

Véges geometria és kódelmélet

Szőnyi Tamás

ELTE Matematikai Intézet

TKP Workshop, 11/06/21



NATIONAL RESEARCH, DEVELOPMENT
AND INNOVATION OFFICE
HUNGARY

PROGRAM
FINANCED FROM
THE NRDI FUND

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 $|B| \leq q\sqrt{q} + 1$.

Tétel (SzT-Weiner Zs.)

Legyen B egy $q\sqrt{q} + 1 - \varepsilon$ pontú ponthalmaz $\text{PG}(2, q)$ -ban, ahol $q = p^2$, $p \geq 787$, $\varepsilon \leq (p - 5)/2$. 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. Eredmény szinten ez januárban megvolt, azóta a bizonyítást ellenőriztük, csiszoltuk.

Jelenleg ezt az eredményt próbáljuk kiterjeszteni **tetszőleges q négyzetre** (ugyanezen ε -nal).

Két pont távolságát a négyzetreemelt szokásos euklideszi távolsággal lehet véges test fölött definiálni. Itt az $\mathbf{x} = (x_1, \dots, x_m)$ és $\mathbf{y} = (y_1, \dots, y_m)$ pontok (m -dimenziós affin $\text{AG}(m, q)$ térbeli) távolsága

$$d(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^m (x_i - y_i)^2.$$

Akkor mondjuk, hogy ez a távolság egész, ha az eredmény a $\text{GF}(q)$ testben négyzetelem vagy nulla. Definiáljuk a $\mathfrak{G}_{m,q}$, amelynek csúcsai $\text{AG}(m, q)$ pontjai és $\mathfrak{G}_{m,q}$ két csúcsát akkor köti össze él, ha a fenti értelemben vett távolságuk egész. **KURZ és MEYER** azt sejtették, hogy bizonyos esetekben a kapott **gráf erősen reguláris**. A Korchmáros, Romaniello, SzT cikket elfogadta a *Finite Fields and their Appl.*, de az utolsó pillanatban kiderült, hogy az eredmény már régebb óta ismert volt (pedig közben Markó Ádám kiterjesztette páratlan dimenzióra).

A lefogó ponthalmazok áttételesen kapcsolódnak a lineáris kódokra vonatkozó [Griesmer-korláthoz](#). Ez a következőt mondja:

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

Ezek (geometriai) vizsgálatában a “[minihyper](#)”-ek játszanak szerepet, amelyek speciális lefogó ponthalmazok. Ezeket HAMADA és TAMARI vezette be, leírhatók vele a BELOV, LOGACHEV, SANDIMIROV gyártotta 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 kódokkal kapcsolatos kérdések I.

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). Az egyik megválaszolandó kérdés, hogy mekkora lehet egy RS és egy MDS kód metszete. Egy török doktorandusz GÜLIZAR GÜNAY bevonásával ezen szeretnénk dolgozni, a kb. 30 éves Storme-SzT eredményeket javítva és továbbfejlesztve.

A lineáris kódok szindrómákkal való dekódolásában fontos a standard táblázatot elkészíteni, amelyben minden lehetséges szindrómához megadjuk a megfelelő mellékosztály egy legkisebb súlyú elemét. Ez azt jelenti, hogy megkeressük a paritásellenőrző mátrix néhány oszlopának egy olyan lineáris kombinációját, amely nem áll elő kevesebb oszlop kombinációjaként. A cél meghatározni, hogy adott minimális súlyú mellékosztály hány van, egy adott mellékosztályban hány minimális súlyú vektor van.

Ezen [AART BLOKHUIS-szal](#) és [RUUD PELLIKAAN-nal](#) dolgoztunk, abban a speciális esetben, ha a paritásellenőrző mátrix oszlopai a harmadrendű térgörbe pontjai (azaz az RS kód 4 kodimenziós). Sikerült meghatározni az “extended coset leader weight enumerator” polinomot. A dolgot a *Designs, Codes, and Cryptography* folyóiratba küldtük be. Kiderült, hogy hasonló témával Davydov, Marcugini és Pambianco is foglalkoztak, valószínűleg az ő eredményeik ismeretében újra kell dolgozzuk a cikket.

Ezen a témán **KLAUS METSCH**-cel 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.

Itt két irány merült fel az eddigiekben.

BENCZÚR ANDRÁS és **MOLNÁR BÁLINT** hipergráfokat használtak informatikai rendszerek modellezéséhez. Ezek színezései úgy tűnik relevánsak. Mivel vannak korábbi eredmények geometriai struktúrák színezéseiről, így az informatikai szempontból fontos hipergráfokat is szeretném vizsgálni.

Ehhez hasonló kérdést tervezünk **BÉRCZI KRISTÓFF**al is vizsgálni.

Itt a motiváció matroidelméleti. A konkrét probléma ez:

Legyen H r -uniform hipergráf, amelyben bármely két hiperél metszete $\leq r - 2$. Tegyük fel, hogy $|V| = kr$. Ekkor van olyan színezés r színnel, amelyben nincs tarka hiperél, és minden szín legfeljebb $2k$ -szor fordul elő.

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 Ádám**mal és **Weiner Zsuzsával** dolgozunk, a fenti legalább $q + 1$ -et kb. $3q/2$ -re tudtuk kombinatorikusan javítani.

Abban az esetben, ha a sík a testre épített sík ($\text{PG}(2, q)$), 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? Eredményeink erre az esetre is kiterjeszthetők.

További általánosítás: sík helyett magasabb dimenziós térre (és adott dimenziós alterekre). Ezen MARKÓ ÁDÁM dolgozik.

KÖSZÖNÖM A FIGYELMET!

