Önálló projektfeladat - Kúpszeletek és alkalmazásaik II.

Fazekas Illés

May 12, 2022

Ebben a félévben a kúpszeleteket véges geometriai irányból közelítjük meg. Az ismert klasszikus projektív síkkal analóg módon felépíthető véges projektív síkokat véges testek felett koordinátázva kapott geometriai struktúrákban másodrendű görbékként megjelenő kúpszeletek önmagukban is érdekesek, és számtalan, eredendően kombinatorikai és kódelméleti probléma kezelésére adnak - nem mellesleg esztétikus - megoldást. Az alábbiakban ezekbe adunk némi betekintést.

Projektív sík felépítése illeszkedési axiómákkal

A klasszikus projektív síkon ismert az alábbi két axióma:

1. Két tetszőleges (egymástól különböző) ponthoz létezik pontosan egy egyenes, amely mindkettőn áthalad.
2. Két tetszőleges (egymástól különböző) egyenes pontosan egy pontban metszi egymást.

Ennek nyomán definiálhatjuk az absztrakt projektív síkot.

Definíció 0.1 *Tekintsük a* $\Pi = (\mathscr{P}, \mathscr{L}, I)$ *hármast, ahol* $\mathscr{P}$ *és* $\mathscr{L}$ *diszjunkt halmazok,* I *pedig egy* $\mathscr{P} \times \mathscr{L}$*-en értelmezett reláció, melyet incidenciarelációnak vagy illeszkedésnek nevezünk,* $\mathscr{P}$ *lesz a pontok halmaza,* $\mathscr{L}$ *pedig az egyeneseké.* Π *absztrakt projektív sík, ha teljesíti a következő axiómákat:*

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

Az 1. és 2., valamint a 3. és 4. axiómák egymás duálisai, ha az egyikben felcseréljük a pontok és egyenesek szerepét, a másikat kapjuk vissza. Így bármely, a projektív síkon megfogalmazott állításnak a duálisa is automatikusan érvényes, elegendő mindig az egyiket bizonyítani.

Hasonlóan elkészíthető minden projektív síkhoz egy duális sík, amelynek pontjai az eredeti sík egyenesei, egyenesei pedig az eredeti sík pontjai, továbbá ezek pontosan akkor illeszkednek az új síkon, ha illeszkedtek a eredetin is. Könnyen meggondolható, hogy az így kapott sík is projektív sík lesz, valamint hogy projektív síkok közt a dualizálás művelete involúció.

Definíció 0.2 *A* Π *projektív síkot véges projektív síknak nevezzük, ha* $\mathscr{P}$ *és* $\mathscr{L}$ *végesek.*

Véges projektív síkra a legegyszerűbb példa az ún. Fano-sík (1. ábra). (Hogy miért a legegyszerűbb, ki fog derülni a koordinátázás során is.) Könnyen ellenőrizhető, hogy erre a konfigurációra teljesülnek a projektív sík axiómái.

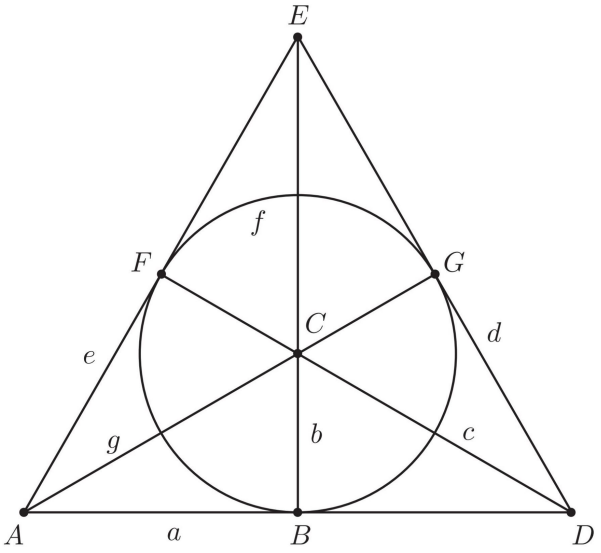

Figure 1: Fano-sík

Tétel 0.3 *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*

Bizonyítás Legyen l a feltételben adott egyenes, melyre illeszkedjenek a P_1, P_2, ..., P_{n+1} pontok. Legyen H egy l-re nem illeszkedő pont. Az 1. axióma miatt H-t összeköthetjük a P_i pontokkal, és az így kapott egyenesek közül semelyik kettő nem esik egybe, mivel l nem tartalmazza H-t. A 2. axióma értelmében viszont a H-n áthaladó egyenesek mind metszik l-et, de ezek a metszéspontok csak a P_i-k lehetnek, így azt kapjuk, hogy H-n pontosan $n+1$ db egyenes halad keresztül. A már említett dualitást használva adódik, hogy ha létezik olyan S pont, ami $n+1$ egyenesre illeszkedik, akkor az S-en át nem haladó egyenesek mindegyikén rendre $n+1$ pont van.

Legyen k egy l-től különböző tetszőleges egyenes. Ekkor a 4. axióma miatt $k \cap l$-en áthalad legalább egy, k-tól és l-től is különböző egyenes, melynek a 3. axióma értelmében van $k \cap l$-től különböző pontja. Jelölje ezt a pontot T. Mivel T nem illeszkedik l-re, ezért rajta $n+1$ egyenes halad át. De T kívül esik k-n is, ezért k-ra is $n+1$ pont esik. Ezzel az 1. állítást beláttuk.

Legyen P tetszőleges pont a Π projektív síkon. Ekkor a 3. és 4. axiómák következtében a sík tartalmaz olyan egyenest, amely nem halad át P-n. A fentiek miatt erre az egyenesre $n+1$ pont illeszkedik, tehát P-n $n+1$ egyenes halad át, ezzel bebizonyítottuk a 2. állítást.

Az 1. axióma értelmében a sík összes pontja előáll, ha felsorakoztatjuk az összes, egy tetszőleges, előre rögzített P ponttal összekötött pontot. Már igazoltuk, hogy P-re $n+1$ egyenes illeszkedik, melyek mindegyike (P-t leszámítva) n pontot tartalmaz, így a sík pontjainak száma $n(n+1)+1 = n^2+n+1$. Az állítást dualizálva kapjuk, hogy a sík egyeneseinek száma is ugyanígy n^2+n+1. Ezzel a tételt beláttuk.

Ezen tétel miatt értelmes a következő definíció:

Definíció 0.4 *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.

Érdekességképp megemlítjük, hogy a mai napig nyitott kérdés, hogy milyen szám lehet projektív sík rendje. Az eddig ismert összes véges projektív sík rendje prímhatvány, és a sejtés is az, hogy csak prímhatvány rendű síkok léteznek, viszont ezt nem sikerült bizonyítani, csupán részleges eredmények vannak, amik bizonyos rendek létezését kizárják.

Koordinátageometriai megközelítés

A klasszikus projektív síkon megismert, O-pont modellen alapuló homogén koordinátázás véges síkok esetében is működik, nagyon hasonlóan. Szerencsés esetben (ha a síkon igaz a klasszikus geometriából is ismert Desargues-tétel), a sík koordinátázható véges test felett. Itt is háromkomponensű koordinátákat használunk, melyek analóg módon invariánsak a nemnulla testelemmel való koordinátánkénti szorzásra. Ezt a felépítést most bemutatjuk a Fano-síkon, $\mathbb{F}_2$ felett.

Az $(a : b : c)$ hármas legyen ekvivalens a $(\lambda a : \lambda b : \lambda c)$ hármassal, ahol $a, b, c, \lambda \in \mathbb{F}_2$, és $\lambda \neq 0$. Szükségképpen, mivel $\mathbb{F}_2$ felett vagyunk, $\lambda = 1$, így a koordináták automatikusan normáltak.

a, b és c egymástól függetlenül 0 vagy 1 lehet, ez összesen 8 lehetőség, de ezek közül ki kell zárni a $(0 : 0 : 0)$ koordinátát, ahogy azt a klasszikus projektív síkon is megtettük, mivel a csupa 0 koordinátájú vektor nem mutatott rá a koordinátázandó sík egy pontjára sem. Így 7 pontot tudunk koordinátázni, éppen ennyi van a Fano-síknak. A konfiguráció koordinátázását az alábbi ábra szemlélteti:

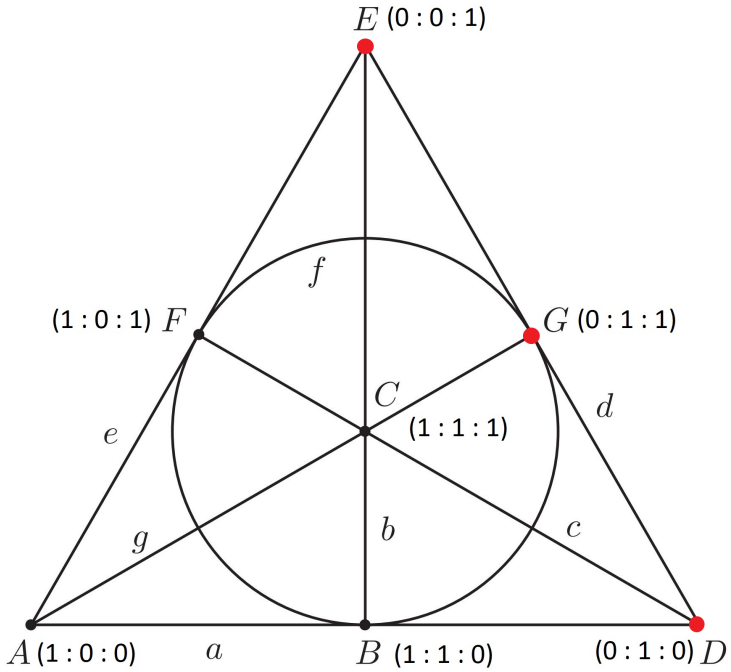

Figure 2: Fano-sík 2

A klasszikus projektív síknál megszokhattuk, 3 különböző pont pontosan akkor kollineáris, ha koordinátáik lineárisan összefüggők, ez itt is igaz. Másképpen megfogalmazva, ha két pont rajta van egy egyenesen, akkor a nemtriviális lineáris kombinációjuk is. Azonban $\mathbb{F}_2$ felett az együtthatók csak 1-esek lehetnek, ennek megfelelően itt a lineáris kombináció összeggé redukálódik. Így, ha önkényesen választunk két különböző pontot reprezentáló 0 - 1 -ekből álló

hármast, az általuk kijelölt egyenesre automatikusan illeszkedik az összegük is, viszont semelyik másik pont nem. (A 3. axiómából következik, hogy ilyen pont van, a koordinátákra kikötött kombinatorikus megszorításból pedig hogy csak egy ilyen van). Ily módon előállítható a fenti ábra, természetesen "forgatás" erejéig.

A klasszikus projektív síkkal analóg módon a 0 első koordinátájú pontok kijelölik a sík ideális egyenesét (az ábrán E, G, D, pirossal jelölve). Látható, hogy speciálisan az ideális egyenes pontjainak koordinátáira is igaz, hogy bármely kettő összege a harmadikat adja, továbbá, az első 0 koordináta az összeadásra nézve invariáns.

Véges projektív síkok alkalmazása titokmegosztási protokollokhoz

Az informatikában felmerülő probléma, hogy adott egy virtuális szoba, adatbázis, megosztott hozzáférésű dokumentum, széf stb, melyet több ember használ, és el szeretnénk érni, hogy egyedül senki se legyen jogosult olvasásra/módosításra/tranzakciók végrehajtására, azonban többen egyszerre (legalább ketten) ezt megtehessék, egymást felügyelve. Ez elérhető véges projektív síkokkal, alább ebbe tekintünk bele.

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 alábbi 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.

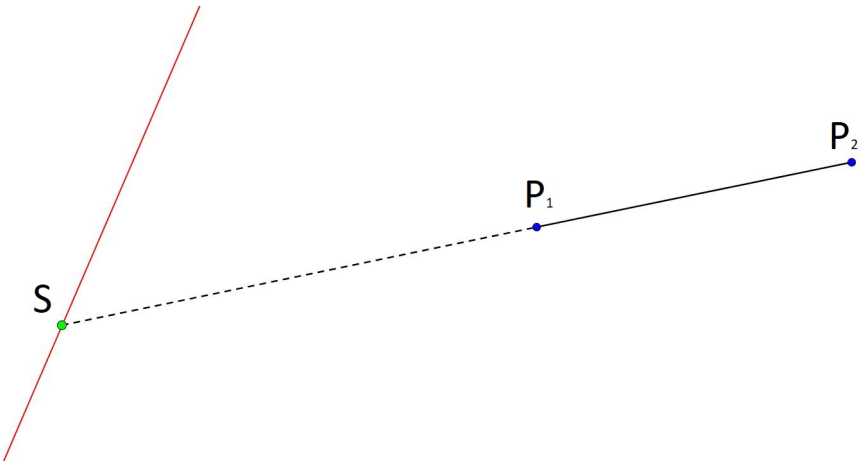

Figure 3: Titokmegosztás

Három potenciális hozzáférő esetén is hasonlóan járhatunk el. Vegyünk egy 3 dimenziós projektív teret, annak egy ideális egyenesén egy pontot, legyen ez a titok. Osszuk ki a hozzáférőknek egy kúpszelet három pontját. Ezekről automatikusan tudjuk, 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.

Az itt vázolt módszer előnye, hogy ún. tökéletes titokmegosztási séma, 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

A q-adrendű, $\mathbb{F}_q$ felett koordinátázott véges projektív síkról leválasztva az ideális egyenest (a 0-val kezdődő koordinátahármassal rendelkező pontokat), kapunk egy $q^2+q+1-(q+1) = q^2$ darab ponttal rendelkező affin síkot, melynek minden koordinátája 1-essel kezdődik, ezért az első komponenst leválaszthatjuk, így (a,b) alakú pontokat kapunk, ahol $a,\ b \in \mathbb{F}_q$, q pedig prímhatvány.

Ezen az affin síkon az egyenesek, a pontok és illeszkedésük a következőképpen alakul:

Pontok: (a,b) $a,b \in \mathbb{F}_q$

Egyenesek: $[c]$, $[m,k]$, $c,\ m,\ k \in \mathbb{F}_q$

Illeszkedés: $(a,b)\ I\ [c] \iff a = c$

$(a,b)\ I\ [m,k] \iff b = ma + k$

Az affin sík egyenesei párhuzamossági osztályokba oszthatók: szétválnak konstans által kifeszített, $[c]$ alakú, és az m meredekség szerint különböző, $[m,k]$ alakú egyenesekre, ahol az osztályok diszjunktak egymástól. Ebből adódik, hogy az affin sík egy adott pontján egy rögzített párhuzamossági osztályból pontosan egy darab egyenes halad át.

Mivel a projektív sík minden egyenesére illeszkedő ideális pont eltávolításával kaptuk az affin síkot, annak minden egyenese q darab pontot tartalmaz. Intuitív módon arra gondolnánk, és viszonylag könnyen bizonyítható is, hogy az affin sík minden pontján $q+1$ egyenes halad át.

Ezen a síkon is - a klasszikus euklideszi/projektív síkhoz hasonlóan - a kúpszeleteket definiálhatjuk analitikusan, másodrendű görbékként, ezt most megmutatjuk a parabolán. Legyen q páratlan prímhatvány, és tekintsük a q-adrendű, $\mathbb{F}_q$ felett koordinátázott affin síkot. Ezen a síkon a következő objektumot q-adrendű parabolának nevezzük:

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

Könnyen látszik, hogy egy q-adrendű parabolának q pontja van, hiszen az első koordináta q-féle lehet, a második pedig meghatározza az elsőt.

Azt mondjuk, hogy egy egyenes érint egy parabolát az affin síkon, pontosan egy közös pontjuk van.

Igazolható az euklideszi síkon megszokott állítás, miszerint a síkon egy parabolának és egy egyenesnek legfeljebb két közös pontja lehet, valamint hogy a $[c]$ konstans típusú egyeneseknek a parabolával mindig egy közös pontja van, a többi párhuzamossági osztályban pedig mindegyikben pontosan egy egyenes van, ami a parabolát érinti.

A fentieket felhasználhatjuk a következő alkalmazásban:

Körmérkőzés-szervezés focibajnokságban

Egy körmérkőzéses focibajnokság megszervezésénél a feladat az, hogy minden induló csapat minden másikkal pontosan egy meccset játsszon, és a fordulók mérkőzései közös időpontban legyenek. Ehhez segítségül hívhatjuk a fenti parabolát, ami majd szolgáltatja a lebonyolítást.

A bajnokságunk tartalmazzon $q+1$ csapatot, ahol legyen q páratlan prímhatvány. Tekintsük az $\mathbb{F}_q$ felett koordinátázott affin síkot, rajta pedig a q-adrendű parabolát. Ennek q darab pontja van, feleltessünk meg minden pontnak egy csapatot, és a kimaradó $q+1$-ediket lássuk el egy címkével. A konstans típusú egyeneseket zárjuk ki, a többi párhuzamossági osztályból pedig minden $[c]$ meredekségnek feleltessünk meg egy fordulót (a párhuzamosság miatt nyilván nem fordulhat elő, hogy két különböző meredekségű egyenes összemetsszen, így semelyik csapaton sem halad át két egyenes egy fordulón belül). A konstans meredekségű, a parabolát egy pontban érintő párhuzamossági osztály által kijelölt érintési pontnak megfelelő csapatot pedig párosítsuk

össze a felcímkézett csapattal. Az így kapott kimetszett pontpárok megadják a fordulók egy lehetséges lebonyolítását, amely eleget tesz annak, hogy mindenki mindenkivel játsszon, és a meccsek egy időben legyenek.

Megjegyezzük, hogy a fenti konstrukcióhoz azért szükséges, hogy q páratlan prímhatvány legyen, mert ellenkező esetben, ha $q = 2^k$, akkor a parabola érintői - elsőre meglepő módon - konkurrensek, és a fenti okoskodás értelmét veszti.

A fenti módszert valóban használják is olyan bajnokságokban, ahol prímhatvány plusz egy csapat indul, többek között ilyen a mostani magyar NB I. is 12 csapattal ($q = 11$).

Felhasznált irodalom

Munkám során Kiss György és Szőnyi Tamás *VÉGES GEOMETRIÁK* c. könyvére, valamint Ujváry János *Focibajnokságok és véges geometriák* c. szakdolgozatára támaszkodtam.