Titokmegosztási sémák és véges geometriák

Diplomamunka

Írta: Bencze Tamás

Matematikus szak

Témavezető:

Kiss György
Geometriai Tanszék
Eötvös Loránd Tudományegyetem, Természettudományi Kar

Eötvös Loránd Tudományegyetem
Természettudományi Kar
2023

NYILATKOZAT

Név: Bencze Tamás

ELTE Természettudományi Kar, szak: Matematikus MSc

NEPTUN azonosító: TMANBH

Diplomamunka címe:
Titokmegosztási sémák és véges geometriák

A **diplomamunka** 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, 2023. 06.11.

Bencze Tamás

a hallgató aláírása

Tartalomjegyzék

1. Bevezető

A legegyszerűbb és legrégebbi gyakorlati példa titokmegosztásra a következő: Egy széfen két zár van, amit két különböző kulccsal lehet nyitni. Ha a két kulcsot odaadjuk két embernek, akkor ők együtt ki tudják nyitni a széfet, egyedül viszont egyikük sem tudja kinyitni, sőt egyedül egyiküknek sincs több hozzáférése a széf tartalmához, mint bárki másnak, akinek egy kulcsa sincs. Az ilyen tulajdonságú rendszereket fogjuk perfekt titokmegosztásnak nevezni s ezekre fogunk a dolgozatban főleg véges geometriai konstrukciókat adni.

Általánosabban a titokmegosztás célja a következő: adva van egy titok (ez akármi lehet, csak képes legyen különböző értékeket fölvenni), erről akarunk úgy információt átadni, hogy ezeknek pontosan az előre meghatározott részhalmazaiból lehessen megfejteni a titkot, miközben az összes többi esetben keveset lehessen megtudni róla. (Ehhez az elfogadott részhalmazok halmazának felszállónak kell lennie, azaz ha tartalmaz egy részhalmazt, akkor az összes őt tartalmazót is.)

A titokmegosztási problémák megoldásait titokmegosztási sémáknak hívjuk.

A titokmegosztási sémák precíz matematikai fogalmát *Blakley* [3] és *Shamir* [16] vezették be egymástól függetlenül 1979-ben írt cikkeikben. Mindketten perfekt t-küszöb sémákat konstruáltak, egyikük algebrai, másikuk pedig geometriai módszereket használva. Modelljükben valamely titkos X adatból bizonyos X_i részeket, úgynevezett *árnyékokat* készítettek. Az árnyékok olyanok, hogy bizonyos előre meghatározott részhalmazaikból X rekonstruálható, a többi részhalmazból viszont nem.

Nem foglalkozunk a sémák megvalósíthatóságának, az árnyékok kiosztásának és kezelésének gyakorlati oldalával, csak előállításuk matematikai problémáit vizsgáljuk.

A titokmegosztás fő alkalmazási módja a jelszavak megosztása: ha például egy cégnek van egy titkos adatbázisa (Pl. egy bankban a számlaadatok), akkor biztonsági szempontból nem szerencsés, ha bizonyos alkalmazottak "csak úgy" hozzáférhetnek, de valahogy mégis hozzá kell férni az adatokhoz. (Ez a felhasználás kivitelezhető lenne titokmegosztási módszerek nélkül is: egyszerűen a gép is leerrenőrizhetné, hogy a kapott részek egy megengedett részhalmazhoz tartoznak-e. Egy jó titokmegosztásnak viszont van 2 előnye: kevesebb tárhelyet igényel, és az ellenőrző program nagy része nem használja, hogy mi a titok, így külső fél által is megírható/karbantartható.)

De használható információ biztonságos tárolására is: ha titokmegosztással részekre bontunk, és ezeket a részeket több különböző gépen tároljuk, akkor ez egyszerre teszi (bizonyos fokig) lopás- és sérülésvédetté az adatot.

1.1. Példa. Egy nem túl komoly példaként legyen a titok egy n hosszú 0-1 sorozat, ezt akarjuk úgy megosztani, hogy bármely legalább 2 ember megfejthesse. Erre, ha n-nél nem több emberünk van, egy megoldás az, hogy az elsőnek az elsőn kívül elmondjuk az összes jegyet, a másodiknak a másodikon kívül, és így tovább. Ezzel az a probléma, hogy bár egy ember valóban nem tudja a titkot, de sokat megtud róla. (2 tippelésből garantáltan eltalálja, ami használhatatlanná teszi a felhasználások szempontjából.)

Optimális esetben a nem elfogadott részhalmazok adataiból semmi sem derül ki a titokról, és ez el is érhető; az ezt teljesítő titokmegosztási sémákat perfektnek hívjuk (az ez után következőek mind ilyenek lesznek). Perfekt sémák esetén tehát ha az előírtnál kevesebb adatot ismerünk, akkor a titok megfejtésére ugyanannyi esélyünk van, mint ha egyszerűen tippelünk.

Az előző konstrukció biztonság szemponjából javítható: ha 0-1 sorozatok helyett 0-tól 9-ig használjuk a számjegyeket, akkor egy ember tudásával 10 lehetséges eset van. Ezt kétféleképpen is megtehetjük: n megtartásával, vagy a sorozatok számának (körülbelüli) megtartásával. Az első esetben azt tapasztaljuk, hogy hogy a nagyobb titok nagyobb biztonságot jelent, a másodikban pedig a résztvevők maximális számát csökkentettük a nagyobb biztonság érdekében. Az első minden titokmegosztási sémában megvalósítható; ezért érdemes egy séma biztonságát a titok méretével arányosan kezelni. A második természetesen egy perfekt sémánál nem lehet kivitelezhető, de a későbbi sémákra bemutatom a résztvevők alacsony számának egy másik felhasználási módját.

A továbbiakban néhány egyszerűbb titokmegosztási feladat megoldására fogok konstrukciókat mutatni véges projektív terek felhasználásával.

A 2. fejezetben tömören összefoglaljuk a projektív és affin terek legfontosabb, a dolgozat későbbi részeiben felhasználásra kerülő tulajdonságait. Sokkal részletesebb bevezetés a véges geometriákba és az itt kimondott állítások bizonyítása megtalálható pl. a [8, 9, 10] könyvekben.

A 3. fejezet először az egyszerűbb küszöb- és rekesz-sémákat tárgyaljuk. Itt kiindulási pontunkat a *Beutelspacher* és *Rosembaum* [1] könyvében leírt modellek adják. Az ott leírt konstrukciók ismertetésén túl saját sémát is készítünk (**3.2.2.** Konstrukció). A fejezet második részében a többszintű küszöb-sémákat vizsgáljuk. Ezek ismert geometriai konstrukciói szorosan kapcsolódnak egyrészt az affin-szabályos sokszögekhez (lásd [2]), másrészt különböző dimenziós véges terek momentumgörbéihez ([4], [7], [13]). A harmadik részben a hierarchikus sémákat vizsgáljuk. Itt a [14] cikkben adott

egyik konstrukció általánosítása szerepel. Végül röviden megemlítjük a súlyozott küszöb-sémák egy lehetséges véges geometriai konstrukcióját.

2. Projektív geometria

A dolgozatban szereplő konstrukciók projektív geometriát használnak, ehhez néhány definíció és alaptulajdonság. A továbbiakban $\mathbf{K}$ egy kommutatív test, a q elemű véges testet pedig $\mathbf{F}_q$-val jelöljük.

2.1. Definíció. Legyen V_{d+1} egy $(d+1)$-dimenziós vektortér $\mathbf{K}$ fölött. A $\mathbf{K}$ fölötti d-dimenziós projektív tér pontjainak nevezzük V_{d+1} 1-dimenziós altereinek a halmazát.

2.2. Definíció. Egy projektív tér k-dimenziós altereinek nevezzük a kiindulási vektortér $(k+1)$-dimenziós altereit. A projektív tér 0, 1 és 2-dimenziós altereit pontoknak, egyeneseknek, illetve síkoknak nevezzük, az üres halmazt pedig (-1)-dimenziós altérnek tekintjük.

Ha a kiindulási vektortérben rögzítünk egy koordinátázást, a projektív tér pontjai koordinátázhatók az őket definiáló alterek egy nemnulla vetkorának koordinátáival, bár ez nem egyértelmű: két koordinátasorozat ugyanazt a pontot jelöli, ha egymás számszorosai.

2.3. Definíció. Egy pont homogén koordinátáinak hívjuk a pontot definiáló 1-dimenziós V_{d+1}-beli altérbe eső bármely nemnulla vektor koordinátáit.

Tehát a $\mathbf{K}$ test fölötti d-dimenziós projektív tér ponthalmaza megfelel a

$$\{\{(ck_0, ck_1, ..., ck_d) \colon c \in \mathbf{K}, c \neq 0\} \colon k_0, k_1, ... \in \mathbf{K}, k_0, k_1, ... \text{ nem mind } 0\}$$

halmaznak.

A homogén koordinátákat kettősponttal szokás elválasztani (Pl.: $(1:0:2)$)

2.4. Állítás. Ha $\mathbf{K} \leq \mathbf{L}$ egy testbővítés, akkor egy koordinátázott $\mathbf{L}$ fölötti projektív tér azon pontjai, amiknek van olyan koordinátasora, aminek minden eleme $\mathbf{K}$-beli, egy projektív teret alkotnak $\mathbf{K}$ fölött (a vektorterekhez hasonlóan).

Ugyanúgy, ahogy vektortér altere is vektortér, projektív tér altere projektív tér.

2.5. Állítás. Alterek metszete altér.

2.6. Definíció. Egy ponthalmaz által generált (avagy feszített) altérnek az őket tartalmazó legkisebb alteret nevezzük.

A H ponthalmaz által generált alteret $\langle H \rangle$-vel jelöljük.

2.7. Tétel. Dimenzióformula: Egy projektív tér bármely két A és B alterének a dimenzióinak az összege megegyezik a metszetük és az általuk generált altér dimenziójának az összegével.

$$\dim A + \dim B = \dim A \cap B + \dim \langle A, B \rangle$$

2.8. Definíció. Egy ponthalmaz összefüggő, ha van olyan pontja, ami benne van a többi által generált altérben, egyébként független.

2.9. Állítás. Egy k elemű ponthalmaz által generált altér dimenziója $k-1$, ha a ponthalmaz független, egyébként kevesebb. Tehát egy d-dimenziós térben bármely független ponthalmaznak legfeljebb $d+1$ pontja lehet.

2.10. Állítás. Minden ponthalmazból kiválasztható egy olyan részhalmaz, ami független, és ugyanazt az alteret generálja, mint az eredeti.

2.11. Definíció. Két ponthalmazt egymástól függetlennek nevezünk, ha az általuk generált alterek nem metszik egymást.

2.12. Definíció. Egy ponthalmazt ívnek nevezünk egy d-dimenziós térben, ha minden olyan részhalmaza független, aminek legfeljebb $d+1$ pontja van. Ez ekvivalens azzal, hogy vagy független, vagy legalább $d+1$ pontja van, és bármely $d+1$ közülük független.

Koordinátákra lefordítva: A generált altér a koordinátavektorok (nemnulla) lineáris kombinációinak megfelelő pontokból áll. Egy ponthalmaz összefüggő, ha a koordinátavektorai lineárisan összefüggők. Egy legalább $d+1$ elemű ponthalmaz pontosan akkor ív, ha semelyik $d+1$ pontjának koordinátavektoraiból alkotott mátrix determinánsa sem 0. (Könnyen meggondolható, hogy az ebben a bekezdésben leírtak mind függetlenek a pontokhoz tartozó vektorok választásától.)

2.13. Definíció. Ívre egy később többször használt példa a következő:

$$\{G(t) = (1 : t : t^2 : ... : t^d) \colon t \in \mathbf{K}\} \cup \{G(\infty) = (0 : 0 : ... : 1)\}$$

Ezt momentumgörbének hívjuk. Ez az $\mathbf{F}_q$ fölötti d dimenziós projektív térben egy $q+1$ elemű ív. Ha ugyanis $t_{i_j} \neq t_{i_k}$, akkor

$$0 \neq \begin{vmatrix} 1 & t_{i_1} & t_{i_1}^2 & \dots & t_{i_1}^d \\ 1 & t_{i_2} & t_{i_2}^2 & \dots & t_{i_2}^d \\ & & \vdots & & \\ 1 & t_{i_{d+1}} & t_{i_{d+1}}^2 & \dots & t_{i_{d+1}}^d \end{vmatrix} \quad \text{és} \quad 0 \neq \begin{vmatrix} 0 & 0 & 0 & \dots & 1 \\ 1 & t_{i_1} & t_{i_1}^2 & \dots & t_{i_1}^d \\ & & \vdots & & \\ 1 & t_{i_d} & t_{i_d}^2 & \dots & t_{i_d}^d \end{vmatrix}.$$

2.14. Definíció. A kiindulási vektortér invertálható lineáris transzformációi hatnak a projektív tér pontjain, és alteret altérbe, ívet pedig ívbe visznek. Egy ilyen hatást projektív lineáris transzformációnak hívunk.

2.15. Állítás. A vektortér két lineáris transzformációja akkor határozza meg ugyanazt a hatást a projektív tér pontjain, ha a mátrixaik egymás számszorosai. A szokásos jelölésekkel

$$\mathrm{PGL}(d+1,\mathbf{K}) \cong \mathrm{GL}(d+1,\mathbf{K})/\mathbf{K}^*$$

2.16. Tétel. Egy d dimenziós projektív térben bármely két rendezett $d+2$ elemű ívhez egyetlen olyan projektív lineáris transzformáció létezik, ami az első pontjait a második megfelelő pontjaiba viszi.

2.17. Állítás. Ha adott két azonos elemszámú (külön-külön) független rendezett ponthalmaz, akkor van olyan (projektív lineáris) transzformáció, ami az elsőt a másodikba viszi, és ezek száma csak a ponthalmazok méretétől függ. Ugyanez igaz azonos dimenziójú alterekre.
Az állítás akkor is igaz marad, ha olyan transzformációkat keresünk, amik egy rögzített, mindkét ponthalmaztól független halmazt fixen hagynak.

A továbbiakban véges testek fölötti projektív tereket fogunk használni.

2.18. Állítás. Az $\mathbf{F}_q$ fölötti d-dimenziós projektív térnek $\frac{q^{d+1}-1}{q-1}$ pontja van, speciálisan egy projektív egyenesnek $q+1$.

Az affin terek néhány tulajdonságára is szükségünk lesz.

2.19. Definíció. $\mathbf{K}$ fölötti d-dimenziós affin térnek nevezzük a $\mathbf{K}^d$ halmazt. Ennek egy alterének nevezzük azokat a hamazokat, amiket $\mathbf{K}^d$ mint vektortér altereinek eltolásával kapunk. Formulákkal, A altér a $\mathbf{K}^d$ affin térben, ha létezik H lineáris altér a $\mathbf{K}^d$ vektortérben és $v \in \mathbf{K}^d$, amire

$$A = H + v = \{h + v \colon h \in H\}$$

Affin terekkel a következő állítás miatt fogunk találkozni:

2.20. Állítás. Egy d dimenziós **2.3.** szerint koordinátázott projektív térben egy pontnak vagy minden koordinátázására $k_0 = 0$, vagy egyértelműen léteznek olyan koordinátái, amire $k_0 = 1$. Az első típusba tartozók egy $(d-1)$-dimenziós alteret alkotnak, míg ha a másodikra megszorítjuk az altereket, a

$$(1 : k_1 : k_2 : ... : k_d) \Longleftrightarrow (k_1, k_2, ..., k_d)$$

hozzárendelés ezeket a pontokat bijektíven és altértartóan képezi a $\mathbf{K}^d$ affin térbe.

Térjünk vissza a momentumgörbére.

2.21. Állítás. Az $f(x : y) = (x^d : x^{d-1}y : ... : xy^{d-1} : y^d)$ leképezés a projektív egyenest ráképezi a momentumgörbére. A megfeleltetés az, ami a projektív térbe beágyazza az affin teret: $f(1 : t) = G(t)$, $f(0 : 1) = G(\infty)$

2.22. Tétel. Legyen f, mint **2.21.**-ben. A projektív egyenes bármely p projektív lineáris transzformációjára létezik a d-dimenziós térnek olyan φ projektív lineáris transzformációja, amire $f(p(x : y)) = \varphi(f(x : y))$
Sőt, ha $q > d + 1$, akkor minden a momentumgörbét, mint halmazt fixen hagyó transzformáció előáll φ-ként alkalmas p-re, és φ egyértelmű.

Végezetül egy állítás a projektív egyenes transzformációiról:
(amik **2.14-15.** szerint a 2x2-es invertálható mátrixok ekvivalenciaosztályai az 'egymás számszorosa' ekvivalenciareláció szerint)

2.23. Állítás. A projektív egyenes pontjain a projektív lineáris transzformációinak a csoportja szigorúan 3-tranzítívan hat. (magyarul, ha tetszőleges 3 pontnak megadjuk a képét, akkor egyetlen olyan transzformáció van, ami a 3 pontot a megadott képeikbe viszi)

3. Konstrukciók

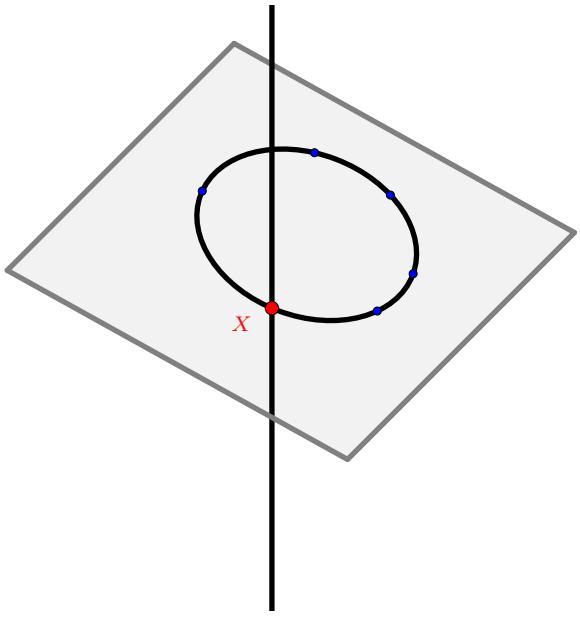
3.1. Küszöb séma

A legegyszerűbb titokmegosztási rendszerek az úgynevezett küszöbsémák.

3.1.1. Definíció. Az X titokhoz tartozó árnyékok egy $\mathcal{S} = \{X_1, X_2, \ldots, X_k\}$ halmazát *n-küszöb sémának* nevezzük, ha $\mathcal{S}$ bármely n eleméből rekonstruálható X, de kevesebb eleméből nem.

A séma *perfekt*, ha $\mathcal{S}$ bármely legfeljebb $n-1$ elemű részhalmazának ismeretében a titok megfejtésének valószínűsége ugyanaz az érték, mintha egyetlen árnyékot sem ismerünk.

3.1.2. Konstrukció. ([1] alapján) Ehhez vegyünk egy n-dimenziós projektív teret, ebben pedig egy egyenest. A titok lehetséges értékeit az egyenes pontjainak feleltetjük meg. Vegyünk egy $(n-1)$-dimenziós alteret, ami az egyenest egyetlen pontban metszi, és ebben egy olyan ívet, ami tartalmazza ezt a metszéspontot. Az ívnek az egyenesen kívüli pontjait hozzárendeljük a résztvevőkhöz. A titokból úgy generálunk információt a résztvevőknek, hogy sorsolunk (véletlenszerűen egyenletesen) egy olyan transzformációját a térnek, ami a kiválasztott egyenest önmagába viszi, az ívvel vett metszetét pedig a titokba, majd minden résztvevőnek megmondjuk a pontja képét.



3.1.3. Állítás. Az előző konstrukció egy perfekt n-küszöb sémát ad, ahol a feltörés valószínűsége $1/(q+1)$.

Bizonyítás. Bármely n adatból úgy lehet megfejteni a titkot, hogy vesszük az általuk feszített alteret (ez a kiválasztott $(n-1)$-dimenziós altér képe lesz), és elmetsszük az egyenessel. Tehát a konstrukció valóban működik, mint titokmegosztás.
Ha viszont n-nél kevesebb adatunk van, akkor az ismert pontok függetlenek a metszésponttól, így a titok bármely lehetséges értékéhez ugyanannyi olyan transzformáció van, ami az egyenes és az altér metszetét ebbe a pontba viszi, az egyenest önmagába képezi, és minden ismert pontot a megadott pontba visz. (Hiszen ha az egyenesen megadjuk még 1 pontnak a képét, akkor néhány független pont képe adott (és az egyenes automatikusan önmagába megy).) Tehát a séma perfekt. Mivel az egyenesen $q+1$ pont van, ezért a feltörés valószínűsége $1/(q+1)$. □

Ezzel a módszerrel az ív méreténél eggyel kevesebb emberrel lehet megosztani a titkot, tehát a momentumgörbét használva q darabbal, a titok méreténél eggyel kevesebbel.

Második nem túl komoly példaként vegyük észre, hogy ezzel a teljesen általános titokmegosztási feladatra is csinálhatunk egy megoldást: vegyünk minden megengedett részhalmazhoz egyet az előző konstrukcióból úgy, hogy azokkal az emberekkel osztjuk meg, akik benne vannak ebben a részhalmazban, és az összes adatból lehet csak meghatározni a titkot (tehát az n a részhalmaz elemszáma, a résztvevők meg az elemei). Egy résztvevő által kapott adat az összes pont, amit ezekben kap. Ez könnyen ellenőrizhetően valóban egy megoldás - sőt, perfekt - de van egy könnyen látható hibája: a résztvevők hatalmas mennyiségű adatot kapnak (ami nehezen használhatóvá teszi bármiféle alkalmazás szempontjából). Azt, hogy mennyire adunk át sok adatot, azt azzal célszerű jellemezni, hogy a titok lehetséges értékeinek számának hányadik hatványa az egy ember által kapható adatok maximális száma (a maximális arra értendő, hogy egyesek lehet többféle adatot kaphatnak, mint mások). **3.1.2.**-ben például ez az érték $\log_{q+1} \frac{q^{n+1}-q^2}{q-1} \approx n$. Egy perfekt titokmegosztásnál ez az érték nem lehet kevesebb, mint 1, és az ezt elérőket ideálisnak hívjuk. Az ezután következőek nem ilyenek lesznek, de fontos, hogy mennyire vannak távol tőle.

Bizonyítás. Először is pontosítsuk egy kicsit az állítást, mert ha azt akarjuk, hogy a titkot senki se tudja megfejteni, vagy bárki meg tudja fejteni (akár 0 résszel is), akkor természetesen egyesével senkinek sem kell mondanunk semmit, tehát ezeket az eseteket kénytelenek vagyunk kizárni. Bármelyik másik esetben viszont vehetünk egy minimális elfogadott halmazt (legyen ez H), és annak egy h elemét. Mivel a séma perfekt, ha h-t elhagyjuk H-ból, a maradék információkból a titok lehetséges értékeinek a halmaza nem szűkíthető. Mivel H elfogadott, a titok minden lehetséges c értékéhez

kell lennie h egy olyan értékének, ami a többi résztvevő (rögzített) adatával együtt éppen c-t adja meg, mint titkot. Ez azt jelenti, hogy h-nak legalább annyi különböző értéke van, mint a titoknak, és ezt akartuk belátni. □

Tehát célszerű minél kisebb adat átadásával megoldani a titok megosztását, és ebben a tekintetben az előző konstrukció javítható: a titkot egy n dimenziós tér egy egyenese helyett válasszuk egy $(n + k - 1)$-dimenziós tér egy k-dimenziós alteréről. A konstrukció ugyanúgy működik, viszont míg az eredeti konstrukcióban a titok értékkészletének nagyságrendileg n-edik hatványa a játékosok által kapható adatok száma, addig ebben csak az $\frac{n+k-1}{k}$-adik. Cserébe míg az elsőben nagyságrendileg annyi emberrel oszthatjuk meg a titkot amekkora a titok értékkészlete, addig ebben csak ennek a k-adik gyökényivel.

3.2. Rekesz séma

Következő feladatként legyenek a résztvevők k részre osztva, és egy csoport akkor tudja megfejteni a titkot, ha a következő feltételekből legalább m teljesül ($m \leq k$ és $n_1, n_2, ..., n_k$ adottak): az első részből legalább n_1 embert tartalmaz; a másodikból legalább n_2-t; ...; a k-adikból legalább n_k-t. Az előző probléma ennek a speciális esete $m = k = 1$-re.

3.2.1. Konstrukció. A feladat megoldásához egyszerűen minden részhez veszünk egyet az előző konstrukcióból, és még egyet, aminek a részek lesznek a résztvevői, mégpedig úgy, hogy az első féléknek a titka az a résznek a pontja a másodikban (a másodiknak a titka a titok, amit meg akarunk osztani). A titok pontosan akkor megfejthető, ha ismerjük m rész pontját, tehát ha a csoportunk megengedett.

De ez kivitelezhető egyetlen projektív térben is:

3.2.2. Konstrukció. ([1] alapján) Vegyünk egy $(m + \sum(n_i - 1))$-dimenziós projektív teret, ebben pedig egy m-dimenziós alteret - legyen ez M -, amiben megcsináljuk az előző konstrukciót a részekre. Ezután minden i-re az i-edik részhez tartozó ponthoz felveszünk egy olyan $(n_i - 1)$-dimenziós alteret, ami M-et pont az i-edik résznek kijelölt pontban metszi, úgy, hogy ezek M-el együtt generálják a teret.
Ez kivitelezhető például a következő módon: legyen a koordinátázott projektív térben

$$M = \{(x_0 : x_1 : ...) \colon x_j = 0 \text{ ha } j > m\}.$$

Ha az i-edik rész pontjának a koordimátái $(p_0^i : p_1^i : ...)$, akkor a hozzá tartozó altér legyen

$$\{(x_0 : x_1 : ...) \colon x_j = 0 \text{ ha } j > m \text{ kivéve, ha } m+\sum_{c<i}(n_c-1) < j \leq m+\sum_{c\leq i}(n_c-1)$$

$$\text{és vagy } \forall j \leq m \colon x_j = p_j^i, \text{ vagy } \forall j \leq m \colon x_j = 0\}.$$

Ha most minden részre a hozzá tartozó altérben veszünk egy olyan ívet, ami tartalmazza a hozzá tartozó pontot, és az ezen ponttól különböző pontjait szétosztjuk a rész tagjai között, akkor pontosan akkor lesz egy csoport által kapott ponthalmaz független a titoktól, ha a csoport nem megengedett.

Bizonyítás. Ha a csoport megengedett, akkor az általuk kapott pontok által generált altér tartalmazza m rész pontját, így az általuk feszített alteret is, ami tartalmazza a titkot.
A másik irányhoz először vegyük észre, hogy a feltételünk garantálja azt,

hogy ha az i-edik részből $n_i - 1$ emberünk van minden i-re, akkor a pontjaik függetlenek, és az általuk generált altér nem metsz bele M-be.
Ez azért van, mert ha ehhez hozzávesszük M-nek egy $m+1$ elemű független részhalmazát (ez generálja M-et), akkor együtt már a teljes teret generálják (hiszen M minden részből tartalmaz egy, a kiadottaktól független pontot, ezért a generált altér tartalmazza az összes rész alterét, így a feltételünk pont az, hogy generálja a teljes teret). Viszont a tér dimenziójánál csak eggyel több pontból áll, tehát ha generál, akkor (**2.9.** szerint) független. Ebből állításunk a dimenzióformula következménye.
Ezután már csak még egyszer használjuk a dimenzióformulát M-re és az adatok által generált altérre (nyilván elég a maximális nem elfogadottakra belátni, ezért feltehető, hogy minden i-re az i-edik részből van legalább $n_i - 1$ adatunk, és pontosan $m-1$-ből több); és mivel együtt generálják a teret, azt kapjuk, hogy a metszetük legfeljebb $m-2$ dimenziós, tehát éppen azon részek pontjai által generált altér, amikből megvan a kellő mennyiségű adat. De ez az altér nem tartalmazza a titkot, és ezzel kész vagyunk. □

A konstrukciót ugyanúgy fejezzük be, mint az előzőnél (**3.1.**): veszünk egy véletlen projektív lineáris transzformációt, ami a titok egyenesét önmagába viszi, a részek pontjai által generált altérrel vett metszetét pedig a titokba, és minden résztvevőnek elmondjuk a pontja képét. Az előző állítás fényében a konstrukció működőképessége és perfektsége ugyanúgy bizonyítható, mint az előző problémáé: ha a csoport elfogadott, akkor a titok a pontjaik által generált altér mtszete a titok egyenesével, míg ha nem elfogadottak, akkor a titok egyenesének bármely pontjához ugyanannyi olyan transzformáció létezik, ami a csoport tagjainak pontjait az ismert helyükre viszi, a titkot meg a választott pontba (**2.17.**)

3.2.3. Megjegyzés. A problémában a részekhez tartozó feltételek lecserélhetőek a **3.2.-3.4** feltételeinek bármelyikére; ekkor a konstrukcióban a részhez tartozó alteret le kell cserélni a megfelelő probléma megoldására.

Bizonyítás. Az előző bizonyításhoz hasonlóan a kapott pontok által feszített altér pontosan akkor tartalmazza a titkot, ha legalább m rész pontjai által feszített altér metsz bele M-be. (A bizonyítás elején az $n_i - 1$ pontot le kell cserélni maximális M-től független halmazra.) Viszont egy rész pontjai által feszített altér pontosan akkor metsz bele M-be, ha elfogadott. □

3.3. Hierarhikus séma

Ebben a részben a többszintű titokmegosztási sémákat tárgyaljuk. Ebben a feladatban az embereket k csoportba osztjuk, a titkot pedig azon részhalmazoknak kell tudnia megfejteni, amik az első csoportból legalább n_1 embert, az első kettőből összesen legalább n_2-t,..., és az első k-ból pedig legalább n_k embert tartalmaznak, ahol $n_1 < n_2 < ... < n_k$ adottak.

3.3.1. Konstrukció. A megoldáshoz vegyünk egy $(n_k - 1)$-dimenziós projektív teret a q elemű test fölött (legyen ez A_0), abban egy $(n_k - n_1 - 1)$-dimenziós alteret (A_1), abban egy $(n_k - n_2 - 1)$-dimenziósat (A_2), és így tovább, az $(n_k - n_{k-1} - 1)$-dimenziósig, majd vegyünk ezekhez az alterekhez egy olyan ponthalmazt, amiben egy ponthalmaz pontosan akkor összefüggő, ha valamelyik kiválasztott altérben több pontja van, mint amennyi az altér dimenziója +1: legyen ez K.
(Arról, hogy ilyet hogyan konstruálunk, később lesz szó.)
Ha van egy ilyen ponthalmazunk, akkor a feladatnak megoldása az, hogy $K \cap (A_0 \setminus A_1)$-ből kiválasztunk egy pontot, ami a titok lesz, a maradékból pedig adunk egyet az első csoport minden tagjának, a második csoport tagjai $K \cap (A_1 \setminus A_2)$-ből kapnak egy-egy pontot, és így tovább, a k-adik csoport tagjai $K \cap (A_{k-1})$-ből kapnak pontot. Ekkor a résztvevők egy halmazának pontosan akkor kellene tudnia megfejtenie a titot, ha az általuk kapott pontok által feszített altér tartalmazza a titkot. Ha ezt tudjuk, a konstrukció befejezhető például azzal, hogy A_0-t beágyazzuk egy eggyel nagyobb dimenziós térbe, közzéteszünk egy egyenest, ami pont a titokban metszi A_0-t, és elmondjuk a résztvevőknek, hogy a titok az egyenes és a pontjaik által feszített altér metszete.

Bizonyítás. Először vegyük észre, hogy ha néhány résztvevő teljesíti a feltételt, akkor közülük az az n_k darab is teljesíti, akik a legkisebb sorszámú csoportból vannak. Viszont n_k darab emberre a feltétel pont azt jelenti, hogy a pontok, amiket kaptak, függetlenek. Tehát feszítik a teljes A_0-t, ami tartalmazza a titkot. Megfordítva, ha a kapott pontok által feszített altér tartalmazza a titkot, akkor először a kapott pontokból kiválasztunk egy maximális független ponthalmazt. Ezek -függetlenek lévén- teljesítik a ponthalmazunk független részeire tett feltételt, de ha a titkot is hozzávesszük, már nem (hiszen feltettük, hogy a titok nem független a pontjainktól), tehát a titok hozzávételével valamelyik altérben túl sok pontunk lett, és ez csak A_0 lehet (hiszen a titok csak abban van benne). Ez viszont azt jelenti, hogy van n_k darab független pontunk, ami azt jelenti, hogy a résztvevőink teljesítik a feltételt. □

Most térjünk vissza arra, hogy hogyan készítünk ilyen K ponthalmazt.

Ilyen ponthalmaz ([14]-beliek általánosításaként) konstruálható mohón: egyesével vesszük hozzá K-hoz a pontokat, két dologra figyelve:

- először választunk pontokat A_{k-1}-ben, aztán $(A_{k-2} \setminus A_{k-1})$-ben, és így tovább
- ha A_i-ből választunk pontot, akkor nem választunk olyan pontot, ami benne van az eddigi pontok bármely olyan részhalmaza által feszített altérben, amik nem feszítik A_i-t

Könnyen látható, hogy kellően nagy q-ra így K mindig bővíthető, ha feltesszük, hogy $\binom{|K|}{n_k-1} \leq q$:

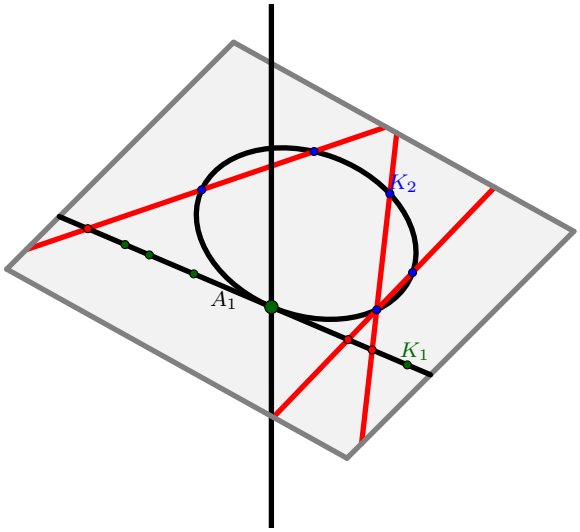
Bizonyítás. Tegyük fel, hogy A_i-t akarjuk bővíteni. Ez egy $(n_k - n_i - 1)$-dimenziós altér, ezért K néhány korábban választott pontjától csak akkor kell függetlennek lennie az új pontnak, ha az a néhány kevesebb, mint $n_k - n_i$. Ha eddig kevesebb, mint $n_k - n_i$ pontja volt K-nak, akkor vehetünk A_i-ben egy tőlük független; ha nem, akkor bármely kis ponthalmaz kiegészíthető K-ból egy $n_k - n_i - 1$ eleműre, tehát legfeljebb $\binom{|K|}{n_k-n_i-1}$ darab altér pontjai vannak kizárva. De q-nál nem több altér nem fedheti a teljes teret (ha egyikük sem a teljes tér), hiszen összesen kevesebb pontjuk van. Kellően nagy q-ra A_0 bővíthetőségéhez a legerősebb a feltétel. □

Ennek a konstrukciónak előnye, hogy mindig működik, viszont hátránya, hogy nagyon kevés pontja van, nagyságrendileg csak $\sqrt[n_k-1]{q}$.

Kis esetekre találtak ennél nagyobb ponthalmazokat is:

Ha például $k = 2$, $n_1 = 1$, $n_2 = 3$:

Ekkor A_0 egy sík, A_1 pedig egy egyenes. Legyen $K_1 = K \setminus A_1$, $K_2 = K \cap A_1$. Ekkor a feltétel az, hogy K_1 ív A_0-ban és K_1 semelyik 2 pontja által feszített egyenes nem tartalmaz pontot K_2-ből. Így ha azt akarjuk, hogy K_2-nek sok pontja legyen, akkor K_2 A_1 összes olyan pontjából fog állni, ami nincs rajta olyan egyenesen, amin K_1-nek 2 pontja van.



Legyen $A_0 = \{(x : y : z) \colon x, y, z \in \mathbf{F}_q\}$, A_1 pedig $x = 0$. **2.20.** szerint $A_0 \setminus A_1$ minden pontja egyértelműen áll elő $(1 : y : z)$ alakban, és az $(1 : y : z) \to (y, z)$ egy egyenestartó megfeleltetés az $\mathbf{F}_q^2$ affin síkkal, ahol két affin egyenes pontosan akkor metszi A_1-et ugyanott, ha az affin térben párhuzamosak.

Összefoglalva $\mathbf{F}_q^2$-ben keresünk olyan ívet, amiben a pontpárok közti egyenesek között kevés a páronként nem párhuzamos (hogy kevés pontot zárjon ki A_1-ről.) Ha k pontot választunk, azok meghatároznak legalább $(k-1)$-et: ha a pontok P_1, P_2,..., akkor a $\langle P_1, P_2\rangle$, $\langle P_1, P_3\rangle$, ... egyenesek páronként nem párhuzamosak. Ez a $k-1$ éles: ha vesszük $\mathbf{F}_2^2$-ben a 4 pontot, azok 3 párhuzamossági osztályt fognak meghatározni. Viszont minden ilyen példára k és q kénytelen páros lenni, ezért megelégedünk olyan halmazokkal, amik k páronként nem párhuzamos egyenest feszítenek.

Ennek egy speciális eseteként kiemelendőek az affin szabályos sokszögek.

3.3.2. Definíció. Egy ponthalmaz akkor affin szabályos sokszög, ha a pontjai bijekcióba állíthatók az euklidészi sík egy szabályos sokszög csúcsaival úgy, hogy a pontok között futó egyenesek párhuzamossága megmarad.

Ezeket páratlan q-ra *Korchmáros* [12] karakterizálta:

3.3.3. Tétel. Páratlan q esetén az $\mathbf{F}_q$ fölötti affin sík bármely affin szabályos sokszöge affinitással átvihető a következő affin szabályos sokszögek valamelyikébe:

1. A test multiplikatív csoportjának (jelöljük ezt $\mathbf{F}_q^*$-gal) egy tetszőleges H részcsoportjára $\{(\frac{1}{h}, h) \colon h \in H\}$
2. A test 1 által generált additív H részcsoportjára $\{(h, h^2) \colon h \in H\}$ (Ez bármely additív részcsoportra a célnak megfelelő K_1-et ad.)

3. Legyen $\mathbf{F}_{q^2}$-ben i az x^2-k ($\mathbf{F}_q$ fölött) irreducibilis polinom egyik gyöke. Ekkor $\mathbf{F}_{q^2}$ minden eleme egyértelműen áll elő $a+bi$ alakban, ahol $a,b\in\mathbf{F}_q$. Azon elemek, amelyekre $a^2-kb^2=1$, csoportot alkotnak a szorzásra nézve; vegyük ennek egy H részcsoportját. Az $(a,b)\leftrightarrow a+bi$ azonosítással élve H pontjai affin szabályos sokszöget alkotnak.

Erre az állításra úgy is lehet gondolni, hogy bármelyik affin szabályos sokszög rajta van egy hiperbolán (1.), parabolán (2.), vagy ellipszisen (3.).

Az első kettő páros q-ra is jó K_1-et ad, és a csúcsszámuk prímosztója q-nak, tetszőleges osztója $q-1$-nek, illetve $q+1$-nek.

Ha $k=2$, $n_1=n_2-2$ ([2] alapján):

A_1 egy egyenes az (n_2-1)-dimenziós A_0-ban. Az előző konstrukiókat fogjuk általánosítani a [2] cikkben közölt vázlatos bizonyítás alapján.

Az első esetben

$$K_1=\{(\frac{1}{h},h)\colon h\in H\}=\{(1:h:h^2)\colon h\in H\}=\{G(h)\colon h\in H\},$$

$$A_1=\{(x:0:y)\colon x,y\in\mathbf{F}_q\}=\langle G(0),G(\infty)\rangle$$

Ezt általánosítva legyen n_2-1 dimenzióban $K_1=\{G(h)\colon h\in H\}$, A_1 pedig a $G(0)$-n és a $G(\infty)$-en átmenő egyenes: $\{(x:0:0:\ldots:0:y)\colon x,y\in\mathbf{F}_q\}$.

Nézzük meg, hogy mikor lesz

$$G(x_1),G(x_2),\ldots,G(x_{n_2-1}),(x:0:\ldots:0:y)$$

ponthalmaz összefüggő. Pontosan akkor, ha a koordinátáikból alkotott mátrix determinánsa 0:

$$0=\begin{vmatrix} x & 0 & \ldots & 0 & y\\ 1 & x_1 & \ldots & x_1^{n_2-2} & x_1^{n_2-1}\\ \vdots & \vdots & & \vdots & \vdots\\ 1 & x_{n_2-1} & \ldots & x_{n_2-1}^{n_2-2} & x_{n_2-1}^{n_2-1}\end{vmatrix}$$

$$=x\cdot\begin{vmatrix} x_1 & \ldots & x_1^{n_2-2} & x_1^{n_2-1}\\ \vdots & & \vdots & \vdots\\ x_{n_2-1} & \ldots & x_{n_2-1}^{n_2-2} & x_{n_2-1}^{n_2-1}\end{vmatrix}+(-1)^{n_2-1}y\cdot\begin{vmatrix} 1 & x_1 & \ldots & x_1^{n_2-2}\\ \vdots & \vdots & & \vdots\\ 1 & x_{n_2-1} & \ldots & x_{n_2-1}^{n_2-2}\end{vmatrix}$$

Mivel az első mátrix minden sorából kiemelve a megfelelő változót visszakapjuk a második mátrixot (aminek a determinánsa nem 0), ez pontosan akkor lesz 0, ha $y=(-1)^{n_2}x\prod x_i$. Tehát ha minden x_i H-beli, és ezek összefüggők, akkor

$$\frac{y}{x}=(-1)^{n_2}\prod x_i\in(-1)^{n_2}H,$$

így ha K_2-t az egyenes azon pontjainak választjuk, amik ezt nem teljesítik, akkor a kapott ponthalmaz független.

Minden részhalmaz, aminek a függetlenségét elvárjuk, 0, 1 vagy 2 pontot tartalmaz az egyenesről, és ami 1-et, az független (mert kiegészíthető független n_2 pontúvá). A 0 pontot tartalmazók függetlenek, mert G egy ív, a 2 pontot tartalmazók által feszített altér pedig megegyezik azzal, mint ha ezt a 2 pontot kicserélnénk $G(0)$-ra és $G(\infty)$-re, tehát ennek a függetlensége is abból következik **2.9.** alapján, hogy G ív.

A második esetben

$$K_1 = \{(1 : h : h^2) \colon h \in H\}, \quad A_1 = \{(0 : x : y) \colon x, y \in \mathbf{F}_q\}.$$

Ennek általánosításaként legyen

$$K_1 = \{(1 : h : ... : h^{n_2-1}) \colon h \in H\},$$

$$A_1 = \{(0 : 0 : ... : 0 : x : y) \colon x, y \in \mathbf{F}_q\}.$$

(Ezt a momentumgörbe ∞-beli érintőjének hívjuk.) Hasonló számolás után ha K_2-t A_1 azon pontjainak választjuk, amire $\frac{y}{x} \notin H$ (megengedve $x = 0$-t), akkor a kapott ponthalmaz jó lesz. (Bár itt azt az esetet is ellenőrizni kell, amikor 2 pontot veszünk az egyenesről, de az könnyű.)

A harmadik esetet is hasonló alakra szeretnénk hozni. K_1 olyan $(a : b : c)$ pontokból áll, amikre $a^2 - kb^2 = c^2$, avagy $k(a + c)(a - c) = (kb)^2$. (Az egyenes pedig a $c = 0$.) Ez azt jelenti, hogy ha vesszük az

$$(a : b : c) \mapsto (a - c : kb : k(a + c)) = (a' : b' : c')$$

projektív lineáris transzformációt, akkor K_1 képére $a'c' = b'^2$ teljesül, és ennek a megoldásai pontosan az $(1 : x : x^2)$ alakú pontok. Ezt fogjuk a momentumgörbére általánosítani. A transzformáció után az egyenes képe: $ka' = c'$. Ennek a momentumgörbével vett metszete azon $G(x)$ pontokból áll, amire $x^2 = k$. Ilyen nem létezik (k-t így választottuk), de ezen lehet segíteni: ha $\mathbf{F}_{q^2}$ fölött nézzük, akkor van 2 gyök: (miután az egyiket elneveztük i-nek) i és $-i$. Tehát az egyenes valójában (a **2.4.** szerint bővített térben) a $G(i)$-n és a $G(-i)$-n átmenő egyenes. Ez már általánosodik $n_2 - 1$ dimenzióba: könnyen látható, hogy ennek az egyenesnek azok a pontjai, amiknek minden koordinátája $\mathbf{F}_q$-beli, egy egyenest alkotnak az $\mathbf{F}_q$ fölötti projektív térben (ha $\mathbf{F}_q$-t mint $\mathbf{F}_{q^2}$ részét tekintjük).

Most már csak egy szorzás hiányzik G elemeire: a

$$G \to \mathbf{F}_{q^2}^*/\mathbf{F}_q^*, \quad G(\frac{a}{b}) \mapsto \{c(a + bi) \colon c \in \mathbf{F}_q^*\} (G(\infty) \to i\mathbf{F}_q^*)$$

megfeleltetéssel élve G-n kaptunk egy szorzást, és ezután számolással ellenőrizhető, hogy az előző esetekhez hasonlóan ha veszünk $n_2 - 1$ pontot G-ről, akkor az átaluk generált altér az egyenest egyetlen pontban fogja metszeni, és hogy melyikben, az csak a választott elemek szorzatától függ. És innentől a befejezés ugyanaz, mint az első esetben (: ha K_1-nek G egy részcsoportját választjuk, akkor A_1-ről csak $: K_1 :$ pontot zárunk ki (a közülük választható pont-$(n_2 - 1)$-esek az egyenessel való meszetét), és a maradékban azok a ponthalmazok, amiknek a függetlenségét elvárjuk, és 1 pontot tartalmaznak az egyenesről, azok függetlenek lesznek. Amik egyet sem, azok függetlenek, mert G ív, és amik 2-t, azok ugyanakkor függetlenek, mint ha ezt a 2 pontot kicserélnénk $G(i)$-re és $G(-i)$-re, és megint azt használjuk, hogy G ív).

De a kellemetlen számolást meg lehet spórolni azzal, ha máshogy nézünk rá a dolgokra: **2.22.** szerint létezik olyan φ projektív lineáris transzformációja az $\mathbf{F}_{q^2}$ fölötti projektív térnek, amire

$$\varphi(f(x : y)) = f(p(x : y))$$

ahol p az a projektív lineáris transzformáció, ami $(1 : i)$-t $(0 : 1)$-be, $(1 : -i)$-t $(1 : 0)$-ba, $(1 : 0)$-t meg $(1 : -1)$-be viszi:

$$p(x : y) = (-ix + y : ix + y).$$

3.3.4. Állítás. A $\{p(x : y) \colon x, y \in \mathbf{F}_q\}$ halmaz az $(1 : t) \Leftrightarrow t$ azonosítással élve részcsoportja $\mathbf{F}_{q^2}^*$-nek.

Bizonyítás. Mivel $p(x_1 : y_1) = \frac{-ix_1+y_1}{ix_1+y_1}$, ezért

$$\begin{aligned} p(x_1 : y_1) \cdot p(x_2 : y_2) &= \frac{(-ix_1 + y_1)(-ix_2 + y_2)}{(ix_1 + y_1)(ix_2 + y_2)} \\ &= \frac{kx_1x_2 - i(x_1y_2 + x_2y_1) + y_1y_2}{kx_1x_2 + i(x_1y_2 + x_2y_1) + y_1y_2} \\ &= p(x_1y_2 + x_2y_1 : kx_1x_2 + y_1y_2) \in \{p(x : y) \colon x, y \in \mathbf{F}_q\}. \end{aligned}$$

□

Tehát ha ezt vesszük, mint műveletet a momentumgörbe pontjain, akkor véve egy részcsoportot, a hozzá tartozó pontok a teljes szelőről csak annyi pontot zárnak ki, amennyi a részcsoport elemszáma, tehát azon pontjaiból is legfeljebb ennyit, amiknek φ szerinti ősének tényleg minden koordinátája $\mathbf{F}_q$-beli.

A konstrukciók páros q-ra is működnek, csak a harmadikat át kell fogalmazni: mivel $x^2 - k$ alakú irreducibilis polinom nincs, ezért egy $x^2 + x + k$

alakút veszünk helyette, aminek ha az egyik gyöke a bővítésben i, akkor a másik $i+1$.

Ezeket a ponthalmazokat egy másik (bár hasonló) feladat megoldására is lehet használni ([7] alapján): legyenek a résztvevők k csoportba osztva, a titkot pedig azon részhalmazoknak kell tudnia megfejteni, amik a következő feltételekből legalább egyet teljesítenek: az első csoportból legalább n_1 embert tartalmaznak; az első kettőből összesen legalább n_2-t;...; az első k-ból összesen legalább n_k-t. ($n_1 < n_2 < ... < n_k$ adottak)

Ennek egy megoldása az, hogy veszünk egy hasonló ponthalmazt, mint az előzőben, csak A_i dimenziója legyen $n_{k-i} - 1$, és a titkot A_{k-1}-ből választjuk, az i-edik csoportba tartozóknak pedig $A_{k-i} \setminus A_{k-i+1}$-ből adunk pontot, a konstrukció többi része ugyanaz.

Ekkor ha egy részhalmaznak meg kéne tudnia fejteni a titkot, akkor a legkisebb olyan i-re, amire teljesítették az i-edik feltételt, a pontjaik feszítik P_{k-i}-t. (hiszen ha veszünk az első i csoportból összesen n_i pontot, akkor azok függetlenek a feltétel szerint, és P_{k-i} dimenziójánál többen vannak) Tehát az általuk generált altér tartalmazza a titkot.

Ha viszont a részhalmazunk nem elfogadott, akkor a feltétel szerint a pontjaik a titokkal együtt független halmazt alkotnak.

3.4. Súlyozott küszöb séma

Végezetül vegyük észre hogy az eddigi példák (a nem túl komoly példáktól eltekintve) mind egy kaptafára készültek: vettünk egy alteret, amin rajta van a titok, és úgy adtunk a résztvevőknek 1-1 pontot, hogy ha néhányan nem alkotnak elfogadott részt, akkor a pontjaik által generált altér ne metssze a titok alterét, ha pedig elfogadott, akkor pont a titokban metssze. Ilyen megoldást nem lehet minden titokmegosztási feladatra adni: a legkisebb ellenpéldában 4 résztvevő van, és az elfogadott halmazok azok, amik tartalmazzák az első résztvevőt és legalább még valakit, vagy az elsőn kívül mindenkit.

Ennek a bizonyítása egyszerű: magát a titkot nem adhatjuk oda az első résztvevőnek, mert akkor ő egyedül is meg tudná fejteni, úgyhogy beszélhetünk a titok és az első játékos pontjának az egyeneséről. Ezen az egyenesen rajta kell legyen a másik három játékos pontja, hiszen ellenkező esetben az első játékos pontjával egy ettől különböző egyenest feszítenének, ami nem megy át a titkon. viszont ha a másik három játékosból valamelyik kettő különböző pontokat kap ezen az egyenesen, akkor ők is meg tudnák fejteni, tehát mindhármuk ugyanazt a pontot kapta. Ekkor viszont ők hárman sem tudják megfejteni a titkot. Most ennek az általánosítására következik egy megoldás:

Legyen minden résztvevőre adott egy pozitív egész "súly", és egy részhalmaz akkor elfogadó, ha a súlyaik összértéke elér egy k küszöböt. Az előző példában az első játékos súlya 2, a többieké 1, a küszöb 3.

A megoldás a következő: egyszerűen kezeljünk minden résztvevőt annyi résztvevőként, amennyi a súlya, és vegyük az első példa megoldását rájuk (más szóval, vegyük a **3.1.2.** konstrukciót $n = k$-ra, és mindenkinek annyi pontot adunk, amennyi a súlya). Ez nyilvánvalóan működik, és van egy természetes javítása is: nem kell a pontokat odaadnunk a résztvevőnek, elég a pontjai által generált alteret. m-dimenziós altérből (főleg, ha m nagy) sokkal kevesebb van, mint független pont $m+1$-esből, hiszen egy m-dimenziós alteret $\prod_{i=0}^{d} \frac{q^{m+1}-q^i}{q-1}$-féle pont $m+1$-essel lehet generálni. Egy további javítás található [4]-ben.

Hivatkozások

[1] A. Beutelspacher, U. Rosenbaum, *Projective Geometry: From Foundations to Applications,* Cambridge University Press, 1998.

[2] A. Beutelspacher, F. Wettl, *On 2-level secret sharing,* Des. Codes Crypt. 3 (1993), 127–134.

[3] G. R. Blakley, *Safeguarding cryptographic keys,* In: Proceedings of the national computer conference 48 (1979), 313–317.

[4] S. Caputo, G. Korchmáros, A. Sonnino, *Multilevel secret sharing schemes arising from the normal rational curve,* Discrete Applied Math. 284 (2020), 158–165.

[5] H. S. M. Coxeter, *Affinely regular polygons,* Abh. Math. Sem. Univ. Hamburg 34 (1970), 38–58.

[6] G. C. Fisher, E. R. Jamison, *Properties of affinely regular polygons,* Geom. Dedicata 69 (1998), 241–259.

[7] M. Giulietti, R. Vincenti, *Three-level secret sharing schemes from the twisted cubic,* Discrete Math. 310 (2010), 3236–3240.

[8] J. W. P. Hirschfeld, J. A. Thas, *General Galois Geometries* (Oxford Mathematical Monographs), Clarendon Press, 1991.

[9] Kiss Gy., Szőnyi T., *Véges geometriák,* Polygon Kiadó, 2001.

[10] Gy. Kiss, T. Szőnyi, *Finite Geometries,* CRC Press,Taylor & Francis Group, 2019.

[11] A. Klein, L. Storme, *Applications of finite geometry in coding theory and cryptography,* Comp. Sci., Math 29 (2011), 38–58.

[12] G. Korchmáros, *Poligoni affin-regolari dei piani di Galois d'ordine dispari,* Atti Aacad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur 56 (1974), 690—697.

[13] G. Korchmáros, V. Lanzone, A. Sonnino, *Projective k-arcs and 2-level secret sharing schemes,* Des. Codes Crytogr. 64 (2012), 3–15.

[14] P. Ligeti, P. Sziklai,A. Takáts,*Generalized treshold secret sharing and finite geometry,* Des. Codes Crytogr. 89 (2021), 2067—2078.

[15] C. M. O'Keefe, *Applications of Finite Geometries to Information Security,* Australasian J. Combin. 7 (1993), 195–212.

[16] A. Shamir, *How to share a secret,* Commun ACM 22 (1979), 612–613.