Eötvös Loránd Tudományegyetem

Természettudományi Kar

Pituk Sára

Többszörösen telítő halmazok és MCF-kódok

Matematikus MSc

TDK dolgozat

Témavezető:

Kiss György
Geometriai Tanszék

Budapest, 2020

Tartalomjegyzék

1. Alapfogalmak **4**

2. Konstrukció $(4k-1)$-dimenzióban **9**

3. Alkalmazás: MCF-kódok **16**

Bevezető

A q elemű véges test feletti 3-dimenziós projektív térben momentumgörbének nevezzük a

$$\{(t^3, t^2, t, 1) \colon t \in GF(q)\} \cup \{(1, 0, 0, 0)\}$$

ponthalmazt. A görbe számos érdekes alkalmazása közül az egyik legújabb Bartoli, Davydov, Marcugini és Pambianco 2020-ban megjelent cikkében [3] található. Ebben a szerzők a $PG(3, q)$ tér pont-sík illeszkedési mátrixának szerkezetét vizsgálták, ahol a pontokat is és a síkokat is a momentumgörbéhez viszonyított helyzetük szerint osztályozták és ennek segítségével aszimptotikusan optimális MCF (multiple covering of the farthest-off points)-kódokat adtak meg. Az MCF-kódok az R sugarú térlefedő kódok egy részcsaládját alkotják, ahol minden x szóhoz, ami R Hamming-távolságra van a kódtól, egynél több olyan w kódszó is van, amire $d(x, w) = R$. A kódelméletben megszokott módon ezeknek a kódoknak is megfeleltethetünk bizonyos tulajdonsággal rendelkező véges projektív térbeli ponthalmazokat, ezeket többszörösen telítő halmazoknak hívjuk. Ilyenre példa a 3-dimenziós momentumgörbe is.

A dolgozat első fejezetében a momentumgörbe legfontosabb tulajdonságainak bemutatása után áttekintjük az említett cikk számunkra szükséges eredményeit, majd a második fejezetben azokat felhasználva és a $PG(4k - 1, q)$ terekre általánosítva megadunk egy konstrukciót aszimptotikusan optimális többszörösen telítő halmazokra. A többszörösen telítő halmazok és MCF-kódok kapcsolatáról az utolsó fejezetben lesz szó, ahol megvizsgáljuk, hogy milyen kódok származnak az általunk konstruált halmazokból.

1. fejezet

Alapfogalmak

A momentumgörbe $PG(3,q)$-ban

A háromdimenziós momentumgörbéről részletesen az [1] könyv 21. fejezetében lehet olvasni.

1.1. Definíció. [1] *A $PG(n,q)$ térben* momentumgörbének *nevezünk egy a*

$$\mathcal{C}_n = \{(t^n, t^{n-1}, \ldots, t, 1) \colon t \in GF(q)\} \cup \{(1,0,0,\ldots,0,)\}$$

ponthalmazzal projektíve ekvivalens halmazt.

Így például a $PG(2,q)$ sík momentumgörbéje az $X_1^2 = X_0X_2$ egyenlettel leírt ponthalmaz, ami egy kúpszelet, a normál parabola projektív lezártja.

Minden momentumgörbe $(q+1)$-ív, azaz semelyik $n+1$ pontja nem illeszkedik egy hipersíkra.

Tekintsük $\mathcal{C} = \mathcal{C}_3$-at, azaz a $PG(3,q)$-beli momentumgörbe standard alakját. Ez a $P(t)$ alakú pontokból áll, ahol

$$P(t) = \begin{cases} (t^3, t^2, t, 1), & \text{ha} \quad t \in GF(q), \\ (1,0,0,0), & \text{ha} \quad t = \infty. \end{cases}$$

Ha bevezetjük a $\mathbb{K}$ testre a $\mathbb{K}^+ = \mathbb{K} \cup \{\infty\}$ jelölést, akkor ezt úgy írhatjuk, hogy $\mathcal{C} = \{P(t) \colon t \in GF(q)^+\}$. Ha $P(t_1)$, $P(t_2)$ és $P(t_3)$ három pont $\mathcal{C}$-n, akkor a rajtuk átmenő sík homogén koordinátái: $(1, -(t_1+t_2+t_3), t_1t_2 + t_1t_3 + t_2t_3, -t_1t_2t_3)$. Ha most $t = t_1 = t_2 = t_3$, akkor a $\pi(t) = (1, -3t, 3t^2, -t^3)$ homogén koordinátákkal leírt síkot kapjuk. Ezt a síkot a görbe $P(t)$ pontbeli *oszkuláló síkjának* nevezzük. A $P(\infty)$-beli oszkuláló sík $\pi(\infty) = (0,0,0,1)$. A $\pi(t)$ sík a momentumgörbét pontosan a $P(t)$ pontban metszi. A $\Gamma = \{\pi(t) \colon t \in GF(q)^+\}$ halmazban levő síkok $q \equiv 0 \pmod 3$ esetén egy síksorhoz

tartoznak (azaz van egy közös egyenesük), a többi esetben pedig a duális tér egy harmadrendű görbéjét alkotják.

Legyen $\gamma = GF(q)$, és legyen γ' egy másodfokú bővítése γ-nak. A $\mathcal{C}' = \{P(t)\colon t \in \gamma'^{+}\}$ görbe pontjaira mint $\mathcal{C}$ *komplex* pontjaira hivatkozunk. A $\mathcal{C}$-beli pontokat néha $\mathcal{C}$ *valós* pontjainak, a $\mathcal{C}'\backslash\mathcal{C}$-belieket pedig $\mathcal{C}$ *képzetes* pontjainak is nevezzük. Azt mondjuk, hogy a $P(t_1)$ és $P(t_2)$ komplex pontok egymás *konjugáltjai*, ha t_1 és t_2 konjugáltak γ felett.

$\mathcal{C}$ egy *húrja* alatt egy olyan $PG(3,q)$-beli egyenest értünk, amely vagy $\mathcal{C}$ két (nem feltétlenül különböző) valós pontját köti össze, vagy két képzetes pontját, amelyek egymás konjugáltjai. A húrokat három csoportba sorolhatjuk: Két különböző valós pontot összekötő egyenes esetén *valós húrról*, két képzetes pontot összekötő egyenes esetén *képzetes húrról* beszélünk; két egybeeső valós pontot összekötő húr pedig a $\mathcal{C}$ adott pontbeli *érintője*.

1.2. Állítás. [1] *Semelyik két húr nem metszi egymást $\mathcal{C}$-n kívül. Minden $\mathcal{C}$-n kívül eső pontot pontosan egy húr tartalmaz.*

1.3. Jelölés. [3] *Vezessünk be néhány jelölést:*

$\mathcal{C}$-pont	*$\mathcal{C}$ egy pontja*
RC-pont	*$PG(3,q)\backslash\mathcal{C}$ egy pontja, amely rajta van egy valós húron*
IC-pont	*$PG(3,q)\backslash\mathcal{C}$ egy pontja, amely rajta van egy képzetes húron*
T-pont	*$PG(3,q)\backslash\mathcal{C}$ egy pontja, amely rajta van egy érintőn ($q \not\equiv 0 \pmod 3$ esetén)*
TO-pont	*$PG(3,q)\backslash\mathcal{C}$ egy pontja, amely rajta van egy érintőn és pontosan egy oszkuláló síkon ($q \equiv 0 \pmod 3$ esetén)*
μ_Γ-pont	*$PG(3,q)\backslash\mathcal{C}$ egy pontja, amely pontosan μ Γ-beli oszkuláló síkra illeszkedik ($\mu = 0, 1, 3, q+1$)*
$d_\mathcal{C}$-sík	*olyan sík, amelyre pontosan d darab $\mathcal{C}$-pont illeszkedik ($d = 0, 1, 2, 3$)*

Legyen G_q azon projektivitások csoportja, amelyek fixen hagyják $\mathcal{C}$-t. Ez a csoport $q \geq 5$ esetén $PGL(2,q)$-val izomorf. Meg lehet határozni, hogy mik lesznek a $PG(3,q)$ tér pontjainak, illetve síkjainak orbitjai ezen csoport hatása alatt. Ezzel a pontokat és a síkokat is 5 osztályra particionálhatjuk. Legyenek a pontok osztályai $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_5$, a síkok osztályai pedig $\mathcal{N}_1, \mathcal{N}_2, \ldots, \mathcal{N}_5$.

1.4. Állítás. [1] *Legyen $q \geq 5$. Ekkor*

1. *a síkok orbitjai G_q hatása alatt*

   $\mathcal{N}_1 = \Gamma$, $\mathcal{N}_2 = \{2_\mathcal{C}$*-síkok*$\}$, $\mathcal{N}_3 = \{3_\mathcal{C}$*-síkok*$\}$, $\mathcal{N}_4 = \{1_\mathcal{C}$*-síkok*$\}\backslash\Gamma$, $\mathcal{N}_5 = \{0_\mathcal{C}$*-síkok*$\}$,

2. *a pontok orbitjai G_q hatása alatt $q \not\equiv 0 \pmod 3$ esetén*

   $\mathcal{M}_1 = \mathcal{C}$, $\mathcal{M}_2 = \{T\text{-}pontok\}$, $\mathcal{M}_3 = \{3_\Gamma\text{-}pontok\}$, $\mathcal{M}_4 = \{1_\Gamma\text{-}pontok\}$, $\mathcal{M}_5 = \{0_\Gamma\text{-}pontok\}$,

3. $q \equiv 0 \pmod 3$ *esetén pedig*

   $\mathcal{M}_1 = \mathcal{C}$, $\mathcal{M}_2 = \{(q+1)_\Gamma\text{-}pontok\}$, $\mathcal{M}_3 = \{TO\text{-}pontok\}$, $\mathcal{M}_4 = \{RC\text{-}pontok\}$, $\mathcal{M}_5 = \{IC\text{-}pontok\}$.

Bartoli, Davydov, Marcugini és Pambianco [3] cikkükben ezeket az orbitokat vizsgálták, és minden i, j párra $(i, j = 1, \ldots, 5)$ megadták, hogy az $\mathcal{N}_i$-beli síkok hány $\mathcal{M}_j$-beli pontot tartalmaznak, valamint az $\mathcal{M}_j$-beli pontokon keresztül hány $\mathcal{N}_i$-beli sík megy. (Könnyen látszik, hogy ez csak i-től és j-től függ.) Ebből nekünk arra lesz szükségünk, hogy az egyes típusú pontokon hány $\mathcal{N}_3$-beli, azaz a momentumgörbe 3 pontját tartalmazó sík halad át. Ezeket az értékeket az alábbi táblázatok tartalmazzák.

Mindkét táblázat első sorában a megfelelő típusú pontok száma szerepel, a második sorban pedig az, hogy azokra a pontokra hány $3_\mathcal{C}$-sík illeszkedik.

1. Legyen $q \equiv \xi \pmod 3$, $\xi = -1, 1, q \geq 5$.

$\mathcal{C}$-pontok	T-pontok	3_Γ-pontok	1_Γ-pontok	0_Γ-pontok
$q+1$	q^2+q	$\frac{1}{6}(q^3-q)$	$\frac{1}{2}(q^3-q)$	$\frac{1}{3}(q^3-q)$
$\frac{1}{2}(q^2-q)$	$\frac{1}{6}(q^2-3q+2)$	$\frac{1}{6}(q^2+\xi q+4)$	$\frac{1}{6}(q^2-\xi q)$	$\frac{1}{6}(q^2+\xi q-2)$

2. Legyen $q \equiv 0 \pmod 3$, $q \geq 5$.

$\mathcal{C}$-pontok	$(q+1)_\Gamma$-pontok	TO-pontok	RC-pontok	IC-pontok
$q+1$	$q+1$	q^2-1	$\frac{1}{2}(q^3-q)$	$\frac{1}{2}(q^3-q)$
$\frac{1}{2}(q^2-q)$	$\frac{1}{6}(q^2-q)$	$\frac{1}{6}(q^2-3q)$	$\frac{1}{6}(q^2+q)$	$\frac{1}{6}(q^2-q)$

Szükségünk lesz még az alábbi összefüggésre:

1.5. Állítás. [1] *Ha $q \equiv 1 \pmod 3$, akkor*

$$\{RC\text{-}pontok\} = \{3_\Gamma\text{-}pontok\} \cup \{0_\Gamma\text{-}pontok\},$$

ha pedig $q \equiv -1 \pmod 3$, akkor

$$\{RC\text{-}pontok\} = \{1_\Gamma\text{-}pontok\}.$$

1.6. Megjegyzés. [1] *Ha $q = 2, 3$ vagy 4, akkor is ismertek a G_q csoportok:*

$$G_4 \cong \mathbf{S}_5, \quad G_3 \cong \mathbf{S}_4 \rtimes \mathbf{Z}_2^3, \quad G_2 \cong \mathbf{S}_3 \rtimes \mathbf{Z}_2^3.$$

($\mathbf{Z}_n$-nel jelöljük az n-edrendű ciklikus csoportot, $\mathbf{S}_n$-nel pedig az n-edfokú szimmetrikus csoportot.) Ezekben az esetekben szintén meg lehet adni a pontok és a síkok orbitjait, valamint a különböző síkorbitokon és pontorbitokon levő objektumok közötti illeszkedések számát is. Számunkra azonban ennek nem lesz jelentősége, mert majd q-val végtelenhez szeretnénk tartani, hogy aszimptotikus tulajdonságokat tudjunk vizsgálni.

Többszörösen telítő halmazok

1.7. Definíció. [2] *Egy n elemű $S \subseteq PG(N, q)$ halmazt* (ρ, μ)-telítőnek *nevezünk, ha*

- *létezik olyan $Q \in PG(N, q)$ pont, amely nincs benne semelyik S pontjai által generált $(\rho - 1)$-dimenziós altérben sem, valamint*
- *minden az előbbi tulajdonsággal rendelkező Q pont legalább μ olyan ρ-dimenziós altérben van benne, amit S pontjai generálnak.*

Vegyük észre, hogy ekkor S szükségképpen generálja a teljes $PG(n, q)$ teret.

1.8. Definíció. [2] *Egy n elemű (ρ, μ)-telítő halmaz* minimális*, ha nem tartalmaz $n - 1$ elemű (ρ, μ)-telítő halmazt.*

A többszörösen telítő halmazok optimalitását kifejező egyik természetes mennyiség a μ-sűrűség:

1.9. Definíció. [2] *Legyen S egy (ρ, μ)-telítő halmaz. S-nek a* μ-sűrűsége *az a $\gamma_\mu(S, \rho)$ érték, amit úgy kapunk, hogy annak az átlagos értékét, hogy az S által generált $(\rho - 1)$-dimenziós alterekből kimaradó pontokon át hány S által generált ρ-dimenziós altér megy, elosztjuk μ-vel.*

Könnyen látszik, hogy egy S ponthalmaz μ-sűrűsége legalább 1, és pontosan akkor teljesül egyenlőség, ha minden S által generált $(\rho - 1)$-dimenziós alterek által le nem fedett pontot pontosan μ S által generált ρ-dimenziós altér tartalmaz. *Optimálisnak* nevezünk egy többszörösen telítő halmazt, ha a μ-sűrűsége 1.

A többszörösen telítő halmazok valójában a térlefedő kódok egy speciális osztályának, az MCF-kódoknak a geometriai megfelelői. Az ezekkel való kapcsolatról bővebben a 3. fejezetben lesz szó.

1.10. Példa. [3] *$PG(3,q)$-ban a momentumgörbe egy $q+1$ elemű minimális $(2,\mu)$-telítő halmaz, ahol*

$$\mu = \begin{cases} \frac{q^2-3q}{6}, & ha \quad q \equiv 0 \pmod 3, \\ \frac{q^2-3q+2}{6}, & ha \quad q \not\equiv 0 \pmod 3. \end{cases}$$

Továbbá

$$\gamma_\mu(\mathcal{C},2) = \begin{cases} \frac{\frac{1}{12}q^6-\frac{1}{2}q^4+\frac{1}{3}q^3+\frac{5}{12}q^2-\frac{1}{3}q}{\frac{1}{12}q^6-\frac{11}{12}q^4+\frac{1}{2}q^3+\frac{5}{6}q^2-\frac{1}{2}q}, & ha \quad q \equiv 0 \pmod 3, \\ \\ \frac{\frac{1}{12}q^6-\frac{1}{2}q^4+\frac{1}{3}q^3+\frac{5}{12}q^2-\frac{1}{3}q}{\frac{1}{12}q^6-\frac{3}{4}q^4+\frac{2}{3}q^3+\frac{2}{3}q^2-\frac{2}{3}q}, & ha \quad q \not\equiv 0 \pmod 3. \end{cases}$$

Tehát $q \to \infty$ esetén $\gamma_\mu(\mathcal{C},2) \to 1$, és így a $PG(3,q)$ terekben a momentumgörbék egy aszimptotikusan optimális többszörösen telítő halmazsorozatot adnak meg.

A következő fejezetben ezt a konstrukciót fogjuk kiterjeszteni magasabb dimenziós terekre.

1.11. Megjegyzés. *Az 1.10 Példában a μ kiszámolásához azt kell megnézni, hogy mi a minimuma a $\mathcal{C}$ valós húrjain rajta nem levő (azaz nem RC-, és nem is $\mathcal{C}$-beli) pontokon áthatadó $3_{\mathcal{C}}$-síkok számának. Ezt ki lehet olvasni az előző szakaszban szereplő táblázatokból. A μ-sűrűség értékének meghatározásáról pedig később ennél általánosabban is lesz szó.*

2. fejezet

Konstrukció $(4k-1)$-dimenzióban

Először megmutatjuk, hogy $PG(n_1+n_2+\cdots+n_k+k-1,q)$-ban fel tudunk venni k darab V_i ($\dim(V_i)=n_i$) alteret úgy, hogy közülük semelyik altérnek ne legyen közös pontja a maradék $k-1$ altér generátumával: Vegyük fel V_1-et tetszőlegesen, és ha már felvettük $V_1,\dots,V_i$-t, akkor V_{i+1}-et úgy vegyük, hogy diszjunkt legyen $\langle V_1,\dots,V_i\rangle$-től. A dimenzióformulából következik, hogy

$$\dim(\langle V_1,\dots,V_i,V_{i+1}\rangle)=\left(\sum_{j=1}^{i}n_j+i-1\right)+n_{i+1}-(-1)=\sum_{j=1}^{i+1}n_j+i,$$

és így végül

$$\dim(\langle V_1,\dots,V_k\rangle)=n_1+n_2+\cdots+n_k+k-1,$$

tehát k darab ilyen kitérő altér pont elfér az $(n_1+n_2+\cdots+n_k+k-1)$-dimenziós térben. Szintén a dimenzióformula alkalmazásával kapjuk, hogy ekkor mindegyik kiválasztott altérnek a maradék $(k-1)$-gyel vett metszete üres.

2.1. Lemma. *Legyen $k\in\mathbb{Z}^+$. Legyen $\mathcal{P}_i$ a $V_i=PG(n_i,q)$ térben egy (ρ_i,μ_i)-telítő halmaz $(i=1,\dots,k)$. Vegyük fel ezeket $PG(n_1+n_2+\cdots+n_k+k-1,q)$-ban a fenti módon. Ekkor $\mathcal{P}=\mathcal{P}_1\cup\mathcal{P}_2\cup\cdots\cup\mathcal{P}_k$ egy (ρ,μ)-telítő halmaz, ahol*

$$\rho=\left(\sum_{i=1}^{k}\rho_i\right)+k-1\ \text{ és }\ \mu=\prod_{i=1}^{k}\mu_i.$$

Továbbá ha mindegyik $\mathcal{P}_i$ minimális, akkor $\mathcal{P}$ is az.

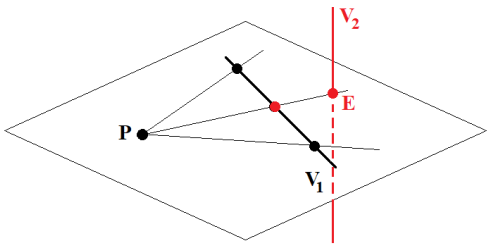
Bizonyítás. k szerinti indukciót végzünk. A $k=1$ esetet tudjuk. Tegyük fel, hogy $(k-1)$-re igaz az állítás. Legyen $N=n_1+n_2+\cdots+n_k+k-1$. Azt kell ellenőrizni, hogy

- létezik olyan pont $PG(N,q)$-ban, ami nincs benne egyik olyan $\left(\left(\sum_{i=1}^{k}\rho_i\right)+k-2\right)$-dimenziós altérben sem, amit $\mathcal{P}$ valamely $\left(\sum_{i=1}^{k}\rho_i\right)+k-1$ pontja generál

- és minden ilyen ponton át legalább μ olyan $\left(\left(\sum_{i=1}^{k}\rho_i\right)+k-1\right)$-dimenziós altér megy, amit $\mathcal{P}$ $\left(\sum_{i=1}^{k}\rho_i\right)+k$ pontja generál.

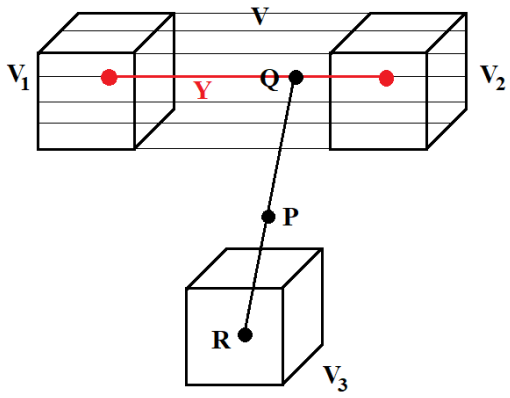
Az állítás első felének ellenőrzéséhez nézzük először azokat a pontokat, amik benne vannak már $k-1$ darab altér generátumában is. Feltehető, hogy ez az első $k-1$ altér. Az összes ilyen pont fedve van valamelyik $\left(\sum_{i=1}^{k}\rho_i\right)+k-1$ pont által generált $\left(\left(\sum_{i=1}^{k}\rho_i\right)+k-2\right)$-dimenziós altér által, mert a $k-1$ altérben levő $k-1$ darab $\mathcal{P}_i$ halmaz az indukciós feltevés szerint egy $\left(\left(\sum_{i=1}^{k-1}\rho_i\right)+k-2,\Pi_{i=1}^{k-1}\mu_i\right)$-telítő halmaz, tehát ki tudunk választani róla $\left(\sum_{i=1}^{k-1}\rho_i\right)+k-1$ pontot úgy, hogy azok egy olyan $\left(\left(\sum_{i=1}^{k-1}\rho_i\right)+k-2\right)$-dimenziós alteret generáljanak, ami tartalmazza a kiválasztott pontot. Mivel $0\le\rho_k\le n_k-1$, készen vagyunk.

Legyen most P olyan pont, ami nincs benne semelyik $k-1$ darab altér generátumában. Ekkor P-n át egyértelműen létezik egy olyan $(k-1)$-dimenziós altér, amely mind a k darab V_i-t egy-egy pontban metszi. Ezt is k szerinti indukcióval látjuk be. A $k=1$ eset triviális. Ha $k=2$, akkor is igaz az állítás, mert a $\langle V_1,P\rangle$ altér V_2-t a dimenzióformula miatt egyetlen E pontban metszi, és ekkor az EP egyenes az az egyértelmű egyenes, ami elmetszi V_1-et is és V_2-t is.



2.1. ábra. A $k=2$ eset, ha V_1 és V_2 is 1-dimenziós

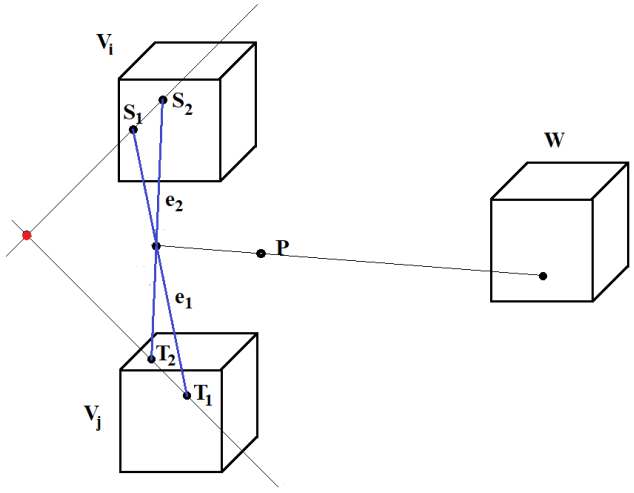
Legyen $k \geq 3$, és tegyük fel, hogy $(k-1)$-re már beláttuk az állítást. P benne van az egymástól diszjunkt $V = \langle V_1, \ldots, V_{k-1} \rangle$ és V_k alterek által generált térben, vagyis rajta van egy olyan egyenesen, ami V egy Q pontját V_k egy R pontjával köti össze. (Csak egy ilyen egyenes mehet P-n át, mert ha RQ és $R'Q'$ két különböző ilyen P-n átmenő egyenes lenne, akkor R, R', Q és Q' egy síkban lennének, így RR' és QQ' is metszené egymást, ami lehetetlen, mert a két egyenes két kitérő altérben van.) Q nincs benne semelyik $k-2$ darab V_i generátumában $(i = 1, \ldots, k-1)$, mert akkor P benne lenne az azokból és V_k-ból álló $k-1$ altérében. Az indukciós feltevés miatt létezik Q-n át pontosan egy $(k-2)$-dimenziós Y altér, ami V_1-et, $\ldots$, V_{k-1}-et is egy-egy pontban metszi. Így $\langle Y, P \rangle$ egy megfelelő $(k-1)$-dimenziós altér P-n át.



2.2. ábra. Az indukciós lépés $k = 2$-ről $k = 3$-ra

Az egyértelműség bizonyításához tegyük fel, hogy van P-n át két különböző $(k-1)$-dimenziós altér, ami mindegyik V_i-t pontosan egy pontban metszi. Legyenek ezek U_1 és U_2. Ekkor van legalább két olyan index $(i < j)$, amelyre $U_1 \cap V_i = S_1 \neq S_2 = U_2 \cap V_i$ és $U_1 \cap V_j = T_1 \neq T_2 = U_2 \cap V_j$. (Ha $k-1$ darab altérrel vett metszete ugyanaz U_1-nek és U_2-nek, akkor U_1 és U_2 is megegyezik az ezen $k-1$ metszéspont és P által együttesen generált altérrel.) Legyen $W = \langle V_1, \ldots V_{i-1}, V_{i+1}, \ldots, V_{j-1}, V_{j+1}, \ldots, V_k \rangle$. Mivel P benne van az $e_1 = T_1S_1$ egyenes és W által generált altérben, valamint az $e_2 = T_2S_2$ egyenes és W által generált altérben is, rajta van egy e_1-en

levő pontot egy W-beli ponttal összekötő egyenesen és egy e_2-n levő pontot egy W-beli ponttal összekötő egyenesen is. De W és $\langle V_i, V_j \rangle$ kitérőek, így az előző gondolatmenet szerint ez a két egyenes egybeesik. Ez viszont azt jelenti, hogy e_1 és e_2 metszi egymást, vagyis S_1, S_2, T_1 és T_2 egy síkban van, de ez, ugyanúgy, mint az előbb, ellentmondás.



2.3. ábra. Az egyértelműség bizonyítása

Nézzük tehát ezt a $(k-1)$-dimenziós alteret P-n át. Ha ez valamelyik V_i-t olyan pontban metszi, ami benne van már $\mathcal{P}_i$ valamely ρ_i pontja által generált $(\rho_i - 1)$-dimenziós altérben, akkor P fedve van $\left(\left(\sum_{i=1}^{k} \rho_i\right) + k - 2\right)$-dimenziós altér által, mégpedig az az altér fedi, amit úgy kapunk, hogy vesszük ennek a $(\rho_i - 1)$-dimenziós altérnek, és a többi V_j térben tetszőleges, a metszéspontokon átmenő, $\mathcal{P}_j$ pontjai által generált ρ_j-dimenziós altereknek a generátumát. Ebből az is látszik, hogy ha egyiket sem ilyen pontban metszi a $(k-1)$-dimenziós altér, akkor P nincs fedve $\left(\left(\sum_{i=1}^{k} \rho_i\right) + k - 2\right)$-dimenziós altér által. Utóbbi esetben akkor lesz a P-n áthaladó, $\mathcal{P}$ pontjai által generált $\left(\left(\sum_{i=1}^{k} \rho_i\right) + k - 1\right)$-dimenziós alterek száma minimális, ha mindegyik V_i altérrel vett metszéspontra a lehető legkevesebb, az adott térben levő $\mathcal{P}_i$ pontjai által generált ρ_i-dimenziós altér illeszkedik. Ugyanis azok az alterek fedik P-t, amit a metszéspontokon az adott terekben áthaladó alterek együttesen generálnak. Így ez a minimális érték az egyes alterekben előforduló minimális értékek szorzata lesz, ami $\prod_{i=1}^{k} \mu_i$. □

2.2. Következmény. *Legyen $k \in \mathbb{Z}^+$. Vegyünk fel $PG(4k-1,q)$-ban k darab 3-dimenziós alteret az előző lemmában megadott módon, legyenek ezek $V_1, \ldots, V_k$. Vegyünk mindegyik V_i-ben egy $\mathcal{C}_i$ momentumgörbét. Ekkor $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \cdots \cup \mathcal{C}_k$ egy $k(q+1)$ elemű minimális $(3k-1,\mu^k)$-telítő halmaz, ahol*

$$\mu = \begin{cases} \frac{q^2-3q}{6}, & ha \quad q \equiv 0 \pmod 3, \\ \frac{q^2-3q+2}{6}, & ha \quad q \not\equiv 0 \pmod 3. \end{cases}$$

Bizonyítás. Azonnal adódik, felhasználva az 1.10 Példát és a 2.2 Következményt. □

2.3. Tétel. *Az így kapott $\mathcal{C}$ többszörösen telítő halmaz μ-sűrűsége 1-hez tart, ahogy $q \to \infty$.*

Bizonyítás. Először számoljuk meg azt, hogy ha kiválasztunk mindegyik V_i-ből egy pontot, akkor az ezek által generált $(k-1)$-dimenziós altérhez hány olyan P pont tartozik, ami nincs benne semelyik $k-1$ darab V_i által generált altérben sem. (Ezeket a továbbiakban *kimaradó pontoknak* nevezzük.) Ezt az M értéket a szita-formula alkalmazásával kaphatjuk meg: Egy d-dimenziós altér pontjainak száma $q^d + q^{d-1} + \cdots + q + 1$, és a k pont által generált $(k-1)$-dimenziós altér összesen $\binom{k}{d+1}$ darab olyan d-dimenziós alteret tartalmaz, aminek a generátorrendszere a k pont közül kerül ki. Továbbá a $(k-1)$-dimenziós altér l darab $(k-2)$-dimenziós alterének metszete a dimenzióformula szerint egy $(k-1-l)$-dimenziós altér. Tehát

$$M = (q^{k-1} + \cdots + q + 1) - \binom{k}{k-1}(q^{k-2} + \cdots + q + 1) + \cdots \pm \binom{k}{1}.$$

Ebből nekünk csak annyira lesz szükségünk, hogy M-ben a q legmagasabb hatványa q^{k-1}.

Jelölje N annak a számát, hogy hányféleképpen tudunk mind a k darab 3-dimenziós altérből egy-egy nem a momentumgörbére eső és nem RC-pontot kiválasztani:

$$N = \left(q^3 + q^2 + q + 1 - (q+1) - \frac{1}{2}(q^3 - q)\right)^k = \left(\frac{1}{2}q^3 + q^2 + \frac{1}{2}q\right)^k,$$

hiszen a momentumgörbének $q+1$ pontja van, az RC-pontok száma pedig $\binom{q+1}{2}(q-1) = \frac{1}{2}(q^3-q)$.

Ekkor azon $PG(4k-1,q)$-beli pontok száma, amelyeken nem megy át $\mathcal{C}$ semelyik $3k-1$ pontja által generált $(3k-2)$-dimenziós altér, MN. Ugyanis ha kiválasztunk mindegyik 3-dimenziós altérből egy pontot, amit N-féleképpen

tehetünk meg, akkor az ezek által generált altérre M kimaradó pont illeszkedik, és így minden kimaradó pontot pontosan egyszer kaptunk meg, mivel a kimaradó pontokhoz egyértelműen tartozik egy $(k-1)$-dimenziós altér, ami mindegyik 3-dimenziós teret egy pontban metszi. Tehát a μ-sűrűséget az alábbi képlet adja meg:

$$\gamma_\mu(\mathcal{C}, 3k-1) = \frac{1}{\mu^k}\frac{S}{MN},$$

ahol S-et úgy kapjuk, hogy összegezzük a kimaradó P pontokra a P-n átmenő, $\mathcal{C}$ valamely $3k$ pontja által generált $(3k-1)$-dimenziós alterek számát.

Három esetet kell megkülönböztetnünk q-nak a 3-mal vett osztási maradéka szerint. A nevező mindhárom esetben

$$\mu^k MN = \left(\frac{1}{6}\right)^k q^{2k} q^{k-1} \left(\frac{1}{2}\right)^k q^{3k} + F(q) = \frac{1}{12^k} q^{6k-1} + F(q)$$

alakú, ahol F egy $(6k-1)$-nél kisebb fokú polinom. Ugyan μ értéke eltér a különböző esetekben, így az F polinom sem lesz mindig ugyanaz, viszont az aszimptotikus viselkedés szempontjából a számlálónak és a nevezőnek is csak a főtagja számít, és μ legmagasabb fokú tagja mindig $\frac{1}{6}q^2$.

S-et a következőképpen számolhatjuk ki: Vonjuk össze a tagokat aszerint, hogy az adott pontra illeszkedő $(k-1)$-dimenziós altérnek az egyes V_i-kkel vett metszéspontja milyen típusú. Így S-et részösszegekre bonthatjuk. Mivel minket S-nek is csak a főtagja érdekel, elég azokkal a részösszegekkel foglalkozni, amikben q a lehető legmagasabb hatványon fordul elő. Azt már láttuk, hogy k kiválasztott ponthoz M kimaradó pont tartozik, így M-et ki is emelhetünk. Ha van egy fix P kimaradó pontunk, akkor a P-re illeszkedő $\mathcal{C}$ valamely $3k$ pontja által generált $(3k-1)$-dimenziós alterek számát úgy kapjuk, hogy mindegyik altérben megnézzük, hogy a P-n áthaladó $(k-1)$-dimenziós altérrel vett metszésponton át hány $3_\mathcal{C}$-sík megy, és ezeket az értékeket – amiket a 6. oldalon szereplő táblázatból olvashatunk ki – összeszorozzuk. Ha csak azt rögzítjük, hogy a k darab metszéspont milyen típusú, akkor az egyes alterekben levő adott típusú pontok számát egymással összeszorozva kapjuk az ilyen alterek számát. Tehát azokban a részösszegekben fordul elő q a legmagasabb hatványon, amelyek felírása során minden altérben olyan pontot választunk, amire a megfelelő pontok számának és az olyan pontokon átmenő $3_\mathcal{C}$-pontok számának a szorzatában q kitevője maximális.

1. $q \equiv 1 \pmod 3$:

   A számlálóban szereplő összegben azokból a tagokból származnak q legnagyobb kitevős előfordulásai, amikor olyan P pontot nézünk, amin

átmenő $(k-1)$-dimenziós altér mind a k 3-dimenziós teret 1_Γ-pontban metszi. Ezek S-hez a

$$\left(\frac{1}{2}(q^3-q)\right)^k M \left(\frac{1}{6}(q^2-q)\right)^k$$

mennyiséggel járulnak hozzá. Ebből azt kapjuk, hogy a számláló főtagja $\frac{1}{12^k}q^{6k-1}$, ami megegyezik a nevező főtagjával. Ebből már következik, hogy 1-hez tart a μ-sűrűség.

2. $q \equiv -1 \pmod 3$: Ha a számlálóban meg akarjuk határozni a főtagot, akkor az összes olyan esetet figyelembe kell vennünk, amikor valahány 3-dimenziós altérből 3_Γ-pontot, a maradékból pedig 0_Γ-pontot választunk. Ezekből a tagokból az alábbi értéket kapjuk:

$$M\sum_{i=0}^{k}\binom{k}{i}\left(\frac{1}{6}(q^3-q)\frac{1}{6}(q^2-q+4)\right)^i\left(\frac{1}{3}(q^3-q)\frac{1}{6}(q^2-q-2)\right)^{k-i}.$$

Vagyis a főtag:

$$q^{6k-1}\sum_{i=0}^{k}\binom{k}{i}\left(\frac{1}{36}\right)^i\left(\frac{1}{18}\right)^{k-i} = q^{6k-1}\frac{1}{18^k}\sum_{i=0}^{k}\binom{k}{i}\left(\frac{1}{2}\right)^i =$$
$$= q^{6k-1}\frac{1}{18^k}\left(1+\frac{1}{2}\right)^k = \frac{1}{12^k}q^{6k-1}.$$

Így a számlálónak is ugyanaz a főtagja, mint a nevezőnek, tehát a hányados ebben az esetben is 1-hez tart.

3. $q \equiv 0 \pmod 3$:

Most S-ben akkor kapjuk a legnagyobb hatványát q-nak, ha mind a k altérben IC-pontot választunk, vagyis a

$$\left(\frac{1}{2}(q^3-q)\right)^k M \left(\frac{1}{6}(q^2-q)\right)^k$$

tag adja a számláló főtagját. Tehát

$$S = \frac{1}{12^k}q^{6k-1} + G(q),$$

ahol G egy $(6k-1)$-nél kisebb fokú polinom. Tehát most is 1-hez tart a hányados.

□

3. fejezet

Alkalmazás: MCF-kódok

Mint már említettük, a többszörösen telítő halmazok szoros kapcsolatban állnak bizonyos típusú térlefedő kódokkal. Ezek az MCF-kódok, amelyeket a következőképpen definiálunk:

3.1. Definíció. [2] *Legyen C egy $[n,k,d]_qR$-kód, azaz egy olyan k-dimenziós lineáris kód $GF(q)^n$-ben, melynek minimális távolsága d, fedési sugara pedig R. Azt mondjuk, hogy C (R,μ)-*MCF (multiple covering of the farthest-off points)*, ha minden $x \in GF(q)^n$ szóhoz, amire $d(x,C) = R$, legalább μ olyan $c \in C$ kódszó van, amelyre $d(x,c) = R$.*

Az MCF-kódok vizsgálata több szempontból hasznos. Ezek közül egy az általánosított totó feladattal való kapcsolatuk, egy másik pedig az a tény, hogy a lista dekódolásnál a kódtól legtávolabbi szavak fontos szerepet játszanak a lista méretére adott felső becslésekben az általánosított Reed-Solomon kódok esetén.

A többszörösen telítő halmazok és az MCF-kódok között az alábbi állítás teremt összefüggést:

3.2. Állítás. [2] *Legyen S egy n elemű (ρ,μ)-telítő halmaz $PG(n-k-1,q)$-ban. Tekintsük azt a C lineáris $[n,k,d]_qR$-kódot, melynek paritásellenőrző mátrixát az S-beli pontok reprezentáló vektorainak mint oszlopvektoroknak egymás mellé írásával kapjuk. Ekkor C egy $(\rho+1,\mu)$-MCF-kód. Továbbá S-nek a μ-sűrűsége megegyezik annak az átlagos értéknek, hogy egy a kódtól $\rho+1$ távolságra levő szó hány kódszótól van $\rho+1$ távolságra, és μ-nek a hányadosával.*

Így tehát az előző fejezetben megadott konstrukcióból minden $k \geq 1$ egészre és q prímhatványra kapunk egy $[k(q+1), k(q-3), d]_q 3k$-kódot, és ezek aszimptotikusan optimális MCF-kódok lesznek.

Irodalomjegyzék

[1] J. W. P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford University Press (1979).

[2] Daniele Bartoli, Alexander A. Davydov, Massimo Giuiletti, Stefano Marcugini, Fernanda Pambianco, *Multiple coverings of the farthest-off points with small density from projective geometry*, Advan. Math. Commun. 9 (1) (2015) 63-85.

[3] Daniele Bartoli, Alexander A. Davydov, Stefano Marcugini, Fernanda Pambianco, *On planes through points off the twisted cubic in PG(3,q) and multiple covering codes*, Finite Fields and Applications 67 (2020) paper 101710.