjük fel a diszjunkt Baer részsíkokat.

Jegyezzük meg, hogy a $t = 1$ esetben is van újdonság ebben a tételben. Ha ugyanis q nem négyzet, akkor a Blokhuis [4] becslés $|B| \geq q + \sqrt{pq} + 1$-et adott, ahol $q = p^h$, $h > 1$, páratlan, míg a fenti eredmény $|B| \geq q + q^{2/3} + 1$-et ad. Abban az esetben, ha q négyzet, akkor a fenti eredményből az kapható, hogy Baer-részsíkot nem tartalmazó lefogó ponthalmaz méretére $|B| \geq q + c_p q^{2/3} + 1$ teljesül (illetve a (3) alatti megfelelő becslés, ha $q = p^2$). Korábban erre csak a Ball és Blokhuis által bizonyított $|B| \geq q + 2\sqrt{q} + 1$ volt ismert. Erre a kérdésre a későbbiekben még visszatérünk.

4. Algebrai görbék, lefogó ponthalmazok és (k, n)-ívek

Az értekezés ezen fejezete algebrai görbék egy újfajta felhasználását mutatja Galois geometriákban. A korábban már említett becslések $m'(2,q)$-ra mind arra a Segre-től származó ötletre épülnek, hogy egy k-ív érintői benne vannak egy alacsony fokú ($q+2-k$, ha q páros, $2(q+2-k)$, ha q páratlan) algebrai vonalgörbében. B. Segre ezt a Menelaosz-tétel tetszőleges fokú görbékre való kiterjesztésével, valamint a gyakran *Segre-lemmának* nevezett trükkel mutatta meg. Meglepő, hogy az íveken kívül nem túl sok olyan problémát ismerünk, amelyben ez a szép ötlet alkalmazható lenne. Ugyanakkor sokáig semmilyen más ötlet sem volt ismert, amellyel bizonyos ponthalmazokhoz algebrai görbét rendelhetünk hozzá úgy, hogy a görbe tulajdonságai a ponthalmaz bizonyos kombinatorikus tulajdonságait tükrözzék. Az utolsó három feldolgozott cikk arra ad példát, hogy a korábban a polinomos módszereknél használt *Rédei polinom* hogyan használható arra, hogy algebrai görbéket asszociáljunk lefogó ponthalmazokhoz, (k, n)-ívekhez és esetleg más objektumokhoz.

A Rédei polinomnak (ld. 3.4) az a legfőbb haszna, hogy segítségével algebrai feltétellé (egy bizonyos gyök multiplicitása) fordíthatjuk le azt a geometriai feltételt, hogy az $Y = mX + b$ egyenes hány pontban metszi U-t. A Rédei polinom hátránya ugyanakkor, hogy foka nagy. A most következő mindhárom cikkben az történik, hogy a Rédei polinom felhasználásával alacsonyabb fokú polinomokat gyártunk, melyek még mindig tükrözik azt, hogy az egyenesek hány pontban metszik U-t, de elegendően sok pontjuk van $\mathrm{GF}(q)$ fölött ahhoz, hogy algebrai geometriai eredményeket (Weil becslés, Stöhr–Voloch módszer, vagy egyszerűen csak a Bézout tétel) tudjunk használni. Érdekes, hogy hasonlóan a teljes ívek általánosított Menelaosz tételre épülő B. Segre által kidolgozott elméletéhez, itt is olyan görbéket kapunk, melyeknek „sok" $\mathrm{GF}(q)$ feletti pontja van, valamint, hogy a ponthalmazok tartalmazásra vonatkozó minimalitása illetve maximalitása itt is a görbék lineáris komponenseivel van kapcsolatban.

Az első cikk ([G]) közvetlenül kapcsolódik a Rédei által felvetett kérdéshez. Azt vizsgáltuk meg, hogy ha egy ponthalmaz q-nál kevesebb, de majdnem q pontot tartalmaz, akkor mennyire csökkenhet a meghatározott irányok száma. Itt az alábbi eredményt sikerült megmutatni.

4.1. Tétel. ([G], Thm. 4) *Legyen U az $\mathrm{AG}(2,q)$ egy $q-n$ ($n \leq \sqrt{q}/2$) pontú ponthalmaza, mely a D-beli irányokat határozza meg. Ha $|D| < (q+1)/2$, akkor van olyan $V \supset U$ halmaz, melyre $|V| = q$ és V ugyanazokat az irányokat határozza meg, mint U.*

Általában csak kicsit kevesebb igaz, nevezetesen a következő tétel.

Tétel. *Ha $\mathrm{AG}(2,q)$ egy $q-n$ pontú, nem csupa kollineáris pontból álló ponthalmaza kevesebb, mint $(q+3-n)/2$ irányt határoz meg, akkor része olyan q pontú ponthalmaznak, mely ugyanazokat az irányokat határozza meg, mint az eredeti ponthalmaz.*

Az értekezésbeli cikkben ez csak a $q = p$ esetre található meg ([G], Remark 5), amikor egyszerűen azt mondhatjuk, hogy a ponthalmaz legalább $(p+3-n)/2$ irányt határoz meg. A [G]-ben csak említett hézagos polinomos okoskodás a [23] dolgozatban jelenik meg.

Az értekezésben szereplő következő cikk tetszőleges lefogó ponthalmazokra terjeszti ki Rédei eredményeit. Itt is azt mutatjuk meg, hogy egy lefogó ponthalmaz mérete $q = p^e$ esetén $1 + e/2$ darab intervallum valamelyikében kell legyen. A Rédei féle eredményhez (ld. [19], Thm. 24, illetve 3.3 Tétel) képest az itteni intervallumok kb. kétszer olyan hosszúak.

4.2. Tétel. ([H], Thms. 5.6, 5.12) *Legyen B minimális blokkoló halmaz $\mathrm{PG}(2,q)$-ban, $q = p^n$ és tegyük fel, hogy $|B| < 3(q+1)/2$. Ekkor van olyan $1 \leq e \leq n/2$ egész szám, hogy minden egyenes B-t 1 modulo p^e pontban metszi és*

$$q + 1 + \frac{q}{p^e+2} \leq |B| \leq \frac{qp^e + 1 - \sqrt{(qp^e+1)^2 - 4q^2p^e}}{2}, \tag{1}$$

Aszimptotikusan ez azt jelenti, hogy

$$|B| \leq q + \frac{q}{p^e} + 2\frac{q}{p^{2e}} + 5\frac{q}{p^{3e}} + \ldots$$

Speciálisan $|B| \leq q + 9q/(4p^e)$ minden p és e-re.

Jegyezzük meg, hogy a tétel azon része, hogy minden egyenes 1 modulo p^e pontban metszi a lefogó ponthalmazt ([H], Thm. 5.12), Blokhuis egy sejtését ([4]) igazolja. A $q = p^2$ esetben tételünkből a Baer-részsíkok alábbi jellemzése következik, mely az előző fejezetben említett Ball–Blokhuis eredménynél, de a javított Blokhuis, Storme, Szőnyi eredménynél is lényegesen erősebb.

4.3. Tétel. ([H], Thm. 5.7) *Legyen $q = p^2$, ($p > 2$), B pedig olyan blokkoló halmaz, amely nem tartalmaz Baer-részsíkot. Ekkor $|B| \geq 3(q+1)/2$.*

Természetesen ez az eredmény is éles, az ú. n. projektív háromszögek (melyekről a prím esetben a Lovász–Schrijver eredmény kapcsán már volt szó) minden páratlan prímhatványra $3(q+1)/2$ pontú blokkoló halmazokat adnak.

Itt is érdemes a bizonyítás vázlatát áttekinteni. A Rédei polinom segítségével két görbét rendelünk a ponthalmazhoz. Ezeknek nincs közös komponensük, GF(q) feletti pontjaik viszont azonosak. Bézout tételét használva egy ilyen polinom foka vagy elég nagy, vagy a polinom X^p-nek is polinomja.

Blokhuis és Polverino azt is észrevette, hogy kihasználva, hogy B-t minden egyenes 1 modulo p^e pontban metszi, tisztán kombinatorikus módszerekkel (a variancia trükkel) az intervallum felső határa is kissé megjavítható. Azt lehetne mondani, hogy a 4.2 Tételben $|B|$ aszimptotikus becslésében a harmadik tag 2 együtthatóját 1-re lehet javítani. Abban az esetben, ha $q = p^3$ (v. ö. 5.14. Állítás a cikkben), Blokhuis és Polverino eredménye a következőt adja.

Tétel. (Blokhuis–Polverino) PG$(2, q)$, *$q = p^3$ minimális blokkoló halmazainak mérete $p^3 + p^2 + 1$, $p^3 + p^2 + p + 1$ lehet, vagy legalább $3(q + 1)/2$.*

Mindegyik esetre van is ilyen méretű lefogó ponthalmaz (mely az első két esetben Rédei típusú). Nemrégiben Olga Polverino azt is megmutatta, hogy a $p^3 + p^2 + 1$ és a $p^3 + p^2 + p + 1$ méretű minimális blokkoló halmazok szükségképpen Rédei típusúak. (Ennek megfelelője, hogy tudniillik a $3(q+1)/2$-nél kisebb lefogó ponthalmazok mindig Rédei típusúak volnának, nem igaz, ha $q = p^h$ és $h \geq 4$. Ezt nemrégiben Polito és Polverino látta be, [18].)

Az utolsó cikk (k, p)-ívekre terjeszti ki Segre eredményeit, ahol $q = p^h$. Abban az esetben, ha q páros, csak a k-ívekre vonatkozó Segre-féle korlátnál gyengébb eredményt kapunk. Páratlan q-ra fő eredményünk a következő.

4.4. Tétel. ([I], Thm. 4.13) *Legyen $q = p^h$, $p > 2$, K pedig olyan (k, p)-ív a* PG$(2, q)$ *síkon, melyre $|K| = qp - q + p - \varepsilon$, ahol $\varepsilon \leq \sqrt[4]{q}/2$. Ekkor K nem teljes.*

Más szóval, figyelembe véve Ball, Blokhuis és Mazzocca [3] eredményét $(qn - q + n, n)$-ívek nemlétezéséről páratlan q-ra, ez azt jelenti, hogy $|K| < qp - q + p - \sqrt[4]{q}/2$. Tisztán kombinatorikus okoskodásokkal nem sokat lehet mondani erről a kérdésről: Thas [24] $\varepsilon = 1$-re látta be a megfelelő eredményt, de már a $\varepsilon = 2$ esetre is csak részeredmények vannak (Wilson [25]).

Az általános n osztja q esetben Ball és Blokhuis [2] egy n-től függő korlátot tudott megadni ε-ra polinomos módszerek alkalmazásával. Az egyszerűség kedvéért csak az $n \leq q/4$ esetre mondjuk ki eredményüket.

Tétel. (Ball–Blokhuis) *Ha $n \leq q/4$ és n osztja q-t, akkor* PG$(2,q)$ *legalább $nq - q + n/2$ pontú (k,n)-ívei nem teljesek.*

A $q/n = 2$ és 3 esetekre $n/2$ helyett kicsit nagyobb konstansszor n jött ki nekik. Ebben az irányban Hadnagy Évával sikerült egy görbéket használó bizonyítást adnunk, amely kicsit javít az $n/2$ tagon. Az is talán figyelemre méltó, hogy az algebrai görbe itt a fenti 4.4 Tételtől lényegesen különböző módon lett a nagy (k,n)-ívhez hozzárendelve.

Összefoglalva: azt reméljük, hogy Segre híres módszerének ezen módosítása — a ponthalmazokhoz a Rédei polinom segítségével algebrai görbét rendelni — hozzásegít kombinatorikus tulajdonságokkal definiált ponthalmazok tanulmányozásához. A kialakult módszer még nem igazán módszer abban az értelemben, hogy szemben a Segre-féle érintők lemmájával, eddig nem sikerült mechanikus bizonyítási technikává egyszerűsíteni a görbék konstrukcióját. Ez persze némi rugalmasságot kölcsönöz a módszernek, amely például a Segre-féle módszerrel kombinálható is, mindenesetre attól teljesen függetlennek látszik.

Egyelőre még csak kéziratos formában további alkalmazásai is vannak a módszernek: többszörösen lefogó ponthalmazokra a blokkoló halmazokhoz hasonló jellegű eredményeket láttunk be Lovász Lászlóval, Aart Blokhuis-szal pedig érintőmentes halmazokra sikerült a módszert alkalmazni.

5. Köszönetnyilvánítás

Először társszerzőimnek mondanék köszönetet, közülük is kiemelném azokat, akikkel több közös cikket is írtunk: Aart Blokhuist, Boros Endrét, James Hirschfeldet, Korchmáros Gábort, Leo Stormét és Wettl Ferencet.

A véges geometriákban Kárteszi Ferenc indított el, akinek sok segítségét, támogatását ezúton is köszönöm.

Végül, de nem utolsósorban annak szeretnék köszönetet mondani, akinek talán legnagyobb része volt a jelen dolgozat megszületésében: Lovász Lászlónak. Túl azon, hogy aspiránsvezetőm volt, és rengeteget tanultam tőle, a jelen dolgozat eredményei közül két kulcsfontosságú dolgozat a Yale-en született 1995/96-ban. Lovász László kérdései, megjegyzései nagyban hozzásegítettek ahhoz, hogy ez a két dolgozat (a két utolsó a jelen értekezésben) megszülessen jelenlegi formájában.

6. A dolgozatban feldolgozott saját cikkek

[A] L. Storme, T. Szőnyi, Caps in PG(n,q), q even, $n \geq 3$, *Geom. Dedicata* **45** (1993), 163–169.

[B] G. P. Nagy, T. Szőnyi, Caps in finite projective spaces of odd order, *J. of Geometry* **59** (1997), 103–113.

[C] L. Storme, T. Szőnyi, Intersection of arcs and normal rational curves in spaces of even order, *J. of Geometry* **51** (1994), 150–166.

[D] T. Szőnyi, On cyclic caps in projective spaces, *Designs, Codes and Cryptography* **8** (1996), 327–332.

[E] A. Blokhuis, A. E. Brouwer, T. Szőnyi, The number of directions determined by a function f on a finite field, *J. Combinat. Theory Ser. (A)* **70** (1995), 349–353.

[F] A. Blokhuis, L. Storme, T. Szőnyi, Lacunary polynomials, multiple blocking sets and Baer subplanes, *J. London Math. Society*, megjelenőben.

[G] T. Szőnyi, On the number of directions determined by a set of points in an affine Galois plane, *J. Combinat. Theory Ser. (A)* **74** (1996), 141–146.

[H] T. Szőnyi, Blocking sets in Desarguesian affine and projective planes, *Finite Fields and Appl.* **3** (1997), 187–202.

[I] T. Szőnyi, On the embedding of (k, p)-arcs in maximal arcs, *Designs, Codes and Cryptography*, megjelenőben.

Hivatkozások

[1] S. M. Ball, Multiple blocking sets and arcs in finite planes *J. London Math. Soc. (2)* **54** (1996), 581–593.

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

[3] S. M. Ball, A. Blokhuis and F. Mazzocca, Maximal arcs in PG$(2, q)$, q odd do not exist, *Combinatorica* **17** (1997), 31–41.

[4] A. Blokhuis, Blocking sets in Desarguesian planes, in: *Paul Erdős is Eighty, Volume 2*, (eds.:D. Miklós, V.T. Sós and T. Szőnyi, Bolyai Soc. Math. Studies **2** Bolyai Society, Budapest, 1996, 133–155.

[5] A. Blokhuis, R. Pellikaan and T. Szőnyi, Blocking sets of almost Rédei type, *J. Combin. Theory Ser. A* **78** (1997), 141–150.

[6] A. Blokhuis, S. Ball, A. E. Brouwer, L. Storme, T. Szőnyi, On the number of slopes of the graph of a function defined on a finite field, *J. Combinat. Theory Ser. (A)* **86** (1999), 187–196.

[7] Jin-Ming Chao, On the size of a cap in PG(n, q) with q even and $n \geq 3$, *Geom. Ded.* **74** (1999), 91–94.

[8] G. Cohen, I. Honkala, S. Lytsin, A. Lobstein, *Covering codes*, North-Holland, 1997.

[9] R. J. Evans, J. Greene, H. Niederreiter, Linearized polynomials and permutation polynomials of finite fields, *Michigan Math. J.* **39** (1992), 405–413.

[10] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields.* Oxford: Oxford University Press, 2nd Ed. 1998.

[11] J.W.P. Hirschfeld, *Finite Projective Spaces of Three Dimensions.* Oxford: Oxford University Press 1985.

[12] J.W.P. Hirschfeld and J.A. Thas, Linear independence in finite spaces, *Geom. Dedicata* **23** (1987), 15-31.

[13] J.W.P. Hirschfeld and J.A. Thas, *General Galois Geometries.* Oxford: Oxford University Press 1991.

[14] J. W. P. Hirschfeld and G. Korchmáros, On the embedding of an arc into a conic in a finite plane, *Finite Fields and Appl.* **2** (1996), 274–292

[15] J. W. P. Hirschfeld, G. Korchmáros, The number of rational points on an algebraic curve over a finite field, *Bull. Belg. Math. Soc. Simon Stevin* **5** (1998), 313–340.

[16] G. Korchmáros, T. Szőnyi, The number of rational points on Fermat curves over finite fields and cyclic subsets of projective spaces, *Finite Fields and Appl.* **5** (1999), 206–217.

[17] R. Meshulam, On subsets of finite abelian groups with no 3-term arithmetic progression, *J. Comb. Theory Ser. (A)* **71** (1995), 168–172.

[18] P. Polito, O. Polverino, On small blocking sets, *Combinatorica* **18** (1997), 133–137.

[19] L. Rédei, *Lacunary polynomials over finite fields*, Akadémiai Kiadó, North-Holland, 1973.

[20] L. Storme, J. A. Thas, S. K.J. Veerecke, New upper bounds for the sizes of caps in finite projective spaces, manuscript.

[21] L. Storme, T. Szőnyi, Intersection of arcs and normal rational curves in spaces of odd characteristic, in: *Finite Geometry and Combinatorics* (eds.: F. De Clerck et al.) Cambridge Univ. Press, 1993, 359–378.

[22] T. Szőnyi, Arcs, caps, codes and 3-independent subsets, in: *Giornate di Geometrie Combinatorie* (eds.: G. Faina, G. Tallini), Univ. Perugia, 1993, 57–80.

[23] T. Szőnyi, Around Rédei's theorem, *Discrete Math.*, megjelenőben

[24] J. A. Thas, Some results concerning $\{(q+1)(n-1), n\}$-arcs and $\{(q+1)(n-1)+1, n\}$-arcs in finite projective planes of order q, *J. Combin. Theory Ser. A* **19** (1975), 228–232.

[25] B. J. Wilson, Incompleteness of $(nq+n-q-2, n)$-arcs in finite projective planes of even order, *Math. Proc. Cambr. Phil. Soc.* **91** (1982), 1–8.