

dc_637_12

**APPLICATIONS OF
POLYNOMIALS OVER FINITE
FIELDS**

Sziklai Péter

MTA doktori disszertáció
tézisfüzet
Budapest, 2013

dc_637_12

0. Előszó

A véges testekkel koordinátázott terek több okból is figyelemre méltóak. Csoportelméleti szempontból, mert több olyan fontos csoport van, mely természetes módon szépen hat egy véges geometrián, vagy annak valamely részhalmazán. Kombinatorikus szempontból, mert több extremális problémára szolgáltatnak megoldást. Kódelméleti szempontból, mert belőlük nagyon jó paraméterekkel bíró hibajavító kódok nyerhetők. Kriptográfiai szempontból, mert több titkosító módszer is épül véges terekben definiált struktúrákra. Végül geometriai szempontból, mert számos klasszikus geometriai kérdés kerül új megvilágításba, amikor véges test feletti analogonját vizsgáljuk.

Dolgozatomban véges testekkel koordinátázott (vektor-, affin- és projektív) terek kombinatorikusan definiált részstruktúráival foglalkoztam. Ezen a területen a tipikus gondolatmenet/munkaterv a következő. Definiálunk egy struktúra-osztályt, mely leggyakrabban bizonyos metszési tulajdonságú ponthalmazokból áll. Például ilyenek a *lefogó ponthalmazok* (melyeket minden egyenes legalább 1 pontban metsz), vagy általában a *k-lefogóhalmazok* (melyeket minden k kodimenziós altér metsz), vagy a síkbeli *ívek* (melyeket minden egyenes legfeljebb 2 pontban metsz). Ezután megnézzük, hogy az adott osztályba tartozó struktúrák (ponthalmazok) mérete milyen értékeket vehet fel, ezen belül mi a legkisebb, ill. legnagyobb érték. A következő lépésben klasszifikáljuk az ilyen szélső értékekhez tartozó példák szerkezetét: ezek az extrém konstrukciók gyakran „szépek”. Végezetül belátjuk, hogy „a szépség magányos”, azaz hogy az extrém/szép példák „stabilak”: ha találunk egy hozzá „közeli” másik példát (itt a közelség általában méretet, ritkábban a struktúrát leíró tulajdonság „majdnem teljesítését” jelenti), akkor az a másik példa valójában kis változtatásokkal „kijavítható”, azaz pl. kevés pont törlésével/hozzáadásával a szép/extremális példához jutunk.

A dolgozat témája a fenti problémátípus talán legerősebb módszerének, a polinomos módszernek a bemutatása. A módszer kezdetei a hetvenes évek elejére nyúlnak vissza, Rédei, Jamison, Lovász, Schrijver, Bruen voltak az első alkalmazói. A gondolat természetes: rendeljünk hozzá a speciális kombinatorikus/geometriai tulajdonsággal bíró struktúrához/ponthalmazhoz egy (tipikusan többváltozós, véges test felett definiált) polinomot. Vizsgáljuk meg, hogy az eredeti speciális tulajdonság milyen polinom-tulajdonságot eredményez. Ezután jellemezzük az ilyen tulajdonságú polinomokat. (Ez szokott nehéz lenni.) Végül a kapott polinomos eredményt „fordítsuk vissza” az eredeti, kombinatorikus/geometriai nyelvre.

A módszer kezdeti alkalmazói a polinomok együtthatóit vizsgálták, ennek egyik irányzata volt a Rédei könyvéből kinövő „hézagos polinomos” módszer.

Ez a 90-es évek végére érte el csúcspontját, egyszersmind a határait is. Ekkor kezdődött a következő korszak, Szőnyi Tamásnak köszönhetően, aki a síkbeli problémákból nyert polinomokat mint algebrai síkgörbéket kezdte használni. Ebben az ötlet még az ötvenes évekből, Segre-től való, de Segre görbéi mások, nem algebrai, hanem geometriai definícióból jönnek, és nehezebben kezelhetőek. A téma mai állása: a módszer háromfelé ágazott, Szőnyi és Weiner egy rezultánsokra épülő technikával, Ball a Segre-módszer újraértelmezésével ért el a közelmúltban szép eredményeket. Egy harmadik útról szól a dolgozat 14. szakasza, erről kicsit lejjebb írok.

Az előszó végén a könnyebb olvashatóság kedvéért megadok pár definíciót, jelölést. $\text{GF}(q)$ mindig egy q elemszámú véges test, $q = p^h$ prímszám, p a karakterisztika. E test felett definiált projektív n -dimenziós teret $\text{PG}(n, q)$ -val, az affin teret $\text{AG}(n, q)$ -val jelöljük. $\text{PG}(n, q)$ -nak $q^n + q^{n-1} + \dots + q + 1$, $\text{AG}(n, q)$ -nak q^n pontja van. A projektív teret úgy képzeljük, mint az affin térnek és egy „ideális hipersíknak” az unióját, ez utóbbit H_∞ -vel jelöljük, pontjait pedig ideális pontoknak vagy irányoknak hívjuk. Az affin tér pontjait vektortér-koordinátákkal, a projektív tér pontjait homogén koordinátákkal írjuk le, azaz $(a_1, a_2, \dots, a_n) \in \text{AG}(n, q)$ ill. $(a_1, a_2, \dots, a_{n+1}) \in \text{PG}(n, q)$. A projektív tér hipersíkjaira szintén homogén, szögletes zárójelbe írt koordinátákat használunk: $[x_1, x_2, \dots, x_{n+1}]$, és egy pont illeszkedik egy hipersíkra, ha a koordináta-vektoraik skalárszorzata $\sum a_i x_i = 0$.

Az affin $\text{AG}(n, q)$ tér egy U pontthalmaza által *meghatározott irányok*: az U -ból vett pontpárok által meghatározott egyenesek ideális pontjai.

A $\text{PG}(n, q)$ projektív tér *k-lefogóhalmazának* nevezünk egy olyan pontthalmazt, mely minden k -kodimenziós alteret metsz.

Az alábbiakban igyekeztem a dolgozat tétel- (és egyéb) sorszámaikat, elnevezéseiket használni.

1. A háttér

A dolgozat első néhány (4-8) szakaszában a témakörhöz szükséges háttérismereteket gyűjtöttem össze. Ez a rész is tartalmaz kisebb-nagyobb új eredményeket, valamint nehezen elérhető, esetenként „folklór” eredményeket. Mindebből kiemelném az 5. szakaszt.

A dolgozat (és a témakör) legfontosabb fogalma a Rédei-polinom. Legyen S egy pontthalmaz $\text{PG}(n, q)$ -ban. Ennek Rédei-polinomja $R^S(X_1, X_2, \dots, X_{n+1}) =$

$$R(X_1, X_2, \dots, X_{n+1}) := \prod_{(a_1, \dots, a_{n+1}) \in S} (a_1 X_1 + a_2 X_2 + \dots + a_{n+1} X_{n+1}).$$

Ez tehát egy teljesen reducibilis polinom, amelybe behelyettesíteni a tér $[x_1, x_2, \dots, x_{n+1}]$ hipersíkjaikat szoktuk. $R(x_1, x_2, \dots, x_{n+1})$ pontosan akkor lesz 0, ha a behelyettesített hipersík metszi S -et, sőt, mivel R mint algebrai hiperfelület (a duális n -dimenziós projektív térben) éppen a lineáris faktorainak megfelelő hipersíkok uniója, ezért a (duális) tér $(x_1, x_2, \dots, x_{n+1})$ pontjának multiplicitása R -en nyilván annyi, ahány pontban az $[x_1, x_2, \dots, x_{n+1}]$ hipersík metszi S -et. Speciálisan pl. ha S lefoghalmaz a hipersíkokra nézve, akkor R minden helyettesítésre eltűnik, az ilyen polinomok pedig könnyen jellemezhetőek (lásd később).

Egy érdekes példa az alábbi:

Result 5.7. (SzP) *Legyen S az $X^2 - YZ$ egyenletű kúpszelet $\text{PG}(2, q)$ -ban. Ekkor S Rédei-polinomja*

$$R^S(X, Y, Z) = Y \prod_{t \in \text{GF}(q)} (tX + t^2Y + Z) = Y(Z^q + Y^{q-1}Z - C_{\frac{q-1}{2}}Y^{\frac{q-1}{2}}Z^{\frac{q+1}{2}} - \\ - C_{\frac{q-3}{2}}X^2Y^{\frac{q-3}{2}}Z^{\frac{q-1}{2}} - C_{\frac{q-5}{2}}X^4Y^{\frac{q-5}{2}}Z^{\frac{q-3}{2}} - \dots - C_1X^{q-3}YZ^2 - C_0X^{q-1}Z),$$

ahol $C_k = \frac{1}{k+1} \binom{2k}{k}$ a híres Catalan-számok.

Szintén az 5. szakaszban található a Rédei-polinom deriváltjairól és Hasse-deriváltjairól egy részletes elemzés.

A dolgozat sűrűbb része a 9. szakaszban kezdődik. Itt először egy általános sémát vázolunk fel, és ízelítőt adunk a klasszikus görbés stabilitási eredmények stílusából. Íme közülük néhány példa:

Result 9.1. (Szőnyi) *Legyen $B \subset \text{PG}(2, q)$ egy olyan lefoghalmaz, amely „majdnem Rédei típusú”, azaz $|B \cap \text{AG}(2, q)| = q + \varepsilon$ affin pontja van, $\varepsilon < \sqrt{q}/2$. (A „Rédei típusú” azt jelentené, hogy $\varepsilon = 0$.) Ekkor B -ből ki lehet törölni ε affin pontot úgy, hogy a maradék még mindig lefoghalmaz (és persze már Rédei-féle) legyen.*

Result 9.2. (SzP) *Legyenek $f_i(T)$, $i = 1, \dots, q - \varepsilon$ legfeljebb d -edfokú polinomok, és tegyük fel, hogy $\{(t, f_i(t)) : t \in \text{GF}(q)\}$ grafikonjaik páronként diszjunktak. Ekkor ha $\varepsilon < c\sqrt{q}$ akkor találhatunk további $f_{q-\varepsilon+1}(T), \dots, f_q(T)$, szintén legfeljebb d -edfokú polinomokat úgy, hogy ezen q polinomgrafikon partícionálja az $\text{AG}(2, q)$ affin síkot.*

Megjegyezzük, hogy itt, kis módosítással a foksámfeltétel helyett kiköthetjük azt is, hogy a polinomok egy előre rögzített polinom-altérből valók legyenek.

Ide kapcsolódik, mint klasszikus jellegű stabilitási eredmény, a 13. szakasz anyaga.

Adott $\text{PG}(3, q)$ -ban egy kúp (azaz egy síkban $q + 1$ pont, a kúp alapja, a síkon kívül egy V pont, a kúp csúcsa, ekkor a kúp az alap pontjait a csúccsal

összekötő egyenesek uniója, $q(q+1)+1$ pont). Ha az alap egy másodrendű síkgörbe, kvadratikus kúpnak hívjuk. Egy kúp flockja: a csúctól különböző pontok partíciója q diszjunkt síkmetszetre, azaz a kúp palástját q darab, az alappal hasonló síkidomra partícionáljuk. Erre egy lehetőség: egy fix, a kúptól diszjunkt egyenesen átmenő síkokkal felszeletelni a kúpot (ún. lineáris flock). A kérdések: van-e más, illetve ha már találtunk $q-\varepsilon$ diszjunkt síkmetszetet (parciális flock), akkor az mindig kiegészíthető-e flock-ká, ha ε elég kicsi (stabilitás, kiegészíthetőség). A kérdés nem önmagáért való, számtalan geometriai probléma ekvivalens vagy visszavezethető a flock-os kérdésekre (már a kapcsolódási viszonyoknak is külön irodalma van): ide kapcsolódnak $\text{PG}(3, q)$ bizonyos egyenes-partíciói (spread), translációsíkok, q -klánok, elációs általánosított négyszögek, $\text{PG}(2, q)$ ovális-seregei (herd), stb.

Kvadratikus kúpra a speciális $q = 2^h$ esetben Storme és Thas (más tételek alkalmazásával) bebizonyították a fent leírt kiegészíthetőséget $\varepsilon \leq \sqrt{q}$ ill. $\varepsilon \leq \sqrt{2q}$ esetén, attól függően, hogy q négyzetszám vagy sem, de általános q -ra semmit sem tudtunk. Kvadratikus kúpra sikerült általános egyértelmű kiegészíthetőséget bizonyítanom, ha $\varepsilon \leq \frac{1}{4}\sqrt{q}$, illetve $q = p$ prím esetén ha $\varepsilon \leq \frac{1}{40}p + 1$. Majd ezt általánosítottam arra az esetre, ha a kúp alapja az $\{(1, t, t^d) : t \in \text{GF}(q) \cup \{\infty\}\}$ homogén síkgörbe. Ekkor az analóg korlát $\varepsilon \leq \lfloor \frac{1}{d^2}\sqrt{q} \rfloor$ lesz. A bizonyításaim teljesen különböznek a Storme–Thas-féle „geometriai” úttól, elemi szimmetrikus polinomokra és algebrai görbékre épülnek, lényegében a fentebb, ill. a 9. szakaszban leírt klasszikus értelemben. A kapott eredmények több esetben direkt módon átfordíthatók a fent említett kapcsolódó struktúrák stabilitási eredményeivé.

2. Irányok és lefogóhalmazok

A dolgozat nagyobbik része irányokkal és lefogóhalmazokkal foglalkozik. Az affin $\text{AG}(n, q)$ tér egy U ponthalmaza által meghatározott irányok: az U -ból vett pontpárok által meghatározott egyenesek ideális pontjai. A klasszikus, Rédei-től származó kérdés az volt, hogy hány irányt határoz meg egy $f : \text{GF}(q) \rightarrow \text{GF}(q)$ függvény grafikonja, azaz a q elemű $\{(x, f(x)) : x \in \text{GF}(q)\} \subset \text{AG}(2, q)$ ponthalmaz. Itt az irányok nyilván az $\frac{f(x)-f(y)}{x-y}$ különbségi hányadosoknak felelnek meg. Az eredeti irányproblémát Rédei Abel-csoportok (Pólya-féle) faktorizációs kérdéseire kapcsolódva kezdte vizsgálni, de rengeteg az alkalmazás, pl. a lefogóhalmazokat, permutációs polinomokat, Paley-gráfok automorfizmusait vizsgálók is kötöttek itt ki.

Ha $\text{AG}(2, q)$ egy q -elemű ponthalmazához hozzávesszük az általa meghatározott $D \subseteq H_\infty$ irányhalmazt, akkor a kapott ponthalmaz a sík minden egyenesét lefogja. Az ilyen lefogóhalmazokat nevezzük Rédei típusúaknak.

Ezek extrémálisak abban az értelemben, hogy $\text{PG}(2, q)$ tetszőleges B lefogóhalmaza legalább q affin pontot kell tartalmazzon, és egyenlőség esetén a $B \cap \text{AG}(2, q)$ által meghatározott irányoknak is B -ben kell lenniük (azaz ha minimális lefogó volt, akkor Rédei-féle).

2.1. Irányok és kis lefogóhalmazok

A $\text{PG}(n, q)$ projektív tér k -lefogóhalmazának neveztünk egy olyan ponthalmazt, mely minden k -kodimenziós alteret metsz. Könnyű látni, hogy a legkisebb ilyen egy k -dimenziós projektív altér ponthalmaza, mely tehát $q^k + q^{k-1} + \dots + q + 1$ elemű. Kis k -lefogóhalmaznak a legfeljebb kb. másfélszer ekkora, $\frac{3}{2}(q^k + 1)$ -nél kisebb lefogóhalmazokat szokás hívni, és világos, hogy csak a (tartalmazásra nézve) minimálisak érdekesek. Az 1970-es évek óta kérdés, és a mai napig megoldatlan ezek teljes leírása, még a $\text{PG}(2, q)$, $k = 1$, azaz síkbeli egyeneslefogók esetén is. Rédei László konstruált olyan (Rédei típusú) lefogóhalmazokat a síkban, melyek egy kevés irányt (különbségi hányadost) meghatározó $\text{GF}(q) \rightarrow \text{GF}(q)$ függvénygrafikon pontjaiból és az általuk meghatározott egyenesek meredekségeiből, mint ideális egyenesen lévő ponthalmazból álltak. Hosszú ideig tartotta magát az a Blokhuis-tól származó sejtés, hogy minden síkbeli kis lefogóhalmaz Rédei-féle. A Rédei-féléket Ball, Blokhuis, Brouwer, Storme és Szőnyi (BBBSS) egy rafinált polinomos módszer segítségével lényegében teljesen le is írta a következő módon. Vegyünk $\text{GF}(q)$ -ban, $q = p^h$, egy $\text{GF}(p^e)$ résztestet. Válasszunk ki az affin síkon h/e darab, a résztest felett független vektort, és legyen U ezek generátuma a résztest felett, így q affin pontot kapunk. Vegyük hozzájuk a meghatározott irányokat. Pontosan ilyen alakú lesz minden kis minimális Rédei-féle lefogóhalmaz (azaz egy $\frac{q+3}{2}$ -nél kevesebb irányt meghatározó affin q -elemű ponthalmaz, irányostul) BBBSS szerint.

Ezt a tételt sikerült kiterjesztenünk minden dimenzióra a következő módon (lásd a 12. szakaszt):

Theorem 12.10. (SzP, Storme) *Legyen $U \subset \text{AG}(n, q)$, $|U| = q^k$, mely legfeljebb $\frac{q+3}{2}q^{k-1} + q^{k-2} + \dots + q^2 + q$ irányt határoz meg. Ekkor U egy alkalmas résztest felett lineáris ponthalmaz (azaz résztest feletti lineáris altér eltöltja).*

Fentebb már esett szó síkbeli Rédei típusú lefogóhalmazokról, és (résztest felett) lineáris ponthalmazokról. Storme-val kiterjesztettük a definíciót: $\text{PG}(n, q)$ -ban Rédei típusú k -lefogóhalmaznak nevezünk egy $U \cup D$ ponthalmazt, ahol $U \subset \text{AG}(n, q)$, $|U| = q^k$, $D \subseteq H_\infty$, és D éppen az U által meghatározott irányokból áll. Megmutattuk, hogy így valóban a k -kodimenziós projektív altereket lefogó ponthalmazt kapunk, melynek ráadásul a lehető

legkevesebb affin pontja van. Tehát a legutóbbi tétel valóban a kis Rédei-féle k -lefogók leírását adja. A dolgozat 12. szakaszában azt is beláttuk, hogy D -nek mindig nagyon speciális struktúrája van, aminek egy következménye a $k = n - 1$ speciális esetben (egyeneslefogás), hogy D az ideális hipersík néhány hipersíkjának $((n - 2)$ -dimenziós alterének) uniója. Ez később rop-pant fontos eredménnyé vált: Alderson és Gács gyönyörű tételének (mely szerint ha egy lineáris kód kiterjeszthető, akkor lineárisan is kiterjeszthető) egyik kulcslépése lett.

Az affin terekben lévő, résztest felett lineáris pontthalmazok tehát fontos-sá váltak számunkra. A k -lefogóthalmazok közül azok az érdekesek, melyek nem kúpok (mert könnyű áttérni a kúp „alapjának” vizsgálatára, és így alacsonyabb dimenzióssá egyszerűsödik a helyzet). A paraméterek kedvezőtlen összjátéka viszont esetleg kikényszerítheti, hogy egy résztest felett lineáris pontthalmaz kúp legyen. Tehát meg kellett nézni, mikor érdekesek, ill. érdektelenek a lineáris pontthalmazok. Erre bizonyítottunk egy éles korlátot: $\text{AG}(n, q)$ -ban, $q = p^h$, ha egy $\text{GF}(p)$ -lineáris U pontthalmazra $|U| > p^{n(h-1)}$, akkor kúp (és adtunk egy Descartes-szorzat konstrukciót, az élességet bizonyítandó).

Lunardon, Polito és Polverino konstruáltak Rédei- és nem-Rédei-féle további, általánosabb, szintén „*résztest felett lineáris*”-nak hívott lefogóthalmazokat, ezek **magas dimenziós, résztest feletti részgeometriák vetületei** a síkba (vagy a vizsgált $\text{PG}(n, q)$ -ba); az előbbi Rédei típusú konstrukció is közéjük tartozik (az a speciális eset, amikor a vetítendő részgeometria „affin része” injektíven vetül az affin síkba/térbe, az ideális rész pedig – valahogy, mint meghatározott irányok – az ideálisba).

Egyszerű „dimenziótétel”-lel látszik, hogy $\text{PG}(n, q)$ -ban az alkal-masan választott paraméterű $\text{PG}(n', q')$ tartalmazott részgeometriák k -lefogóthalmazok; illetve kontrollálható, hogy vetítés során ez a k hogyan változik, tehát arra jutottam, hogy nemcsak arról van szó, hogy ez egy újabb konstrukció, hanem hogy valamilyen értelemben ez „a” természetes konstrukció. Ezért és az alábbiak miatt fogalmaztam meg a következő sejtést:

Conjecture 11.1. Linearitási sejtés (SzP) $\text{PG}(n, q)$ -ban minden mi-nimális kis k -lefogó egy alkalmas résztest felett lineáris halmaz.

Sőt, több jel mutat arra, hogy ennek többszörös lefogóthalmazokra vonatkozó analogonja is igaz lehet. Korábban ismert volt már Szőnyi eredménye, hogy egy minimális kis lefogó minden egyenesmetszete $1 \bmod p$ méretű, ahol p a test karakterisztikája. Az volt a célom, hogy bebizonyítsam a Linea-ritási sejtés „minél nagyobb részét”. Legyen $\text{PG}(2, q)$ -ban ($q = p^h$), B egy kis minimális lefogóthalmaz, melyet minden egyenes $1 \bmod p^e$ pontban metsz, és e maximális erre a tulajdonságra nézve (ezt hívják B exponensének). A

következőket sikerült belátnom.

Theorem 11.33. *B szelő egyenesei közül majdnem mind pontosan $p^e + 1$ pontban metszi B -t. (A többi persze legalább $2p^e + 1$ pontban.) Ezen rövid szelők mindegyike izomorf egy $\text{PG}(1, p^e)$ egydimenziós részegyenessel, mely a $\text{GF}(p^e)$ test felett van definiálva. Tehát $\text{GF}(p^e)$ részttest $\text{GF}(q)$ -ban, azaz $e|h$.*

Ez éppen az, amit egy lineáris pontthalmaztól várunk, az kombinatorikusan éppen így néz ki, és algebrailag is majdnem teljesen így.

Ezt a síkbeli eredményt sikerült kiterjesztenem nagyon általános formában (részben felhasználva Szőnyi és Weiner egy spektrum-eredményét):

Jelölje $S(q)$ a kis minimális lefogóhalmazok $\text{PG}(2, q)$ -beli lehetséges méreteit tartalmazó halmazt.

Corollary 11.38. (SzP) *Legyen B egy kis minimális, k -lefogó pontthalmaz $\text{PG}(n, q)$ -ban, $q = p^h$, melyre $|B| < \frac{3}{2}(q^k + 1)$, illetve $|B| < \sqrt{2}q^k$ ha $p = 2$. Ekkor*

- $|B| \in S(q^k)$;
- ha $p > 2$ akkor $(|B| - 1)(q^k)^{n-2} + 1 \in S((q^k)^{n-1})$.

Ha $p > 2$ akkor létezik egy egész e szám, B exponense, $1 \leq e|h$, melyre az igaz, hogy ha egy tetszőleges altér metszi B -t, akkor 1 modulo p^e pontban metszi. $|B|$ értéke egy bizonyos e' -höz tartozó intervallumba kell essen, ahol $e' \leq e$, $e'|h$. Tekintsük azon $(n - k)$ -dimenziós altereket, melyek B -t egynél több pontban metszik: az ilyen szelő alterek döntő többsége pontosan $(p^e + 1)$ pontban metszi B -t, és ezen $(p^e + 1)$ pontú metszetek mindegyike egy-egy kollineáris pontthalmaz, mely izomorf a $\text{PG}(1, p^e)$ részegyenessel.

A fenti Theorem 11.33 következményeként kapunk egy „tíz soros” bizonyítást Ball, Blokhuis, Brouwer, Storme és Szőnyi fent említett „tízoldalas”, híres tételére (Corollary 11.36), illetve pontosítani lehetett a minimális kis lefogóhalmazok lehetséges méreteire vonatkozó becsléseket.

A bizonyításban a Rédeitől eredő polinomos módszert használjuk. A módszer korábbi „csúcsában” Szőnyi az egyik polinomot mint algebrai síkgörbét tekintette, ebből jött ki a fent idézett „1 mod p ” eredménye. A Theorem 11.33 itt közölt bizonyítása hasznosítja az algebrai helyzet szimmetriatulajdonságait, és nem egy, hanem három algebrai görbét vizsgál egyszerre. A másik továbblépés három új görbe bevezetése, melyek egészen váratlan (és máig nem teljesen feltárt) tulajdonságokkal bírnak, pl. a lefogóhalmaz érintői között egy fixpontmentes leképezést definiálnak, tehát kicsit úgy viselkednek, mintha a sík egy automorfizmusát definiálnák (kanonikus Baer-részsík esetén például pontosan ezt teszik, az $(x, y, z) \mapsto (x^{\sqrt{q}}, y^{\sqrt{q}}, z^{\sqrt{q}})$ leképezést adják).

2.2. Stabilitás

Az irányprobléma stabilitási verziója is régóta tárgya vizsgálatoknak, sok alkalmazással. Adott $\text{PG}(n, q)$ -ban q^{n-1} -nél kicsit kevesebb vagy kicsit több pont, az első esetben az a kérdés, hogy kiegészíthető-e q^{n-1} pontúvá a halmaz úgy, hogy ne keletkezzen újabb meghatározott irány. A második esetben pedig azt kérdezzük, hogy kidobható-e a „fölösleg”, azaz annyi pont, hogy éppen q^{n-1} maradjon, és azok maradjanak a „nem meghatározott irányok” (azon ideális pontok, melyeken átmenő párhuzamos egyenesre mind a q^{n-1} egyenesén volt pontja a pontthalmaznak), akik a ponttörlés előtt voltak. Mindkét kérdésre voltak korábbi eredmények, tipikusan (i) síkban és (ii) erős feltétel mellett a meghatározott irányok számára (Szőnyi et al). A dolgozat 14. fejezete az alsó stabilitással foglalkozik, egy iránythalmazokra vonatkozó, nagyon általános eredményt, de még inkább a hozzá vezető módszert írja le. Adott $\text{AG}(n, q)$ -ban egy $q^{n-1} - \varepsilon$ pontú U pontthalmaz, mely által meghatározott irányok halmaza $D \subseteq H_\infty$. Azt igazoljuk, hogy (nagyon idézőjelbe téve) „tipikusan” van kiegészülés, azaz ha nincs, akkor a nem meghatározott irányok H_∞ -ben egy (persze ε -től függően) nagyon erős struktúrát kell alkotniuk. A módszer újdonsága, hogy a geometriai problémát algebraizálás után a duális térben definiált hiperfelületet „teljesen reducibilisen metsző” hipersíkok nyelvére fordítja le: a pontthalmaz geometriai „hiányának” a duális térben definiált algebrai hiperfelület felel meg. Ha erről kiderül, hogy tartalmaz lineáris faktort, akkor az egy „hozzávehető” pontot jelent az eredeti geometriai nyelven (és indukcióval készen vagyunk), ez a cél. Ugyanakkor azt is tudjuk, hogy minden egyes nem-meghatározott iránynak e hiperfelület olyan speciális hipersík-metszete felel meg, mely teljesen reducibilis (azaz $(n-2)$ -dimenziós lineáris alterekre bomlik a hipersíkban). Ebből pedig, ha a felület maga nem teljesen reducibilis, a nem-meghatározott irányok halmazának nagyon erős jellemzése adódik. A dolgozatban kifejtett konkrét eredmények a következők:

Theorem 14.12. (De Beule, SzP, Takáts) *Legyen $n \geq 3$, $U \subset \text{AG}(n, q) \subset \text{PG}(n, q)$, $|U| = q^{n-1} - 2$, és $D \subseteq H_\infty$ az U által meghatározott irányok halmaza, $N = H_\infty \setminus D$ pedig a nem-meghatározott irányoké. Ekkor U -t ki lehet egészíteni egy $\bar{U} \supseteq U$, $|\bar{U}| = q^{n-1}$ pontú halmazzá úgy, hogy az ugyanazokat az irányokat határozza csak meg, vagy N pontjai kollineárisak és $|N| \leq \lfloor \frac{q+3}{2} \rfloor$, vagy N pontjai egy síkbeli kúpszeleten vannak.*

Theorem 14.13. (De Beule, SzP, Takáts) *Legyen $U \subset \text{AG}(3, q) \subset \text{PG}(3, q)$, $|U| = q^2 - \varepsilon$, ahol $\varepsilon < p$ és $D \subseteq H_\infty$ az U által meghatározott irányok halmaza, $N = H_\infty \setminus D$ pedig a nem-meghatározott irányoké. Ekkor N egy $\varepsilon^4 - 2\varepsilon^3 + \varepsilon$ fokú síkgörbén helyezkedik el, vagy U kiegészíthető egy $\bar{U} \supseteq U$, $|\bar{U}| = q^2$ pontú halmazzá.*

Ezek speciális eredményeknek tűnnek, de arról van szó, hogy ez két olyan eset volt, amikor könnyű volt kiolvasni a hiperfelület nem-faktorizálódásából a nem-meghatározott irányok jellemzését. A kapott leírásból általában is látszik a nem-meghatározott irányok speciális szerkezete. Másrészt a kapott algebrai geometriai probléma – jellemezzük azokat a hiperfelületeket, melyekhez sok, teljesen reducibilisen metsző hipersík található – önmagában is érdekes, klasszikus ízű kérdés, és egyelőre megoldatlan.

2.3. Egy általánosítás

A 15. szakaszban a klasszikus, Rédeitől származó irányprobléma egy általánosítását adjuk, a [SzP2func] cikk alapján. Az alapkérdés: adott $\text{AG}(n, q)$ -ban egy U pontthalmaz, mit mondhatunk D -ről, az általuk meghatározott ideális pontok (irányok) halmazáról. Síkban, ha $|U| = q$ és nincs minden irány meghatározva, akkor szokás U -ra mint egy függvény grafikonjára gondolni, $U = \{(x, f(x)) : x \in \text{GF}(q)\}$ és $D = \left\{ \frac{f(y)-f(x)}{y-x} : x \neq y \in \text{GF}(q) \right\}$. Ekkor egy c elem pontosan akkor van benne $\bar{D} = \text{GF}(q) \setminus D$ -ben, ha az $x \mapsto f(x) - cx$ leképezés **permutáció** $\text{GF}(q) \rightarrow \text{GF}(q)$, azaz ha a c meredekségű q darab párhuzamos affin egyenes egy-egy pontban metszi U -t. A disszertációban feldolgozott cikkben a $q = p$ prím esettel foglalkoztunk. Gács korábban igazolta, hogy $\text{AG}(2, p)$ -ben, ha $M(f) := |\bar{D}| \geq 2\lceil \frac{p-1}{6} \rceil + 1$ akkor f grafikonja lefedhető két egyenes uniójával (és az ilyenek már korábban klasszifikálva voltak (Szőnyi), amiből az következett, hogy vagy $M(f) \leq 2\lceil \frac{p-1}{6} \rceil$, vagy f lineáris, vagy f „ekvivalens” az $x^{\frac{p+1}{2}}$ függvénnyel).

Először lehelletnyit megjavítjuk a Gács-féle eredményt, egy hatványösszegetes feltétel segítségével. A bizonyítás, hol nyíltan, hol rejtve, bizonyos polinomok által feszített vektorterek komplikált dimenzióbecslésére, és az ezzel párhuzamos fokszámbecslésekre épül. A módszer tudomásunk szerint teljesen új a polinomos technikák között.

Ezután tekintünk két $\text{GF}(p) \rightarrow \text{GF}(p)$ függvényt, f -et és g -t, és a fenti $M(f)$ analogonjaként azt mondjuk, hogy ők *nem határoznak* meg bizonyos „irányokat”, valójában a 3-dimenziós tér bizonyos ideális egyeneseit, mégpedig azon (c, d) párokhoz „tartozókat”, melyekre az $x \mapsto f(x) + cg(x) + dx$ leképezés **permutáció** $\text{GF}(p) \rightarrow \text{GF}(p)$. Itt tehát, a síkbelihez hasonló értelemben, a pontthalmazunk $U = \{(x, f(x), g(x)) : x \in \text{GF}(p)\} \subset \text{AG}(3, p)$, továbbra is $q = p$ pontunk van, és egy, az „irány” szerepét játszó ideális egyenes akkor nincs meghatározva, ha a rajta átmenő p affin (párhuzamos) sík mindegyike 1-1 pontot tartalmaz U -ból. A kérdés, megint, $M(f, g)$: az ilyen (c, d) párok száma. A fő eredményünk (Ball-Gács-SzP), hogy ha kb. $\frac{2}{9}p^2$ -nél több ilyen (c, d) pár van, akkor az U pontthalmaz síkbeli (ekkor per-

sze a kérdés rögtön egyszerűvé válik). Végül megmutatjuk, hogy a becslés aszimptotikusan éles, ha $p = 1 \bmod 3$ prím.

3. Konstans (mod p) metszetű halmazok

A dolgozat 10. szakasza olyan $\text{PG}(2, q)$ -beli ponthalmazokkal foglalkozik, melyeket a sík egyenesei valamilyen rögzített konstans számú pontban metszik, modulo p számolva. Általánosságban a következőt mondhatjuk:

Theorem 10.3. *Legyen adott egy ponthalmaz, $S = \{(a_i, b_i, c_i) : i = 1, \dots, s\} = \{(a_i, b_i, 1) : i = 1, \dots, s_1\} \cup \{(a_j, b_j, 0) : j = s_1 + 1, \dots, s\} \subseteq \text{PG}(2, q)$ -ban, ekkor az alábbiak ekvivalensek:*

- (i) S minden egyenest $t \bmod p$ pontban metsz, valamilyen fix t értékre;
- (ii) $G(X, Y, Z) = \sum_{i=1}^{|S|} (a_i X + b_i Y + c_i Z)^{q-1} \equiv 0$;
- (iii) minden $0 \leq k+l \leq q-1$, $\binom{k+l}{k} \not\equiv 0 \bmod p$ esetén $\sum_{i=1}^{|S|} a_i^{q-1-k-l} b_i^k c_i^l = 0$ (itt $0^0 = 1$).
- (iv) minden $0 \leq k+l \leq q-2$, $\binom{k+l}{k} \not\equiv 0 \bmod p$ esetén $\sum_{i=1}^{s_1} a_i^k b_i^l = 0$ és minden $0 \leq m \leq q-1$ esetén $\sum_{i=1}^s a_i^{q-1-m} b_i^m = 0$.

Ahogy látható, egy ilyen halmaz koordinátáinak rengeteg hatványösszege nulla, ezért adtuk nekik az általánosított Vandermonde-halmaz nevet (a magyarázatot lásd lentebb).

3.1. Ponthalmazok 0 mod r metszetekkel

Ennek a szakasznak a legerősebb eredménye az alábbi:

Theorem 10.15. (Ball, Blokhuis, Gács, SzP, Weiner) *Legyen $1 < r < q = p^h$. Egy olyan $S \subset \text{PG}(2, q)$ ponthalmaznak, mely minden egyenest 0 mod r pontban metsz, legalább $|S| \geq (r-1)q + (p-1)r$ pontja van, továbbá r -nek osztania kell q -t.*

Megjegyezzük, hogy az eredeti cikkben e tétel magas dimenziós analógját is igazoltuk. A tétel erősségét az alábbi két következmény mutatja.

Corollary 10.16. *Ha egy 3 dimenziós kód súlyainak és hosszának közös osztója r , és duális minimális távolsága legalább 3, akkor a kód hossza legalább $(r-1)q + (p-1)r$.*

Maximális ímek nevezik a projektív sík egy olyan S ponthalmazát, melyet minden egyenes pontosan 0 vagy r pontban metsz. Persze triviális példák az

üres halmaz, egy pont, az affin sík és az egész sík ($r = 0, 1, q$ ill. $q + 1$). További példák ismertek (Denniston) minden páros q esetén, q minden r osztójára. Ball, Blokhuis és Mazzocca alábbi híres és nehéz eredménye a fenti Theorem 10.15 egyszerű, egysoros következményévé vált:

Corollary 10.17. *Páratlan q esetén nem léteznek nem-triviális maximális ívek $\text{PG}(2, q)$ -ban.*

3.2. Vandermonde- és szuper-Vandermonde halmazok

Fentebb láttuk, hogy geometriailag érdekes halmazokból $\text{GF}(q)$ olyan részhalmazai adódnak, melyeknek sok hatványösszege eltűnik. Ezért értelmes kérdésnek tűnt az ilyen elemhalmazok vizsgálata. Legyen $1 < t < q$. *Vandermonde-halmaznak* nevezünk egy $T = \{y_1, \dots, y_t\} \subseteq \text{GF}(q)$ halmazt, ha $\pi_k = \sum_i y_i^k = 0$ minden $1 \leq k \leq t - 2$ esetén. Azt mondjuk, hogy T *szuper-Vandermonde halmaz*, ha $\pi_k = \sum_i y_i^k = 0$ minden $1 \leq k \leq t - 1$ esetén. Könnyű látni (Vandermonde-determináns segítségével, innen az elnevezés), hogy $p|t$ esetén a Vandermonde-, különben meg a szuper-Vandermonde halmazok extrémálisak abban az értelemben, hogy ennél több hatványösszeg nem tűnhet el. (A Vandermonde-halmazt $p|t$ esetére Gács és Weiner definiálta.) Néhány példa:

- $\text{GF}(q)$ tetszőleges additív részcsoportha Vandermonde-halmaz;
- $\text{GF}(q)$ tetszőleges multiplikatív részcsoportha szuper-Vandermonde halmaz;
- ha azonosítjuk $\text{AG}(2, q)$ -t $\text{GF}(q^2)$ -tel, akkor ha veszünk egy olyan hiperovális, melynek 2 ideális pontja van, akkor az affin rész Vandermonde-halmaz $\text{GF}(q^2)$ -ben;
- ha azonosítjuk $\text{AG}(2, q)$ -t $\text{GF}(q^2)$ -tel, akkor egy kis Rédei-féle lefogóhalmaz affin része Vandermonde-halmaz $\text{GF}(q^2)$ -ben.

Sok nagyon nehezen klasszifikálható, geometriailag definiált halmaz is Vandermonde-féle, mint például a hiperoválisok (azaz $(q + 2)$ -pontú olyan halmazok, melyeket minden egyenes 0 vagy 2 pontban metsz), melyek klasszifikálása reménytelen feladatnak tűnik, ezért általában az sem várható, hogy a (szuper-) Vandermonde-halmazokat teljesen leírjuk. Amit a 10. szakaszban bemutatunk, az a kicsi és a nagy szuper-Vandermonde halmazok teljes leírása.

Theorem 10.12. (SzP, Takáts) *Legyen $T \subset \text{GF}(q)$ egy szuper-Vandermonde halmaz. Ha $|T| < p$ vagy $|T| > q/p$, akkor T egy multiplikatív részcsoporth (vagy annak mellékosztálya).*

4. Köszönetnyilvánítás

Szeretnék köszönetet mondani társszerzőimnek, közülük is kiemelném azokat, akikkel a témában több közös cikket is írtunk: Aart Blokhuis, Simeon Ball, Jörg Eisfeld, Fancsali Szabolcs, Sandy Ferret, Gács András, Leo Storme, Szőnyi Tamás, Takáts Marcella, Weiner Zsuzsa.

Hálás vagyok családom, szeretteim kitartó támogatásáért, segítségéért.

Végül, de nem utolsósorban annak szeretnék köszönetet mondani, aki nek talán legnagyobb része volt a jelen dolgozat megszületésében: Szőnyi Tamásnak, akitől már diákként eltanulhattam a szép véges struktúrák iránti lelkesedést, és aki azóta is számtalan módon — tanárként, aspiránsvezetőként, társszerzőként — segítette, segíti munkámat tanácsaival.

Irodalomjegyzék

[A disszertáció a következő cikkekre épül:]

- [SzP2func] S. BALL, A. GÁCS, P. SZIKLAI, On the number of directions determined by a pair of functions over a prime field, *J. Combin. Theory Ser. A* **115** (2008), 505-516.
- [SzPflock] P. SZIKLAI, Partial flocks of the quadratic cone, *J. Combin. Th. Ser. A*, **113** (2006), 698-702.
- [SzPflhigh] P. SZIKLAI, Flocks of cones of higher degree, *J. Algebraic Combin.*, **25** (2007), 233–238.
- [SzPnopts] P. SZIKLAI, A conjecture and a bound on the number of points of a plane curve, *Finite Fields Appl.*, **14** (2008), 41–43.
- [SzPblin] P. SZIKLAI, On small blocking sets and their linearity, *J. Combin. Th. Ser. A*, **115** (2008), 1167-1182.
- [SzPvdm] P. SZIKLAI AND M. TAKÁTS, Vandermonde and super-Vandermonde sets, *Finite Fields Appl.*, **14** (2008), 1056-1067.
- [SzPdirec] J. DE BEULE, P. SZIKLAI AND M. TAKÁTS, On the structure of the directions not determined by a large affine point set, *J. Algebr. Combin.*, DOI 10.1007/s10801-013-0430-4.
- [SzPkblock] L. STORME AND P. SZIKLAI, Linear point sets and Rédei type k -blocking sets in $\text{PG}(n, q)$, *J. Alg. Comb.* **14** (2001), 221–228.
- [SzPcomd] S. BALL, A. BLOKHUIS, A. GÁCS, P. SZIKLAI, ZS. WEINER, On linear codes whose weights and length have a common divisor, *Advances in Mathematics* **211** (2007), 94–104.

[A szerző további, a disszertációban megemlített cikkei:]

- [SzPnuc] P. SZIKLAI, Nuclei of point sets in $\text{PG}(n, q)$, *Disc. Math.*, **174** (1997), 323-327.
- [SzPdpow] P. SZIKLAI, Subsets of $\text{GF}(q^2)$ with d -th power differences, *Disc. Math.*, **208-209** (1999), 547-555.
- [SzPrand] P. SZIKLAI, A lemma on the randomness of d -th powers in $\text{GF}(q)$, *Bull. Belg. Math. Soc.* **8** (2001), 95-98.
- [SzPnuc2] A. GÁCS, P. SZIKLAI AND T. SZŐNYI, Two remarks on blocking sets and nuclei in planes of prime order, *Designs, Codes and Cryptography*, **10** (1997), 29-39.
- [SzPszt] P. SZIKLAI AND T. SZŐNYI, Blocking sets and algebraic curves, *Rend. Circ. Mat. Palermo* **51** (1998), 71-86.
- [SzPmult1] S. FERRET, L. STORME, P. SZIKLAI, Zs. WEINER, A $t \bmod p$ result on weighted multiple $(n - k)$ -blocking sets in $\text{PG}(n, q)$, *Innovations in Incidence Geometry*, **6-7** (2009), 169-188.
- [SzPmult2] S. FERRET, L. STORME, P. SZIKLAI, Zs. WEINER, A characterization of multiple $(n - k)$ -blocking sets in projective spaces of square order, *Advances Geom.*, **14** (2012), 739-756.
- [SzPfewpt] SZ. FANCSALI, P. SZIKLAI, M. TAKÁTS The number of directions determined by less than q points, *J. Algebr. Combin.* **37** (2013), 27-37.
- [SzPVdV] P. SZIKLAI, G. VAN DE VOORDE, A small minimal blocking set in $\text{PG}(n, p^t)$, spanning a $(t - 1)$ -space, is linear, *Designs, Codes, Crypt.*, DOI 10.1007/s10623-012-9751-x.
- [SzPpolybk] P. SZIKLAI, Polynomials in finite geometry, <http://www.cs.elte.hu/~sziklai/poly.html> , in preparation.

[Néhány fontos hivatkozás:]

- [1] T.L. ALDERSON, A. GÁCS, On the maximality of linear codes, *Des. Codes Cryptogr.* **53** (2009), 59–68.
- [11] S. BALL, A. BLOKHUIS, F. MAZZOCCA, Maximal arcs in Desarguesian planes of odd order do not exist, *Combinatorica* **17** (1997), 31–41.
- [20] A. BARLOTTI, Sui $\{k, n\}$ -archi di un piano lineare finito, *Boll. Un. Mat. Ital.* **11** (1956), 553–556.
- [24] A. BLOKHUIS, On the size of a blocking set in $\text{PG}(2, p)$, *Combinatorica* **14** (1994), 273–276.
- [32] A. BLOKHUIS, Á. SERESS, H. A. WILBRINK, On sets of points without tangents, *Mitt. Math. Sem. Univ. Giessen* **201** (1991), 39–44.
- [33] A. BLOKHUIS, S. BALL, A. BROUWER, L. STORME AND T. SZÖNYI, On the number of slopes determined by a function on a finite field, *J. Comb. Theory Ser. (A)* **86** (1999), 187–196.
- [44] A.A. BRUEN AND J.C. FISHER, The Jamison method in Galois geometries, *Designs, Codes and Cryptography* **1** (1991), 199–205.
- [62] A. GÁCS, ZS. WEINER, On $(q + t, t)$ -arcs of type $(0, 2, t)$, *Designs, Codes and Cryptography* **29** (2003), 131–139.
- [69] J. W. P. HIRSCHFELD, G. KORCHMÁROS AND F. TORRES, *Algebraic Curves over a Finite Field*, Princeton University Press.
- [72] M. HOMMA, S.J. KIM, Around Sziklai’s conjecture on the number of points of a plane curve over a finite field, *Finite Fields Appl.* **15** (2009), 468–474.
- [73] M. HOMMA, S.J. KIM, Sziklai’s conjecture on the number of points of a plane curve over a finite field II, *Finite fields: theory and applications*, 225–234, Contemp. Math., **518**, Amer. Math. Soc., Providence, RI, 2010.
- [74] M. HOMMA, S.J. KIM, Sziklai’s conjecture on the number of points of a plane curve over a finite field III, *Finite Fields Appl.* **16** (2010), 315–319.

- [75] R.E. JAMISON, Covering finite fields with cosets of subspaces, *J. of Comb. Th. Ser. A* **22** (1977), 253–266.
- [82] G. LUNARDON, Linear k -blocking sets, *Combinatorica* **21** (2001), 571–581.
- [85] P. POLITO, O. POLVERINO, On small blocking sets, *Combinatorica* **18** (1998), 133–137.
- [91] L. RÉDEI, *Lückenhafte Polynome über endlichen Körpern*, Akadémiai Kiadó, Budapest, and Birkhäuser Verlag, Basel, 1970 (English translation: *Lacunary polynomials over finite fields*, Akadémiai Kiadó, Budapest, and North Holland, Amsterdam, 1973).
- [109] T. SZŐNYI, ZS. WEINER, Small blocking sets in higher dimensions, *J. Combin. Th. Ser. A* **95** (2001), 88–101.