Önálló projektfeladat II. - Kúpszeletek és alkalmazásaik

Fazekas Illés

Alkalmazott matematikus MSc

Témavezető: Kiss György

Bevezetés

Ebben a félévben a kúpszeleteket véges geometriai irányból közelítettük meg. Ehhez megtettük a szükséges előkészületeket, áttekintettük az absztrakt projektív sík fogalmát, és megnéztük, hogy a véges projektív síkok hogyan koordinátázhatók véges testek felett, ezután megvizsgáltuk, hogyan állíthatunk elő véges projektív síkból véges affin síkot, majd láttuk, hogy a véges síkok kúpszeletei hogyan alkalmazhatók különféle problémák megoldására.

Projektív síkok felépítése

Definíció

Tekintsük a $\Pi = (\mathcal{P}, \mathcal{L}, I)$ hármast, ahol $\mathcal{P}$ és $\mathcal{L}$ diszjunkt halmazok, I pedig egy $\mathcal{P} \times \mathcal{L}$-en értelmezett reláció, melyet incidenciarelációnak vagy illeszkedésnek nevezünk, $\mathcal{P}$ lesz a pontok halmaza, $\mathcal{L}$ pedig az egyeneseké. Π absztrakt projektív sík, ha teljesíti a következő axiómákat:

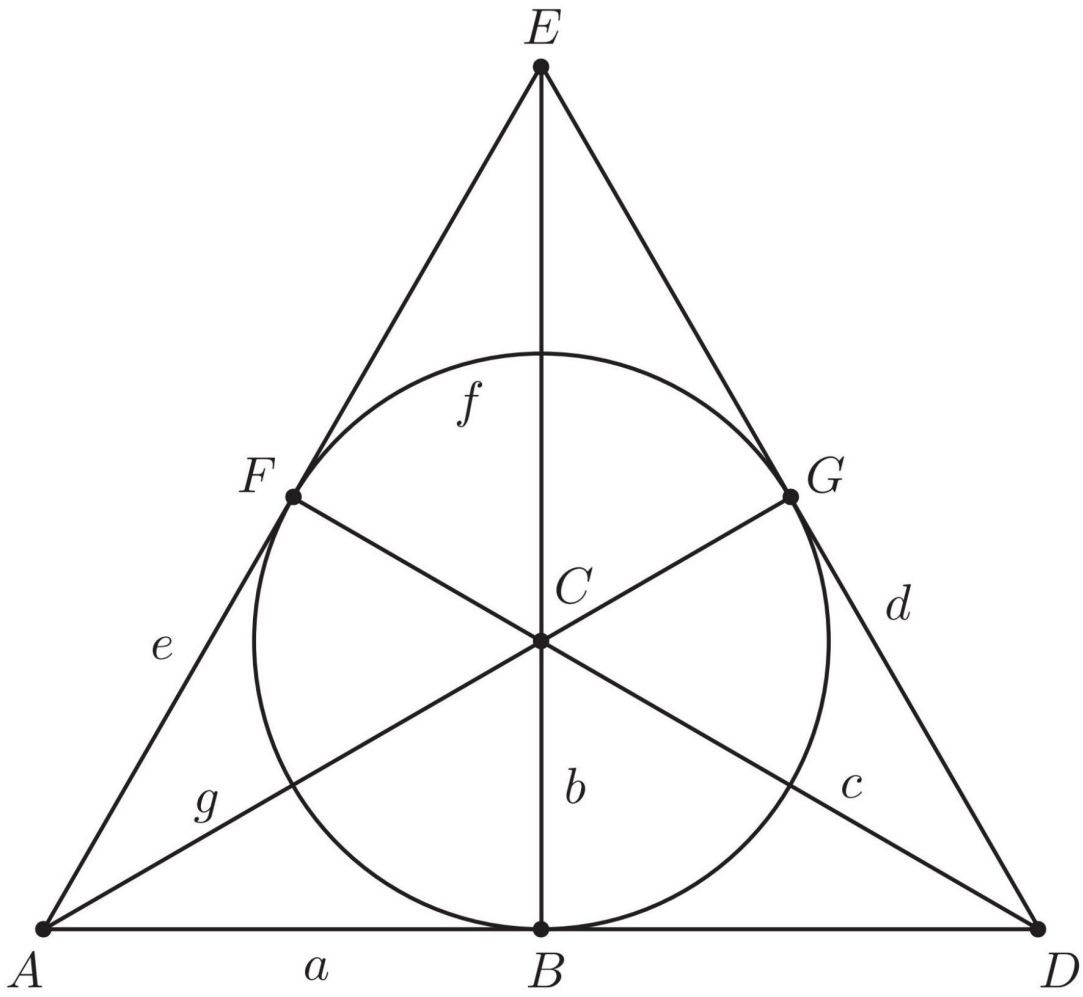
1. $\forall P_1, P_2\ (P_1 \neq P_2) \in \mathcal{P}$-re $\exists! l \in \mathcal{L}$, hogy $(P_1, l), (P_2, l) \in I$, azaz bármely két különböző pontra pontosan egy egyenes illeszkedik.
2. $\forall l_1, l_2\ (l_1 \neq l_2) \in \mathcal{L}$-re $\exists! P \in \mathcal{P}$, hogy $(P, l_1), (P, l_2) \in I$, azaz bármely két különböző egyenesnek pontosan egy metszéspontja van.
3. $\forall l \in \mathcal{L}$-re $|\{\ P \in \mathcal{P} \mid (P, l) \in I\}| \geq 3$, azaz minden egyenes tartalmaz legalább három pontot.
4. $\forall P \in \mathcal{P}$-re $|\{\ l \in \mathcal{L} \mid (P, l) \in I\}| \geq 3$, azaz minden ponton áthalad legalább három egyenes.

A projektív síkot végesnek nevezzük, ha $\mathcal{P}$ és $\mathcal{L}$ véges halmazok.

Projektív síkok felépítése

A fenti felépítés magasabb dimenziókban is működik, így kaphatunk projektív tereket (melyek projektív síkokat tartalmaznak).
Ezek a terek a később látott módon a síkokhoz nagyon hasonlóan koordinátázhatók is.

Példa véges projektív síkra: az ún. Fano-sík



Sík pontjainak és egyeneseinek száma

Tétel

Legyen Π *véges projektív sík. Ha* Π*-nek van olyan egyenese, amelyre* $n+1$ *pont illeszkedik, akkor a következők teljesülnek:*

1. Π *minden egyenesére* $n+1$ *pont illeszkedik*
2. Π *minden pontjára* $n+1$ *egyenes illeszkedik*
3. Π n^2+n+1 *pontot tartalmaz*
4. Π n^2+n+1 *egyenest tartalmaz*

Sík rendje

Definíció

Legyen Π véges projektív sík, melynek minden egyenesére $n+1$ pont illeszkedik. Ekkor az n számot a sík rendjének nevezzük.

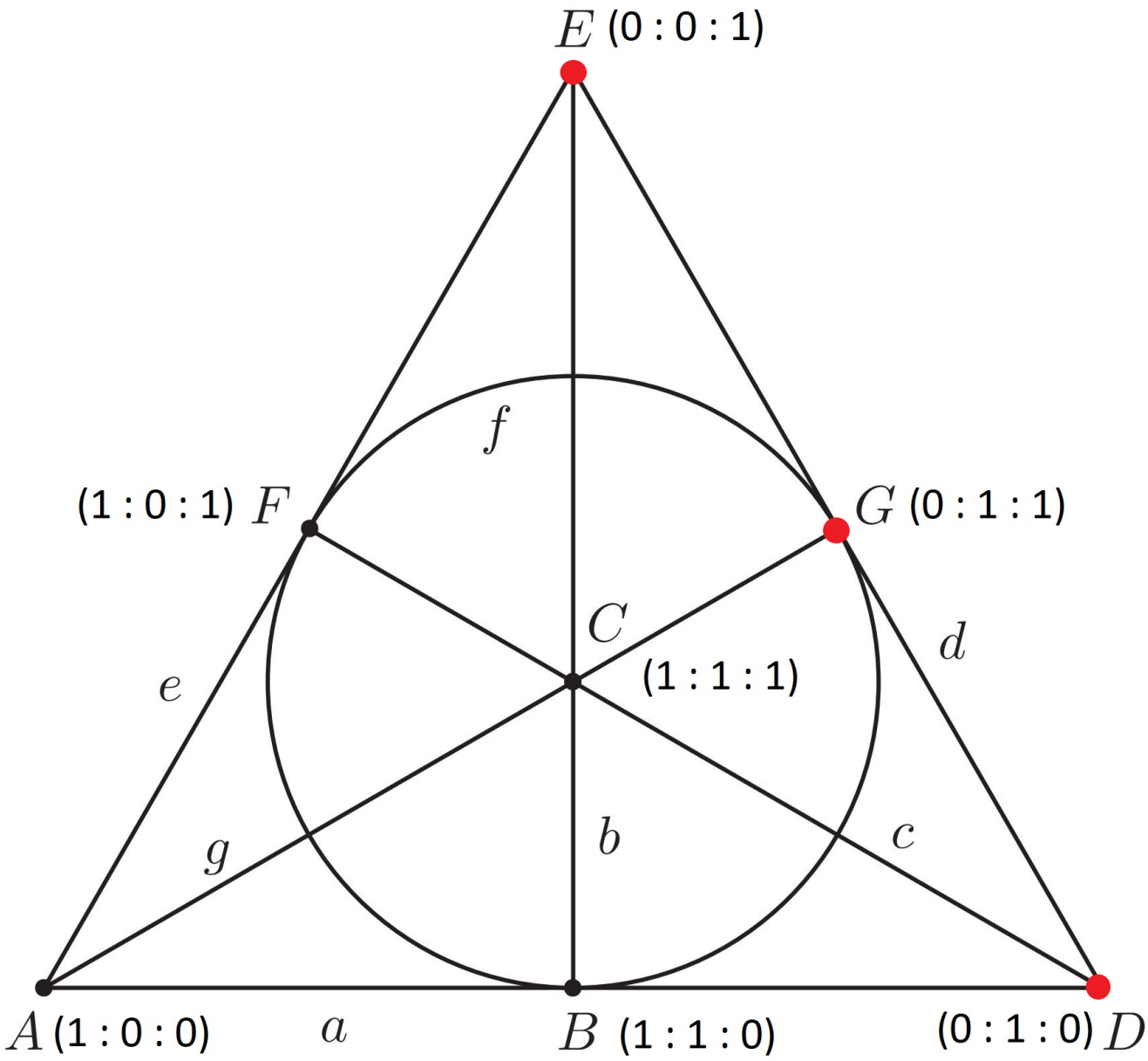
Megjegyezzük, hogy a 3. és 4. axiómák értelmében $n+1 \geq 3$, azaz $n \geq 2$. Ezt visszahelyettesítve a fenti formulába, kapjuk, hogy egy véges projektív síknak legalább $2^2+2+1=7$ pontja és egyenese van, ezzel a minimális tulajdonsággal rendelkezik a fent látott Fano-féle konfiguráció.

A mai napig nyitott, hogy milyen szám lehet projektív sík rendje. Ha q prímhatvány, akkor lehet konstruálni q-adrendű projektív síkot, és az eddig ismert összes projektív sík rendje prímhatvány, a sejtés pedig az, hogy nem is lehet más, de ezt eddig nem sikerült igazolni, csak bizonyos nem prímhatvány rendek létezését kizárni.

Koordinátázás

A véges projektív sík, ha igaz rajta a Desargues-tétel, a klasszikus projektív síkhoz hasonlóan koordinátázható háromkomponensű homogén koordinátákkal, véges test felett. Ezt most bemutatjuk a Fano-síkon, $\mathbb{F}_2$ felett.
A koordinátahármasok itt is invariánsak egy $\lambda \neq 0$ testelemmel való szorzásra, $(a : b : c) \sim (\lambda a : \lambda b : \lambda c)$.
Viszont $\mathbb{F}_2$-ben ilyenkor automatikusan $\lambda = 1$, így a koordináták normáltak, és a nemnulla lineáris kombináció összeggé redukálódik.
Itt is igaz, hogy egy két pont által kijelölt egyenesen akkor van rajta egy harmadik pont, ha az a másik kettő nemnulla lineáris kombinációja, azaz összege.

Koordinátázás



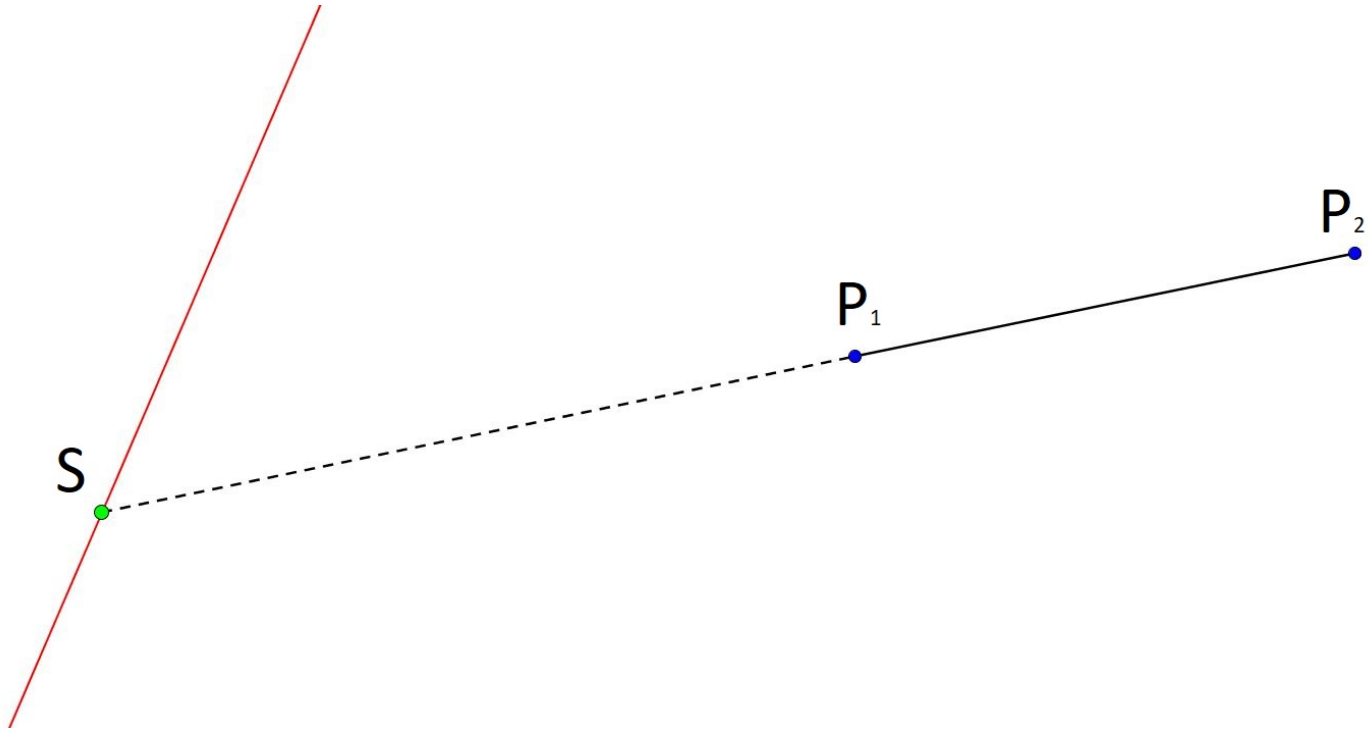
Koordinátázás

A $(0:0:0)$ pont a klasszikus projektív síkkal összhangban itt sincs értelmezve. $\mathbb{F}_2$ felett minden koordináta 0 vagy 1 lehet, ez 8 lehetőség, ebből elvéve a $(0:0:0)$-t, 7 pontot tudunk koordinátázni, éppen ennyi pontja van a konfigurációnak.
Ezeket figyelembe véve szimmetria erejéig a fent ábrázolt koordinátázást kapjuk.
A pirossal jelölt pontok, amelyeknek első koordinátája 0, alkotják az ideális egyenest. Jól látható ebből is, hogy ideális pontok koordinátaösszege ideális pontot ad.

Alkalmazás titokmegosztásra

Adott egy informatikai probléma: egy adatbázisnál/más többek által használt objektumnál szeretnénk megoldani, hogy egy felhasználó egyedül ne férhessen hozzá, ne hajthasson végre módosításokat rajta, viszont többen egyszerre, egymást felügyelve ezt megtehessék.
Két potenciális hozzáférő esetén legyen a megosztani kívánt titok egy véges projektív síknak egy ideális pontja, a hozzáférni kívánóknak kiosztott kulcsok pedig közönséges pontok ezen a síkon, amelyeken átfektetett egyenes a sík ideális egyenesét éppen a titkos pontban metszi, ahogy az ábra mutatja, ahol a piros egyenes az ideális egyenes, a rajta fekvő S pont a titkos pont, P_1 és P_2 pedig a hozzáférni kívánók.

Alkalmazás titokmegosztásra



Alkalmazás titokmegosztásra

Három potenciális hozzáférő esetén is hasonlóan járhatunk el. Vegyünk egy 3 dimenziós, q rendű projektív teret, annak egy ideális egyenesén egy pontot, legyen ez a titok. Osszuk ki a hozzáférőknek a projektív tér egy projektív síkjában fekvő kúpszeletének három pontját. Mivel a pontok egy kúpszeleten fekszenek, automatikusan tudjuk róluk, hogy nem kollineárisak, így meghatároznak egy síkot. Ebből a síkból az előre kijelölt egyenes kimetszi a titkos pontot, viszont a három közül bármely kettő még nem elég a titok meghatározásához.

Megjegyezzük, hogy ez a módszer ún. tökéletes titokmegosztási sémát ad, a kiosztott pontok együtt egyértelműen meghatározzák a titkot, azonban közülük elvéve egyet is, ugyanakkora statisztikai esélye van a titok kitalálásának, mintha vakon próbálkoznánk. (Az ideális egyenesen $q + 1$ pont van ($\frac{1}{q+1}$ valószínűséggel találjuk el a titkot), és ugyanennyi egyenes megy át egy darab előre kiosztott ponton is.)

Véges affin síkok

Egy $\mathbb{F}_q$ felett koordinátázott q-adrendű projektív síkról (q prímhatvány) leválasztva az ideális egyenest, kapunk egy affin síkot q^2 ponttal, ahol a koordináták (a, b) alakúak ($a,\ b \in \mathbb{F}_q$). Ezen affin síkon az egyenesek, a pontok és illeszkedésük analitikus viszonya így alakul:

1. Pontok: (a, b) $a, b \in \mathbb{F}_q$
2. Egyenesek: $[c]$, $[m, k]$, $c,\ m,\ k \in \mathbb{F}_q$
3. Illeszkedés:
   $(a, b)\ I\ [c] \iff a = c$
   $(a, b)\ I\ [m, k] \iff b = ma + k$

Parabola a véges affin síkon

Definíció

A q-adrendű, $\mathbb{F}_q$ felett koordinátázott affin síkon a következő objektumot q-adrendű parabolának nevezzük:

$$\{ (t, t^2) \mid t \in \mathbb{F}_q \}$$

Definíció

Azt mondjuk, hogy az affin síkon egy egyenes érint egy parabolát, ha pontosan egy közös pontja van vele.

Könnyen látszik, hogy a q-adrendű parabolának q pontja van. Igaz az euklideszi síkon is érvényes állítás, hogy egy egyenesnek és egy parabolának legfeljebb 2 közös pontja van, valamint hogy a $[c]$ konstans típusú egyeneseknek a parabolával mindig egy közös pontja van, a többi párhuzamossági osztályban pedig az azonos meredekségűek között pontosan egy egyenes van, ami a parabolát érinti.

Alkalmazás körmérkőzés-szervezésre

Feladat: megszervezni, hogy minden induló csapat minden másikkal pontosan egyszer játsszon, és a fordulók mérkőzései legyenek egy időpontban. Ez $q+1$ csapatra, ahol q páratlan prímhatvány, kivitelezhető q-adrendű parabolával.
Tekintsünk a q-adrendű affin síkon egy q-adrendű parabolát, pontjainak feleltessünk meg q csapatot, a $q+1$-ediket pedig lássuk el egy címkével.

Alkalmazás körmérkőzés-szervezésre

Zárjuk ki a konstans típusú egyeneseket, a többi párhuzamossági osztályból pedig minden meredekségnek feleltessünk meg egy fordulót. Mivel az egyenesek párhuzamosak, egy fordulón belül nem haladhatnak át kétszer ugyanazon a csapaton, viszont az áthaladó egyenesek így diszjunkt csapatpárokat metszenek ki a parabolából, játsszanak ezek egymással a fordulón belül. A 0 meredekségű egyenesosztály egyik egyenese a parabolát egy pontban érinti, az ennek a pontnak megfelelő csapatot párosítsuk össze a felcímkézett csapattal.
Megjegyezzük, hogy az említett módszer páros prímhatvány q-ra azért nem alkalmazható, mert ilyenkor a parabola érintői egy ponton haladnak át, így a fenti gondolatmenet értelmét veszti.