Szegedi Tudományegyetem
Bolyai Intézet
Geometria Tanszék

A Segre-féle MDS-sejtés

BSc szakdolgozat

Készítette:
Szabó Izabella
matematika szakos
hallgató

Témavezető:
Dr. Nagy Gábor Péter
egyetemi docens

Szeged
2018

Tartalomjegyzék

1. Bevezetés

A világ hatalmas fejlődésen ment keresztül az elmúlt évszázadokban, és ez az információközlésen is meglátszik, ugyanis napjainkban rengeteg információ cserél gazdát másodpercenként, főleg a technológiának köszönhetően. Egy-egy üzenetküldés esetén pedig igen fontos, hogy nagy sebességgel, olcsón és hiba nélkül érjen el az üzenet, gondoljunk csak egy pendrive-ra vagy a nagy adatközpontokra.

A modern eljárásoknak köszönhetően ma már az üzeneteinket tömöríthetjük, ami a hatékony és hibamentes információközlést eredményez. Az üzenet tömörítése nem jelent mást, mint az üzenet lekódolását, és ennek köszönhetően kevesebb bitből áll majd, mint az eredeti. Amint a kódolt üzenet megérkezik, a címzett a kitömörítés után már meg is kapja az eredeti üzenetet. Néha viszont előfordulhat olyan, hogy zaj vagy egyéb tényező hatására, hibák lépnek fel az információközlés során, így dekódolás után a címzett nem a neki szánt üzenetet kapja meg, hanem annak egy változatát. Ekkor a kitömörítés általában már nem lehetséges. Ezekre az esetekre fejlesztették ki a hibajavító kódokat, amik egy adott üzenetben a hibák kontrollálására, azaz észlelésére, illetve kijavítására szolgálnak.

Richard Hamming úttörő volt ezen a területen, az 1950-es években ő találta fel az első hibajavító kódot, amit ma Hamming-kódnak hívunk. A hibajavító kódok lehetőséget adnak a címzetteknek, hogy anélkül találják meg a hibás biteket, hogy szükség lenne egy újabb csatornára, amin keresztül újra kellene küldeni az üzeneteket. Viszont ennek az az ára, hogy nagyobb sávszélességű csatornára van szükség. Tehát a hibajavító kódokat általában olyan esetekben használják, amikor az üzenetek újraküldése majdnem lehetetlen, például az egyirányú kommunikációnál. A hiányzó vagy megváltozott bitek, amik kijavíthatóak, függenek a hibajavító kódok felépítésétől, tehát különböző hibajavító kódok más-más esetekben a leghatékonyabbak. Egy jó hibajavító kódtól ugyanis elvárjuk, hogy kis valószínűsége legyen a hibás javításnak, a kódolás és dekódolás legyen gyors és egyszerű, illetve kicsi legyen a kontroll jelek aránya a hasznos bitekhez képest (redundancia).

Ez utóbbiaknak eleget tevő lineáris kódok egy széles osztályát alkotják az MDS-kódok. Már korán felismerték, hogy ezek kapcsolatban állnak bizonyos véges geometriai pont-konfigurációkkal. B. Segre, olasz matematikus, 1955-ben fogalmazta meg MDS-kódokra vonatkozó sejtését. Ezzel kapcsolatosan S. Ball, angol matematikus, 2011-ben ért el lényeges áttörést.

Szakdolgozatomban ismertetem az MDS-kódokat, a véges projektív terek íveivel való kapcsolatukat, magát a Segre-féle MDS-sejtést és S. Ball ide

vonatkozó eredményeit.

2. Alapfogalmak

2.1. Definíció. *A $(G;\circ)$ algebrai struktúrát csoportnak nevezzük, ha az alábbiak mindegyike teljesül:*

1. *G nemüres halmaz és zárt a $\circ : G^2 \longrightarrow G$ kétváltozós műveletre, azaz bármely $g_1, g_2 \in G : g_1 \circ g_2 \in G$;*
2. *$\circ$ művelet asszociatív, azaz bármely $g_1, g_2, g_3 \in G$-re teljesül, hogy $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$;*
3. *G-ben van egységelem, azaz létezik $e \in G$ úgy, hogy bármely $g \in G$: $g \circ e = e \circ g = g$;*
4. *G-ben minden elemnek van inverze, azaz bármely $g \in G$-re létezik $g^{-1} \in G$ úgy, hogy $g \circ g^{-1} = g^{-1} \circ g = e$.*

2.2. Definíció. *Abel-csoportnak nevezzük a $(G;\circ)$ csoportot, ha a $\circ$ művelet kommutatív, vagyis bármely $g_1, g_2 \in G : g_1 \circ g_2 = g_2 \circ g_1$.*

2.3. Definíció. *A $(T;+,\cdot)$ algebrai struktúrát testnek nevezzük, ha a következők teljesülnek:*

1. *$(T;+)$ Abel-csoport;*
2. *$(T\backslash\{0\};\cdot)$ Abel-csoport, ahol 0 a $(T;+)$ csoport egységelemét jelöli;*
3. *a szorzás disztributív az összeadásra, vagyis bármely $r_1, r_2, r_3 \in R$ esetén $r_1 \cdot (r_2 + r_3) = (r_1 \cdot r_2) + (r_1 \cdot r_3)$ és $(r_1 + r_2) \cdot r_3 = (r_1 \cdot r_3) + (r_2 \cdot r_3)$.*

A $(T;+)$ Abel-csoportot a test additív csoportjának, míg a $(T\backslash\{0\};\cdot)$ csoportot a test multiplikatív csoportjának nevezzük.

2.4. Definíció. *Egy T testet véges testnek nevezünk, ha T véges halmaz.*

Jelölje az $\overline{a}$ egész szám modulo p maradékosztályát. Rögzített p esetén a modulo p maradékosztályok halmazát $\mathbb{Z}_p$-vel jelöljük, azaz $\mathbb{Z}_p = \{\overline{0}, \overline{1}, ..., \overline{p-1}\}$. Megmutatható, hogy ha p tetszőleges prímszám, akkor $\mathbb{Z}_p$ testet alkot. Ekkor bármely prímhatványra, $q = p^n$, ahol p prímszám, n pedig pozitív egész szám, létezik egy q-elemű véges test, amit $\mathbb{F}_q$-val vagy $GF(q)$-val jelölünk.

2.5. Definíció. *Legyen V egy nemüres halmaz, $(T;+,\cdot)$ pedig test. V-t T feletti vektortérnek nevezzük, ha értelmezve van az alábbi két művelet, és teljesülnek az adott tulajdonságok:*

1. $+ : V \times V \longrightarrow V$ *az összeadás,* $(V;+)$ *Abel-csoport;*
2. $\cdot : T \times V \longrightarrow V$ *a skalárral való szorzás művelet, és ez disztributív az összeadásra nézve.*

2.6. Definíció. *Legyenek U és V tetszőleges vektorterek. Azt mondjuk, hogy $\varphi : U \longrightarrow V$ lineáris leképezés, ha a következők teljesülnek:*

1. *φ felcserélhető az összeadással, vagyis tetszőleges $u_1, u_2 \in U$ esetén $(u_1 + u_2)\varphi = u_1\varphi + u_2\varphi$;*
2. *φ felcserélehtő a skalárral való szorzással, vagyis tetszőleges $u \in U$ és $c \in \mathbb{R}$ esetén $(c \cdot u)\varphi = c \cdot (u\varphi)$*

2.7. Definíció. *Legyen V vektortér. Ekkor az invertálható lineáris leképezéseket lineáris transzformációknak nevezzük.*

2.8. Definíció. *Legyen V vektortér T test felett, $A, B \subseteq V$ tetszőleges halmazok. Azt mondjuk, hogy az A és B halmazok lineárisan ekvivalensek, ha létezik egy olyan $\varphi : V \longrightarrow V$ lineáris transzformáció, ami egyiket a másikba viszi.*

2.9. Definíció. *Legyen $(T;+,\cdot)$ test, $\alpha_1, \alpha_2, \ldots, \alpha_m \in T$. Vandermonde-mátrixnak nevezünk egy olyan $m \times n$-es mátrixot, ami a következő képpen épül fel:*

$$\begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_m & \alpha_m^2 & \cdots & \alpha_m^{n-1} \end{bmatrix}$$

Ha $m = n$, a mátrix determinánsa $\prod_{1 \le i \le j \le n} (\alpha_j - \alpha_i)$.

2.10. Definíció. *Ha T test és $F = T[x] \backslash T$, azaz ha F az összes nemkonstans polinomból álló halmaz, akkor az F polinomhalmaz T feletti felbontási testét a T test algebrai lezártjának nevezzük.*

3. Ívek a projektív síkon

A projektív geometriában beszélhetünk pontokról, egyenesekről és egy illeszkedési relációról. Ugyanúgy, mint az euklideszi geometriában, itt is teljesülnie kell néhány axiómának, amik a következőek:

1. Bármely két különböző ponthoz pontosan egy egyenes van, amelyre mindkét pont illeszkedik.
2. Bármely két egyeneshez pontosan egy pont létezik, amely mindkét egyenesre illeszkedik.
3. Létezik négy általános helyzetű pont, vagyis ezek közül a pontok közül semelyik három nem illeszkedik egy egyenesre.

3.1. Definíció. *A $\mathcal{P}$ projektív sík, mint illeszkedési rendszer, a $\mathcal{P} = (P, E, I)$ hármas, ahol P és E nemüres halmazok, $I \subseteq P \times E$ reláció, amik teljesítik a fent felsorolt axiomákat. Ekkor P elemeit pontoknak, E elemeit egyeneseknek, az I-t pedig illeszkedési relációnak nevezzük.*

A továbbiakban az egyszerűség kedvéért geometriai nyelvezetet használunk, vagyis egyenesek metszéspontjairól, összekötő egyenesekről, stb. beszélünk, illetve a projektív síkon levő egyeneseket azonosítjuk a rájuk illeszkedő pontok halmazával.

3.2. Definíció. *A $\mathcal{P} = (P, E, I)$ projektív sík véges, ha P véges halmaz.*

3.3. Tétel. *A $\mathcal{P}$ véges projektív síkon minden egyenes azonos számosságú.*

3.4. Definíció. *A $\mathcal{P}$ véges projektív sík rendje n, ha $\mathcal{P}$ bármely egyenesére $n+1$ pont illeszkedik.*

3.5. Definíció. *A q-adrendű véges projektív sík olyan véges projektív sík, amelyben pontosan q^2+q+1 pont és egyenes található, valamint minden egyenesen $q+1$ pont van, és bármely $q+1$ egyenes egy pontban metszi egymást.*

3.6. Definíció. *Egy illeszkedési struktúrában a K ponthalmazt ívnek nevezzük, ha bármely egyenes legfeljebb két K-beli pontot tartalmaz. Ha az ív k pontot tartalmaz, akkor k-ívről beszélünk. A K ív teljes, ha tartalmazásra nézve maximális.*

3.7. Definíció. *A sík valamely egyenese k-ívre nézve szelő, ha 2, érintő, ha 1 és külső egyenes, ha 0 közös pontja van a k-ívvel.*

3.8. Tétel (Bose-tétel). *A q-adrendű véges projektív síkon bármely K ívre teljesül:*

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

Bizonyítás. Vegyünk egy K ívet és rajta egy tetszőleges P pontot. Tekintsük az összes P-n átmenő egyenest (ezelből $q+1$ van), és ezek a P ponton kívül legfeljebb még egy pontot tartalmazhatnak. Vagyis $|K| \leq q+2$.

Tegyük fel, hogy $|K| = q+2$. Ekkor bármely $P \in K$, teljesül, hogy bármely P-re illeszkedő m egyenesen van P-től különböző pont, tehát K-nak nincsenek érintői. Ebből következik, hogy a P-n átmenő egyenesek vagy 0-szelők vagy 2-szelők. Tehát q páros.

Ha q páratlan, akkor $|K| = q+2$ nem fordulhat elő, így $|K| \leq q+1$. □

3.9. Definíció. *Ha T test feletti projektív síkról beszélünk, akkor a pontokat homogén számhármasoknak, $((x : y : z) \neq 0)$, az egyeneseket pedig homogén lineáris egyenleteknek, $(ax + by + cz = 0)$, tekintjük, valamint az illeszkedés relációt azonosítjuk a behelyettesítéssel. Ekkor a projektív síkot $PG(2, T)$-vel jelöljök.*

Ha $T = \mathbb{F}_q$, akkor $PG(2, q)$-ról beszélünk.

3.10. Definíció. *A projektív síkon másodrendű görbék alatt olyan görbéket értünk, amelyek megkaphatóak az*

$$F(X : Y : Z) = a_{11}X^2 + a_{22}Y^2 + a_{33}Z^2 + a_{12}XY + a_{13}XZ + a_{23}YZ = 0$$

homogén másodrendű egyenlettel.

3.11. Definíció. *$F(X : Y : Z) = 0$ irreducibilis másodfokú görbe, ha F irreducibilis polinom, azaz nem bomlik fel alacsonyabb fokú polinomok szorzatára.*

3.12. Példa. *Példák reducibilis másodrendű görbékre:*

1. $XY = 0$;
2. $X^2 + Y^2 = 0$ *reducibilis* $\mathbb{C}$ *felett,* $X^2 + Y^2 = (X + iY)(X - iY)$.

Példák irreducibilis másodrendű görbékre:

1. $X^2 - YZ = 0$;
2. $X^2 - Y^2 - Z^2 = 0$

3.13. Definíció. *Kúpszelet alatt olyan másodrendű görbét értük, amik irreducibilisek az alaptest algebrai lezártja felett.*

3.14. Tétel (Segre, 1955). *Ha q páratlan, akkor a $PG(2, q)$ sík $q+1$ méretű ívei pontosan az irreducibilis másodrendű görbék.*

4. MDS-kódok

Ebben a fejezetben, ahogy már a címe is említi, főleg *MDS*-kódokkal fogunk foglalkozni. Az *MDS*-kód név a "maximális távolságú szétválasztható kód (maximum distance separable code)" kifejezésből származik, vagyis az *MDS*-kódok esetében meghatározható a legnagyobb lehetséges távolság két kódszó között, rögzített k és n esetén, illetve a kódszavak szétválaszthatóak két részre: információt hordozó részre és kontroll jelekre.

4.1. Definíció. *Legyen Q "ábécé" véges halmaz. Ekkor $C \subseteq Q^n$ halmazt kódnak nevezzük. A kód hossza n, elemei pedig kódszavak.*

4.2. Definíció. *Legyen $\underline{x} = (x_1, x_2, \ldots, x_n)$ és $\underline{y} = (y_1, y_2, \ldots, y_n) \in Q^n$ két kódszó. A két kódszó Hamming-távolságán azon koordináták számát értjük, amelyeken a két kódszó különbözik egymástól, vagyis*

$$d_{Hamming} = d_H(\underline{x}, \underline{y}) = |\{i | i = 1, 2, \ldots, n; x_i \neq y_i\}|.$$

4.3. Definíció. *A $C \in Q^n$ kód minimális távolságán bármely két különböző kódszó Hamming-távolságának a minimumát értjük, vagyis*

$$d = d(C) = min\{d_H(\underline{x}, \underline{y}) | \underline{x}, \underline{y} \in C; \underline{x} \neq \underline{y}\}.$$

4.4. Definíció. *Legyen $\mathbb{F}_q$ véges test. Ha $C \subseteq \mathbb{F}_q^n$ altér, akkor C lineáris kód.*

A továbbiakban csak lineáris kódokkal foglalkozunk, azon belül is a $q = 2$ esettel, másnéven az n-hosszúságú bináris kódokkal.

4.5. Definíció. *Az $\underline{x} \in \mathbb{F}_q^n$ vektor Hamming-súlyán azon koordináták számát értjük, amelyeken a vektor különbözik a null-vektortól, vagyis*

$$wt(\underline{x}) = d_H(\underline{0}, \underline{x}) = |\{i | i = 1, 2, \ldots, n; x_i \neq 0\}|.$$

4.6. Tétel. *$C \leq \mathbb{F}_q^n$ lineáris kód esetén a minimum távolság*

$$d = d(C) = min\{wt(\underline{x}) | \underline{x} \in C \backslash \{0\}\}.$$

4.7. Definíció. *A $C \subseteq Q^n$ kód rátája $R = \frac{\log_q |C|}{n}$, ahol $q = |Q|$. Ha $C \leq \mathbb{F}_q^n$ lineáris kód, akkor a ráta $R = \frac{k}{n}$, ahol C dimenzióját k, míg C kódszavainak hosszát n jelöli.*

4.8. Definíció. *Legyen C lineáris kód $\mathbb{F}_q^n$ felett n, d, k paraméterekkel. Ekkor ha $\underline{c_1}, \underline{c_2}, \ldots, \underline{c_k}$ egy bázisa C-nek, akkor ezt a $k \times n$-es mátrixot, melynek i. sora éppen a $\underline{c_i}$ vektor, $(i = 1, 2, \ldots, k)$, C generátor mátrixának nevezzük, és G-vel jelöljük.*

A generátor mátrix ismeretében az összes kódszót ismerjük, azaz

$$C = \{\underline{x}G | \underline{x} \in \mathbb{F}_q^k\}.$$

4.9. Definíció. *Legyen C lineáris kód $\mathbb{F}_q^n$ felett n, d, k paraméterekkel. Ekkor az $(n-k) \times n$-es H mátrixot paritás-ellenőrző mátrixnak nevezzük, ha $\underline{x} \in \mathbb{F}_q^n$ akkor és csak akkor kódszó, ha $H\underline{x}^\top = \underline{0}$.*

Tehát a paritás-ellenőrző mátrix ismeretében eldönthető egy vektorról, hogy kódszó-e vagy sem.

4.10. Tétel (Singleton-korlát)**.** *Legyen $C \subseteq Q^n$. Ha C minimális távolsága d, akkor teljesül a következő egyenlőtlenség*

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

4.11. Definíció. *Egy C kódot MDS-kódnak nevezünk, ha teljesíti a Singleton-korlát egyenlőségét, vagyis*

$$d = n - k + 1.$$

4.12. Állítás. *Lineáris kódok esetében a kód minimális távolsága pontosan a paritás ellenőrző mátrixban a lineárisan összefüggő oszlopok minimális száma.*

Bizonyítás. Azt kell megmutatnunk, hogy a H mátrix k különböző $i_1, \ldots, i_k$ oszlopa pontosan akkor lineárisan összefüggő, ha van olyan nemnulla $\underline{x}$ kódszó, amelyben a nemnulla koordináták indexei az $\{i_1, \ldots, i_k\}$ halmazba esnek.

Az $\underline{x} \in C$ kódszó súlya legyen k. Mivel $H\underline{x}^\top = \underline{0}$, ezért H-nak van k oszlopa, melyek lineárisan összefüggőek.

Fordítva, ha H-nak van k lineárisan összefüggő oszlopa, akkor az ezek közti $x_{i_1}h_{i_1} + \ldots + x_{i_k}h_{i_k} = 0$ lineáris összefüggést mátrixalakba írva egy olyan nemnulla, és legfeljebb k súlyú $\underline{x}$ vektorhoz jutunk, melyre $H\underline{x}^\top = \underline{0}$, azaz amely benne van C-ben.

Tehát pontosan akkor van C-ben legfeljebb k súlyú kószó, ha H-ban van k darab lineárisan összefüggő oszlop. Ez azt jelenti, hogy ha C minimális távolsága d, akkor H-nak minden $d-1$ oszlopa lineárisan független, de van d darab lineárisan összefüggő oszlopa.

□

4.13. Tétel. *Az $(n-k) \times n$-es H mátrix akkor és csak akkor egy MDS-kód paritás ellenőrző mátrixa, ha H bármely $n-k$ oszlopa lineárisan független.*

Bizonyítás. Legyen C MDS-kód n, d, k paraméterekkel és H paritás ellenőrző mátrixszal. Ekkor $d = n - k + 1$ és a 4.12 Állítás szerint H-nak nincs $n - k$ lineárisan függő oszlopa.

Fordítva, ha C nem MDS-kód, akkor $d \leq n - k$, azaz ismét a 4.12 Állítást alkalmazva találhatunk $n - k$ darab lineárisan független oszlopot H-ban. □

4.14. Definíció. *Egy C kód duálisán a következő lineáris kódot értjük:*

$$C^{\perp} = \{\underline{v} \cdot \underline{x} = \underline{0} | \forall \underline{x} \in C; \underline{v} \in \mathbb{F}_q^n\}.$$

4.15. Tétel. *MDS-kód duálisa is MDS-kód, vagyis a generátor mátrix és a paritás ellenőrző mátrix szerepe felcserélődik.*

Bizonyítás. Legyen $C \in \mathbb{F}_q^n$ egy kód. Azt kell megmutatnunk, hogy C lineáris kód MDS-kód, akkor és csak akkor, ha a G generátor mátrixának bármely k darab oszlopa lineárisan független.

Tekintsük a $k \times n$-es G generátor mátrixot. Tegyük fel, hogy $i_1, i_2, \ldots, i_k$ oszlopai lineárisan függőek. Ekkor léteznek $a_1, a_2, \ldots, a_k \in \mathbb{F}_q$, úgy hogy

$$a_1 x_{i_1} + a_2 x_{i_2} + \cdots + a_k x_{i_k} = 0$$

teljesül bármely $\underline{x} \in C$ vektorra. Vagyis az i_k-dik oszlop előáll az $i_1, \ldots, i_{k-1}$ oszlopok lineáris kombinációjaként, azaz bármely C-beli $\underline{x}$ kódszóra, az x_{i_k} koordináta kikombinálható az $x_{i_1}, x_{i_2}, \ldots, x_{i_{k-1}}$ koordinátákból.

Legyen $U = C \cap \{x_{i_1} = x_{i_2} = \ldots = x_{i_{k-1}} = 0\}$ altér. Ez megadható $(n-k) + (k-1) = n - 1$ egyenlettel, amiből következik, hogy $\dim U \geq 1$, vagyis létezik $\underline{y} \in U \backslash \{0\}$.

Az $y_{i_k} = 0$, mert kikombinálható az $y_{i_1}, y_{i_2}, \ldots, y_{i_{k-1}}$ koordinátákból. Innen következik, hogy $wt(\underline{y}) \leq n - k = d - 1$, ami ellentmond a d minimális távolság definíciójának. □

Legyen $C \leq \mathbb{F}_q^n$ lineáris kód. Tudjuk, hogy C két féle képpen is megadható:

1. k darab generátorral, vagyis egy $k \times n$-es mátrixszal (ez C generátor mátrixa);

2. $n - k$ darab homogén lineáris egyenlettel, vagyis egy $(n - k) \times n$-es mátrixszal (ez C paritás ellenőrző mátrixa).

A 4.15 tétel alapján tudjuk, hogy C generátor mátrixa éppen a duális kód paritás-ellenőrző mátrixa, és fordítva.

Tegyük fel, hogy C MDS-kód. Használva az eddigi észrevételeinket és a 4.12 Állítást, kapjuk, hogy C minimális távolsága $d = n - k + 1$, míg $C^{\perp}$ minimális távolsága $d = k + 1$. Ez azt is jelenti, hogy $C^{\perp}$ paritás ellenőrző mátrixában minden $d - 1 = k$ oszlop lineárisan független.

Ilyen módon C-hez hozzárendelhetjük az $S \subseteq \mathbb{F}_q$ halmazt, mint C paritás ellenörző mátrixának oszlopvektorait. Ekkor azt kapjuk, hogy bármely ilyen $S \subseteq \mathbb{F}_q$ halmazban minden k-elemű részhalmaz bázis.

5. Segre-féle MDS-sejtés

Ebben a fejezetben ismertetjük a [2] cikket.

Legyen S egy vektorhalmaz $\mathbb{F}_q^k$-ban olyan módon, hogy S minden k-elemű részhalmaza bázis. Ekkor bizonyított tény, hogy S maximális elemszáma $q+1$, ha $k \leq p$, és $q+k-p$, abban az esetben, ha $q \geq k \geq p+1 \geq 4$, ahol $q = p^h$ és p prím. Sőt, ha $k \leq p$, S maximális elemszáma osztályozva van, amit Beniamino Segre általánosított.

Ezeknek az eredményeknek többféle interpretációja is van. Az egyik ilyen, hogy egy $k \times (p+2)$-es mátrixnak, ahol $k \leq p$ és a mátrix elemei $\mathbb{F}_p$-ből vannak, van k darab oszlopa, amik lineárisan függőek. A másik, hogy igaz a lentebb olvasható sejtés az MDS-kódokra prím testek esetén; vagyis nincs MDS-kód $\mathbb{F}_p$ felett, aminek a dimenziója legfeljebb p, ami hosszabb, mint a Reed-Solomon kódok. Az osztályozás arra is utal, hogy az MDS-kódok, amiknek a dimenziója korlátozva van a test karakterisztikájától, csak Reed-Solomon kódok lehetnek.

Legyen S egy vektorhalmaz $\mathbb{F}_q^k$-ban olyan módon, hogy bármely k-elemű részhalmaza bázis.

Ebben a cikkben megmutatjuk, hogy S elemszámának létezik egy felső korlátja, $k \leq p$ esetén, ahol $q = p^h$ és p prím, úgy hogy a példáink ekvivalensek a következővel.

5.1. Példa. *Az*

$$S = \{(1, t, t^2, ..., t^{k-1}) | t \in \mathbb{F}_q\} \cup \{(0, ..., 0, 1)\}$$

egy $q+1$ elemű halamaz. Könnyen belátható, hogy S-nek van k darab vektorból álló Vandermonde-mátrixa, aminek a determinánsa nem 0.

5.2. Lemma. *Legyen S egy vektorhalmaz $\mathbb{F}_q^k$-ban olyan módon, hogy bármely k-elemű részhalmaza bázis. Ekkor S maximális elemszáma $q + k - 1$.*

Bizonyítás. Tekintsük, a $(k-2)$-dimenziós U alteret S-ben. Ekkor bármely $q+1$ hipersík, ami tartalmazza U-t, tartalmaz legalább még egy vektort S-ből. Tehát $|S| \leq k-2+q+1 = q+k-1$. □

5.3. Lemma. *Legyen S egy vektorhalmaz $\mathbb{F}_q^k$-ban, $k \geq q$, olyan módon, hogy S bármely k-elemű részhalmaza bázis. Ekkor S maximális elemszáma $k+1$. Azok a halmazok, amelyeknek az elemszáma eléri ezt a határt, ekvivalensek*

$$\{(\lambda_1, 0, ..., 0), (0, \lambda_2, 0, ..., 0), ..., (0, ..., 0, \lambda_k), (1, ..., 1)\}$$

-el.

Bizonyítás. A megfelelő bázis megválasztása után, feltételezhetjük, hogy

$$S \supseteq S' = \{(\lambda_1, 0, ..., 0), (0, \lambda_2, 0, ..., 0), ..., (0, ..., 0, \lambda_k), (1, ..., 1)\}$$

valamilyen $\lambda_i \in \mathbb{F}_g \backslash \{0\}$. Tegyük fel, hogy létezik $x \in S \backslash S'$. Mivel $k \geq q$, ezért két eset lehetséges. Az első, hogy létezik két koordináta x-ben, az i-dik és a j-dik, amik egyenlőek. Ekkor az $X_i = X_j$ egyenlet által meghatározott hipersík tartalmaz k darab S-beli vektort. A második esetben x valamelyik koordinátaja, mondjuk az i-dik, 0. Ebben az esetben az $X_i = 0$ egyenlet által meghatározott hipersík szintén k darab S-beli vektort tartalmaz. Tehát mindkét esetben ellentmondásra jutottunk, vagyis $S = S'$. □

5.4. Sejtés. *Legyen S egy vektorhalmaz $\mathbb{F}_q^k$-ban olyan módon, hogy bármely k-elemű részhalmaza bázis, $k \leq q$. Ekkor S maximális elemszáma $q+1$. Abban az esetben, ha q páros és $k = 3$ vagy $k = q-1$, akkor pedig $q+2$.*

Jelen esetben mi a $k \leq p+1$, ahol $q = p^k$ és p prím, esetet fogjuk vizsgálni. Ebben az esetben a sejtés biztosan igaz bármely q prímre.

A sejtést már belátták bármely $q \leq 27$-re, és $k \leq 5$, bármely $k \geq q-3$ és $k = 6, 7, q-4, q-5$-re néhány kivétellel.

Ha $p = 2$ és $q = 3$, hozzáadva a (0,1,0) vektort az 5.1. Példához, egy $q+2$ elemű példát kapunk. Ezekkel a paraméterekkel rendelkező $q+2$ elemű halmazokat *hiperoválisoknak* nevezzük. Sok olyan példát tudunk, ami nem ekvivalens az 5.1. Példával, az elsőt Segre találta meg.

Olyan $q+1$ elemű halmazok, amelyek nem ekvivalensek az 5.1. Példával a következőek:

5.5. Példa. *Az*

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

egy 10 elemű halmaz $\mathbb{F}_9^5$-ben, úgy hogy $\eta^4 = -1$.

5.6. Példa. *Az*

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

egy $q+1$ elemű halmaz $\mathbb{F}_q^4$-ban, úgy hogy $q = 2^h$ és $(r, h) = 1$.

Legyen S egy halmaz $\mathbb{F}_q^k$-ban. Ekkor minden példa meghatároz egy újabb S elemszámú példát $\mathbb{F}_q^{|S|-k}$-ban valamilyen eljárás útján. Például a hiperoválisok meghatároznak nekünk $q+2$ elemszámú példákat $\mathbb{F}_q^{q-1}$-ben.

Sok hasonló felső határt ismerünk $|S|$-re, mint amit mi is vizsgálunk. Ami releváns a mi esetünkhez, azt Voloch állapította meg, mégpedig, hogy ha $3 \leq k \leq q/45 + c_1$, ahol q prím és c_1 konstans, akkor $|S| \leq q+1$. Szintén fontos számunkra q prímhatvány esetén, ha $3 \leq k \leq \sqrt{q}/4 + c_2$, ahol q egy páratlan négyzetszám és c_2 konstans, akkor $|S| \leq q+1$.

Ha k eggyel kevesebb, mint S felső határa és $|S| = q+1$, akkor S ekvivalens az 5.1. Példához. Minden osztályozás $|S| = q+1$-re Segre tételét alkalmazza, vagyis ha $|S| = q+1$ és $p \geq k = 3$, akkor S ekvivalens az 5.1. Példával.

Segre az érintőkre vonatkozó tétel segítségével bebizonyította, hogy ha $k = 3$ és q páros, akkor létezik egy $t = q + k - 1$-fokú ív, amely a duális térben tartalmazza az összes vektort, amik megfelelnek az érintők hipersíkjainak. Ha q páratlan, akkor pedig egy $2t$-fokú ív létezik, ugyanezekkel a tulajdonságokkal, és a metszéspontok száma a hipersíkokkal és S duális vektoraival 2.

6. S. Ball eredményei a Segre-sejtésről

Végezetül ismertetjük S. Ball [2] cikkének fő eredményeit. Megjegyezzük, hogy az eredmények egy része tovább lett fejlesztve S. Ball és J. de Beule [3] cikkében.

Legyen $q = p^h$, ahol p prím.

6.1. Tétel (S. Ball, 2011)**.** *Legyen S egy vektorhalmaz $\mathbb{F}_q^k$-ban olyan módon, hogy bármely k-elemű részhalmaza bázis. Ekkor S maximális elemszáma $q + k + 1 - min(k, p)$, ahol $k \leq q$.*

6.2. Tétel (S. Ball, 2011)**.** *Ha $p \geq k$, akkor egy $q+1$ elemű S vektorhalmaz $\mathbb{F}_q^k$-ban olyan módon, hogy bármely k-elemű részhalmaza bázis, ekvivalens az 5.1. Példával.*

6.3. Tétel (S. Ball, 2011)**.** *Legyen S egy vektorhalmaz $\mathbb{F}_q^k$-ban olyan módon, hogy bármely $k \geq 4$-elemű részhalmaza bázis, ahol $q \geq k \geq p$. Ekkor S maximális elemszáma $q + k - p$.*

6.4. Tétel (S. Ball, 2011)**.** *Legyen S egy vektorhalmaz $\mathbb{F}_q^k$-ban olyan módon, hogy bármely k-elemű részhalmaza bázis, ahol $3 \leq q - p + 1 \leq k \leq q - 2$. Ekkor S maximális elemszáma $q + 1$. Sőt, ha teljesül az egyenlőség, S ekvivalens az 5.1 Példával.*

Hivatkozások

[1] Y. Achnine, *On the main conjecture on algebraic-geometric MDS codes*, Mathematisch Instituut, Universiteit Leiden, 2011 Link 2018.05.14

[2] 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. (JEMS)* 14 (2012), no. 3, 733–748.

[3] S. Ball and 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 (2012), no. 1-2, 5–14.

[4] Czédli Gábor, *Csoportok és testek (előadásjegyzet)*, Szegedi Tudományegyetem, 2017.

[5] Hajnal Péter, *Szimmetrikus kombinatorikus struktúrák MSc hallgatók számára (előadásjegyzet)*, Szegedi Tudományegyetem, 2013. Link 2018.05.07.

[6] Hajnal Péter, *Halmazrendszerek MSc hallgatók számára (előadásjegyzet)*, Szegedi Tudományegyetem, 2011. Link 2018.05.07.

[7] Kiss György és Szőnyi Tamás, *Véges geometriák*, Polygon Könyvtár, Szeged, 2001.

[8] Nagy Gábor Péter, *Véges geometriák és kódok (előadásjegyzet)*, Szegedi Tudományegyetem, 2017.

[9] Szendrei Mária, *Lineáris algebra (előadásjegyzet)*, Szegedi Tudományegyetem, 2015.

[10] Wettl Ferenc, *Kódelmélet és kriptográfia (előadásjegyzet)*, BME, 2011. Link 2018.05.07.

[11] Error correction code, Wikipedia Link 2018.05.14.

Nyilatkozat

Alulírott Szabó Izabella kijelentem, hogy a szakdolgozatban foglaltak saját munkám eredményei, és csak a hivatkozott forrásokat (szakirodalom, eszközök, stb.) használtam fel. Tudomásul veszem, hogy szakdolgozatomat a Szegedi Tudományegyetem könyvtárában a kölcsönözhető könyvek között helyezik el, és az interneten is nyilvánosságra hozhatják.

Szeged, 2018. május 24. .....

aláírás