# Kódelmélet és környéke (OTKA 49662) záró beszámoló

A beszámolóban használt jelölések: $q = p^h$ prímhatvány, GF$(q)$ véges, $q$-elemű test, PG$(n, q)$ illetve AG$(n, q)$ a GF$(q)$ feletti $n$ dimenziós projektív illetve affin tér. A hivatkozások részben a feltöltött közlemény-jegyzékre, részben a beszámoló végén felsorolt, még meg nem jelent dolgozatainkra utalnak.

Kódelméletben gyakran hasznos véges projektív terek speciális egyenes-, illetve hipersíkmetszetű ponthalmazainak vizsgálata. Kutatásaink ilyen problémákra koncentrálódtak. Bizonyos cikkeinknek (pl. [SzW] és [BBGSzW]) közvetlen kódelméleti alkalmazása is van, mások a geometriai ill. algebrai szálakon keresztül kapcsolódnak a témakörhöz. Eredményeink közül kiemelnénk a polinom módszer *közvetlen* térbeli alkalmazásait (mely ma még kezdetleges állapotban van), ami új eszközt jelenthet a véges test feletti kódok vizsgálatában. A felsorolt cikkek közül [BBGSzW], [BG] és [BGSz] használ polinom módszert közvetlenül a térbeli problémára.

A korábbiaknak megfelelően a vizsgált problémák nagy része véges projektív terek részhalmazainak hipersíkokkal való metszési számaival kapcsolatos. Ezek a kérdések direkt módon fordíthatóak le kódelméleti alkalmazásokra. Ugyancsak szorosan kapcsolódik kódelmélethez a Rédei által kezdeményezett irány-probléma is, amint az Alderson, Bruen és Silverman munkáiból látható.

[BBGSzW]-ben a szerzők a polinomos módszer szellemes alkalmazásával bebizonyították, hogy PG$(2, q)$ egy olyan ponthalmaza, melyet minden egyenes egy adott $r$ mod $p$ pontban metsz, legalább $(r-1)q + (p-1)r$ pontú kell legyen, ahol $p$ a karakterisztika, továbbá $r$ osztja $q$ -t. Az eredményből következik, hogy egy 3 dimenziós kód, melynek hossza és súlyai is oszthatók $r$-rel és melynek minimális távolsága legalább 3, legalább $(r-1)q+(p-1)r$ hosszú kell legyen. A cikk magasabb dimenzióra is általánosítja az eredményeket. Megjegyezzük, hogy Ball, Blokhuis és Mazzocca híres, maximális ívek nemlétezéséről szóló tétele is egyszerű következménye az eredménynek.

A [FSSzW] dolgozatban, **Sziklai** és **Weiner** Ferret-tel és Storme-val megmutatták, hogy PG$(n, q)$-beli, kis méretű minimális, súlyozott, $t$-szeres, $k$-dimenziós altereket lefogó ponthalmazok olyanok, hogy minden $k$-dimenziós alteret $t$ mod $p$ pontban metszenek. A [FSSzW] dolgozatbeli eredmény **Szőnyi** és **Weiner** korábbi, egyszeres lefogó ponthalmazokról szóló hasonló eredményét általánosítja.

Blokhuis, Lovász, Storme és **Szőnyi** elkészítették a testre épített síkok többszörös lefogó ponthalmazairól szóló dolgozatukat [BLSSZ]. Ennek fő eredménye, hogy a kis $t$-szeres lefogó ponthalmazokat minden egyenes $t$ modulo $p$ pontban metszi, ahol $p$ a koordinátatest karakterisztikája. Felhasználva ezt az eredményt, megjavítják a $t$-szeres lefogó ponthalmazokra vonatkozó eddig ismert becsléseket is.

Fancsali és **Sziklai** [FSz] általánosítják **Gács** és **Szőnyi** korábbi, részleges egyenes-befedésekre vonatkozó eredményeit. Itt a módszer a Lovásztól származó törtlefogásos becslésen és magas dimenziós Segre-varietások vizsgálatán alapszik. A cikk eredménye, hogy nagyon sok különböző méretre konstruálnak $(3m-1)$-dimenziós projektív térben tartalmazásra nézve maximális, síkokból álló részleges befedést.

**Sziklai** és Ligeti a [LSz] cikkben két részbenrendezett halmaz, $D^{k,n}$ és $B_{m,n}$

automorfizmus-csoportját határozta meg. A kérdéskör az insertion-deletion kódokhoz kapcsolódik. A $D^{k,n}$ struktúra DNS-kódokat tartalmaz, az itt bizonyított eredmény a ,,sima" szavakra vonatkozó korábbi eredmény analogonja, noha a bizonyítás - a struktúra bonyolultsága miatt - nehezebb. A $B_{m,n}$ struktúra automorfizmus-csoportja korábban is ismert volt (Burosch-Gronau-Laborde 1999), de a korábbi több mint 10 oldalas bizonyítást (a kifejlesztett technika segítségével) 1 oldalasra sikerült redukálni.

**Gács** Jan De Beule-vel közösen azt mutatta meg, hogy a $Q(4,q)$ poláris térben nincsenek $q^2-1$ méretű maximális parciális ovoidok ha $q$ egy prímszám legalább második hatványa. Ismert konstrukció $q = 3, 5, 7, 11$ esetén, így izgalmas kérdés maradt, hogy nagy $q$-ra van-e példa olyankor, ha $q$ prím. Módszerük azt használja ki, hogy $Q(4,q)$ Tits-től származó $T_2(O)$ reprezentációjában a probléma arra a sokat vizsgált kérdésre vezethető vissza, hogy egy AG$(3,q)$-beli ponthalmaz milyen irányokat határoz meg. A kidolgozott módszer megoldja az említett eredmény irányos megfelelőjét és új bizonyítást ad Ballék eredményeire.

**Sziklai** [Sz1]-ben (polinomokat és algebrai görbéket használva) azt bizonyította be, hogy PG(3,$q$)-ban egy kúp részleges flock-ja, mely $q-\varepsilon$ síkból áll, egyértelműen kiegészíthető (további $\varepsilon$ sík hozzávételével) flock-ká, ha $\varepsilon < cq^{(1/2)}$. [Sz3]-ban az [Sz1]-beli eredményt sikerült (másodrendűnél) magasabb fokú görbére emelt kúpokra általánosítani. A bizonyításhoz a korábbiak mellett új ötletek is kellenek, pl. egy szimmetrikus szerkezetű determináns vizsgálata.

**Sziklai** [Sz2]-ben AG$(3,p)$-beli, $p^2$ pontú ponthalmaz által meghatározott irányok számára bizonyít korlátokat, majd **Gács** egy eredményét felhasználva megmutatja, hogy a kevés irányt meghatározó ponthalmazok hengeres szerkezetűek; végül Rédei ill. Wielandt egy-egy csoportelméleti tételét általánosítja, felhasználva a geometriai eredményt.

**Sziklai** [Sz5]-ben PG$(2,q)$ kisméretű, azaz $3(q+1)/2$-nél kevesebb pontú lefogóhalmazaira igazol egy struktúratételt. Itt a régi nagy sejtés, hogy az ilyen lefogóhalmazok GF($q$) egy részteste felett lineárisak; a cikk azt igazolja, hogy a lefogóhalmaz minden egyenesmetszete 1 mod $p^e$ méretű, ahol GF($p^e$) résztest, és hogy majdnem minden egyenes GF($p^e$)-lineáris ponthalmazban metsz.

**Weiner** Ball-lal közösen, 'An Introduction to Finite Geometry' címmel egyetemi jegyzetet írt [BW]. A jegyzet felsőbb éves hallgatóknak körülbelül 12 előadásra való anyagot tartalmaz.

**Gács** és **Szőnyi** áttekintő cikket írt arról a véletlen módszerről, mellyel sűrűségi eredményeket bizonyítottak projektív síkok lefogó ponthalmazairól és projektív terek részleges egyenes fedéseiről [GSZ].

**Gács** és **Sziklai** Ballal közösen a klasszikus irány probléma egy 3-dimenziós általánosítását vizsgálta és bizonyított nagyságrendileg éles becslést nem síkbeli ponthalmazok által meghatározott irányok számáról [BGSz]. Az eredmény permutációpolinomok nyelvén a következő: ha $f$ és $g$ a $p$ (prím) elemű véges test feletti polinomok, melyekre nem teljesül $g(x) = f(x) + cx + d$, akkor legfeljebb $2p^2/9$ $(a,b)$ párra teljesülhet, hogy $f(x) + ag(x) + bx$ permutáció polinom (azaz bijektív függvény).

[GH] **Gács** Hégerrel közösen véges geometriai módszerekkel kis csúcsszámú $(k,g)$-gráfokat konstruált ($k$-reguláris, $g$ bőségű gráfok). A konstrukció megjavítja a korábbi becsléseket a minimális csúcsszámra azokban az esetekben, amikor $g = 6$

és $k$ négyzet prímhatvány, illetve $g = 8$ és $k$ prímhatvány. Azt is megmutatják, hogy a konstrukciós módszerből (mely Browntól származik és lényege, hogy egy általánosított sokszög illeszkedési gráfjából dob ki pontokat) $g = 6$ esetén jobb nem is jöhet ki, a fenti esetben.

[KSz] **Szőnyi** Korchmárossal közösen összefoglaló cikket írt affin szabályos sokszögekről, amelyben az affin szabályos sokszögek Bachmann-Schmidt és Kárteszi féle felépítését tárgyalják, valamint az affin szabályos sokszögek véges geometriai alkalmazásait. Megvizsgálják azt a problémát is, hogy egy affin szabályos sokszögnek hány szelője megy át a sík egy pontján.

**Sziklai** megfogalmazott egy sejtést algebrai síkgörbék pontjainak számáról: $n$-edfokú, lineáris komponens nélküli görbének legfeljebb $(n-1)q+1$ pontja lehet. Az $(n-1)q+n$ -es felső becslés triviális (Barlotti), a cikkben $(n-1)q+n/2$ -t sikerült igazolni. Ilyen görbék nagy $(k, n)$-íveket, és így hatékony kódokat adnak. Az eredmény a 2008-ban megjelent, Hirschfeld-Korchmáros-Torres által írt, algebrai görbékről szóló könyvbe is belekerült.

Az alábbiakban kiemeljük a pályázat utolsó évének eredményeit.

**Szőnyi** Blokhuis-szal és Brouwer-rel dolgozott az elmúlt egy évben. Egyszerű bizonyítást találtak az affin lefogó ponthalmazokról szóló Jamison, Brouwer–Schrijver féle eredményre. A bizonyítás kis módosításával több struktúrára (másodrendű felületek, Hermite-felületek, bizonyos algebrai görbék) megvizsgálható a majdnem fedések kérdése, azaz becslés adható azon hipersíkok számára, amelyekkel az adott struktúra egy pont híján lefedhető. A bizonyítás projektív terek hipersíkjai által generált kódok polinomfüggvények segítségével történő leírását (is) használja. Érdemes megemlíteni, hogy projektív terek $r$-dimenziós alterekkel egy pont híján történő fedésére is éles eredményt kapták. Ugyancsak vizsgálták a Hilton-Milner tétel $q$-analógját [BBCFMPS]. Egy halmazrendszeres eredmény $q$-analógját úgy kapjuk, hogy az „$i$-elemű halmaz" kifejezést „$i$-dimenziós vektortér"-re cseréljük. Az Erdős-Ko-Rado tétel vektorterekre vonatkozó megfelelőjét Hsieh, valamint az $n = 2k$ esetben Frankl és Wilson bizonyította a hetvenes években. A Hilton-Milner tétel a második legnagyobb metsző halmazrendszer méretére ad éles becslést, ennek $q$-analógját látta be a $q \geq 3$, $n \geq 2k+1$ esetre Blokhuis, Brouwer, Chowdhury, Frankl, Mussche, Patkós és **Szőnyi**. Érdekes, hogy elég nagy dimenzióra ($n \geq 3k$) stabilitási eredményt láttunk be: egy a Hilton-Milner korlátnál jóval kisebb korlátnál nagyobb metsző altérrendszerek lényegében leírhatók.

**Irányok a síkban és a térben.** A síkbeli irányprobléma azt kérdezi, hogy egy $q$ rendű affin síkon adott $q$-elemű ponthalmaz hány irányt határozhat meg. A probléma teljesen meg van oldva (Ball-Blokhuis-Brouwer-Storme-**Szőnyi**) olyankor, amikor az irányok száma legfeljebb $q/2$. A $q/2$-nél több irányt meghatározó ponthalmazokról eddig csak a prím esetben volt ismert eredmény (Rédei-Megyesi, Lovász-Schrijver, **Gács**). Az eredmény bizonyításában nagy szerepet játszottak polinomok dupla hatványösszegei. Később ugyanezek jöttek elő a probléma térbeli általánosításánál. **Gács**, Lovász és **Szőnyi** a $q = p^2$ esetben ért el eredményt a nyitott esetben. Megmutatták, hogy ilyenkor az irányok száma vagy $(q+3)/2$ (és izomorfia erejéig egyetlen ilyen halmaz van) vagy több, mint $(q+\sqrt{q})/2$. Ez egy Polverino-**Szőnyi-Weiner** konstrukció miatt éles. A bizonyítás a dupla hatványösszeges módszer és a hézagos polinomos módszer ötvözete.

**Gács** és Ball (a tavalyi térbeli eredmény által motivált) alábbi problémát vizsgálták. Milyen lehet egy prímtest feletti polinom grafikonja, ha tudjuk, hogy első néhány dupla hatványösszege nulla. Kiderül, hogy már akkor nagyon erős struktúrája van a grafikonnak, ha az első gyök $p$ dupla hatványösszeg nulla. Ez sokkal erősebb, mint azok az algebrai segédtételek, melyek a már idézett irányos cikkekben kellenek. Megmutatták, hogy ha az első $p/3$ dupla hatványösszeg nulla, akkor a grafikon része egy másodrendű görbének. Ez a fent emlegetett sík- és térbeli iránytételek eredeti bizonyítását jelentősen lerövidíti. Azt sejtjük, hogy sokkal kevesebb dupla hatványösszeg eltűnéséből is következik, hogy a grafikon része egy alacsony fokú algebrai görbének. Ez egy önmagában érdekes algebrai probléma. A sejtésben elért további részeredmények segíthetnek abban, hogy az eddigi $2p/3$ helyett $3p/4$ irányig teljesen leírjuk a síkbeli irányproblémát, illetve a térbeli problémában a nagyságrendileg éles becslést teljesen élessé tegyük.

Alderson és **Gács** azt bizonyítják, hogy ha egy lineáris $[n, k, d]_q$ kód kiterjeszthető nem feltétlenül lineáris $[n+1, k, d+1]_q$ kóddá, akkor a kiterjesztést lineáris módon is meg lehet csinálni. Vannak példák, amikor „nagyon nem-lineáris" bővítések is vannak, de az eredmény szerint ezek megléte magával vonja a lineáris létezését. Az eredményből az következik, hogy ha egy lineáris kód nem bővíthető lineárisan, akkor egyáltalán nem bővíthető. Sokféle olyan lineáris kód van, melyről korábbról tudjuk, hogy lineárisan nem bővíthető, például a véges geometriában sokat vizsgált teljes ívek adnak ilyet. Az eredmény Alderson, Bruen és Silverman korábbi eredményeinek általánosítása, az új ötlet az, hogy a kiterjeszthetőség vizsgálatára korábban kidolgozott véges geometriai modellben nem vetítéseket és síkbeli eredményeket, hanem közvetlenül térbelieket használnak. Érdekes kérdés, hogy kiterjeszthető-e az eredmény többszörös bővíthetőségre is. Egy ilyen eredményből például az következne, hogy az MDS sejtés lineáris és tetszőleges kódokra ekvivalens.

A [GHNP] dolgozatban **Gács** több társszerzővel egy S. Vinatier által felvetett kombinatorikus számelméleti problémát old meg. Az eredmény véges geometriai nyelven azt mondja, hogy néhány esettől eltekintve egy véges test feletti vektortér minden hipersíkja tartalmaz olyan vektort, melynek páronként különbözők a koordinátái. A kivételes esetek klasszifikálhatók. Kombinatorikus trükkök mellett a polinom módszert használták. Az eredmény másik ekvivalens formája azt vizsgálja, hogy egy előírt értékkészlethez mikor található kis fokú polinom véges test felett. Ez érdekes nyitott kérdéseket vet fel.

A [GHW] dolgozatban **Gács**, Héger és **Weiner** olyan gráfokat vizsgál, melyek $k$-regulárisak és 6 bőségűek (legrövidebb körük hossza 6). Egy először Brown által a hatvanas években alkalmazott, majd az utóbbi években több szerző által más terminológiával újrafelfedezett módszer ilyenek konstruálására az, hogy egy $q$ rendű projektív sík illeszkedési gráfjából (mely $q+1$-reguláris és 6 bőségű) kihagyunk pontokat úgy, hogy a maradék rész $k$-reguláris legyen. Ezt a módszert véges geometriai eszközökkel a Gács és Héger a korábbi [GH] dolgozatában kezdte vizsgálni. Ebben a cikkben algebrai módszereket (a stabilitási eredményeknél is alkalmazott rezultánsokat) is használva azt mutatták meg, hogy ha a kiindulási sík a $p$-elemű véges testre épített projektív sík, akkor olyankor, amikor $k$ nincs túl messze $q$-tól, a konstrukciós módszerből nem jöhet ki jobb, mint a már ismert konstrukciók. A következő lépés annak az általánosabb módszernek a vizsgálata lehet, melyben a

projektív sík illeszkedési gráfjának nem feltétlenül feszített részgráfját keressük.

**Sziklai** és Fancsali [FSz2]-ben a korábbi [FSz] cikkben már érintőlegesen tárgyalt kérdést elemzik részletesen: Adott a $\mathrm{PG}(1,q^h)$ projektív egyenes, és rajta egy $q^2+1$ elemű, $\mathrm{GF}(q)$ felett lineáris ponthalmaz. Milyen lehet e ponthalmaz geometriai és algebrai struktúrája? Az derül ki, hogy egy $\mathrm{PG}(1,q)$ részegyenessel való metszet 0,1,2,3 vagy $q+1$ pontú lehet. A ponthalmaznak tipikusan van egy kitüntetett pontja (és a többi $q^2$ ponton egy tranzitív csoport hat), egy speciális esetben pedig a $q^2+1$ pont az általa tartalmazott $\mathrm{PG}(1,q)$ részegyenesekkel egy úgynevezett Mőbius-síkot alkot (azaz bármely 3 pontra pontosan egy részegyenes illeszkedik).

**Sziklai** és Takáts a következő kérdést vizsgálták. $\mathrm{GF}(q)$ adott $t$ elemű részhalmazának fontos jellemzője az a legnagyobb pozitív egész $k$ szám, melyre a halmaz elemeinek első, második, ..., $(k-1)$-edik hatványösszege mind 0. Ez a szám legfeljebb $t-1$ vagy $t$ lehet attól függően, hogy a karakterisztika osztója-e $t$-nek vagy sem. Az olyan halmazokat, melyek elérik e felső korlátot, Vandermonde ill. szuper-Vandermonde halmazoknak hívjuk. E halmazok, amennyiben $\mathrm{GF}(q)$-ra mint a prímtestje feletti vektortérre gondolunk, szép geometriai tulajdonságokkal bírnak, és megfordítva, kiderül, hogy sok érdekes extremális geometriai konfiguráció ilyen részhalmazokhoz vezet. Az egyik érdekes eredmény, hogy nagy és kis $t$ érték esetén teljesen le tudtuk írni a szuper-Vandermonde halmazokat $\mathrm{GF}(q^2)$-ben: ezek csak akkor léteznek, ha $t$ osztja $(q-1)$-et, és akkor éppen a multiplikatív csoport $t$ elemű részcsoportjai (és ezek bizonyos transzformált képei) lehetnek csak.

Jelölje $C_k(n,q)$ a $\mathrm{GF}(p)$ felett $\mathrm{PG}(n,q)$ pontjai és $k$-dimenziós altereinek incidenciamátrixa által definiált kódot. Lavrauw, Storme, **Sziklai** és Van de Voorde belátta, hogy $C_k(n,q) \setminus C_{n-k}(n,q)^T$-ban nincs $(q^{(k+1)}-1)/(q-1)$ és $2q^k$ közötti súlyú kódszó, amiből következik, hogy nincs ilyen súlyú kódszó $C_k(n,q) \setminus C_k(n,q)^T$ -ben se, ha $k \geq n/2$. Az eredményt $k=n-1$ esetén alkalmazva $C_{n-1}(n,q)$ kis súlyú kódszavaira, bebizonyítottuk az éles korlátot általános $q$-ra, mely eddig csak speciális esetekben volt ismert.

[HMSzW]-ben **Szőnyi** és **Weiner**, Harrach-hal és Metsch-csel közösen $\mathrm{PG}(3,q)$, $q=p^{3h}$, $p \geq 7$ prím, $3(q^{n-1}+1)/2$-nél kisebb méretű olyan ponthalmazait vizsgálták, melyek minden egyenest 1 mod $\sqrt[3]{q}$ pontban metszenek. (Az ilyenek mind egyenesekre nézve lefogó halmazok.) Megmutatták, hogy ezen ponthalmazok ún. lineáris lefogó halmazok (speciális osztályba tartozó lefogó ponthalmazok). Valamint azt is, hogy $h=1$ esetén minden, $3(q^{n-1}+1)/2$-nél kisebb méretű, (tartalmazásra nézve) minimális, egyeneseket lefogó ponthalmaz lineáris.

[SzW]-ben **Szőnyi** és **Weiner** különböző véges geometriai struktúrákra, például $\mathrm{PG}(2,q)$ lefogó ponthalmazaira, páros halmazaira (olyan ponthalmazokra, melyek minden egyenest páros sok pontban metszenek), hiperoválisaira (legkisebb méretű páros halmazokra) vonatkozó stabilitási tételeket bizonyítottak. Ezek arról szólnak, hogy ha egy struktúra egy valamilyen értelemben extremális példához közel van (az extremális példához képest nem túl sok „irreguláris" egyenessel rendelkezik), akkor az mindig megkapható az extremálisból kis változtatással, azaz néhány pont hozzávételével illetve törlésével. A tételekben a megengedett irreguláris egyenesek nagyságrendje $q^{3/2}$. A [SzW]-beli módszerek következménye Jamison affin síkbeli lefogó ponthalmazok minimális méretére vonatkozó tételének, illetve Segre ívek beágyazhatóságára vonatkozó eredményének egy-egy új bizonyítása.

$\mathrm{PG}(2, 2^h)$ egyenesei által generált lineáris kód kódszavainak duálisai páros halmazok. Így az ide vonatkozó stabilitási eredmény következménye egy, a kódszavak súlyainak spektrumát leíró állítás, mely megjavítja Lavrauw, Storme, **Sziklai** és Van de Voorde korábbi spektrumra vonatkozó eredményét.

## Hivatkozások


[BBCFMPS] A. Blokhuis, A. E. Brouwer, A. Chowdhury, P. Frankl, T. Mussche, B. Patkós, T. Szőnyi, *A Hilton-Milner theorem for vector spaces*, (2009), kézirat.

[BBS] A. Blokhuis, A. E. Brouwer, T. Szőnyi, Covering all points except one, *J. Alg. Combinatorics* (2009), benyújtva.

[BSzSz] A. Blokhuis, P. Sziklai, T. Szőnyi, Blocking sets in projective spaces, Current research topics in Galois geometries, Nova Science Publishers, előkészületben.

[BW] S. Ball, Zs. Weiner, An introduction to finite geometry, http://www-ma4.upc.es/∼simeon/IFG.pdf, kézirat.

[FSz2] Sz. L. Fancsali, P. Sziklai, Description of the clubs, benyújtva.

[GHNP] A. Gács, T. Héger, L.Z. Nagy, D. Pálvölgyi, Permutations, hyperplanes and polynomials over finite fields, *Finite Fields and Their Applications*, benyújtva.

[GHW] A. Gács, T. Héger, Zs. Weiner, On $(k, 6)$ graphs arising from projective planes, kézirat.

[HMSzW] N. Harrach, K. Metsch, T. Szőnyi, Zs. Weiner, Small point sets of $\mathrm{PG}(n, p^{3h})$ intersecting each line in 1 mod $p^h$ points, *J. of Geometry*, benyújtva.

[SzW] T. Szőnyi, Zs. Weiner, On stability theorems in finite geometry, http://www.cs.elte.hu/∼weiner/stab.pdf, kézirat.