Eötvös Loránd Tudományegyetem
Természettudományi Kar

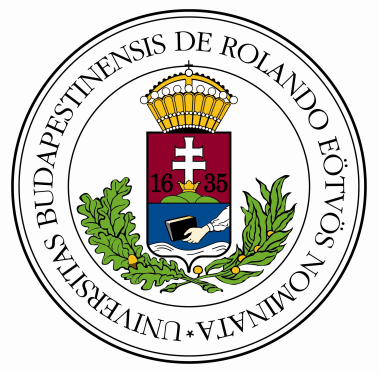
Kocsis Júlia
Matematika BSc, matematikus szakirány

A lineáris kódokra vonatkozó MDS-sejtés

Szakdolgozat

Témavezető: Csajbók Bence
tudományos munkatárs

Geometria Tanszék



Budapest, 2020.

NYILATKOZAT

Név: Kocsis Júlia

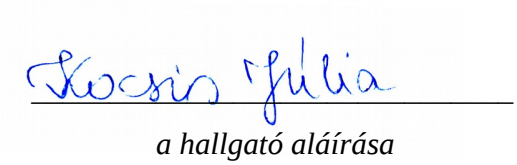
ELTE Természettudományi Kar, szak: Matematika BSc

NEPTUN azonosító: MYYF23

Szakdolgozat címe:
A lineáris kódokra vonatkozó MDS-sejtés

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2020. 05. 28.



a hallgató aláírása

Köszönetnyilvánítás

Szeretnék köszönetet mondani elsősorban témavezetőmnek, Csajbók Bencének, hogy elvállalta a témavezetést, rendszeres konzultációt tartott, a felmerülő problémákat mindig lelkiismeretesen segített megoldani, időt nem sajnálva. Rá bármikor számíthattam. Köszönöm azt a sok észrevételt és javaslatot, amik nélkül szakdolgozatom nem nyerhette volna el jelenlegi formáját.
Hálás köszönet illeti Simeon Ball-t, aki amellett, hogy munkásságával a szakdolgozatom alapját adta meg, a felmerült kérdéseinkre is személyesen válaszolt.
Köszönettel tartozom még Poór Márknak a LaTeX-hez nyújtott segítségéért.
Köszönöm családomnak, hogy biztosították mindazt, ami tanulmányaimhoz szükséges volt, mind anyagilag, mind szellemileg támogattak. Végül köszönöm Andrásnak, hogy mindvégig mellettem állt.

Tartalomjegyzék

1. Bevezetés

Dolgozatom célja a lineáris kódokra vonatkozó MDS-sejtés és a hozzá szorosan kapcsolódó véges projektív terek íveinek bemutatása.

Azokat a lineáris $[n,k]_q$ kódokat, amik a Singleton-korlátot egyenlőséggel teljesítik, azaz a minimális távolságuk a lehető legnagyobb, $n-k+1$, MDS (Maximum Distance Separable rövidítése) kódoknak nevezzük. Egy kódnak minél nagyobb a minimális távolsága, gyakorlati szempontból annál kívánatosabb, ugyanis több hiba esetén is visszafejthető.

Ezek alapján feltehető a kérdés, hogy adott k-ra és q-ra mik a leghosszabb MDS kódok, azaz a szokásos jelöléssel mi n maximális értéke, hiszen minél nagyobb n, annál nagyobb a kód minimális távolsága, feltéve, hogy a kód MDS marad.

Az MDS kódok szép tulajdonsága, hogy egy $[n,k]_q$ MDS kód ekvivalens egy q elemű véges test feletti $k-1$ dimenziós projektív térbeli, n pontból álló ívvel. Ez lehetővé teszi, hogy véges geometriai eszközökkel vizsgáljuk az MDS kódokat, így az előbbi kérdés átfogalmazható arra, hogy egy adott projektív térben mi az ívek maximális mérete.

Ez a kérdés motiválta Beniamino Segrét is 1955-ben, amikor megfogalmazta a híres MDS-sejtését, miszerint ha $k \leq q$, akkor ez a maximális hossz $q+1$, kivéve ha q páros és $k=3$ vagy $k=q-1$, mert akkor $q+2$ (ha $k \geq q+1$, akkor könnyen belátható, hogy a válasz $k+1$). Segre sejtése teljes általánosságban a mai napig megoldatlan, mégis számos speciális esetben bizonyított. A főbb eredmények időrendben a következők:

- $k=2$-re triviális,
- $k=3$, Bose, 1947,
- $k=4$, 5, q páratlan, Segre, 1955,
- $k<\frac{1}{4}\sqrt{q}$, q páratlan és $k<\sqrt{q}$, q páros Segre, 1967,
- $k<\sqrt{pq}$, $q=p^{2h+1}$, Voloch, 1991,
- $k<\frac{1}{2}\sqrt{q}$, $q=p^{2h}$, $p>5$, Hirschfeld, Korchmáros, 1996,
- $k\leq p$, q páratlan, Ball, 2012,
- $k\leq 2p-2$, q páratlan, Ball, De Beule, 2012,
- $k<\sqrt{q}-\frac{1}{p}\sqrt{q}+2$, $q=p^{2h}$, q páratlan, Ball, Lavrauw, 2018.

A $k\leq q$ általános esetre Ball adta az eddigi legjobb felső korlátot, hogy $n\leq q+k+1-\min(k,p)$ ([7]-ben), amiből $k\leq p$-re adódik a sejtés.

Szakdolgozatomban ezek közül (a $k=2$, 3 eset mellett) Simeon Ball legfrissebb eredményeinek, a $k\leq p$ és $k\leq 2p-2$ eseteknek a bizonyítását fogom ismertetni a 4. fejezetben a [3] cikk alapján, ami az eredeti [7] és [8] cikkekben szereplő bizonyításokat már letisztultabban, egységesen írja le. A bizonyítások alapötlete az ún. érintők lemmája és a skálázási módszer. Az előbbit már

Segre is használta az egyik leghíresebb tételének bizonyításában, miszerint a projektív síkon minden ovális ($q+1$ méretű ív) kúpszelet. Erről az 5., konstrukciókról szóló fejezetben, mint következmény lesz szó. Ebben a fejezetben bemutatok néhány $q+1$ illetve $q+2$ méretű ívet. Ezek közül a legáltalánosabb példa a momentumgörbe, ami minden k-ra és q-ra ($k \leq q$) ívet alkot, sőt, bizonyos esetekben lényegileg az egyetlen $q+1$ méretű ív. Az 5.2. alfejezetben részletesebben megvizsgáltam bizonyos tulajdonságait is. Nyitott kérdés még az is, hogy milyen (k, q) párra igaz, hogy $\mathrm{PG}(k-1, q)$ egyetlen $q+1$ méretű íve a momentumgörbe.
Végül az utolsó fejezet betekintést nyújt az MDS kódokhoz hasonló, egy fokkal gyengébb paraméterekkel rendelkező, de gyakorlati szempontból még mindig hasznos kódok világába. Ezek a near-MDS és almost-MDS kódok, amik szintén megfeleltethetőek egy-egy alkalmas projektív téren értelmezett, speciális tulajdonságokkal bíró ponthalmaznak. Ez a kitekintő fejezet illusztrálja, hogy az MDS kódok mellett még mennyi mindent lehet hasonló szemlélettel vizsgálni.
A 2. és 3. fejezet kódelméleti bevezető az alapvető fogalmak, tulajdonságok tisztázására szolgál. Az alapszintű algebrai és geometriai összefüggéseket a mű ismertnek tekinti.

2. Kódelméleti ismeretek

Ahhoz, hogy jobban megértsük, hogy mi az MDS-sejtés kódelméleti motivációja, először ismerkedjünk meg néhány alapfogalommal. Ezekhez az [1] és [2] forrásokat illetve jegyzeteimet használtam fel.
A kódolás alapvető modellje szerint fix, valamely Q ábécé feletti k hosszú üzenetdarabokat szeretne a küldő, egy csatornán keresztül eljuttatni a fogadónak. Erről a csatornáról feltételezzük, hogy zajos (azaz nem feltétlenül pontosan ugyanaz az üzenet érkezik meg, mint amit elküldtünk), ezért ellenőrző részeket veszünk hozzá az üzenethez, így n hosszú blokkokat küldünk a csatornán, hogy abból lehetőleg a fogadó ki tudja találni az eredeti üzenetet.

2.1. Alapfogalmak

1. Definíció (kód, kódszó). *Legyen Q egy véges halmaz. $C \subseteq Q^n$ kód, hossza n, elemei a kódszavak.*

Ez a definíció eléggé általános, hiszen a halmaz elemei bármik lehetnek. A későbbiek során Q leginkább $\mathbb{F}_q$, a q elemű véges test lesz, a kódszavakat pedig $\mathbb{F}_q^n$ vektortérbeli vektoroknak tekintjük.

2. Definíció (Hamming-távolság). *Két kódszó Hamming-távolságán a különböző jegyeinek számát értjük. Azaz ha $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ és $\mathbf{w} = (w_1, w_2, \ldots, w_n)$ két kódszó, akkor a Hamming-távolságuk*

$$d(\mathbf{v}, \mathbf{w}) = |\{i : v_i \neq w_i\}|.$$

Vegyük észre, hogy a Hamming-távolság egy metrika Q^n-en.

3. Definíció (C minimális távolsága). *A C kód minimális távolságán a különböző kódszavak közt fellépő Hamming-távolságok minimumát értjük, jele $d(C)$ vagy d,*

$$d(C) = \min\{d(\mathbf{v}, \mathbf{w}) : \mathbf{v}, \mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}.$$

2.2. Lineáris kódok

Innentől tegyük fel, hogy $Q = \mathbb{F}_q$ véges test és legyen $V = \mathbb{F}_q^n$ a test feletti n dimenziós vektortér.

4. Definíció (súly). *$\mathbf{v} \in C$ kódszó súlya a nemnulla koordinátáinak a száma, jele: $w(\mathbf{v})$,*

$$w(\mathbf{v}) = |\{i : v_i \neq 0\}| = d(\mathbf{0}, \mathbf{v}).$$

5. Definíció (lineáris kód). *A $C \subseteq V$ kód lineáris, ha C lineáris altere V-nek. Ha ennek az altérnek a dimenziója k, akkor lineáris $[n, k]_q$-kódnak nevezzük.*

1. Állítás. *$C \leq V$ lineáris kód esetén a kód minimális távolsága megegyezik a legkisebb súlyú nem $\mathbf{0}$ vektorának a súlyával, azaz*

$$d(C) = min\{w(\mathbf{v}) : \mathbf{v} \in C \setminus \{\mathbf{0}\}\}.$$

Bizonyítás. Mivel C egy lineáris altér, ezért $\mathbf{0} \in C$. Két különböző kódszó (legyenek $\mathbf{f}$ és $\mathbf{w}$) távolsága a különböző jegyeik száma, ami nem más, mint a különbségüknek a $\mathbf{0}$-tól különböző számjegyeinek a száma (amelyik koordináták megegyeznek, pontosan ott lesz a különbségben 0). Tehát $d(\mathbf{v}, \mathbf{w}) = w(\mathbf{v}-\mathbf{w}) = d(\mathbf{0}, \mathbf{v}-\mathbf{w})$. Szintén C lineáris altér tulajdonsága miatt $\mathbf{v}-\mathbf{w} \in C$, így valóban

$$d(C) = \min\{d(\mathbf{v}, \mathbf{w}) : \mathbf{v}, \mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\} = \min\{w(\mathbf{v} - \mathbf{w}) : \mathbf{v}, \mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\},$$

amiből már látszik, hogy a minimális távolság a legkisebb súlyú kódszó súlya. □

6. Definíció (Generátor mátrix). *Legyen C lineáris $[n,k]_q$ kód $\mathbb{F}_q^n$ vektortérben. Ha $\mathbf{c_1}, \ldots, \mathbf{c_k}$ egy bázisa C-nek, akkor az ezen sorvektorok egymás alá írásából képzett $k \times n$-es mátrixot C generátor mátrixának hívjuk. Jele: G.*

A bázis tulajdonsága miatt tehát

$$C = \{\mathbf{x}G : \mathbf{x} \in \mathbb{F}_q^k\},$$

hiszen az alteret pontosan a bázisvektorok lineáris kombinációi alkotják, amit a fenti módon is írhatunk.

7. Definíció (Paritásellenőrző mátrix). *A $C \leq \mathbb{F}_q^n$ lineáris $[n,k]_q$ kódnak az $(n-k) \times n$-es H mátrix paritásellenőrző mátrixa, ha $\mathbf{x} \in \mathbb{F}_q^n$ akkor és csak akkor kódszó, ha $\mathbf{x}H^T = \mathbf{0}$. Ha $\mathbf{y} \in \mathbb{F}_q^n$ tetszőleges vektor, akkor $\mathbf{y}$ tünetének az $s(\mathbf{y}) = \mathbf{y}H^T$ vektort nevezzük.*

Ilyen H mátrix pedig létezik, hiszen ha vesszük C direkt kiegészítő alterének (amiről lineáris algebrából tudjuk, hogy mindig létezik) egy bázisából képzett mátrixát (sorvektorokat írunk egymás alá), akkor az teljesíti a definíció feltételét.

8. Definíció (Duális kód). *Egy C $[n,k]_q$ lineáris kód duálisán a következő kódot értjük:*

$$C^\perp = \{\mathbf{v} \in \mathbb{F}_q^n : \mathbf{v} \cdot \mathbf{x} = 0 \, \forall \mathbf{x} \in C\},$$

ahol $\mathbf{v} \cdot \mathbf{x}$ alatt a szokásos skaláris szorzást értjük.

1. Megjegyzés. *A duális kód definíciójából következik, hogy a generátor mátrixa az eredeti kód paritásellenőrző mátrixa és fordítva, illetve, hogy egy lineáris kód duálisának a duálisa önmaga.*

2. Megjegyzés. *Két kódot (szűkebb értelemben) ekvivalensnek nevezünk, ha egyik a másikból a koordináták permutációjával megkapható.*
Lineáris kódokra ezen felül meg szokás engedni egy koordináta nemnulla testelemmel való végigszorzását is: két lineáris $[n,k]_q$ kód, C_1 és C_2 lineárisan ekvivalens, ha van olyan G_1 és G_2 generátormátrixuk, hogy G_2 megkapható G_1-ből oszlopcserékkel és oszlopok nemnulla skalárral való végigszorzásával.

2.3. A minimális távolság tulajdonságai

9. Definíció (e-hibajavító kód). *Legyen e pozitív egész. $C \subseteq V$ kódot e-hibajavító kódnak nevezzük, ha tetszőleges* **v** *kódszóban legfeljebb e hiba elkövetése után (e jegyet megváltoztatva) még egyértelműen meg tudjuk mondani, hogy melyik volt a kiindulási kódszó.*

Ebben a definícióban felmerül a kérdés, hogy mit értünk az alatt, hogy egyértelműen meg tudjuk mondani, hogy melyik volt a kiindulási kódszó. Ennek megértéséhez képzeljük el, hogy kapunk egy n hosszú **w** szót, amiben legfeljebb e helyen hiba van. Ismerjük C elemeit és **w**-ben akárhogy is változtatunk meg legfeljebb e koordinátát, csak egyféleképpen kaphatunk C-beli szót (különben nem tudnánk egyértelműen megmondani, hogy melyik kódszóban követtük el a hibákat).

2. Állítás. *C e-hibajavító kód $\iff d(C) \geq 2e+1$.*

Bizonyítás. $\Longrightarrow$: Indirekt módon tegyük fel, hogy van két olyan kódszó, **u** és **v**, amelyek Hamming távolsága legfeljebb $2e$. Ekkor előfordulhat, hogy mindkét kódszóban $e-e$ hibát követünk el úgy, hogy ugyanazt a szót kapjuk mindkét esetben (először **u**-ban e olyan helyen változtatunk, ahol eltér **v**-től, majd **v**-ben az ettől eltérő legfeljebb e koordinátát írjuk át azokkal egyezővé).
$\Longleftarrow$: Nyilvánvaló, hiszen legrosszabb esetben is ha minden kódszóban van e hiba, akkor sem kaphatjuk két kódszóból ugyanazt. □

Egy kód (adott hosszal és adott elemszámmal) gyakorlati szempontból akkor a legideálisabb, hogyha minél nagyobb a minimális távolsága, mert akkor annál több hibát bír kivédeni.
A következő tételekben nézzük meg, hogy mit mondhatunk el a minimális távolságról lineáris kódok esetében.

3. Állítás. *Legyen C egy $[n,k]_q$ lineáris kód. Ekkor C minimális távolsága pontosan a paritás-ellenőrző mátrixban lévő lineárisan összefüggő oszlopok minimális száma.*

Bizonyítás. Az 1 állítás alapján tudjuk, hogy a minimális távolság a legkisebb súlyú kódszó súlya.
Azt is tudjuk, hogy a H mátrix $i_1, i_2, \ldots, i_l$ különböző oszlopai pontosan akkor lineárisan összefüggőek, ha létezik olyan **x** kódszó (nem **0**), aminek a nem 0 koordinátái az $\{i_1, i_2, \ldots, i_l\}$ halmazba esnek.
Ez azt jelenti, hogy ha C minimális távolsága d, akkor van d lineárisan összefüggő oszlopa a fentiek miatt, de bármely $d-1$ lineárisan független. Ezzel beláttuk az állítást. □

1. Tétel (Singleton-korlát). *Legyen $C \leq \mathbb{F}_q^n$ egy lineáris $[n,k]_q$ kód. Ekkor a d minimális távolságra teljesül, hogy*

$$d \leq n-k+1.$$

Bizonyítás. $|C| = q^k$, mert annyi kódszó van egy k dimenziós lineáris altérben, mint amennyi vektor a k dimenziós térben, $\mathbb{F}_q^k$-ban.
Az, hogy a minimális távolság d, vagyis bármely két különböző kódszó Hamming-távosága legalább d, azt jelenti, hogy ha az összes kódszóból elhagyjuk az első $d-1$ koordinátát, akkor nem kaphatunk ugyanolyan szavakat, ebből kifolyólag

$$|C| \leq q^{n-(d-1)},$$

$$q^k \leq q^{n-(d-1)},$$

$$k \leq n - d + 1,$$

$$d \leq n - k + 1,$$

és ezt szerettük volna belátni. □

3. Megjegyzés. *A Singleton-korlát tetszőleges kódokon is értelmes, ebben a formában:* $|C| \leq q^{n-(d-1)}$*, ahol* $q = |Q|$*. Ez látszik is a fenti bizonyításból.*

3. MDS kódok

Ebben a fejezetben az [1] és [2] illetve [5] alapján vezetjük be az MDS kódokat és vizsgáljuk számunkra legfontosabb tulajdonságaikat.

10. Definíció (MDS kód). *Azokat a lineáris kódokat, amik a Singleton-korlátot egyenlőséggel teljesítik, MDS kódoknak hívjuk (Maximum Distance Separable rövidítése).*

Először nézzünk néhány konkrét példát MDS kódra az [5] könyv 7. fejezete alapján, ahol már a definícióból is egyszerűen belátható, hogy MDS kódok.

1. Példa. *Az alábbi kód MDS kód:*

$$C = \{(x_1, x_2, \dots x_k, x_1 + \dots + x_k) : x_1, \dots, x_k \in \mathbb{F}_q\}.$$

Bizonyítás. A kódszavak (vektorok) $n = k + 1$ hosszúak. Maga a kód pedig az

$$X_1 + X_2 + \dots + X_k - X_{k+1} = 0$$

egyenletű hipersíkot alkotó vektorokból áll (k dimenziós altér).
A kód minimális távolsága $d = 2$, hiszen az 1 állítás miatt elegendő a minimális súlyt meghatározni, ami 1 nyilvánvalóan nem lehet, hiszen pontosan egy nem 0 koordinátája nem lehet egyik kódszónak sem, mert ha az az első k koordináta között van, akkor az utolsó nem lehetne 0, mert az az előzőek összege, ha pedig az utolsó koordináta nem lenne 0, akkor az nem lenne az előtte lévők összege. 2-súlyúra pedig könnyű példát mutatni.
Ekkor $n-k+1 = k+1-k+1 = 2 = d$, tehát valóban egyenlőséggel teljesíti a Singleton-korlátot, így definíció szerint MDS kód. □

2. Példa. *Legyen* $\mathbb{F}_q = \{a_1, a_2, \dots, a_q\}$ *és*

$$C = \{(f(a_1), f(a_2), \dots, f(a_q), f_{k-1}) : f \in \mathbb{F}_q[X], \deg(f) \leq k-1\},$$

ahol f_{k-1} *az* X^{k-1} *együtthatója* f*-ben. Ekkor* C *egy* $q+1$ *hosszú szavakból álló MDS kód.*

Bizonyítás. Először is C egy lineáris altér $\mathbb{F}_q^{q+1}$-ben, mert a legfeljebb $k-1$-edfokú polinomok lineáris kombinációja is egy legfeljebb $k-1$-edfokú polinom.
Egy m-edfokú 1-változós polinom (ha nem azonosan 0) legfeljebb m helyen vehet fel 0-t , ezért $\forall\, \mathbf{0} \neq \mathbf{u} \in C$ vektorban legfeljebb $k-1$ koordináta helyén áll 0 (megjegyzendő, hogy ez $f_{k-1} = 0$ esetén is igaz, hiszen akkor f-nek legfeljebb $k-2$ gyöke van).
Emiatt $w(\mathbf{u}) \geq n-(k-1)$. Ezért az 1 állítás miatt $d \geq n-k+1$, a Singleton-korlát miatt pedig $d \leq n-k+1$, azaz $d = n-k+1$, vagyis C egy MDS kód. □

4. Megjegyzés. *Az előbbi típusú kódokat Reed-Solomon kódoknak hívjuk.*

3.1. Ekvivalens tulajdonságok, dualitás

A következő két tétel lehetővé teszi, hogy MDS kódok tárgyalásánál ne kelljen többé a kódról beszélni, hanem csak az (egyik) azt generáló mátrixról.

2. Tétel. *Egy C lineáris $[n,k]_q$ kód akkor és csak akkor MDS kód, ha a paritásellenőrző mátrixa egy olyan $(n-k)\times n$-es H mátrix, amelynek bármely $n-k$ oszlopa lineárisan független.*

Bizonyítás. Ha C egy lineáris $[n,k]_q$ MDS kód, akkor a d minimális távolság definíció szerint $d=n-k+1$. A 3 állítás miatt C minimális távolsága pontosan a paritásellenőrző mátrixban lévő lineárisan összefüggő oszlopok minimáis száma. Emiatt H-nak nem lehet $n-k+1=d$-nél kevesebb lineárisan összefüggő oszlopa, ezért bármely $n-k$ oszlopa lineárisan független.
Megfordítva indirekt módon tegyük fel, hogy C nem MDS kód, emiatt $d\leq n-k$. Szintén a 3 állítás miatt ekkor van H-nak $n-k$ darab lineárisan összefüggő oszlopa, ami ellentmond annak a feltevésnek, hogy bármely $n-k$ oszlop lineárisan független. □

3. Tétel. *Egy lineáris MDS kód duálisa is MDS kód.*

Bizonyítás.[20] Legyen C egy $[n,k]_q$ paraméterű lineáris MDS kód.
Az 1 megjegyzés és az előző tétel miatt elég annyit bizonyítanunk, hogy a $k\times n$-es G generátormátrixnak bármely k oszlopa lineárisan független.
Indirekt módon tegyük fel, hogy $\exists\, i_1,i_2,\ldots,i_k$ indexű oszlopok, melyek lineárisan összefüggenek, ami definíció szerint azt jelenti, hogy $\exists\, a_1,a_2,\ldots,a_k\in\mathbb{F}_q$, hogy

$$a_1x_{i_1}+a_2x_{i_2}+\cdots+a_kx_{i_k}=0,$$

ahol x_{i_j}, $j=1,\ldots,k$, az i_j-edik oszlopvektort jelöli. Feltehető, hogy $a_k\neq 0$ (különben az indexeket felcseréljük). Átrendezve azt kapjuk, hogy az i_k-adik oszlop előáll az $i_1,\ldots,i_{k-1}$ oszlopok lineáris kombinációjaként. Figyelembe véve, hogy ez egy generátormátrix, látszik, hogy minden C-beli x kódszó i_k-adik koordinátája előáll az $i_1,\ldots,i_{k-1}$-adik koordinátái lineáris kombinációjaként.
Legyen $U=C\cap\{X_{i_1}=X_{i_2}=\cdots=X_{i_{k-1}}=0\}$ altér. Ez megadható $(n-k)+(k-1)=n-1$ darab hipersík egyenlettel, ezért $\dim U\geq 1\Rightarrow\exists\,\mathbf{y}\in U\setminus\{\mathbf{0}\}$.
Az $y_{i_k}=0$, mert előáll az $i_1,\ldots,i_{k-1}$-edik koordinátáinak lineáris kombinációjaként, de azok mind 0-k U-ban. Ebből kifolyólag $w(\mathbf{y})\leq n-k=d-1$, ami ellentmond az 1 állításnak, tehát az indirekt feltétel hibás volt, emiatt a G generátormátrix bármely k oszlopa lineárisan független, így a duális kód is MDS, hiszen annak pont G lesz a paritásellenőrző mátrixa. □

1. Következmény. *Egy C lineáris $[n,k]_q$ kód akkor és csak akkor MDS kód, ha a generátor mátrixa egy olyan $k\times n$-es G mátrix, amelynek bármely k oszlopa lineárisan független.*

3.2. Kapcsolat a projektív terekkel

Az előző részben beláttuk, hogy egy lineáris kód akkor és csak akkor MDS kód, ha a paritásellenőrző mátrixában bármely $n-k$ oszlop által meghatározott $n-k$ darab vektor lineárisan független. Azt is láttuk, hogy lineáris MDS kód duálisa is az, és a paritásellenőrző- illetve generátormátrixok felcserélődnek, ezért ahhoz, hogy a kód MDS legyen az is szükséges és elégséges feltétel, hogy a generátormátrixának bármely k oszlopa által meghatározott vektorai lineárisan függetlenek legyenek. Felmerül a kérdés, hogy rögzített k és $\mathbb{F}_q$ mellett mi az elérhető leghosszabb lineáris MDS kód, azaz n-et szeretnénk maximalizálni, amivel persze a maximális távolságot is maximalizáljuk ($d = n-k+1$ miatt). Ezzel a kérdéssel foglalkozik a lineáris kódokra vonatkozó MDS-sejtés. Ehhez érdemes lesz megvizsgálni, hogy hogyan írhatjuk át a problémát a véges test feletti projektív tér nyelvezetére.
A továbbiakban a $\mathrm{PG}(k-1,q)$ jelölést alkalmazzuk a $k-1$ dimenziós $\mathbb{F}_q$ q-elemű test feletti projektív térre.

11. Definíció (ív). $\mathrm{PG}(k-1,q)$ *projektív térben egy* $\mathcal{A}$ *ponthalmazt ívnek nevezünk, ha semelyik* k *pontja sincs ugyanazon a hipersíkon. Az ív teljes, ha a tartalmazásra nézve maximális, azaz nem része semmilyen nagyobb méretű ívnek.*

Ez azt jelenti, hogy bármely k darab különböző, $\mathcal{A}$-beli pontokat reprezentáló vektor lineárisan független.

4. Tétel. *Egy* G *generátormátrixszal generált* $[n,k]_q$ *lineáris kód MDS akkor és csak akkor, ha a* G *oszlopai által meghatározott* $\mathrm{PG}(k-1,q)$*-beli vektorok egy ívet alkotnak.*

Bizonyítás. Az odafele irány az előző részben megfogalmazott tételekből következik.
Megfordítva, ha van n darab $\mathrm{PG}(k-1,q)$-beli pontunk melyek egy ívet alkotnak, akkor az azokat reprezentáló k hosszú vektorok közül bármelyik k lineárisan független, azaz bázist alkot, így az oszlopvektorok egymás mellé írásából képzett mátrix egy lineáris MDS kód generátormátrixának felel meg. □
A következő tulajdonsága az íveknek még hasznos lesz számunkra:

4. Állítás. *Pontosan akkor létezik* $\mathrm{PG}(k-1,q)$*-ban* n *pontú ív, ha létezik* $\mathrm{PG}(n-k-1,q)$*-ban is* n *pontú ív.*

Bizonyítás. A 3 és 4 tételekből következik. □

Ezek alapján a maximális hosszúságú MDS kódokhoz elég maximális méretű íveket találnunk, így a továbbiakban áttérünk a $\mathrm{PG}(k-1,q)$ véges projektív tér íveinek vizsgálatára. Azt is látjuk, hogy a 2 megjegyzés alapján egy adott ív kölcsönösen egyértelműen megfeleltethető egymással lineárisan ekvivalens kódok egy osztályának.
A továbbiakban gyakran fogunk a projektív tér pontjait reprezentáló homogén koordinátákkal számolni, viszont az egyszerűség kedvéért az $(x_1 : x_2 : \ldots : x_k)$ jelöléstől általában eltekintünk.

Először nézzük meg, hogy $k \geq q+1$ esetén milyen felső korlátot adhatunk a $\mathrm{PG}(k-1,q)$-beli ívek méretére.

5. Állítás. *Legyen $k \geq q+1$ és $\mathcal{A}$ egy ív $\mathrm{PG}(k-1,q)$-ban úgy, hogy $|\mathcal{A}| = n$. Ekkor $n \leq k+1$, sőt, ha $n = k+1$, akkor az ívhez tartozó MDS kód ekvivalens az 1 példával.*

Bizonyítás.[5] Indirekt módon tegyük fel, hogy $n > k+1$. Megválaszthatjuk úgy a bázist, hogy az $\mathcal{A}' = \{(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,\ldots,0,1),(1,1,\ldots,1)\}$ homogén koordinátákkal leírt ponthalmaz része $\mathcal{A}$-nak. Ekkor az indirekt feltétel miatt $\exists\, x \in \mathcal{A} \setminus \mathcal{A}'$, legyen az ezt a pontot reprezentáló vektor $(x_1, x_2, \ldots, x_k)$ a bázisunkban. Mivel $k \geq q+1$, ezért a skatulya-elv miatt $\exists\, x_i = x_j$, $i \neq j$.
Ekkor viszont jól látható, hogy az $X_i - X_j = 0$ egyenletű hipersíkon lesz k darab $\mathcal{A}$-beli pont, ami ellentmond annak, hogy $\mathcal{A}$ egy ív. $\square$

4. A Segre-féle MDS-sejtés

Most már minden rendelkezésünkre áll, hogy rátérjünk a dolgozat témájára, a maximális méretű MDS kódokra vonatkozó sejtésre.
Először mondjuk ki a sejtést kódokra az [5] könyv (7.8. sejtés) alapján.

1. Sejtés (MDS-sejtés, kódokra vonatkozó változat). *Legyen C egy lineáris $[n,k]_q$ kód, tegyük fel, hogy $k \leq q$. Ekkor $n \leq q+1$, kivéve, ha $k=3$ vagy $k=q-1$ és q páros, mert ebben az esetben $n \leq q+2$.*

Ezt az 1 következmény, illetve a 4 tétel miatt az alábbiak szerint ekvivalens módon átfogalmazhatjuk.

2. Sejtés (MDS-sejtés, vektorváltozat). *Ha az $S \subseteq \mathbb{F}_q^k$ vektorhalmaz bármely k vektorból álló eleme bázis és $k \leq q$, akkor S elemszáma legfeljebb $q+1$, kivéve, amikor q páros és $k=3$ vagy $k=q-1$, mert akkor S elemszáma legfeljebb $q+2$.*

3. Sejtés (MDS-sejtés, ívekre). *Legyen $\mathcal{A} \subseteq \mathrm{PG}(k-1,q)$ egy $k-1$ dimenziós projektív téren értelmezett ív, tegyük fel, hogy $k \leq q$. Ekkor $|\mathcal{A}| \leq q+1$, kivéve ha $k=3$, vagy $k=q-1$ és q páros, mert akkor $|\mathcal{A}| \leq q+2$.*

A problémát először Segre tűzte ki ez utóbbi megfogalmazásban ívekre.
A sejtést azért csak a $k \leq q$ esetben mondjuk ki, mert ha $k \geq q+1$, akkor a 5 állításban leírtak szerint egyszerűen adható felső korlát $|\mathcal{A}| = n$-re.

A következő részekben megnézzük az MDS-sejtés néhány speciális esetének bizonyítását. Innentől végig a

$$q = p^h$$

jelölést alkalmazzuk valamely p prímre és $h \in \mathbb{N}^+$ számra (akkor is, ha nincs külön kikötve).
Vegyük észre, hogy az MDS-sejtés triviálisan igaz ha $k=2$, hiszen akkor egy $[n,2]_q$ kód generátormátrixába minél több 2 hosszúságú oszlopvektort szeretnénk írni úgy, hogy semelyik kettő se legyen egymásnak a többszöröse. Ebből persze legfeljebb annyi van, mint ahány pont a projektív egyenesen, ami $q+1$.

4.1. A projektív sík esete

A definíció alapján a projektív síkbeli ívek pontosan azok a ponthalmazok, amelyeknek semelyik három pontja nem esik egy egyenesre.

5. Tétel (Bose, 1947.). *Legyen $\mathcal{A}$ egy ív az $\mathbb{F}_q$ feletti véges projektív síkon. Ekkor*

$$|\mathcal{A}| \leq \begin{cases} q+1 & \text{ha } q \text{ páratlan,} \\ q+2 & \text{ha } q \text{ páros.} \end{cases}$$

Bizonyítás.[1] Vegyünk egy tetszőleges $P \in \mathcal{A}$ pontot az íven. Ezen a ponton át $q+1$ egyenes megy. Ezek mindegyike P-n kívül még legfeljebb egy pontot tartalmazhat, ezért $|\mathcal{A}| \leq q+2$.
Tegyük fel, hogy $|\mathcal{A}| = q+2$. Ekkor minden $P \in \mathcal{A}$ pontra igaz, hogy minden rá illeszkedő egyenes tartalmaz még egy pontot, így az $\mathcal{A}$ ívnek nincsenek érintői. Legyen Q egy tetszőleges $\mathcal{A}$-n kívüli pont. A Q-n átmenő egyenesek az $\mathcal{A}$ ívnek 0- vagy 2-szelői, emiatt $|\mathcal{A}| = q+2$ páros, így ez az eset csak akkor állhat fenn, ha q páros.
Ha q páratlan, akkor pedig az eddigiek alapján $|\mathcal{A}| \leq q+1$. □
Ezzel tehát könnyedén beláttuk az MDS-sejtés síkbeli esetét. Nézzük meg a következő állítást, ami szerint páros elemű test fölött egy $q+1$ méretű ív mindig teljessé tehető.

6. Állítás. *Ha q páros, akkor minden* $\mathrm{PG}(2,q)$*-beli $q+1$ méretű ív része egy $q+2$ méretűnek.*

Bizonyítás.[1] Az állítást úgy fogjuk belátni, hogy találunk egy olyan pontot, amit összekötve az $\mathcal{A}$ ív mindegyik pontjával, nem lesz rajta más $\mathcal{A}$-beli pont, vagyis a szóban forgó $q+1$ egyenes mind különböző pontban érintője $\mathcal{A}$-nak.
$\mathcal{A}$ egy P pontját összekötve az ív többi pontjával q darab különböző egyenest kapunk, marad egy, ami csak P-n megy keresztül, vagyis $\mathcal{A}$-nak minden pontjában pontosan egy érintője van. Ahhoz, hogy belássuk, hogy ezek egy ponton mennek át, elég lenne azt megmutatnunk, hogy ezek az érintők lefedik a sík pontjait, mert q^2+q+1 pontja van a síknak, nekünk pedig $q+1$ egyenesünk, ezek mindegyikén $q+1$ pont van. Ha az egyenesek átmennek a sík összes pontján, akkor figyelembe véve, hogy bármely kettőnek van közös pontja, ez csak úgy lehet, hogy egy pontban metszik egymást.
Tehát már csak azt kell belátnunk, hogy az érintő egyenesek lefedik a síkot. Vegyünk egy tetszőleges $Q \notin \mathcal{A}$ pontot. Ezt kössük össze $\mathcal{A}$ minden pontjával. Mivel $q+1$ páratlan, ezért lesz olyan ezek között, ami csak egy pontján megy át $\mathcal{A}$-nak, azaz minden $Q \notin \mathcal{A}$ rajta van egy érintőn, ezért az érintők egy pontban metszik egymást. □
A síkbeli ívek karakterizálásának problémájáról még az 5.1 alfejezetben lesz szó.

A következő két eset bizonyítását először Simeon Ball [7], Ball és De Beule [8] publikálták, majd Ball és Lavrauw a [3] cikkben egységesítették a bizonyításokat.

A következő részekben ismerkedjünk meg a $4 \leq k \leq p$ és $p < k < 2p-2$ esetének bizonyításához szükséges eszközökkel. Ezek az új fogalmak, állítások önmagukban is jelentősek, illetve más problémáknál is hasznosak lehetnek. Ezeknél jórészt Ball és Lavrauw [3] cikkét dolgoztam fel. A bizonyítások érdekessége, hogy alapvetően Segre ötletét használja fel magasabb dimenzióban. Az eredeti, síkbeli változatról részletesebben a [6] forrásban lehet olvasni.

4.2. Érintők lemmája

1. Lemma. *Ha S egy $(k-2)$ elemű részhalmaza egy $\mathcal{A}$,* $\mathrm{PG}(k-1,q)$*-beli ívnek, akkor pontosan $t = q+k-|\mathcal{A}|-1$ olyan hipersík van, ami pontosan S-ben metszi $\mathcal{A}$-t.*

Bizonyítás. Összesen $q+1$ darab hipersík tartalmazza az S által kifeszített $(k-3)$ dimenziós alteret ([1], 4.6. tétel). Mivel $\mathcal{A}$ egy ív, ezért mindegyik hipersík még legfeljebb egy $\mathcal{A} \setminus S$-beli pontot tartalmaz, ezért pontosan $q+1-|\mathcal{A} \setminus S| = q+1-(|\mathcal{A}|-(k-2)) = q+k-|\mathcal{A}|-1 = t$ olyan hipersík van, ami csak S-ben metszi $\mathcal{A}$-t. □
Ennek a t-nek hamarosan nagy szerepe lesz az új fogalmak bevezetésével kapcsolatban.

2. Következmény. *Egy* $\mathrm{PG}(k-1,q)$*-beli ívnek legfeljebb* $q+k-1$ *pontja van.*

Bizonyítás. Az előző lemmából következik, mivel $t \geq 0$ és $t = q+k-|\mathcal{A}|-1$-et behelyettesítve, átrendezve pont a kívánt felső korlátot kapjuk $|\mathcal{A}|$-ra. □

Mostantól tegyük fel, hogy $\mathcal{A}$ egy $q+k-1-t$ méretű ív $\mathrm{PG}(k-1,q)$-ban, és $\mathcal{A}$-ban valahogyan sorba rendezzük a pontokat. Legyen $S \subset \mathcal{A}$ egy $k-2$ méretű részhalmaz ugyanúgy rendezve, mint $\mathcal{A}$-ban. Legyenek $\alpha_1, \ldots, \alpha_t$ lineáris formák, az 1 lemmabeli S-en áthaladó, $\mathcal{A}$-t csak S-ben metsző hipersíkok egyenletei. Definiáljunk (skalárszorzó erejéig) egy homogén k-változós, t-edfokú polinomot:

$$f_S(X) = \prod_{i=1}^{t} \alpha_i(X), \tag{1}$$

ahol $X = (X_1, \ldots, X_k)$ a változók. S minden σ permutációjára legyen

$$f_{\sigma(S)}(X) = (-1)^{s(\sigma)(t+1)} f_S(X),$$

ahol $s(\sigma)$ a σ inverziószáma.
Az f k-változós homogén polinom meghatároz egy $\tilde{f}\colon \mathbb{F}_q^k \to \mathbb{F}_q$ függvényt. Ha megváltoztatjuk a bázist $\mathbb{F}_q^k$-ban, akkor ugyan f meg fog változni, de $\tilde{f}$ nem.

2. Lemma (Koordinátafüggetlen érintők lemmája). *Legyen* $\mathcal{A}$ *egy ív* $\mathrm{PG}(k-1,q)$*-ban, és legyen* D *egy* $k-3$ *elemű részhalmaza* $\mathcal{A}$*-nak. Ekkor minden* $x, y, z \in \mathcal{A} \setminus D$*-re*

$$f_{D\cup\{x\}}(y) f_{D\cup\{y\}}(z) f_{D\cup\{z\}}(x) = (-1)^{t+1} f_{D\cup\{y\}}(x) f_{D\cup\{z\}}(y) f_{D\cup\{x\}}(z). \tag{2}$$

Bizonyítás. Legyen f_a^* az a polinom, amit $f_{D\cup\{a\}}$-ból kapunk a $B = \{x, y, z\} \cup D$ bázisban (ez azt jelenti, hogy $x = (1, 0, \ldots, 0)$, $y = (0, 1, 0, \ldots, 0)$, $z = (0, 0, 1, 0, \ldots, 0)$ felírásokat használjuk). Mivel elég tetszőleges bázisban igazolnunk az állítást, ezért dolgozhatunk az ily módon kapott, *-gal ellátott polinomokkal. Ekkor

$$f_x^*(X) = \prod_{i=1}^{t}(a_{i2}X_2 + a_{i3}X_3),\ f_y^*(X) = \prod_{i=1}^{t}(b_{i1}X_1 + b_{i3}X_3),\ f_z^*(X) = \prod_{i=1}^{t}(c_{i1}X_1 + c_{i2}X_2)$$

valamely $a_{ij}, b_{ij}, c_{ij} \in \mathbb{F}_q \setminus \{0\}$ számokra (ezek egyike sem lehet 0, mert akkor vagy nem kapnánk hipersík egyenletet, vagy $X_i = 0$ típusút kapnánk, ami B-nek, így $\mathcal{A}$-nak is már $k-1$ pontján átmenne, de itt pont nem ilyeneket írtunk fel). Egy $D \cup \{x\}$ és $s = (s_1, \ldots, s_k)$ pontokra illeszkedő hipersík egyenlete $(s_3X_2 - s_2X_3) = 0$.
Ha s befutja $\mathcal{A} \setminus B$ pontjait, akkor s_2 és s_3 egyike sem lehet 0, mert ha például $s_2 = 0$, akkor s rajta van az x, z és D által meghatározott hipersíkon, de akkor nem lehet rajta az íven, ugyanígy

s_3 sem lehet 0. Ekkor $-\frac{s_2}{s_3}$ értelmes és végigfut $\mathbb{F}_q \setminus (\{\frac{a_{i3}}{a_{i2}} : i = 1, \ldots, t\} \cup \{0\})$ elemein, hiszen a hipersíkok különbözőek kell, hogy legyenek és nem lehetnek olyanok, amik $\mathcal{A}$-t csak $D \cup \{x\}$-ben metszik (ezért nem fut végig a teljes $\mathbb{F}_q \setminus \{0\}$-n $-\frac{s_2}{s_3}$).
Felhasználva, hogy $\mathbb{F}_q$ nem nulla elemeinek szorzata -1 (Wilson-tétel), ezt kapjuk:

$$\prod_{s \in \mathcal{A} \setminus B} -\frac{s_2}{s_3} \prod_{i=1}^{t} \frac{a_{i3}}{a_{i2}} = -1,$$

mivel $f_x^*(z) = \prod_{i=1}^{t} a_{i3}$ és $f_x^*(y) = \prod_{i=1}^{t} a_{i2}$, ezért átszorozva

$$f_x^*(z) \prod_{s \in \mathcal{A} \setminus B} (-s_2) = -f_x^*(y) \prod_{s \in \mathcal{A} \setminus B} s_3.$$

Ehhez hasonlóan felírhatjuk $D \cup \{y\}$ és $D \cup \{z\}$ ponthalmazokra is:

$$f_y^*(x) \prod_{s \in \mathcal{A} \setminus B} (-s_3) = -f_y^*(z) \prod_{s \in \mathcal{A} \setminus B} s_1,$$

$$f_z^*(y) \prod_{s \in \mathcal{A} \setminus B} (-s_1) = -f_z^*(x) \prod_{s \in \mathcal{A} \setminus B} s_2.$$

A három egyenletet összeszorozva azt kapjuk, hogy

$$f_x^*(z) f_y^*(x) f_z^*(y) (-1)^{3(q-1-t)} = (-1)^3 f_x^*(y) f_y^*(z) f_z^*(x).$$

Ha q páratlan, akkor pontosan a

$$f_x^*(z) f_y^*(x) f_z^*(y) = (-1)^{t+1} f_x^*(y) f_y^*(z) f_z^*(x),$$

kifejezést kapjuk, ami a bizonyítandó állítással ekvivalens. Ha q páros, akkor is írhatjuk így az eredményt, hiszen a 2^h elemű test karakterisztikája 2, így ott $(-1) = 1$, és ezt szerettük volna belátni. □

5. Megjegyzés. *Vegyük észre, hogy a $k = 3$, q páratlan, síkbeli esetben az érintők lemmája azt mondja ki, hogy az $\mathcal{A}$, $q+1$ méretű ív bármely három pontja által meghatározott háromszög és az azokon a pontokon átmenő $\mathcal{A}$-hoz tartozó érintők által meghatározott háromszögek perspektívek (ez a [6] forrásban is szereplő Menelaosz-tételből látszik).*

4.3. Skálázás

Legyen $\mathcal{E}$ az $\mathcal{A}$ első $k-2$ eleméből képzett halmaz. $\mathcal{A}$ minden $k-2$ elemű $\mathcal{E} \neq S \subset \mathcal{A}$ részhalmazára skálázzuk az $f_S(X)$ polinomot úgy, hogy

$$f_S(e) = (-1)^{s(t+1)} f_{S \cup \{e\} \setminus \{a\}}(a), \tag{3}$$

ahol e az első eleme $\mathcal{E} \setminus \mathcal{S}$ halmaznak, a pedig $S \setminus \mathcal{E}$ utolsó eleme és s annak a permutációnak a paritása, ami (S, e)-t az $\mathcal{A}$-beli rendezésébe viszi (itt az (S, e) rendezését úgy kell érteni, hogy S-nek az eredeti $\mathcal{A}$-beli rendezése alkotja az első $k-2$ elemet, az utolsó pedig e, vagyis

e-t egyszerűen csak hozzáillesztjük az S végéhez). Itt mindkét oldalon az f indexében lévő halmazon az $\mathcal{A}$ szerinti rendezést értjük.
Ezt a következőképpen érjük el: először minden $\mathcal{A}$-beli ponthoz rögzítsük a reprezentáló vektor koordinátáit (tehát innentől nem mindegy, hogy (a, b, c) vagy például $(2a, 2b, 2c)$-vel reprezentáljuk az $(a : b : c)$ pontot). Eddig $f_S(X)$ polinom is csak skalárszorzó erejéig volt egyértelműen definiálva. Ezt a skalárszorzót állítja be a skálázás, hogy teljesüljön (3). Ehhez először rögzítsük $f_{\mathcal{E}}(X)$ skalárszorzóját tetszőlegesen. Ezután pedig $|\mathcal{E} \cap S|$ szerint csökkenő sorrendben rekurzívan skálázzuk az összes $S \subseteq \mathcal{A}$, $|S| = k-2$ részhalmazhoz tartozó $f_S(X)$ polinomot. Ha $|\mathcal{E} \cap S| = k-3$, akkor (3) jobb oldalán már egy konkrét szám áll, hiszen ekkor $S \cup \{e\} \setminus \{a\}$ csakis $\mathcal{E}$ lehet, amihez már van skálázott $f_{\mathcal{E}}(X)$, ezért hogy teljesüljön az egyenlőség $f_S(X)$-et már egyértelműen tudjuk skálázni. Vegyük észre, hogy ez a skálázás valóban megtehető, hiszen egyik oldal sem 0. Ezt tovább folytatva a jobb oldalon mindig már skálázott polinom áll, hiszen ha $|\mathcal{E} \cap S| = l$, akkor $|\mathcal{E} \cap (S \cup \{e\} \setminus \{a\})| = l + 1$.

3. Lemma. *Legyen $\mathcal{A}$ egy ív a $\mathrm{PG}(k-1, q)$ projektív téren, D pedig egy $k-3$ elemű részhalmaza. Ekkor minden $x, y \in \mathcal{A} \setminus D$ pontokra fennáll:*

$$f_{D\cup\{x\}}(y) = (-1)^{s(\sigma)(t+1)} f_{D\cup\{y\}}(x),$$

ahol σ az a permutáció, ami $(D \cup \{x\}, y)$-t átrendezi $(D \cup \{y\}, x)$ sorrendbe és $s(\sigma)$ ennek a permutációnak a paritása.

Bizonyítás. Indukcióval $|D \cap \mathcal{E}|$ szerint.
Először tegyük fel, hogy $|D \cap \mathcal{E}| = k-3$ és legyen e az egyetlen eleme $\mathcal{E} \setminus D$-nek. Ha e az x vagy y pontok valamelyikével egybeesik, akkor ez utóbbi, $e = y$ esetet vizsgálva legyen $S = D \cup \{x\}$. Ekkor $S \setminus \mathcal{E} = \{x\}$, tehát $\{x\}$ az egyetlen és eredeti sorrend szerint utolsó eleme $S \setminus \mathcal{E}$-nak, továbbá $\mathcal{E} \setminus S$ első és egyetlen eleme pedig y. Ezekre a (3), skálázás alapján

$$f_{D\cup\{x\}}(y) = f_S(e) = (-1)^{s(t+1)} f_{S\cup\{e\}\setminus\{x\}}(x) = (-1)^{s(t+1)} f_{D\cup\{y\}}(x),$$

ahol s annak a permutációnak az inverziószáma, ami $(S, e) = (D\cup\{x\}, y)$-t az $\mathcal{A}$-beli rendezésébe viszi át, ami éppen a $(D \cup \{y\}, x)$ sorrend is egyben. Tehát ebben az esetben igaz a lemma. Az $e = x$ eset is szerepcserével ugyanígy belátható.
Ha pedig x, y és e különbözőek, akkor ezekre a pontokra alkalmazva a 2 lemmát, az

$$f_{D\cup\{x\}}(y) f_{D\cup\{y\}}(e) f_{D\cup\{e\}}(x) = (-1)^{t+1} f_{D\cup\{y\}}(x) f_{D\cup\{e\}}(y) f_{D\cup\{x\}}(e) \tag{4}$$

kifejezést kapjuk.
A skálázás miatt

$$f_{D\cup\{x\}}(e) = (-1)^{s(\theta)(t+1)} f_{D\cup\{e\}}(x), \tag{5}$$

ahol θ az a permutáció, ami $(D \cup \{x\}, e)$-t $(D \cup \{e\}, x)$ sorrendbe rendezi át és

$$f_{D\cup\{y\}}(e) = (-1)^{s(\tau)(t+1)} f_{D\cup\{e\}}(y), \tag{6}$$

ahol τ az a permutáció, ami $(D \cup \{y\}, e)$-t $(D \cup \{e\}, y)$ sorrendbe rendezi.
Behelyettesítve (4) egyenlet jobb oldalába (5) és (6) egyenleteket, azt kapjuk, hogy

$$f_{D\cup\{x\}}(y) = (-1)^{(s(\theta)+s(\tau)+1)(t+1)} f_{D\cup\{y\}}(x).$$

Legyen σ az a permutáció, ami $(D \cup \{x\}, y)$-t a $(D \cup \{y\}, x)$ sorrendbe viszi. Vegyük észre, hogy ennek a paritása éppen $s(\sigma) = s(\theta) + s(\tau) + 1$, mert $s(\theta) = s(\tau)$, hiszen mindkettő permutációban ugyanannyi transzpozíciót kell végrehajtani, illetve $s(\sigma) = 1$, mivel σ egyetlen transzpozíció. Ebből pedig következik a lemma állítása $|D \cap \mathcal{E}| = k - 3$ esetben.

A továbbiakban tegyük fel, hogy $|D \cap \mathcal{E}| \leq k - 4$ és az állítás igaz minden olyan $D' \subseteq \mathcal{A}$, $|D'| = k - 3$ halmazra, ahol $|D' \cap \mathcal{E}| > |D \cap \mathcal{E}|$ (az indukció lefele megy).
Legyen e az első eleme $\mathcal{E} \setminus (D \cup \{y\})$-nak.
Ha $e = x$, akkor legyen z az utolsó eleme $D \cup \{y\}$-nak. Ekkor a skálázás miatt

$$f_{D\cup\{y\}}(x) = f_{D\cup\{y\}}(e) = (-1)^{s(\alpha)(t+1)} f_{D\cup\{e,y\}\setminus\{z\}}(z), \tag{7}$$

ahol α az a permutáció, ami $(D\cup\{y\}, e)$-t $(D\cup\{e, y\}\setminus\{z\}, z)$, eredeti $\mathcal{A}$-beli sorrendjébe rendezi vissza. Ha $y = z$, akkor ezzel be is láttuk ebben az esetben az állítást. Ha nem, akkor alakítsuk tovább, legyen $D^* = D \cup \{e\} \setminus \{z\}$. Erre már $|D^* \cap \mathcal{E}| > |D \cap \mathcal{E}|$, hiszen $e \in \mathcal{E}$ és $z \notin \mathcal{E}$, ezért alkalmazhatjuk az indukciós feltételt D^*-ra:

$$f_{D\cup\{e,y\}\setminus\{z\}}(z) = (-1)^{s(\beta)(t+1)} f_{D\cup\{e\}}(y), \tag{8}$$

ahol β az a permutáció, ami $(D \cup \{e, y\} \setminus \{z\}, z)$-t átviszi $(D \cup \{e\}, y)$-ba. Ezt behelyettesítve 7 egyenletbe:

$$f_{D\cup\{y\}}(x) = (-1)^{s(\alpha)(t+1)} f_{D\cup\{e,y\}\setminus\{z\}}(z) =$$
$$= (-1)^{(s(\alpha)+s(\beta))(t+1)} f_{D\cup\{e\}}(y) = (-1)^{(s(\alpha)+b(\beta))(t+1)} f_{D\cup\{x\}}(y),$$

ahol $s(\alpha)+s(\beta)$ megegyezik annak a permutációnak a paritásával, ami $(D\cup\{x\}, y)$-t $(D\cup\{y\}, x)$-be viszi át, ezzel az $x = e$ esetet beláttuk (az $y = e$ eset pedig ezzel teljesen analóg módon megy).
Ha $e \neq x$, akkor ismét jelölje z a $D \cup \{y\}$ utolsó elemét. A skálázás miatt

$$f_{D\cup\{y\}}(e) = (-1)^{s(\tau)(t+1)} f_{D\cup\{e,y\}\setminus\{z\}}(z),$$

ahol τ az a permutáció, ami $(D \cup \{y\}, e)$-t átrendezi $(D \cup \{e, y\} \setminus \{z\}, z)$-be.
Az indukciós feltétel miatt igaz az állítás $D^* := D \cup \{e\} \setminus \{z\}$-re, mert $|D^* \cap \mathcal{E}| > |D \cap \mathcal{E}|$, hiszen ez előbbiben benne van e, míg az utóbbiban nem. Felhasználva, hogy $D^* \cup \{y\} = D \cup \{e, y\} \setminus \{z\}$ és $D^* \cup \{z\} = D \cup \{e\}$, tudjuk, hogy

$$f_{D\cup\{e,y\}\setminus\{z\}}(z) = (-1)^{s(\theta)(t+1)} f_{D\cup\{e\}}(y),$$

ahol $\theta \circ \tau$ az a permutáció, ami $(D \cup \{y\}, e)$-t átviszi $(D \cup \{e\}, y)$-ba.
Vegyük észre, hogy e az első eleme $\mathcal{E} \setminus (D \cup \{x\})$-nek is (mert $x \neq e$), az $x = e$ esetben leírtakkal megegyező gondolatmenet alapján (gondolhatunk úgy rá, hogy x váltja fel az ottani y szerepét)

$$f_{D\cup\{x\}}(e) = (-1)^{s(\pi)(t+1)} f_{D\cup\{e\}}(x),$$

ahol π az a permutáció, ami átviszi $(D \cup \{x\}, e)$-t $(D \cup \{e\}, x)$-be.
Ismét alkalmazzuk a 2 lemmát D-re és x, y, és e-re és helyettesítsük be az előbbi eredményeket:

$$f_{D\cup\{x\}}(y) f_{D\cup\{y\}}(e) f_{D\cup\{e\}}(x) = (-1)^{t+1} f_{D\cup\{y\}}(x) f_{D\cup\{e\}}(y) f_{D\cup\{x\}}(e),$$

$$f_{D\cup\{x\}}(y) = (-1)^{(s(\tau)+s(\theta)+s(\pi)+1)(t+1)} f_{D\cup\{y\}}(x).$$

Ebből pedig már következik az indukciós lépés és egyben a lemma is, hiszen ha σ az a permutáció, ami $(D \cup \{y\}, x)$-et átviszi $(D \cup \{x\}, y)$-ba, akkor

$$s(\sigma) = s(\theta) + s(\tau) + s(\pi) + 1,$$

mivel $(D \cup \{x\}, y)$-ra x és y transzpozíciója után alkalmazva π-t, majd $(\theta \circ \tau)^{-1}$-et, pont a $(D \cup \{y\}, x)$ rendezést kapjuk, ezzel beláttuk a bizonyítandó állítást. □

Vezessük be az alábbi, $\mathcal{A}$-nak a rendezett $k-1$ elemű részhalmazain értelmezett g függvényt:

$$g(S, a) = (-1)^{s(t+1)} f_S(a), \tag{9}$$

ahol S az $\mathcal{A}$ ívnek egy tetszőlegesen rendezett $k-2$ elemű részhalmaza, s pedig annak a permutációnak az inverziószáma, ami S-et visszarendezi az eredeti, $\mathcal{A}$-beli sorrendjébe (tehát a [18] cikk 3. fejezete szerint definiáljuk s-et). Jegyezzük meg, hogy itt $f_S(a)$-t az S $\mathcal{A}$-beli rendezésén tekintjük.

4. Lemma (Érintők lemmája-skálázott, koordinátafüggetlen változat). *Legyen σ egy* $\mathrm{Sym}(k-1)$*-beli permutáció és C egy rendezett $k-1$ elemű részhalmaza $\mathcal{A}$-nak. Ekkor*

$$g(C^\sigma) = (-1)^{s(\sigma)(t+1)} g(C),$$

ahol $s(\sigma)$ a σ permutáció paritása.

Bizonyítás. Legyenek C rendezett elemei $c_1, c_2, \ldots, c_{k-1}$. Alkalmazva σ permutációt C elemein, jelöljük $s_1, s_2, \ldots, s_{k-1}$-gyel a C permutált elemeit σ szerint. Ekkor g definíciója alapján

$$g(C^\sigma) = g(\{s_1, \ldots, s_{k-2}\}, s_{k-1}) = (-1)^{s(\tau)(t+1)} f_{\{s_1,\ldots s_{k-2}\}}(s_{k-1}), \tag{10}$$

ahol τ az a permutáció, ami a $\{s_1, \ldots, s_{k-2}\}$ rendezett halmazt visszarendezi az eredeti, $\mathcal{A}$-beli sorrendjébe.
Ha $c_{k-1} = s_{k-1}$, akkor

$$g(C^\sigma) = (-1)^{s(\tau)(t+1)} f_{\{c_1,\ldots c_{k-2}\}}(c_{k-1}) = (-1)^{s(\theta\circ\sigma^{-1})(t+1)} f_{\{c_1,\ldots c_{k-2}\}}(c_{k-1}) = (-1)^{s(\sigma)(t+1)} g(C),$$

ahol θ az a permutáció, ami $\{c_1, \ldots, c_{k-2}\}$ rendezett halmazt visszarendezi az eredeti, $\mathcal{A}$-beli sorrendjébe. Vegyük észre, hogy ebben az esetben θ és τ ugyanazon a halmazon hatnak, és hogy $s(\sigma|_{\{c_1,\ldots,c_{k-2}\}}) = s(\sigma)$. Mivel $s(\theta \circ (\sigma|_{\{c_1,\ldots,c_{k-2}\}})^{-1}) = s(\theta) + s((\sigma|_{\{c_1,\ldots,c_{k-2}\}})^{-1}) = s(\theta) + s(\sigma)$, ezért ebben az esetben beláttuk az állítást.

Ha pedig $c_{k-1} \neq s_{k-1}$, akkor a 3 lemmát alkalmazhatjuk a $D = \{c_1, \ldots, c_{k-2}\} \setminus \{s_{k-1}\}$, $x = c_{k-1}$, $y = s_{k-1}$ szereposztással:

$$f_{\{s_1,\ldots,s_{k-2}\}}(s_{k-1}) = (-1)^{s(\alpha)(t+1)} f_{\{c_1,\ldots,c_{k-2}\}}(c_{k-1}),$$

ahol α az a permutáció, ami $(\{s_1, \ldots, s_{k-2}\}_{\mathcal{A}}, s_{k-1})$-et $(\{c_1, \ldots, c_{k-2}\}_{\mathcal{A}}, c_{k-1})$-be viszi át, ahol $\{.\}_{\mathcal{A}}$ jelölés arra emlékeztet, hogy az adott halmazon belül a $\mathcal{A}$-beli rendezést tekintjük. Az így kapottakat helyettesítsük be (10) egyenletbe:

$$(-1)^{s(\tau)(t+1)} f_{\{s_1,\ldots s_{k-2}\}}(s_{k-1}) = (-1)^{(s(\tau)+s(\alpha))(t+1)} f_{\{c_1,\ldots,c_{k-2}\}}(c_{k-1}),$$

ami éppen $(-1)^{s(\sigma)(t+1)} g(C)$-vel egyenlő, mivel $s(\tau) + s(\alpha) = s(\sigma) + s(\theta)$. Ezzel beláttuk a bizonyítandó állítást. □

4.4. Ívhez tartozó egyenletrendszer

Legyen $\mathcal{A}$ továbbra is egy $\mathrm{PG}(k-1, q)$-beli $q+k-1-t \geq k+t$ méretű ív (a pontjait valahogyan sorba is rendezzük). Legyen $E \subset \mathcal{A}$ egy $k+t$ méretű részhalmaza $\mathcal{A}$-nak. Az $\mathcal{A}$ $k-1$ elemű rendezett részhalmazain értelmezzük g függvényt a fentiek szerint. Vezessük be a

$$\det(u, C)$$

jelölést annak a mátrixnak a determinánsára, aminek első sora u pont koordinátáiból áll, a többi sora pedig C pontjainak a koordinátáiból. Vegyük észre, hogy ha $u \notin C$, de $u \in \mathcal{A}$, akkor $\det(u, C) \neq 0$, hiszen lineárisan független vektorok alkotják a sorait, tehát a későbbiekben vehetjük $\det(u, C)$ inverzét minden további nélkül.

5. Lemma. *Bármely $k-2$ elemű S részhalmazára E-nek fennáll a következő:*

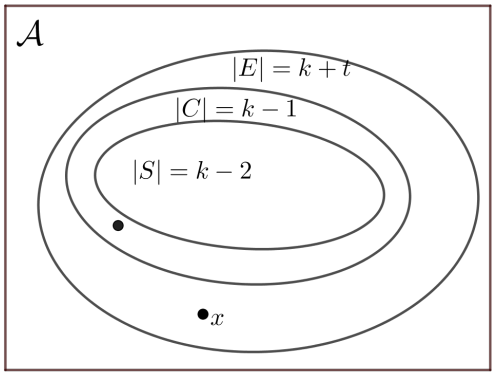
$$\sum_C g(C) \prod_{u \in E \setminus C} \det(u, C)^{-1} = 0,$$

ahol az olyan $k-1$ elemű C részhalmazaira összegzünk E-nek, amik S-et tartalmazzák.

Bizonyítás. Legyen S egy $k-2$ elemű részhalmaza E-nek. Mivel a belső szorzat $t+1$ darab determinánsból tevődik össze, ezért adott C-nek minden σ permutációja az előjelet $(-1)^{s(\sigma)(t+1)}$-re változtatja, és a 4 lemma miatt $g(C^\sigma)$-t $(-1)^{s(\sigma)(t+1)} g(C)$-ként felírva az előjelek kiejtik egymást, ezért az összeg nem függ a C halmazok rendezettségétől, így elegendő abban az esetben bebizonyítanunk az állítást, amikor a $C \subset E$ részhalmazok úgy vannak rendezve, hogy az első $k-2$ elemük S-beli, S-en belül pedig az $\mathcal{A}$-beli rendezést tekinthetjük.
Legyen B egy k elemű részhalmaza $\mathcal{A}$-nak, ami tartalmazza S-t. Ekkor a B bázisban felírt $f_S(X)$ polinom egy homogén kétváltozós t-edfokú polinom.
Legyen x egy rögzített eleme $E \setminus S$-nek. Ekkor a

$$\sum_{e \in E \setminus (S \cup \{x\})} f_S(e) \prod_{u \in E \setminus (S \cup \{x,e\})} \frac{\det(X, u, S)}{\det(e, u, S)}$$

polinom éppen $f_S(e')$ értékét adja meg minden $e' \in E \setminus (S \cup \{x\})$-re. Mivel mind az előbbi, mind $f_S(X)$ homogén t-edfokú kétváltozós polinomok (vegyük észre, hogy $\det(X, u, S)$ is csak ugyanazoktól az X_i és X_j változóktól függ, mint $f_S(X)$) és $t+1$ különböző pontban megegyezik az értékük, ezért ugyanazok.



1. ábra.

Írjuk fel a polinom értékét $X = x$-ben:

$$f_S(x) = \sum_{e \in E \setminus (S \cup \{x\})} f_S(e) \prod_{u \in E \setminus (S \cup \{x,e\})} \frac{\det(x, u, S)}{\det(e, u, S)}.$$

Osszunk le ezzel:

$$\prod_{u \in E \setminus (S \cup \{x\})} \det(x, u, S).$$

A kapott kifejezés:

$$f_S(x) \prod_{u \in E \setminus (S \cup \{x\})} \det(x, u, S)^{-1} = \sum_{e \in E \setminus (S \cup \{x\})} f_S(e) \cdot \det(x, e, S)^{-1} \prod_{u \in E \setminus (S \cup \{x,e\})} \det(e, u, S)^{-1}.$$

Itt $\det(x, e, S)^{-1} = -\det(e, x, S)^{-1}$, ami bevihető a jobb oldalon lévő szorzatba:

$$f_S(x) \prod_{u \in E \setminus (S \cup \{x\})} \det(x, u, S)^{-1} = -\sum_{e \in E \setminus (S \cup \{x\})} f_S(e) \prod_{u \in E \setminus (S \cup \{e\})} \det(e, u, S)^{-1},$$

amit egy oldalra rendezve a

$$\sum_{e \in E \setminus S} f_S(e) \prod_{u \in E \setminus (S \cup \{e\})} \det(u, S, e)^{-1} = 0$$

kifejezést kapjuk, amiből következik az állítás g definíciója miatt, hiszen a fentebb leírt sorrendek miatt így $g(C) = f_S(e)$, és az összegzés is pont az S-et tartalmazó E-beli $C = S \cup \{e\}$ halmazokra megy. □

Ha $k \leq p$, akkor az előző lemmában lévő egyenletrendszer jól jön a maximális méretű ívek meghatározásához.

6. Lemma. *Legyen E egy $k+t$ elemű részhalmaza $\mathcal{A}$-nak és Δ az E-nek egy $t+2$ elemű részhalmaza. Ha $k \leq p$, akkor*

$$\sum_C g(C) \prod_{u \in E \setminus C} \det(u, C)^{-1} = 0,$$

ahol az összeg azokon a $k-1$ elemű részhalmazain fut E-nek, amik Δ részhalmazai.

Bizonyítás. Használjuk ki, hogy 5 lemma miatt minden $k-2$ elemű $S \subset \mathcal{A}$-ra fennáll, hogy

$$\operatorname{eqn}(S) := \sum_C g(C) \prod_{u \in E \setminus C} \det(u, C)^{-1} = 0, \tag{11}$$

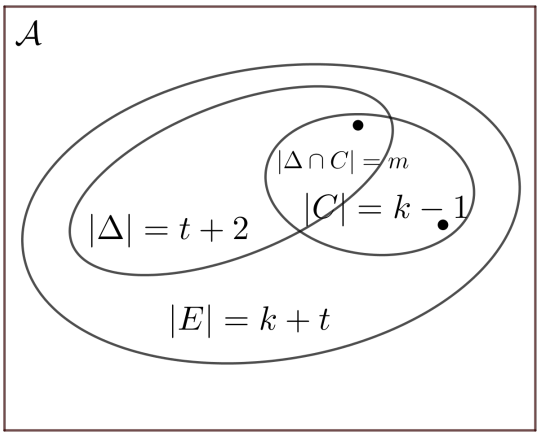
ahol az összeg E-nek az S-et tartalmazó $k-1$ elemű részhalmazain fut végig. Minden egyes S-re vezessük be

$$\lambda_S = (-1)^{m^*}(k - m^* - 2)! m^*!$$

kifejezést, ahol $m^* = |S \cap \Delta|$. Tekintsük a

$$\sum_S \lambda_S \operatorname{eqn}(S) \tag{12}$$

összeget, ahol S végigfut az E $k-2$ elemű részhalmazain.



2. ábra.

A 12 kifejezés kibontva:

$$\sum_{S \subset E} \lambda_S \operatorname{eqn}(S) = \sum_S \lambda_S \sum_{C(S \subset C)} g(C) \prod_{u \in E \setminus C} \det(u, C)^{-1} = \sum_C g(C) \prod_{u \in E \setminus C} \det(u, C)^{-1} \sum_{S \subset C} \lambda_S.$$

Legyen C egy $k-1$ elemű részhalmaza E-nek úgy, hogy $|C \cap \Delta| = m$.
Ha $C \not\subseteq \Delta$, akkor a

$$g(C) \prod_{u \in E \setminus C} \det(u, C)^{-1}$$

kifejezés az alábbi együtthatóval jelenik meg a 12 kifejezésben:

$$(k-1-m)(-1)^m(k-m-2)!m! + m(-1)^{m-1}(k-m-1)!(m-1)! = 0,$$

ahol az első tag azokhoz az S halmazokhoz tartozó λ_S számokból áll, amikre $|S \cap \Delta| = m$ (adott C-hez $k-1-m$ darab ilyen S van, hiszen $|(E \setminus \Delta) \cap C| = k-1-m$, ennyi féle képpen lehet elhagyni egy pontot C-ből, hogy megfelelő $k-2$ elemű S halmazt kapjunk, vagyis melyre $|S \cap \Delta| = m$), illetve a második tag azokhoz az S halmazokhoz tartozó λ_S számokból jön össze, ahol $|S \cap \Delta| = m-1$, mert ilyen S-ből adott C-hez m darab van (hiszen itt a $\Delta \cap C$-ből kell elhagynunk egy pontot, hogy megfelelő S-et kapjunk, amiből m darab van). Ehhez a leszámláláshoz persze kellett, hogy $m \neq k-1$.

Ha $C \subseteq \Delta$, akkor a

$$g(C) \prod_{u \in E \setminus C} \det(u, C)^{-1}$$

tag együtthatója:

$$(k-1)(-1)^{k-2}(k-k+2-2)!(k-2)! = (-1)^{k-2}(k-1)!.$$

Mivel $k \leq p$, ezért $(-1)^{k-2}(k-1)! \neq 0$, így 12 kifejezésben csak azon C részhalmazokhoz tartozó tagok együtthatója nem 0, ahol $C \subseteq \Delta$, ezért, mivel $\sum_S \lambda_S \operatorname{eqn}(S) = 0$,

$$\sum_S \lambda_S \operatorname{eqn}(S) = (-1)^{k-2}(k-1)! \sum_{C \subseteq \Delta} g(C) \prod_{u \in E \setminus C} \det(u, C)^{-1} = 0,$$

amiből már következik az állítás. □

4.5. A $4 \leq k \leq p$ esete

Az előző részekben szereplő eredmények felhasználásával már be tudjuk bizonyítani az MDS-sejtést bizonyos prímhatvány elemű testek fölött.

6. Tétel. *Ha $4 \leq k \leq p$, akkor egy $\mathrm{PG}(k-1,q)$-beli ív legfeljebb $q+1$ pontból áll.*

Bizonyítás. Indirekt módon tegyük fel, hogy létezik olyan $\mathcal{A} \subset \mathrm{PG}(k-1,q)$ ív, ami $q+2$ pontból áll, azaz a korábbiak szerint $q+2 = q+k-1-t$, ami egyszerűbben írva $t = k-3$. A 4, dualitásra vonatkozó állítás miatt ha van $\mathrm{PG}(k-1,q)$-ban $q+2$ méretű ív, akkor $\mathrm{PG}(q+2-k-1,q)$-ban is van, ezért feltehető, hogy $k \leq \frac{1}{2}q+1$, azaz $k+t = 2k-3 \leq q-1$. Legyen E egy $k+t = 2k-3$ elemű részhalmaza $\mathcal{A}$-nak és Δ egy $t+2 = k-1$ elemű részhalmaza E-nek. Ekkor a 6 lemma miatt

$$g(\Delta) \prod_{u \in E \setminus \Delta} \det(u, \Delta)^{-1} = 0,$$

hiszen Δ $k-1$ elemű részhalmazaiból csak egy van, maga Δ, hiszen $|\Delta| = k-1$.
De ez ellentmondás, mert definíció szerint $g(\Delta) \neq 0$, ahogyan $\det(u, \Delta)$ sem lehet 0 egyik $u \in \mathcal{A} \setminus \Delta$-ra sem. □

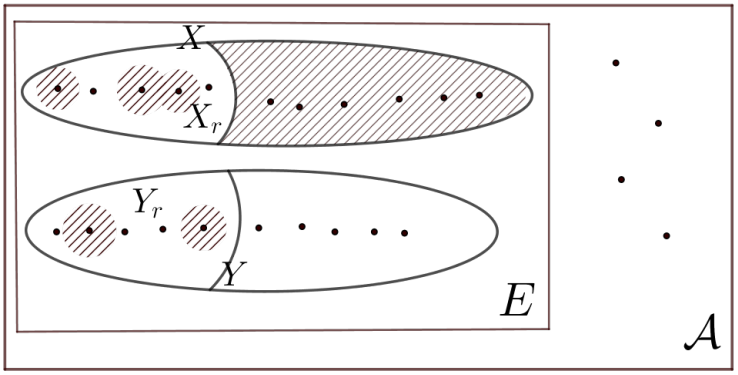
4.6. A $k \leq 2p-2$ esete

Ebben a részben megnézünk egy az előzőhöz hasonló, az ott elért eredményeket is felhasználó bizonyítást szintén Simeon Ball, és Michael Lawrauw [3] cikke alapján.

Tegyük fel, hogy $\mathcal{A}$ egy $q+2$ méretű ív $\mathrm{PG}(k-1,q)$-ban és $k \geq p$ (az ellenkező esetet már fentebb beláttuk), $g(C)$-t definiáljuk úgy, mint fentebb, (9)-ben.
Legyenek $X = \{x_1, \ldots, x_{k-1}\}$ és $Y = \{y_1, \ldots, y_{k-2}\}$ diszjunkt részhalmazai $\mathcal{A}$-nak és legyen $E = X \cup Y$. Vegyük észre, hogy E ebben az esetben mindig létezik, hiszen a feltétel miatt $|X| + |Y| = 2k - 3 \leq 4p - 7$, ami mivel q nem prím, kisebb, mint $q+2$. Megjegyezzük, hogy itt X egy ponthalmaz, nem pedig vektorváltozó úgy, mint eddig.
Legyen r egy nemnegatív egész úgy, hogy $0 \leq r \leq k-p$ és legyen $X_r = \{x_1, \ldots, x_r\}$ és $Y_r = \{y_1, \ldots y_r\}$.
Továbbá minden $T \subseteq \{1, 2, \ldots, r\}$ halmazra legyen $X_T = \{x_j : j \in T\}$ és $Y_T = \{y_j : j \in T\}$.
Ezek alapján az E halmaz $k-1$ elemű $C_{r,T}$ részhalmazát a következőképpen definiáljuk:

$$C_{r,T} = (X \setminus X_r) \cup X_T \cup (Y_r \setminus Y_T)$$

(a szemléltető ábrán $C_{r,T}$-t a csíkozott részek jelölik). Megjegyezzük, hogy ily módon $C_{0,\emptyset} = X$ is értelmezhető.



3. ábra.

7. Lemma. *Legyen $\mathcal{A} \subseteq \mathrm{PG}(k-1,q)$, $|\mathcal{A}| = q+2$ és tegyük fel, hogy $k \geq p$. Legyen $E = X \cup Y \subseteq \mathcal{A}$, $|E| = 2k-3$. Ekkor*

$$\sum_{T \subseteq \{1,\ldots,k-p\}} (-1)^{|T|} g(C_{k-p,T}) \prod_{u \in E \setminus C_{k-p,T}} \det(u, C_{k-p,T})^{-1} = 0.$$

Bizonyítás. Legyen $S \subset E$, $|S| = k-2$ és rögzítsük $r = k-p$-t.
Ha $S \cap (X_r \cup Y_r) = X_T \cup (Y_r \setminus Y_T)$ valamely $T \subseteq \{1, 2, \ldots, r\}$-re, akkor legyen

$$\lambda_S = m!(p-2-m)!(-1)^{m+|T|},$$

ahol $m = |S \cap (X \setminus X_r)|$, különben pedig legyen 0.
Továbbra is a (11) kifejezés alapján

$$\mathrm{eqn}(S) = \sum_C g(C) \prod_{u \in E \setminus C} \det(u, C)^{-1} = 0, \tag{13}$$

ahol $S \subseteq C \subseteq E$ és $|C| = k-1$.
Legyen α_C a $g(C)\prod_{u\in E\setminus C}\det(u,C)^{-1}$ tag együtthatója a

$$\sum_{S\subset E}\lambda_S \mathrm{eqn}(S)$$

összegben. Ekkor nyilván $\alpha_C = 0$, ha $|C\cap(X_r\cup Y_r)| \notin \{r, r+1\}$ (mert akkor minden $S\subset C$-hez $\lambda_S = 0$).
Ha $|C\cap(X_r\cup Y_r)| = r+1$, akkor létezik $i\in\{1,\dots,r\}$, amire $x_i, y_i \in C$. Ha i nem az egyetlen ilyen index, akkor $\lambda_S = 0$ C minden $k-2$ elemű részhalmazára (nem teljesül, hogy $S\cap(X_r\cup Y_r) = X_T\cup(Y_r\setminus Y_T)$), így ekkor $\alpha_C = 0$. Ha pedig i az egyetlen, akkor $\alpha_C = \lambda_{C\setminus\{x_i\}} + \lambda_{C\setminus\{y_i\}} = 0$ (hiszen itt a két tag csak a (-1) kitevőjében tér el eggyel).
Ha $|C\cap(X_r\cup Y_r)| = r$ és $C\cap(X_r\cup Y_r) \neq X_T\cup(Y_r\setminus Y_T)$ minden $T\subseteq\{1,\dots,r\}$-re, akkor $\alpha_C = 0$.
Ha $|C\cap(X_r\cup Y_r)| = r$ és $C\cap(X_r\cup Y_r) = X_T\cup(Y_r\setminus Y_T)$ valamely $T\subseteq\{1,\dots,r\}$-re és $C\setminus(X_r\cup Y_r) \neq X\setminus X_r$, akkor

$$\alpha_C = (-1)^{|T|}(m(m-1)!(p-1-m)!(-1)^{m-1} + (p-1-m)m!(p-2-m)!(-1)^m) = 0,$$

ahol $m = |C\cap(X\setminus X_r)|$.
A többi esetben pedig $C = C_{r,T}$ alakú valamely $T\subseteq\{1,\dots,r\}$-re és

$$\alpha_C = (-1)^{|T|}(k-1-r)(p-2)! = (-1)^{|T|}(p-1)!,$$

mert $k-1-r$ darab $S\subset C$ esetén nem 0 λ_S és mindegyik esetben $|S\cap(X\setminus X_r)| = m = k-1-r-1 = p-2$. Tehát $\alpha_C \neq 0$, így $(p-1)!$-al leoszthatunk és akkor azt kapjuk, hogy az állításban szereplő kifejezés 0. □

8. Lemma. *Legyen C egy $k-1$ elemű részhalmaza $\mathcal{A}$-nak. Tegyük fel, hogy W és Δ diszjunkt részhalmazai $\mathcal{A}$-nak úgy, hogy $|W| = k-|\Delta|$ és $\Delta\subseteq C$. Ekkor minden $u\in\mathrm{PG}(k-1,q)$-ra*

$$\sum_{w\in W}\frac{\det(u, W\setminus\{w\},\Delta)}{\det(w, W\setminus\{w\},\Delta)}\det(w,C) = \det(u,C).$$

Bizonyítás. A bal és a jobb oldal nyilván megegyezik minden $u\in\Delta\cup W$-re, és tekinthetjük a két oldalt úgy, mint egy $u = (u_1,u_2,\dots,u_k)$-ban k ismeretlenes homogén elsőfokú polinom. Így mivel $|\Delta\cup W| = k$, ezért k helyen megegyeznek, azaz a két polinomnak ugyanannak kell lennie. □

7. Tétel. *Ha q nem prím és $4\le k\le 2p-2$, akkor egy $\mathrm{PG}(k-1,q)$-beli ívnek legfeljebb $q+1$ pontja van.*

Bizonyítás. Legyen $\mathcal{A}$ egy $q+2$ méretű ív $\mathrm{PG}(k-1,q)$-ban. A 6 tétel miatt feltehetjük, hogy $k\ge p$. Legyen r egy olyan nemnegatív egész, hogy $r\le k-p$. Tekintsük $g(C)$-t (9) szerint és vegyük X, Y, E, X_r, Y_r, X_T, Y_T és $C_{r,T}$ halmazokat úgy, mint fentebb.

Azt fogjuk belátni, hogy

$$\sum_{T\subseteq\{1,\dots,r\}} (-1)^{|T|} g(C_{r,T}) \prod_{u\in E\setminus C_{r,T}} \det(u, C_{r,T})^{-1} = 0$$

kifejezésből következik, hogy

$$\sum_{T\subseteq\{1,\dots,r-1\}} (-1)^{|T|} g(C_{r-1,T}) \prod_{u\in E\setminus C_{r-1,T}} \det(u, C_{r-1,T})^{-1} = 0.$$

Ezt iterálva kijön, hogy

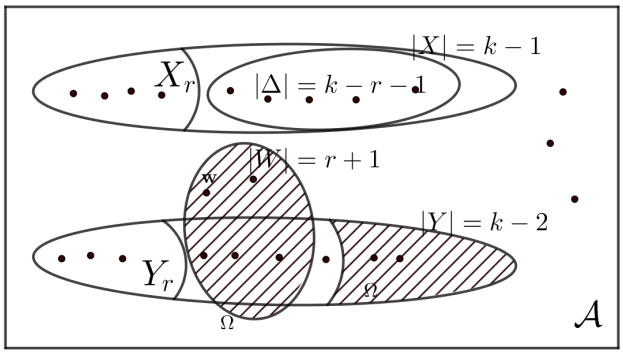
$$g(X) \prod_{u\in Y} \det(u, X)^{-1} = 0,$$

ami ellentmondás, hiszen $g(X)$ a definíciója miatt nem lehet 0, illetve nyilván $\det(u, X)^{-1}$ sem. A 7 lemmából tudjuk, hogy ez igaz $r = k - p$-re, úgyhogy elegendő csak az indukciós lépést belátnunk.

Legyen W és Δ két diszjunkt részhalmaza $\mathcal{A}$-nak úgy, hogy
$W \subseteq \mathcal{A} \setminus \{x_1, \dots, x_{k-1}, y_1, \dots y_r, y_{2r+1}, \dots, y_{k-2}\}$ és $\Delta = X \setminus X_r$ és rendre $r+1$ és $k-r-1$ eleműek.

Ilyen W és Δ diszjunkt halmazok persze léteznek, hiszen
$|\mathcal{A} \setminus \{x_1, \dots, x_{k-1}, y_1, \dots y_r, y_{2r+1}, \dots, y_{k-2}\}| = q + 2 - (k-1) - (k-2-r) \geq r+1$, átrendezve $q + 4 \geq 2k$, ami igaz hiszen $q \geq p^2$ és $k \leq 2p-2$.

Legyen $\Omega = W \cup \{y_{2r+1}, \dots, y_{k-2}\}$. Megjegyzendő, hogy $k-2 \geq 2r$, mert $r \leq k-p$ és $k \leq 2p-2$. Így $|\Omega| = k-1-r$ (a szemléltető ábrán Ω a satírozott részekből áll össze).



4. ábra.

Legyen $w \in W$, az indukciós lépésben írjunk be $\{y_{r+1}, \dots y_{2r}\}$ helyett $W \setminus \{w\}$-t. Ez megtehető, hiszen az így keletkezett $X' = X$ és $Y' = Y \setminus \{y_{r+1} \dots y_{2r}\} \cup (W \setminus \{w\})$ diszjunktak lesznek. Azt kapjuk, hogy

$$\sum_{T\subseteq\{1,\dots,r\}} (-1)^{|T|} g(C_{r,T}) \prod_{u\in(X\cup Y_r\cup\Omega)\setminus C_{r,T}} \det(u, C_{r,T})^{-1} \det(w, C_{r,T}) = 0,$$

ahol a $\det(w, C_{r,T})$-vel való beszorzás azért kell, mert a produktum $u \in (X \cup Y_r \cup \Omega) \setminus C_{r,T}$ pontokon fut végig, amiben benne van w is, de az indukciós feltétel miatt nem lenne. Ezt

beszorozva $\frac{\det(y_r,W\setminus w,\Delta)}{\det(w,W\setminus w,\Delta)}$-val:

$$\sum_{T\subseteq\{1,\dots,r\}}(-1)^{|T|}g(C_{r,T})\prod_{u\in(X\cup Y_r\cup\Omega)\setminus C_{r,T}}\det(u,C_{r,T})^{-1}\frac{\det(y_r,W\setminus w,\Delta)}{\det(w,W\setminus w,\Delta)}\det(w,C_{r,T})=0.$$

Ezt összegezzük $\forall w\in W$-re. A 8 lemma alapján (aminek a feltételei teljesülnek, hiszen W és Δ diszjunktak és együtt k pontot tartalmaznak, illetve $\Delta\subseteq C_{r,T}\ \forall T\subseteq\{1,\dots,r\}$-re) kijön, hogy

$$\sum_{T\subseteq\{1,\dots,r\}}(-1)^{|T|}g(C_{r,T})\prod_{u\in(X\cup Y_r\cup\Omega)\setminus C_{r,T}}\det(u,C_{r,T})^{-1}\det(y_r,C_{r,T})=0.$$

Mivel $\det(y_r,C_{r,T})=0$ ha $r\notin T$, ha pedig $r\in T$, akkor $C_{r-1,T}=C_{r,T}$, ezért

$$\sum_{T\subseteq\{1,\dots,r-1\}}(-1)^{|T|}g(C_{r-1,T})\prod_{u\in(X\cup Y_{r-1}\cup\Omega)\setminus C_{r-1,T}}\det(u,C_{r-1,T})^{-1}=0.$$

Tehát ez az egyenlet már nem függ y_r-től, és minden a fentiek szerint definiált halmazra igaz is. Ezért legyen $Y^*=Y\setminus\{y_r\}\cup\{z\}$, ahol $z\in\mathcal{A}\setminus(X\cup Y\cup W)$. Így Ω választható $\Omega=\{y_r,\dots y_{k-2}\}$ halmaznak is, amiből pont az jön ki, hogy

$$\sum_{T\subseteq\{1,\dots,r\}}(-1)^{|T|}g(C_{r,T})\prod_{u\in E\setminus C_{r,T}}\det(u,C_{r,T})^{-1}=0$$

kifejezésből következik, hogy

$$\sum_{T\subseteq\{1,\dots,r-1\}}(-1)^{|T|}g(C_{r-1,T})\prod_{u\in E\setminus C_{r-1,T}}\det(u,C_{r-1,T})^{-1}=0.$$

Innen pedig már fentebb megmutattuk, hogy hogyan jön ki az ellentmondás. Ezzel tehát $p<k\leq 2p-2$ esetén is beláttuk, hogy a $\mathrm{PG}(k-1,q)$-ban az ívek legfeljebb $q+1$ pontból állhatnak. □

5. Konstrukciók

Azt, hogy az MDS-sejtésben megfogalmazott felső korlátok éles felső becslést is adnak, számos példa igazolja. Ebben a fejezetben megpróbáljuk összeszedni a maximális ívekre adható különböző konstrukciókat a teljesség igénye nélkül.

Két $\mathrm{PG}(k-1,q)$-beli ívet, $\mathcal{A}$-t és $\mathcal{A}'$-t (projektíven) ekvivalensnek tekintünk, ha létezik egy olyan ϕ projektivitása $\mathrm{PG}(k-1,q)$-nak, amelyre $\mathcal{A}' = \mathcal{A}^\phi$. Projektivitás alatt olyan $\phi : \mathrm{PG}(k-1,q) \to \mathrm{PG}(k-1,q)$ bijekciót értünk, ami egy $A \in \mathrm{PGL}(k,q)$ mátrixszal adható meg úgy, hogy minden $P = \langle x \rangle$ pont képe $P^\phi = \langle Ax \rangle$, ahol $\langle x \rangle$ jelöli a P pontot meghatározó x vektor által meghatározott alteret.
Vegyük észre, hogy az ily módon definiált ekvivalenciával a $\mathrm{PG}(k-1,q)$-beli n pontú ívek ekvivalenciaosztályai és az $[n,k]_q$ lineáris MDS kódok ekvivalenciaosztályai között egy kölcsönösen egyértelmű megfeleltetést kapunk. Ehhez a korábbiak miatt már csak azt kell látnunk, hogy ugyan egy adott $C = [n,k]_q$ lineáris kódhoz több generátormátrix is tartozhat, mindegyik ugyanannak az $U \leq \mathbb{F}_q^n$, k dimenziós altérnek a bázisa, de ezek a bázisok alkalmasan megválasztott $A \in \mathrm{GL}(k,q)$ lineáris transzformációval egymásba vihetőek. Ezen kívül A-ra tekinthetünk úgy is, mint egy, a $\mathrm{PG}(k-1,q)$ pontjain ható projektivitás mátrixára, ami pont úgy hat a generátormátrix oszlopvektorai által meghatározott íven, hogy egy azzal ekvivalens ívet reprezentáló vektorokba viszi át azt (persze amikor a mátrixok éppen egymás skalárszorosai, akkor pont ugyanazokat az íveket kapjuk).

5.1. A projektív sík ívei

Az 5 tétel miatt már tudjuk, hogy a véges projektív sík ívei legfeljebb $q+1$ illetve $q+2$ pontból állnak. Ennél a résznél célunk a síkbeli ívek karakterizálása lesz. Az itt szereplő definíciók és állítások jó része megtalálható az [1] könyvben is.

12. Definíció (Ovális, hiperovális). *A $q+1$, illetve $q+2$ méretű síkbeli íveket oválisnak illetve hiperoválisnak nevezzük.*

Az 1 lemmát felhasználva jól látszik, hogy ez a két definíció ekvivalens azzal, hogy az az ívnek minden pontja pontosan egy, illetve nulla darab érintőre illeszkedik. Ezzel a két tulajdonsággal viszont akár tetszőleges pontokból és egyenesekből álló rendszeren lehet ovális okat, illetve hiperoválisokat definiálni.

Írjuk fel a 4.2 alfejezetben használt fogalmakat egy $\mathcal{A} \subset \mathrm{PG}(2,q)$ maximális méretű ívre. Először ha q páratlan:

$|\mathcal{A}| = q+1$, $\qquad k = 3$,
$S \subset \mathcal{A}$, $|S| = 1$ egy pontja az ívnek, $\qquad t = q + k - |\mathcal{A}| - 1 = 1$,
$f_x(X)$: az x ponton áthaladó érintő egyenlete.

Írjuk fel a 6 lemmát erre az esetre:

3. Következmény. *Tetszőleges $x, u, v, w, \in \mathcal{A}$ pontokra fennáll, hogy*

$$f_x(w)\det(u,v,x) + f_x(v)\det(w,u,x) + f_x(u)\det(v,w,x) = 0.$$

Bizonyítás. Vegyük észre, hogy az állítás pontosan a 6 lemmában szereplő egyenlőség mindkét oldalról beszorozva $\det(u,v,x)\det(w,u,x)\det(v,w,x)$-szel pont a fenti kifejezést kapjuk (hiszen itt $E = \{x,u,v,w\}$, ha $S = x, \quad C \in \{\{u,x\},\{v,x\},\{w,x\}\}$). □

8. Tétel (Segre, 1955.). *Ha q páratlan, akkor az $\mathcal{A}$ $q+1$ méretű ív egy nem elfajuló kúpszelet, amelynek egyenlete az u, v, w bázisban:*

$$2X_1X_2f_u(v) + 2X_1X_3f_w(u) + 2X_2X_3f_v(w) = 0.$$

Bizonyítás.[6] Alkalmazzuk az előbbi, 3 következményt minden $x = (x_1, x_2, x_3) \in \mathcal{A}$ pontra és u, v, w bázisra. Vegyük észre, hogy $\det(u,v,x) = x_3$, $\det(w,u,x) = x_2$ és $\det(v,w,x) = x_1$:

$$f_x(w)x_3 + f_x(v)x_2 + f_x(u)x_1 = 0.$$

Kihasználva, hogy a 3 lemma síkbeli változata szerint

$$f_x(y) = f_y(x) \quad \forall x, y \in \mathcal{A}, \tag{14}$$

és f lineáris, ezért az egyenletet átalakíthatjuk így:

$$(f_w(u)x_1 + f_w(v)x_2 + f_w(w)x_3)x_3 + (f_v(u)x_1 + f_v(v)x_2 + f_v(w)x_3)x_2 +$$

$$+(f_u(u)x_1 + f_u(v)x_2 + f_u(w)x_3)x_1 = 0.$$

Mivel tetszőleges $y \in \mathcal{A}$-ra $f_y(y) = 0$, ezért leegyszerűsíthetünk:

$$(f_w(u)x_1 + f_w(v)x_2)x_3 + (f_v(u)x_1 + f_v(w)x_3)x_2 + (f_u(v)x_2 + f_u(w)x_3)x_1 = 0.$$

Átrendezve és a (14) egyenletet használva megkapjuk, hogy minden $x \in \mathcal{A}$-ra:

$$2(x_1x_2f_u(v) + x_1x_3f_w(u) + x_2x_3f_v(w)) = 0,$$

ahol $f_u(v)$, $f_w(u)$ és $f_v(w)$ nem nullák, mert nem az érintőn lévő pontok, ezért $\mathcal{A}$ pontjai valóban ennek a nem elfajuló kúpszeletnek a pontjain vannak rajta (és mivel egy $\mathbb{F}_q$ feletti síkon egy nem elfajuló kúpszeletnek pontosan $q+1$ pontja van, ezért maga $\mathcal{A}$ ív a kúpszelet). □

Ha viszont q páros, akkor nem ennyire egyszerű a $q+2$ méretű ívek karakterizálása. Több, projektíven nem ekvivalens példa ismert. A következő tétel ezeknek egy közös tulajdonságát mutatja meg.

9. Tétel. *Legyen $\mathcal{H}$ egy olyan hiperovális, amely tartalmazza a $(0,0,1), (0,1,0), (1,0,0)$ és $(1,1,1)$ pontokat. Ekkor van olyan f polinom, amelyre*

$$\mathcal{H} = \{(1,t,f(t)) : t \in \mathbb{F}_q\} \cup \{(0,1,0),(0,0,1)\},$$

és az f polinom $\mathbb{F}_q$ olyan permutációja, amelyre $f(0) = 0$ és $f(1) = 1$.

Bizonyítás.[1] Legyen a vektorok első koordinátája az ideális egyenesre vonatkozó koordináta (akkor 0, ha a pont rajta van az ideális egyenesen). Mivel $\mathcal{H}$ tartalmazza a $(0,0,1)$ pontot, ami a függőleges egyenesek ideális pontja, ezért az affin síkban minden függőleges egyenesen pontosan egy $\mathcal{H}$-beli pont lesz még, így $\mathcal{H}$ affin része egy f függvény grafikonja. Mivel a vízszintes egyenesek ideális pontja is $\mathcal{H}$-ban van, ezért minden vízszintes egyenes is egy pontban metszi $\mathcal{H}$ affin részét, így f valóban egy permutációja $\mathbb{F}_q$ pontjainak. Az $f(0) = 0$ és $f(1) = 1$ abból következik, hogy $(0,0,1)$ és $(1,1,1)$ $\mathcal{H}$-beli. □

13. Definíció. *[1] Az f polinomot permutációs polinomnak nevezzük, ha $\mathbb{F}_q$-n egy permutációt hoz létre. Az f polinomot o-polinomnak hívjuk, ha az általa definiált $\{(1,t,f(t)) : t \in \mathbb{F}_q\} \cup \{(0,1,0),(0,0,1)\}$ ponthalmaz egy hiperoválist.*

A hiperoválisok listája jelenleg $q = 8$, 16, 32 és 64-re teljes.[23]
Ezek közül vizsgáljunk meg néhányat a teljesség igénye nélkül. További konstrukciók találhatóak a [3] forrásban.

Mielőtt megnéznénk az első példát, lássuk be az alábbi egyszerű számelméleti lemmát, ami még hasznos lesz a későbbiekben.

9. Lemma. *Legyenek $e, a \in \mathbb{N}$ számok úgy, hogy $(e,a) = 1$. Ekkor $(2^e - 1, 2^a - 1) = 1$, ahol (x,y) jelöli az x és y természetes számok legnagyobb közös osztóját.*

Bizonyítás.[5] Indirekt módon tegyük fel, hogy egy p prím osztója $2^e - 1$-nek és $2^a - 1$-nek is. Legyen $r \in \mathbb{N}$ a legkisebb olyan szám, amire $p \mid 2^r - 1$. Mivel $2^e - 1 = 2^{e-r}(2^r - 1) + (2^{e-r} - 1)$, ezért $p \mid 2^{e-mr} - 1$ $\forall m \in \mathbb{N}$-re, ahol $m \leq \frac{e}{r}$. Ekkor r minimalitása miatt $\exists m \in \mathbb{N}$, hogy $e = mr$, úgyhogy $r \mid e$. Hasonlóan belátható, hogy $r \mid a$. Mivel $(e,a) = 1$, ezért p-nek 1-nek kellene lennie, ami ellentmondás. □

3. Példa. *Az alábbi $S \subseteq \mathrm{PG}(2,q)$ ponthalmaz egy ívet alkot:*

$$S = \{(1,t,t^{2^r}) : t \in \mathbb{F}_q\} \cup \{(0,0,1),(0,1,0)\},$$

ahol $q = 2^h$, $(r,h) = 1$.

Bizonyítás. [17] Azt kell belátnunk, hogy S bármely 3 különböző eleme lineárisan független, vagyis az általuk meghatározott mátrix determinánsa nem 0.
Legyen $2^r = \sigma$.

- 1. eset: Ha mindhárom S-beli pontot reprezentáló vektor $(1,t,t^\sigma)$ alakú, legyenek ezek $(1,a,a^\sigma),(1,b,b^\sigma)$ és $(1,c,c^\sigma)$. Írjuk be ezeket egy mátrixba, és számoljuk ki annak a determinánsát, felhasználva a determináns elemi tulajdonságait, vagyis, hogy sorokat és oszlopokat kivonva az értéke nem változik, utána fejtsük ki.

$$\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^\sigma & b^\sigma & c^\sigma \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ 0 & b-a & c-a \\ 0 & b^\sigma - a^\sigma & c^\sigma - a^\sigma \end{vmatrix} = (b-a)(c^\sigma - a^\sigma) - (b^\sigma - a^\sigma)(c-a) =$$

$$= (b-a)(c-a)^\sigma - (b-a)^\sigma(c-a),$$

felhasználtuk, hogy $\mathbb{F}_q$ fölött a 2^r-edik hatványra emelés tagonként végezhető. Indirekt módon tegyük fel, hogy ez a determináns 0 és oldjuk meg a keletkezett egyenletet. Mivel három különböző vektort vettünk, ezért $s := (b-a) \neq 0$ és $t := (c-a) \neq 0$. Ezeket az új változókat behelyettesítve a $ts^\sigma - st^\sigma = 0$ egyenletet kapjuk. Ezt megoldva:

$$ts^\sigma = st^\sigma, \tag{15}$$

$$ts(s^{\sigma-1} - t^{\sigma-1}) = 0.$$

$ts \neq 0$ hiszen egyik tényező sem lehet 0, ezért $(s^{\sigma-1} - t^{\sigma-1}) = 0$, azaz $s^{\sigma-1} = t^{\sigma-1}$, amit leoszthatunk t-vel, azt kapjuk, hogy

$$\left(\frac{s}{t}\right)^{\sigma-1} = 1,$$

ami csak akkor lehetséges, ha $\alpha := \frac{s}{t}$ rendje osztója $\sigma - 1 = 2^r - 1$-nek. De az alaptestünk miatt $\alpha^{2^h-1} = 1$, vagyis rendje osztója $q - 1 = 2^h - 1$-nek is, ezért a 9 lemma miatt α rendje osztója (r, h)-nak is, ami 1. Ez pedig csak akkor lehetséges, ha $\alpha = 1 (= -1)$, ami nem lehet, mert visszahelyettesítve azt kapnánk, hogy $s = t$, azaz $b - a = c - a$, $b = c$, ami ellentmondás, mert különböző vektorokat vettünk.

- 2.eset: Ha az egyik kiválasztott pont a $(0, 0, 1)$, a másik kettő pedig $(1, t, t^\sigma)$ alakú:

$$\begin{vmatrix} 0 & 1 & 1 \\ 0 & a & b \\ 1 & a^\sigma & b^\sigma \end{vmatrix} = b - a \neq 0,$$

  mert $a \neq b$.

- 3.eset:Ha az egyik kiválasztott pont a $(0, 1, 0)$, a másik kettő pedig $(1, t, t^\sigma)$ alakú:

$$\begin{vmatrix} 0 & 1 & 1 \\ 1 & a & b \\ 0 & a^\sigma & b^\sigma \end{vmatrix} = a^\sigma - b^\sigma = (a-b)^\sigma \neq 0.$$

- 4. eset: Ha két pont a $(0, 0, 1)$ és $(0, 1, 0)$, a harmadik pedig $(1, t, t^\sigma)$ alakú:

$$\begin{vmatrix} 0 & 0 & 1 \\ 1 & 0 & a \\ 0 & 1 & a^\sigma \end{vmatrix} = 1 \neq 0.$$

Ezzel beláttuk, hogy ez a példa valóban egy hiperoválisz. □

A következő konstrukció bizonyítása a [16] forrásban leírtak alapján készült, de először a [22] cikkben jelent meg.

4. Példa. *Az alábbi $S \subseteq \mathrm{PG}(2,q)$ ponthalmaz egy ívet alkot:*

$$S = \{(1,t,t^6) : t \in \mathbb{F}_q\} \cup \{(0,0,1),(0,1,0)\},$$

ahol $q = 2^h$ és h páratlan.

Bizonyítás. Legyen $h = 2k+1$, ahol $k \in \mathbb{N}$.
Itt is azt kellene belátnunk, hogy a halmaz semelyik 3 különböző pontja nem esik egy egyenesre, azaz a reprezentáló vektoraikból képzett mátrix determinánsa nem 0. Ugyanúgy, mint az előző példában, itt is ugyanaz a 4 eset van, amik közül a 2. és 4. ugyanazon indoklás miatt nem lehet 0. Tehát a maradék két eset:

- 1. eset: Ha mindhárom S-beli pontot reprezentáló vektor $(1,t,t^6)$ alakú, legyenek ezek $(1,a,a^6),(1,b,b^6)$ és $(1,c,c^6)$. Azt kellene belátnunk, hogy

$$\begin{vmatrix} 1 & a & a^6 \\ 1 & b & b^6 \\ 1 & c & c^6 \end{vmatrix} \neq 0.$$

  Mivel a,b,c különböző testelemek, és a testnek 2 a karakterisztikája, ezért a determinánst leoszthatjuk $(a+b)(b+c)(c+a)$-val. Ekkor egy 3 ismeretlenes homogén 4-edfokú polinomot kapunk, nevezzük el ezt $g(a,b,c)$-nek:

$$g(a,b,c) = \frac{\begin{vmatrix} 1 & a & a^6 \\ 1 & b & b^6 \\ 1 & c & c^6 \end{vmatrix}}{(a+b)(b+c)(c+a)}.$$

  Elegendő erről belátnunk, hogy sehol sem 0, ha a,b,c különbözőek. Indirekt módon tegyük fel, hogy $g(a,b,c) = 0$.

  (i) Ha c=0: $g(a,b,0) = \frac{a^5+b^5}{a+b} = a^4 + a^3b + a^2b^2 + ab^3 + b^3$. Ha $b = 0$, akkor ahhoz, hogy $g(a,0,0) = 0$ legyen, $a = 0$ kellene, ami ellentmondás. Így b-vel leoszthatunk, legyen $w = \frac{a}{b} \neq 1$, azaz $\frac{w^5+1}{w+1} = 0$, ami azt jelenti, hogy $w^5 = 1$.
  $w \in \mathbb{F}_{2^h} = \mathbb{F}_{2^{2k+1}}$, aminek a multiplikatív csoportja ciklikus és a rendje $2^{2k+1}-1$, azaz $w^{2^{2k+1}-1} = 1 \Rightarrow 5 \mid 2^{2k+1}-1 = 2\cdot 4^k - 1$, ami ellentmondás.

  (ii) Ha $c \neq 0$: $g(a,b,c)$ leoszthető c^4-nel. Ekkor kapunk egy $x := \frac{a}{c}$ és $y := \frac{b}{c}$ ismeretlenekre $g(x,y)$ polinomot. Ez a polinom pedig (kifejtve a determinánst és leosztva a megfelelő kifejezésekkel, kihasználva, hogy a karakterisztika 2):

  $$g(x,y) = y^4 + y^3(1+x) + y^2(1+x+x^2) + y(1+x+x^2+x^3) + 1 + x + x^2 + x^3 + x^4.$$

  Tekintsük az $\mathbb{F}_4 = \{0,1,\omega,\omega^2\}$ 4-elemű testet. Vegyük észre, hogy $g(x,y)$ felbomlik $\mathbb{F}_4$ fölött, úgy, hogy

$$g(x,y) = A(x,y)B(x,y),$$

ahol $A(x,y) = 1+\omega x+x^2+(\omega+\omega x)y+y^2$ és $B(x,y) = 1+\omega^2 x+x^2+(\omega^2+\omega^2 x)y+y^2$. Ekkor $A(x,y) = 0$, vagy $B(x,y) = 0$. Ha $A(x,y) = 0$ valamely $x, y \in \mathbb{F}_{2^{2k+1}}$ esetén, akkor átrendezés után két lehetőség van:

(1) $\omega(x+y+xy) = 1+x^2+y^2 = 0$, vagy

(2) leoszthatunk, azaz $\omega = \frac{1+x^2+y^2}{x+y+xy}$.

Ha ez utóbbi áll fent, akkor egyrészt a jobb oldal $\mathbb{F}_{2^{2k+1}}$-beli, másrészt a bal oldal $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$, ami ellentmondás, mert $\mathbb{F}_4 \not\leq \mathbb{F}_{2^{2k+1}}$ (azaz $\mathbb{F}_q$ nem bővítése $\mathbb{F}_4$-nek).

Ha viszont (1) áll fent, akkor $0 = 1+x^2+y^2 = (1+x+y)^2$, azaz $x+y = 1$, illetve $x+y+xy = 0 \Rightarrow xy = 1$. Ezekből $x(x+1) = 1$ adódik, vagyis $x^2+x+1 = 0$, ami $\mathbb{F}_2$ felett irreducibilis, ezért gyökei $\mathbb{F}_2$ másodfokú bővítésében vannak benne, vagyis $\mathbb{F}_4 \setminus \mathbb{F}_2$-ben, ami megint csak ellentmondás.

Ugyanezzel a gondolatmenettel belátható, hogy $B(x,y)$ sem lehet 0.

- 2. eset: Ha az egyik pont a $(0,1,0)$, a másik kettő pedig $(1,a,a^6)$ és $(1,b,b^6)$, $a \neq b$. Ekkor

$$\begin{vmatrix} 0 & 1 & 0 \\ 1 & a & a^6 \\ 1 & b & b^6 \end{vmatrix} = b^6 - a^6 = (b^3-a^3)^2,$$

ami pontosan akkor 0, ha $b^3 - a^3 = 0$. Ha $b = 0$, akkor $a = 0$, ami nem lehet, ezért b-vel leoszthatunk: $(\frac{a}{b})^3 + 1 = 0$, ami nem oldható meg $\frac{a}{b} \neq 1$-re $\mathbb{F}_{2^{2k+1}}$ fölött, hiszen különben $3 \mid 2^{2k+1} - 1 = 2 \cdot 4^k - 1$ is teljesülne, ami ellentmondás. □

5.2. Momentumgörbék

Az MDS-sejtéshez kapcsolódóan Segre 1955-ben azt a kérdést is feltette, hogy milyen k-ra és q-ra lesz az összes $q+1$ méretű ív az alább vizsgált momentumgörbékkel ekvivalens [3, 1. fejezet]. Ebben a részben a [3] forrás szerint ezeket a ponthalmazokat vizsgáljuk meg.

14. Definíció. *(Momentumgörbe) Az* $\mathcal{N}_{k-1} \subseteq \mathrm{PG}(k-1,q)$ *ponthamazt momentumgörbének nevezzük, ha projektíven ekvivalens a* $\{(1,t,t^2,\ldots,t^{k-1}) : t \in \mathbb{F}_q\} \cup \{(0,0,\ldots,1)\}$ *halmazzal.*

Érdemes megnéznünk ezekről a görbékről néhány állítást, hogy lássuk, hogy ezek a legfontosabb példák $q+1$ méretű ívekre.

7. Állítás. *Az*

$$\mathcal{N}_{k-1} = \{(1,t,t^2,\ldots,t^{k-1}) : t \in \mathbb{F}_q\} \cup \{(0,\ldots,0,1)\}$$

momentumgörbe pontjai mindig egy íven helyezkednek el.

Bizonyítás. Ahhoz, hogy $\mathcal{N}_{k-1}$ semelyik k pontja ne legyen egy hipersíkon, azt kell belátnunk, hogy bármely k darab vektorból képzett mátrix determinánsa nem 0. Vegyük észre, hogy az ilyenek mindig egy Vandermonde-determinánst határoznak meg (amikor a $(0,\ldots,0,1)$ benne

van, akkor is, mert aszerint kifejtve egy kisebb Vandermonde-determinánst kapunk). Tudjuk, hogy a Vandermonde-determináns értéke mindig

$$\prod_{j<i}(t_i - t_j),$$

ahol a vektorokban a $t_1, \ldots, t_k$ különböző testelemek hatványai szerepelnek. Ez a szorzat pedig nem lehet 0, mert nem tartalmaz a tényezői között 0-t ($\mathbb{F}_q$ nullosztómentes). □

6. Megjegyzés. *A momentumgörbe ekvivalens a 2 példában szereplő MDS kóddal.*

Bizonyítás. Vegyük észre, hogy a 2 példának egyik generátormátrixát kapjuk, ha $\mathcal{N}_{k-1}$ pontjait reprezentáló vektorokat, mint oszlopvektorok egymás mellé írjuk. □

7. Megjegyzés. *Momentumgörbét határoz meg a képe az alábbi* $\nu_{k-1} : \mathrm{PG}(1,q) \to \mathrm{PG}(k-1,q)$ *leképezésnek:*

$$\nu_{k-1} : (x_1, x_2) \mapsto (x_1^{k-1}, x_1^{k-2}x_2, x_1^{k-3}x_2^2, \ldots, x_2^{k-1}). \tag{16}$$

10. Lemma. *Legyen* $\alpha \in \mathrm{PGL}(2,q)$. *Ekkor létezik egy* $\tilde{\alpha} \in \mathrm{PGL}(k,q)$ *projektivitás, hogy* $\nu_{k-1}(x)^{\tilde{\alpha}} = \nu_{k-1}(x^{\alpha}) \ \ \forall x \in \mathrm{PG}(1,q)$. *Ha* $q \geq k$, *akkor* $\tilde{\alpha}$ *egyértelmű.*

Bizonyítás. Az egyszerűen leellenőrizhető, hogy $\forall \alpha \in \mathrm{PGL}(2,q)$-ra $\nu_{k-1}(x) \mapsto \nu_{k-1}(x^{\alpha})$ egy projektivitás:
legyen $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a,b,c,d \in \mathbb{F}_q$ testelemek úgy, hogy $ad - bc \neq 0$. Ekkor felírhatjuk tetszőleges $x \in \mathrm{PG}(1,q)$ pontra az egyik, (x_1, x_2) reprezentáló vektorával α általi képét így: $x^{\alpha} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix}$. Így

$$\nu_{k-1}(x^{\alpha}) = ((ax_1 + bx_2)^{k-1}, (ax_1 + bx_2)^{k-2}(cx_1 + dx_2), \ldots, (cx_1 + dx_2)^{k-1}).$$

Annak az $\tilde{\alpha}$ projektivitásnak a mátrixát, ami $\nu_{k-1}(x_1, x_2)$-t átviszi $\nu_{k-1}(x^{\alpha})$-ba megkaphatjuk, ha $\nu_{k-1}(x^{\alpha})$ koordinátáit felírjuk homogén $(k-1)$-edfokú polinomokként és ezeknek a polinomoknak az együtthatói adják a mátrix sorait (az i-edik koordinátában lévő polinom együtthatói lexikografikusan rendezve az i-edik sort). Ahhoz, hogy $\tilde{\alpha}$ valóban projektivitás legyen, már csak az kell, hogy a mátrixának a determinánsa ne legyen 0. Ez valóban teljesül, mert ez a determináns $(ad - bc)^{\frac{k(k-1)}{2}}$ lesz, ami a $(ad - bc) \neq 0$ feltétel miatt nem 0. Az egyértelműség abból következik, hogy $q \leq k$ esetén ν_{k-1} képe tartalmaz $k+1$ általános helyzetű pontot, és egy projektivitást egyértelműen meghatároz a hatása $k+1$ általános helyzetű ponton (a $(k-1)$ dimenziós projektív téren). □
Tekintsük a következő leképezést:

$$\tilde{\phi} : \mathrm{PGL}(2,q) \to \mathrm{PGL}(k,q),$$

$$\alpha \mapsto \tilde{\alpha}.$$

11. Lemma. *Legyen* $\operatorname{Im}\tilde{\phi} = \mathrm{H}$. *Ekkor* $\mathrm{H} \simeq \mathrm{PGL}(2,q)$, $\mathrm{H} \leq \mathrm{PGL}(k,q)$ *és* H *hatásának az* $\mathcal{N}_{k-1}$ *görbe pontjaira vett megszorítása hű hatás, ha* $q \geq k$. *Speciálisan* H *regulárisan hat* $\mathcal{N}_{k-1}$ *ponthármasain (csak az egységelemnek vannak fixpontjai és tranzitív).*

Bizonyítás. A $\tilde{\phi}$-ként definiált leképezés egy csoporthomomorfizmus, a triviális maggal. Az $\mathcal{N}_{k-1}$ ponthármasain való regularitás pedig azért igaz, mert $\mathrm{PGL}(2,q)$ is így hat $\mathrm{PG}(1,q)$ pontjain. □

8. Megjegyzés. *Ha* $\mathcal{N} \subseteq \mathrm{PG}(k-1,q)$ *a* (16) *szerinti és* $\mathcal{N}' \subseteq \mathrm{PG}(k-1,q)$ *egy tetszőleges momentumgörbe, akkor definíció szerint létezik egy olyan* M *projektivitás, amire* $\mathcal{N}'^M = \mathcal{N}$. *Tudjuk, hogy* $M\mathrm{Aut}(\mathcal{N})M^{-1} = \{MAM^{-1} : A \in \mathrm{Aut}(\mathcal{N})\} = \mathrm{Aut}(\mathcal{N}')$, *ezért a 10 lemmában látottak tetszőleges momentumgörbére elmondhatóak.*

8. Állítás. *Ha* $\mathrm{PG}(k-1,q)$*-ban* $q \geq k+1$, *akkor egy* $k+2$ *méretű ívhez egyértelműen létezik egy, az ív pontjait tartalmazó momentumgörbe.*

Bizonyítás. Tekintsünk egy $k+2$ méretű ívet $\mathrm{PG}(k-1,q)$-ban, a pontjai legyenek $p_0, p_1, \ldots, p_{k+1}$. Tegyük fel, hogy a p_0 és p_{k+1} pontokat reprezentáló vektorok $(u_1, \ldots u_k)$ és $(v_1, \ldots, v_k)$ a $p_1, \ldots, p_k$ bázisban.
Vegyük észre, hogy az (u_i, v_i), $i = 1, \ldots, k$ vektorok k darab különböző pontot definiálnak a projektív egyenesen, hiszen ha nem így lenne, akkor lenne két pont, (u_i, v_i) és (u_j, v_j), $i \neq j$, hogy $u_i = \lambda u_j$ és $v_i = \lambda v_j$ valamilyen $0 \neq \lambda \in \mathbb{F}_q$ testelemre, amiből az következne, hogy k darab pont rajta lenne az $X_j = \lambda X_i$ egyenletű hipersíkon (pontosan a $\{p_0, p_1, \ldots, p_{k+1}\} \setminus \{p_i, p_j\}$ pontok lennének rajta ezen a hipersíkon, hiszen ezekben az i-edik és j-edik koordináta 0, vagy $u_i = \lambda u_j$ és $v_i = \lambda v_j$ teljesül).
Most tekintsük az alábbi $\mathrm{PG}(1,q) \to \mathrm{PG}(k-1,q)$ leképezést:

$$\phi_f : (x_1, x_2) \mapsto (f_1(x_1, x_2), \ldots, f_k(x_1, x_2)),$$

ahol

$$f_i(X_1, X_2) = \prod_{j=1, j\neq i}^{k} (u_j^{-1} X_1 - v_j^{-1} X_2),\ i = 1, \ldots, k.$$

Ekkor f_i homogén, $(k-1)$-edfokú polinom minden $i \in \{1, \ldots, k\}$-ra. Vegyük észre, hogy valóban léteznek is ezek az együtthatók, mert $u_i \neq 0, v_i \neq 0, i = 1, \ldots, k$, különben megint csak lenne k darab pont egy hipersíkon, ezért valóban, mindegyiknek van inverze.
Vizsgáljuk meg f_i polinomok függetlenségét: $\sum_{i=1}^{k} a_i f_i = 0 \Rightarrow a_i = 0$, miután felírjuk az (u_i, v_i) helyettesítéseket minden $i = 1, \ldots k$-ra. Így $f_1, \ldots, f_k$ bázist alkotnak a $\mathbb{F}_q[X_1, X_2]$-beli $(k-1)$-ed fokú homogén polinomok vektorterén. Ebből következik, hogy a bázis megváltoztatásának erejéig ϕ_f képe megegyezik ν_{k-1} képével ((16) szerint), amit jelöljünk $\mathcal{N}_f$-el. (Azért mert ν_{k-1}-ben is lineárisan független homogén polinomok vannak a leképezés definíciójában és azok átvihetőek egymásba lineáris transzformációval, mert bármely bázis átvihető bármelyikbe).

Ezután ϕ_f alkalmazásával (u_l, v_l) $l = 1, \ldots, k$ képe p_l, mivel $f_i(u_l, v_l) = 0$, ha $i \neq l$ és $f_i(u_i, v_i) = \prod_{j \neq i}(u_j^{-1}u_i - v_j^{-1}v_i)$, ami nem 0. Ezen kívül $\phi_f(1,0) = p_0$ és $\phi_f(0,1) = p_{k+1}$ ezzel megmutattuk, hogy $p_0, \ldots, p_{k+1}$ pontok egy momentumgörbén vannak.
Egyértelműség vizsgálata: Tudjuk, hogy miden momentumgörbe előáll valamilyen $g_1, g_2, ..., g_k$ polinomokra az alábbi leképezés képeként:

$$\phi_g : (x_1, x_2) \mapsto (g_1(x_1, x_2), \ldots, g_k(x_1, x_2)),$$

ahol $g_1, \ldots, g_k$ homogén $(k-1)$-edfokú polinomok bázist alkotnak $\mathbb{F}_q[X_1, X_2]$-ben. A képét jelöljük $\mathcal{N}_g$-vel. Tegyük fel, hogy $\mathcal{N}_g$ tartalmazza $p_0, \ldots, p_{k+1}$ pontokat. Az általánosság csorbítása nélkül feltehetjük, hogy az $(1,0)$ és $(0,1)$ pontok a p_0 és p_{k+1} ősképei, ha szükséges, ennek eléréséhez alkalmazzunk egy $\beta \in \mathrm{PGL}(2,q)$ transzformációt, ami $(0,1)$-et és $(1,0)$-t átviszi p_0 és p_{k+1} ősképébe. Ekkor legyen $g' = g \circ \beta$ és $\phi_{g'} = \phi_{g \circ \beta}$. A 10 lemma miatt $\mathcal{N}_{g'} = \mathcal{N}_g^{\tilde{\beta}}$, ezért innentől kezdve dolgozhatunk $\phi_{g'}$-vel és elég azt belátnunk, hogy $\mathcal{N}_{g'} = \mathcal{N}_f$. Abból a feltételből, hogy minden $i \in \{1, \ldots k\}$-ra $p_i \in \mathcal{N}_{g'}$, következik, hogy van olyan $(a_i, b_i) \in \mathrm{PG}(1,q)$, hogy $\phi_{g'}(a_i, b_i) = p_i$. Ekkor minden g'_j szorzatként felírt alakjában kell lennie egy $(a_i^{-1}X_1 - b_i^{-1}X_2)$ tényezőnek, ha $j \neq i$. Ez meghatározza g_i polinomokat egy nem 0 skalárszorzó erejéig, azaz

$$g'_j(X_1, X_2) = \lambda_j \prod_{i \neq j}(a_i^{-1}X_1 - b_i^{-1}X_2),$$

így $\phi'_g(1,0) = (\lambda_1 \prod_{i \neq 1} a_i^{-1}, \ldots, \lambda_k \prod_{i \neq k} a_i^{-1})$ tehát $\phi'_g(1,0)$ a $(\lambda_1 a_1, \ldots, \lambda_k a_k) = \lambda(u_1, \ldots, u_k)$ vektor által meghatározott ponttal egyezik meg.
Hasonlóan $\phi_{g'}(0,1) = ((-1)^{k-1}\lambda_1 \prod_{i \neq 1} b_i^{-1}, \ldots, (-1)^{k-1}\lambda_k \prod_{i \neq k} b_i^{-1})$, ami a homogén koordináták miatt megegyezik a $(\lambda_1 b_1, \ldots, \lambda_k b_k) = \mu(v_1, \ldots, v_k)$ vektor által meghatározott ponttal.
Ezekből adódik, hogy minden $i \in \{1, \ldots, k\}$-ra

$$\lambda_i = \lambda \frac{u_i}{a_i} = \mu \frac{v_i}{b_i},$$

amiből valóban $\phi_{g'}(\lambda u_i, \mu v_i) = p_i$. A 10 lemma és a 8 megjegyzés miatt (az ottani jelöléseket használva) $\mathcal{N}_{g'} = \mathcal{N}_g^{\tilde{\alpha}}$, ahol $\alpha \in \mathrm{PGL}(1,q)$ az a leképezés, ami az $(x_1, x_2) \mapsto (\lambda x_1, \mu x_2)$ hozzárendelést végzi el, ezért elég azt belátni, hogy $\mathcal{N}_{g'}^{\tilde{\alpha}} = \mathcal{N}_f$. A továbbiakban az egyszerűség kedvéért $\mathcal{N}_{g'}^{\tilde{\alpha}}$-t jelöljük $\mathcal{N}_h$-val, azaz a momentumgörbe legyen a $h = g' \circ \alpha$ által definiálva. Azt szeretnénk megmutatni, hogy $\phi_h(x_1, x_2) = \tau_x \phi_f(x_1, x_2)$ minden $x \in \mathrm{PG}(2,q)$-ra valamilyen τ_x skalárszorzóval.
Tudjuk, hogy ϕ_h és ϕ_f a $(0,1)$ és $(1,0)$ pontokhoz ugyanúgy a p_0 és p_{k+1} pontoknak megfelelő vektorokat rendelik. Azt is tudjuk, hogy $h_j(X_1, X_2) = \gamma_j \prod_{i \neq j}(t_i X_1 - X_2)$ alakú, ahol $t_i = \frac{v_i}{u_i}$, ezért $\phi_h(0,1) = (-1)^k(\gamma_1, \gamma_2, \ldots, \gamma_k) = \xi(v_1, v_2, \ldots, v_k)$, tehát skalárszorzó erejéig $(\gamma_1, \gamma_2, \ldots, \gamma_k)$ megegyezik $(v_1, v_2, \ldots, v_k)$-val. Tehát ϕ_f és ϕ_h egymás skalárszorosai, ezzel beláttuk az egyértelműséget is. □

12. Lemma. *Legyen $x(\mathcal{N})$ az $\mathcal{N}$ $\mathrm{PG}(k-1,q)$-beli momentumgörbe egy x pontjából vett, Π hipersíkra vonatkozó vetítése, úgy, hogy $x \notin \Pi$. Ekkor $x(\mathcal{N})$ rajta van egy egyel kisebb dimenziós momentumgörbén, amit ez egyértelműen meg is határoz, ha $q \geq k+1$.*

Bizonyítás. Legyen $\mathcal{A}$ a görbe pontjainak a halmaza (ahogy 7 -ben definiáltuk). Feltehetjük, hogy az $x = (1, 0, \ldots, 0)$ pontból vetítünk az $X_1 = 0$ hipersíkra. Ekkor $\mathcal{A}$ képe az alábbi ponthalmaz lesz:

$$\{(0, 1, t, \ldots, t^{k-2}) : t \in \mathbb{F}_q \setminus \{0\}\} \cup \{(0, 0, \ldots, 1)\},$$

amihez hozzávéve a $(0, 1, 0, \ldots, 0)$ pontot egy Π-beli eggyel kisebb dimenziós momentumgörbét kapunk.

Az egyértelműség 8 állításból következik. □

A $\mathrm{PG}(k-1, q)$-beli $\mathcal{N}_{k-1}$ momentumgörbének a $p = \nu_{k-1}(x_1, x_2)$ pontjában vett érintő egyenese $l_p = \langle p, p_1, p_2 \rangle$, ahol p_i az a pont, aminek a koordinátái az (x_1, x_2)-ben vett X_i szerinti parciális derivált értékei $\nu_{k-1}(X_1, X_2)$-nek. Az, hogy egy egyenest három ponttal adunk meg, elsőre furcsának tűnhet, erre azért van szükség, mert előfordulhat, hogy p_1 és p_2 közül az egyikre a csupa 0 vektor jönne ki, ami nem reprezentál projektív pontot. Ha viszont mindhárom pont létezik, akkor egy egyenesen vannak úgyis (erről bővebben a [10] könyv 326. oldalán lehet olvasni).

13. Lemma. *Egy $\mathcal{N}_{k-1}$ momentumgörbének az érintőegyenesei páronként diszjunktak (ha $k \geq 4$) és szelőket is csak érintési pontban metszenek.*

Bizonyítás. Vizsgáljuk meg a $\nu_{k-1}(0, 1)$ és $\nu_{k-1}(1, 0)$ pontokban vett érintő egyeneseket. Ha az érintőket meghatározó két-két pontot meghatározó vektorok lineárisan függetlenek, akkor diszjunktak, hiszen csak akkor metszenék egymást, ha az általuk meghatározott altér egy sík lenne. A

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & 1 \\ 0 & 0 & \ldots & 0 & 1 & 0 \\ 1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 & 0 \end{pmatrix}$$

mátrix rangja 4, ezért lineárisan függetlenek, így ezek az érintők diszjunktak. A 11 lemma szerinti tranzitív tulajdonság miatt ugyanez elmondható $\mathcal{N}_{k-1}$ bármely másik két pontjának érintő egyeneseiről, hiszen minden $\tilde{\alpha} \in \operatorname{Im} \tilde{\phi}$ transzformációra igaz, hogy az érintőket érintőkbe viszi.

A második részhez tekintsük a $\nu_{k-1}(1, 0)$-hoz tartozó l_p érintő egyenest és az l $\nu_{k-1}(0, 1)$ és $\nu_{k-1}(1, 1)$ pontokon átmenő szelőt. Itt is azt mutatjuk meg, hogy az általuk kifeszített altér 3 dimenziós $\mathrm{PG}(k-1, q)$-ban, ezért diszjunktak. A

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 1 & 1 & 1 & \ldots & 1 & 1 \end{pmatrix}$$

mátrix rangja is 4, ezért l és l_p egyenesek is kitérőek. A 11 lemma miatt itt is ugyanígy bármely $\mathcal{N}_{k-1}$-beli pont és azon át nem menő szelő átvihető ez előbbiekbe. □

14. Lemma. *Legyen $\mathcal{N} = \mathcal{N}_{k-1}$ egy $\mathrm{PG}(k-1,q)$-beli momentumgörbe, a $q \geq k+1$ feltétel mellett. Tekintsük $\mathcal{N}$ egy x pontjából vett, egy x-et nem tartalmazó Π hipersíkra való vetítését. Legyen $\mathcal{N}_x$ az ezen az $x(\mathcal{N})$ vetületen áthaladó egyetlen momentumgörbe. Ekkor $\mathcal{N}$-nek az x pontban vett érintő egyenese áthalad az egyetlen $p = \mathcal{N}_x \setminus x(\mathcal{N})$ ponton.*

Bizonyítás. A 11 lemmában szereplő tranzitív tulajdonság miatt feltehetjük, hogy $x = \nu_{k-1}(1,0)$. A korábbiakhoz hasonlóan itt is vehetjük a $\Pi = \{(x_1,\ldots,x_k) : x_1 = 0\}$ hipersíkot. Ekkor a 12 és 13 lemmákban kiszámolt eredmények alapján $p = (0,1,0,\ldots,0)$, az x-en áthaladó érintő pedig az $(1,0,\ldots,0)$ és $(0,1,0,\ldots,0)$ pontok által meghatározott egyenes, amiből valóban következik a bizonyítandó állítás. □

10. Tétel (Vetítős tétel). *Legyen $\mathcal{A}$ egy ív a $\mathrm{PG}(k-1,q)$ térben, tegyük fel, hogy $k \geq 4$ és $q \geq k+1$. Ekkor ha $\mathcal{A}$-t két különböző pontjából is ugyanarra a hipersíkra vetítve egy momentumgörbe részhalmazát kapjuk képnek, akkor maga $\mathcal{A}$ is része egy momentumgörbének.*

Bizonyítás. Feltehetjük, hogy $\mathcal{A}$-nak van legalább $k+3$ pontja, mert ellenkező esetben a 8 állítás következményeként teljesülne az állítás (minden legfeljebb $k+2$ méretű ív része egy momentumgörbének).
Tekintsük az $x \neq y \in \mathcal{A}$ pontokból való $x(\mathcal{A})$ és $y(\mathcal{A})$ vetítéseket a $\mathcal{H}$ hipersíkra ($x, y \notin \mathcal{H}$). Jelöljük a (feltétel szerint) így kapott $\mathcal{H}$-beli momentumgörbéket $\mathcal{N}_x$ és $\mathcal{N}_y$-al.
Tekintsünk egy tetszőleges $S \subseteq \mathcal{A}$ x-et és y-t tartalmazó $k+2$ elemű részhalmazt. Legyen $\mathcal{N}$ az egyetlen, S pontjain átmenő momentumgörbe (itt az egyértelműséghez kell a $q \geq k+1$ feltétel). Ekkor $\mathcal{A}$ és $\mathcal{N}$ is része két különböző kúpnak: $x\mathcal{N}_x$-nek és $y\mathcal{N}_y$-nak, ahol $p\mathcal{N}$ alatt az $\mathcal{N}$ pontjait p-vel összekötő egyenesek unióját értjük. Tekintsük $z \in \mathcal{A} \setminus \{x,y\}$ pontot és legyen $l_x = xz$ és $l_y = yz$ egyenes.
Indirekt módon tegyük fel, hogy $z \notin \mathcal{N}$.
Ha ℓ_x nem metszi $\mathcal{N}$-et x-en kívüli pontban, akkor ℓ_x érintője $\mathcal{N}$-nek, hiszen akkor az $x(\ell_x)$ vetület lesz az $\mathcal{N}_x \setminus x(\mathcal{N})$ kitüntetett pont és a 14 lemma alkalmazható. Hasonlóan ha ℓ_y nem metszi $\mathcal{N}$-et y-on kívüli pontban, akkor ℓ_y is érintője lesz $\mathcal{N}$-nek. Tehát ℓ_x és ℓ_y mindegyike vagy szelője, vagy érintője $\mathcal{N}$-nek. Ugyanakkor nem lehet mindkét szóban forgó egyenes érintő, mivel azokról a 13 lemma első felében beláttuk, hogy nem metszhetik egymást. Ha viszont a kettő közül az egyik érintő, a másik szelő lenne, akkor a 13 lemma második fele miatt jutnánk ellentmondásra, hiszen akkor a szelőnek át kell haladnia x, y és z pontokon, amik viszont nem lehetnek kollineárisak, ha ugyanazon az íven vannak. Így l_x és l_y mindketten szelői $\mathcal{N}$-nek (egyik sem lehet érintő).
Az $\langle l_x, l_y\rangle$ egyenesek által generált sík ekkor $\mathcal{N}$-nek legalább 4 pontját tartalmazza, ami ellentmondás, ezért $z \in \mathcal{N}$ feltételnek teljesülnie kell. Mivel z-t tetszőlegesen választottuk, ezért $\mathcal{A}$ minden pontja $\mathcal{N}$-nek is pontja és ezt szerettük volna belátni. □

4. Következmény. *Ha a $\mathrm{PG}(k-1,q)$ projektív térben minden $q+1$ méretű ív egy momentumgörbe, akkor igaz az MDS-sejtés $\mathrm{PG}(k,q)$ térben a $q+1 \geq k+3 \geq 6$ feltétel mellett.*

Bizonyítás. Indirekt módon tegyük fel, hogy létezik $\mathcal{A}$, egy $q+2$ méretű ív $\mathrm{PG}(k,q)$ projektív térben. Ekkor $\mathcal{A}$-t bármelyik pontjából vetítve egy $q+1$ méretű, $\mathrm{PG}(k-1,q)$-beli ívet kapunk, ami a feltétel szerint egy momentumgörbe. Az előző, 10 tétel miatt ekkor $\mathcal{A}$ is része egy momentumgörbének, ami ellentmondás, hiszen annak $q+1$ pontja van. □

5.3. Példák $q+1$ méretű ívekre

Nézzük meg az eddig ismert összes, nem ekvivalens, a momentumgörbétől különböző konstrukciót $q+1$ méretű ívekre.

5. Példa (Glynn, 1986.). *Az alábbi $S \subseteq \mathrm{PG}(4,9)$ ponthalmaz egy ívet alkot:*

$$S = \{(1, t, t^2 + \eta t^6, t^3, t^4) : t \in \mathbb{F}_9\} \cup \{(0,0,0,0,1)\},$$

ahol $\eta \in \mathbb{F}_9$ úgy, hogy $\eta^4 = -1$.

Bizonyítás.[4] Ahhoz, hogy belássuk, hogy az ezek által a (homogénen koordinátázott) vektorok által meghatározott pontok egy íven vannak, elég azt megmutatnunk, hogy ennek a 10 elemű vektorhalmaznak bármely 5 eleme lineárisan független.
Indirekt módon tegyük fel, hogy van olyan 5 különböző vektor, amikre ez nem igaz, tehát lineárisan összefüggenek.

- 1.eset: Ha nincs az 5 között a $(0,0,0,0,1)$ vektor.

  A lineáris összefüggőség azt jelenti, hogy

  $$\begin{vmatrix} 1 & t_1 & t_1^2 + \eta t_1^6 & t_1^3 & t_1^4 \\ 1 & t_2 & t_2^2 + \eta t_2^6 & t_2^3 & t_2^4 \\ 1 & t_3 & t_3^2 + \eta t_3^6 & t_3^3 & t_3^4 \\ 1 & t_4 & t_4^2 + \eta t_4^6 & t_4^3 & t_4^4 \\ 1 & t_5 & t_5^2 + \eta t_5^6 & t_5^3 & t_5^4 \end{vmatrix} = 0,$$

  ahol t_1, t_2, t_3, t_4, és t_5 különböző testelemek.

  A determinánsok linearitási tulajdonsága miatt:

  $$\begin{vmatrix} 1 & t_1 & t_1^2 & t_1^3 & t_1^4 \\ 1 & t_2 & t_2^2 & t_2^3 & t_2^4 \\ 1 & t_3 & t_3^2 & t_3^3 & t_3^4 \\ 1 & t_4 & t_4^2 & t_4^3 & t_4^4 \\ 1 & t_5 & t_5^2 & t_5^3 & t_5^4 \end{vmatrix} = -\eta \begin{vmatrix} 1 & t_1 & t_1^6 & t_1^3 & t_1^4 \\ 1 & t_2 & t_2^6 & t_2^3 & t_2^4 \\ 1 & t_3 & t_3^6 & t_3^3 & t_3^4 \\ 1 & t_4 & t_4^6 & t_4^3 & t_4^4 \\ 1 & t_5 & t_5^6 & t_5^3 & t_5^4 \end{vmatrix}. \tag{17}$$

  Emeljük mindkét oldalt köbre, és használjuk, hogy $t^9 = t \ \forall t \in \mathbb{F}_9$:

  $$\begin{vmatrix} 1 & t_1^3 & t_1^6 & t_1 & t_1^4 \\ 1 & t_2^3 & t_2^6 & t_2 & t_2^4 \\ 1 & t_3^3 & t_3^6 & t_3 & t_3^4 \\ 1 & t_4^3 & t_4^6 & t_4 & t_4^4 \\ 1 & t_5^3 & t_5^6 & t_5 & t_5^4 \end{vmatrix} = -\eta^3 \begin{vmatrix} 1 & t_1^3 & t_1^2 & t_1 & t_1^4 \\ 1 & t_2^3 & t_2^2 & t_2 & t_2^4 \\ 1 & t_3^3 & t_3^2 & t_3 & t_3^4 \\ 1 & t_4^3 & t_4^2 & t_4 & t_4^4 \\ 1 & t_5^3 & t_5^2 & t_5 & t_5^4 \end{vmatrix}. \tag{18}$$

Mindkét oldalon a 2. és 4. oszlopot cseréljük meg:

$$\begin{vmatrix} 1 & t_1 & t_1^6 & t_1^3 & t_1^4 \\ 1 & t_2 & t_2^6 & t_2^3 & t_2^4 \\ 1 & t_3 & t_3^6 & t_3^3 & t_3^4 \\ 1 & t_4 & t_4^6 & t_4^3 & t_4^4 \\ 1 & t_5 & t_5^6 & t_5^3 & t_5^4 \end{vmatrix} = -\eta^3 \begin{vmatrix} 1 & t_1 & t_1^2 & t_1^3 & t_1^4 \\ 1 & t_2 & t_2^2 & t_2^3 & t_2^4 \\ 1 & t_3 & t_3^2 & t_3^3 & t_3^4 \\ 1 & t_4 & t_4^2 & t_4^3 & t_4^4 \\ 1 & t_5 & t_5^2 & t_5^3 & t_5^4 \end{vmatrix}. \tag{19}$$

Vegyük észre, hogy a (17) kifejezés baloldala megegyezik a (19) egyenlet jobboldalán található determinánssal (egy Vandermonde determináns), ezért helyettesítsük be a (17) egyenlet jobb oldalát a (19) jobb oldalába:

$$\begin{vmatrix} 1 & t_1 & t_1^6 & t_1^3 & t_1^4 \\ 1 & t_2 & t_2^6 & t_2^3 & t_2^4 \\ 1 & t_3 & t_3^6 & t_3^3 & t_3^4 \\ 1 & t_4 & t_4^6 & t_4^3 & t_4^4 \\ 1 & t_5 & t_5^6 & t_5^3 & t_5^4 \end{vmatrix} = (-\eta^3)(-\eta) \begin{vmatrix} 1 & t_1 & t_1^6 & t_1^3 & t_1^4 \\ 1 & t_2 & t_2^6 & t_2^3 & t_2^4 \\ 1 & t_3 & t_3^6 & t_3^3 & t_3^4 \\ 1 & t_4 & t_4^6 & t_4^3 & t_4^4 \\ 1 & t_5 & t_5^6 & t_5^3 & t_5^4 \end{vmatrix}.$$

Tudjuk, hogy eredetileg egy nem 0 kifejezés van mindkét oldalon (Vandermonde determinánst helyettesítettünk be, amiről tudjuk, hogy nem 0), ezért a determinánssal leosztva azt kapjuk, hogy $\eta^4 = 1$, ami ellentmond a kezdeti feltételnek, hogy $\eta^4 = -1$.

- 2. eset: Ha az egyik vektor a $(0, 0, 0, 0, 1)$.

  A determinánst kifejtve a $(0, 0, 0, 0, 1)$ sor szerint egy 4×4-es mátrix determinánsát kell megvizsgálnunk. Innentől annak a bizonyítása, hogy ez a determináns nem lehet 0 szóról-szóra ugyanaz, mint az 1. esetben, annyi különbséggel, hogy nem kell az utolsó oszlopot nézni, de az az előbbi bizonyításban sem volt számottevő. □

Glynn példájának további tulajdonságai megtalálhatóak a [19] cikkben.

6. Példa (Hirschfeld). *Az alábbi $S \subseteq \mathrm{PG}(3, q)$ ponthalmaz egy ívet alkot:*

$$S = \{(1, t, t^{2^r}, t^{2^r+1}) : t \in \mathbb{F}_q\} \cup \{(0, 0, 0, 1)\},$$

ahol $q = 2^h$, $(r, h) = 1$.

Bizonyítás. A bizonyítás a [21] könyv 44. fejezete és az [5] könyv 7.6. példája alapján készült. Be kell látnunk, hogy a fenti S vektorhalmaz bármely 4 eleme lineárisan független, azaz a belőlük képzett 4×4-es mátrix determináns nem 0.
A bizonyítás lényege az, hogy mutatunk olyan lineáris transzformációkat (projektivitásokat), amikkel S pontjait fixen hagyva S bármely 2 pontját átvihetjük a „kedvenc” S-beli pontpárunkba, amivel megkönnyíthetjük a számolást.

Először mutatunk egy olyan $G(\sigma) \leq GL(4,q)$ részcsoportját az $\mathbb{F}_q$ feletti lineáris transzformációknak (4×4-es nem 0 determinánsú mátrixokkal írhatóak le), amely S halmazt fixen hagyja és 2-tranzitívan hat S pontjain.

Legyen $2^r = \sigma$.

Legyen $G(\sigma) = \left\{ \begin{pmatrix} aa^\sigma & ba^\sigma & ab^\sigma & bb^\sigma \\ ca^\sigma & da^\sigma & cb^\sigma & db^\sigma \\ ac^\sigma & bc^\sigma & ad^\sigma & bd^\sigma \\ cc^\sigma & dc^\sigma & cd^\sigma & dd^\sigma \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,q) \right\}$.

Az, hogy $G(\sigma)$ elemei invertálhatóak elemi számolásokkal ellenőrizhető. Kihasználva, hogy $\mathbb{F}_q$ 2-karakterisztikájú és a σ-adik hatványra emelés tagonként végezhető, azt kapjuk, hogy

$$\det \begin{pmatrix} aa^\sigma & ba^\sigma & ab^\sigma & bb^\sigma \\ ca^\sigma & da^\sigma & cb^\sigma & db^\sigma \\ ac^\sigma & bc^\sigma & ad^\sigma & bd^\sigma \\ cc^\sigma & dc^\sigma & cd^\sigma & dd^\sigma \end{pmatrix} = (ad-bc)^{2\sigma+2} = \begin{vmatrix} a & b \\ c & d \end{vmatrix}^{2\sigma+2} \neq 0.$$

Továbbá $G(\sigma)$ elemei valóban egy csoportot alkotnak, hiszen az alap csoporttulajdonságok nyilván teljesülnek amiatt, hogy a 4×4-es mátrixok gyűrűt alkotnak és $G(\sigma)$-nak eleme az egységmártix, ezért csak azt kell belátnunk, hogy $G(\sigma)$ zárt a szorzásra nézve. Ez onnan is látható, hogy egy $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$-nek és $\begin{pmatrix} x & y \\ z & v \end{pmatrix}$-nek megfelelő mátrix szorzata a $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & v \end{pmatrix}$-nek megfelelő $G(\sigma)$-beli mátrix lesz, ami elemi számolásokkal egyszerűen leellenőrizhető. Vagyis a $\phi : \mathrm{GL}(2,q) \to \mathrm{GL}(4,q)$ leképezés, ahol $\phi \begin{pmatrix} a & b \\ b & d \end{pmatrix} = \begin{pmatrix} aa^\sigma & ba^\sigma & ab^\sigma & bb^\sigma \\ ca^\sigma & da^\sigma & cb^\sigma & db^\sigma \\ ac^\sigma & bc^\sigma & ad^\sigma & bd^\sigma \\ cc^\sigma & dc^\sigma & cd^\sigma & dd^\sigma \end{pmatrix}$ egy homomorfizmus (ennek a leképezésnek még érdekes algeberai tulajdonságai vannak a [21] könyv 44. fejezetében).

Be kell még látnunk, hogy $G(\sigma)$ elemei fixen hagyják S pontjait. Ehhez végezzük el $G(\sigma)$ egy tetszőleges elemével és S egy általános vektorával a mátrixszorzást, ami megadja a vektor képét a transzformáció elvégzése után:

$$\begin{pmatrix} aa^\sigma & ba^\sigma & ab^\sigma & bb^\sigma \\ ca^\sigma & da^\sigma & cb^\sigma & db^\sigma \\ ac^\sigma & bc^\sigma & ad^\sigma & bd^\sigma \\ cc^\sigma & dc^\sigma & cd^\sigma & dd^\sigma \end{pmatrix} \begin{pmatrix} 1 \\ t \\ t^\sigma \\ t^{\sigma+1} \end{pmatrix} = \begin{pmatrix} a^{\sigma+1} + tba^\sigma + t^\sigma ab^\sigma + (bt)^{\sigma+1} \\ ca^\sigma + tda^\sigma + t^\sigma cb^\sigma + db^\sigma t^{\sigma+1} \\ ac^\sigma + tbc^\sigma + a(td^\sigma) + bd^\sigma t^{\sigma+1} \\ c^{\sigma+1} + tdc^\sigma + c(dt^\sigma) + (dt)^{\sigma+1} \end{pmatrix} =$$

$$= \begin{pmatrix} a^\sigma(a+tb) + (bt)^\sigma(a+tb) \\ a^\sigma(c+dt) + (bt)^\sigma(c+dt) \\ c^\sigma(a+tb) + (dt)^\sigma(a+tb) \\ c^\sigma(c+dt) + (dt)^\sigma(c+dt) \end{pmatrix}.$$

Kihasználva, hogy 2-karakterisztikájú test fölött vagyunk, és, hogy $\sigma = 2^r$, ezért összeg σ-adik hatványra emelését végezhetjük tagonként, a vektor kapott képe az összevonások után:

$$\begin{pmatrix} (a+tb)^{\sigma+1} \\ (c+dt)(a+bt)^{\sigma} \\ (c+dt)^{\sigma}(a+tb) \\ (c+dt)^{\sigma+1} \end{pmatrix}.$$

Az ilyen alakúakról pedig már látszik, hogy benne vannak S-ben, mivel a homogén koordináták miatt ez ekvivalens az $(1, s, s^{\sigma}, s^{\sigma+1})$ vektorral, ahol $s = \frac{c+dt}{a+bt}$ abban az esetben, ha $a + bt \neq 0$, ha pedig 0, akkor a $(0, 0, 0, 1)$ vektorral ekvivalens, ami szintén S-beli.

Azt is vizsgáljuk meg, hogy hova transzformálják ezek a $(0, 0, 0, 1)$ vektort: látszik, hogy a $(b^{\sigma+1}, db^{\sigma}, bd^{\sigma}, d^{\sigma+1})$ vektorba viszi át, ami a korábbi indoklás miatt szintén S-beli vektor lesz. Tehát ezzel beláttuk, hogy minden S-beli pont képe is S-beli lesz és mivel egy ilyen lineáris transzformáció injektív (a mátrixa invertálható), ezért S-et fixen hagyja.

Most lássuk be a 2-tranzitivitást, vagyis, hogy bármely két különböző S-beli vektort bármelyik másik két különböző S-belibe át lehet vinni alkalmas $G(\sigma)$-beli lineáris transzformációval. Ehhez elegendő megmutatnunk, hogy az $(1, 0, 0, 0)$ és $(0, 0, 0, 1)$ vektorokat bármelyik két különböző S-belibe átvihetjük, hiszen akkor az invertálhatóság miatt bármely kettőt át is vihetünk az $(1, 0, 0, 0)$ és $(0, 0, 0, 1)$ vektorpárosba, és ezeket megfelelően komponálva kapjuk a 2-tranzitivitást.

Tegyük fel, hogy $(1, 0, 0, 0)$-t $(A^{\sigma+1}, CA^{\sigma}, AC^{\sigma}, C^{\sigma+1})$-be és a $(0, 0, 0, 1)$-t pedig $(B^{\sigma+1}, DB^{\sigma}, BD^{\sigma}, D^{\sigma+1})$-be szeretnénk átvinni, ahol $AD \neq CB$, hogy különböző pontokat határozzanak meg az előbbi vektorok.

Az előbbiek miatt látszik, hogy a keresett mátrix nem más, mint az $a = A, b = B, c = C, d = D$-ből képzett mátrix, tehát valóban 2-tranzitívan hat $G(\sigma)$ S-en.

Ezért bármely vektornégyes átvihető a $(1, 0, 0, 0)$, $(0, 0, 0, 1)$, $(1, t, t^{\sigma}, t^{\sigma+1})$ és $(1, s, s^{\sigma}, s^{\sigma+1})$ vektornégyesbe, valamely $s \neq t \in \mathbb{F}_q$-kra (azaz itt s és t nincs előre lefixálva). A determinánsok szorzástétele miatt pedig elég csak ezen négy vektor által meghatározott mátrix determinánsáról belátni, hogy nem 0.

Tegyük fel, hogy

$$\begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & t & t^{\sigma} & t^{\sigma+1} \\ 1 & s & s^{\sigma} & s^{\sigma+1} \end{vmatrix} = ts^{\sigma} - st^{\sigma} = 0.$$

Vagyis

$$ts^{\sigma} = st^{\sigma},$$

$$ts(s^{\sigma-1} - t^{\sigma-1}) = 0.$$

Vegyük észre, hogy itt is ugyanazt kaptuk, mint a (15) egyenletben, aminél már láttuk, hogy csak akkor lehet megoldása, ha $s = t$, ami itt a feltétel miatt nem lehet.

Ezzel tehát beláttuk, hogy S bármely négy pontja általános helyzetű. □

6. Lehetséges gyengítések: near-MDS kódok, almost-MDS kódok

Végül nézzünk meg két, az MDS kódokhoz nagyon hasonlító struktúrát. Ezeket először Stefan Dodunekov és Ivan Landgev kezdte el vizsgálni a [11] cikkükben (near-MDS kódok), illetve velük közel egy időben De Boer a [15] cikkében (almost-MDS kódok).
Ezek megismeréséhez szükségünk van néhány újabb, lineáris kódokra vonatkozó fogalom bevezetésére. Ehhez használjuk V. K. Wei [9] cikkét.

Legyen továbbra is C egy $[n,k]_q$ lineáris kód.

15. Definíció (tartó). *A C kód tartójának azokat a koordinátákat nevezzük, amelyek mindegyikéhez van olyan C-beli kódszó, hogy az adott koordinátája nem 0. Jele: $supp(C)$,*

$$supp(C) = \{i : \exists x \in C, x_i \neq 0\}.$$

16. Definíció (Általánosított Hamming-súly). *Egy $C = [n,k]_q$ lineáris kód r-edik általánosított Hamming-súlyán az $[n,r]_q \subseteq C$ altérkódok tartóinak minimális elemszámát értjük.*
Jele: $d_r(C)$, $r = 1, 2, \ldots, k$,

$$d_r(C) = \min\{|supp(D)| : D = [n,r]_q \subseteq C\}.$$

Világos, hogy $d_1(C) = d(C)$, hiszen az 1 dimenziós részkódok között pont azokban van a legtöbb 0, amit a minimális súlyú kódszó generál és az 1 állítás miatt $d(C) = \min\{w(x) : x \in C\}$.

15. Lemma. *Legyen $C = [n,k]_q$ lineáris kód. Ekkor*

$$0 < d_1(C) < d_2(C) < \cdots < d_k(C) \leq n.$$

Bizonyítás. Az, hogy $d_{r-1}(C) \leq d_r(C)$ nyilvánvaló, hiszen egy r dimenziós részkódnak a tartója mindig bővebb, mint az $r-1$ dimenziós részkódjaié. Már csak a szigorú egyenlőtlenséget kell belátnunk. Legyen $D = [n,r]_q \subseteq C$ olyan, hogy $|supp(D)| = d_r(C)$. Legyen $i \in supp(D)$ és $D_i = \{x \in D : x_i = 0\}$. Ekkor $D_i = [n, r-1]_q \subset D$, $\dim D_i = r-1$ is egy lineáris altérkód, ezért $d_{r-1}(C) \leq |supp(D_i)| \leq |supp(D)| - 1 = d_r(C) - 1$, vagyis $d_{r-1}(C) < d_r(C)$. □

5. Következmény (Általánosított-Singleton korlát). *Legyen $C = [n,k]_q$ lineáris kód. Ekkor*

$$d_r(C) \leq n - k + r, \qquad \forall\ r = 1, 2, \ldots, k.$$

Bizonyítás. Az előző lemmából nyilvánvaló. □
Legyen H a $C = [n,k]_q$ lineáris kód paritásellenőrző mátrixa. Jelöljük H_i-vel az i-edik oszlopát.

9. Állítás. *Legyen $C = [n,k]_q$ lineáris kód. Ekkor $\forall\ r \leq k$-ra*

$$d_r(C) = \min\{|I| : |I| - \dim\langle H_i : i \in I\rangle \geq r\}.$$

Bizonyítás. Minden $I \subseteq \{1, 2, \ldots, n\}$ részhalmazra jelölje $S(I) = \langle H_i : i \in I \rangle$ oszlopok által kifeszített alteret. Legyen $S^{\perp}(I) = \{x : x_i = 0 \ \forall i \notin I \text{ és } \sum_{i \in I} x_i H_i = 0\}$, ami szintén egy lineáris altér. Világos, hogy $\dim S(I) + \dim S^{\perp}(I) = |I|$.
Jelöljük az állításban szereplő egyenlet jobb oldalát d-vel. Válasszuk meg I-t úgy, hogy $|I| - \dim(S(I)) = r$ és $|I| = d$. Ez azért tehető meg, mert ha $|I| - \dim S(I) > r$, akkor I-t eggyel csökkentve valamely I' részhalmazára is fennáll, hogy $|I'| - \dim S(I') \geq r$, de itt $|I'| < |I| = d$, ami ellentmond d minimalitásának. Ekkor nyilván $d_r(C) \leq d$ (hiszen ekkor $r = \dim S^{\perp}(I)$, és $d_r(C) \leq |supp(S^{\perp}(I))| \leq |I| = d$).
Lássuk be a másik irányú egyenlőtlenséget is. Legyen $D = [n, r]_q \subseteq C$ részkód és $|supp(D)| = d_r(C)$. Legyen $I^* = supp(D) \Rightarrow D \subseteq S^{\perp}(I^*)$. Ugyanakkor $\dim S(I^*) = |I^*| - \dim S^{\perp}(I) \leq |I| - r$, azaz $|I^*| - \dim S(I^*) \geq r$. Ekkor viszont $d_r(C) = |I^*| \in \{|I| : |I| - \dim\langle H_i : i \in I\rangle \geq r\}$, amiből már $d \leq d_r(C)$ következik, ezzel a másik irányú egyenlőtlenséget is beláttuk. □

6. Következmény. *Legyen H a $C = [n, k]_q$ lineáris kód paritásellenőrző mátrixa. Ekkor $d_r(C) = d$ ekvivalens a következőkkel:*

1. *bármely $d - 1$ oszlop által meghatározott mátrix rangja legalább $d - r$,*
2. *van d oszlopa H-nak, amik által meghatározott mátrix $d - r$ rangú.*

17. Definíció (NMDS kód). *Egy $C = [n, k]_q$ lineáris kód near-MDS kód (a továbbiakban NMDS), ha*

1. *$d_1(C) = n - k$ és*
2. *$d_i(C) = n - k + i$, ha $i = 2, 3, \ldots, k$.*

9. Megjegyzés. *Ezzel a definícióval ekvivalens a következő: egy $C = [n, k]_q$ lineáris kód pontosan akkor NMDS, ha $d_1(C) = n - k$ és $d_2(C) = n - k + 2$.*

Bizonyítás. Következik a 15 ($d_r(C)$ monotonitására vonatkozó) lemmából, és, hogy $d_r(C)$ egész minden $r = 1, 2, \ldots, k$ számra. □

10. Állítás. *Egy $C = [n, k]_q$ lineáris kód NMDS akkor és csak akkor, ha a H paritásellenőrző mátrixára teljesülnek az alábbiak:*

N1 bármely $n - k - 1$ oszlopa lineárisan független,

N2 van $n - k$ lineárisan összefüggő oszlopa,

N3 bármely $n - k + 1$ oszlopából képzett mátrix teljes rangú ($n - k$).

Bizonyítás. Felhasználva, hogy az előbbi ekvivalens definíció miatt elegendő csak a $d_1(C) = n - k$ és $d_2(C) = n - k + 2$ feltételeket kikötnünk, alkalmazzuk a 6 következményt, amiből az $N1$, $N2$ és $N3$ tulajdonságok adódnak. □
A következő állítás hasznos lesz annak a bizonyításához, hogy egy NMDS kód duálisa is NMDS kód.

11. Állítás. *Legyen $C = [n,k]_q$ lineáris kód. Ekkor*

$$\{d_r(C) : r = 1,2,\ldots,k\} \cup \{n+1-d_r(C^\perp) : r = 1,2,\ldots,n-k\} = \{1,2,\ldots,n\}.$$

Bizonyítás. Elég belátnunk azt, hogy minden r-re, ahol $1 \le r \le n-k$ igaz, hogy

$$n+1-d_r(C^\perp) \notin \{d_i(C) : 1 \le i \le k\},$$

mivel a $\{d_r(C) : r = 1,2,\ldots,k\}$ halmaz k elemű, $\{n+1-d_r(C^\perp) : r = 1,2,\ldots,n-k\}$ pedig $n-k$ elemű továbbá mindkét halmaz elemei 1 és n között vannak a 15 lemma miatt. Tehát elég azt megmutatni, hogy a két halmaz diszjunkt.
Először lássuk be azt, hogy $d_t(C) \le n - d_r(C^\perp)$, ahol $t = k + r - d_r(C^\perp)$. Ez a t választás értelmes hiszen az 5, általánosított Singleton-korlát miatt $0 \le t \le k$ (ha esetleg a $t = 0$ esete állna fent, akkor gondolhatunk $d_0(C) = 0$-ra mint egy elfajult, 0 dimenziós altérhez tartozó értékre). Legyen $D \subseteq C^\perp$ úgy, hogy $\dim D = r$ és $|supp(D)| = d_r(C^\perp)$ és legyen H a C paritásellenőrző mátrixa úgy, hogy az első r sorvektora generálja D-t. Ekkor a $\{H_i : i \notin supp(D)\}$ oszlopvektorok első r koordinátája 0 (tartó definíciója miatt). Vegyük észre, hogy

$$\dim\langle H_i : i \notin supp(D)\rangle = (\text{oszlop})rk(\langle H_i : i \notin supp(D)\rangle) = (\text{sor})rk(\langle R_i : r+1 \le i \le n-k\rangle) =$$

$= n-k-r$, ahol R_i az i-edik sorvektora H-nak.
Legyen $I = \{1,2,\ldots,n\} \setminus supp(D)$, $|I| = n - d_r(C^\perp)$. Ekkor a 9 állítás miatt $d_t(C) \le |I| = n - d_r(C^\perp)$, ahol $t = |I| - (n-k-r)$.
Idézzük fel, hogy a célunk nem más, mint annak belátása, hogy $n+1-d_r(C^\perp) \ne d_i(C)$ semmilyen $i \in \{1,\ldots,k\}$-ra. Ebből már az $i \le t$ esetet az előbb láttuk be, hiszen ha $d_t(C) < n+1-d_r(C^\perp)$, akkor a 15 lemma miatt $d_i(C) < n+1-d_r(C^\perp)$ is igaz, ha $i \le t$. Így már elég csak azt megmutatnunk, hogy $d_{t+\Delta}(C) \ne n - d_r(C^\perp) + 1$ semelyik $\Delta \ge 1$-re sem. Indirekt tegyük fel, hogy az egyenlőség fennáll valamely $\Delta \ge 1$-re. Ekkor létezik egy olyan G generátor mátrixa C-nek (ami egyben paritásellenőrző mátrixa $C^\perp$-nek), amiben az utolsó $d_r(C^\perp) - 1$ koordinátája az első $t + \Delta$ sornak mind 0.
Legyen $I = \{n - d_r(C^\perp) + 2, \ldots, n\}$. Ekkor G utolsó $|I|$ oszlopa egy olyan alteret feszít ki aminek a dimenziója legfeljebb $k - t - \Delta = d_r(C^\perp) - r - \Delta$. A 9 állítás miatt $d_s(C^\perp) \le d_r(C^\perp) - 1$, ahol $s = |I| - (d_r(C^\perp) - r - \Delta) = r + \Delta - 1$, ami ellentmond a 15, monotonitásra vonatkozó állításnak, mert $s \ge r$. Ezért $n+1-d_r(C^\perp)$ nem általánosított Hamming súly C-ben semmilyen r-re sem, tehát készen vagyunk. □

11. Tétel. *Egy $C = [n,k]_q$ NMDS kód duálisa is NMDS kód.*

Bizonyítás. A definíciót és az előző állítást felhasználva

$$\{n+1-d_r(C^\perp) : r = 1,2,\ldots,n-k\} = \{1,2,\ldots,n-k-1,n-k+1\},$$

azaz $d_{n-k}(C^\perp) = n$, $d_{n-k-1}(C^\perp) = n-1$, …, $d_2(C^\perp) = k+2$, $d_1(C^\perp) = k$. Ez pedig definíció szerint azt jelenti, hogy $C^\perp = [n, n-k]_q$ is egy NMDS kód. □

7. Következmény. *Egy $C = [n,k]_q$ lineáris kód NMDS $\iff$ ha a G_C generátor mátrixra teljesülnek az alábbiak:*

N1' bármely $k-1$ oszlopa lineárisan független,

N2' van k lineárisan összefüggő oszlopa,

N3' bármely $k+1$ oszlopa által meghatározott mátrix teljes (k) rangú.

□

12. Tétel (NMDS kód projektív geometriai megfelelője). *Egy G generátormátrixszal generált $C = [n,k]_q$ lineáris kód NMDS akkor és csak akkor, ha a G oszlopvektorai által meghatározott $\mathrm{PG}(k-1,q)$-beli S ponthalmazra teljesülnek az alábbiak:*

1. *$\forall$ $k-1$ pontú részhalmaza S-nek általános helyzetű (azaz a pontok egy hipersíkot generálnak),*
2. *$\exists$ k darab pont S-ben, amik egy hipersíkon vannak,*
3. *$\forall$ $k+1$ pont generálja $\mathrm{PG}(k-1,q)$ teret.*

Bizonyítás. Az odafele irány következik a 7, a generátor mátrixra vonatkozó állításból. Visszafele pedig hasonlóan a 4 tétel bizonyításához, itt is a pontokat reprezentáló tetszőleges oszlopvektorok egymásmellé írásával kapott mátrix NMDS kódot generál. □
Könnyen leellenőrizhető, hogy ez például a $k = 3$ esetben annyit jelent, hogy $S \subseteq \mathrm{PG}(2,q)$ olyan síkbeli ponthalmaz, amely tartalmaz 3 egy egyenesre eső pontot, de semelyik 4 pont nem esik egy egyenesre.

Az MDS kódokhoz hasonlóan NMDS kódok esetén is felmerül a kérdés, hogy vajon adott k és q esetén mi a leghosszabb NMDS kód. Ezt a hosszt jelöljük $m'(k,q)$-val.

12. Állítás. *Legyen $m'(k,q)$ a k dimenziós $\mathbb{F}_q$ feletti NMDS kódok maximális hossza. Ekkor*

1. *$m'(k,q) \leq 2q + k$,*
2. *$m'(2,q) = 2q + 2$,*
3. *$m'(k,q) \leq m'(k-\alpha,q) + \alpha$ minden $0 \leq \alpha \leq k$ egészre,*
4. *$m'(k,q) = k+1$, ha $k > 2q$,*
5. *$m'(k,q) \leq 2q + k - 2$, ha $q > 3$,*
6. *$m'(2q,q) = 2q + 2$, ha $q > 3$, $k > 2$,*
7. *$m'(2q-1,q) = 2q + 1$, ha $q > 3$.*

Az állítás bizonyítása megtalálható a [12] forrásban (Theorem 2.7.).

Nézzünk meg néhány egyszerű példát NMDS kódokra kis k és $q = 2$ esetén. További konstrukciók találhatóak még a [12] forrásban.

7. Példa. *Ha $k = 2$, $q = 2$, akkor az alábbi, generátor mátrixával adott $[6, 2]_2$ kód NMDS kód:*

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

8. Példa. *Ha $k = 3$, $q = 2$, akkor az a $[7, 3]_2$ lineáris kód, amelynek a generátormátrixának az oszlopai pontosan a Fano-sík pontjait adják meg, NMDS kód.*

9. Példa. *Ha $k = 3$, $q = 2$, akkor a generátor mártixával adott*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$[6, 3]_2$ *lineáris kód egy NMDS kód.*

Ezekben a példákban elég a 7 következmény alapján ellenőrizni a mátrixokat, vagy a 12 tétel alapján a geometriai megfelelőjét vizsgálni (például a Fano-sík pontjaira azonnal látszik, hogy igazak a tulajdonságok).
További $[n, k]_q$ NMDS kódokat lehet még konstruálni $\mathrm{PG}(k-1, q)$-beli n pontú elliptikus (harmadrendű) görbékből (például $k = 6$-ra a [14] forrásban). Az ilyen görbék maximális méretét jelöljük $N_q(1)$-gyel. Erre a méretre pedig alábbi felső korlátokat ismerjük ([13] forrás alapján):

$$N_q(1) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor & \text{ha } p \mid \lceil 2\sqrt{q} \rceil \text{ és } h \text{ páratlan (továbbra is } q = p^h), \\ q + \lfloor 2\sqrt{q} \rfloor + 1 & \text{különben.} \end{cases}$$

Hasonlóan az MDS kódokhoz, $m'(k, q)$-ra a [13] forrás alapján az alábbi két sejtést fogalmazhatjuk meg:

4. Sejtés (Gyenge NMDS-sejtés). *Minden k pozitív egészre és $q \geq 5$ prímhatványra $m'(k, q) \leq 2(q + 1)$.*

5. Sejtés (Erős NMDS-sejtés). *Létezik egy olyan univerzális c konstans, ami nem függ q-tól, hogy $m'(k, q) \leq N_q(1) + c$.*

Az NMDS kódokéhoz nagyon hasonló, de nem teljesen ekvivalens problémával foglalkozhatunk az almost-MDS kódok vizsgálatakor. Ezzel foglalkozik a [15] cikk. Itt tovább gyengítjük a feltételeinket. Ehhez először vezessünk be egy új fogalmat:

18. Definíció (Singleton-defekt). *Egy $C = [n, k]_q$ lineáris kód Singleton-defektje $s(C) = n - k + 1 - d$, ahol $d = d_1(C)$ a kód minimális távolsága.*

Láthatjuk, hogy a Singleton-korlát miatt $s(C) \geq 0$ és $s(C) = 0$ pontosan akkor, ha C MDS kód.

19. Definíció (Almost-MDS kód). *Egy $C = [n, k]_q$ lineáris kódot almost-MDS kódnak nevezünk (röviden AMDS), ha $s(C) = 1$ (azaz $d_1(C) = n - k$).*

Az NMDS kódokkal ellentétben az AMDS kódok duálisa nem feltétlenül AMDS (viszont, ha mégis az, akkor a kód szükségképpen NMDS kód is egyben).

13. Állítás. *Egy $C = [n, k]_q$ lineáris kód pontosan akkor AMDS, ha a H paritásellenőrző mátrixában bármely $n - k - 1$ oszlopvektor lineárisan független, de van $n - k$ lineárisan összefüggő oszlopa.*

Bizonyítás. Mivel $s(C) = 1$, ezért $d(C) = n-k$, így az állítás a 3 állítás triviális következménye. □

13. Tétel (AMDS kód projektív geometriai megfelelője). *Legyen egy $C = [n, k]_q$ lineáris kód paritásellenőrző mátrixa H. Ekkor C egy AMDS kód akkor és csak akkor, ha a H paritásellenőrző mátrixának oszlopaira, mint $\mathrm{PG}(n-k-1, q)$-beli pontokra teljesül az, hogy bármely $n - k - 1$ pontja általános helyzetű, de van olyan hipersík, ami $n - k$ pontját tartalmazza.*

Bizonyítás. Az előbbi állítás miatt világos, hogy ha H oszlopait, mint $\mathrm{PG}(n - k - 1, q)$-beli pontokat reprezentáló vektorokat tekintjük, akkor az általuk meghatározott $S \subseteq \mathrm{PG}(n-k-1, q)$ ponthalmaz bármely $n-k-1$ különböző pontja általános helyzetű, de van köztük $n-k$, amelyek egy hipersíkra esnek.
Hasonlóan, ha adott $\mathrm{PG}(n - k - 1, q)$-ban egy olyan S ponthalmaz, aminek bármely $n - k - 1$ pontja általános helyzetű, akkor az ezeket reprezentáló oszlopvektorok egymás mellé írva egy AMDS kód paritásellenőrző mátrixát határozzák meg. □
Így AMDS kódok esetén is elég bizonyos projektív térbeli ponthalmazokat vizsgálnunk.

20. Definíció (n-track). *Egy n pontból álló $\mathrm{PG}(r, q)$-beli ponthalmazt, amelynek bármely r pontja általános helyzetű„n-track”-nek hívunk.*

Látjuk, hogy adott k-ra és q-ra a maximális méretű AMDS kód meghatározásához elég meghatározni a $\mathrm{PG}(n - k - 1, q)$-beli track-ek maximális méretét. Ezt $\mu'(k, q)$-val szokták jelölni.

Végül térjünk vissza egy kicsit az NMDS kódokhoz, vizsgáljuk meg az AMDS kódokkal való kapcsolatot. A következő állításból látszik, hogy ha n elég nagy, akkor tulajdonképpen az AMDS kódok is mind NMDS kódok.

14. Állítás. *Ha $n > k + q$, akkor minden $C = [n, k]_q$ lineáris AMDS kód NMDS kód is.*

Bizonyítás. Legyen $n > k + q$ és $C = [n, k]_q$ lineáris kód, amelyre $d_1(C) = n - k$, azaz C egy lineáris AMDS kód. Ekkor C-nek a H paritásellenőrző mátrixa a 13 állítás miatt kielégíti a 10 állításban szereplő N1 és N2 tulajdonságokat. Indirekt módon tegyük fel, hogy N3 tulajdonság

már nem igaz C-re, azaz $\exists\ n-k+1$ oszlop H-ban, legyenek ezek $h_1, h_2, \ldots, h_{n-k+1}$, amik által meghatározott mátrix rangja legfeljebb $n-k-1$. N1 miatt ez a rang pontosan $n-k-1$. Feltehetjük, hogy az első $n-k-1$ oszlop, $h_1, \ldots, h_{n-k-1}$, lineárisan független, azaz

$$h_{n-k} = \sum_{i=1}^{n-k-1} \alpha_i h_i,$$

$$h_{n-k+1} = \sum_{i=1}^{n-k-1} \beta_i h_i,$$

ahol $\alpha_i,\ \beta_i \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, $i = 1, 2, \ldots, n-k-1$ (hiszen ha valamelyik együttható 0 lenne, akkor lenne $n-k-1$ lineárisan összefüggő oszlop, ami ellentmondana N1-nek).
Most tekintsük az $\{\alpha_i \beta_i^{-1} : i = 1, 2, \ldots, n-k-1\}$ halmazt. Ez $\mathbb{F}_q \setminus \{0\}$-beli elemeket tartalmaz, és mivel a kezdeti feltétel miatt $n-k-1 > q-1$, ezért van köztük két egyforma: $\alpha_{i_1}\beta_{i_1}^{-1} = \alpha_{i_2}\beta_{i_2}^{-1} = \gamma \in \mathbb{F}_q^*$.
Tekintsük a

$$h_{n-k} - \gamma h_{n-k+1} = \sum_{i=1}^{n-k-1} (\alpha_i - \gamma\beta_i) h_i$$

kifejezést. A jobb oldalon legalább két együttható is 0, ami azt jelenti, hogy van $n-k-1$ lineárisan összefüggő oszlopa H-nak, ami N1 miatt ellentmondás. Tehát teljesül N3, azaz C egy NMDS kód. $\square$

Hivatkozások

[1] Kiss György, Szőnyi Tamás: *Véges geometriák,* Polygon Kiadó, Szeged, 2001.

[2] Szőnyi Tamás: *Szimmetrikus struktúrák,* Typotex Kiadó, 2013.

[3] S. Ball, M. Lawrauw: Arcs in finite projective spaces, *EMS Surveys in Mathematical Science,* 6 133–172, 2019.

[4] S. Ball, Zs. Weiner: *An Introduction to Finite Geometry,* 2011. https://web.mat.upc.edu/simeon.michael.ball/IFG.pdf (Letöltés dátuma: 2019.07.05.)

[5] S. Ball: *Finite Geometry and Combinatorial Applications,* London Mathematical Society Student Texts 82, Cambridge University Press, 2015.

[6] Csajbók Bence: Segre típusú módszerek véges projektív síkon, http://www.cs.elte.hu/~csajbokb/Segre_UNKP.pdf (Letöltés dátuma: 2019.07.03.)

[7] S. Ball: On sets of vectors of a finite vector space in which every subset of basis size is a basis, *J. Eur. Math. Soc.*, 14 733–748, 2012.

[8] S. Ball, J. De Beule: On sets of vectors of a finite vector space in which every subset of basis size is a basis II, *Des. Codes Cryptogr.*, 65 5–14, 2012.

[9] V. K. Wei: Generalized Hamming Weights for Linear Codes, *IEEE Trans. Inform. Theory* IT-37, 1412–1418, 1991.

[10] J. W. P. Hirschfeld, J. A. Thas: *General Galois Geometries,* Springer Monographs in Mathematics, 2016.

[11] S. M. Dodunekov, I. N. Landgev: On Near MDS Codes, *Journal of Geometry* Vol. 54, 30–43, 1995.

[12] S. M. Dodunekov, I. N. Landgev: Near-MDS codes over some small fields, *Discr. Math.* 213, 55–65, 2000.

[13] I. Landjev, A. Rousseva: The Main Conjecture for Near-MDS Codes, *WCC2015 - 9th International Workshop on Coding and Cryptography* Paris, 2015.

[14] V. Abatangelo, B. Larato: Elliptic near-MDS codes over $\mathbb{F}_5$, *Springer Science+Business Media, LLC* 167-174, 2007.

[15] M. A. De Boer: Almost MDS Codes, *Designs, Codes and Cryptography,* 9, 143-155, 1996.

[16] F. Hernando, G. McGuire: Proof of a conjecture of Segre and Bartocci on monomial hyperovals in projective planes, *Des. Codes Cryptogr.* 65, 275–289, 2012.

[17] S. Ball: Arcs in finite projective spaces, *Notes on Finite Geometry Summer School, University of Sussex,* June 26-30, 2017.

[18] S. Ball, M. Lawrauw: Arcs and tensors, *Designs, Codes and Cryptography*, 88, 17–31, 2020.

[19] D. G. Glynn: The non-classical 10-arc of PG(4, 9), *Discrete Mathematics* 59, 43-51, 1986.

[20] Szabó Izabella: A Segre-féle MDS-sejtés, http://www.math.u-szeged.hu/Geo/_site/index.php/educat/stud-essays-list/category/7-ba-thesis (Letöltés dátuma: 2019.07.03.)

[21] H. Lüneburg: *Translation planes,* Springer-Verlag. Berlin, Heidelberg 1980.

[22] B. Segre: Ovali e curve σ nei piani di Galois di caratteristica due, *Atti Accad. Naz. Lincei Rend.* 8, 32, 785–790, 1962.

[23] P. Vandendriessche: Classification of the Hyperovals in PG(2,64), *Electronic Journal of Combinatorics* 26, P.2.35, 2019.