

Sziklai Péter
„Applications of polinomials over finite fields”
című értekezésének bírálata

Geometriai kérdések algebraizálása Descartes XVII. századi munkájáig és Felix Klein 1872-ben bemutatott Erlangeni programjáig nyúlik vissza. A véges geometriák egyik első komoly eredménye, Segre tétele is egy ilyen algebraizálás eredménye, mely a másodfokú polinomok és az oválisok közt létesít kapcsolatot. A véges geometriai kutatások egyik fő ága a 60-as 70-es években az Erlangeni program szellemében inkább a véges csoportok elmélete felől közelített a problémákhoz. Mára ez az irány részben kimerült, részben a csoportelmélet felé csúszva annak részévé vált.

A 70-es években új erőre kapott a véges síkok pontthalmazainak az azokat leíró egyenletekkel való vizsgálata. Személyes emlékeimben – számomra – Blokhuis és Wilbrink egy egyoldalas frappáns cikke villantotta fel a polinomos megközelítésben rejlő új lehetőséget. Az akkor még ötletszerűnek tűnő megoldások lassan szervesen összekapcsolódó elméletté álltak össze, és mára a polinomos technika sok, rég óta nyitott kérdés megoldásának első számú eszközévé vált. E technika elemei közé kerültek algebrai kutatási eredmények, mint pl. Rédei véges testek fölötti hézagok polinomokra vonatkozó elmélete, vagy az algebrai geometria bizonyos klasszikus és friss eredményei.

Ebben a folyamatban fontos szerepet játszik a Szőnyi Tamás vezette véges geometriai iskola, mely a többségében belga, holland és olasz kutatócsoportokkal szorosan együttműködve meghatározó eredményeket ért el, és amely hosszú ideje e téma kutatásának élvonalában van. Sziklai Péter ennek a kutatócsoportnak egyik tevékeny tagja.

Az algebrai módszerek véges geometriákban való itt vázolt alkalmazása párhuzamba állítható, és több szálon kapcsolódik is a kombinatorika más területein zajló és új utakat nyitó hasonló folyamatokkal – elég, ha csak a Babai László és Frankl Péter befejezetlen könyvében összefoglalt lineáris algebrai technikákra, vagy Alon „Combinatorial Nullstellensatz”-ára gondolunk.

Sziklai Péter doktori disszertációjának formája *értekezés*, mely teljes egészében a cím megszerzése céljából készült. Fő témája nagyon tömören fogalmazva: *véges geometriák adott metszési tulajdonságú pontthalmazai lehetséges méretének meghatározása főként – a halmazt jellemző – valamely polinom vizsgálatával*. Adott metszési tulajdonságon itt egészen egyszerűen megfogalmazható feltételeket kell érteni, melyek kombinatorikai és geometriai feltételnek

egyaránt tekinthetők, pl. a pontthalmazt minden egyenes vagy minden k -dimenziós altér messe, minden egyenes legföljebb 2 pontban messe, minden egyenes egy pontban messe mod p vagy 0 pontban mod r , stb. A méret meghatározásában főként az extrémális értékek érdekesek. Ez maga után vonja az extrémális méretű konstrukciók megkeresését, jellemzését, és azok stabilitásának vizsgálatát, azaz annak eldöntését, hogy az extrémális-hoz valamilyen evidens módon közeli konstrukciók mindegyike származtatható-e az extrémálisból pl. néhány pont el- vagy hozzá vételével.

A disszertáció rövid bevezető fejezetekkel kezdődik, mely tömören áttekinti az alapfogalmakat, így a témában kevésbé jártas olvasó számára is lehetővé teszi a dolgozat eredményeinek követését! Az 5. és 6. fejezet a felhasznált legfontosabb polinomfajtákat és azok alaptulajdonságait veszi sorra (Rédei-polinom, hatványösszeg polinom, gyökpolinom, iránypolinom), míg a 8. fejezet az algebrai geometria néhány klasszikus eredményét, és az újabbak közül az 1986-ból származó és a véges test feletti irreducibilis algebrai görbék racionális pontjainak számát becslő Stöhr–Voloch-tételt. A fejezet Szőnyi egy korábbi lemmájának fontos általánosításával zárul (8.9). Eszerint ha egy $\text{GF}(q)$ fölötti C_n görbének nincs d -edfokú komponense, és α olyan konstans, hogy $n \leq \alpha\sqrt{q} - \frac{1}{\alpha} + 1$ és $\alpha \geq \frac{1}{d+1} + \frac{d(d-1)\sqrt{q}}{(d+1)(q+1)}$, akkor a görbe $\text{PG}(2, q)$ -beli pontjainak száma legföljebb $n(q+1)\alpha$.

A 9. fejezet vezet át az előkészítő részből a tematikus, valamely problémakört áttekintő nagyobb fejezetekhez. Ebben az extrémális-hoz közeli esetek vizsgálatának egyik polinomos technikája van összefoglalva. Az itt említett példák közül azt az eredményt emeljük ki (9.2), amely szerint $q - c\sqrt{q}$ darab, páronként diszjunkt grafikonú legföljebb d -edfokú polinomok rendszere kiegészíthető q -eleművé a diszjunkttság megtartása mellett.

A 10. fejezet olyan pontthalmazokkal foglalkozik, melyeket minden egyenes valamely modulus szerint konstans sok pontban metsz. E kérdés érdekes és fontos voltát két eredménnyel szemléltetjük: az egyik a maximális ívek metszetszámaira adódó oszthatósági feltétel, és páratlan q esetére a nemlétezésükről szóló Ball–Blokhuis–Mazzocca-tétel, a másik Szőnyi Tamásnak az az eredménye, hogy minimális kis lefogóhalmazt minden egyenes egy pontban metsz mod p . A Galois-síkok mod p konstans metszetszámot adó pontthalmazaira vonatkozó eredmény e halmazokra 0-értékű hatványösszegekkel kifejezhető ekvivalens algebrai feltételt ad. Ez így egy önmagában is érdekes végestest-elméleti kérdésre vezet: melyek azok a t -elemű halmazok egy véges testben, melyek minden $t - 1$ -nél (illetve t -nél) kisebb kitevőjű hatványösszegei nullák. Előbbieket *Vandermonde*-, utóbbiakat *super-Vandermonde-halmazoknak* nevezik. E kérdés megválaszolása egyelőre reménytelennek tű-

nik. E fejezetből kiemelem a jelölt Takács Marcellával közös cikkében publikált eredményét (10.12, 10.13), mely szerint a p -nél kisebb és q/p -nél nagyobb szuper-Vandermonde-halmaz csak egy multiplikatív részcsoporthoz tartozhat.

A 11. fejezet lefoglaló ponthalmazokról szól. E több évtizede vizsgált kérdésben épp a polinomos technikák hoztak áttörést. Így e disszertációnak is ez egyik legfontosabb része. A téma szépségét meggyőzően bizonyítja a szerző *linearitási sejtése*. Ez azt mondja, hogy $PG(n, q)$ -ban minden minimális k -lefoglaló ponthalmaz egy alkalmas résztest feletti lineáris részhalmaz. Ez egy egyszerű illeszkedési feltétel és egy egyszerű algebrai feltétel lehetséges ekvivalenciáját állítja. Érdekes ott kutakodni, ahol sok évtizedes vizsgálat után még ilyen egyszerűen megfogalmazható elegáns eredmény elérésének esélye sejlik fel. E sejtés bizonyítása felé a szerző a következő lépést tette: bizonyította (11.33-35), hogy ha $PG(2, p^h)$ -ban egy lefoglaló halmazt minden egyenes 1 pontban metsz mod p^e , akkor a szelők nagy része pontosan $p^e + 1$ pontban metszi, ezek a szelők izomorfak a $PG(1, p^e)$ egyenessel, és $e \mid h$. A következő lépés a $PG(n, q)$ -beli kisméretű, minimális, a k -dimenziós altereket lefoglaló ponthalmazokra egy hasonló tétel igazolása (11.38). Ráadásként egy rövid bizonyítást kapunk a Ball–Blokhuis–Brouwer–Storme–Szőnyi-tételre (továbbiakban B^3S^2), mely szerint kis Rédei-típusú lefoglaló halmaz lineáris. A bizonyításokban fontos szerepet kap a Rédei-polinom ügyes három tagra osztásából származó három algebrai görbének és egymáshoz való viszonyuknak vizsgálata.

A 12. fejezet $PG(n, q)$ Rédei-típusú k -lefoglaló halmazait vizsgálja. Bár e fejezet nem a polinomos technikát alkalmazza, az itteni eredmények sok szállal kapcsolódnak a disszertáció többi részéhez. Egyik fontos eredménye a síkbeli Rédei-féle lefoglalóhalmazokra vonatkozó B^3S^2 -tétel magasabb dimenziós általánosítása, mely szerint egy q^k affin ponttal rendelkező és szelői által legföljebb $\frac{q+3}{2}q^{k-1} + q^{k-2} + \dots + q^2 + q$ ideális pontot lefoglaló $AG(n, q)$ -beli ponthalmaz egy alkalmas résztest fölötti altér eltoltja.

A 13. fejezet a „Stabilitás” címet viseli. Bár e téma a disszertáció korábbi és későbbi fejezeteiben is megjelenik, itt kerül a vizsgálat fókuszpontjába. Először a korlátok közé szorított számú irányt meghatározó és q -hoz közeli pontszámú halmazok stabilitására vonatkozó Szőnyitől származó 1996-os eredmény általánosításait sorolja fel a szerző. Ezek azt állítják, hogy adott korlátok mellett a q -nál kisebb méretű halmazok kiegészíthetők, a nagyobbak pontok elhagyásával lecsökkenthetők q -eleművé, hogy az így kapott halmaz is ugyanazokat az irányokat határozza meg, mint az eredeti. Ezután egy szerteágazó alkalmazásokkal rendelkező témát vizsgál alaposabban a

jelölt, a parciális flokkokét. A kérdés az, hogy ha egy C^* kvadratikus kúpot, vagy még általánosabban egy $(1, T, T^d)$ alakú pontokból álló görbére épített hengert, $q - \varepsilon$ sík diszjunkt irreducibilis görbékben metsz, akkor található-e további ε sík, melyek irreducibilis metszetgörbéit az előzőkhöz véve azok particionálják C^* -ot. A szerző e kérdésre a $2 \leq d \leq \sqrt[6]{q}$, $\varepsilon < \lfloor \frac{1}{d^2} \sqrt{q} \rfloor$ esetben az egyértelmű bővíthetőséget bizonyítja. A bizonyítás egy olyan algebrai görbe megkonstruálásán múlik, melyből kiolvasható a hiányzó elemek egyértelmű létezése.

A 14. fejezet az előzőben is tárgyalt, ponthalmaz által lefoglalt irányok halmazát vizsgálja, de itt épp a le nem fogott irányok struktúrájára koncentrálna. A szerzőtársakkal (De Beule és Takács) írt cikk egy szép eredménye, hogy ha $AG(n, q)$ egy $q^{n-1} - 2$ pontú halmazához nem vehető 2 pont úgy, hogy a szelők által lefoglalt irányok halmaza ne növekedjen, akkor a le nem fogott ideális pontok vagy egy egyenes legföljebb $\lfloor \frac{q+3}{2} \rfloor$ pontját alkotják vagy egy síkbeli kúpszeleten vannak. A 3-dimenziós esetben nagyobb eltérést is sikerült jellemezni: ha az $AG(3, q)$ tér egy $q^2 - \varepsilon$ halmaza nem bővíthető ε ponttal a lefoglalt ideális pontok növekedése nélkül, ahol $\varepsilon < p$, akkor a le nem fogott ideális pontok $\varepsilon^4 - 2\varepsilon^3 + \varepsilon$ -fokú síkgörbén helyezkednek el.

Az utolsó fejezet a dolgozaton végigvonuló Rédei-féle problémakör egy általánosítását tárgyalja. Az $f : GF(q) \rightarrow GF(q)$ függvény grafikonja szelők iránytangensei közt egy c testelem pontosan akkor nem szerepel, ha az $x \mapsto f(x) - cx$ leképezés permutációs polinom. Az általánosítás ötlete az, hogy egy (f, g) függvénytér $(x, f(x), g(x))$ pontokból álló grafikonjának szelők pontjai pontosan akkor nem fognak le egy (c, d) számpárral jellemzett irányt, azaz ideális egyenest, ha az ideális egyenesen átmenő síkok mindegyikén egyetlen pontja van a grafikonnak, azaz ha az $x \mapsto f(x) + cg(x) + dx$ függvény permutációs polinom. E problémára szép választ ad Ball-Gács-Sziklai egy cikkének eredménye, mely szerint ha $p = 6s - k$ alakú prím, ahol $-1 \leq k \leq 4$, és a le nem fogott irányok száma nagyobb, mint $8s^2 + (4 - k)s - k/2$, akkor a pontok egy síkba esnek!

Kritikai megjegyzéseim: az értekezés egyes részein (pl. a 12. fejezetben) az eredmények mellől elmaradtak a hivatkozások, ami pedig egy ilyen összefoglaló dolgozatnál fontos lenne. Bár a mű felépítése, szerkezete világos, a fejezetek nagy száma miatt kissé szétcsúsznak. Ennek oka, hogy az első kilenc fejezet lényegében előkészítő jellegű, döntően az alkalmazott technikák elemeit foglalja össze, közülük több összesen csak 2-3 oldalas, némelyikükben csak egyetlen alfejezet van, vagy épp egy sincs. Megítélésem szerint ezeket egyetlen fejezet alá téve nagyobb hangsúlyt kapott volna az ezt követő 6 fejezet, mely egyébként már világosan – tartalmilag jól elkülönülő részek-

re – van felosztva. Így talán a fejezetek világosabb szerkezetet, arányosabb, egyenletesebb beosztást, áttekinthetőbb struktúrát adtak volna az értekezésnek.

A disszertáció megjelenése megfelel a formai kívánalmaknak, legfeljebb csak néhány tipográfiai hiba szúr szemet (pl. a hibásan írt oszthatósági jelek, azaz $a \mid b$ helyett $a|b$, $\mid$ helyett $|$, a szükségtelen spórolás a hosszú képletek eltörésével, az itt-ott rosszul méretezett zárójelek, a hármaspontok nagyon gyakori három ponttal helyettesítése, ... helyett ...). A dolgozatban értelemzavaró következtetlenségeket vagy tartalmi hibákat nem találtam.

Kérdésem: Mit lehet tudni az értekezésben használt új, és a véges geometriai kérdésekre kihegyezett polinomos technikáknak a matematika egyéb területein való alkalmazhatóságáról?

Összefoglalva: A szerző a polinomos technika elemeinek továbbfejlesztésében és alkalmazásában számos – a legfrissebb nemzetközi kutatások élvonalába tartozó – eredményt ért el. Az ezeket összefoglaló értekezést alkalmasnak tartom a nyilvános védelemre, a benne összefoglalt eredményeket elegendőnek tartom az MTA doktori cím megszerzéséhez.

Budapest, 2014-02-26

Wetl Ferenc