Véges geometria (és kódelmélet)

Szőnyi Tamás

ELTE Matematikai Intézet

TKP Workshop, 14/01/22

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
HUNGARY

PROGRAM FINANCED FROM THE NRDI FUND

Lefogó ponthalmazok

Egy (véges) geometriai struktúrában (pl. projektív sík, tér) vagy hipergráfban *lefogó ponthalmaz* egy olyan B ponthalmaz, amely minden egyenest ill. hiperélt metsz.
Projektív síkokra: $|B| \geq q + 1$, és egyenlőség esetén egyenes
BRUEN-PELIKÁN: Ha B nem-triviális, akkor $|B| \geq q + \sqrt{q} + 1$
Abban az esetben, ha itt egyenlőség teljesül, a ponthalmaz egy $\sqrt{q}$ rendű részsík (Baer részsík).
BRUEN-THAS: Minimális lefogó ponthalmazra $|B| \leq q\sqrt{q} + 1$.

Nagy lefogók stabilitása

Tétel (SzT-Weiner Zs.)

Legyen B egy $q\sqrt{q}+1-\varepsilon$ pontú ponthalmaz $\mathrm{PG}(2,q)$*-ban, ahol $q=p^{2h}$, $p\geq 78$, ha $h=1$, $p>5$, ha $h>1$ ahol $\varepsilon\leq(p-5)/2$. Tegyük fel, hogy B minden pontjában van érintő egyenes. Ekkor B unitál, speciálisan $\varepsilon=0$.*

Unitál: olyan $q\sqrt{q}+1$ pontú ponthalmaz, amelyet minden egyenes 1 vagy $\sqrt{q}+1$ pontban metsz.
Ez a korábbi workshop-on elmondott eredmény kiterjesztése (akkor $q=p^2$-re volt meg, rosszabb korláttal) négyzetrendű síkokra. A dolgozatot a *Finite Fields and their Appl.*-hoz nyújtottuk be.

Kódelméleti kapcsolatok

A lefogó ponthalmazok áttételesen kapcsolódnak a lineáris kódokra vonatkozó Griesmer-korláthoz. Ez a következőt mondja:

Egy $[n, k, d]_q$ *kódra* $n \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil$.

Ezek (geometriai) vizsgálatában a "minihyper"-ek játszanak szerepet, amelyek speciális lefogó ponthalmazok. Ezeket HAMADA és TAMARI vezette be, leírhatók vele a BELOV, LOGACHEV, SANDIMIROV gyátotta kódok. Így azt reméljük, hogy a lefogó ponthalmazokra vonatkozó stabilitási eredményekből a Griesmer-korláthoz közeli kódokra adódnak eredmények. Ehhez hosszú az út: magasabb dimenzióra és esetleg minihyperekre kell kiterjeszteni az eredményeket.

Reed-Solomon kódok

A véges geometriák legrégebbi kódelméleti alkalmazása lineáris MDS kódokkal kapcsolatos. Ezekre a kódokra $d = n - k + 1$ és egy ilyen kód paritásellenőrző mátrixának oszlopvektorai *ívet* alkotnak. Ezekre vonatkozik az MDS sejtés (ami szerint $n \leq q + 1$, ill. néhány speciális esetben $q + 2$). Ennek bizonyított esetei SEGRE ill. BALL véges geometriai eredményein alapulnak. A nevezetes példák a Reed-Solomon (RS) kódok (amiket a CD-k is használnak). A GRS kódok liosta dekódolásához hasznos az ún. "coset leader weight enumerator" ismerete. Ezt RUUD PELLIKAAN-nal és AART BLOKHUIS-szal meghatároztuk abban az esetben, ha a kód 4 kodimenziós. A dolgozatról ősszel kaptunk lektori véleményt és az új változatot október végén küldtük be. A folyóirat a *Designs, Codes, and Cryptography*, reméljük nemsokára elfogadják a cikket.

További véges geometriai tervek

Ezen a témán KLAUS METSCH-csel és LEO STORME-val dolgozunk. Az egyik eredmény:

Tétel

Legyen $\mathcal{S}$ maximális részleges 1-befedés $PG(4,q)$-ban, amelynek mérete kisebb, mint $\frac{3}{2}(q^2-q+1)$. Ekkor $|\mathcal{S}| = q^2+1+kq$, alkalmas $k \in \mathbb{N}$, és $\mathcal{S}$ q^2+1-k egyenest tartalmaz egy alkalmas hipersíkból.

Érdemes megemlíteni, hogy a konstrukció IURLO és RAJOLA eredménye (legalábbis kis q-ra).
Az eredményeket általánosítottuk $(n-1)$-befedésekre, és $3n-2$ dimenziós térre. Ezen Leo Storme budapesti látogatásán szerettünk volna dolgozna, ami meghiúsult, így ez a követlező időszakra csúszik.

Projektív síkok színezése

A nyolcvanas években ERDŐS PÁL vetette fel a következő kérdést: színezzük két színnel a sík pontjai. Mennyi lehet azon egyenesek száma maximum, amelyeken ugyanannyi pont van mindkét színből? Viszonylag egyszerűen megmutatható, hogy legalább $q+1$ olyan egyenes kell legyen, amelyek nem egyenletesek. Ha ugyanis ennél kevesebb nem-egyenletes egyenes van, akkor kell legyen olyan pont, amin csupa egyenletes egyenes megy át. Az ilyen pontok egyszínűek, és ezen szín összesen $(q^2+1)/2$-ször szerepel. Hasonlóan kell legyen olyan pont is, amelyen pontosan egy nem-egyenletes egyenes van. Ennek a pontnak a színe nem lehet az előbbi szín, és a másik szín sem.

A legkevesebb egyenletes egyenest tartalmazó színezést is meg tudjuk adni: egy rögzített ponton átmenő egyenesek fele teljesen piros, a másik fele kék (magát a pontot kivéve).

A kérdésen Markó Ádámmal és Weiner Zsuzsával dolgozunk, a fenti legalább $q+1$-et kb. $3q/2$-re (egész pontosan $3(q+1)/2$-re) tudtuk kombinatorikusan javítani, kombinatorikus módszerekkel.

Projektív síkok színezése II.

Abban az esetben, ha a sík a testre épített sík ($PG(2, q)$), jobb eredményt is tudunk: meg tudjuk határozni a második legkevesebb nem-egyenletes egyenest tartalmazó színezést. Ezt úgy kapjuk, hogy a fenti triviális színezésben egy pont színét megváltoztatjuk. Meglepő módon ennek belátására ugyanazt az algebrai technikát lehet használni, mint a lefogó ponthalmazok stabilitására.

A fenti kérdés csak páratlan q-ra értelmes, de az alábbi általánosítás mindig: adjunk meg egy p és k számot, amelyekre $p + k = q + 1$. Egy a pontok két színnel való színezésében mennyi azon egyenesek maximális száma, amelyeken p db piros és k db kék pont van? Eredményeinket erre az esetre is kiterjesztettük.

Abban az esetben, ha a p, k paraméterek valamelyike kicsi (kb. $cq^{1/2}$ nagyságrendű, akkor le is tudjuk írni azokat a színezéseket, amelyekben a nem p, k eloszlású egyenesek száma kevesebb, mint $cq\sqrt{q}$ (ahol c kicsike konstans).

Ezeken a kérdéseken jelenleg is dolgozunk.

További általánosítás: sík helyett magasabb dimenziós térre (és

Motiváció

Eredeti kérdés motivációja: *diszkrepancia*
Egy 2 színnel színezésre megnézzük minden élre a két szín különbségét. Vesszük ezk maximumát, majd az összes 2-színezésre az előbbi maximumok minimumát. Ez a hipergráf diszkrepanciája.
Projektív síkokra ez legalább $\sqrt{q}$. SPENCER: $\leq C\sqrt{q}$.
Ezt egészíti ki az ERDŐS kérdés, ahol m.m egyenesen a színek eltérése 0.

Majdnem k mod p halmazok

Proposition (Weiner-SzT)

Legyen $\mathcal{M}$ multihalmaz $\mathrm{PG}(2,q)$-ban, $16 < q$, $q = p^h$, ahol p prím. Tegyük fel, hogy az $\mathcal{M}$-et nem k mod p pontban metsző egyenesek száma δ, ahol $\delta < (\lfloor\sqrt{q}\rfloor + 1)(q + 1 - \lfloor\sqrt{q}\rfloor)$. Egy további feltétellel ekkor létezik olyan $\mathcal{M}'$ multihalmaz, amely minden egyenest k mod p pontban metsz és $\mathcal{M}$ módosított pontjainak száma $\lceil\frac{\delta}{q+1}\rceil$.

Az extra feltétel csak a q prím esetben kell. Ezt az eszközt projektív síkok egyenesei által generált kódok kis súlyú kódszavainak leírásához használtuk először.

KÖSZÖNÖM A FIGYELMET!

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
HUNGARY

PROGRAM FINANCED FROM THE NRDI FUND