Eötvös Loránd Tudományegyetem
Természettudományi Kar
Geometriai Tanszék

Véges terekből származó Grassmann-kódok

Szakdolgozat

Témavezető:
Kiss György
egyetemi docens

Készítette:
Pituk Sára
matematika BSc

Budapest, 2020

NYILATKOZAT

Név: Pituk Sára
ELTE Természettudományi Kar, szak: matematika Bsc
NEPTUN azonosító: AE7FG5
Szakdolgozat címe: Véges terekből származó Grassmann-kódok

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. május 28.

Pituk Sára

a hallgató aláírása

Köszönetnyilvánítás

Szeretnék köszönetet mondani témavezetőmnek, Kiss Györgynek a sok segítségért, amit a szakdolgozatom írása során tőle kaptam, valamint azért, hogy a Geometria előadások során megszerettette velem ezt a területet. Köszönöm a hasznos észrevételeket, tanácsokat, melyekkel ellátott, a gyors és körültekintő válaszokat, a dolgozatom alapos átnézését, a biztató szavakat és azt, hogy mindig számíthattam rá.

Köszönettel tartozom a Matematika Intézet oktatóinak azért a lelkiismeretes munkáért, amellyel a hallgatók képzését végzik és motiváló légkört teremtenek.

Szeretném megköszönni a családomnak és barátaimnak a támogatásukat. Külön köszönet illeti Édesapámat, akinek matematika iránti szeretete ösztönzőleg hatott rám.

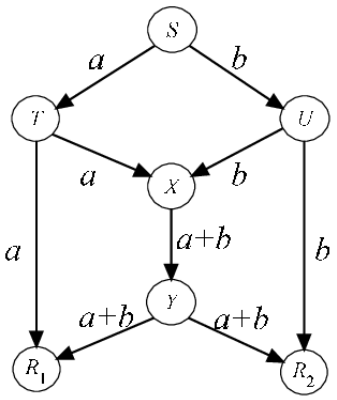
S.D.G.

Tartalomjegyzék

1. Bevezetés

Képzeljük el, hogy van egy hálózatunk (egy irányított gráf, az élein kapacitásokkal), és ki van jelölve benne néhány forrás és nyelő. A forrásoktól a nyelőkhöz szeretnénk eljuttatni bizonyos objektumokat a hálózaton keresztül. A max-flow=min-cut tétel [14] szerint az egyszerre szállítható információ mennyiségére a minimális vágás mérete ad felső korlátot, és ekkora nagyságú folyamot könnyen találhatunk a Ford-Fulkerson algoritmussal [14].

A hálózatok egy viszonylag új alkalmazási területe az interneten történő információtovábbítás. Az ehhez használt kommunikációs hálózatokban a forrásokat adóknak, a nyelőket pedig vevőknek hívjuk. Az egyik cél maximalizálni azt az információmennyiséget, ami az összes vevőhöz eljut. Előfordulhat, hogy mindegyikhez külön-külön eljuttatható lenne a kívánt mennyiségű információ, ha a többi vevőről elfeledkeznénk, azonban ha a forrástól hozzájuk vezető utak nem (él-)diszjunktak, ez nem valósítható meg egyidejűleg. Erre a problémára kínál megoldást a hálózati kódolás elmélete. Míg a klasszikus folyamfeladatban minden csúcs a bemenő élein érkező csomagokat továbbítja más csúcsoknak, a hálózati kódolás során a csúcsok különböző bitsorozatokat kapnak a bemenő éleiken, ezekkel műveleteket végezhetnek – például, ha lineáris hálózati kódolásról beszélünk, kiszámíthatják valamilyen (előre megadott vagy véletlenszerű) lineáris kombinációjukat – és az így kapott vektort (kódot) továbbítják az összes szomszédjuknak. Az alábbi ábrán [4] látszik ennek a folyamata. A hálózatban minden él kapacitása 1, és az a és b csomagokat szeretnénk S-ből R_1-be és R_2-be is eljuttatni. Látható, hogy hagyományos hálózati folyamként ez nem lehetséges. (4 csomagot szeretnénk célba juttatni, de van egy 3 méretű vágás a gráfban.) Azonban egy egyszerű kódolással az (X, Y) élen megoldható a feladat.



Tegyük fel, hogy a gráf, amit vizsgálunk, aciklikus, és minden él kapacitása 1. Ha egyetlen forrás (s) és nyelő (t) van kijelölve, akkor Menger tétele [14] szerint pontosan akkor létezik k nagyságú folyam s-ből t-be, ha vezet s és t között k éldiszjunkt (irányított) út. Ha s az egyetlen forrás, és az összes többi csúcs nyelő, akkor k éldiszjunkt út helyett k éldiszjunkt s gyökerű feszítő fenyőre van szükség ahhoz, hogy mindegyik nyelőhöz k csomagot küldhessünk egy időben. (Edmonds tétele, [5].) Általános esetben, amikor az s-en kívüli csúcsoknak csak egy T részhalmaza van kijelölve nyelőnek, annak, hogy k

csomagot el tudjunk juttatni s-ből T minden pontjába, elégséges feltétele, hogy létezzen a gráfban k éldiszjunkt s gyökerű fenyő, melynek levelei pontosan a T-beli csúcsok. A maximális ilyen k megtalálása, amit a hálózat kapacitásának nevezünk, NP-nehéz feladat, és a Steiner-fa problémára vezethető vissza. Kódolással azonban jelentősen növelhető a hálózat kapacitása, és ráadásul polinomiális időben elérhető a maximum.

Álljon a hálózatunk k adóból $(s_1, s_2, \ldots, s_k)$ és N vevőből $(r_1, r_2, \ldots, r_N)$. Ezzel ekvivalens hálózatot kapunk, ha felveszünk egy további S csúcsot, amiből minden s_i-be $(1 \leq i \leq k)$ vezet egy irányított él. Ezért elég azt az esetet vizsgálni, amikor egyetlen adó van, amiből k csomagot (n hosszú $\mathbb{F}_q$ feletti vektort) szeretnénk továbbítani. Mostantól a lineáris hálózati kódolással foglalkozunk, mert ebben az esetben jól le tudjuk írni, hogy hogyan valósul meg az információszállítás.

Egy csúcs *lokális kódoló vektora* az a vektor, amely a bemenő éleken érkező vektorokból számított lineáris függvény együtthatóiból áll. Természetesen a kiszámított érték az S-ből érkező k vektor lineáris kombinációjaként is felírható, az ebben a felírásban szereplő együtthatók alkotják az adott csúcs *globális kódoló vektorát*. A hálózatot *megoldhatónak* nevezzük, ha léteznek olyan kódoló vektorok az éleken, hogy minden vevő dekódolni tudja az üzenetet a bemenő élein érkező csomagokból.

Ha az S-beli input vektorokat egymás alá írjuk, egy $k \times n$-es X mátrixot kapunk. Minden r_j vevőhöz tartozik egy A_j $k \times k$-as átviteli mátrix, ami kiszámítható az r_j-be vezető út mentén számított lineáris függvényekből, és r_j az $Y = A_j X$ output mátrixot kapja meg. Ebből ki kell tudnia számítani X-et, ezért elvárjuk a hálózattól, hogy A_j invertálható legyen $(1 \leq j \leq N)$. Ez teljesül, ha $\prod_{j=1}^{N} \det A_j \neq 0$. Ez a szorzat a kódoló vektorok együtthatóinak egy p polinomja. Ha $q > \deg(p)$, akkor vannak olyan $\mathbb{F}_q$-beli elemek, amelyeket p változóinak helyére írva a polinom értéke nem 0. Így tehát a hálózat megoldható, ha az alaptest elég nagy.

Azt is megtehetjük, hogy nem adjuk meg előre a kódoló vektorokat, hanem minden csúcs egy véletlen lineáris kombinációt választ (függetlenül, $\mathbb{F}_q$ felett egyenletes eloszlás szerint), és azt alkalmazza a beérkező csomagokra. Ha ez kellően nagy test felett történik, és a hálózat megoldható, akkor nagy valószínűséggel az így kapott kódoló vektorok is megoldják. Pontosabban, ha a hálózatban C közbülső csúcs van, akkor annak a valószínűsége, hogy mind az N vevő dekódolni tudja az üzenetet, legalább $(1-\frac{N}{q})^{Ck}$ [10]. Amikor ezt a módszert alkalmazzuk, akkor *random lineáris hálózati kódolásról* beszélünk.

A kommunikáció során merülhetnek fel hibák. Ezek származhatnak a csatorna nem megfelelő működéséből, abból, hogy a minimális vágás mérete nem elég nagy, de egy harmadik személy is helyezhet el az üzenetben csomagokat. Formálisan az utóbbit így írhatjuk le (egy adó és egy vevő esetén): Az adó az $X \in \mathbb{F}_q^{k \times n}$ üzenetet szeretné elküldeni az A átviteli mátrix segítségével. Ám a vevő AX helyett egy $AX + BE$ mátrixot kap, ahol E az a $t \times n$-es mátrix, melynek sorai a zavaró személy által elhelyezett t csomagot reprezentálják, BE pedig ennek a kódolt változata. *Koherens* hálózati kódolás esetén a vevő ismeri az A mátrixot, így ennek segítségével tudja megfejteni az üzenetet. A *nem koherens* modellben viszont A egy olyan véletlen mátrix, amit sem az adó, sem a vevő nem ismer. Ezért ilyenkor érdemes az üzenetre nem n darab vektorként, hanem az azok által generált lineáris altérként gondolni. Így jutunk el ennek a dolgozatnak a témájához,

az *altér kódokhoz*, amelyek közül is a legfontosabbak a konstans dimenziójú altér kódok, vagyis a *Grassmann-kódok*.

Egy vektortér lineáris altereire tekinthetünk egy eggyel alacsonyabb dimenziós projektív tér projektív altereiként. Így geometriai eszközök segítségével nyerhetünk pontosabb képet az altér kódok szerkezetéről. A dolgozatban több helyen fogunk találkozni ezzel a megközelítéssel, például látni fogjuk, hogy a Grassmann-kódok közeli kapcsolatban állnak a véges projektív terek befedéseivel. Egyébként a kódelmélet véges geometriával való kapcsolata a hálózati kódolás megjelenésénél jóval régebbre nyúlik vissza – elég csak a híres MDS-sejtésre vagy a Reed-Muller kódokra gondolnunk [16].

Miután a jelen bevezető szakaszban a [7] forrást felhasználva bemutattuk az altér kódok vizsgálatának fő motivációját, a szakdolgozat hátralevő része a következőképpen épül fel:

A 2. fejezetben összegyűjtjük azokat a projektív geometriai, illetve kódelméleti fogalmakat és összefüggéseket, amelyekre később szükségünk lesz. Az ebben a fejezetben szereplő definíciók és állítások nagyrészt a [3] és [16] tankönyvekből származnak. Ezalól kivételt képez az elliptikus, hiperbolikus, valamint parabolikus kongruenciák definíciója, melyeknek forrása [9].

A 3. fejezetben definiáljuk a Grassmann-sokaságot és a Grassmann-koordinátákat, majd bevezetünk kétféle metrikát az alterek halmazán, és ezek segítségével jellemezzük a Grassmann-sokaság gömbjeit. Ezeknek az eredményeknek az üzenetek dekódolásában van jelentősége. Az itt leírtak a [21] cikkből származnak.

A 4. fejezetben a [18] forrást felhasználva kicsit közelebbről megvizsgáljuk, hogy miként történik a hibajavító kódolás altér kódokkal. Ezután ismertetünk néhány klasszikus kódelméleti alsó és felső korlátot, valamint ezek Grassmann-kódokra vonatkozó megfelelőit. A korlátokról szóló alfejezetekben a forrásokra az állításoknál hivatkozunk.

Az 5. fejezetben olyan konstrukciókat fogunk látni Grassmann-kódokra, amelyekből újabb korlátokat kapunk ezen kódok maximális méretére. Ebben a fejezetben a három alfejezet forrásai sorra a [2] és [7], a [13] és [20], valamint az [1] cikkek.

Végül pedig egy táblázatban szemléltetjük, hogy nem túl nagy paraméterértékekre a dolgozatban tárgyalt alsó és felső korlátok hogyan viszonyulnak a valódi maximális méretekhez, amelyek a [23] adatbázisban szerepelnek. A korlátok értékeinek kiszámolásához használt Python kód megtalálható a táblázat után.

2. Alapfogalmak

2.1. Véges projektív terek

A q elemű $\mathbb{F}_q$ véges testtel koordinátázott $PG(n-1,q)$ *véges projektív teret* a $V(n,q)$ $\mathbb{F}_q$ feletti n-dimenziós vektortérből úgy konstruáljuk meg, hogy $PG(n-1,k)$ i-dimenziós projektív altereit $V(n,q)$ $(i+1)$-dimenziós lineáris altereivel azonosítjuk. Tehát $V(n,q)$ 1-dimenziós alterei lesznek a projektív tér *pontjai*, a $V(n,q)$ 2-dimenziós alterei a projektív tér *egyenesei*, ..., $V(n,q)$ $(n-1)$-dimenziós alterei pedig a projektív tér $(n-2)$-dimenziós alterei. Ez utóbbiakat *hipersíkoknak* is szokás nevezni.

$PG(n-1,q)$ pontjait *homogén koordináták* segítségével adhatjuk meg, amelyeket a következő módon kapunk: Legyen $V(n,q)$-nak egy bázisa $\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_n}$. Egy rögzített P projektív ponthoz vegyünk egy őt reprezentáló $V(n,q)$-beli vektort, azaz a P-nek megfelelő origón átmenő egyenesnek egy generátorát ($\mathbf{p}$). Ez a vektor egyértelműen felírható az $\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_n}$ bázisvektorok lineáris kombinációjaként alkalmas $a_1, a_2, \ldots, a_n \in \mathbb{F}_q$ együtthatókkal, amelyek közül nem mind 0:

$$\mathbf{p} = \sum_{k=1}^{n} a_k \mathbf{e_k}.$$

Mivel a P pontot reprezentáló $\mathbf{p}$ vektor nemnulla skalárszorzó erejéig egyértelműen meg van határozva, ez igaz a felírásban szereplő $a_1, a_2, \ldots, a_n$ együtthatókra is. Tekintsük az alábbi ekvivalenciarelációt az $\mathbb{F}_q$-beli testelemekből álló rendezett n-esek halmazán:

$$(x_1, x_2, \ldots, x_n) \sim (y_1, y_2, \ldots, y_n) \Leftrightarrow \exists \lambda \in \mathbb{F}_q \backslash \{0\} \colon y_i = \lambda x_i \quad (1 \leq i \leq n).$$

A P ponthoz hozzárendelve az $(a_1, a_2, \ldots, a_n)$ ekvivalenciaosztályát kölcsönösen egyértelmű megfeleltetést kapunk $PG(n-1,q)$ pontjai és a $\sim$ szerinti ekvivalenciaosztályok között, ha az utóbbiak közül kizárjuk a csupa 0-ból álló n-eshez tartozó (egyelemű) ekvivalenciaosztályt. Ez a leképezés adja a projektív tér egy homogén koordinátázását. Az $(a_1, a_2, \ldots, a_n)$ ekvivalenciaosztályára az $(a_1 \colon a_2 \colon \ldots \colon a_n)$ jelölést használjuk. Mivel a fenti koordinátázás függ a $V(n,q)$-beli bázis választásától, sok különböző homogén koordinátarendszer van, amelyek egymásba vihetők, ha $V(n,q)$-ban egy megfelelő lineáris transzformációt alkalmazunk.

A konstrukcióból látszik, hogy k darab $PG(n-1,q)$-beli pont pontosan akkor illeszkedik egy legfeljebb $(k-2)$-dimenziós projektív altérre, ha az őket reprezentáló k vektor lineárisan összefüggő $\mathbb{F}_q^n$-ben.

2.1. Állítás. *$V(n,q)$ k-dimenziós altereinek - és így $PG(n-1,q)$ $(k-1)$-dimenziós projektív altereinek - száma*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{(q^n-1)(q^{n-1}-1)\ldots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\ldots(q-1)}.$$

2.2. Definíció. Ezt a mennyiséget *Gauss-féle binomiális együtthatónak* nevezzük.

A hagyományos binomiális együtthatóval való kapcsolatot az teremti meg, hogy $q \to 1$ esetén $\begin{bmatrix} n \\ k \end{bmatrix}_q \to \binom{n}{k}$. Ezen kívül a hagyományoshoz hasonlóan a Gauss-féle binomiális együtthatóra is teljesül, hogy $\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q$.

Tehát például egy projektív egyenes $q+1$ pontot tartalmaz, egy projektív sík pedig q^2+q+1 pontot és q^2+q+1 egyenest.

2.3. Állítás. *Legyen $t \leq k$. Azon k-dimenziós alterek száma $V(n,q)$-ban, amelyek tartalmazzák a tér egy rögzített t-dimenziós alterét,*

$$\begin{bmatrix} n-t \\ k-t \end{bmatrix}_q.$$

2.4. Állítás. *Ha $\mathcal{U}$ és $\mathcal{V}$ alterek $V(n,q)$-ban, akkor fennáll rájuk az alábbi,* dimenzióformulának *nevezett összefüggés:*

$$\dim(\mathcal{U}) + \dim(\mathcal{V}) = \dim(\mathcal{U} \cap \mathcal{V}) + \dim(\mathcal{U} + \mathcal{V}).$$

Itt $\mathcal{U} + \mathcal{V} \coloneqq \{u+v \colon u \in \mathcal{U}, v \in \mathcal{V}\}$ a két altér Minkowski-összege.

2.5. Definíció. Legyenek $a_{ij} \in \mathbb{F}_q$ testelemek $(1 \leq i, j \leq n)$, és vegyük a

$$F(X_1, X_2, \ldots, X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j$$

kvadratikus alakot. Azon pontok halmazát $PG(n-1,q)$-ban, amelyek homogén koordinátái kielégítik az

$$F(X_1, X_2, \ldots, X_n) = 0 \tag{1}$$

egyenletet, $(n-1)$-dimenziós *másodrendű felületnek* nevezzük.

Az, hogy egy pont homogén koordinátáinak melyik reprezentánsát választjuk, nyilván nem befolyásolja, hogy a pont rajta van-e a felületen. Véges test felett az (1) egyenletnek mindig van nemtriviális megoldása, így az üres halmaz nem alkot másodrendű felületet.

2.6. Definíció. A 2-dimenziós másodrendű felület elnevezése *másodrendű görbe.*

2.7. Állítás. *Ha egy másodrendű felület tartalmazza egy egyenes három különböző pontját, akkor a teljes egyenest tartalmazza.*

Ez tehát azt jelenti, hogy egy másodrendű felület és egy rá nem illeszkedő egyenes közös pontjainak száma 0, 1 vagy 2 lehet.

2.8. Definíció. Egy egyenes egy másodrendű felületnek *elkerülő* egyenese, ha nincs a felülettel közös pontja, *érintő* egyenese, ha 1, és *szelő* egyenese, ha 2 közös pontja van a felülettel.

2.9. Definíció. Az $\mathscr{F}$ másodrendű felületet *szinguláris*nak nevezzük, ha a koordinátarendszer változtatásával elérhető, hogy az $\mathscr{F}$-et leíró egyenlet eggyel kevesebb változót tartalmazzon. Ha ez nem tehető meg, akkor a felületet *nemszinguláris*nak nevezzük.

2.10. Tétel. *Legyen $\mathscr{F}$ nemszinguláris másodrendű felület $PG(n-1,q)$-ban. Ekkor az $\mathscr{F}$-et meghatározó F kvadratikus alak a koordinátarendszer változtatásával az alábbi kanonikus alakok egyikére hozható:*

- *Ha $n-1$ páros, akkor $F(\mathbf{X}) = X_1^2 + X_2X_3 + \ldots X_{n-1}X_n$. Ebben az esetben a másodrendű felületet* parabolikus kvádrikának *nevezzük. Ha $n-1=2$, akkor a* kúpszelet *elnevezést is használjuk.*
- *Ha $n-1$ páratlan, akkor vagy*
  - *$F(\mathbf{X}) = X_1X_2+X_3X_4+\ldots X_{n-1}X_n$, ekkor* hiperbolikus kvádrikáról *beszélünk, vagy*
  - *$F(\mathbf{X}) = f(X_1,X_2)+X_3X_4+\ldots X_{n-1}X_n$, ahol f irreducibilis homogén másodfokú polinom. Az ilyen felületek neve* elliptikus kvádrika.

2.11. Állítás. *A $PG(n-1,q)$ térben a szinguláris másodrendű felületek mindegyike előáll mint valamely Π_{k-1} $(k-1)$-dimenziós altérbeli nemszinguláris másodrendű felületre emelt olyan kúp, melynek csúcsa egy Π_{n-k-1} $(n-k-1)$-dimenziós altér, ahol $\Pi_{k-1}\cap\Pi_{n-k-1}=\emptyset$. (Ez azt jelenti, hogy ha vesszük az összes olyan egyenest, amely Π_{k-1}-ben levő felület egy pontját a Π_{n-k-1} $(n-k-1)$-dimenziós altér egy tetszőleges pontjával köti össze, akkor ezen egyenesek pontjai a másodrendű felületet adják vissza.)*

Ebből következik, hogy $PG(3,q)$-ban egy szinguláris másodrendű felület vagy egy olyan kúp, melynek alapja egy kúpszelet, csúcsa pedig egy arra nem illeszkedő pont, ezt *másodrendű kúpnak* fogjuk nevezni, vagy egy olyan kúp, melynek alapja két pont, csúcsa pedig egy egyenes, ami nem más, mint egy metsző síkpár.

2.12. Állítás. *Ha adott öt pont $PG(2,q)$-ban, melyek közül semelyik három nem illeszkedik egy egyenesre, akkor pontosan egy olyan kúpszelet van, amely mind az öt pontot tartalmazza.*

2.13. Állítás. *Egy $(n-1)$-dimenziós másodrendű felület metszete egy $(k-1)$-dimenziós projektív altérrel $(k-1)$-dimenziós másodrendű felület.*

2.14. Tétel. *Egy $(n-1)$-dimenziós nemszinguláris másodrendű felület által tartalmazott maximális projektív altér dimenziója legfeljebb*

$$k = \begin{cases} \frac{n-2}{2} & \text{ha } n-1 \text{ páratlan,} \\ \frac{n-3}{2} & \text{ha } n-1 \text{ páros.} \end{cases}$$

2.15. Állítás. *$PG(3,q)$-ban a hiperbolikus kvádrika – amelynek tehát a kanonikus egyenlete $X_1X_2+X_3X_4=0$ – minden pontján pontosan két olyan egyenes halad át, amely teljes egészében a felületen van. Ha e egy rögzített, a felületen levő egyenes, akkor $q+1$ olyan másik egyenes van a felületen, amely elmetszi e-t. Ez a $q+1$ egyenes páronként kitérő.*

Eszerint a 3-dimenziós hiperbolikus kvádrika által tartalmazott egyenesek két $q+1$ méretű osztályba sorolhatók. Az azonos osztályban levő egyenesek páronként kitérők, és bármely két, ellentétes osztályban levő egyenes egymást egy pontban metszi. Ezt a két osztályt a kvádrika két *regulusának* is szokták nevezni.

2.16. Állítás. *Ha adott $PG(3,q)$-ban két kitérő egyenes és egy azokra nem illeszkedő pont, akkor egyértelműen létezik egy olyan $PG(3,q)$-beli egyenes, amely áthalad a ponton, és elmetszi mindkét egyenest.*

Vegyünk $PG(3,q)$-ban három páronként kitérő egyenest. A fenti állítást az egyik egyenes $q+1$ pontjára alkalmazva azt kapjuk, hogy pontosan $q+1$ olyan egyenes van $PG(3,q)$-ban, amely mind a három rögzített egyenest metszi. Megmutatható, hogy ha egy egyenes az így kapott $q+1$ egyenes közül legalább hármat metsz, akkor az összeset metszi. Ezért értelmes a következő definíció:

2.17. Definíció. $PG(3,q)$-ban három páronként kitérő egyenes által meghatározott *reguluson* azt a $q+1$ egyenest értjük, amelyeknek minden olyan egyenessel pontosan egy közös pontjuk van, amely egyenesek a három rögzített egyenes mindegyikét metszik.

Tehát három páronként kitérő egyeneshez vehetjük az általuk meghatározott regulust, valamint azt a $q+1$ egyenest, amely ennek a regulusnak minden egyenesét pontosan egy pontban metszi. Így egy hiperbolikus kvádrika két ellentétes regulusát kapjuk. Ezt felhasználva belátható az alábbi állítás:

2.18. Állítás. *Ha adott három páronként kitérő egyenes $PG(3,q)$-ban, akkor pontosan egy olyan hiperbolikus kvádrika van, amely mind a három egyenest tartalmazza.*

2.19. Állítás. *$PG(5,q)$-ban a hiperbolikus kvádrika – amelynek tehát a kanonikus egyenlete $X_1X_2+X_3X_4+X_5X_6=0$ – minden pontján pontosan két olyan sík halad át, amely teljes egészében a felületen van.*

A $PG(n-1,q)$ véges projektív térnek értelmezhetjük a *duális terét*. Ez egy olyan véges projektív tér, amelynek a $(k-1)$-dimenziós altereit a $PG(n-1,q)$ tér $(n-k-1)$-dimenziós alterei alkotják, az alterek közötti tartalmazás pedig megfordul. Ez a $PG(n-1,q)^*$ duális tér az eredeti térrel izomorf.

2.20. Definíció. *Polaritásnak* nevezünk egy olyan $PG(n-1,q) \to PG(n-1,q)^*$ hozzárendelést, amely bijektív, megőrzi az alterek illeszkedését és kétszer alkalmazva a $PG(n-1,q)$ tér identikus leképezésével egyezik meg.

2.21. Állítás. *Tegyük fel, hogy az $\mathscr{F}$ nemszinguláris másodrendű felületet leíró (1) egyenlet alkalmas $A \in \mathbb{F}_q^{n\times n}$ szimmetrikus, nemelfajuló mátrixszal $\mathbf{X}A\mathbf{X}^T=0$ alakba írható. Legyen P egy rögzített pont $PG(n-1,q)$-ban, melynek a reprezentáló vektora $\mathbf{p}$. Ekkor azon $PG(n-1,q)$-beli pontok, melyeknek $\mathbf{r}$ reprezentáló vektoraira teljesül, hogy*

$$\mathbf{p}A\mathbf{r}^T=0,$$

egy hiperíkot alkotnak. Ha a P ponthoz hozzárendeljük ezt a hipersíkot, akkor egy $PG(n-1,q)\to PG(n-1,q)^*$ polaritást kapunk, ez az $\mathscr{F}$ által meghatározott polaritás.

2.22. Definíció. Legyen α a $PG(n-1,q)$ tér egy polaritása, és Σ_{k-1} egy $(k-1)$-dimenziós altér $PG(n-1,q)$-ban $(1 \leq k \leq n)$. A Σ_{k-1} *polárisa* az α-nál vett képe, amely egy $(k-1)$-dimenziós altér $PG(n-1,q)^*$-ban, azaz egy $(n-k-1)$-dimenziós altér $PG(n-1,q)$-ban.

2.23. Definíció. $PG(n-1,q)$-ban $m \geq n$ esetén egy ponthalmazt *m-ívnek* nevezünk, ha m pontból áll, és a pontjai közül semelyik n nincs egy hipersíkban.

2.24. Példa. $PG(2,q)$-ban a kúpszeletek $(q+1)$-íveket alkotnak.

2.25. Definíció. A $PG(n-1,q)$ tér *$(k-1)$-befedésének* nevezzük $(k-1)$-dimenziós projektív alterek egy $\mathcal{H}$ halmazát, ha $\mathcal{H}$ elemei páronként diszjunktak, és $PG(n-1,q)$ minden pontja $\mathcal{H}$-nak pontosan egy elemében van benne. $PG(n-1,q)$ *részleges $(k-1)$-befedésének* nevezzük $(k-1)$-dimenziós projektív alterek egy halmazát $PG(n-1,q)$-ban, ha annak elemei páronként diszjunktak.

2.26. Tétel. *A $PG(n-1,q)$ térnek akkor és csak akkor létezik $(k-1)$-dimenziós alterekből álló befedése, ha $k|n$.*

Ebből speciálisan az is következik, hogy ha $PG(n-1,q)$-nak van $(k-1)$-befedése, és $k < n$, akkor $k \leq \left\lfloor \frac{n}{2} \right\rfloor$. Ez akkor is igaz, ha csak részleges $(k-1)$-befedése van $PG(n-1,q)$-nak, mert különben a dimenzióformulából következne, hogy bármely két $(k-1)$-dimenziós altér metszete nemüres.

A $PG(3,q)$ tér természetes módon beágyazható a $PG(3,q^2)$ térbe. (Az $\mathbb{F}_q$-beli koordinátákat tekinthetjük $\mathbb{F}_{q^2}$-belieknek.) Ha $PG(3,q^2)$ egy egyenese legalább két pontot tartalmaz $PG(3,q)$-ból, akkor azok összekötő egyenesét is tartalmazza, és így $q+1$ $PG(3,q)$-beli pontja van. Tehát egy $PG(3,q^2)$-beli egyenes a $PG(3,q)$ teret 0, 1 vagy $q+1$ pontban metszheti. Egyszerű leszámlálásból adódik, hogy van olyan $PG(3,q^2)$ beli egyenes, amely elkerüli $PG(3,q)$-t. Legyen t egy ilyen egyenes, és $P = (x : y : z : v)$ egy pont t-n. Belátható, hogy ekkor P-t a $P^q = (x^q : y^q : z^q : v^q)$ ponttal összekötő egyenes $q+1$ pontban metszi, valamint a P-n átmenő összes többi egyenes elkerüli $PG(3,q)$-t. Azaz t mind a q^2+1 pontján át pontosan egy olyan egyenes van, amely $PG(3,q)$-nak is egyenese, és ezek az egyenesek $PG(3,q)$-ban páronként kitérők, vagyis egy befedést alkotnak.

2.27. Definíció. A $PG(3,q)$ tér fenti konstrukcióval kapott 1-dimenziós alterekből álló befedését *elliptikus kongruenciának* nevezzük.

2.28. Definíció. Rögzítsünk két kitérő egyenest a $PG(3,q)$ térben. *Hiperbolikus kongruenciának* nevezzük azon $(q+1)^2$ egyenest, amelyeket úgy kapunk, hogy a két rögzített egyenesről az összes lehetséges módon egy-egy pontot kiválasztva vesszük azok összekötő egyenesét. A két rögzített egyenes a kongruencia két *tengelye*.

Vegyük észre, hogy a hiperbolikus kongruencia két különböző egyenese csak a két tengely valamelyikén metszheti egymást.

2.29. Definíció. Egy rögzített ponton átmenő $q+1$ egyenest a $PG(2,q)$ síkban *sugársornak* nevezünk.

2.30. Definíció. *Parabolikus kongruenciának* nevezünk q^2+q+1 egyenest, amelyeket úgy kapunk, hogy veszünk egy rögzített egyenest (ez lesz a kongruencia *tengelye*), és annak minden pontjában még q-q másik egyenest, amelyek a tengellyel együtt mind egy-egy sugársort alkotnak, és két különböző sugársorhoz tartozó egyenes nem metszi egymást. (Azaz a sugársorok különböző síkokban vannak.)

Megemlítjük még a véges projektív sík ún. *ciklikus modelljét.* Amint láttuk, a $PG(2,q)$ sík egy $V(3,q)$ 3-dimenziós $\mathbb{F}_q$ feletti vektortérből származtatható. Ilyen vektortér például $\mathbb{F}_{q^3}$, vagyis a q^3 elemű test. Mivel $\mathbb{F}_{q^3}$ egy véges test, a multiplikatív csoportja ciklikus, így kiválaszthatunk benne egy $\omega \in \mathbb{F}_{q^3}^*$ generátorelemet. Ennek segítségével $\mathbb{F}_{q^3}$ elemeit az alábbi módon sorolhatjuk fel:

$$\mathbb{F}_{q^3} = \{0\} \cup \{\omega^0, \omega^1, \omega^2, \ldots, \omega^{q^3-2}\}.$$

Ebben a felsorolásban ω^k és ω^l mint $\mathbb{F}_q$ feletti vektorok pontosan akkor határozzák meg ugyanazt a $PG(2,q)$-beli pontot, ha

$$\exists \lambda \in \mathbb{F}_q\{0\}\colon \omega^k = \lambda\omega^l \iff \omega^{k-l} = \lambda \in \mathbb{F}_q \iff$$

$$\iff (\omega^{k-l})^{q-1} = 1 \iff q^3-1 | (k-l)(q-1) \iff q^2+q+1 | k-l.$$

Ez azt jelenti, hogy ha vesszük az $1, \omega, \omega^2, \ldots, \omega^{q^2+q}$ vektorok által meghatározott $PG(2,q)$-beli pontokat, akkor a sík összes pontját megkapjuk. Tehát a pontok valójában az ezen vektorok által alkotott (q^2+q+1)-rendű ciklikus csoport elemeinek feleltethetők meg. (A csoportművelet az $\mathbb{F}_{q^3}^*$-beli szorzás, ω kitevőjével modulo q^2+q+1 számolva.) Az egyeneseknek pedig $q+1$ elemű részhalmazok felelnek meg ebben a csoportban. Ezért van értelme egy pont inverzéről beszélni. Sőt egy e egyenes inverzét is definiálhatjuk: Vegyük e minden pontjának az inverzét, és az ezekből álló $q+1$ elemű halmaz legyen az e inverze.

2.31. Tétel (Hall, [8])**.** *A ciklikus modellben az egyenesek inverzei kúpszeletek.*

2.2. Kódelméleti alapfogalmak

A kódelmélet által vizsgált kommunikációs modellben egy adó egy vevőnek szeretne továbbítani egy üzenetet valamilyen csatornán keresztül. Ezt úgy szeretné megtenni, hogy ha küldés közben az adatok egy része megváltozik, a vevő akkor is meg tudja fejteni az eredeti üzenetet. Ennek érdekében a kommunikáció résztvevői *hibajavító kódoláshoz* folyamodnak.

Tegyük fel, hogy a továbbítandó üzenet egy $\mathbb{F}_q$-beli testelemekből álló n hosszú sorozat, vagyis az $\mathbb{F}_q^n$ vektortér egy eleme. (Tipikus esetben $q=2$, azaz bináris sorozatok az üzenetek.) Azt mondjuk, hogy a küldés során *t hiba* történt, ha t koordináta módosult, azaz a küldött $\mathbf{x}$ üzenet helyett a vevő egy $\mathbf{x}+\mathbf{e}$ üzenetet kapott egy olyan $\mathbf{e} \in \mathbb{F}_q^n$ hibavektorral, amelynek t nemnulla koordinátája van. A vevő célja dekódolni az üzenetet, azaz $\mathbf{x}+\mathbf{e}$ és C ismeretében kitalálni $\mathbf{x}$-et.

2.32. Definíció. $\mathbb{F}_q$ *feletti kódon* egy $C \subseteq \mathbb{F}_q^n$ halmazt értünk. C elemeit *kódszavaknak* nevezzük.

2.33. Megjegyzés. Általánosabb értelemben *kódnak* hívjuk bármilyen véges halmaz egy részhalmazát is. Ilyen véges halmaz lehet például egy véges test feletti vektortér összes altereinek halmaza (a dolgozat nagy részében ez lesz a helyzet), vagy éppen egy véges test feletti rögzített méretű mátrixok halmaza. Az előbbi esetben a részhalmazokat *altér kódoknak*, az utóbbiban *mátrix kódoknak* nevezzük. Ebben a bevezető részben az $\mathbb{F}_q$ feletti kódokra szorítkozunk.

2.34. Definíció. Azt mondjuk, hogy a C kód *t-hibajavító*, ha legfeljebb t hiba esetén a vevő dekódolni tudja az üzenetet.

2.35. Definíció. Legyenek $\mathbf{v}$ és $\mathbf{w}$ vektorok $\mathbb{F}_q^n$-ben. A két vektor *Hamming-távolsága* azon koordináták száma, amelyekben $\mathbf{v}$ és $\mathbf{w}$ eltér egymástól, azaz

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

2.36. Állítás. *A Hamming-távolság metrika $\mathbb{F}_q^n$-en.*

2.37. Definíció. A $\mathbf{v} \in \mathbb{F}_q^n$ vektor *(Hamming-)súlya* a $\mathbf{v}$ nemnulla koordinátáinak száma, azaz

$$w_H(\mathbf{v}) = d_H(\mathbf{v}, \mathbf{0}) = |\{i \colon v_i \neq 0\}|.$$

2.38. Definíció. Legyen C egy $\mathbb{F}_q$ feletti kód. A C *minimális távolsága*

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

2.39. Definíció. Legyen C egy $\mathbb{F}_q$ feletti kód. A C *súlya*

$$w_H(C) = \min\{w_H(\mathbf{v}) \colon \mathbf{v} \in C\}.$$

2.40. Állítás. *Legyen t pozitív egész, és C egy $\mathbb{F}_q$ feletti kód. C pontosan akkor t-hibajavító, ha*

$$d_H(C) \geq 2t + 1.$$

Az $\mathbb{F}_q$ feletti kódok fontos osztályát alkotják a lineáris kódok:

2.41. Definíció. A $C \subseteq \mathbb{F}_q^n$ kód *lineáris*, ha C lineáris altere az $\mathbb{F}_q^n$ vektortérnek.

2.42. Állítás. *Egy lineáris kód minimális távolsága megegyezik a kód súlyával.*

2.43. Definíció. Legyen $C \subseteq \mathbb{F}_q^n$ lineáris kód, melynek dimenziója k. Az $M \in \mathbb{F}_q^{(n-k)\times n}$ mátrix a C kód *paritásellenőrző mátrixa*, ha

$$C = \{\mathbf{v} \in \mathbb{F}_q^n \colon M\mathbf{v}^T = \mathbf{0}\}.$$

2.44. Állítás. *Egy C lineáris kód minimális távolsága az a legnagyobb d szám, amelyre teljesül, hogy C paritásellenőrző mátrixának bármely $d-1$ oszlopa lineárisan független.*

A kódelmélet célja minél „jobb” kódokat létrehozni, azaz olyanokat, amelyekkel egyrészt rögzített karakterhossz mellett minél többféle üzenetet lehet küldeni (tehát a kód mérete minél nagyobb), másrészt minél több hibát képesek kijavítani (tehát a kód minimális távolsága minél nagyobb). Ez a két tulajdonság persze csak egymás rovására javítható, ahogy azt majd látni fogjuk a 4. fejezet felső korlátokról szóló szakaszában.

Mivel minden $\mathbb{F}_q$ feletti n-dimenziós vektortér izomorf $\mathbb{F}_q^n$-nel, nem veszítünk az általánosságból, ha a továbbiakban csak ezzel a vektortérrel foglalkozunk. A dolgozatban q mindig prímhatványt jelöl.

3. Gömbök $G_q(k,n)$-ben

Ahogy a Bevezetésben láttuk, fontos kérdés, hogy hogyan tudja a vevő dekódolni az üzenetet abban az esetben, amikor a kódszavak egy vektortér alterei. Másszóval azt kell eldöntenünk, hogy egy adott k-dimenziós altér melyik másik - nem feltétlenül azonos dimenziójú - alterektől van egy rögzített számnál kisebb távolságra egy alkalmas távolságfogalom mellett. Ebben a fejezetben a célunk, hogy leírjuk az olyan $\mathbb{F}_q^n$-beli k-dimenziós alterekből álló gömböket, amelyeknek a középpontja $\mathbb{F}_q^n$ valamely k'-dimenziós altere.

3.1. Grassmann-sokaság, Grassmann-koordináták

3.1. Definíció. $\mathbb{F}_q^n$ k-dimenziós altereinek a halmazát $\mathbb{F}_q^n$ feletti k-dimenziós *Grassmann-sokaságnak* nevezzük, és $G_q(k,n)$-nel jelöljük.

Legyen $\mathcal{U} \in G_q(k,n)$. Vegyünk $\mathcal{U}$-ban egy bázist, és tekintsük azt az U mátrixot, amelynek sorai ezen bázis vektorai. Ekkor $\mathcal{U} = \mathrm{rs}(U)$, azaz az $\mathcal{U}$ alteret előállítottuk egy $(k \times n)$-es mátrix sortereként.

Jelölje $M_{i_1,i_2,\dots,i_k}(U)$ U-nak azt az aldeterminánsát, amelyet az $i_1, i_2, \dots, i_k$ indexű oszlopok jelölnek ki.

$G_q(k,n)$ beágyazható az $\mathbb{F}_q$ feletti $\binom{n}{k} - 1$ dimenziós projektív térbe a következő leképezéssel:

$$\phi\colon G_q(k,n) \to PG\left(\binom{n}{k} - 1, q\right)$$
$$\mathrm{rs}(U) \mapsto [M_{1,\dots,k}(U)\colon M_{1,\dots,k-1,k+1}(U)\colon \dots : M_{n-k+1,\dots,n}(U)].$$

3.2. Állítás. *ϕ jóldefiniált, azaz $\phi(\mathcal{U})$ nem függ az U mátrix választásától. Továbbá ϕ injektív.*

Bizonyítás. Tegyük fel, hogy az U_1 és U_2 mátrixok ugyanazt az $\mathcal{U} \in G_q(k,n)$ alteret határozzák meg. Jelöljük $j = 1, 2$ esetén $U_j[i_1, \dots, i_k]$-val az U_j $i_1, \dots, i_k$ indexű oszlopai által meghatározott $k \times k$-as mátrixot. Tudjuk, hogy létezik egy olyan $A \in GL(k,q)$ mátrix, amelyre $U_2 = AU_1$, és minden $1 \le i_1, \dots, i_k \le n$ esetén $U_2[i_1, \dots, i_k] = AU_2[i_1, \dots, i_k]$. Ebből következik a jóldefiniáltság, hiszen a determinánsok szorzástétele szerint $M_{i_1,\dots,i_k}(U_2) = \det(A) M_{i_1,\dots,i_k}(U_1) \quad (\forall 1 \le i_1, \dots, i_k \le n)$, vagyis az U_1 és U_2 aldeterminánsaiból alkotott rendezett $\binom{n}{k}$-asok egymás skalárszorosai. (És nem lehet $\phi(\mathcal{U})$ minden koordinátája 0, mert U rangja k.)

Az injektivitás bizonyításához tegyük fel, hogy U_2-nek minden $k \times k$-as aldeterminán sa λ-szorosa U_1 megfelelő aldeterminánsának ($\lambda \in \mathbb{F}_q^*$). Feltehető, hogy $\lambda = 1$, mert ha $\lambda \neq 1$, akkor U_1-re alkalmazhatunk egy olyan lineáris transzformációt, amelynek a determinánsa λ. Tehát azt kell belátnunk, hogy ha két $k \times n$-es mátrixnak az összes $k \times k$-as aldeterminánsa megegyezik, akkor ugyanaz a sorterük. Mivel U_1 és U_2 rangja k, feltehető, hogy $M_{1,\dots,k}(U_1) \neq 0 \neq M_{1,\dots,k}(U_2)$. Elemi sortranszformációs lépésekkel elérhető, hogy az első k oszlop helyén U_1-ben és U_2-ben is I_k álljon. Legyen $i \le k < j$.

Ekkor az i-edik sor j-edik eleme mindkét mátrixban megegyezik az $1, \dots, i-1, i+1, \dots k, j$ indexű oszlopok által meghatározott aldeterminánssal, tehát U_1 és U_2 minden eleme egyenlő. Így $\mathrm{rs}(U_1) = \mathrm{rs}(U_2)$. □

3.3. Definíció. Legyen $\mathcal{U} = \mathrm{rs}(U) \in G_q(k,n)$. Az $\mathcal{U}$ altér *Grassmann-koordinátái* a fenti ϕ leképezésnél vett képének a projektív koordinátái, azaz az U reprezentáló mátrix $k \times k$-as aldeterminánsai.

3.4. Állítás ([17]). *Legyen* $x \coloneqq [x_{1,\dots,k} \colon \dots \colon x_{n-k+1,\dots,n}] \in PG\left(\binom{n}{k} - 1, q\right)$. *Pontosan akkor létezik olyan* $\mathcal{U} \in G_q(k,n)$ *altér, amelyre* $\phi(\mathcal{U}) = x$, *ha*

$$\sum_{j \in \{i_1,\dots,i_{k+1}\}} \mathrm{sgn}(\sigma_j) x_{i_1,\dots,i_{j-1},i_{j+1},\dots,i_{k+1}} x_{j,i_{k+2},\dots,i_{2k}} = 0$$

$\forall (i_1, \dots, i_{k+1}) \in \binom{[n]}{k+1}$, $(i_{k+2}, \dots i_{2k}) \in \binom{[n]}{k-1}$, *ahol* $\mathrm{sgn}(\sigma_j)$ *jelöli annak a permutációnak az előjelét, amelyre*

$$\sigma_{i_l}(i_1, \dots, i_{k+1}) = (i_l, i_1, \dots, i_{l-1}, i_{l+1}, \dots, i_{k+1}).$$

3.5. Példa. A Grassmann-koordináták speciális eseteként kapjuk egy projektív térbeli egyenes – azaz egy $G_q(2,4)$-beli elem – *Plücker-koordinátáit.* Ezekre a 3.4 Állításból az

$$x_{12}x_{34} + x_{31}x_{24} + x_{14}x_{23} = 0.$$

összefüggést kapjuk.

3.2. A gömbök jellemzése lineáris egyenletekkel

Ahhoz, hogy gömbökről beszélhessünk, először is távolságot kell definiálnunk az altereken.

3.6. Definíció. Az $\mathcal{U}$ és $\mathcal{V}$ $\mathbb{F}_q^n$-beli alterek *altér távolságán* a

$$d_S(\mathcal{U}, \mathcal{V}) = \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U} \cap \mathcal{V}) = \dim(\mathcal{U} + \mathcal{V}) - \dim(\mathcal{U} \cap \mathcal{V})$$

számot értjük.

3.7. Állítás. *d_S metrika $\mathbb{F}_q^n$ összes altereinek halmazán.*

Bizonyítás. Az, hogy $d_S \geq 0$ és $d_S(\mathcal{U}, \mathcal{V})$ pontosan akkor 0, ha $\mathcal{U} = \mathcal{V}$, nyilván teljesül, valamint az is, hogy d_S szimmetrikus. A háromszög-egyenlőtlenség ellenőrzéséhez tegyük fel, hogy $\mathcal{U}, \mathcal{V}$ és $\mathcal{W}$ alterek $\mathbb{F}_q^n$-ben. Ekkor

$$\begin{aligned}\frac{1}{2}(d_S(\mathcal{U}, \mathcal{V}) - d_S(\mathcal{U}, \mathcal{W}) - d_S(\mathcal{V}, \mathcal{W})) &= \dim(\mathcal{U} \cap \mathcal{W}) + \dim(\mathcal{V} \cap \mathcal{W}) - \\ &- \dim(\mathcal{W}) - \dim(\mathcal{U} \cap \mathcal{V}) = \\ &= \dim(\mathcal{U} \cap \mathcal{W} + \mathcal{V} \cap \mathcal{W}) - \dim(\mathcal{W}) + \\ &+ \dim(\mathcal{U} \cap \mathcal{V} \cap \mathcal{W}) - \dim(\mathcal{U} \cap \mathcal{V}) \leq \\ &\leq 0 + 0 = 0.\end{aligned}$$

Itt felhasználtuk a dimenzióformulát, valamint azt, hogy $\mathcal{U} \cap \mathcal{W} + \mathcal{V} \cap \mathcal{W} \subseteq \mathcal{W}$ és $\mathcal{U} \cap \mathcal{V} \cap \mathcal{W} \subseteq \mathcal{U} \cap \mathcal{V}$. □

Az így kapott metrikus térben akkor lesz két pont közel egymáshoz, ha a metszetük dimenziója elég nagy.

Ez a távolságfogalom természetes általánosítása a Hamming-távolságnak. Tekintsünk ugyanis egy $\mathbf{v} = (v_1, \dots v_n)$ $\mathbb{F}_2$ feletti n hosszú vektort, és jelöljük $\mathbf{e_i}$-vel az i-edik standard bázisvektort $\mathbb{F}_2^n$-ben. Legyen ${\mathbf{e_i}}^\epsilon = \mathbf{e_i}$, ha $\epsilon = 1$ és $\mathbf{0}$, ha $\epsilon = 0$. Ekkor $\mathbf{v}$ azonosítható a $\{{\mathbf{e_i}}^{v_i} : 1 \leq i \leq n\}$ által generált $\sum_{i=1}^n v_i$-dimenziós altérrel. Két kódszó Hamming-távolsága pont az így kapott alterek közötti altér távolsággal lesz egyenlő.

3.8. Lemma. *$d_S(\mathcal{U}, \mathcal{V}) = d_S(\mathcal{U}^\perp, \mathcal{V}^\perp)$.*

Bizonyítás. Legyen $k = \dim(\mathcal{U})$ és $k' = \dim(\mathcal{V})$. Felhasználva a dimenzióformulát és azt, hogy $(\mathcal{U} \cap \mathcal{V})^\perp = \mathcal{U}^\perp + \mathcal{V}^\perp$, azt kapjuk, hogy

$$\begin{aligned} d_S(\mathcal{U}, \mathcal{V}) &= \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U} \cap \mathcal{V}) = \\ &= k + k' - 2\dim(\mathcal{U}^\perp + \mathcal{V}^\perp)^\perp = \\ &= k + k' - 2(n - \dim(\mathcal{U}^\perp + \mathcal{V}^\perp)) = \\ &= k + k' - 2(n - ((n-k) + (n-k') - \dim(\mathcal{U}^\perp \cap \mathcal{V}^\perp))) = \\ &= (n-k) + (n-k') - 2\dim(\mathcal{U}^\perp \cap \mathcal{V}^\perp) = \\ &= \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U}^\perp \cap \mathcal{V}^\perp) = \\ &= d_S(\mathcal{U}^\perp, \mathcal{V}^\perp). \end{aligned}$$

□

Szükségünk lesz az alábbi részbenrendezési relációra:

3.9. Definíció. Legyen $(i_1, \dots, i_k)$ és $(j_1, \dots, j_k)$ két k hosszú részsorozata az $(1, 2, \dots, n)$ sorozatnak. Azt mondjuk, hogy $(i_1, \dots, i_k) \preceq (j_1, \dots, j_k)$, ha $i_l \leq j_l \quad \forall l \in \{1, \dots, k\}$. Ez az ún. *Bruhat-rendezés.*

3.10. Definíció. Legyen $\mathcal{R}$ tetszőleges altér $\mathbb{F}_q^n$-ben. Jelölje

$$B_{S,\tau}^k(\mathcal{R}) \coloneqq \{\mathcal{U} \in G_q(k,n) \colon d_S(\mathcal{R}, \mathcal{U}) \leq \tau\}$$

az $\mathcal{R}$ középpontú, τ sugarú gömböt az altér távolság szerint.

3.11. Lemma. *Legyenek $\mathcal{U}$ és $\mathcal{V}$ alterek $\mathbb{F}_q^n$-ben. Tegyük fel, hogy $\dim(\mathcal{U}) = k$ és $\dim(\mathcal{V}) = k'$. Ekkor $k - k' + d_S(\mathcal{U}, \mathcal{V})$, $k' - k + d_S(\mathcal{U}, \mathcal{V})$ és $k + k' - d_S(\mathcal{U}, \mathcal{V})$ páros számok.*

Bizonyítás. Mivel $d_S(\mathcal{U}, \mathcal{V}) = k + k' - 2\dim(\mathcal{U} \cap \mathcal{V})$, $d_S(\mathcal{U}, \mathcal{V})$ pontosan akkor páratlan, ha k és k' paritása különböző. Ezért $d_S(\mathcal{U}, \mathcal{V})$ és $k - k'$, $d_S(\mathcal{U}, \mathcal{V})$ és $k' - k$, valamint $d_S(\mathcal{U}, \mathcal{V})$ és $k + k'$ is egyszerre párosak vagy páratlanok, vagyis az összegük páros. □

3.12. Tétel. *Legyen* $U_0^{k'} \coloneqq \mathrm{rs}[I_{k'}0_{k'\times n-k'}]$. *Legyen* τ *olyan, hogy* $|k-k'| \leq \tau < \min(k'+k, 2n-(k'+k))$ *és* $\frac{k+k'-\tau}{2} \in \mathbb{Z}$. *Ekkor*

$$B_{S,\tau}^k(\mathcal{U}_0^{k'}) = \Big\{ \mathcal{V} = \mathrm{rs}(V) \in G_q(k,n) \colon M_{i_1,\ldots,i_k}(V) = 0 \quad \forall \quad (i_1,\ldots,i_k) \not\geq \left(\frac{k'-k+\tau}{2}+1, \ldots, k', n-\frac{k-k'+\tau}{2}+1, \ldots, n \right) \Big\}.$$

Bizonyítás. Az olyan $\mathcal{V} = \mathrm{rs}(V) \in G_q(k,n)$ altereket szeretnénk meghatározni, amelyekre

$$d_S(\mathcal{U}_0^{k'}, \mathcal{V}) \leq \tau \Longleftrightarrow \dim(\mathcal{U}_0^{k'}, \mathcal{V}) \geq \frac{k+k'-\tau}{2}.$$

Vagyis $\mathcal{U}_0^{k'}$-nek legalább $\frac{k+k'-\tau}{2}$ lineárisan független elemet kell tartalmaznia $\mathcal{V}$-ből. Ha ez teljesül, akkor $\mathcal{V}$-t fel tudjuk írni egy olyan mátrix sortereként, amelynek az első $\frac{k+k'-\tau}{2}$ sora $\mathcal{U}_0^{k'}$-beli elemeket tartalmaz, azaz V az alábbi alakú:

$$V = \left[\begin{array}{c|c} * & 0_{\frac{k+k'-\tau}{2}\times(n-k')} \\ \hline * & * \end{array}\right].$$

Ekkor a $V \in \mathbb{F}_q^{k\times n}$ $k\times k$-as részmátrixai a következőképpen néznek ki:

$$M = \left[\begin{array}{c|c} M_1 & 0_{\frac{k+k'-\tau}{2}\times x} \\ \hline M_2 & M_3 \end{array}\right],$$

ahol x azon oszlopok száma, amelyeket V jobb oldali $(n-k')$ oszlopából választottunk, M_1 pedig egy $\frac{k+k'-\tau}{2} \times (k-x)$ -es mátrix. Azt állítjuk, hogy ha $x \geq \frac{k-k'+\tau}{2}+1$, akkor $\det(M) = 0$. Ugyanis

$$\mathrm{rk}(M) \leq \mathrm{rk}(M_1) + \mathrm{rk}([M_2 M_3]) \leq (k-x) + \frac{k-k'+\tau}{2} = k - (x - \frac{k-k'+\tau}{2}),$$

így ha $x > \frac{k-k'+\tau}{2}$, akkor azt kapjuk, hogy $\mathrm{rk}(M) < k$, azaz $\det(M) = 0$. Megfordítva, ha minden ilyen x esetén a megfelelő aldeterminánsok 0-k, akkor a V sortere benne lesz a gömbben, hiszen V-ben bármit írhatunk a *-os blokkok helyére (úgy, hogy a teljes mátrix rangja k legyen). Jelöljük y-nal a $\frac{k-k'+\tau}{2}$ számot. Az, hogy $\{i_1,\ldots,i_k\}$ közül legalább $y+1$ indexet választunk a {k'+1, ..., n } halmazból, azzal ekvivalens, hogy létezik egy olyan $l \in \{1,\ldots,k-y\}$ szám, amire $i_l \geq k'+1$, ami pedig pont azt jelenti, hogy

$$(i_1,\ldots,i_k) \not\geq (k'-(k-y)+1,\ldots,k', n-y+1,\ldots,n) = \left(\frac{k'-k+\tau}{2}+1, \ldots, k', n-\frac{k-k'+\tau}{2}+1, \ldots, n \right).$$

□

Eszerint az a feltétel, hogy egy $\mathcal{V}$ altér benne van a $B_{S,\tau}^k(\mathcal{U}_0^{k'})$ gömbben, egy lineáris egyenletrendszernek felel meg a $\mathcal{V}$ Grassmann-koordinátáira.

Vizsgáljuk meg, hogy miért éppen ezeket a tulajdonságokat érdemes feltenni τ-ról. Azt láttuk a 3.11 Lemmában, hogy $\frac{k+k'-\tau}{2} \in \mathbb{Z}$ feltehető, hiszen ha τ előáll két altér távolságaként, akkor $k + k' - \tau$ szükségképpen páros. A következő állítás indokolja a másik feltételt, hiszen ha τ nem az ott megadott intervallumba esik, akkor a gömb, amit kapunk, triviális:

3.13. Állítás. *Legyen $\mathcal{U} \in G_q(k', n)$.*

1. *Ha $\tau = \min(k' + k, 2n - (k' + k))$, akkor $B^k_{S,\tau}(\mathcal{U}) = G_q(k, n)$.*
2. *Ha $\tau < |k' - k|$, akkor $B^k_{S,\tau}(\mathcal{U}) = \emptyset$.*

Bizonyítás.

1. Először nézzük azt az esetet, amikor $\tau = k' + k$. Ekkor $d_S(\mathcal{U}, \mathcal{V}) \leq \tau \Leftrightarrow \dim(\mathcal{U} \cap \mathcal{V}) \geq 0$. De ez $G_q(k, n)$ minden $\mathcal{V}$ elemére teljesül, tehát $B^k_{S,\tau}(\mathcal{U}) = G_q(k, n)$. Ha pedig $\tau = 2n - (k' + k))$, akkor a 3.8 Lemma szerint $d_S(\mathcal{U}, \mathcal{V}) = d_S(\mathcal{U}^\perp, \mathcal{V}^\perp)$, így

$$B^k_{S,2n-(k+k')}(\mathcal{U}) = (B^{n-k}_{S,(n-k)+(n-k')}(\mathcal{U}^\perp))^\perp = G_q(n-k, n)^\perp = G_q(k, n).$$

2. Tegyük fel, hogy $\tau < |k' - k|$ és $\exists \quad \mathcal{V} \in B^k_{S,\tau}(\mathcal{U})$. Ekkor teljesül, hogy

$$\min(k, k') = \frac{k + k' - |k' - k|}{2} < \frac{k + k' - \tau}{2} = \dim(\mathcal{U} \cap \mathcal{V}) \leq \min(k, k'),$$

ami ellentmondás.

□

3.14. Példa. Tekintsük $G_q(2, 5)$-öt és $\mathcal{U}^3_0 = \mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$-t. Tehát most $n = 5$, $k = 2$ és $k' = 3$. Ekkor az $\mathcal{U}_0$ középpontú $\tau = 3$ sugarú gömb

$$\begin{aligned} B^2_{S,3}(\mathcal{U}^3_0) &= \{\mathcal{V} = \mathrm{rs}(V) \in G_q(2,5) \colon M_{i_1,i_2}(V) = 0 \quad \forall \quad (i_1, i_2) \not\leq (3,5)\} = \\ &= \{\mathcal{V} = \mathrm{rs}(V) \in G_q(2,5) \colon M_{4,5}(V) = 0\}. \end{aligned}$$

Most rátérünk arra az általánosabb kérdésre, hogy hogyan lehet jellemezni az olyan gömböket, amelyeknek a középpontja tetszőleges $\mathcal{U} \in G_q(k', n)$ altér. Ismert, hogy bármely $\mathcal{U} \in G_q(k', n)$-hez létezik egy olyan $A \in GL(n, q)$ invertálható mátrix, amelyre $\mathcal{U}^{k'}_0 A = \mathcal{U}$.

3.15. Állítás. *Tetszőleges $\mathcal{U} \in G_q(k', n)$ és $A \in GL(n, q)$ esetén*

$$B^k_{S,\tau}(\mathcal{U}^{k'}_0 A) = B^k_{S,\tau}(\mathcal{U}^{k'}_0)A.$$

Bizonyítás. Mivel $\dim(\mathcal{U}_0^{k'}A \cap \mathcal{V}) = \dim(\mathcal{U}_0^{k'} \cap \mathcal{V}A^{-1})$, teljesül, hogy

$$\begin{aligned} d_S(\mathcal{U}_0^{k'}A, \mathcal{V}) \leq \tau &\iff \dim(\mathcal{U}_0^{k'}A \cap \mathcal{V}) \geq \frac{k+k'-\tau}{2} \\ &\iff \dim(\mathcal{U}_0^{k'} \cap \mathcal{V}A^{-1}) \geq \frac{k+k'-\tau}{2} \\ &\iff d_S(\mathcal{U}_0^{k'}, \mathcal{V}A^{-1}) \leq \tau. \end{aligned}$$

□

Az A mátrix segítségével már meg tudjuk adni, hogy milyen lineáris egyenleteket kell teljesíteni azon alterek Grassmann-koordinátáinak, amelyek benne vannak $B_{S,\tau}^k(\mathcal{U})$-ban, ugyanis a VA^{-1}-ben szereplő $k \times k$-as aldeterminánsokat ki tudjuk fejezni a V és A^{-1} mátrixok aldeterminánsaiból az alábbi tétel szerint:

3.16. Tétel (Cauchy-Binet formulák)**.** *Legyen $\mathbb{K}$ test és legyen A $m\times n$-es, B pedig $n\times m$-es mátrix $\mathbb{K}$ felett. Jelölje $A_{j_1,j_2,\dots,j_m}$ az A $j_1, j_2, \dots, j_m$ indexű oszlopaiból, $B_{j_1,j_2,\dots,j_m}$ pedig a B $j_1, j_2, \dots, j_m$ indexű soraiból képzett $m \times m$-es mátrixot ($1 \leq j_1, j_2, \dots, j_m \leq n$). Ekkor*

$$\det(AB) = \sum_{1\leq j_1<j_2<\dots<j_m\leq n} \det(A_{j_1,j_2,\dots,j_m}) \det(B_{j_1,j_2,\dots,j_m}).$$

3.17. Következmény. *Legyen $\mathcal{U} = \mathcal{U}_0^{k'}A \in G_q(k,n)$. Ekkor*

$$\begin{aligned} B_{S,\tau}^k(\mathcal{U}) = \Bigg\{ &\mathcal{V} = \mathrm{rs(V)} \in G_q(k,n) \colon \\ &\sum_{1\leq j_1<j_2<\dots<j_k\leq n} M_{j_1,j_2,\dots,j_k}(V) \det(A^{-1}_{j_1,j_2,\dots,j_k}[i_1,i_2,\dots,i_k]) = 0 \\ &\forall \quad (i_1,\dots,i_k) \not\preceq \left(\frac{k-k'+\tau}{2}+1,\dots,k', n-\frac{k-k'+\tau}{2}+1,\dots,n\right) \Bigg\}, \end{aligned}$$

ahol $A^{-1}_{j_1,j_2,\dots,j_k}[i_1,i_2,\dots,i_k]$ az A^{-1} mátrix $j_1, j_2, \dots, j_k$ indexű sorai és $i_1, i_2, \dots i_k$ indexű oszlopai által meghatározott részmátrixot jelöli.

Bizonyítás. Ahogy a 3.15 Állítás bizonyításában láttuk, $d_S(\mathcal{U}_0^{k'}A, \mathcal{V}) \leq \tau \Leftrightarrow d_S(\mathcal{U}_0^{k'}, \mathcal{V}A^{-1}) \leq \tau$. Továbbá a 3.16 Tétel szerint

$$M_{i_1,\dots,i_k}(VA^{-1}) = \sum_{1\leq j_1<j_2<\dots<j_k\leq n} M_{j_1,j_2,\dots,j_k}(V) \det(A^{-1}_{j_1,j_2,\dots,j_k}[i_1,i_2,\dots,i_k]).$$

Ezután alkalmazzuk a 3.12 Tételt. □

3.3. A gömbök jellemzése bilineáris egyenletekkel

3.18. Következmény. *Definiáljuk $\mathcal{U}_0^{k'}$-t úgy, mint eddig. Legyen $\nu := \frac{k-k'+\tau}{2}$. Ekkor*

$B_{S,\tau}^k(\mathcal{U}_0^{k'}) = \{\mathcal{V} = \mathrm{rs}[V_1V_2] \in G_q(k,n) \colon V_1 \in \mathbb{F}_q^{k\times k'}, \exists X \in \mathbb{F}_q^{k\times\nu}, Y \in \mathbb{F}_q^{\nu\times(n-k')} \colon V_2 = XY\}$.

Bizonyítás.

$$d_S(\mathcal{U}_0^{k'}, \mathcal{V}) \le \tau \iff \mathrm{rk}\begin{bmatrix} I_{k'} & 0_{k'\times(n-k')} \\ V_1 & V_2 \end{bmatrix} \le \frac{k+k'+\tau}{2}$$

$$\iff k' + \mathrm{rk}(V_2) \le \frac{k+k'+\tau}{2} \iff \mathrm{rk}(V_2) \le \nu.$$

Az utolsó állítás pedig azzal ekvivalens, hogy létezik olyan $X \in \mathbb{F}_q^{k\times\nu}$ és $Y \in \mathbb{F}^{\nu\times(n-k')}$, amire $V_2 = XY$. □

3.19. Megjegyzés. A gömböknek ezt a fajta leírását racionális paraméterezésnek is szokták nevezni. Ez az elnevezés onnan származik, hogy a legfeljebb ν rangú $k \times m$-es mátrixok ún. *racionális varietás*t alkotnak. Jelöljük ezen mátrixok halmazát $D_\nu^{k\times m}$-vel. Egy varietás akkor racionális, ha egy Zariski-nyílt halmaza megegyezik egy alkalmas vektortér egy nyílt halmazával. Esetünkben ez a következőt jelenti: Azonosítsuk azon $k \times \nu$-es mátrixokat, amelyeknek a felső $\nu \times \nu$-es részmátrixa invertálható, $\mathbb{F}_q^{k\nu}$ egy nyílt részhalmazával. Hasonlóan azonosítsuk azon $\nu \times m$-es mátrixokat, amelyekben az első $\nu \times \nu$-es részmátrix helyén az egységmátrix áll, a $\mathbb{F}_q^{\nu\times(m-\nu)}$ vektortérrel. Ekkor az alábbi leképezés ad egy paraméterezést:

$$f \colon \mathbb{F}_q^{k\nu} \times \mathbb{F}_q^{\nu\times(m-\nu)} \to D_\nu^{k\times m}$$
$$(X, Y) \mapsto XY.$$

Ahogy az előbb, a 3.15 Állítás segítségével a 3.18 Következmény alapján most is fel tudjuk írni, hogy milyen elemekből állnak azok a gömbök, amelyeknek a középpontja tetszőleges altér lehet:

3.20. Tétel. *Legyen $\mathcal{R} = \mathrm{rs}[R_1R_2] \in G_q(k',n)$ olyan, hogy $R_1 \in \mathbb{F}_q^{k'\times k'}, R_2 \in \mathbb{F}_q^{k'\times(n-k')}$. Definiáljuk ν-t úgy, mint az előbb. Ekkor létezik egy olyan $A \in GL(n,q)$ mátrix, amire $\mathcal{R} = \mathrm{rs}[I_{k'}0_{k'\times(n-k')}]A$. Ekkor*

$B_{S,\tau}^k(\mathcal{R}) = \{\mathcal{V} = \mathrm{rs}[V_1V_2]A \in G_q(k,n) \colon V_1 \in \mathbb{F}_q^{k\times k'}, \exists X \in \mathbb{F}_q^{k\times\nu}, Y \in \mathbb{F}_q^{\nu\times(n-k')} \colon V_2 = XY\}$.

3.21. Megjegyzés. Az A mátrixról tudjuk, hogy $\begin{bmatrix} R_1 & R_2 \\ R_3 & R_4 \end{bmatrix}$ alakú. Ezért $\mathrm{rs}[V_1V_2]A = rs[V_1R_1 + V_2R_3 \quad V_1R_2 + V_2R_4]$. Ha $\det(R_1) \neq 0$, akkor $\mathrm{rs}[R_1R_2] = \mathrm{rs}[I_{k'}\overline{R_2}]$. Ebben az esetben az átmeneti mátrix választható $A = \begin{bmatrix} I_{k'} & \overline{R_2} \\ 0 & I_{n-k'} \end{bmatrix}$-nak. Így a 3.20 Tétel egyszerűbb alakot ölt:

$B_{S,\tau}^k(\mathcal{R}) =$

$= \{\mathcal{V} = \mathrm{rs}[V_1 \quad V_1\overline{R_2} + V_2] \in G_q(k,n) \colon V_1 \in \mathbb{F}_q^{k\times k'}, \exists X \in \mathbb{F}_q^{k\times\nu}, Y \in \mathbb{F}_q^{\nu\times(n-k')} \colon V_2 = XY\}$,

3.22. Példa. Tekintsük $G_q(2,4)$-et és benne az $\mathcal{R} = \mathrm{rs}\begin{pmatrix}1 & 0 & 1 & 1\\ 0 & 1 & 0 & 1\end{pmatrix}$ alteret. Tehát most $n=4$, $k=k'=2$, és $\nu=1$. Ekkor az $\mathcal{R}$ középpontú, $\tau=2$ sugarú gömb

$$B^2_{S,2}(\mathcal{R}) = \left\{ \mathrm{rs}\left[V_1 \quad V_1\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} + V_2\right] \in G_q(2,4)\colon V_1 \in \mathbb{F}_q^{2\times 2}, \exists \mathbf{x}=(x_1,x_2),\right.$$
$$\left.\mathbf{y}=(y_1,y_2)\in\mathbb{F}_q^2\colon V_2 = \mathbf{x}^T\mathbf{y}\right\} =$$
$$= \left\{ \mathrm{rs}\begin{pmatrix}a & b & a+x_1y_1 & a+b+x_1y_2\\ c & d & c+x_2y_1 & c+d+x_2y_2\end{pmatrix} \in G_q(2,4)\colon a,b,c,d,x_1,x_2,y_1,y_2\in\mathbb{F}_q\right\}.$$

3.23. Példa. Nézzük meg, hogy adható meg ezzel a leírással a 3.14 Példa gömbje:

$$B^2_{S,3}(\mathcal{U}^3_0) = \left\{ \mathrm{rs}\begin{pmatrix}a & b & c & x_1y_1 & x_1y_2\\ d & e & f & x_2y_1 & x_2y_2\end{pmatrix} \in G_q(2,4)\colon a,b,c,d,e,f,x_1,x_2,y_1,y_2\in\mathbb{F}_q\right\}.$$

Ahogy az előző alfejezetbeli leírás lineáris egyenleteket szolgáltatott a gömb pontjainak Grassmann-koordinátáira, a fenti leírás a következő bilineáris egyenleteket adja a generáló mátrixok elemeire:

Az eddigi jelölések mellett rögzített $\mathcal{R}\in G_q(k',n)$ esetén a $\mathrm{rs}(V_1R_1+XYR_3 \quad V_1R_2+XYR_4)$ alakú $G_q(k,n)$-beli alterek lesznek benne $B^k_{S,\tau}(\mathcal{R})$-ben, ahol $V_1\in\mathbb{F}_q^{k\times k'}$, $X\in\mathbb{F}_q^{k\times\nu}$ és $Y\in\mathbb{F}_q^{\nu\times(n-k')}$. Legyen $\bar{V} := V_1R_2+XYR_4$ és $\hat{V} := V_1R_2+XYR_4$. Tehát a $(\bar{V} \quad \hat{V})$ mátrix elemeire azt kapjuk, hogy

$$\bar{V}_{ij} = \sum_{l=1}^{k'}(V_1)_{il}(R_1)_{lj} + \sum_{l=1}^{n-k'}\sum_{m=1}^{\nu} X_{im}Y_{ml}(R_3)_{lj},$$
$$\hat{V}_{ij} = \sum_{l=1}^{k'}(V_1)_{il}(R_2)_{lj} + \sum_{l=1}^{n-k'}\sum_{m=1}^{\nu} X_{im}Y_{ml}(R_4)_{lj}.$$

A dekódolás során ezeket az egyenleteket kell felírnunk olyan más egyenletek mellett, amelyek azt fejezik ki, hogy az alteret melyik (hány dimenziós) Grassmann-sokaságban keressük. (Lásd 3.4 Állítás.)

3.4. Az injektív távolság

A következő definíció egy másik lehetőséget ad az alterek közötti távolság értelmezésére.

3.24. Definíció. Az $\mathcal{U}$ és $\mathcal{V}$ $\mathbb{F}_q^n$-beli alterek *injektív távolságán* a

$$d_I(\mathcal{U},\mathcal{V}) = \max(\dim(\mathcal{U}),\dim(\mathcal{V})) - \dim(\mathcal{U}\cap\mathcal{V}) = \dim(\mathcal{U}+\mathcal{V}) - \min(\dim(\mathcal{U}),\dim(\mathcal{V}))$$

számot értjük.

3.25. Definíció. Legyen $\mathcal{R}$ tetszőleges altér $\mathbb{F}_q^n$-ben. Jelölje

$$B_{I,\tau}^k(\mathcal{R}) \coloneqq \{\mathcal{U} \in G_q(k,n) \colon d_I(\mathcal{R},\mathcal{U}) \leq \tau\}$$

az $\mathcal{R}$ középpontú, τ sugarú gömböt az injektív távolság szerint.

Vegyük észre, hogy az injektív távolságot csak $\dim(\mathcal{U}) \neq \dim(\mathcal{V})$ esetén érdemes külön vizsgálni, hiszen ha a két altér dimenziója megegyezik, akkor $d_S(\mathcal{U},\mathcal{V}) = 2d_I(\mathcal{U},\mathcal{V})$. Eltérő dimenziók esetén a következő állítás adja a d_S és d_I közötti kapcsolatot:

3.26. Állítás. *Legyen $\mathcal{U} \in G_q(k',n)$ és $\mathcal{V} \in G_q(k,n)$. Ekkor*

$$d_S(\mathcal{U},\mathcal{V}) = 2d_I(\mathcal{U},\mathcal{V}) + k + k' - 2\max(k',k) \tag{2}$$

és

$$B_{I,\tau}(\mathcal{U}) = B_{S,2\tau+k+k'-2\max(k',k)}(\mathcal{U}).$$

3.27. Állítás. *d_I metrika $\mathbb{F}_q^n$ összes altereinek halmazán.*

Bizonyítás. Most is csak a háromszög-egyenlőtlenséget bizonyítjuk, a többi metrikatulajdonság triviálisan teljesül. Legyenek $\mathcal{U},\mathcal{V}$ és $\mathcal{W}$ tetszőleges alterek $\mathbb{F}_q^n$-ben, dimenziójukat jelölje k_u, k_v illetve k_w. Azt szeretnénk belátni, hogy

$$d_I(\mathcal{U},\mathcal{V}) \leq d_I(\mathcal{U},\mathcal{W}) + d_I(\mathcal{W},\mathcal{V}),$$

amivel (2) miatt ekvivalens, hogy

$$d_S(\mathcal{U},\mathcal{V}) + 2\max(k_u,k_v) \leq d_S(\mathcal{U},\mathcal{W}) + d_S(\mathcal{V},\mathcal{W}) - 2k_w + 2\max(k_u,k_w) + 2\max(k_w,k_v).$$

Mivel d_S-re teljesül a háromszög-egyenlőtlenség, elég azt megmutatni, hogy

$$k_u \leq \max(k_u,k_w) + \max(k_w,k_v) - k_w$$

és

$$k_v \leq \max(k_u,k_w) + \max(k_w,k_v) - k_w.$$

Ez viszont igaz, mert $\max(k_v,k_w) - k_w$ és $\max(k_u,k_w) - k_w$ is legalább 0, valamint $k_u \leq \max(k_u,k_w)$ és $k_v \leq \max(k_w,k_v)$. Így k_u és k_v közül a nagyobbik is kisebb vagy egyenlő a jobboldalnál. □

Az injektív távolság szerinti Grassmann-gömbökre az altér távolság segítségével kimondottakkal teljesen analóg módon bizonyíthatók be az alábbi állítások:

3.28. Tétel. *Legyen $U_0^{k'} \coloneqq \mathrm{rs}[I_{k'}0_{k'\times n-k'}]$. Legyen τ olyan, hogy $|k-k'| \leq \tau < \min(\max(k',k), n-k+1)$. Ekkor*

$$B_{I,\tau}^k(\mathcal{U}_0^{k'}) = \{\mathcal{V} = \mathrm{rs(V)} \in G_q(k,n) \colon M_{i_1,\ldots,i_k}(V) = 0 \quad \forall \quad (i_1,\ldots,i_k)$$
$$\not\leq (k' - \max(k',k) + \tau + 1, \ldots, k', n-k+\max(k'k) - \tau + 1, \ldots, n)\}.$$

3.29. Állítás. *Legyen $\mathcal{U} \in G_q(k', n)$.*

1. *Ha $\tau = \min(\max(k, k'), n - \min(k, k'))$, akkor $B^k_{I,\tau}(\mathcal{U}) = G_q(k, n)$.*
2. *Ha $\tau < |k' - k|$, akkor $B^k_{I,\tau}(\mathcal{U}) = \emptyset$.*

3.30. Tétel. *Legyen $\mathcal{U} = \mathcal{U}_0^{k'} A \in G_q(k, n)$. Ekkor*

$$B^k_{I,\tau}(\mathcal{U}) = \{\mathcal{V} = \mathrm{rs(V)} \in G_q(k, n) \colon$$
$$\sum_{1 \le j_1 < j_2 < \cdots < j_k \le n} M_{j_1, j_2, \ldots, j_k}(V) \det(A^{-1}_{j_1, j_2, \ldots, j_k}[i_1, i_2, \ldots, i_k]) = 0$$
$$\forall \quad (i_1, \ldots, i_k) \not\leq (k' - \max(k', k) + \tau + 1, \ldots, k', n - k + \max(k', k) - \tau + 1, \ldots, n)\}.$$

3.31. Következmény. *Definiáljuk $\mathcal{U}_0^{k'}$-t úgy, mint eddig. Legyen $\omega \coloneqq \min(0, k - k') + t$. Ekkor*

$$B^k_{I,t}(\mathcal{U}_0^{k'}) = \{\mathcal{V} = \mathrm{rs}[V_1 V_2] \in G_q(k, n) \colon V_1 \in \mathbb{F}_q^{k \times k'}, \exists X \in \mathbb{F}_q^{k \times \omega}, Y \in \mathbb{F}_q^{\omega \times (n-k')} \colon V_2 = XY\}.$$

3.32. Tétel. *Legyen $\mathcal{R} = \mathrm{rs}[R_1 R_2] \in G_q(k', n)$ olyan, hogy $R_1 \in \mathbb{F}_q^{k' \times k'}, R_2 \in \mathbb{F}_q^{k' \times (n-k')}$. Definiáljuk ω-t úgy, mint az előbb. Ekkor létezik egy olyan $A \in GL(n, q)$ mátrix, amire $R = \mathrm{rs}[I_{k'} 0_{k' \times (n-k')}] A$. Ekkor*

$$B^k_{I,t}(\mathcal{R}) = \{\mathcal{V} = \mathrm{rs}[V_1 V_2] A \in G_q(k, n) \colon V_1 \in \mathbb{F}_q^{k \times k'}, \exists X \in \mathbb{F}_q^{k \times \omega}, Y \in \mathbb{F}_q^{\omega \times (n-k')} \colon V_2 = XY\}.$$

Továbbá a 3.21 Megjegyzés jelöléseivel

$$B^k_{I,t}(\mathcal{R}) =$$
$$= \{\mathcal{V} = \mathrm{rs}[V_1 \quad V_1 \overline{R_2} + V_2] \in G_q(k, n) \colon V_1 \in \mathbb{F}_q^{k \times k'}, \exists X \in \mathbb{F}_q^{k \times \omega}, Y \in \mathbb{F}_q^{\omega \times (n-k')} \colon V_2 = XY\}.$$

4. Altér kódok tulajdonságai

Ebben a fejezetben megvizsgáljuk, hogy milyen hibajavító tulajdonsággal rendelkeznek az altér kódok, illetve megnézzük, hogy mik az $\mathbb{F}_q$ feletti kódok méretére ismert becsléseknek a megfelelői altér kódokra. Csak azzal az esettel foglalkozunk, amikor minden kódszó dimenziója megegyezik. Az ilyen altér kódokat *Grassmann-kódoknak* is nevezik, mert a kód ez esetben egy Grassmann-sokaság részhalmaza.

4.1. Hibakezelés

Tekintsünk egy hálózatot egy adóval és egy vevővel. A nem koherens random hálózati kódolási modellben az üzenet sérülésének az alábbi két típusát különböztetjük meg:

1. Nem ér célba az összes továbbítandó csomag, azaz a küldött altér helyett a vevő egy másik, kisebb dimenziós alteret kap. Ez akkor fordul elő, ha az A átviteli mátrix rangja kisebb, mint a csomagok száma. Ennek oka lehet például, hogy a hálózatban a minimális vágás mérete túl kicsi. Ezt a továbbiakban *törlődésnek* (erasure) nevezzük.

2. A csomagok közül néhány útközben módosul, azaz hibavektorok adódnak hozzá a küldött csomagokhoz. Ez azt jelenti, az $\mathcal{U}$ altér helyett a vevő egy $\mathcal{U}+\mathcal{E}$ alteret kap, ahol $\mathcal{E}$ a hibák altere. Ez a jelenség a *hibásodás* (error).

Vezessünk be minden $k \geq 0$-ra egy, az $\mathbb{F}_q^n$ összes altereinek halmazán értelmezett „törlő-operátort", amely rögzített k esetén az alábbi módon van definiálva:

$$\mathcal{H}_k(\mathcal{U}) := \begin{cases} \mathcal{U} \text{ egy véletlen } k\text{-dimenziós altere} & \text{ha } \dim(\mathcal{U}) > k, \\ \mathcal{U} & \text{különben.} \end{cases}$$

Az most nem lényeges számunkra, hogy milyen eloszlás szerint választjuk az első esetben az alteret, de gondolhatunk például egyenletes eloszlásra.

Ha $\mathcal{U}$ és $\mathcal{V}$ egy vektortér alterei, akkor van olyan $\mathcal{V}'$ altér, amellyel $\mathcal{V} = (\mathcal{U} \cap \mathcal{V}) \oplus \mathcal{V}'$. (Ez a $\mathcal{V}'$ izomorf a $\mathcal{V}/(\mathcal{U} \cap \mathcal{V})$ faktortérrel.) Ezért az $\mathcal{U}+\mathcal{V}$ altérösszeget fel tudjuk írni direkt összegként, ha $\mathcal{V}$-t lecseréljük $\mathcal{V}'$-re: $\mathcal{U}+\mathcal{V} = \mathcal{U}+((\mathcal{U}\cap\mathcal{V})\oplus\mathcal{V}') = \mathcal{U}\oplus\mathcal{V}'$. Továbbá $\mathcal{U}$ mindig $\mathcal{H}_k(\mathcal{V}) \oplus \mathcal{E}$ alakba írható alkalmas $\mathcal{E}$ altérrel, feltéve, hogy $k = \dim(\mathcal{U}\cap\mathcal{V})$ és $\mathcal{H}_k(\mathcal{V}) = \mathcal{U}\cap\mathcal{V}$.

4.1. Definíció. Tegyük fel, hogy a hálózati kommunikáció során az adó az $\mathcal{V}$ alteret küldi el, a vevő pedig a $\mathcal{U}$ alteret kapja meg. Láttuk, hogy ekkor $\mathcal{U} = \mathcal{H}_k(\mathcal{V}) \oplus \mathcal{E}$, ahol $k = \dim(\mathcal{U}\cap\mathcal{V})$, és $\mathcal{E}$ a hibák altere. Azt mondjuk, hogy a kommunikáció során $\rho = \dim(\mathcal{V}) - k$ *törlődés* és $t = \dim(\mathcal{E})$ *hibásodás* történt.

Az $\mathbb{F}_q$ feletti kódok esetén a kódszavak között fellépő minimális Hamming-távolság segítségével tudtuk a kód által kijavított hibák maximális számát leírni. Az alábbi eredmény, melynek bizonyítása megtalálható a [22] cikkben, altér kódokra ad hasonló jellemzést:

4.2. Tétel. *Legyen C egy $\mathbb{F}_q^n$ feletti altér kód. A vevő pontosan akkor tudja az üzenetet dekódolni legfeljebb t hibásodás és ρ törlődés után, ha C-ben a kódszavak közötti d minimális injektív távolságra teljesül, hogy $d > 2t + \rho$.*

4.3. Megjegyzés. A tétel állítása $\rho = 0$ esetén rögtön következik a háromszög-egyenlőtlenségből.

Eszerint tehát az előző fejezetben definiált két metrika közül az injektív távolság alkalmas az altér kódok hibajavításának a karakterizációjára, az altér távolsággal csak elégséges feltételt tudunk adni adott mennyiségű hiba kijavítására, felhasználva, hogy $d_I \geq \frac{1}{2} d_S$. Azonban nem haszontalan az altér távolság sem: Abban az esetben, amikor a törlődések és hibásodások együttes számára van felső korlátunk, az altér távolságot érdemes nézni. Igaz ugyanis a következő:

4.4. Tétel. *Legyen C egy $\mathbb{F}_q^n$ feletti altér kód. Tegyük fel, hogy legfeljebb t hibásodás és ρ törlődés történhet. Ha C-ben a kódszavak közötti d minimális altér távolságra teljesül, hogy $d > 2(t + \rho)$, akkor a vevő dekódolni tudja az üzenetet.*

Bizonyítás. Legyen $\mathcal{V}' \coloneqq \mathcal{H}_k(\mathcal{V})$. A háromszögegyenlőtlenség szerint

$$d_S(\mathcal{V},\mathcal{U}) \leq d_S(\mathcal{V},\mathcal{V}') + d_S(\mathcal{V}',\mathcal{U}) \leq \rho + t.$$

Másrészt ha $\mathcal{M} \neq \mathcal{V}$, akkor

$$d \leq d_S(\mathcal{M},\mathcal{V}) \leq d_S(\mathcal{M},\mathcal{U}) + d_S(\mathcal{U},\mathcal{V})$$

$$\implies d_S(\mathcal{M},\mathcal{U}) \geq d - d_S(\mathcal{U},\mathcal{V}) > 2(t+\rho) - d_S(\mathcal{U},\mathcal{V}) \geq t + \rho.$$

Tehát egyetlen olyan altér van, ami a kapott $\mathcal{V}$ altértől legfeljebb $t + \rho$ altér távolságra van, mégpedig $\mathcal{U}$. □

4.2. Felső korlátok

Egy $\mathbb{F}_q$ feletti C kódot $(n,d)_q$-kódnak nevezünk, ha n hosszú szavakból áll, és a minimális Hamming-távolsága d. $\mathcal{A}(n,d)_q$ jelöli az $(n,d)_q$-kódok maximális méretét. $G_q(k,n)$ egy részhalmazát $[n,d,k]_q^I$-kódnak nevezzük, ha a minimális injektív távolság benne d, és $[n,d,k]_q^S$-kódnak, ha a minimális altér távolság benne d. Mivel minden $[n,d,k]_q^S$-kód egyben $[n,\frac{d}{2},k]_q^I$-kód is, a korlátokat csak $[n,d,k]_q^I$-kódokra bizonyítjuk. $\mathcal{A}[n,d,k]_q$ jelöli a $[n,d,k]_q^I$-kódok maximális méretét. Mivel $\mathcal{A}[n,d,k]_q = \mathcal{A}[n,d,n-k]_q$, ezért mindig feltehetjük, hogy $k \leq \left\lfloor \frac{n}{2} \right\rfloor$.

4.5. Tétel (Gömbpakolási (Hamming-) korlát $\mathbb{F}_q$ feletti kódokra, [19])**.** *Legyen $d \leq n$. Ekkor*

$$\mathcal{A}(n,d)_q \leq \frac{q^n}{\sum_{k=0}^{t} \binom{n}{k} (q-1)^k},$$

ahol $t = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Bizonyítás. Legyen C egy $(n,d)_q$-kód. Mivel C-ben a minimális távolság d, a kódszavak köré írt $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ sugarú Hamming-gömbök $\mathbb{F}_q^n$-ben diszjunktak. Így legfeljebb annyi kódszó lehet C-ben, ahány diszjunkt $\mathbb{F}_q^n$-beli t sugarú Hamming-gömb van. Ezek száma legfeljebb $\frac{q^n}{\sum_{k=0}^{t}\binom{n}{k}(q-1)^k}$, ahol $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ lehet. A tört számlálójában az $\mathbb{F}_q^n$-beli pontok száma, a nevezőjében pedig egy t sugarú Hamming-gömb térfogata szerepel, amit úgy kapunk meg, hogy minden $0 \le k \le t$-re összeadjuk a középponttól éppen k távolságra lévő pontok számát. □

4.6. Megjegyzés ([19])**.** Azon $\mathbb{F}_q$ feletti kódok, amelyek a gömbpakolási korlátot egyenlőséggel teljesítik, az ún. *perfekt kódok*. Ilyenre kevés példa van, ezek egyike a *Hamming-kód*, amelyet a következőképpen adhatunk meg: Rögzített k esetén legyen $n \coloneqq \begin{bmatrix} k \\ 1 \end{bmatrix}_q$, és készítsük el azt az $M \in \mathbb{F}_q^{k\times n}$ mátrixot, amelynek oszlopait az $\mathbb{F}_q^k$ vektortér n darab egyenesének egy-egy irányvektora alkotja. (Ez a mátrix persze nem egyértelmű. Egy lehetőség, hogy minden egyenesnek azt az irányvektorát vesszük be a mátrix oszlopai közé, amelyben balról az első nemnulla koordináta értéke 1.) Legyen $Ham(k,q)$ az az n hosszú, $(n-k)$-dimenziós lineáris kód, amelynek M a paritásellenőrző mátrixa. Az így definiált kód valóban perfekt, hiszen elemszáma q^{n-k}, valamint a 2.44 Állításból következik, hogy a minimális távolsága 3, ezért a gömbpakolási korlát ebben az esetben

$$\frac{q^n}{1+n(q-1)} = \frac{q^n}{1+\frac{q^k-1}{q-1}(q-1)} = \frac{q^n}{1+q^k-1} = q^{n-k}.$$

A minimális távolság értékéből látszik, hogy a Hamming-kódok 1-hibajavítók.

4.7. Tétel (Gömbpakolási (Hamming-) korlát Grassmann-kódokra, [15])**.** *Legyen $d \le k \le n$. Ekkor*

$$\mathcal{A}[n,d,k]_q \le \frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{\sum_{i=0}^{t} q^{i^2}\begin{bmatrix} k \\ i \end{bmatrix}_q\begin{bmatrix} n-k \\ i \end{bmatrix}_q},$$

ahol $t = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Bizonyítás. Azt kell belátni, hogy az egy rögzített $\mathcal{V} \in G_q(k,n)$ altértől pontosan i injektív távolságra levő pontok száma $q^{i^2}\begin{bmatrix} k \\ i \end{bmatrix}_q\begin{bmatrix} n-k \\ i \end{bmatrix}_q$. Ha ez sikerül, akkor az előző bizonyítás gondolatmenetével pont a kívánt eredményt kapjuk. Ehhez a következőt igazoljuk:

4.8. Állítás. *Legyen $k \le n$, $j \le n$ és $l \le \min(j,k)$. Legyen $\mathcal{V} \in G_q(k,n)$. Ekkor*

$$|\{\mathcal{W} \in G_q(j,n)\colon \mathcal{V}\cap\mathcal{W} \in G_q(l,n)\}| = q^{(j-l)(k-l)}\begin{bmatrix} k \\ l \end{bmatrix}_q\begin{bmatrix} n-k \\ j-l \end{bmatrix}_q.$$

Bizonyítás. $\mathcal{U} = \mathcal{V}\cap\mathcal{W}$-t $\begin{bmatrix} k \\ l \end{bmatrix}_q$-féleképpen választhatjuk ki. Ezt szeretnénk j-dimenziós altérré kiegészíteni. Először választunk $\mathcal{U}$-hoz egy tetszőleges vektort, ami nincs $\mathcal{V}$-ben, ezt (q^n-q^k)-féleképpen tehetjük meg. Ezután (q^n-q^{k+1})-féleképpen vehetünk egy újabb vektort, ami nincs benne az $\mathcal{U}$ és az előbb választott vektor által generált $k+1$ dimenziós altérben. Ezt addig folytatjuk, amíg a generált altér j-dimenziós nem lesz. Így

minden lehetséges kiegészítését $\mathcal{U}$-nak annyiszor számoltuk, ahányféleképpen $\mathcal{U}$ bázisát kiegészíthetjük egy rögzített $\mathcal{W}$ bázisává, azaz $(q^j - q^l)(q^j - q^{l+1}) \dots (q^j - q^{j-1})$-szer. Tehát a megfelelő kiegészítések száma

$$\frac{(q^n - q^k)(q^n - q^{k+1}) \dots (q^n - q^{k+j-l-1})}{(q^j - q^l)(q^j - q^{l+1}) \dots (q^j - q^{j-1})} = q^{(j-l)(k-l)} \begin{bmatrix} n-k \\ j-l \end{bmatrix}_q.$$

□

A 4.7 Tétel bizonyításának befejezéséhez a 4.8 Állításban $j = k$ és $l = k - i$ választást alkalmazunk. □

4.9. Tétel (Singleton-korlát $\mathbb{F}_q$ feletti kódokra, [19])**.** *Legyen $d \leq n$. Ekkor*

$$\mathcal{A}(n, d)_q \leq q^{n-d+1}. \tag{3}$$

Bizonyítás. Legyen C egy $(n, d)_q$-kód. Válasszunk ki $d - 1$ koordinátát és töröljük ki ezeket a koordinátákat C minden szavából. Az így keletkező $n - d + 1$ hosszú szavak mind különbözőek, mert ha két szóból is ugyanazt kaptuk volna, akkor azok legfeljebb $d - 1$ koordinátában térhettek volna el egymástól. Ezért C mérete nem lehet nagyobb az $n - d + 1$ hosszú $\mathbb{F}_q$ feletti szavak számánál. □

4.10. Megjegyzés ([16])**.** Azon $\mathbb{F}_q$ feletti kódok, amelyek a Singleton-korlátot egyenlőséggel teljesítik, az ún. *MDS-kódok* (maximum distance separable codes). Lineáris k-dimenziós kódok esetén a (3) egyenlőtlenség azzal ekvivalens, hogy $k \leq n - d + 1$. Tehát egy lineáris k-dimenziós kód akkor lesz MDS-kód, ha a minimális távolsága $d = n - k + 1$. Ilyen kódok nem minden (n, k) párhoz léteznek. A 2.44 Állításból következik, hogy adott n és k természetes számok esetén pontosan akkor létezik $\mathbb{F}_q^n$-ben k-dimenziós MDS-kód, ha $PG(n - k - 1, q)$-ban létezik n-ív, azaz n olyan pont, amelyek közül semelyik $n - k$ nincs egy hipersíkban. Ugyanis egy n-ív pontjait reprezentáló $\mathbb{F}_q^n$-beli vektorok megfeleltethetők egy $M \in \mathbb{F}_q^{(n-k)\times n}$ paritásellenőrző mátrix n darab oszlopának, amelyek közül bármelyik $n - k$ lineárisan független.

4.11. Tétel (Singleton-korlát Grassmann-kódokra, [15], [18])**.** *Legyen $d \leq k \leq n$. Ekkor*

$$\mathcal{A}[n, d, k]_q \leq \begin{bmatrix} n-d+1 \\ k-d+1 \end{bmatrix}_q.$$

Bizonyítás. Legyen C egy $[n, d, k]_q^I$-kód. Az előzőhöz hasonlóan szeretnénk csökkenteni C dimenzióját. Ehhez bevezetjük az alábbi „pontozó" műveletet: Jelölje $\mathcal{W}$ az $\mathbb{F}_q^n$ vektorteret, és válasszuk ki $\mathcal{W}$ egy $\mathcal{W}'$ $(n-1)$-dimenziós alterét. Rögzített $\mathcal{V} \in C$ esetén definiáljuk a $\mathcal{V}' := \mathcal{H}_{k-1}(\mathcal{V} \cap \mathcal{W}')$ $(k-1)$-dimenziós alteret. (Itt $\mathcal{H}_{k-1}$ az előző szakaszban bevezetett törlő operátor.) Ezt C minden elemére elvégezve kapunk egy (nem egyértelműen meghatározott) $C' = \{\mathcal{V}' \colon \mathcal{V} \in C\}$ $[n-1, d', k-1]_q$-kódot. Azt állítjuk, hogy $d' \leq d - 1$. Valóban, mivel $\mathcal{U}' \subseteq \mathcal{U}$ és $\mathcal{V}' \subseteq \mathcal{V}$, $\mathcal{U}' \cap \mathcal{V}' \subseteq \mathcal{U} \cap \mathcal{V}$ is igaz, továbbá $d_I(\mathcal{U}, \mathcal{V}) \geq d$, ezért

$$\dim(\mathcal{U}' \cap \mathcal{V}') \leq \dim(\mathcal{U} \cap \mathcal{V}) \leq k - d$$

$$\Longrightarrow d' \geq d_I(\mathcal{U},\mathcal{V}) = (k-1) - \dim(\mathcal{U}' \cap \mathcal{V}') \geq (k-1) - (k-d) = d-1.$$

Ha ezt a műveletet megismételjük $(d-1)$-szer, akkor kapunk egy C'' $[n-d+1, d'', k-d+1]_q$-kódot, ahol $d'' \geq 1$, vagyis C'' $G_q(n-d+1, k-d+1)$ csupa különböző elemeiből áll, és $|C''| = |C|$. Ezért C mérete nem lehet nagyobb $G_q(n-d+1, k-d+1)$ méreténél, ami $\begin{bmatrix} n-d+1 \\ k-d+1 \end{bmatrix}_q$. □

$\mathcal{A}(n,d,w)_q$-val jelöljük az olyan $\mathbb{F}_q$ feletti kódok maximális méretét, amelyekben minden kódszó Hamming-súlya w. Azon kódokat, amelyekre igaz ez a tulajdonság, $(n,d,w)_q$-kódoknak nevezzük. Ezek a konstans dimenziójú kódok (azaz a Grassmann-kódok) $\mathbb{F}_q$ feletti megfelelői. Nyilvánvaló, hogy ha $w < \frac{d}{2}$, akkor $\mathcal{A}(n,d,w)_q = 1$.

4.12. Tétel (Johnson-korlát $\mathbb{F}_q$ feletti kódokra, [19])**.** *Legyen $w \leq n$, $d \leq min(n, 2w)$. Ekkor*

$$\mathcal{A}(n,d,w)_q \leq \left\lfloor \frac{n(q-1)}{w} \mathcal{A}(n-1,d,w-1)_q \right\rfloor.$$

Bizonyítás. Legyen C egy $(n,d,w)_q$-kód. Ha tetszőlegesen rögzítünk egy $1 \leq i \leq n$ számot, és egy $0 \neq x \in \mathbb{F}_q$ elemet – amit $n(q-1)$-féleképpen tehetünk meg –, akkor legfeljebb $\mathcal{A}(n-1,d,w-1)_q$ olyan kódszó lehet C-ben, aminek az i. koordinátája x, és minden kódszóban w nemnulla koordináta van. □

4.13. Következmény. *Legyen $w \leq n$, $d \leq min(n, 2w)$. Ekkor*

$$\mathcal{A}(n,d,w)_q \leq \left\lfloor \frac{n(q-1)}{w} \left\lfloor \frac{(n-1)(q-1)}{w-1} \left\lfloor \dots \left\lfloor \frac{(n-w+\lceil \frac{d}{2} \rceil)(q-1)}{\lceil \frac{d}{2} \rceil} \right\rfloor \dots \right\rfloor \right\rfloor \right\rfloor.$$

4.14. Tétel (Johnson-korlát Grassmann-kódokra, [11])**.** *Legyen $d \leq k \leq n$. Ekkor*

$$\mathcal{A}[n,d,k]_q \leq \left\lfloor \frac{q^n-1}{q^k-1} \mathcal{A}[n-1,d,k-1]_q \right\rfloor.$$

Bizonyítás. Legyen C egy $[n,d,k]_q^I$-kód. Ha tetszőlegesen rögzítünk a tér $\frac{q^n-1}{q-1}$ egyenese közül egyet, akkor arra legfeljebb $\mathcal{A}[n-1,d,k-1]_q$ C-beli kódszó illeszkedhet, és minden kódszó $\frac{q^k-1}{q-1}$ egyenest tartalmaz. □

4.15. Következmény. *Legyen $d \leq k \leq n$. Ekkor*

$$\mathcal{A}[n,d,k]_q \leq \left\lfloor \frac{q^n-1}{q^k-1} \left\lfloor \frac{q^{n-1}-1}{q^{k-1}-1} \left\lfloor \dots \left\lfloor \frac{q^{n-k+d}-1}{q^d-1} \right\rfloor \dots \right\rfloor \right\rfloor \right\rfloor.$$

Bizonyítás. Elég belátni, hogy $\mathcal{A}[n-k+d,d,d]_q \leq \left\lfloor \frac{q^{n-k+d}-1}{q^d-1} \right\rfloor$. Az, hogy egy d dimenziós alterekből álló kódban a minimális injektív távolság d, azt jelenti, hogy az alterek csak az origóban metszik egymást. Ezeket tekinthetjük $PG(n-k+d-1,q)$ diszjunkt $(d-1)$-dimenziós projektív altereinek is. Ezért a számuk legfeljebb akkora, mint ha elosztjuk $PG(n-k+d-1)$ pontjainak számát egy $(d-1)$-dimenziós projektív altér pontjainak számával. □

4.16. Megjegyzés. A 4.15 Következményt azért mondtuk ki ebben a formában, mert az volt a célunk, hogy az $\mathbb{F}_q$ feletti kódokra vonatkozó 4.13 Következménnyel analóg állítást írjunk fel. Azonban a fenti bizonyításban szereplő felső becslésnél általában jobbat is tudunk adni $\mathcal{A}[n-k+d,d,d]_q$-re, sőt ennek a pontos értékét is ismerjük, ahogy azt majd látni fogjuk később, a részleges befedésekről szóló alfejezetben.

4.3. Alsó korlátok

4.17. Tétel (Gömbbefedési (Gilbert–Varshamov-) korlát $\mathbb{F}_q$ feletti kódokra, [19])**.** *Legyen $d \leq n$. Ekkor*

$$\mathcal{A}(n,d)_q \geq \frac{q^n}{\sum_{j=0}^{d-1}\binom{n}{j}(q-1)^j}.$$

Bizonyítás. Legyen C egy maximális $(n,d)_q$-kód, azaz $|C| = \mathcal{A}(n,d)_q$. Vegyünk egy tetszőleges $x \in \mathbb{F}_q^n$ elemet. Ehhez tudunk találni legalább egy olyan $c_x \in C$ kódszót, amelyre $d_H(x,c_x) \leq d-1$. Ugyanis ha az $x \in \mathbb{F}_q^n \backslash C$ elemhez nem lenne ilyen c_x, akkor x-et bevehetnénk C-be úgy, hogy az még mindig $(n,d)_q$-kód maradna, ami ellentmond C maximalitásának. Tehát

$$\mathbb{F}_q^n = \bigcup_{c\in C} B_{H,d-1}(c),$$

ahol $B_{H,d-1}(c)$ a c középpontú, $d-1$ sugarú Hamming-gömböt jelöli. Láttuk, hogy ennek a térfogata a középponttól függetlenül $\sum_{j=0}^{d-1}\binom{n}{j}(q-1)^j$. Vagyis azt kaptuk, hogy

$$q^n = |\mathbb{F}_q^n| = \Big|\bigcup_{c\in C} B_{H,d-1}(c)\Big| \leq \sum_{c\in C}|B_{H,d-1}(c)| = \mathcal{A}(n,d)_q \sum_{j=0}^{d-1}\binom{n}{j}(q-1)^j.$$

Ez pedig átrendezve pont a bizonyítandó állítás. □

Ha az előző érvelésben $\mathbb{F}_q^n$-t $G_q(k,n)$-re, a Hamming-távolságot pedig az injektív távolságra cseréljük, akkor a Grassmann-kódokra kapunk egy hasonló korlátot:

4.18. Tétel (Gömbbefedési (Gilbert–Varshamov-)korlát Grassmann-kódokra, [15])**.** *Legyen $d \leq k \leq n$. Ekkor*

$$\mathcal{A}[n,d,k]_q \geq \frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{\sum_{i=0}^{d-1} q^{i^2}\begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} n-k \\ i \end{bmatrix}_q}.$$

Altér kódok esetében a legjobb ismert alsó korlátok konstrukciókból származnak. Ilyenekre fogunk látni példákat a következő fejezetben.

5. Konstrukciók

5.1. Mátrix kódok felemelése

Amint azt már a Bevezetésben is említettük, az altér kódok azért hasznosak, mert nem koherens hálózati kódolásnál – ami majdnem olyan hatékony, mint a koherens változat, viszont bizonyos szempontból praktikusabb – az üzenet alkotta mátrixnak a sortere az, ami invariáns marad a kommunikáció során. Ha viszont a kommunikációban részt vevő felek ismerik a hálózat belső szerkezetét, vagyis a küldött csomagokon végzett műveleteket, akkor a vevő ennek ismeretében magát a küldött mátrixot is dekódolhatja. Ilyenkor mátrix kódokat érdemes alkalmazni. Ezeket *rank-metric kódoknak* is hívják, utalva arra, hogy hogyan mérjük bennük a kódszavak távolságát:

5.1. Definíció. Legyenek $A, B \in \mathbb{F}_q^{k\times m}$. Az A és B *rang távolsága*

$$d_R(A,B) = \mathrm{rk}(A-B).$$

5.2. Állítás. *A rang távolság metrika az összes $\mathbb{F}_q^{k\times m}$-beli mátrixok halmazán.*

Bizonyítás. Egy mátrix rangja nemnegatív szám, a nullmátrixé 0, és minden tőle különböző mátrixé nagyobb, mint 0. A (-1)-gyel való szorzás nem változtat a rangon, ezért d_R szimmetrikus. Ezen kívül

$$\mathrm{rk}(A-C) = \mathrm{rk}((A-B)+(B-C)) \le \mathrm{rk}(A-B)+\mathrm{rk}(B-C)$$

is teljesül, mivel tetszőleges $U, V \in \mathbb{F}_q^{k\times m}$ mátrixokra $\mathrm{rs}(U+V) \subseteq \mathrm{rs}(U)+\mathrm{rs}(V)$, és ebből valamint a dimenzióformulából következik, hogy

$$\dim(\mathrm{rs}(U+V)) \le \dim(\mathrm{rs}(U)+\mathrm{rs}(V)) \le \dim(\mathrm{rs}(U))+\dim(\mathrm{rs}(V)).$$

□

Legyen $M \subseteq \mathbb{F}_q^{k\times(n-k)}$ egy mátrix kód. Ebből elkészíthetjük az alábbi k-dimenziós Grassmann-kódot:

$$G \coloneqq \{\mathrm{rs}([I_k|A])\colon A \in M\} \subseteq G_q(k,n).$$

Ez az eljárás az M kód *felemelése*. Az alábbi lemma azt mutatja, hogy a felemelt kód az eredeti kóddal izometrikus:

5.3. Lemma. *Legyen $U, V \in \mathbb{F}_q^{k\times(n-k)}$, $\mathcal{U} = \mathrm{rs}([I_k|U])$ és $\mathcal{V} = \mathrm{rs}([I_k|V])$. Ekkor*

$$d_I(\mathcal{U},\mathcal{V}) = d_R(U,V).$$

Bizonyítás. Tekintsük az $\left[\begin{array}{c|c} I_k & U \\ \hline I_k & V \end{array}\right]$ mátrixot, melynek sortere $\mathcal{U}+\mathcal{V}$. Ez elemi sortranszformációs lépésekkel $\left[\begin{array}{c|c} I_k & U \\ \hline 0 & V-U \end{array}\right]$ alakra hozható. $\mathcal{U}+\mathcal{V}$ dimenziója ennek a mátrixnak a rangjával egyenlő, ami $k+\mathrm{rk}(V-U)$. Tehát

$$d_I(\mathcal{U},\mathcal{V}) = \dim(\mathcal{U}+\mathcal{V}) - k = \mathrm{rk}(V-U) = d_R(U,V).$$

□

5.4. Állítás (Singleton-korlát mátrix kódokra)**.** *Legyen* $1 \leq d \leq \min(k, m)$*. Legyen* $M \subseteq \mathbb{F}_q^{k\times m}$ *egy mátrix kód, melyben a kódszavak között fellépő minimális rang távolság* d*. Ekkor* M *maximális mérete legfeljebb*

$$\min(q^{m(k-d+1)}, q^{k(m-d+1)}).$$

Bizonyítás. Feltehetjük, hogy $k \leq m$, ugyanis ha transzponáljuk az összes M-beli mátrixot, akkor nem változik a rang távolságuk. Azt kell belátnunk, hogy $|M| \leq q^{m(k-d+1)}$. M-et tekinthetjük egy $\mathbb{F}_{q^m}$ feletti k hosszú kódnak, melynek minimális távolsága legalább d. Ugyanis ha lenne két mátrix M-ben, amelyeknek legfeljebb $d-1$ különböző sora van (vagyis legalább $k-d+1$ sorukban megegyeznek), akkor a különbségük rangja legfeljebb $k-(k-d+1) = d-1$ lehetne. Alkalmazva a 4.9 Tételt a kívánt eredményt kapjuk. □

5.5. Definíció. Azon $M \subseteq \mathbb{F}_q^{k\times m}$ mátrix kódokat, amelyek a fenti egyenlőtlenséget egyenlőséggel teljesítik, *MRD-kódoknak* (maximum rank distance codes) nevezzük.

5.6. Megjegyzés. Eszerint tehát az MRD-kódok speciális MDS-kódok.

Az alábbi állítás bizonyítása megtalálható a [18] cikkben:

5.7. Állítás. *Tetszőleges* $1 \leq d \leq \min(k, m)$ *egész számok esetén létezik olyan* $M \subseteq \mathbb{F}_q^{k\times m}$ *MRD-kód, amelyben a kódszavak között fellépő minimális rang távolság* d*.*

Az MRD-kódokból pedig felemeléssel készíthetünk altér kódokat, így ezek maximális méretére a következő alsó korlát adódik:

5.8. Következmény. $\mathcal{A}[n, d, k]_q \geq \min(q^{(n-k)(k-d+1)}, q^{k(n-k-d+1)})$.

5.2. $\mathcal{A}[n, k, k]_q$ és a véges projektív terek (részleges) befedései

A 2.26 Tétel szerint $PG(n-1, q)$-nak pontosan akkor létezik $(k-1)$-befedése, ha $k|n$. Ebben az esetben egy $(k-1)$-befedés $PG(n-1, q)$-ban tekinthető egy maximális $[n, k, k]_q^I$-kódnak, amelynek a számossága ekkor

$$\mathcal{A}[n, k, k]_q = \frac{\begin{bmatrix} n \\ 1 \end{bmatrix}_q}{\begin{bmatrix} k \\ 1 \end{bmatrix}_q}.$$

$PG(n-1, q)$ egy részleges $(k-1)$-befedése pedig egy (nem szükségképpen maximális) $[n, k, k]_q^I$-kód. Így ezeknek a véges geometriában már régóta tanulmányozott objektumoknak az elmélete újabb motivációt nyert az altér kódoknak köszönhetően.

Jelölje $\mu_q(n, k) = \mathcal{A}[n, k, k]_q$ a $PG(n-1, q)$-beli $(k-1)$-befedések maximális méretét. Az előzőek szerint $n \equiv 0 \mod k$ esetén ismerjük $\mu_q(n, k)$ értékét. Mit mondhatunk akkor, ha $n \equiv r \mod k$ tetszőleges $1 \leq r \leq k-1$ egész számra? Ki fog derülni, hogy ilyenkor is a legtöbb n, q és k paraméterérték esetén meg tudjuk mondani $\mu_q(n, k)$ értékét, ugyanis igaz a következő tétel:

5.9. Tétel. *Legyen* $0 \leq r < k \leq \left\lfloor \frac{n}{2} \right\rfloor$, *és tegyük fel, hogy* $n \equiv r \mod k$. *Ekkor ha*

$$k > \begin{bmatrix} r \\ 1 \end{bmatrix}_q, \tag{4}$$

akkor a $PG(n-1,q)$*-beli* $(k-1)$*-befedések maximális mérete*

$$\mu_q(n,k) = \frac{q^n - q^{k+r}}{q^k - 1} + 1. \tag{5}$$

A Tételt két lépésben fogjuk igazolni: Egyrészt megadunk egy $\frac{q^n - q^{k+r}}{q^k - 1} + 1$ méretű részleges befedést $PG(n-1,q)$-ban (ehhez még nem lesz szükségünk a (4) feltételre), másrészt bebizonyítjuk, hogy ennél nagyobb részleges befedés nem létezhet a $PG(n-1,q)$ térben. Lássuk először a konstrukciót.

5.10. Lemma. $PG(n-1,q)$*-nak létezik egy olyan* q^{n-k} *méretű részleges* $(k-1)$*-befedése, amely pontosan az*

$$S = \{\mathbf{x} \in \mathbb{F}_q^n \colon x_1 = x_2 = \cdots = x_k = 0\}$$

$(n-k)$*-dimenziós* $\mathbb{F}_q^n$*-beli altérnek megfelelő* $(n-k-1)$*-dimenziós projektív altéren kívül eső pontokat fedi.*

Bizonyítás. Tekintsük az $\mathbb{F}_{q^{n-k}}$ testet, ami egy $(n-k)$-dimenziós vektortér $\mathbb{F}_q$ felett. Rögzítsük ennek a vektortérnek egy bázisát, és minden $\alpha \in \mathbb{F}_{q^{n-k}}$ elemre tekintsük az alábbi $\mathbb{F}_q$-lineáris leképezést:

$$\begin{aligned} M(\alpha) \colon \mathbb{F}_{q^{n-k}} &\to \mathbb{F}_{q^{n-k}} \\ x &\mapsto \alpha x \end{aligned}$$

Ezeket a leképezéseket a rögzített bázisban felírva $\mathbb{F}_q$ feletti $(n-k)\times(n-k)$-as mátrixokkal reprezentálhatjuk. Jelöljük $\mathscr{D}$-vel ezen mátrixok halmazát. Világos, hogy tetszőleges $\alpha, \beta \in \mathbb{F}_{q^{n-k}}$ elemekre $M(\alpha+\beta) = M(\alpha) + M(\beta)$, $M(\alpha\beta) = M(\alpha)M(\beta)$, valamint $M(1) = I_{n-k}$. Ebből következik, hogy a $\mathscr{D}$-beli mátrixok közül $M(0)$-t kivéve mindegyik invertálható ($(M(\alpha))^{-1} = M(\alpha^{-1})$), és $\mathscr{D}$ bármely két különböző elemének a rang távolsága $n-k$, hiszen ha $\alpha \neq \beta$ két különböző testelem $\mathbb{F}_{q^{n-k}}$-ban, akkor $\mathrm{rk}(M(\alpha) - M(\beta)) = \mathrm{rk}(M(\alpha-\beta)) = n-k$.

Tekintsük azt a $\mathscr{D}'$ mátrix kódot, amelyet úgy kapunk, hogy $\mathscr{D}$ elemeinek az utolsó $n-2k \geq 0$ sorát töröljük. Ekkor $\mathscr{D}'$ mérete q^{n-k}, minimális rang távolsága pedig k. Készítsük el ennek a kódnak a felemeltjét az előző szakaszban ismertetett módon. Ekkor az 5.3 Lemma szerint egy olyan Grassmann-kódhoz jutunk, melynek dimenziója és minimális injektív távolsága is k, erről pedig már láttuk, hogy egy $(k-1)$-befedésnek felel meg $PG(n-1,q)$-ban.

A felemeléssel kapott kódban szereplő alterek nyilván csak S-en kívüli pontokat tartalmazhatnak, hiszen minden alteret előállító mátrix első k oszlopában az egységmátrix áll, tehát ezek az oszlopok lineárisan függetlenek. Belátjuk, hogy minden S-en kívül eső

pont fedve van. Valóban, legyen $\mathbf{p} \in \mathbb{F}_q^n \backslash S$ tetszőleges. Ekkor $\mathbf{p} = (\mathbf{a}|\mathbf{b})$ alakú, ahol $\mathbf{a} \in \mathbb{F}_q^k \backslash \{\mathbf{0}\}$ és $\mathbf{b} \in \mathbb{F}_q^{n-k}$. Vegyük észre, hogy ha $X \neq X'$ két mátrix $\mathscr{D}'$-ben, akkor $\mathbf{a}X \neq \mathbf{a}X'$, ugyanis $X - X'$ teljes rangú, így $\mathbf{a}X - \mathbf{a}X' = \mathbf{a}(X - X')$ nem lehet $\mathbf{0}$. Ezért az $\{\mathbf{a}X \colon X \in \mathscr{D}'\}$ halmaz számossága megegyezik $\mathscr{D}'$ számosságával, ami q^{n-k}, vagyis minden $n-k$ hosszú $\mathbb{F}_q$ feletti vektor előáll $\mathbf{a}X$ alakban. Speciálisan $\mathbf{b}$ is előáll, tehát létezik egy olyan $D \in \mathscr{D}'$, amellyel $\mathbf{a}D = \mathbf{b}$. Ekkor viszont $\mathbf{p}$ előáll az $(I_k|D)$ mátrix sorainak lineáris kombinációjaként. (A lineáris kombinációban szereplő együtthatókat az $\mathbf{a}$ komponensei adják meg.) □

A fenti lemma segítségével most már elkészíthetjük a megfelelő méretű befedést:

5.11. Tétel. *Legyen* $0 \leq r < k \leq \left\lfloor \frac{n}{2} \right\rfloor$ *és* $n \equiv r \mod k$. *Ekkor* $PG(n-1,q)$*-nak létezik*

$$\frac{q^n - q^{k+r}}{q^k - 1} + 1$$

méretű részleges $(k-1)$*-befedése.*

Bizonyítás. Legyen $n = tk + r$. Az 5.10 Lemmát használva t szerinti teljes indukcióval belátjuk, hogy létezik $PG(n-1,q)$-nak

$$1 + \sum_{i=1}^{t-1} q^{ik+r}$$

méretű részleges $(k-1)$-befedése. A $t = 1$ esetből indulunk ki. Ekkor az az állításunk, hogy $k \leq n < 2k$ esetén ki tudunk választani $PG(n-1,q)$-ban egy $(k-1)$-dimenziós alteret, ami nyilván teljesül. Az indukciós lépéshez tegyük fel, hogy van $PG(n-k-1,q)$-ban egy

$$1 + \sum_{i=1}^{t-2} q^{ik+r}$$

méretű részleges $(k-1)$-befedésünk. Ebből úgy kapjuk a $PG(n-1,q)$ tér megfelelő méretű befedését, hogy az 5.10 Lemmában szereplő S altérnek megfelelő projektív altérben, ami izomorf $PG(n-k-1,q)$-val, vesszük az indukciós feltevés miatt létező altereket, és ezt kiegészítjük azzal a $q^{n-k} = q^{(t-1)k+r}$ darab altérrel, amelyek a Lemma szerint az S-en kívül eső pontokat fedik. Végül használjuk fel, hogy

$$\sum_{i=1}^{t-1} q^{ik+r} = \frac{q^n - q^{k+r}}{q^k - 1}.$$

□

Az (5) egyenlet másik irányú egyenlőtlenségének igazolásához először bevezetjük az altér partíciók fogalmát.

5.12. Definíció. Az $\mathbb{F}_q^n$ vektortér nemtriviális altereinek egy $\mathscr{P}$ rendszerét $\mathbb{F}_q^n$ *altér partíciójának* nevezzük, ha $\mathbb{F}_q^n$ minden 0-tól különböző pontja pontosan egy $\mathscr{P}$-beli altérben van benne. Tegyük fel, hogy a $\mathscr{P}$-ben szereplő alterek dimenzióiként a $d_s > \cdots > d_1$ számok fordulnak elő, és az i-dimenziós alterek száma $\mathscr{P}$-ben n_i. Ekkor azt mondjuk, hogy a $\mathscr{P}$ partíció $[d_s^{n_{d_s}}, \ldots, d_1^{n_{d_1}}]$-*típusú*.

5.13. Megjegyzés. Ha adott egy n_k méretű részleges $(k-1)$-befedése $PG(n-1,q)$-nak, akkor abból elkészíthetjük az $\mathbb{F}_q^n$ vektortér egy $[k^{n_k}, 1^{n_1}]$-típusú altér partícióját, ha a befedésből kimaradó pontoknak megfelelő egyeneseket egyesével hozzávesszük a befedésben szereplő projektív altereknek megfelelő k-dimenziós alterek halmazához.

Szükségünk lesz még a következő jelölésekre: Ha $\mathscr{P}$ egy $[d_s^{n_{d_s}}, \ldots, d_1^{n_{d_1}}]$-típusú altér partíciója $\mathbb{F}_q^n$-nek, akkor a H hipersíkra jelölje $b_{H,d}$ a H által tartalmazott d-dimenziós alterek számát $\mathscr{P}$-ben, és legyen $b_H = [b_{H,d_s}, \ldots, b_{H,d_1}]$ a H hipersík *típusa*. Legyen

$$\mathcal{B} \coloneqq \{b_H \colon H \text{ hipersík } \mathbb{F}_q^n\text{-ben}\}.$$

Továbbá ha $b \in \mathcal{B}$, akkor jelölje s_b a b-típusú $\mathbb{F}_q^n$-beli hipersíkok számát.

Most már megfogalmazhatjuk a bizonyításhoz szükséges lemmát.

5.14. Lemma. *Ha $\mathscr{P}$ egy $[d_s^{n_{d_s}}, \ldots, d_1^{n_{d_1}}]$-típusú altér partíciója $\mathbb{F}_q^n$-nek, akkor*

1. *$\mathbb{F}_q^n$ minden H hipersíkjára*

$$|\mathscr{P}| = 1 + \sum_{i=1}^{s} b_{H,d_i} q^{d_i}.$$

2. $$\sum_{b \in \mathcal{B}} s_b = \begin{bmatrix} n \\ 1 \end{bmatrix}_q,$$

és $\mathbb{F}_q^n$ minden d-dimenziós alterére

$$\sum_{b \in \mathcal{B}} b_d s_b = n_d \begin{bmatrix} n-d \\ 1 \end{bmatrix}_q.$$

Bizonyítás.

1. Egy k-dimenziós altérnek $q^k - 1$ nemnulla pontja van. Mivel $\mathscr{P}$ partíció, $\mathbb{F}_q^n$ nemnulla vektorainak a száma

$$q^n - 1 = \sum_{i=1}^{s} n_{d_i}(q^{d_i} - 1). \tag{6}$$

Számoljuk össze a H hipersík 0-tól különböző pontjait is két részre bontva aszerint, hogy olyan $\mathscr{P}$-beli altérben vannak-e, amelyet tartalmaz H, vagy sem. (Ha H nem tartalmaz egy k-dimenziós alteret, akkor az azzal vett metszete $(k-1)$-dimenziós.)

$$\sum_{i=1}^{s} b_{H,d_i}(q^{d_i} - 1) + \sum_{i=1}^{s} (n_{d_i} - b_{H,d_i})(q^{d_i - 1} - 1) = q^{n-1} - 1.$$

Ezt átrendezve, és felhasználva a (6) összefüggést azt kapjuk, hogy

$$\frac{q-1}{q}\sum_{i=1}^{s} b_{H,d_i} q^{d_i} + \frac{q-1}{q} = \frac{q-1}{q} - 1 + q^{n-1} - \sum_{i=1}^{s} n_{d_i}(q^{d_i-1}-1) =$$

$$= \frac{q-1}{q} - 1 + q^{n-1} - q^n + 1 + \frac{q-1}{q}(q^n-1) + \frac{q-1}{q}\sum_{i=1}^{s} n_{d_i} = \frac{q-1}{q}\sum_{i=1}^{s} n_{d_i}.$$

Ezt $\frac{q-1}{q}$-val osztva pont a kívánt eredmény adódik, hiszen $\sum_{i=1}^{s} n_{d_i} = |\mathscr{P}|$.

2. Az első egyenlőség rögtön következik abból, hogy az $\mathbb{F}_q^n$-beli hipersíkok száma $\begin{bmatrix} n \\ n-1 \end{bmatrix}_q = \begin{bmatrix} n \\ 1 \end{bmatrix}_q$. Másrészt mivel minden d-dimenziós altér $\begin{bmatrix} n-d \\ n-1-d \end{bmatrix}_q = \begin{bmatrix} n-d \\ 1 \end{bmatrix}_q$ hipersíkban van benne (lásd 2.3 Állítás), ha kétféleképpen megszámoljuk az olyan párokat, amelyek egy $\mathscr{P}$-beli d-dimenziós altérből és egy azt tartalmazó $\mathbb{F}_q^n$-beli hipersíkból állnak, pont a második egyenlőséget kapjuk. (A baloldalon a hipersíkok típusai szerint csoportosítva végezzük a leszámlálást.)

□

Vezessük be még az

$$l = \frac{q^{n-k} - q^r}{q^k - 1}$$

jelölést. Ezzel (5) jobb oldala $lq^k + 1$ alakra egyszerűsödik. A tételünket így a következőképpen fogalmazhatjuk meg:

5.15. Tétel. *Legyen* $0 \le r < k \le \left\lfloor \frac{n}{2} \right\rfloor$ *és* $n \equiv r \mod k$. *Ha* $k > \begin{bmatrix} r \\ 1 \end{bmatrix}_q$, *akkor a* $PG(n-1,q)$ *tér* $(k-1)$*-befedéseinek maximális mérete*

$$\mu_q(n,k) \le lq^k + 1.$$

Bizonyítás. Minden $i \ge 1$ egész szám esetén legyen

$$\delta_i := \frac{q^i - 2q^{i-1} + 1}{q-1}.$$

Indirekt bizonyítunk. Tegyük fel, hogy létezik $PG(n-1,q)$-nak egy $lq^k + 2$ méretű $(k-1)$-befedése. Ekkor az 5.13 Megjegyzés szerint létezik $\mathbb{F}_q^n$-nek egy $[k^{n_k}, 1^{n_1}]$-típusú altér partíciója, ahol

$$n_1 = \frac{q^n - 1}{q-1} - \left(\frac{q^n - q^{r+k}}{q^k - 1} + 2\right)\frac{q^k - 1}{q-1} = \left(\begin{bmatrix} r \\ 1 \end{bmatrix}_q - 1\right) q^k + \delta_{k+1}.$$

Jelöljük ezt a partíciót $\mathscr{P}_0$-lal.

Azt állítjuk, hogy ekkor minden $0 \le j \le \begin{bmatrix} r \\ 1 \end{bmatrix}_q - 1$ egész szám esetén létezik $\mathbb{F}_q^{n-j}$-nek egy olyan $\mathscr{P}_j$ altér partíciója, amelynek típusa

$$[k^{m_{j,k}}, (k-1)^{m_{j,k-1}}, \ldots, (k-j)^{m_{j,k-j}}, 1^{m_{j,1}}],$$

ahol $0 \le m_{j,k}, \dots, m_{j,k-j}$ olyan egész számok, amelyekre teljesül, hogy

$$\sum_{i=k-j}^{k} m_{j,i} = n_k = lq^k + 2 \quad \text{és}$$

$$m_{j,1} = c_j q^{k-j} + \delta_{k+1-j}$$

alkalmas $0 \le c_j \le \begin{bmatrix} r \\ 1 \end{bmatrix}_q - 1 - j$ egész számmal.

Ezt teljes indukcióval bizonyítjuk. $j = 0$-ra $\mathscr{P}_0$ megfelel a feltételeknek. Tegyük fel, hogy valamely $0 \le j \le \begin{bmatrix} r \\ 1 \end{bmatrix}_q - 1$ számra adott egy $\mathscr{P}_j$ altér partíciója $\mathbb{F}_q^{n-j}$-nek a megadott tulajdonságokkal. Az 5.14 Lemma 2. pontja szerint $\mathbb{F}_q^{n-j}$ hipersíkjaira $b_{H,1}$ átlagos értéke

$$\overline{b}_1 = \frac{m_{j,1} \begin{bmatrix} n-1-j \\ 1 \end{bmatrix}_q}{\begin{bmatrix} n-j \\ 1 \end{bmatrix}_q} = (c_j q^{k-j} + \delta_{k+1-j}) \left(\frac{q^{n-1-j} - 1}{q^{n-j} - 1} \right) < c_j q^{k-j-1} + \delta_{k-j}.$$

Ebből következik, hogy létezik olyan H_{j+1} hipersík, amelyre

$$b_{H_{j+1}} < c_j q^{k-j-1} + \delta_{k-j}. \tag{7}$$

Legyen

$$\mathscr{P}_{j+1} \coloneqq \{\mathcal{W} \cap H_{j+1} \colon \mathcal{W} \in \mathscr{P}_j\}.$$

Mivel a H_{j+1} hipersík izomorf $\mathbb{F}_q^{n-j-1}$-gyel, ezzel az $\mathbb{F}_q^{n-j-1}$ vektortérnek egy altér partícióját kapjuk. Ez teljesíti a kívánt tulajdonságokat:

- Ha a W alteret elmetsszük egy hipersíkkal, a dimenziója 0-val vagy 1-gyel csökken. Továbbá abból, hogy $j + 1 < \begin{bmatrix} r \\ 1 \end{bmatrix}_q < k$, következik, hogy $k - j > 2$. Így a $\mathscr{P}_{j+1}$ típusa
$$[k^{m_{j+1,k}}, (k-1)^{m_{j+1,k-1}}, \dots (k-j-1)^{m_{j+1,k-j-1}}, 1^{m_{j+1,1}}].$$

- Mivel $\mathscr{P}_j$-ben nem voltak 2-dimenziós alterek, az egynél nagyobb dimenziókhoz tartozó multiplicitások összege nem változik:
$$\sum_{i=k-j-1}^{k} m_{j+1,i} = \sum_{i=k-j}^{k} m_{j,i} = n_k.$$

- Az 5.14 Lemma 1. pontja szerint
$$\begin{aligned} 1 + b_{H_{j+1},1} q + \sum_{i=k-j}^{k} b_{H_{j+1},i} q^i = |\mathscr{P}_j| = n_k + m_{j,1} = \\ = lq^k + 2 + c_j q^{k-j} + \delta_{k+1-j} = 1 + lq^k + c_j q^{k-j} + q\delta_{k-j}. \end{aligned} \tag{8}$$
Az utolsó egyenlőségnél felhasználtuk, hogy $1 + \delta_{i+1} = q\delta_i$. (8) elejéből és végéből is 1-et kivonva, majd mindkét oldalt q-val osztva azt kapjuk, hogy
$$b_{H_{j+1},1} + \sum_{i=k-j}^{k} b_{H_{j+1},i} q^{i-1} = lq^{k-1} + c_j q^{k-j-1} + \delta_{k-j}.$$

$$\Longrightarrow b_{H_{j+1},1} \equiv \delta_{k-j} \mod q^{k-j-1}.$$

(A definícióból következik, hogy $0 < \delta_i < q^{i-1}$.) Eszerint tehát létezik egy olyan c_{j+1} egész szám, amivel

$$m_{j+1,1} = b_{H_{j+1},1} = c_{j+1}q^{k-j-1} + \delta_{k-j},$$

és erre (7) miatt teljesül, hogy $0 \le c_{j+1} \le c_j \le \begin{bmatrix} r \\ 1 \end{bmatrix}_q - 2 - j$.

Azt kaptuk tehát, hogy $j = \begin{bmatrix} r \\ 1 \end{bmatrix}_q - 1$-re is létezik egy ilyen altér partíció. Ebből szeretnénk ellentmondásra jutni.

Vegyük észre, hogy ekkor a $\mathscr{P}_j$-hez tartozó $c_j = 0$, és ezért $m_{j,1} = \delta_{k+1-j}$. Írjuk fel ebben a partícióban is a hipersíkokra $b_{H,1}$ átlagos értékét az 5.14 Lemma 2. pontjának segítségével:

$$\bar{b}_1 = \frac{m_{j,1}\begin{bmatrix} n-j-1 \\ 1 \end{bmatrix}_q}{\begin{bmatrix} n-j \\ 1 \end{bmatrix}_q} = \delta_{k+1-j}\frac{q^{n-j-1}-1}{q^{n-j}-1} < \delta_{k-j}.$$

Ebből következik, hogy létezik egy olyan H^* hipersík $\mathbb{F}_q^{n-j}$-ben, amelyre

$$b_{H^*,1} < \delta_{k-j}. \tag{9}$$

Felírva ismét az 5.14 Lemma 1. pontját, majd ugyanazokat a műveleteket elvégezve, mint az indukciós lépésnél, azt kapjuk, hogy

$$b_{H^*,1} \equiv \delta_{k-j} \mod q^{k-j-1}.$$

Ebből viszont $k-j-1 \ge 1$ miatt az adódik, hogy $b_{H^*,1} \ge \delta_{k-j}$, ami ellentmond a (9) egyenlőtlenségnek. Ezért nem létezhet $PG(n-1,q)$-nak lq^k+2 méretű $(k-1)$-befedése, és ezt szerettük volna belátni. □

5.16. Megjegyzés. Ha a (4) feltétel nem teljesül, akkor nem igaz az 5.9 Tétel állítása. A [6] cikkben a szerzők megmutatták, hogy $\mathcal{A}[8,3,3]_2 = 34$, ami nagyobb az 5.15 Tételből adódó 33-nál.

5.3. $[6,2,3]_q^I$-kód q^6+2q^2+2q+1 elemmel

Ebben a szakaszban mutatunk még egy szép példát arra, hogy hogyan lehet geometriai módszereket felhasználva nagy elemszámú Grassmann-kódot konstruálni. Az egyik fontos fogalom, amire szükségünk lesz, a *Klein-megfeleltetés*. Ehhez tekintsük a $PG(3,q)$-beli projektív egyenesek 3.5 Példában bevezetett Plücker-koordinátáit. Legyenek $p_{01}, p_{02}, p_{03}, p_{23}, p_{31}, p_{12} \in \mathbb{F}_q$ nem mind 0 testelemek. Ekkor a $(p_{01}, p_{02}, p_{03}, p_{23}, p_{31}, p_{12})$ hatoshoz pontosan akkor létezik olyan egyenes, amelynek ezek a Plücker-koordinátái, ha

$$p_{01}p_{23} + p_{02}p_{31} + p_{03}p_{12} = 0. \tag{10}$$

Ha a (10) egyenletre egy kicsit máshogy nézünk, akkor észrevehetjük, hogy ez egy másodrendű felületet ír le a $PG(5,q)$ térben.

5.17. Definíció. Tekintsük a $PG(5,q)$ térben az $X_0X_3 + X_1X_4 + X_2X_5 = 0$ homogén másodfokú egyenlet által leírt hiperbolikus kvádrikát. Ez az ún. *Klein-kvádrika*. Az előzőek szerint ennek pontjai kölcsönösen egyértelmű megfeleltetésben állnak a $PG(3,q)$ tér egyeneseivel. Ezt nevezzük *Klein-megfeleltetésnek*.

A Klein-megfeleltetés (számunkra) legfontosabb tulajdonságait foglalja össze az alábbi állítás:

5.18. Állítás ([9], Sect. 15.4)**.**

- *A Klein-kvádrika minden pontjának egy egyenes felel meg $PG(3,q)$-ban.*
- *A Klein-kvádrika által tartalmazott minden egyenes $q+1$ pontjának $q+1$ egyenes felel meg $PG(3,q)$-ban, amelyek egy ponton mennek át és egy síkban vannak.*
- *A Klein-kvádrika által tartalmazott minden sík q^2+q+1 pontjának q^2+q+1 egyenes felel meg $PG(3,q)$-ban, amelyek vagy egy ponton mennek át, vagy egy síkban vannak. Azokat a Klein-kvádrikán levő síkokat, amelyeknek egy síkban levő $PG(3,q)$-beli egyenesek felelnek meg,* görög síkoknak*, azokat, amelyeknek egy ponton átmenők,* latin síkoknak *nevezzük.*
- *Bármely két görög sík, illetve bármely két latin sík egy pontban metszi egymást. Egy görög és egy latin sík metszete vagy egy egyenes, vagy üres halmaz.*
- *Vegyünk egy olyan síkot $PG(5,q)$-ban, aminek a Klein-kvádrikával vett metszete egy kúpszeletet határoz meg. Minden így keletkező kúpszelet $q+1$ pontjának $q+1$ egyenes felel meg $PG(3,q)$-ban, amelyek egy hiperbolikus kvádrika egyik regulusát alkotják. Ha π és $\pi^\perp$ két olyan sík, amelyek a Klein-kvádrikára nézve egymás polárisai, akkor az ezek által a felületből kimetszett kúpszeleteknek megfelelő két $PG(3,q)$-beli egyenessereg ugyanazon hiperbolikus kvádrika két ellentétes regulusát adja. Ekkor π és $\pi^\perp$ nem metszi egymást.*
- *A $PG(3,q)$ térben egy elliptikus kongruencia egyeneseinek egy elliptikus kvádrika felel meg $PG(5,q)$-ban, amely egy olyan 3-dimenziós térnek a Klein-kvádrikával vett metszeteként áll elő, melynek poláris egyenese elkerüli a Klein-kvádrikát.*
- *A $PG(3,q)$ térben egy hiperbolikus kongruencia egyeneseinek egy hiperbolikus kvádrika felel meg $PG(5,q)$-ban, amely egy olyan 3-dimenziós térnek a Klein-kvádrikával vett metszeteként áll elő, melynek poláris egyenese a Klein-kvádrikának szelője.*
- *A $PG(3,q)$ térben egy parabolikus kongruencia egyeneseinek egy másodrendű kúp felel meg $PG(5,q)$-ban, amely egy olyan 3-dimenziós térnek a Klein-kvádrikával vett metszeteként áll elő, melynek poláris egyenese érinti a Klein-kvádrikát.*

Olyan kódot szeretnénk konstruálni, amelyben a szavak az $\mathbb{F}_q$ feletti 6-dimenziós vektortér 3-dimenziós alterei, és a közöttük fellépő minimális injektív távolság 2. Ez azt jelenti, hogy minden $\mathcal{U}, \mathcal{V} \in C$-re

$$\max(\dim(\mathcal{U}), \dim(\mathcal{V})) - \dim(\mathcal{U} \cap \mathcal{V}) \geq 2 \iff 3 - \dim(\mathcal{U} \cap \mathcal{V}) \geq 2 \iff \dim(\mathcal{U} \cap \mathcal{V}) \leq 1.$$

Azaz a C-ben szereplő alterek metszete legfeljebb 1-dimenziós lehet. Ha most ugyanezekre az alterekre projektív alterekként tekintünk, akkor ezt úgy fogalmazhatjuk át, hogy olyan síkokat szeretnénk megadni $PG(5,q)$-ban, amelyek páronként legfeljebb egy pontban metszik egymást. Ha sikerül megadnunk q^6+2q^2+2q+1 ilyet, akkor a következő alsó korlátot kapjuk:

5.19. Tétel. $q^6+2q^2+2q+1 \leq \mathcal{A}[6,2,3]_q$.

5.20. Megjegyzés. A maximális $[6,2,3]_q^I$-kód méretére a Johnson-korlátból (4.14 Tétel) és az $\mathcal{A}_q(n,k,k)$-ra vonatkozó eredményből (5.9 Tétel) az $\mathcal{A}[6,2,3]_q \leq (q^3+1)^2$ felső becslés adódik.

Ezeket az altereket úgy adjuk meg, hogy először $PG(3,q)$-beli struktúrákat veszünk, majd ezekre alkalmazzuk a Klein-megfeleltetést, hogy $PG(5,q)$-beli síkokat kapjunk.

Vegyünk először egy rögzített π síkot $PG(3,q)$-ban.

5.21. Lemma. *Ebben a síkban létezik q^2+q+1 kúpszelet, amelyek páronként egy pontban metszik egymást.*

Bizonyítás. A 2.31 Tétel szerint $PG(2,q)$ ciklikus modelljében az egyenesek inverzei kúpszeletek. Így az összes π-beli egyenes inverzét véve q^2+q+1 kúpszeletet kapunk, és ezek páronként egy pontban metszik egymást, éppen úgy, ahogy a hozzájuk tartozó egyenesek is. □

5.22. Lemma. *Minden π-beli kúpszelethez létezik $\frac{q^3(q-1)}{2}$ hiperbolikus kvádrika $PG(3,q)$-ban, ami tartalmazza a kúpszeletet.*

Bizonyítás. Ismert, hogy 5 általános helyzetű pont meghatároz egy kúpszeletet $PG(2,q)$-ban, továbbá 3 páronként kitérő egyenes meghatároz egy hiperbolikus kvádrikát $PG(3,q)$-ban. Legyen $\mathscr{C}$ tetszőleges kúpszelet π-ben, és rögzítsünk rajta 5 pontot. Olyan hiperbolikus kvádrikákat fogunk megadni, amelyek tartalmazzák ezt az 5 pontot. Mivel egy ilyen felületnek a π-vel vett metszete egy olyan másodrendű görbe, ami tartalmazza a rögzített 5 pontunkat, a metszet csak $\mathscr{C}$ lehet. Válasszunk ki az 5 pont közül 2-t, jelöljük őket P-vel és R-rel. P-n át $(q^2+q+1)-(q+1)=q^2$ olyan $PG(3,q)$-beli egyenes halad, ami nincs benne π-ben. Ha rögzítünk egy ilyen e egyenest, akkor R-en át $(q^2+q+1)-(q+1)-q=q(q-1)$ olyan egyenes halad, ami nincs benne π-ben és nem metszi e-t. (Azaz nincs benne az R és e által generált síkban sem.) Ebből az adódik, hogy összesen $q^3(q-1)$ -féleképpen adható meg két kitérő egyenes, amelyek közül az egyik P-ben, a másik Q-ban metszi a π síkot. Rögzítsünk egy ilyen egyenespárt, legyen e és f a két egyenes.

Ha adott a térben két kitérő egyenes és egy azokra nem illeszkedő pont, akkor egyértelműen létezik egy olyan egyenes, amely áthalad a ponton, és elmetszi mindkét egyenest. Húzzuk meg ezeket az egyértleműen létező szelő egyeneseket e-hez és f-hez a kúpszeleten eredetileg rögzített maradék 3 pontból. Az így kapott 3 páronként kitérő egyeneshez egyértelműen létezik egy őket tartalmazó hiperbolikus kvádrika. Ez nyilván tartalmazza a 3 pontot $\mathscr{C}$-n, valamint P-t és R-et is, mivel az ezeken átmenő e és f

egyenesek mind a 3 alkotó egyenest metszik, így a kvádrika egyik regulusához tartoznak. Tehát $q^3(q-1)$ $\mathscr{C}$-t tartalmazó hiperbolikus kvádrikát kaptunk, de mindegyiket kétszer számoltuk, mert egy kvádrikában P-n és R-en keresztül is 2 olyan egyenes van, ami a felületen halad, és ezek 2 kitérő egyenespárt alkotnak. □

Vegyünk tehát π-ben q^2+q+1 egymást páronként egy pontban metsző kúpszeletet, és vegyünk mindegyikhez $\frac{q^3(q-1)}{2}$ rajta átmenő hiperbolikus kvádrikát. Legyen a kiválasztott kúpszeletek halmaza $\mathscr{K}$, a hiperbolikus kvádrikáké pedig $\mathscr{H}$. Így összesen $\frac{q^6-q^3}{2}$ hiperbolikus kvádrikát választottunk ki. Mindegyikhez két regulus tartozik, így kapunk összesen q^6-q^3 regulust. Ezeknek $PG(5,q)$-ban q^6-q^3 olyan kúpszelet felel meg, amelyeket a Klein-kvádrikából egy-egy $PG(5,q)$-beli sík metsz ki. Jelölje ezen síkok halmazát $\mathscr{L}_1$.

5.23. Állítás. *$\mathscr{L}_1$ elemei páronként legfeljebb egy pontban metszik egymást.*

Bizonyítás. Először is vegyük észre, hogy ha két $\mathscr{H}$-beli hiperbolikus kvádrika nem ugyanarra a π-beli kúpszeletre illeszkedik, akkor mindkettőn egy-egy regulust véve legfeljebb egy olyan egyenes létezhet, amely mindkét regulusban benne van, mert különben az általuk π-ből kimetszett kúpszeleteknek legalább két közös pontja lenne. Azt is láttuk a kúpszeletre illeszkedő hiperbolikus kvádrikák konstrukciójánál, hogy a kúpszelet és azt metsző két kitérő egyenes már meghatározza a hiperbolikus kvádrikát, ezért az előbbi akkor is igaz, ha két olyan regulust veszünk, amelyek ugyanazt a kúpszeletet metszik ki π-ből.

Az is teljesül, hogy ha veszünk egy C és egy C' kúpszeletet $\mathscr{K}$-ban, amelyek a P pontban metszik egymást, akkor C-nek és C'-nek a P-beli érintő egyenese különböző. Ugyanis P-re a két rögzítetten kívül még $q-1$ kúpszelet illeszkedik π-ben, amelyek C-vel és C'-vel együtt lefedik az egész síkot. Ha C és C' közös érintője P-ben az e egyenes, akkor e a maradék $q-1$ kúpszelet mindegyikét P-n kívül még legfeljebb egy pontban metszi. Ekkor viszont e-nek van legalább egy olyan pontja, ami nincs lefedve a $q+1$ kúpszelet által, ami ellentmondás.

Tegyük fel, hogy van két sík $\mathscr{L}_1$-ben, σ_1 és σ_2, melyek metszete egy f egyenes. Ekkor az általuk generált Σ 3-dimenziós térnek a Klein-kvádrikával vett metszete 3-dimenziós másodrendű felület, azaz lehet egy hiperbolikus kvádrika, egy elliptikus kvádrika vagy egy másodrendű kúp. (Két sík uniója nem lehet, mert σ_1 és σ_2 kúpszeletekben metszik a Klein-kvádrikát.) Legyen R_1 és R_2 az a két regulus $PG(3,q)$-ban, ami a Klein-megfeleltetésnél σ_1-nek és σ_2-nek felel meg. Ekkor ezek rendre egy hiperbolikus, egy elliptikus vagy egy parabolikus kongruenciához tartoznak.

Azt az esetet, amikor egy elliptikus kongruenciához tartoznak, kizárhatjuk, mert az elliptikus kongruencia egyenesei páronként kitérők, de R_1 és R_2 egyeneseinek van legalább egy metszéspontja.

Az sem lehetséges, hogy R_1 és R_2 egy hiperbolikus kongruenciához tartozik, ugyanis ekkor Σ egy olyan 3-dimenziós tér, melynek poláris egyenese a Klein-kvádrika szelője. Ez azt jelenti, hogy σ_1-nek és σ_2-nek a Klein-kvádrikára vonatkozó poláris síkjai ($\sigma_1^\perp$ és $\sigma_2^\perp$) egy olyan egyenesben metszik egymást, amelynek 2 közös pontja van a Klein-kvádrikával. Vagyis a $\sigma_1^\perp$-nek és $\sigma_2^\perp$-nek $PG(3,q)$-ban megfelelő két regulusnak van két közös egyenese, azonban láttuk, hogy ez nem fordulhat elő.

Nézzük végül azt az esetet, amikor R_1 és R_2 egy parabolikus kongruenciához tartozik. R_1 és R_2 nem metszheti ki ugyanazt a kúpszeletet π-ből, mert a bennük levő egyeneseknek csak a kongruencia tengelyén lehet metszéspontjuk. Legyen t a kongruencia tengelye. Ekkor t benne van R_1 és R_2 ellentétes regulusában is, vagyis áthalad a megfelelő két $\mathscr{K}$-beli kúpszelet T metszéspontján. A parabolikus kongruencia úgy áll elő, hogy a t tengely mind a $q+1$ pontjában veszünk q azon átmenő egyenest, amelyek a tengellyel együtt egy sugársort alkotnak. Ez a $q+1$ sugársor $q+1$ különböző t-t tartalmazó síkban van. Tehát a T ponton keresztül is van egy sík, amely a parabolikus kongruencia $q+1$ egyenesét tartalmazza. Ennek a síknak t-n kívül R_1-gyel és R_2-vel sem lehet metszéspontja, amiből viszont az következik, hogy a sík π-vel vett metszete egy olyan egyenes, amely az R_1 és R_2 által π-ből kimetszett mindkét kúpszeletet érinti, amiről láttuk, hogy nem lehetséges.

Ezzel mindhárom esetet kizártuk, tehát nem lehet két $\mathscr{L}_1$-beli sík metszete egyenes.

Második lépésben tekintsük a rögzített π síkban levő egyeneseknek megfelelő Π görög síkot a Klein-kvádrikán. A kvádrikán található még további q^3+q^2+q görög sík. Vegyük hozzá ezeket az $\mathscr{L}_1$-beli síkokhoz, így egy q^6+q^2+q elemű $\mathscr{L}_2$ halmazt kapunk.

- A görög síkok egymással való metszete egy pontból áll.
- Egy görög sík egy $\mathscr{L}_1$-beli síkot nem metszhet egyenesben, mivel akkor az az egyenes benne lenne az $\mathscr{L}_1$-beli sík Klein-kvádrikával való metszetében is, amiről viszont tudjuk, hogy egy kúpszelet.

Végül tekintsük újra a Klein-kvádrikán a π által meghatározott Π görög síkot. Ennek minden r egyeneséhez található $q-1$ olyan $PG(5,q)$-beli sík, amely a Klein-kvádrikát pontosan r-ben metszi. (Összesen $q+1$ sík halad át r-en, amiből kettő – egy görög és egy latin sík – teljes egészében a felületen van.) Minden r-hez válasszunk ki egy ilyen síkot, és legyen $\mathscr{L}_3$ az a halmaz, amit $\mathscr{L}_2$-höz ezt a q^2+q+1 síkot hozzávéve kapunk. $\mathscr{L}_3$ elemei továbbra is páronként legfeljebb egy pontban metszik egymást:

- Tegyük fel, hogy az újonnan bevett síkok közül kettőnek a metszete egy egyenes. Legyen ez a két sík S_1 és S_2, és messék a síkok Π-t az r_1 és r_2 egyenesekben. Ekkor S_1 és S_2 egy 3-dimenziós projektív alteret generál, amelynek a Klein-kvádrikával vett metszete tartalmazza a Π görög síkot. Tehát a metszetként előálló másodrendű felület egy metsző síkpár. Így a generált 3-dimenziós altér tartalmaz egy latin síkot is a Klein-kvádrikán, jelöljük ezt Π'-vel. Mivel $\Pi \cap \Pi'$ egy egyenes, legalább az egyik S_i $(i=1,2)$ sík egy r_i-től különböző egyenesben metszi a Π' latin síkot. Ez ellentmond annak, hogy S_i pontosan az r_i egyenesben metszi a Klein-kvádrikát.
- Egy új sík és egy $\mathscr{L}_2$-beli görög sík metszete sem lehet egyenes, mert akkor az az egyenes benne lenne az új sík Klein-kvádrikával vett metszetében is, amiről tudjuk, hogy egy Π-beli egyenes. De minden egyenes pontosan egy görög síkban van benne, és $\Pi \notin \mathscr{L}_2$.
- Végül egy új sík és egy $\mathscr{L}_1$-beli sík azért nem metszheti egymást egyenesben, mert akkor az az egyenes a Klein-kvádrika érintője lenne a Π egy pontjában. Ugyanakkor

nincs olyan egyenes a $PG(3,q)$-ban kiválasztott regulusokban, ami benne lenne π-ben, ezért az $\mathscr{L}_1$-beli síkoknak a Klein-kvádrikával vett metszeteként előálló kúpszeletek diszjunktak Π-től.

5.24. Megjegyzés. $\mathcal{A}[6,2,3]_2 = 77$, azaz $q = 2$-re a fenti konstrukcióval maximális elemszámú kódot kapunk [12].

Gizella Királyné kilátó, Veszprém.
A kilátó acélszerkezetét egy hiperbolikus
másodrendű felületre illeszkedő egyenesek alkotják.

6. Táblázat a Grassmann-kódok maximális méreteiről

	Alsó korlátok				Felső korlátok			
Paraméterek (q,n,k,d)	Gilbert-Varshamov	5.8 Következmény	5.11 Tétel	5.19 Tétel	Hamming	Singleton	Johnson + 5.9 Tétel	Valódi érték
2 4 2 2	1	4	5	—	35	7	5	**5**
2 5 2 2	3	8	9	—	155	15	9	**9**
2 6 2 2	7	16	21	—	651	31	21	**21**
2 6 3 2	14	64	—	77	1395	155	81	**77**
2 6 3 3	1	8	9	—	14	15	9	**9**
2 7 2 2	14	32	41	—	2667	63	41	**41**
2 7 3 2	55	256	—	—	11811	651	381	333-381
2 7 3 3	2	16	17	—	55	31	17	**17**
3 4 2 2	2	9	10	—	130	13	10	**10**
3 5 2 2	7	27	28	—	1210	40	28	**28**
3 6 2 2	22	81	91	—	11011	121	91	**91**
3 6 3 2	66	729	—	754	33880	1210	784	754-784
3 6 3 3	2	27	28	—	66	40	28	**28**
3 7 2 2	68	243	271	—	99463	364	271	**271**
3 7 3 2	593	6561	—	—	925771	11011	7651	6978-7651
3 7 3 3	6	81	82	—	593	121	82	**82**
4 4 2 2	3	16	17	—	357	21	17	**17**
4 5 2 2	13	64	65	—	5797	85	65	**65**
4 6 2 2	54	256	273	—	93093	341	273	**273**
4 6 3 2	213	4096	—	4137	376805	5797	4225	4137-4225
4 6 3 3	3	64	65	—	213	85	65	**65**
4 7 2 2	218	1024	1089	—	1490853	1365	1089	**1089**
4 7 3 2	3390	65536	—	—	24208613	93093	70993	66828-70993
4 7 3 3	12	256	257	—	3390	341	257	**257**
5 4 2 2	4	25	26	—	806	31	26	**26**
5 5 2 2	21	125	126	—	20306	156	126	**126**
5 6 2 2	108	625	651	—	508431	781	651	**651**
5 6 3 2	532	15625	—	15686	2558556	20306	15876	15686-15876
5 6 3 3	4	125	126	—	532	156	126	**126**
5 7 2 2	542	3125	3251	—	12714681	3906	3251	**3251**

```
import math

def q_binom(n,k,q):
        szamlalo = 1
        i = n
        while (i >= n-k+1):
            szamlalo = szamlalo * ((q**i)-1)
            i = i-1
        nevezo = 1
        j = k
        while j >= 1:
            nevezo = nevezo * (q**j-1)
            j = j-1
        return szamlalo/nevezo

def Gilbert(n,d,k,q):
    szamlalo = q_binom(n,k,q)
    nevezo = 0
    i = 0
    while i <= d-1:
        nevezo = nevezo + q**(i**2) * q_binom(k,i,q) * q_binom(n-k,i,q)
        i = i+1
    return int(math.floor(szamlalo/nevezo))

def MRD(n,d,k,q):
    return int(min(q**((n-k)*(k-d+1)), q**(k*(n-k-d+1))))

def befedes(n,k,q):
    r = n % k
    return (q**n - q**(k+r))/(q**k -1) + 1

def befedes_also(n,d,k,q):
    if d==k:
        return int(befedes(n,k,q))
    else:
        return "-"

def Cossidente(n,d,k,q):
    if n==6 and d==2 and k==3:
        return int(q**6 + 2*q**2 + 2*q + 1)
    else:
        return "-"
```

```
def Hamming(n,d,k,q):
    szamlalo = q_binom(n,k,q)
    nevezo = 0
    i = 0
    t = math.floor((d-1)/2)
    while i <= t:
        nevezo = nevezo + q**(i**2) * q_binom(k,i,q) * q_binom(n-k,i,q)
        i = i+1
    return int(math.floor(szamlalo/nevezo))

def Singleton(n,d,k,q):
    return int(q_binom(n-d+1, k-d+1, q))

def Johnson(n,d,k,q):
    m = n-k+d
    r = m % d
    if k <= q_binom(r,1,q):
        return "-"
    else:
        r = befedes(m,d,q)
        i = m+1
        j = d+1
        while i <= n:
            r = math.floor((r * (q**i-1))//(q**j-1))
            i = i+1
            j = j+1
        return int(r)
```

Hivatkozások

[1] A. Cossidente, F. Pavese: *On subspace codes*, Des. Codes Cryptogr., (2016) 78:527-531.

[2] A. Cossidente, F. Pavese, L. Storme: *Geometrical aspects of subspace codes*, In: Network Coding and Subspace Designs, pages 107-129, Springer, 2018.

[3] Csikós Balázs, Kiss György: *Projektív geometria*, Polygon Kiadó, 2011.

[4] X. Chu, Y. Jiang: *Random linear network coding for peer-to-peer applications*, IEEE Network (2010) 24(4):35-39.

[5] J. Edmonds: *Edge-disjoint branchings*, In: Rustin R. (ed.) Combinatorial Algorithms, pp. 91-96. Algorithmics Press, New York (1972).

[6] S. El-Zanati, H. Jordon, G. Seelinger, P. Sissokho, L. Spence: *The maximum size of a partial* 3*-spread in a finite vector space over* $GF(2)$, Des. Codes Cryptogr. (2010) 54:101-107.

[7] T. Etzion, L. Storme: *Galois geometries and coding theory*, Des. Codes Cryptogr. (2016) 78:311-350.

[8] M. Hall, Jr.: *Difference sets. Combinatorics, Part 3: Combinatorial group theory*, Proc. NATO Advanced Study Inst., Breukelen, 1974), pp. 1–26. Math. Centre Tracts, No. 57, Math. Centrum, Amsterdam, 1974.

[9] J. W. P. Hirschfeld: *Finite Projective Spaces of Three Dimensions*, Oxford University Press, 1985.

[10] T. Ho, M. Médard, R. Kötter, D. R. Karger, M. Effros, J. Shi, B. Leong: *A random linear network coding approach to multicast*, IEEE Trans. Inf. Theory (2006) 52(10):4413-4430.

[11] T. Honold, M. Kiermaier, S. Kurz: *Johnson type bounds for mixed dimension codes*, Electron. J. Combin. 26 (2019), Paper 3.39, 21 pp.

[12] T. Honold, M. Kiermaier, S. Kurz: *Optimal binary subspace codes of length* 6*, constant dimension* 3 *and minimum distance* 4, Contemp. Math. (2015) 632:157-176.

[13] T. Honold, M. Kiermaier, S. Kurz: *Partial spreads and vector space partitions*, In: Network Coding and Subspace Designs, pages 131-170. Springer, 2018.

[14] Katona Gyula Y., Recski András, Szabó Csaba: *A számítástudomány alapjai*, Typotex Kiadó, 2002.

[15] A. Khalegi, D. Silva, F. R. Kschischang: *Subspace codes*, In: IMA International Conference Cryptography and Coding (2009), pp. 1-21.

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

[17] S. L. Kleiman, D. Laksov: *Schubert calculus*, Am. Math. Mon. (1972) 79:1061-1082.

[18] R. Kötter, F. R. Kschischang: *Coding for errors and erasures in random network coding*, IEEE Trans. Inf. Theory (2008) 54(8):3579-3591.

[19] J. H. van Lint: *Introduction to Coding Theory*, Springer Verlag Berlin Heidelberg, 1999.

[20] E. L. Nastase, P. Sissokho: *The maximum size of a partial spread in a finite projective space*, J. Combin. Theory Ser. A (2017) 152:353-362.

[21] J. Rosenthal, N. Silberstein, A.-L. Trautmann: *On the geometry of balls in the Grassmannian and list decoding of lifted Gabidulin codes*, Des. Codes Cryptogr. (2014) 73:393-416.

[22] D. Silva, F. R. Kschischang: *On metrics for error correction in network coding*, IEEE Trans. Inf. Theory (2009) 55(12):5479-5490.

[23] `http://subspacecodes.uni-bayreuth.de/`