SZIMMETRIKUS STRUKTÚRÁK

Szőnyi Tamás

Oktatási segédanyag, 1998.

1 ILLESZKEDÉSI STRUKTÚRÁK

1.1 PROJEKTÍV ÉS AFFIN SÍKOK ÉS TEREK

Ebben a szakaszban a projektív és affin síkokkal kapcsolatos alapismereteket tekintjük át. A felhasznált algebrai tények szerepelnek szinte minden standard algebra jegyzetben.

Definíció 1.1 *Projektív sík*nak nevezünk egy (Π, Λ) párt, ahol Π nem-üres halmaz (elemeit *pont*nak fogjuk nevezni), Λ pedig Π bizonyos részhalmazainak halmaza (elemeit *egyenes*nek mondjuk), ha eleget tesz az alábbi axiómáknak:

Ax.1 Π bármely két különböző pontjához egy és csak egy olyan egyenes található, amely mindkettőt tartalmazza.

Ax.2 Λ bármely két különböző egyeneséhez egy és csak egy olyan pont van Π-ben, amelyet mindkét egyenes tartalmaz.

Ax.3 Létezik négy olyan pont Π-ben, amelyek közül semelyik hármat nem tartalmazza egy egyenes.

Alkalmazzuk a szokásos geometriai terminológiát, "eleme" ill. "tartalmaz" helyett gyakran használjuk majd az "illeszkedik", "átmegy", "rajta van" stb. szemléletes kifejezéseket.

Definíció 1.2 Egy projektív sík véges, pontosabban szólva *q-adrendű*, ha a következő (végességi) axiómát is teljesíti:

Ax.4 Van olyan egyenes (Λ-beli elem) amely $q + 1$ pontot tartalmaz.

Mielőtt továbblépünk idézzük fel a q-adrendű véges projektív síkok néhány aritmetikai tulajdonságát:

(1) minden egyenesnek $q + 1$ pontja van.

(2) minden pontot $q + 1$ egyenes tartalmaz.

(3) a pontok és az egyenesek száma egyaránt $q^2 + q + 1$.

Axiómarendszerünk talán legismertebb modellje, a 7 pontból és 7 egyenesből álló Fano-sík (aholis $q = 2$), ld. később az 1.11, 1.13, 1.18 Példákat. Jólismert tény, hogy tetszőleges testre (annak kommutativitásától függetlenül) mindig építhetünk projektív síkot. Az eljárás a klasszikus projektív geometriából ismert homogén koordináták bevezetésére épül.

Abban az esetben, ha a test véges, algebrából ismert tény, hogy elemszáma prímhatvány, és hogy minden prímhatványhoz egyetlen annyi elemet tartalmazó véges test van. Ezt a testet szokás *Galois-test*nek nevezni és $GF(q)$-val jelölni. Az eddigiek szerint ekkor $q = p^h$, ahol p prímszám, h pedig természetes szám. A $GF(q)$ testre épített projektív sík q-adrendű lesz, ezt a síkot $PG(2,q)$-val fogjuk jelölni.

Tekintsük át röviden a homogén és inhomogén koordinátákkal kapcsolatos ismereteket. Először lássuk a homogén koordináták bevezetését:

Legyenek a "pontok" a $(x_1,x_2,x_3)\in GF(q)^3\setminus\{(0,0,0)\}$ vektorok ekvivalencia-osztályai az alábbi ekvivalencia-relációnál: $(x_1,x_2,x_3)\sim(y_1,y_2,y_3)$, akkor és csak akkor ha van olyan $0\neq\lambda\in GF(q)$, amelyre $x_i=\lambda y_i$, $i=1,2,3$. Az egyenesek az $\{(x_1,x_2,x_3) : u_1x_1+u_2x_2+u_3x_3=0\}$ alakú ponthalmazok. Így egy egyeneshez is hozzárendelhetünk homogén koordinátákat, t.i. az $[u_1,u_2,u_3]$ homogén számhármast.

Geometriailag ezt nagyon könnyű elképzelni. Legyenek a pontok a háromdimenziós vektortér origón átmenő "egyenesei" (azaz egydimenziós alterei), az egyenesek pedig az origón átmenő "síkok" (azaz kétdimenziós alterek). Az illeszkedés természetesen a tartalmazás. Ekkor pont egy koordinátája az egyenes egy irányvektora, míg egyenesé az őt reprezentáló sík normálvektora. Ez sugallja is a rövid vektor-jelölést, mind pontra, mind egyenesre, az illeszkedés pedig valóban a skaláris szorzat nulla voltának felel meg.

Tétel 1.3 *A $GF(q)$ véges testre a homogén koordináták segítségével egyértelműen építhetünk projektív síkot, melyet $PG(2,q)$-val jelölünk.*

Hasonlóan a projektív síkokhoz, az affin síkokat is definiálhatnánk axiomatikusan. Ezt a rövidség kedvéért most nem tesszük meg (ld. 1.1. Feladatot), csupán azt jegyezzük meg, hogy egy "absztrakt" projektív síkból egy egyenes és annak pontjai törlésével kaphatunk "absztrakt" affin síkot. Természetesen ugyanúgy, mint a klasszikus geometriában nemcsak projektív, hanem affin síkot is építhetünk testekre. Ez a konstrukció is fontos lesz számunkra. Ezt a szokásos módon (a középiskolából ismert analitikus geometria mintájára) tehetjük meg, és mindaz amit ideális térelemekről valamint az affin és a homogén koordinátákról klasszikus geometriából ismerünk kiterjeszthető tetszőleges testre épített affin és projektív síkokra (ld. például Coxeter, Kárteszi, illetve Radó–Orbán könyveit). A $GF(q)$ véges testre épített affin síkot $AG(2,q)$-val jelöljük. Mivel az $AG(2,q)$ affin sík a q-adrendű $PG(2,q)$-ból egy egyenes törlésével kapható, így a következő tételt könnyű belátni.

Tétel 1.4 *$AG(2,q)$-ban minden egyenesnek q pontja van, minden pontot $q+1$ egyenes tartalmaz, a pontok száma q^2, az egyenesek száma q^2+q.* ∎

Eszerint tehát az AG$(2,q)$ affin sík a $K=GF(q)$ alaptestre épített kétdimenziós vektortér, az egyenesek az egydimenziós alterek és eltoltjaik. Idézzük fel a homogén és inhomogén koordináták közti áttérést: az (x,y) inhomogén koordinátájú pontnak az $(x,y,1)$ által reprezentált pont felel meg, míg a (x,y,z), $(z\neq 0)$ pont inhomogén koordinátája $(x/z,y/z)$. Ha egy egyenes inhomogén egyenlete $Ax+By=C$, akkor az egyenes homogén koordinátái $[A,B,-C]$. Megfordítva, ha a homogén egyenlet $u_1x_1+u_2x_2+u_3x_3=0$, akkor az inhomogén egyenlet $u_1x+u_2y=-u_3$ (persze ez csak akkor értelmes, ha u_1 és u_2 valamelyike nem nulla.)

Érdemes megfogalmaznunk a *"dualitás elvét"*, vagyis, hogy egy projektív síkról szóló állításban a pont és egyenes szavak felcserélhetőek. Ez persze csak akkor igaz, ha állításunkat csupán az axiómák segítségével tudjuk belátni, vagy ha ezeken kívül önduális állításokat használunk.

Az eddig ismertetett konstrukciók fő előnye, hogy magasabb dimenzióra gond nélkül kiterjeszthetőek. Itt eltekintenénk az "absztrakt" véges terek definiálásától, mert ez több technikai nehézséget vet fel. Mindjárt az első az, hogy mit tekintsünk alapelemeknek. Lehet ugyanis csupán a pontokat és egyeneseket alapelemnek tekinteni, de lehet a pontokat, síkokat, tereket, ..., hipersíkokat is. Mindegyik megközelítésnek megvan a maga létjogosultsága. Most azonban elég, ha csak annyit említünk meg, hogy az absztrakt projektív tereket az jellemzi, hogy minden síkjuk (azaz bármely három pont összekötésre és metszésre vonatkozó generátuma) projektív sík. A legfontosabb ismeret projektív terekről az, hogy bennük érvényes a *Desargues tétel*. (Itt a Desargues tétel szokásos "térbeli" bizonyítására kell gondolnunk, amely megtalálható pl. Coxeter: Projektív geometria c. könyvében a 32–33. oldalakon (2.31., 2.32.).) Ebből azt is le lehet vezetni, hogy van olyan ferdetest, amellyel koordinátázhatjuk a teret. Mivel Wedderburn tétele miatt minden véges ferdetest test, így a véges terek leírásához elegendő azt tudnunk, hogy (kommutatív) testtel hogyan koordinátázhatunk projektív teret.

Nézzük először az affin tereket. Ezek a koordinátatest feletti valahány dimenziós vektorterek, az egyenesek az egydimenziós alterek és eltoltjaik, a síkok a kétdimenziós alterek és eltoltjaik, s.í.t., a hipersíkok az egy kodimenziós alterek és eltoltjaik.

Az n dimenziós projektív tér pontjai egy $n+1$-dimenziós vektortér 1-dimenziós alterei, egyenesei a kétdimenziós alterek, s.í.t., a hipersíkok az 1 kodimenziós alterek. Ezzel a szemléltetéssel mindazt, amit lineáris algebrában vektorterekkel kapcsolatban tanultunk, (pl. lineáris függetlenség, függőség, generálás, bázis, stb.) könnyen átvihetjük projektív és affin terekre.

A részletekkel kapcsolatosan Kárteszi könyvének 2.1 és 2.2 szakaszára utalunk. Ugyancsak melegen ajánljuk Radó–Orbán: A geometria mai szemmel c. könyvének második fejezetét, valamint a harmadik és negyedik fejezet egyes részeit.

A vektorteres reprezentáció arra is jó, hogy segítségével a projektív és affin síkok automorfizmusait (a geometriai szóhasználattal: *kollineációit*), azaz az egy egyenesen levő pontokat egy egyenesen levőkbe vivő bijekciókat is könnyen át tudjuk tekinteni.

Tétel 1.5 *$AG(n,K)$ minden kollineációja $x \to Ax^\sigma + b$ alakú, ahol A $n \times n$-es nem-szinguláris mátrix, b fix vektor, míg σ rögzített test-automorfizmus. (Ezek a kollineációk az $A\Gamma L(n,K)$ csoportot alkotják.)*

Hasonlóan $PG(n,K)$ kollineációi $x \to Ax^\sigma$ alakúak, ahol A $(n+1)\times(n+1)$-es nem-szinguláris mátrix, σ testautomorfizmus.

E tétel második felét gyakran a **Projektív geometria alaptételének** is nevezik.

Teljesen hasonlóan írhatók le a korrelációk is, csak itt az eredményül kapott vektort egyenes koordinátáinak tekintjük. *Polaritás*nak másodrendű korrelációt nevezünk. Geometriából tudjuk, hogy polaritás esetén a σ automorfizmus másodrendű kell legyen (ill. identitás). Ha $\sigma = id$, akkor a mátrix szimmetrikus kell legyen ilyenkor az autokonjugált pontok kúpszeletet alkotnak (ha q páratlan). Ha $\sigma \neq id$, akkor az A mátrixnak Hermite-félének kell lennie, azaz ha elemenként alkalmazzuk rá σ-t, akkor a mátrix transzponáltját kapjuk. Mindaz amit most elmondtunk, magasabb dimenzióban is így van. A különbség csak annyi, hogy a $\sigma = id$ esetben a mátrix lehet ferdén szimmetrikus is. Az ilyen mátrixok determinánsa akkor lehet nem nulla, ha a méretük páros, azaz, ha a dimenzió páratlan. Három dimenzióban egy ilyen mátrix ú. n. nullapolaritást ad meg. A q páros eset kissé bonyolultabb, azzal most mi nem foglalkozunk. Lényeges tehát, hogy a polaritásokat pontosan ismerjük, és testre épített síkok esetén csupán kétféle polaritás van.

További természetes kérdés, hogy egy polaritásnak hány autokonjugált pontja (azaz olyan pont, amely illeszkedik a polárisára) lehet. Bose bizonyította, hogy projektív sík polaritásának mindig legalább annyi autokonjugált pontja van, mint egy egyenesnek. A másik oldalról az is érdekes, hogy legfeljebb hány autokonjugált pont lehet. Erre q-adrendű sík esetén az a válasz, hogy legfeljebb $q^{3/2}+1$. Testre épített négyzetrendű síkokon vannak is olyan (unitér vagy Hermite-féle) polaritások, amelyeknek pontosan ennyi autokonjugált pontja van. Ezzel kapcsolatban ld. még a 2. Feladatot. Ismerünk olyan nem testre épített síkokat, amelyeken az autokonjugált pontok száma $q^{5/4}+1$.

1.2 Feladatok

1.1., affin sík axiómái:

A.1. két ponton egy és csak egy egyenes megy.

A.2. egy egyeneshez és egy rajta nem levő ponthoz egy és csak egy olyan, a ponton átmenő egyenes van, amely az egyenest nem metszi.

A.3. van három nem egy egyenesen fekvő pont.

1.2., az $(x_1,x_2,x_3)^\sigma = (x_1^{\sqrt{q}}, x_2^{\sqrt{q}}, x_3^{\sqrt{q}})$ leképezés olyan polaritás, amelynek $q\sqrt{q}+1$ autokonjugált pontja van.

1.3., Számítsuk ki, hogyan hat egy kollineáció a hipersíkokon!

1.4., Mit jelent a dualitás elve magasabb dimenzióban?

1.5., Lássuk be, hogy affin sík mindig beágyazható projektívba!

1.3 ILLESZKEDÉSI STRUKTÚRÁK

Definíció 1.6 *Illeszkedési struktúrá*nak egy $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ hármast nevezünk, ahol $\mathbf{P}$ és $\mathbf{B}$ két diszjunkt halmaz, I pedig egy $\mathbf{P}$ és $\mathbf{B}$ elemei közti reláció, azaz $I \subset \mathbf{P} \times \mathbf{B}$. Az elnevezés geometriai indíttatású, ennek megfelelően $\mathbf{P}$ elemeit *pont*oknak, $\mathbf{B}$ elemeit *blokkok*nak nevezzük, az I relációt pedig *illeszkedési relációnak*. Az I elemeit (mint rendezett párokat) *zászló*knak is fogjuk mondani.

A geometriai terminológiának megfelelően ahelyett, hogy $(p, B) \in I$ azt írjuk majd, hogy pIB és azt mondjuk, hogy a p pont *illeszkedik* a B blokkra vagy a B blokk *átmegy* p-n, stb. A motiváló geometriai példa a sík pontjainak és egyeneseinek példája, az egyenes elnevezést azonban csak olyan esetekben fogjuk használni, amikor a blokkok valóban egyeneshez hasonló tulajdonságokkal rendelkeznek. Geometriában is gyakran azonosítjuk az egyeneseket az őket alkotó pontok halmazával és ezt illeszkedési struktúrákra is megtehetjük csekély megszorítások mellett. Mielőtt azonban ezt megtennénk, vezessünk be néhány további fogalmat. Mindenekelőtt az izomorfizmus fogalmát definiáljuk.

Definíció 1.7 Legyen $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ és $\mathbf{D}' = (\mathbf{P}', \mathbf{B}', I')$ két illeszkedési struktúra. A $\pi : \mathbf{P} \cup \mathbf{B} \to \mathbf{P}' \cup \mathbf{B}'$ leképezés *izomorfizmus*, ha bijekció és

$$\mathbf{P}^\pi = \mathbf{P}', \quad \mathbf{B}^\pi = \mathbf{B}';$$

$$pIB \iff p^\pi I' B^\pi, \ \forall p \in \mathbf{P}, \ \forall B \in \mathbf{B}.$$

Azt is mondjuk, hogy ilyenkor $\mathbf{D}$ és $\mathbf{D}'$ *izomorf.* Ha $\mathbf{D} = \mathbf{D}'$, akkor π-t *automorfizmus*nak nevezzük.

A geometriai szóhasználat motiválja a duális struktúra bevezetését is.

Definíció 1.8 A $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ illeszkedési struktúra *duálisa* a $\mathbf{D}^* = (\mathbf{P}^*, \mathbf{B}^*, I^*)$ rendszer, ahol $\mathbf{P}^* = \mathbf{B}$, $\mathbf{B}^* = \mathbf{P}$, míg I^* az I reláció inverze.

Nem igaz, hogy egy struktúra duálisa izomorf volna az eredeti struktúrával, de az persze igen, hogy duális duálisa az eredeti.

Definíció 1.9 Legyen $p \in \mathbf{P}$ egy pont. A *p pont fok*a a p-hez illeszkedő blokkok száma, azaz

$$\deg(p) = |\{B \in \mathbf{B} \ : \ p \ I \ B\}| \, .$$

Hasonló módon egy *B blokk fok*a a hozzá illeszkedő pontok száma, azaz

$$\deg(B) = |\{p \in \ : \ p \ I \ B\}| \, .$$

Jegyezzük meg, hogy egy illeszkedési struktúrában előfordulhat, hogy két különböző blokk (egyenes) ugyanazokhoz a pontokhoz illeszkedik. Ha ez nem történik meg, az illeszkedési struktúrát *egyszerű*nek nevezzük. Egyszerű illeszkedési struktúrára a blokkok azonosíthatók a hozzájuk illeszkedő pontokkal. Ez pontosan azt jelenti, hogy $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ izomorf lesz a $\mathbf{D}^* = (\mathbf{P}, \mathbf{B}^*, \in)$ struktúrával, ahol $\mathbf{B}^* = \{\{p : pIB\} \ : \ B \in \mathbf{B}\}$. Mostantól kezdve főleg ilyen egyszerű illeszkedési struktúrákat vizsgálunk, és úgy képzeljük, hogy a fenti azonosítást már elvégeztük, azaz a blokkok a pontok bizonyos részhalmazai. Egyszerű illeszkedési struktúra helyett használjuk a *hipergráf* illetve a *halmazrendszer* kifejezéseket is. Ebben az esetben a blokk foka helyett a blokk mérete kifejezést is használjuk.

Definíció 1.10 A $\mathcal{H} = (V(\mathcal{H}), E(\mathcal{H}))$ pár hipergráf, ha $E(\mathcal{H})$ elemei a $V(\mathcal{H})$ bizonyos részhalmazai. Egy hipergráfot *r-reguláris*nak nevezünk, ha benne minden pont foka r. Hasonlóan a hipergráf *k-uniform*, ha minden blokk (él) mérete (foka) k. Gyakran az r és k paramétereket elhagyjuk, és egyszerűen reguláris illetve uniform hipergráfról beszélünk.

Érdemes megjegyezni, hogy egy illeszkedési struktúra duálisa akkor lesz egyszerű, ha nincsenek olyan pontok az eredeti struktúrában, amelyek pontosan ugyanazokra a blokkokra illeszkednek (azaz mintegy párban fordulnak elő). Természetesen reguláris hipergráf duálisa uniform, és megfordítva.

Példa 1.11 Legyen $\mathbf{P} = \{0, \ldots, 6\}$, míg

$$\mathbf{B} = \{\{0,1,3\}, \{1,2,4\}, \{2,3,5\}, \{3,4,6\}, \{4,5,0\}, \{5,6,1\}, \{6,0,2\}\}.$$

Az illeszkedés természetesen legyen az $\in$ reláció. Ezt az illeszkedési struktúrát Fano-síknak nevezik, az alábbi rajzot már valószínűleg mindenki látta.

Az elnevezés onnan származik, hogy G. Fano olasz geométer ezt a konfigurációt zárta ki a projektív (tér)geometria axiomatizálásakor.

Az illeszkedési struktúrák mátrixokkal is reprezentálhatók.

Definíció 1.12 Legyen $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ véges illeszkedési struktúra. Soroljuk fel a pontokat: $p_1, \ldots, p_v$, valamint a blokkokat: $B_1, \ldots, B_b$. $\mathbf{D}$ *illeszkedési* *mátrixa* az az $M = (m_{ij})$ $(i = 1, \ldots, v; j = 1, \ldots b)$ mátrix, amelyben

$$m_{ij} = \begin{cases} 1, & \text{ha} \quad p_i \; I \; B_j \\ 0, & \text{különben.} \end{cases}$$

A későbbiekben gyakran előfordul, hogy illeszkedési mátrix helyett *incidencia mátrix*ot mondunk. Szokás hasonlóan a $(-1, 1)$-illeszkedési mátrixot is definiálni, itt a 0 helyett -1-eket írunk.

A $\mathbf{D}$ *adjacencia mátrix*a az $A = MM^T$ mátrix, amely természetesen szimmetrikus. Az adjacencia mátrix i-edik sorának j-edik eleme azt számolja, hogy hány olyan blokk van, amely p_i-hez és p_j-hez egyaránt illeszkedik. Speciálisan, a főátlóban az egyes pontok fokai szerepelnek.

Hasonló módon a duális illeszkedési struktúrára szintén bevezethetjük az adjacencia mátrixot. Ezt az eredeti illeszkedési struktúra *blokk-adjacencia* mátrixának fogjuk hívni, mely nem más, mint $M^T M$.

Példa 1.13 A Fano-sík illeszkedési mátrixa

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Lemma 1.14 *Tetszőleges illeszkedési struktúrában*

$$\sum_{p \in \mathbf{P}} \deg(p) = \sum_{B \in \mathbf{B}} \deg(B). \tag{1}$$

Bizonyítás. Számoljuk meg a zászlókat (illeszkedő pont-blokk párokat) kétféleképpen. ∎

Korollárium 1.15 *Legyen $\mathcal{H}$ r-reguláris, k-uniform hipergráf, melynek v pontja és b blokkja (éle) van. Ekkor $vr = bk$.* ∎

Definíció 1.16 Egy illeszkedési struktúra *komplementer*ének azt a struktúrát nevezzük ahol a pontok és a blokkok változatlanok, az illeszkedési reláció pedig a komplementer reláció (azaz a komplementer struktúrában egy pont akkor és csak akkor illeszkedik egy blokkra, ha az eredetiben nem illeszkedett.)

Hipergráfokra persze ezt úgy is elmondhatjuk, hogy az éleket cseréljük ki a komplementerükre. Nyilvánvaló, hogy reguláris hipergráf komplementere reguláris, uniformé pedig uniform, mégpedig $k' = v - k$ és $r' = b - r$.

Példa 1.17 A Fano-sík komplementere 7 pontú, 7 blokkú struktúra, minden pont foka 4, minden blokk mérete 4. (Később majd újra találkozunk ezzel a struktúrával az ú.n. Hadamard-féle blokkrendszerek között.)

Ugyan illeszkedési struktúrák izomorfizmusát már korábban definiáltuk, most azonban nézzük meg egy kicsit közelebbről mit jelent az izomorfizmus az illeszkedési mátrixok nyelvén. Ez azt jelenti, hogy az egyik struktúra illeszkedési mátrixa ugyanaz, mint a másiké, ha ott a π permutáció által megadott sorrendben írjuk fel a sorokat és oszlopokat. Más szavakkal, ha tetszőlegesen felírt illeszkedési mátrixokból indulunk, akkor ez pontosan azt jelenti, hogy az egyik illeszkedési mátrix a másikból a sorok és oszlopok permutációjával megkapható. Formálisan ez azt jelenti, hogy vannak olyan P, Q permutáció-mátrixok, amelyekre

$$PMQ = M', \tag{2}$$

ahol persze M illetve M' a $\mathbf{D}$ ill. $\mathbf{D}'$ illeszkedési mátrixa. Egy $\mathbf{D}$ illeszkedési struktúra automorfizmusai (a kompozíció műveletére nézve) csoportot alkotnak, melyet $\mathbf{D}$ *teljes automorfizmus-csoportjá*nak nevezünk, és $\mathrm{Aut}(\mathbf{D})$-vel jelölünk. Ha csak azt mondjuk, hogy automorfizmus-csoport (a teljes jelző nélkül), akkor $\mathrm{Aut}(\mathbf{D})$ részcsoportjaira gondolunk.

Példa 1.18 A Fano-sík automorfizmus-csoportját fogjuk meghatározni. A $\varphi : x \to x + 1$ (ahol az összeadást mod 7 végezzük) nyilván automorfizmus (így definiáltuk a blokkokat). Ezenkívül az ábrából látszik, hogy a szabályos háromszög egybevágóságai a középpontot (2) önmagába vivő automorfizmusok. Ezenkívül minden 'magasságvonal'-hoz meg tudunk adni néhány további (másodrendű) automorfizmust: ilyen pl. az (1)(2)(4)(35)(06), valamint az (1)(2)(4)(50)(36) leképezés (a harmadik hasonlóan kapható automorfizmus épp a magasságvonalra való tükrözés, amely az (1)(2)(4)(30)(56) permutáció). Végezetül az (14)(2)(3)(5)(60) leképezés is automorfizmus. Ezek mind másodrendű permutációk, amelyek fixálják az 142 egyenest, így ezek szorzata is ilyen. Könnyen ellenőrizhető, hogy a felsorolt elemek nyolcadrendű elemi Abel csoportot generálnak (amelyben az először felsorolt három elem az identitással egy negyedrendű részcsoportot alkot). Ennek alapján az automorfizmuscsoport rendje legalább $168 = 7 \cdot 3 \cdot 8$ elemet tartalmaz.

Persze, az előző szakasz szerint a Fano-sík a kételemű testre épített projektív sík, így a projektív geometria alaptételéből azonnal tudjuk, hogy a teljes automorfizmus-csoport a 168 elemű $\mathrm{PGL}(3, 2)$ egyszerű csoport. Geometriából azt is tudhatjuk, hogy testre épített projektív síkon tetszőleges négyszög leképezhető tetszőleges négyszögre. (Most és a következőkben, négyszögnek négy olyan pontot nevezünk, amelyből semelyik három nincs egy egyenesen, s a háromszöget is hasonló értelemben használjuk.) A Fano-síkban minden háromszög egyetlen négyszögben van benne, így ez ugyanazt jelenti, mintha azt mondanánk, hogy bármely háromszög átvihető bármely más háromszögbe. Azt pedig könnyű látni (illetve ellenőrizni), hogy ha egy automorfizmus egy háromszög mindhárom csúcsát fixálja, akkor az az identitás. Ebből az észrevételből geometriai ismeretek nélkül is adódik, hogy az automorfizmus-csoport rendje legfeljebb a háromszögek száma, ami $7 \cdot 6 \cdot 4 = 168$. Mivel fentebb meg is konstruáltunk ennyi elemet, így a fenti automorfizmusokból tényleg előállítható valamennyi automorfizmus.

Mindazokat a geometriai fogalmakat, amelyeket most használtunk, megtalálhatjuk az 1.1 szakaszban.

Definíció 1.19 Olyan illeszkedési struktúrát, amelyben a pontok száma azonos a blokkok számával, *négyzetes*nek (vagy nagynéha *szimmetrikus*nak) nevezünk.

Tétel 1.20 *Legyen* $\mathbf{D}$ *olyan négyzetes illeszkedési struktúra, melynek illeszkedési mátrixa nem szinguláris, továbbá legyen* $\alpha \in \mathrm{Aut}(\mathbf{D})$. *Ekkor* α *fixpontjainak száma megegyezik a fixblokkok számával.*

Bizonyítás. Legyen a szóbanforgó illeszkedési mátrix M. α automorfizmus volta miatt létezik két permutációmátrix P, Q, melyekre $PMQ = M$ teljesül (ld. (2)). P az α pontokon, Q a blokkokon való hatását írja le. Nyilván a fixpontok száma éppen P nyoma, azaz $\mathrm{tr}(P)$, s hasonlóan a fixblokkok száma $\mathrm{tr}(Q)$. Mivel M nem-szinguláris, így

$$Q = M^{-1}P^{-1}M,$$

azaz Q nyoma megegyezik P^{-1} nyomával. Másrészt viszont P permutációmátrix, így P nyoma megegyezik P^{-1} nyomával. ∎

Ennek alapján természetes azt kérdezni, hogy vajon $\mathrm{Aut}(\mathbf{D})$ ugyanúgy hat-e a pontokon és a blokkokon. Erre általában a válasz nemleges, azonban az előző bizonyításból még további információkat is ki tudunk deríteni. Ehhez lássunk először egy elemi lemmát permutáció-csoportokra. A lemmát igen gyakran Burnside-lemmának nevezik, de helyesebb volna Cauchy–Frobenius lemmának hívni, mivel már Cauchy is implicite felhasználta.

Lemma 1.21 (Burnside-lemma) *Legyen* $G \leq Sym(\Omega)$ *(azaz* G *permutációcsoport az* Ω *jegyhalmazon). Tegyük fel, hogy* G*-nek* s *orbitja van. Egy* $g \in G$ *elemre jelöljük* $Fix(g)$*-vel a* g *fixpontjainak halmazát. Ekkor*

$$\frac{1}{|G|}\sum_{g \in G} |Fix(g)| = s.$$

Bizonyítás. Számoljuk le kétféleképpen az (ω, g) párokat, ahol $\omega \in \Omega$, $g \in G$ és $\omega^g = \omega$. A bizonyítandó összefüggés bal oldalán levő szumma ezt számolja csoportelemről csoportelemre. A másik irányból egy $\omega \in \Omega$ elemre $|G_\omega|$ olyan g csoportelem van, amely ω-t fixen hagyja (G_ω-val szokás szerint a stabilizátor részcsoportot jelöljük), azaz így

$$\sum_{\omega \in \Omega} |G_\omega|$$

lesz az összeg. Ha azonban ω és ω' egy orbitban vannak, akkor a megfelelő stabilizátorok konjugáltak, így rendjük is megegyezik. Másrészt az ω orbitjának mérete a stabilizátor indexe, vagyis egy orbit adaléka a fenti szummához éppen $|G|$. Így Ω elemei szerint számolva az (ω, g) párok száma éppen $s|G|$. ∎

Tétel 1.22 *Legyen* $\mathbf{D}$ *négyzetes illeszkedési struktúra, és tegyük fel, hogy* $\mathbf{D}$ *illeszkedési mátrixa nem-szinguláris. Legyen továbbá* $G \leq Aut(\mathbf{D})$. *Ekkor* G *pont-orbitjainak száma megegyezik a blokk-orbitok számával.*

Bizonyítás. Legyen s a pont, t a blokk orbitok száma. Lemma 1.21 miatt ezek egy-egy összeggel írhatók fel, melyeknek tagjai Tétel 1.20 miatt rendre egyenlőek. ∎

A geometriai motiváció szerint haladva, az automorfizmusok után nézzük a dualitásokat, vagy más szóval a korrelációkat. Mivel a duális struktúrát fentebb már definiáltuk, a formális definíció előtt röviden azt is mondhatjuk, hogy egy korreláció nem más, mint egy illeszkedési struktúra és annak duálisa közötti izomorfizmus.

Definíció 1.23 Legyen $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ egy illeszkedési struktúra. A $\varrho : \mathbf{P} \cup \mathbf{B} \to \mathbf{P} \cup \mathbf{B}$ leképezés *korreláció*, ha bijekció és

$$\mathbf{P}^\varrho = \mathbf{B}, \quad \mathbf{B}^\varrho = \mathbf{P};$$

$$pIB \iff p^\varrho I B^\varrho, \ \ \forall p \in \mathbf{P},\ \forall B \in \mathbf{B}.$$

Ha a korreláció másodrendű, akkor *polaritás*nak hívjuk. Ha $\mathbf{D}$-nek van korrelációja, akkor *önduális*nak nevezzük.

Nézzük meg mit jelent a polaritás létezése az illeszkedési mátrixok nyelvén. Ehhez először is vegyük észre, hogy ha π polaritás, akkor

$$pIq^\pi \iff qIp^\pi \quad \forall p, q \in \mathbf{P}.$$

Ha tehát azt az illeszkedési mátrixot nézzük, amelyben az első blokk az első pont polárisa, s.í.t., akkor ez a mátrix szimmetrikus lesz. Megfordítva, ha az illeszkedési mátrix szimmetrikus, akkor az a leképezés, amely az i-edik ponthoz az i-edik blokkot rendeli, polaritás lesz. Így tehát elmondhatjuk, hogy egy illeszkedési struktúrának pontosan akkor van polaritása, ha van szimmetrikus illeszkedési mátrixa.

Két korreláció szorzata automorfizmus, egy korreláció és egy automorfizmus szorzata pedig korreláció, az azonban nem világos, hogy ha egy négyzetes illeszkedési struktúrának sok automorfizmusa van, akkor van-e polaritása vagy korrelációja. Ez általában nem is várható (pl. vannak olyan projektív síkok, amelyek nem önduálisak és viszonylag nagy az automorfizmus-csoportjuk), bizonyos esetekben azonban ez így van.

Tétel 1.24 (Marshall Hall) *Legyen* $\mathbf{D}$ *véges illeszkedési struktúra, amelynek van egy* $\Gamma \leq Aut(\mathbf{D})$ *automorfizmus-csoportja, amely mind a pontokon, mind a blokkokon regulárisan hat. Ha* Γ *Abel-féle (kommutatív) is, akkor* $\mathbf{D}$*-nek van polaritása.*

Bizonyítás. Válasszunk egy p 'alappontot'. Ekkor minden további q pont egyértelműen áll elő $q = p^\alpha$ alakban (valamilyen $\alpha \in \Gamma$ elemre). Hasonlóan válasszunk egy B 'alapblokkot' is és definiáljuk a π leképezést a következő módon:

Legyen
$$(p^\alpha)^\pi := B^{\alpha^{-1}}, \quad (B^\alpha)^\pi := p^{\alpha^{-1}}.$$

Ekkor $p^\beta \ I \ (p^\alpha)^\pi$ akkor és csak akkor, ha $p^\beta \ I \ B^{\alpha^{-1}}$. α-t alkalmazva mindkét oldalon azt kapjuk, hogy ez ekvivalens azzal, hogy $p^\alpha \ I \ p^{\beta\pi}$. Ez pedig éppen azt jelenti, hogy π polaritás. ∎

A testre épített projektív síkok eleget tesznek ennek a feltételnek (amint azt majd a differencia-halmazokról szóló fejezetben meg fogjuk látni). Persze a szokásos geometriai módon (szimmetrikus mátrixszal) is származtathatunk polaritást, vagyis ezek a síkok önduálisak. További információk $\mathrm{PG}(2,q)$ ill. általában $\mathrm{PG}(n,q)$ polaritásairól az előző alfejezetben találhatók.

2 A DE BRUIJN–ERDŐS TÉTEL ÉS KÖRNYÉKE: LINEÁRIS TEREK

Ebben a fejezetben hipergráfok egy speciális osztályával, a lineáris terekkel fogunk foglalkozni, melyek az affin és projektív síkok és terek messzemenő általánosításai.

Definíció 2.1 Az $\mathcal{L} = (V, E)$ hipergráf *lineáris tér*, ha

(i) bármely két különböző ponthoz pontosan egy olyan blokk (él) van, amely őket tartalmazza,

(ii) minden blokk (él) legalább két pontot tartalmaz,

(iii) legalább két blokk (él) van.

Ebben az esetben blokk helyett *egyenes*t mondunk majd. Talán a lineáris tér helyett is jobb lenne az "egyenestér" elnevezés. A geometriai szóhasználattal élve, nem-metsző egyenesek helyett beszélünk majd *párhuzamos* egyenesekről is. Tetszőleges V alaphalmazon megadhatunk ilyen lineáris tereket. Válasszuk ki V egy w pontját és legyenek a blokkok (egyenesek) a következők:

$$V \setminus \{w\}, \{w, x\}, \quad x \in V \setminus \{w\}.$$

Ezt a banális struktúrát *degenerált* lineáris térnek nevezzük, a későbbiekben igen gyakran kell majd kizárnunk. Említsük meg, hogy ugyanannyi pontja van, mint blokkja, azonban a struktúra nem uniform (és nem is reguláris).

Egy lineáris teret le is tudunk rajzolni, ha elég kevés pontunk van. Mivel minden pontpárt összeköt egyenes, így azokat az egyeneseket nem jelöljük, amelyek kétpontúak. A többi egyenest egy (nem feltétlenül egyenes) vonallal rajzolhatjuk le. Persze ez csak akkor ad áttekinthető ábrát, ha elég kevés ilyen egyenes van. Lássunk néhány sporadikus lineáris teret, amelyek a későbbiekben szerepelni fognak ($\mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3$):

Most lássuk, hogy milyen elemi leszámlálási egyenlőségek teljesülnek lineáris térben:

Az illeszkedő pont-egyenes párok kétféle leszámlálásával kapjuk a hipergráfokra érvényes alap-egyenlőséget (amit már az első fejezetben is láttunk, v.ö. 1.14, (1)):

$$\sum_{p\in\mathbf{P}} \deg(p) = \sum_{B\in\mathbf{B}} |B|. \tag{3}$$

Kétféleképpen leszámolva az illeszkedő pontpár-egyenes hármasokat az alábbi egyenlőséget kapjuk:

$$v(v-1) = \sum_{L\in\mathbf{B}} |L|(|L|-1). \tag{4}$$

Ha pedig egy p pontot fixálunk és a (1) egyenlőséget csak az azon átmenő blokkokra alkalmazzuk, akkor a

$$v-1 = \sum_{p\in B} (|B|-1) \tag{5}$$

egyenlőséghez jutunk. Ez szemléletesen azt tükrözi, hogy a p pont egyértelmű egyenessel össze van kötve minden további ponttal.

Még egy hasonló leszámlálási összefüggés: legyen L egy egyenes, és legyen $\mathcal{M}$ az L-et nem metsző egyenesek halmaza. Ekkor

$$\sum_{p\notin L} (\deg(p) - |L|) = \sum_{M\in\mathcal{M}} |M|. \tag{6}$$

Valóban, ez nem más, mint az (1) egyenlőség alkalmazva arra a hipergráfra, amelynek pontjai az eredeti pontok minusz L pontjai, blokkjai pedig az $\mathcal{M}$-beli egyenesek.

Most már rátérünk a de Bruijn–Erdős tétel bizonyítására. A tételnek az eredetin kívül is több bizonyítása született, melyek lényegében kétfélék, leszámláláson vagy lineáris algebrai eszközökön alapulnak. A legfrappánsabb leszámlálós bizonyítás Conwaytól ered, most ezt ismertetjük.

Tétel 2.2 (de Bruijn–Erdős) *Lineáris térben a blokkok száma legalább annyi, mint a pontok száma ($b \geq v$). Ha $b = v$, akkor a lineáris tér vagy degenerált vagy projektív sík.*

Bizonyítás 2.2 Legyen tehát $\mathcal{L} = (\mathbf{P}, \mathbf{L}, I)$ lineáris tér, melynek v pontja és b egyenese van. Feltesszük, hogy $b \leq v$ és be szeretnénk látni, hogy itt egyenlőség kell legyen. Az első észrevételt annyiszor használjuk majd a későbbiekben is, hogy külön lemmaként fogalmazzuk meg.

Lemma 2.3 *Legyen $\mathcal{L} = (\mathbf{P}, \mathbf{L}, I)$ lineáris tér, p egy az L-hez nem illeszkedő pont. Ekkor $\deg(p) \geq |L|$, és egyenlőség pontosan akkor áll, ha minden p-n átmenő egyenes metszi L-et.*

Bizonyítás. A p-t össze tudjuk kötni L minden pontjával, s az így kapott $|L|$ egyenes páronként különböző lesz. ∎

Mivel $b \leq v$ és $\deg(p) \geq |L|$ minden nem-illeszkedő (p, L) pont-egyenes párra, így

$$\frac{\deg(p)}{b - \deg(p)} \geq \frac{|L|}{v - |L|},$$

szintén minden nem-illeszkedő (p, L) pont-egyenes párra. Adjuk össze ezeket az egyenlőtlenségeket minden ilyen párra. Ha a bal oldalakat pontról pontra összeadjuk, akkor a következőt kapjuk:

$$\sum_{p\notin L} \frac{\deg(p)}{b - \deg(p)} = \sum_{p\in\mathbf{P}} \sum_{L: p\notin L} \frac{\deg(p)}{b - \deg(p)} = \sum_{p\in\mathbf{P}} \deg(p),$$

mivel minden p ponthoz pontosan $b - \deg(p)$ olyan egyenes található, amely őt nem tartalmazza. Hasonlóan, ha a jobb oldalakat egyenesről egyenesre adjuk össze, akkor azt kapjuk, hogy

$$\sum_{p\notin L} \frac{|L|}{v - |L|} = \sum_{L\in\mathbf{L}} |L|.$$

A kiindulási egyenlőtlenség miatt

$$\sum_{p\in\mathbf{P}} \deg(p) \geq \sum_{L\in\mathbf{L}} |L|,$$

itt viszont az (1) alapegyenlőség miatt egyenlőség kell legyen. Ez viszont csak úgy lehet, ha $b = v$ és valamennyi (p, L) nem-illeszkedő pont-egyenes párra $\deg(p) = |L|$. Ez azt jelenti, hogy $b = v$ esetén bármely két egyenes metszi egymást. Ha van olyan egyenes, amely két pontból áll, akkor nem nehéz belátni, hogy a lineáris terünk degenerált (ld. 2.3. Feladat). Ha viszont minden egyenes legalább három pontból áll, akkor struktúránk eleget tesz a projektív sík 1.1 szakaszbeli axiómáinak. Így a $b = v$ feltételnek eleget tevő lineáris terek a degeneráltak, valamint a projektív síkok. Ezzel a de Bruijn–Erdős tételt beláttuk. ∎

Érdemes megemlíteni, hogy a tétel eredeti megfogalmazása a duális lineáris terekre vonatkozott. Először is gondoljuk meg, hogy egy lineáris tér duálisa (mint hipergráf) egyszerű illeszkedési struktúra lesz (ld. 2.4. Feladat). Eszerint van egy alaphalmazunk (az eredeti egyenesek halmaza), vannak részhalmazaink (az egy ponton átmenő egyenesek), és bármely két részhalmaz pontosan egy elemben metszi egymást (t.i. a két pont összekötő egyenese). Ekkor legalább annyi pontunk van, mint ahány részhalmazunk. Az egyenlőség esete is könnyen dualizálható, vagy projektív síkot alkotnak a halmazok, vagy degenerált lineáris teret (hiszen ezen struktúrák duálisa is ilyen).

Most térjünk át a de Bruijn–Erdős tétel egy (jóval hosszabb) lineáris algebrai bizonyítására. Az ötlet, hogy adjacencia-mátrixokat használjunk, talán Majumdartól (1953) származik. Kezdjük két tisztán lineáris algebrai lemmával.

Lemma 2.4 *Tegyük fel, hogy C $m \times n$-es mátrix, és CC^T nem-szinguláris. Ekkor $n \geq m$.*

Bizonyítás. Indirekte tegyük fel, hogy $n < m$. Ekkor C rangja legfeljebb n, azaz a sorok összefüggők. Akkor viszont CC^T sorai is összefüggőek lennének. Ez pedig ellentmondás, hisz CC^T nem szinguláris. ∎

Lemma 2.5 *Legyen $\mathbf{A}$ $n \times n$-es mátrix és tegyük fel, hogy van az $\{1, \ldots, n\}$-nek egy $I_1 \cup I_2 \cup \ldots \cup I_t$ partíciója oly módon, hogy a mátrix eleget tesz az alábbiaknak:*

(1) $a_{jj} \neq 0$ semmilyen j-re,

(2) $a_{jk} = 0$, ha $j \neq k$ és j, k ugyanabban az I_s-ben van,

(3) $a_{jk} = 1$, különben (azaz, ha j, k a partíció különböző halmazaiban van).

Végezetül tegyük fel, hogy az $s_k = \sum_{j \in I_k} \frac{1}{a_{jj}}$ mennyiségekre $0 \leq s_k \leq 1$ teljesül és legfeljebb egy olyan k index van, amelyre $s_k = 1$.

Ekkor az $\mathbf{A}$ mátrix reguláris.

Mielőtt a bizonyításra térnénk jegyezzük meg, hogy (alkalmas permutáció után) mátrixunk a diagonális mentén elhelyezkedő négyzetes blokkokból áll. Ezen kívül csupa egyes van, a blokkok maguk olyan kis diagonális mátrixok, ahol a főátlóban csupa nem-nulla elem áll.

Bizonyítás. Azt fogjuk megmutatni, hogy az $\mathbf{Ax} = \mathbf{0}$ homogén lineáris egyenletrendszernek csak triviális megoldása van. Itt persze $\mathbf{x} = (x_1, \ldots, x_n)$ egy n hosszú ismeretlen vektor. Vezessük be az

$$y_k = \sum_{j=1}^{n} x_j - \sum_{j \in I_k} x_j, \qquad k = 1, \ldots, t$$

új ismeretleneket. Ezek segítségével az eredeti egyenletrendszer j-edik egyenlete így írható (mondjuk legyen $j \in I_h$):

$$a_{jj} x_j + \sum_{r \notin I_h} x_r = a_{jj} x_j + y_h = 0. \tag{7}$$

Ez azt jelenti, hogy $x_j = -\frac{1}{a_{jj}} y_h$, minden $j \in I_h$-ra. Adjuk össze a kapott egyenleteket. Így azt kapjuk, hogy

$$\sum_{j \in I_h} x_j = -\sum_{j \in I_h} \frac{1}{a_{jj}} y_h = -s_h y_h.$$

Ennek segítségével persze y_k-t is kifejezhetjük:

$$y_k = \sum_{h \neq k} \sum_{j \in I_h} x_j = \sum_{h \neq k} - \sum_{j \in I_h} \frac{1}{a_{jj}} y_h = \sum_{h \neq k} -s_h y_h.$$

Ez viszont újra homogén lineáris egyenletrendszer az új y_k ismeretlenekre ($k = 1, \ldots, t$), melynek mátrixa

$$\mathbf{B} = \begin{pmatrix} 1 & s_2 & s_3 & \ldots & & s_t \\ s_1 & 1 & s_3 & \ldots & & s_t \\ s_1 & s_2 & 1 & \ldots & & s_t \\ \vdots & & & \ldots & & \vdots \\ s_1 & s_2 & s_3 & \ldots & 1 & s_t \\ s_1 & s_2 & s_3 & \ldots & s_{t-1} & 1 \end{pmatrix}.$$

Azt fogjuk megmutatni, hogy ez a $\mathbf{B}$ mátrix reguláris. Ebből persze az következik, hogy az eredeti $\mathbf{Ax} = \mathbf{0}$ egyenletrendszer minden megoldásából csak $y_k = 0$ jöhet. Ekkor viszont (7) alapján valamennyi x_j is 0 kell legyen, azaz az eredeti egyenletrendszernek csak triviális megoldása lehet.

$\mathbf{B}$ regularitása a mátrix méretére vonatkozó indukcióval azonnal következik, ha valamelyik $s_k = 0$, így feltehetjük, hogy minden $s_k > 0$. Nézzük először azt az esetet, amikor valamelyik s_k (mondjuk s_1) pontosan 1. Ekkor az első oszlopban csupa egyes áll. Ha $\mathbf{B}$ első sorát rendre levonjuk a többiből, akkor az első sor megmarad, a második sortól kezdve viszont csak a diagonális elem lesz nem-nulla. Ez éppen $1 - s_k$ lesz a k-adik sorban. Így $\mathbf{B}$ determinánsa (az első oszlop szerint kifejtve) $1(1-s_2)(1-s_3)\ldots(1-s_t)$ lesz, ami a feltétel miatt nem zérus.

Ha nincs olyan k, amelyre $s_k = 1$, akkor egy tanulságos trükköt alkalmazhatunk. Osszuk el a mátrix oszlopait rendre $s_1, \ldots s_t$-vel. Ekkor olyan mátrixot kapunk, amelyben a főátlón kívüli elemek egyesek, a főátlóban pedig egynél nagyobb elemek vannak (azaz, ez a mátrix is teljesíti a lemma feltételeit, ha a partíció elemei egyeleműek!). Egy ilyen mátrix viszont előáll, mint a csupa egyesből álló $\mathbf{J}$ mátrix és egy diagonális $\mathbf{D}$ mátrix összege. A $\mathbf{J}$ szimmetrikus mátrix pozitív szemidefinit (az $(x_1 + \ldots + x_t)^2$ kvadratikus alaknak felel meg), míg a diagonális $\mathbf{D}$ mátrix pozitív definit (hiszen a főátlóban álló elemek pozitívak). Így e két mátrix összege, azaz $\mathbf{B}$ is pozitív definit, tehát reguláris. (A $\mathbf{B}$ regularitása egy másik gyakran hasznos trükkel, az ú. n. "bordering trick"-kel is igazolható, ld. a 2.5. Feladatot.)

Ezzel a Lemmát beláttuk. ∎

Állítás 2.6 *Legyen q az $\mathbf{L}$ lineáris tér egy pontja, és jelöljük $L_1, \ldots, L_r$-rel a q-n átmenő egyeneseket ($r = deg(q)$). A sorrendet válasszuk úgy, hogy $|L_j| \leq |L_r|$ teljesüljön minden j-re. Vezessük be az*

$$S_k = \sum_{q \neq p \in L_k} \frac{1}{\deg(p) - 1}$$

mennyiséget és jelöljük w-vel azon $j < r$ indexek számát, melyekre $S_j \neq 1$. Ekkor:

(i) Ha $j < r$, akkor $0 < S_j \leq 1$. Ráadásul, S_j pontosan akkor 1, ha $|L_j| = |L_r|$ továbbá $deg(p) = |L_r|$ minden q-tól különböző $p \in L_j$ pontra.

(ii) $b \geq v + w - 1$.

(iii) Ha $w \leq r - 2$ vagy ha $w = r - 1$ és $S_r \leq 1$, akkor $b \geq v + w$.

Bizonyítás. Először is, $S_j > 0$ triviális. Másrészt, ha $j < r$, akkor L_j minden pontjának foka legalább $|L_r|$ a 2.3 Lemma miatt. Így az S_j-t megadó összeg minden tagja legfeljebb $1/(|L_r| - 1)$ és az összegnek $|L_j| - 1 \leq |L_r| - 1$ tagja van. Ebből azonnal látszik $S_j \leq 1$, sőt az egyenlőségre vonatkozó feltétel is.

A tétel (ii) és (iii) részének bizonyításához természetesen választhatjuk úgy az indexelést, hogy $S_k < 1$ legyen, ha $k \leq w$. (Akkor persze $S_k = 1$, ha $w < k < r$.) Tekintsük azt az $\mathcal{L}'$ hipergráfot, amely $\mathcal{L}$-ből a q pont, valamint az $L_1, \ldots L_{w+1}$ élek (egyenesek) törlésével kapható. Ez már nem lineáris tér, a kitörölt egyenesekbe tartozó pontok összekötetlenek. Legyen M ennek a hipergráfnak a pont-blokk illeszkedési mátrixa (azaz v sorunk és $b - w - 1$ oszlopunk van). Képezzük a struktúra adjacencia-mátrixát, az $A = MM^T$ mátrixot.

Belátjuk, hogy ez a mátrix eleget tesz az előző lemma feltételeinek. Az első 'négyzetes blokkot' éppen $L_1 \setminus \{q\}$ pontjai alkotják, majd hasonlóan találunk $w + 1$ blokkot. Végül az $L_1 \cup \ldots \cup L_{w+1}$-ben nem levő pontoknak megfelelő egypontú négyzetes blokkok következnek. Lássuk például azt, hogy a négyzetes blokkokon kívüli elemek 1-ek. Ehhez azt kell észrevennünk, hogy egy ilyen mező azt számolja, hogy a sorának ill. oszlopának megfelelő pontokon hány egyenes megy át. Ha ez a mező a négyzetes blokkokon kívül van, akkor ez két olyan pontnak felel meg, amelyek nincsenek ugyanazon L_j egyenesen ($j \leq w + 1$), így az eredeti $\mathcal{L}$-beli (egyértelmű) összekötő egyenesük a törlés után is megmarad. Hasonlóan látszik az is, hogy a négyzetes blokkokon belüli, de főátlón kívüli elemek nullák, hisz az $\mathcal{L}$-beli összekötő egyenest töröltük. A főátlóban a pontok $\mathcal{L}'$-beli foka áll, ami az $\mathcal{L}$-beli fokszám mínusz 1 azokra a pontokra, amelyek valamely L_j-ben vannak, és az $\mathcal{L}$-beli fokszám a további pontokra. Ez azt is jelenti, hogy a lineáris algebrai 2.5 Lemmában szereplő s_k mennyiség azonos az ezen tételben bevezetett S_k-val, ha $k \leq w + 1$. A fennmaradó egypontú blokkokra pedig s_k a fokszám reciproka, így pozitív és legfeljebb $1/2$.

Summa summárum, az adjacencia-mátrix nem-szinguláris, amiből a 2.4 Lemma szerint következik, hogy M-nek legalább annyi oszlopa van, mint sora, vagyis $b - w - 1 \geq v - 1$.

A $w = r - 1$ esetben megismételhetjük a fenti okoskodást, ha $S_r \leq 1$. Ha viszont $S_r > 1$, akkor csak w egyenest hagyhatunk el. ∎

2. bizonyítás a de Bruijn–Erdős tételre. Az előző lemmából azonnal következik, hogy $b \geq v$, tehát csak a $b = v$-nek eleget tevő lineáris tereket kell vizsgálnunk. A 2.3. Feladat szerint a lineáris tér degenerált, ha van két pontú egyenes.

Válasszunk egy tetszőleges q pontot. Ennek $\deg(q) = r$ foka a 2.3 Lemma miatt legalább három. A 2.5 Lemma szerint $w = 0$ kell legyen, akkor viszont a lemma első része szerint minden a q ponton átmenő egyenes egyforma méretű, mondjuk x pontú. Eszerint akármelyik egyenest választhatjuk L_r-nek. Megint 2.5 (i) miatt az következik, hogy minden q-tól különböző pont foka x. Mivel a q tetszőleges volt, így minden pont foka és minden egyenes mérete x kell legyen. Ebből 2.3 szerint következik, hogy minden egyenes metszi egymást. Mivel $x \geq 3$, a lineáris tér $(x - 1)$-edrendű projektív sík. ∎

A továbbiakban célunk a de Bruijn–Erdős tétel javítása lesz. A de Bruijn–Erdős egyenlőtlenség csak akkor éles, ha a pontok száma $v = n^2 + n + 1$ alakú. Ha v nem ilyen, akkor szorítsuk be két szomszédos ilyen alakú szám közé, azaz legyen $n^2 - n + 2 \leq v \leq n^2 + n + 1$. Azt szeretnénk belátni, hogy tetszőleges nem-degenerált lineáris térben legalább annyi egyenes van, mint ahány egy ugyanannyi pontú, de az n-edrendű projektív síkból néhány pont törlésével kapható lineáris térben. Ha tehát egy pontot törlünk, vagy általában n-nél kevesebbet, akkor a blokkok száma $n^2 + n + 1$ marad. Ha legalább n pontot törlünk, akkor elképzelhető, hogy egy egyenest egy pontja híján kitöröltünk, így mivel lineáris térben nincsenek egy pontú egyenesek, az egyenesek száma eggyel csökken. Hasonlóan, amíg kevesebb, mint $2n - 1$ pontot töröltünk, addig nem tudtunk egy második egyenest egy pontúvá tenni, így továbbra is legalább $n^2 + n$ egyenesünk maradt. Alkalmasan törölve $2n - 1$ pontot viszont elképzelhető, hogy két egyenest is kitöröltünk, azaz ekkor csak $b \geq n^2 + n - 1$-et várhatunk.

A következő lemma alsó becslést ad egy lineáris tér egyeneseinek számára.

Lemma 2.7 (Stanton–Kalbfleisch, 1972) *Legyen $\mathbf{L}$ lineáris tér, L egy egyenese. Tegyük fel, hogy $\mathbf{L}$-nek v pontja, b egyenese van és $|L| = k$. Ekkor*

$$b \geq 1 + \frac{k^2(v - k)}{v - 1},$$

és egyenlőség pontosan akkor áll, ha L metsz minden egyenest és minden L-től különböző egyenes mérete ugyanaz a k', ahol ráadásul $k(k' - 1) = v - 1$.

Mielőtt a bizonyításra térnénk vezessünk be egy jelölést: legyen $f(k,v) = 1 + \frac{k^2(v-k)}{v-1}$.

Bizonyítás. A bizonyításhoz egy tipikus leszámlálási trükköt használunk, a "variancia-trükköt" (szokás a módszert "kvadratikus leszámolásnak" is nevezni, ld. még a 2.6. Feladatot).

Legyen $\mathcal{M}$ az L-et metsző egyenesek halmaza, valamint legyen $|\mathcal{M}| = m$. Ekkor

$$\sum_{M\in\mathcal{M}} 1 = m, \quad \sum_{M\in\mathcal{M}} (|M|-1) = k(v-k),$$

$$\sum_{M\in\mathcal{M}} (|M|-1)(|M|-2) \le (v-k)(v-k-1).$$

A második egyenlőség az olyan (p,M) zászlók leszámolásával adódik, ahol $p \notin L$, $M \in \mathcal{M}$, míg az utolsó egyenlőtlenség a (p,q,M) hármasokéból, ahol $p \ne q \notin L$, $M \in \mathcal{M}$. Ezek az összefüggések lehetővé teszik, hogy $|M|$-nek tetszőleges másodfokú kifejezését előállítsuk segítségükkel. Például

$$\sum_{M\in\mathcal{M}} |M| = k(v-k) + m,$$

$$\sum_{M\in\mathcal{M}} |M|^2 \le (v-k)(v+2k) + m.$$

Ezekből a számtani és kvadratikus közép közti egyenlőtlenség (vagy akinek jobb tetszik, a Cauchy–Bunyakovszkij–Schwarz egyenlőtlenség) alkalmazásával az következik, hogy

$$\left(\sum_{M\in\mathcal{M}} |M|\right)^2 \le m\left(\sum_{M\in\mathcal{M}} |M|^2\right).$$

Ebből $(k(v-k)+m)^2 \le m((v-k)(v+2k)+m)$ adódik, azaz valóban $m \ge \frac{k^2(v-k)}{v-1}$. A b-re vonatkozó egyenlőség egyszerűen azért következik, mert $b \ge m+1$. Ha $b = f(k,v)$, akkor a számtani–kvadratikus közép közti egyenlőtlenségben is egyenlőség kell álljon, vagyis minden $M \in \mathcal{M}$-re $|M| = k'$ kell legyen. Végül, ha $p \notin L$, akkor minden p-n átmenő egyenes metszi L-et, így $\deg(p) = k$, és a szokásos módon (5) alkalmazásával kapjuk, hogy $v - 1 = k(k'-1)$. ∎

Hogy kicsit pontosabb képünk legyen az $f(k,v)$ függvényről, vizsgáljuk meg menetét mindkét változója szerint. v szerint $f(k,v)$ monoton csökken, míg k szerint a $[2,v]$ intervallumon a függvény nő $k = 2v/3$-ig, csökken $k = v$-ig. Ez azt jelenti, hogy k szerint akármilyen részintervallumát is vesszük a $[2,v]$-nek, azon a legkisebb értéket $f(k,v)$ az intervallum valamelyik végpontjában veszi fel. Ezt az észrevételt fogjuk felhasználni a következő lemmában.

Lemma 2.8 *Legyen $\mathcal{L} = (\mathbf{P},\mathbf{L},\in)$ nem-degenerált lineáris tér, melyre $v \ge n^2-n+2$ és $b \le n^2+n+1$ valamely $n \ge 2$ természetes számra. Legyen továbbá k a legnagyobb egyenes mérete, azaz $k = \max_L |L|$. Ha $k > n+1$, akkor $\mathcal{L}$ az $\mathbf{E}_2$ és $\mathbf{E}_3$ lineáris terek valamelyike.*

Bizonyítás. Mivel $\mathbf{L}$ nem-degenerált, $3 \le k \le v-2$. Az $f(k,v)$ függvény Lemma előtt említett tulajdonságaiból következik, hogy $f(k,v) \ge \min\{f(n+2,v), f(v-2,v)\}$. A v-re és b-re tett kikötések miatt az $f(v-2,v)$ érték nem jön szóba, így $b \ge f(n+2,v)$. Mivel $v \ge n^2-n+2$ és $f(k,v)$ v-ben monoton csökken, kapjuk, hogy

$$n^2+n+1 \ge b \ge f(n+2,n^2-n+2) = n^2+n+1+\frac{2n^3-4n^2-9n}{n^2-n+1},$$

amiből rögtön adódik, hogy $n \le 3$. Könnyű azt is belátni (ld. 2.7. Feladat), hogy $n = 3$ és $k = 5$ vagy 6, amiből $v = 8$ következik. Azt se nehéz ellenőrizni, hogy $\mathcal{L} = \mathbf{E}_2$, ha $k = 6$, valamint $\mathcal{L} = \mathbf{E}_3$, ha $k = 5$. ∎

A következő tétel lesz főtételünk. Mielőtt kimondanánk, vezessük be az alábbi $B(v)$ függvényt (amelyet a de Bruijn–Erdős tétel élesítésének motivációjakor már említettünk):

Szorítsuk v-t az $(n-1)^2+(n-1)+1$ és n^2+n+1 értékek közé (valamely n természetes számra) és legyen

$$B(v) = \begin{cases} n^2+n-1, & \text{ha } v = n^2-n+2 \text{ és } v \ne 4,\\ n^2+n, & \text{ha } n^2-n+3 \le v \le n^2+1 \text{ vagy } v = 4,\\ n^2+n+1, & \text{ha } n^2+2 \le v.\end{cases}$$

Tétel 2.9 (Erdős, Mullin, T. Sós, Stinson, 1983) *Nem-degenerált lineáris térre $b \ge B(v)$.*

Bizonyítás. A szokásos módon legyen $n^2-n+2 \le v \le n^2+n+1$ és jelöljük k-val a maximális egyenes-méretet. A 2.8 Lemma miatt feltehetjük, hogy $k \le n+1$. Mivel $v \ge n^2-n+2$, így ebből következik, hogy minden pont foka legalább n.

A bizonyítás esetszétválasztással történik.

1. eset: $k = n+1$.

Legyen L egy $n+1$ pontból álló egyenes. Ha L minden pontjának foka $n+1$, akkor már az L-et metsző egyeneseket számolva látunk $(n+1)(n+1-1)+1$ egyenest, így ekkor $b \ge B(v)$.

Feltehetjük tehát, hogy L-en van olyan p pont, amelynek foka n. Jegyezzük meg, hogy ekkor $v-1 \le \deg(p)n$, azaz $v \le n^2+1$.

Két alesetet különböztetünk meg.

1.a aleset: Létezik egy $H \neq L$ egyenes p-n, amely szintén $n+1$ pontú. Ekkor a 2.3 Lemma miatt L minden p-től különböző pontjának foka legalább $|H| = n+1$. Tehát a blokkok száma $b \geq n^2+n$, míg $v \leq n^2+1$, azaz ekkor is fennáll $b \geq B(v)$.

1.b aleset: L az egyetlen p-n átmenő $n+1$ pontú egyenes. Ekkor $v \leq n+1+(n-1)(n-1) = n^2-n+2$. A kiindulási egyenlőtlenség miatt itt egyenlőség kell álljon, azaz a további p-n átmenő egyenesek mind n pontúak. Feltehető, hogy $n \neq 2$, mert akkor $v=4$ és $k=3$ miatt a lineáris tér degenerált lenne. Soroljuk fel a p-n átmenő egyeneseket: $L = R_1, R_2, \ldots, R_n$. Ha $p \neq q \in R_2 \cup R_3$, akkor q foka 2.3 miatt legalább $n+1(=|L|)$. Így az R_2-t és R_3 valamelyikét metsző egyenesek száma legalább $n+(n-1)(n-1)+2(n-1) = n+n^2-1 = B(v)$, amit bizonyítani akartunk. Az előző összeszámláláskor az első tag a p-n átmenő egyenesek száma, a második a mind R_2-t, mind R_3-at metsző egyenesek száma, végül a harmadik tag az R_i-t metsző, R_j-t nem metsző egyenesek száma ($\{i,j\} = \{2,3\}$).

2. eset: $k = n$. Ekkor a $v-1 \leq \deg(p)(n-1)$ összefüggésből adódik, hogy $\deg(p) \geq n+1$ minden pontra. Így egy n pontú N egyenes n^2 további egyenest metsz, vagyis $b \geq n^2+1+c$, ahol c az N-et nem metsző egyenesek számát jelöli. Mivel minden pont foka legalább $n+1$, minden ponton át megy N-et nem metsző egyenes. Kétféleképpen megszámolva a (p, M) párokat, ahol $p \notin N$, $N \cap M = \emptyset$, kapjuk, hogy $cn \geq v-n$. Ezt $b = n^2+1+c$-vel összevetve $b \geq B(v)$ adódik.

3. eset: $k \leq n-1$.

Ebben az esetben is tudjuk, hogy minden pont foka legalább $n+1$ (ugyanúgy, mint a 2. esetben). Eszerint $v(n+1) \leq b(n-1)$ ((1) miatt), vagyis $b \geq n^2+n+1 \geq B(v)$. ∎

Fontos megjegyezni, hogy az Erdős, Mullin, T. Sós, Stinson tétel jelentősen javít a de Bruijn–Erdős tétel egyenlőtlenség részén, de a "teljes" általánosítás az volna, hogy egy v pontú $B(v)$ egyenesű lineáris tér mindig megkapható projektív síkból néhány pont és a két pontnál kevesebb pontot tartalmazó egyenesek törlésével. (Más szóval: egy ilyen lineáris tér *beágyazható* projektív síkba.) Ezt a módosítást nemrégiben Klaus Metsch látta be: egyetlen kivétel van, az $\mathbf{E}_1$ lineáris tér.

Jegyezzük meg azt is, hogy a tétel semmit nem állít abban az esetben, ha $v = n^2+n+1$, de nem létezik n-edrendű projektív sík. Persze a Metsch-féle kombinatorikus beágyazási tétel ekkor kettővel megjavítja a de Bruijn–Erdős tételben szereplő korlátot.

Hasonló ízű eredmény több is van: Bridges 1972 jellemezte azokat a lineáris tereket, amelyekre $b = v+1$. Ezt többen továbbfejlesztették, majd Totten 1976-ban jellemezte azokat a lineáris tereket, amelyekre $(b-v)^2 \leq b$. Hanani (1954-55) és Varga (1985) belátta, hogy azok a lineáris terek, amelyben minden maximális méretű egyenes legalább $v-1$ további egyenest metsz, pontosan

a degeneráltak és a projektív síkok. Végül említsük meg a Dowling–Wilson sejtést, amelyet nemrégen Metsch bizonyított: Ha egy adott ponton át egy egyenessel t párhuzamos egyenes van, akkor $b \geq v+t$.

A fejezet hátralevő részében azzal fogunk foglalkozni, hogy érzékeltessük a fentebb említett beágyazási tételek bizonyítását, legalábbis abban az esetben, ha minden pont foka $n+1$.

Definíció 2.10 Ha egy lineáris tér $(n+1)$-reguláris, akkor $(n+1,1)$-*rendszer*nek nevezzük. Minden egyenesre jelöljük d_L-lel az $n+1-|L|$ differenciát. (Jegyezzük meg, hogy a regularitást megkönnyítendő, az $(n+1,1)$-rendszer definíciójában szokás megengedni egypontú egyeneseket is, sőt azok lehetnek többszörösek is, mi azonban ezt nem tesszük.)

Lemma 2.11 *Legyen* $\mathbf{D}$ $(n+1,1)$*-rendszer; a pontok számát jelölje* $v = n^2+n+1-s$*, az egyeneseket pedig* $b = n^2+n+1+z$*. Ekkor*

(i) Egy rögzített L *egyenessel párhuzamos egyenesek száma* $d_L n + z$*.*

(ii) Két egyenessel, L*-lel és* H*-val párhuzamos egyenesek száma* $d_H d_L + z$*, ha* H *és* L *metszők,* $n-1+(d_H-1)(d_L-1)+z$*, ha* H *és* L *párhuzamos.*

(iii) Ha $\mathcal{M}$ *jelöli egy adott* L *egyenessel párhuzamos egyenesek halmazát, akkor*

$$(v-|L|)d_L = \sum_{X \in \mathcal{M}} |X|.$$

A bizonyítás olyan egyszerű, hogy feladatnak hagyjuk (ld. 2.8. Feladat). ∎

Lemma 2.12 *Legyen* $\mathbf{D} = (\mathbf{P}, \mathbf{L})$ $(n+1,1)$*-rendszer; a pontok számát jelölje* $v = n^2+n+1-s$*, az egyeneseket pedig* $b = n^2+n+1+z$*. Ekkor*

$$\sum_{L \in \mathbf{L}} d_L = (s+z)(n+1) \quad \text{és} \quad \sum_{L \in \mathbf{L}} {d_L}^2 = s(n+s)+(n+1)^2 z.$$

A bizonyítást ld. a 2.9. Feladatban (csak (1)-t és (4)-et kell használni). ∎

Lemma 2.13 *Legyen* $\mathbf{D} = (\mathbf{P}, \mathbf{L})$ $(n+1,1)$*-rendszer; a pontok számát jelölje* $v = n^2+n+1-s$*, az egyeneseket pedig* $b = n^2+n+1$*. Ekkor*

(i) Az n *pontú egyenesek* b_n *számára* $b_n \geq s(n+2-s)$ *teljesül. Ha speciálisan* $n^2+1 \leq v \leq n^2+n-1$*, akkor* $b_n \geq 2n$*.*

(ii) Ha nincs n *pontú egyenes, akkor*

$$\sum_L |L|(|L|-2) = s(s-2-n).$$

A bizonyítást ld. a 2.10. Feladatban. ∎

A most következő eredmény arról szól, hogy bizonyos lineáris tereket be lehet ágyazni projektív síkba.

Tétel 2.14 *Tegyük fel, hogy egy* $\mathbf{D} = (\mathbf{P}, \mathbf{L})$ $(n+1,1)$*-rendszernek* v *pontja,* n^2+n+1 *egyenese van, továbbá találunk benne* t *páronként metsző* n *pontú egyenest. Ekkor* $\mathbf{D}$ *beágyazható egy* $v+t$ *pontú (és továbbra is* n^2+n+1 *egyenesű)* $(n+1,1)$*-rendszerbe.*

Bizonyítás. Legyenek $N_1, \ldots, N_t$ a tételben említett páronként metsző n pontú egyenesek. Mivel minden pont foka $n+1$, minden N_j-n nem levő ponton pontosan egy N_j-vel párhuzamos egyenes megy át. Legyen $\Pi_j = \{N_j\} \cup \{L : L \cap N_j = \emptyset\}$ $(j = 1 \ldots, t)$; szemléletesen Π_j az N_j "párhuzamossági osztálya". 2.11 (i) szerint $|\Pi_j| = n+1$. Ha $j \neq k$, akkor N_j és N_k metszi egymást, továbbá $|N_j| = n$ miatt N_j pontosan n egyenesét metszi Π_k-nak. Van tehát egy (és csak egy) olyan Π_k-beli egyenes, amely nem metszi N_j-t. Más szavakkal ez azt jelenti, hogy $|N_j \cap N_k| = 1$. Az affin sík projektívvá bővítését fogjuk imitálni, azaz minden Π_j párhuzamossági osztályhoz hozzárendelünk egy ∞_j "ideális pontot" (ez csak annyit jelent, hogy ∞_j nem pontja $\mathbf{P}$-nek). Precízebben, legyenek az $\infty_j \notin \mathbf{P}$ szimbólumok páronként különbözőek, és definiáljunk egy új $\mathbf{D}'$ illeszkedési struktúrát a következőképpen:

(a) $\mathbf{D}' = (\mathbf{P} \cup \{\infty_1, \ldots, \infty_t\}, \mathbf{L}, I)$, ahol

(b) $p \in \mathbf{P}$, $L \in \mathbf{L}$ esetén $p\ I\ L$ akkor és csak akkor ha $p \in L$ (megtartjuk a $\mathbf{D}$-beli illeszkedést),

(c) $L \in \mathbf{L}$-re legyen $\infty_j\ I\ L$ pontosan akkor, ha $L \in \Pi_j$.

Esetszétválasztással könnyen ellenőrizhető (ld. a 2.11. Feladatot), hogy $\mathbf{D}'$-ben bármely két ponton egy és csak egy egyenes megy át, és persze $\mathbf{D}'$ $v+t$ pontú. ∎

Korollárium 2.15 (Vanstone, 1973) *Ha egy* $\mathbf{D}$ $(n+1,1)$*-rendszernek* n^2+n+1 *egyenese van és a pontok száma* $v \geq n^2$*, akkor* $\mathbf{D}$ *beágyazható* n*-edrendű projektív síkba.*

Bizonyítás. $s = n^2+n+1-v$-re vonatkozó indukciót alkalmazunk. Ha $s = 0$, akkor 2.11 szerint minden egyenes $n+1$ pontú, azaz $\mathbf{D}$ maga projektív sík.

Tegyük fel, hogy $s > 0$. 2.11 (i) mutatja, hogy létezik N egyenes, melynek n pontja van. 2.14 szerint ilyenkor tudjuk bővíteni $\mathbf{D}$-t ($t \geq 1$ ponttal, ahol t a páronként metsző egyenesek maximális száma). Ilyenkor viszont s csökken, azaz a bővített struktúra n-edrendű projektív síkba ágyazható. ∎

2.1 Feladatok

2.1., *(Transfer-lemma)* Legyen $\mathcal{L} = (\mathbf{P}, \mathbf{L}, I)$ lineáris tér.

Tegyük fel, hogy L és L' egyenesek, p pedig olyan pont, amely sem L-en, sem L'-n nincs rajta. Legyen t azon egyenesek száma, amelyek átmennek p-n, metszik L-et de nem metszik L'-t. Ekkor azon p-n átmenő egyenesek száma, amelyek L'-t metszik, de L-et nem, $t + |L'| - |L|$.

Ha most H, L és L' egyenesek úgy, hogy H metszi L-et, de nem metszi L'-t, akkor legalább $(|H|-1)(1+|L'|-|L|)$ olyan egyenes van, amely H-t és L'-t metszi, de nem metszi L-et.

2.2., *(Parallel-lemma)* Legyen $\mathcal{L} = (\mathbf{P}, \mathbf{L}, I)$ lineáris tér. Legyen továbbá N egy n-pontú egyenes, valamint L_1, L_2 olyan metsző egyenesek, amelyek nem metszik N-et. Legyen $|L_j| = n + 1 - d_j$ ($j = 1, 2$-re), valamint $t = \sum_{p \in N}(\deg(p) - n - 1)$. Ekkor

$$d_1 d_2 \geq n - t.$$

2.3., Ha egy lineáris térben $b = v$ és van két pontú egyenes, akkor az degenerált.

2.4., Fogalmazzuk meg (és bizonyítsuk) a de Bruijn–Erdős tétel duálisát!

2.5., Legyen $B = \lambda J_n + \mathrm{diag}(\gamma_1, \ldots, \gamma_n)$. (Persze J_n az $n \times n$-es csupa 1 mátrix.) Szegélyezzük ezt a mátrixot egy csupa 1-es első sorral és egy az első elemet kivéve csupa 0 első oszloppal. Ezt könnyen triangulárissá alakíthatjuk, így B determinánsa

$$\gamma_1 \ldots \gamma_n \left(1 + \lambda(\frac{1}{\gamma_1} + \ldots \frac{1}{\gamma_n})\right)$$

lesz (ezt szokás "bordering trick"-nek hívni.)

2.6., Egy projektív sík pontjait két színnel színeztük. Egy E egyenesre legyen p_E ill. k_E az első (piros) ill. a második (kék) pontok száma. Mutassuk meg, hogy $\sum_E (p_E - k_E)^2$ csak a színosztályok számától függ (attól, hogy hogyan színeztünk nem)!

2.7., Vizsgáljuk meg az $n \leq 3$ eseteket a 2.8 Lemma bizonyításában!

2.8., Bizonyítsuk be a 2.10 lemmát!

2.9., Bizonyítsuk be a 2.11 lemmát!

2.10., Bizonyítsuk be a 2.12 lemmát!

2.11., Ellenőrizzük, hogy a 2.13 tétel bizonyításában szereplő $\mathbf{D}'$ illeszkedési struktúrában bármely két ponton egy és csak egy egyenes megy át!

3 BLOKKRENDSZEREK

Ebben a szakaszban kezdjük igazán a szimmetrikus struktúrák tárgyalását.

Definíció 3.1 A $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ hipergráfot *blokkrendszer*nek vagy pontosabban *2-(v,k,λ)-blokkrendszer*nek nevezzük, ha v pontja van ($|\mathbf{P}| = v$), k-uniform (azaz $\forall B \in \mathbf{B}: \ |B| = k$), továbbá bármely két különböző pont λ blokkban (élben) van benne. 2-(v,k,λ)-blokkrendszer helyett gyakran csak *(v,k,λ)-rendszert* mondunk és írunk. Abban a speciális esetben, ha $\lambda = 1$, a blokkrendszert szokás *Steiner-rendszer*nek is nevezni. Tehát a Steiner-rendszerek nem mások, mint az uniform lineáris terek.

Abban az esetben, ha a $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ illeszkedési struktúra tartalmaz többszörös éleket, de a másik két feltételt teljesíti (minden blokkhoz k pont, minden pontpárhoz λ blokk illeszkedik), akkor *(uniform) 2-(v,k,λ)-struktúrá*ról beszélünk. Ha az uniformitási feltétel sem teljesül, de minden pontpárra λ blokk illeszkedik, akkor egyszerűen csak *2-struktúrá*ról beszélünk.

A most bevezetett osztályok közötti kapcsolatra a következő szakaszban, a Fisher-egyenlőtlenség tárgyalásakor még visszatérünk.

A blokkrendszerek nemcsak uniformak, hanem regulárisak is, amint azt a következő állítás mutatja.

Állítás 3.2 *(v,k,λ)-rendszerben (sőt (v,k,λ)-struktúrában) minden pont foka r, ahol*

$$r = \lambda(v-1)/(k-1),$$

a blokkok száma pedig

$$b = \lambda v(v-1)/k(k-1).$$

Bizonyítás. Rögzítsünk egy p pontot. Számoljuk meg kétféleképpen azokat a (q, L) zászlókat, amelyekben $p \in L$. Ez egyrészt $\deg(p)(k-1)$, másrészt (pontról pontra számolva) $(v-1)\lambda$. Ebből az r-re vonatkozó állítás azonnal, a b-re vonatkozó pedig a $bk = vr$ (ld. 1.15) felhasználásával adódik. ∎

Korollárium 3.3 *A (v,k,λ)-rendszerek létezéséhez szükséges, hogy*

$$\begin{aligned} &(1) \quad \lambda(v-1) \equiv 0 \pmod{k-1};\\ &(2) \quad \lambda v(v-1) \equiv 0 \pmod{k(k-1)}. \ ∎ \end{aligned}$$

Természetesen az alapvető kérdés az, hogy ezek a feltételek elégségesek-e a megfelelő paraméterű blokkrendszerek létezéséhez. Mint később látni fogjuk, a válasz nemleges. Akkor viszont az az érdekes, hogy lehet-e találni további feltételeket úgy, hogy azokkal együtt a 3.3-beli feltételek már elégségesek legyenek. További feltételek vannak, az elégségességtől azonban messze vagyunk. Időrendben először a $k = 3$ esetet vizsgálták részletesen. 1850-ben Kirkman vetette fel (és oldotta meg még abban az évben) az alábbi problémát:

15 iskoláslány egy hétig minden nap sétálni megy. Egy sorban hárman mennek. Tervezzünk olyan sétarendet, amelyben semelyik két lány nem sétál egy sorban kétszer.

Matematikai nyelven ez a következőt jelenti: 15 elemen adjunk meg $35 = 7 \cdot 5$ hármast úgy, hogy bármely két elem legfeljebb egy hármasban legyen benne. Könnyen látható (ld. 3.1. Feladat), hogy amiatt, hogy 35 hármast adtunk meg, bármely két elem pontosan egy hármasban van benne. A fenti terminológia szerint tehát a sétarend egy $(15,3,1)$-rendszert ad meg. Ez tehát egy $k = 3$ blokkméretű Steiner-rendszer. A Kirkman problémában szereplő sétarendnek azonban van még egy tulajdonsága. Egy-egy napon a sorok (azaz a blokkok) páronként diszjunktak és lefedik a pontokat. Ez valami olyasmi, mint a geometriában a párhuzamosság. Erre a kérdéskörre később még visszatérünk. Most lássuk a Kirkman probléma egy szép (ciklikus) megoldását:

Jegyezzük meg, hogy a Kirkman problémának 6 megoldása van, ha azonos hármasrendszereket különböző párhuzamossággal különbözőnek tekintünk. Ha csupán a hármasrendszereket nézzük, akkor 4 különböző van. Említsük meg, hogy 15 ponton összesen 80 hármasrendszer van.

Térjünk rá a $k = 3$ eset vizsgálatára (a párhuzamosság extra követelménye nélkül). A $(v,3,1)$-rendszereket szokták Steiner hármasrendszereknek is nevezni. A rövidség kedvéért a v pontú Steiner hármasrendszereket STS(v)-vel fogjuk jelölni. A 3.3-as Következmény azt mondja, hogy $2|v-1$ és $6|v(v-1)$ szükséges feltétel a létezéshez. Magyarul Steiner hármasrendszerek csak $v \equiv 1$ vagy $v \equiv 3 \pmod 6$ esetén létezhetnek. Célunk az lesz, hogy néhány konstrukció segítségével megmutassuk, hogy minden $v \equiv 1$ vagy $v \equiv 3 \pmod 6$ esetén léteznek Steiner hármasrendszerek.

Konstrukció 3.4. (Kirkman $v \to 2v+1$ konstrukció) Ez egy rekurzív konstrukció lesz. Azt mutatjuk meg, hogy ha létezik egy T STS(v), akkor létezik STS($2v+1$) is. Ráadásul ez olyan lesz, amelyben a kiindulási STS(v)-t részrendszerként megtaláljuk. Legyen T ponthalmaza $\{1,\dots,v\}$. Válasszunk $v+1$ további pontot $\{v+1,\dots 2v+1\}$-et. Tekintsük a K_{v+1} teljes gráfot, és bontsuk fel v darab 1-faktor egyesítésére. Minden ilyen 1-faktorhoz rendeljük hozzá T valamelyik pontját, és ezt a hozzárendelt pontot vegyük hozzá az 1-faktorban szereplő minden párhoz. Ezenkívül tartsuk meg T blokkjait. Szinte magától értetődő, hogy így Steiner hármasrendszert kapunk (ld. a 3.2. Feladatot, valamint a 3.3,4 Feladatokat).

A Fano-síkból kiindulva így éppen egy 15 pontú Steiner-rendszert kapunk. A Kirkman-konstrukció azonban kevés ahhoz, hogy minden $v \equiv 1$ vagy 3 (mod 6)-ra konstruáljunk annyi ponton STS-et. Ismerjünk meg egy további elemi eljárást.

Konstrukció 3.5. (Skolem módszere) Ezt először a $v = 6m+1$ esetben mondjuk el. Ekkor 3.2 miatt a hármasok (blokkok) száma $b = m(6m+1)$. Legyenek a pontok: $0, 1, \dots, 6m$. Hogy a konstrukciót könnyebb legyen elmondani, a pontokat egy kivétellel mátrix alakba rendezzük:

$$\begin{array}{cccc|cccc} 0 & 1 & \dots & m-1 & m & m+1 & \dots & 2m-1 \\ 2m & 2m+1 & \dots & 3m-1 & 3m & 3m+1 & \dots & 4m-1 \\ 4m & 4m+1 & \dots & 5m-1 & 5m & 5m+1 & \dots & 6m-1 \end{array}$$

A blokkok három típusba oszthatók:

(i) $\{i, 2m+i, 4m+i\}$, ahol $0 \le i \le m-1$

(ii) $\{m+i, 2m+i, 6m\}$, $\{3m+i, 4m+i, 6m\}$, $\{5m+i, i, 6m\}$, ismét $0 \le i \le m-1$-re,

(iii) Azon $\{a, b, c\}$ hármasok, ahol a és b a fenti mátrix azonos sorában van és c a következőben (mod 3), továbbá

ha $a+b$ páros, $2c \equiv a+b \pmod{2m}$, és c a sor első felében van,

ha $a+b$ páratlan, $2c \equiv a+b-1 \pmod{2m}$, és c a sor második felében van.

Hosszadalmas, de könnyű verifikálni, hogy így valóban STS-t kapunk (ld. 3.5. Feladat). ∎

Használhatjuk Skolem módszerét a $v = 6m+3$ esetben is. Mátrixunk ebben az esetben

$$\begin{array}{cccc} 0 & 1 & \dots & 2m \\ 2m+1 & 2m+2 & \dots & 4m+1 \\ 4m+2 & 4m+3 & \dots & 6m+2 \end{array}$$

és blokkunk is csak kétféle lesz:

(i) "függőleges blokkok": $\{j, j+2m+1, j+4m+2\}$, $(j = 0, \dots, 2m)$.

(ii) $\{a, b, c\}$, ahol a, b azonos sorban vannak, c a következőben, továbbá $2c \equiv a+b \pmod{2m+1}$.

Újra csak könnyű ellenőrizni, hogy STS-t kapunk (ld. 3.6. Feladat). ∎

Az eddigi konstrukciók mutatják, hogy STS-eket viszonylag könnyű konstruálni. Az ismertetettek talán a legegyszerűbb konstrukciók, szinte számtalan további konstrukció ismert. Érdemes megemlíteni, hogy több véges testek elemi tulajdonságait használó konstrukció is ismert (melyek általában szép automorfizmus-csoporttal rendelkező STS-eket adnak), a 3.7. Feladatban egy Netto-tól eredő ilyen konstrukciót ismertetünk.

A Steiner hármasrendszerek egy másik algebrai vonatkozása a következő: Definiálunk egy műveletet az STS pontjain a természetes módon. Legyen $a \circ b = c$, ha $a \neq b$ és az a, b-t tartalmazó blokk épp $\{a, b, c\}$. Ha ezt kiegészítjük az $a \circ a = a$ definícióval, akkor (idempotens) kvázicsoportot kapunk, amelyben teljesül az

$$(a \circ b) \circ a = b$$

azonosság. Megfordítva, egy a fenti azonosságnak eleget tevő, kommutatív, idempotens kvázicsoportból Steiner hármasrendszert kaphatunk (ld. 3.8. Feladat). Ebből pl. az is következik, hogy ha létezik v_1 és v_2 ponton STS, akkor $v_1 v_2$ ponton is, hiszen a megfelelelő kvázicsoportok direkt szorozhatók.

Zárjuk a Steiner hármasrendszerek áttekintését a kis v értékekkel: $v = 7$-re egyetlen STS van, a Fano-sík, $v = 9$-re szintén, az AG$(2,3)$ affin sík. $v = 13$-ra két hármasrendszer volt, melyeket már a század elején ismertek, végül $v = 15$-re 80 nem-izomorf rendszer van. Ez is mutatja, hogy bekövetkezik a kombinatorikus robbanás v növelésével.

Mi történik, ha k értéke nagyobb? A $k = 4$ esetben a szükséges feltételek (3.3) azt adják, hogy $v \equiv 1$ vagy 4 (mod 12), és Hanani minden ilyen v-re konstruált is Steiner-rendszert. A $k = 5$ eset már bonyolultabb, a szükséges feltétel most $v \equiv 1$ vagy 5 (mod 20), és minden ilyen v-re ismert konstrukció: Hanani, Wilson és Ray-Chaudhuri [HR-CW]. Azonban már a $k = 6$ esetben sem ismert, hogy a 3.3 szükséges feltétel által megengedett minden v-re lenne Steiner-rendszer. Elég nagy v-re és rögzített k-ra azonban ez így van, mint azt a Wilson tétel mutatja (ld. később).

Lássunk néhány további példát blokkrendszerekre:

Példa 3.4 Legyen $\mathcal{P}$ n-edrendű projektív sík. Ekkor $\mathcal{P}$ $(n^2+n+1, n+1, 1)$-rendszer. Jegyezzük meg, hogy ez lényegében ekvivalens a projektív síkok első szakaszban szereplő definíciójával (ld. 3.9. Feladat), azaz $(n^2+n+1, n+1, 1)$-rendszer projektív sík.

Példa 3.5 Legyen $\mathcal{P}$ n-edrendű affin sík. Ekkor $\mathcal{P}$ $(n^2, n, 1)$-rendszer. Jegyezzük meg, hogy ez lényegében ekvivalens az affin síkok 1.1 szakaszban (1.1 Feladat) szereplő definíciójával (ld. 3.10. Feladat), azaz $(n^2, n, 1)$-rendszer affin sík.

Általánosabban a projektív és affin terek is blokkrendszereket adnak:

Példa 3.6 Legyen Σ a $\mathrm{PG}(n, q)$ projektív tér. Definiáljunk egy illeszkedési struktúrát, melyben a pontok Σ pontjai, a blokkok Σ d-dimenziós alterei (valamely rögzített $1 \le d \le n-1$-re). Ez persze hipergráf, és könnyen verifikálható, hogy blokkrendszer is lesz, az alábbi paraméterekkel

$$v = \frac{q^{n+1}-1}{q-1}, \quad k = \frac{q^{d+1}-1}{q-1},$$

$$\lambda = \frac{(q^{n-1}-1)(q^{n-2}-1)\dots(q^{n-d+1}-1)}{(q^{d-1}-1)\dots(q-1)}.$$

Ezt a blokkrendszert $\mathrm{PG}_d(n, q)$-val fogjuk jelölni. Jegyezzük meg, hogy ez a blokkrendszer csak akkor lesz négyzetes (azaz $v = b$), ha $d = n-1$, azaz ha a hipersíkokat tekintjük blokkoknak.

Megjegyzés 3.7 A λ meghatározásában szereplő kifejezést szokás Gauss-féle binomiális együtthatónak (vagy q-binomiális együtthatónak) nevezni. Általában a Gauss-féle binomiális együtthatókat az

$$\begin{bmatrix} n \\ d \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-d+1}-1)}{(q^d-1)(q^{d-1}-1)\dots(q-1)}$$

kifejezés definiálja. Lineáris algebrából tudhatjuk, hogy ez nem más, mint egy n dimenziós vektortér d dimenziós altereinek száma. Ezzel a jelöléssel nagyon könnyű felírni a $\mathrm{PG}_d(n, q)$ blokkrendszer paramétereit:

$$v = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q; \quad k = \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q, \quad \lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q.$$

A további paraméterek (r, b) szintén egyszerűen felírhatók:

$$r = \begin{bmatrix} n \\ d \end{bmatrix}_q; \quad b = \begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_q.$$

Példa 3.8 Lemásolhatjuk a 3.6 Példát affin terekre. Ekkor az $\mathrm{AG}_d(n, q)$ blokkrendszer pontjai az affin tér pontjai, a blokkok a d dimenziós affin alterek (azaz a vektortér alterek mellékosztályai), a paraméterek pedig:

$$v = q^n, \quad k = q^d, \quad \lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q,$$

$$r = \begin{bmatrix} n \\ d \end{bmatrix}_q, \quad b = q^{n-d} \begin{bmatrix} n \\ d \end{bmatrix}_q.$$

Hasonlóan adhatunk további geometriai példákat blokkrendszerekre. Ezek ugyan végtelen osztályok, azonban arra a kérdésre, hogy aritmetikailag megengedett paraméterekre mikor létezik olyan paraméterű blokkrendszer, nagyon kevés információt adnak, hiszen a λ nagyon gyorsan végtelenhez tart. Általában a legtöbb (persze sok sporadikus konstrukció mellett), amit erről a kérdésről tudunk, az Wilson nevezetes tétele:

Wilson tétele. *Ha k és λ rögzített, akkor van olyan v_0, hogy $v > v_0$-ra tetszőleges a 3.3 által megengedett v-re létezik (v, k, λ)-rendszer.*

A bizonyítás az algebrai és valószínűségi módszer kombinálása, mi ezt nem részletezzük.

Ismerkedjünk meg a Latin négyzetek fogalmával is.

Definíció 3.9 Egy $n \times n$-es mátrixot *Latin négyzet*nek nevezünk, ha sorai és oszlopai valamely S halmaz (pl. az $\{1, \dots n\}$) permutációi. Két Latin négyzet, A és B *ortogonális*, ha $a_{ij} = a_{kl}$ esetén $b_{ij} \neq b_{kl}$.

Ha valaki algebrai szemmel nézi a Latin négyzeteket, akkor azok nem mások, mint az ú.n. *kvázicsoport*ok művelettáblái. Emlékeztetünk arra, hogy a csoportot definiáló axiómákat szokás úgy is megfogalmazni, hogy csoportban az asszociativitás mellett minden a, b-re az $ax = b$ ill. az $xa = b$ egyenletek egyértelműen megoldhatók. Ha az asszociativitás nem, de ez az "osztási szabály" teljesül, akkor kvázicsoportról beszélünk. Az egységelemes kvázicsoportokat *loop*nak szokás nevezni. Ezekután nem meglepő, hogy a szokásos algebrai konstrukciók, mint pl. a direkt szorzat, alkalmazhatók Latin négyzetekre. Egy speciális kvázicsoport-osztállyal a Steiner hármasrendszereknél már megismerkedtünk.

A továbbiakban mindig úgy képzeljük, hogy a Latin négyzetek elemei az $1, \dots, n$ számok. Szemléletesen az ortogonalitás azt jelenti, hogy ha egymás mellé helyezzük a két Latin négyzetet, akkor minden (i, j) pár pontosan egyszer fordul elő.

Ortogonális latin négyzetekre a fő kérdés az, hogy mennyi a páronként ortogonális Latin négyzetek maximális száma? Ezt $N(n)$-nel jelöljük. Könnyű belátni, (ld. 3.11. Feladat) hogy legfeljebb $n-1$ páronként ortogonális Latin négyzet van. (Ez egyébként a 3.8 Tétel bizonyításából is kiolvasható.) $n = 2$-re nincsen két ortogonális Latin négyzet, és Euler (a 36 tiszt problémája) azt sejtette (ill. nem teljesen bizonyította), hogy $n = 6$-ra sincs ortogonális Latin négyzetpár. E két példa alapján Euler azt sejtette, hogy $n \equiv 2 \pmod 4$ esetén általában sincs két ortogonális Latin négyzet. Az $n = 6$ esetet a század elején Tarry precizírozta (megmutatta, hogy nincs ortogonális pár), az általános sejtést viszont a hatvanas években Bose, Shrikhande és Parker megcáfolta.

Lássuk először, hogy mi a kapcsolat Latin négyzetek és affin síkok között.

Tétel 3.10 *Pontosan akkor létezik n-edrendű affin sík, ha van $n-1$ páronként ortogonális Latin négyzet.*

Bizonyítás. Legyenek $A_1, \ldots A_{n-1}$ Latin négyzeteink, és szokás szerint legyenek az elemek az $1, \ldots, n$ számok. Legyen $X = \{1, \ldots, n\} \times \{1, \ldots, n\}$ és definiáljuk az egyeneseket az alábbi módon:

$$H_i = \{(x, i) \ : \ 1 \leq x \leq n\}, \ \ 1 \leq i \leq n\text{-re},$$

$$V_i = \{(i, y) \ : \ 1 \leq y \leq n\}, \ \ 1 \leq i \leq n\text{-re},$$

$$L_{ij} = \{(x, y) \ : \ (A_j)_{xy} = i\}, \ \ 1 \leq i \leq n, \ 1 \leq j \leq n-1\text{-re}.$$

Könnyű megmutatni, hogy így olyan illeszkedési struktúrát kapunk, amelyben minden blokk (egyenes) n pontú, minden pont foka $n+1$, a pontok száma n^2, az egyeneseké n^2+n, továbbá minden pontpáron legfeljebb egy egyenes megy át. Ha az egy ponton átmenő egyeneseket tekintjük, akkor azok (a pontot leszámítva) diszjunktak, tehát a pontok száma legalább $1+(n+1)(n-1)$ kell legyen. Mivel pontosan ennyi pontunk van, bármely két ponton át van is blokk, azaz valóban affin síkot kapunk. (Ez lényegében a 3.10. Feladat bizonyítása is.)

Vegyük észre, hogy a H_i, V_j egyenesek tulajdonképpen a Latin négyzetek egy pozícióját jelölik ki. Az L_{ij} alakú egyenesek azonos j-re nem metszik egymást, így ezek felelnek meg egy párhuzamossági osztálynak az affin síkon. Ezen észrevételek alapján könnyű $n-1$ páronként ortogonális Latin négyzetet gyártani. ∎

Ebből speciálisan következik, hogy $N(q) = q-1$, ha q prímhatvány. Általában a következőt lehet tudni.

Tétel 3.11 (Chowla–Erdős–Straus) *$N(n) \to +\infty$, ha $n \to +\infty$.*

A tételt nem bizonyítjuk. Ez a Wilson tétel megfelelője Latin négyzetekre, sőt a Wilson tétel bizonyításában is kulcsszerepet játszik. Ennél erősebb eredmény is igaz. Jelölje n_r azt a legnagyobb méretet, amelyre nincs r páronként ortogonális Latin négyzet. (Tehát $N(n) \geq r$, ha $n > n_r$.) Erre (ha r elég nagy), Beth bizonyította, hogy $n_r = O(r^{14.8})$. Illusztrációként egy "pontos" eredmény: $n_{30} \leq 52502$.

3.1 Feladatok

3.1., A Kirkman-féle 15 iskoláslány problémában megkívánt sétarendben bármely két lány pontosan egyszer sétál egy sorban.

3.2., K_{v+1} felbontható v darab diszjunkt 1-faktorra.

3.3., Bizonyítsuk a Kirkman féle $v \to 2v+1$ konstrukciót.

3.4., Mutassuk meg, hogy a v pontú részrendszer komplementere nem tartalmaz teljes blokkot. Mutassuk meg azt is, hogy ilyen tulajdonsággal egy STS(w)-ben legfeljebb $(w+1)/2$ pont választható ki.

3.5., Verifikáljuk a Skolem konstrukciót $v = 6m+1$-re.

3.6., Verifikáljuk a Skolem konstrukciót $v = 6m+3$-ra.

3.7., Netto konstrukció: Legyen $v = 6m+1$ prím, g pedig egy primitív gyök modulo p. Legyenek a blokkok a

$$\{x, x+g^j, x+g^{m+j} \ : \ j = 0, \ldots m-1, x = 0, \ldots 6m\}.$$

Mutassuk meg, hogy így STS(v)-t kapunk!

3.8., Biz. be, hogy egy $(n^2+n+1, n+1, 1)$-rendszer projektív sík. (A proj. sík axiómáit ld. az 1.1 szakaszban.)

3.9., Biz. be, hogy egy $(n^2, n, 1)$-rendszer affin sík. (Az affin sík axiómáit ld. az 1.1 szakaszban.)

3.10., Bizonyítsuk be, hogy legfeljebb $n-1$ darab $n \times n$-es páronként ortogonális Latin négyzet van.

3.11. Induljunk ki a PG$(2,2)$ Fano-síkból és alkalmazzuk iterálva a Kirkman konstrukciót. Milyen Steiner hármasrendszert kapunk?

4 A FISHER EGYENLŐTLENSÉG ÉS TÁRSAI

Emlékezzünk arra, hogy a de Bruijn–Erdős tétel azt állította, hogy egy lineáris térnek mindig legalább annyi blokkja (egyenese) van, mint pontja. Abban a speciális esetben, ha $\lambda = 1$, ez a tétel blokkrendszerekről állít valamit. A de Bruijn–Erdős tétel $\lambda > 1$ paraméterű blokkrendszerekre való kiterjesztése igazából előbb megvolt, mint maga a de Bruijn–Erdős tétel, a statisztikus Fisher találta. (Ez persze annyiban kevesebb a de Bruijn–Erdős tételnél, hogy csak uniform struktúrákra vonatkozik.) Lássuk tehát a Fisher-egyenlőtlenség bizonyítását.

Tétel 4.1 (Fisher-egyenlőtlenség) *Ha egy blokkrendszerben $k < v$, akkor $b \geq v$.*

Bizonyítás. Legyen M a blokkrendszer illeszkedési mátrixa. Az $A = MM^T$ adjacencia-mátrix nem más, mint az a mátrix, melynek főátlójában r-ek, azon kívül λ-k állnak. Végigosztva minden sort és oszlopot a nem-nulla λ-val, olyan mátrixot kapunk, amely (csupa egyelemű osztállyal) kielégíti az 2.5 Lemma feltételeit, azaz nem szinguláris. Innen a 2.4 Lemma szerint $b \geq v$ következik. ∎

Mivel később szükségünk lesz rá, számítsuk ki explicite az adjacencia-mátrix determinánsát.

Lemma 4.2 $\det(xI + yJ) = (x + yn)x^{n-1}$ *(a mátrixok $n \times n$-esek).*

Bizonyítás. (Ezt már láttuk az előző szakaszban, pl. a 2.5. Feladatban, a jelen bizonyításviszont később is hasznos lineáris algebrai dolgokat elevenít fel. A csupa egyesből álló $\mathbf{j}$ vektor sajátvektora $A = xI + yJ$-nek, a hozzá tartozó sajátérték $x + yn$. A szimmetrikus, így van sajátvektorokból álló ortonormált bázisa, sőt olyan is, ami $\mathbf{j}$-t tartalmazza. A további $\mathbf{v}$ báziselemek merőlegesek $\mathbf{j}$-re, azaz $\mathbf{v}J = 0$, amiből $\mathbf{v}(xI + yJ) = x\mathbf{v}$, vagyis az x lesz $(n-1)$-szeres sajátérték. ∎

Korollárium 4.3 *Blokkrendszer ($k < v$) adjacencia-mátrixának determinánsa $rk(r-\lambda)^{v-1}$. Így az illeszkedési mátrix rangja v.* ∎

A $b = v$ esetben további érdekes tulajdonságokat kapunk.

Tétel 4.4 *Egy a $k < v$ feltételnek eleget tevő blokkrendszerben a következő állítások egyenértékűek:*

(a) $b = v$;

(b) $r = k$;

(c) bármely két blokk λ pontban metszi egymást;

(d) bármely két blokk metszete ugyanakkora.

Bizonyítás. (a) és (b) ekvivalenciája a $vk = br$ egyenlőség miatt triviális. Ha $r = k$, akkor $MJ = JM$, azaz M felcserélhető az MM^T mátrixszal is, azaz $M^2M^T = MM^TM$. Mivel MM^T nem-szinguláris, így M sem, azaz $MM^T = M^TM$. Ez viszont éppen azt fejezi ki, hogy a duális illeszkedési struktúra is blokkrendszer, azaz az eredetiben két blokk λ pontban metszette egymást. Eszerint (b)-ből következik (c). (c)$\to$(d) triviális. Ha (d) teljesül, akkor a blokkrendszer duálisa is blokkrendszer. A Fisher-egyenlőtlenséget az eredeti blokkrendszerre alkalmazva azt kapjuk, hogy $b \geq v$, a duálisra alkalmazva pedig azt, hogy $v \geq b$, azaz $b = v$, vagyis (a) teljesül. ∎

Lássuk az előző tétel egy másik bizonyítását. A bizonyításban használt trükk, a variancia-trükk, vagy négyzetes leszámlálási trükk nagyon fontos (bár elemi). 2.7-ben ezt a módszert már használtuk.

Állítás 4.5 *Legyen B egy $2-(v,k,\lambda)$ blokkrendszer blokkja. A B-től diszjunkt blokkok száma kevesebb, mint*

$$b - \frac{k(r-1)^2}{((k-1)(\lambda-1)+(r-1))}.$$

Egyenlőség pontosan akkor áll, ha a B-t metsző blokkok ugyanannyi, mégpedig $1 + (k-1)(\lambda-1)/(r-1)$ pontban metszik B-t.

Bizonyítás. Legyen d a B-t metsző és tőle különböző blokkok száma. Jelöljük n_i-vel ezek közül azon blokkok számát, amelyek B-t i pontban metszik. Ekkor

$$\sum n_i = d,$$

$$\sum in_i = k(r-1),$$

$$\sum i(i-1)n_i = k(k-1)(\lambda-1).$$

Ezekből az egyenlőségekből az n_i-k minden i-ben másodfokú együtthatós kifejezése előállítható, például a

$$\sum (i-x)^2 n_i = dx^2 - 2k(r-1)x + k((k-1)(\lambda-1)+(r-1))$$

is. Ez a kifejezés nyilván x-től függetlenül nem-negatív, ami csak úgy lehet, ha diszkriminánsa nem-pozitív. Ebből azonnal jön az állításban szereplő egyenlőtlenség. Egyenlőség csak akkor állhat, ha a diszkrimináns nulla, azaz, ha

$$d = \frac{k(r-1)^2}{(k-1)(\lambda-1)+(r-1)}.$$

Az egyenlőségből az is következik, hogy $n_i = 0$ minden $i \neq 1+(k-1)(\lambda-1)/(r-1)$-re. ∎

Ebből az állításból a Fisher-egyenlőtlenség némi számolással kihozható, továbbá az egyenlőség bekövetkeztekor a paraméterek értéke is (ld. 4.1. Feladat).

Nézzük meg most azt, hogy hogyan terjeszthető ki a Fisher-egyenlőtlenség 2-struktúrákra. Ehhez mindenekelőtt jegyezzük meg, hogy a blokkrendszerek létezésére adott szükséges feltételek, illetve a paraméterek összefüggését megadó 3.2 állítás bizonyításában nem használtuk fel, hogy nincsenek többszörös blokkok. Így láthatjuk, hogy uniform 2-struktúra automatikusan r-reguláris, ahol $r = \lambda(v-1)/(k-1)$. Hasonlóan a 3.3-ban megadott szükséges feltételek 2-(v,k,λ)-struktúrákra is érvényesek.

Lemma 4.6 *Ha egy 2-(v,k,λ)-struktúrában $v > k$, akkor nem fordulhat elő, hogy különböző pontok azonos blokkokra illeszkedjenek.*

Bizonyítás. Ha két pont ugyanazokra a blokkokra illeszkedne, akkor $\lambda = r$ lenne, amiből 3.2 miatt $v = k$ következne, ami ellentmondás. ∎

Definíció 4.7 Egy $\mathbf{D}$ 2-struktúrát *valódi*nak (vagy nem-degeneráltnak) nevezünk, ha van olyan blokkja, amelyre egynél több pont illeszkedik, de nem illeszkedik rá minden pont.

Lemma 4.8 *Valódi 2-struktúrában minden pont foka nagyobb, mint λ.*

Bizonyítás. $\deg(p) \geq \lambda$ triviális. Tegyük fel, hogy valamely p pontra egyenlőség van, és legyen q egy p-től különböző pont. Mivel λ olyan blokk van, amely p-n és q-n átmegy, minden olyan blokk, amely illeszkedik p-re, illeszkedik q-ra is. Ez elmondható minden p-től különböző pontra, azaz a legalább két pontot tartalmazó blokkok minden pontot tartalmaznak. ∎

Ha ezt az észrevételt összevetjük a Fisher-egyenlőtlenség első (2.5 Lemmán alapuló) bizonyításával, akkor látni fogjuk, hogy a Fisher-egyenlőtlenség érvényes valódi 2-struktúrákra. Ehhez először az illeszkedési mátrixra vonatkozó egyenletet kell módosítanunk.

Lemma 4.9 *Ha A valódi 2-struktúra illeszkedési mátrixa, akkor*

$$AA^T = \lambda J + \mathrm{diag}(r_i - \lambda),$$

ahol r_i az i-edik pont fokát jelenti. ∎

Állítás 4.10 *Valódi 2-struktúrára $b \geq v$.* ∎

Ennek az állításnak egy másik bizonyítását kapjuk, ha explicite kiszámoljuk a Lemma 4.9-ben szereplő mátrix determinánsát.

Állítás 4.11 *Ha A valódi 2-struktúra illeszkedési mátrixa, akkor*

$$\det(AA^T) = \prod_{i=1}^{v}(r_i - \lambda)\left(1 + \lambda\sum_{j=1}^{v}\frac{1}{(r_j-\lambda)}\right). \quad ∎$$

A bizonyítást feladatnak hagyjuk (ld. 4.2. Feladat, lényegében megcsináltuk a 2.5. Feladatban).

A következő állítás azt mutatja, hogy a $b = v$ esetben a 2-(v,k,λ)-struktúrák automatikusan blokkrendszerek.

Állítás 4.12 *Valódi négyzetes 2-struktúra nem tartalmazhat többszörös blokkokat.*

Bizonyítás. Ha egy 2-struktúra tartalmaz többszörös blokkokat, akkor illeszkedési mátrixa tartalmaz két azonos sort, tehát rangja legfeljebb $b-1$. Másrészt viszont az illeszkedési mátrix rangja v, ami a $b = v$ esetben lehetetlen. ∎

Vegyük észre, hogy a Fisher-egyenlőtlenség 4.10 nem-uniform változata valójában a de Bruijn–Erdős tétel megfelelője a $\lambda > 1$ esetre. A de Bruijn–Erdős tétel alapján azt várhatnánk, hogy egyenlőség csak akkor lehet, ha a 2-struktúra uniform, vagyis ha blokkrendszer. Ez azonban sajnos nem igaz, amint a következő példa mutatja:

Példa 4.13 Legyen $\mathbf{D}$=($\mathbf{P}$,$\mathbf{B}$) reguláris 2-struktúra és p egy pontja. A $\mathbf{D}^*(p)$ struktúra pontjai legyenek $\mathbf{D}$ pontjai. $\mathbf{D}$ minden Y blokkjához definiáljuk $\mathbf{D}^*(p)$ egy Y^* blokkját a következőképpen: Ha $p \in Y$, akkor legyen $Y^* = \mathbf{P} \setminus Y$, ha pedig $p \notin Y$, akkor legyen $Y^* = Y \cup \{p\}$. Könnyű ellenőrizni, hogy $\mathbf{D}^*(p)$ 2-struktúra lesz, melyre $\lambda^* = r - \lambda$ (ld. 4.3. Feladat). Ha $\mathbf{D}$ négyzetes blokkrendszer, akkor $\mathbf{D}^*(p)$ valódi négyzetes 2-struktúra, melyben kétféle blokkméret van, $k+1$ és $v-k$ (ld. a 4.3. Feladatot is). ∎

Eszerint nem várhatjuk a de Bruijn–Erdős tétel teljes megfelelőjét $\lambda > 1$-re. Az azonban tipikus a fenti példában, hogy ha egy valódi négyzetes 2-struktúra nem uniform, akkor csak két blokkméret van, melyek összege $v+1$.

Tétel 4.14 *Legyen* $\mathbf{D}$ *olyan valódi, négyzetes 2-struktúra, amely nem blokkrendszer. Ekkor* $\mathbf{D}$*-ben csak kétféle blokkméret fordul elő, s e két méret összege* $v+1$.

Bizonyítás. Írjuk fel a szokásos módon $\mathbf{D}$ illeszkedési, majd adjacencia-mátrixát. Ez nem más, mint

$$AA^T = N + \lambda J, \tag{8}$$

ahol N az a diagonális mátrix, melyben a főátlóban a $\deg(p) - \lambda (> 0)$ értékek állnak. Ezenkívül $AJ = (N + \lambda I)J$. Fel tudjuk írni $N + \lambda J$ inverzét is, ez nem más, mint

$$(N + \lambda J)^{-1} = N^{-1} - cN^{-1}JN^{-1},$$

ahol $c = \lambda(1 + \lambda \sum n_i^{-1})^{-1}$. Ha most (8)-t beszorozzuk a jobb oldal inverzével jobbról, A^{-1}-gyel balról, akkor azt kapjuk, hogy $A^T(N+\lambda J)^{-1} = A^{-1}$, amit A-val jobbról szorozva

$$A^T N^{-1} A = I + cA^T N^{-1} J N^{-1} A \tag{9}$$

adódik. Ebből az egyenlőségből a főátlóbeli elemek összehasonlításával a

$$\sum_{P_j \in y_i} \frac{1}{n_j} = 1 + c \left(\sum_{P_j \in y_i} \frac{1}{n_j} \right)^2$$

egyenlőséghez jutunk, minden y_i blokkra. Az $s_i = \sum_{P_j \in y_i} 1/n_j$ ismeretlent bevezetve ez

$$s_i = 1 + cs_i^2.$$

Ha most (9)-t jobbról beszorozzuk J-vel, akkor azt kapjuk, hogy

$$A^T(J - c(v-1)N^{-1}J) = J.$$

A bal oldalon az i-edik sorban mindenütt $|y_i| - c(v-1)s_i$ áll, így

$$|y_i| - c(v-1)s_i = 1, \quad \Rightarrow \quad s_i = \frac{|y_i| - 1}{c(v-1)}.$$

Ha ezt a kifejezést behelyettesítjük a fenti s_i-re vonatkozó egyenletbe, akkor $(|y_i| - 1)$-re nézve másodfokú egyenletet kapunk, mégpedig az

$$(|y_i| - 1)^2 - (v-1)(|y_i| - 1) + c(v-1)^2 = 0$$

egyenletet. Eszerint $(|y_i| - 1)$-re két értéket kaphatunk, melyek összege $v-1$. ∎

Nevezetes sejtés, az ú. n. λ-*design sejtés*, hogy a fenti 4.13 konstrukcióval megkapjuk az összes négyzetes valódi 2-struktúrát.

Térjünk vissza a Fisher-egyenlőtlenséghez. A Fisher-egyenlőtlenség bizonyításából további érdekes információkat deríthetünk ki. Azt beláttuk, hogy $AA^T = (r-\lambda)I + \lambda J$, és ennek a mátrixnak a sajátértékei kr (1 multiplicitással) és $(r-\lambda)$ ($v-1$ multiplicitással). Azt is tudjuk, hogy A rangja pontosan v. Tekintsük most $A^T A$-t, azaz a blokk-adjacencia-mátrixot.

Lemma 4.15 AA^T *sajátértékei* $A^T A$*-nak is sajátértékei, méghozzá ugyanazzal a multiplicitással, továbbá 0 lesz még sajátérték, multiplicitása pedig* $b-v$.

Bizonyítás. Standard lineáris algebra. ∎

Eszerint a $Q = (r-\lambda)I + (\lambda k/r)J - A^T A$ mátrix pozitív szemidefinit (sajátértékei 0 (v multiplicitással) és $(r-\lambda)$ $b-v$ multiplicitással). Ha tehát tekintjük Q egy főminorját (néhány sorés ugyanezen oszlopok alkotta részmátrix), akkor az is pozitív szemidefinit lesz. Ezt az észrevételt a blokkok metszetére vonatkozó egyenlőtlenségek igazolására használhatjuk fel. Ha 1×1-es főminort veszünk, azaz egy blokkot, akkor Q főátlójában szereplő elemet kapjuk rész-mát-rix-ként, ami nem-negatív. Ebből visszakapjuk a Fisher-egyenlőtlenséget, hisz $r - \lambda + \lambda k/r - k \geq 0$-ből $r \geq k$ vagy $r \leq \lambda$ következik, ez utóbbi viszont lehetetlen, ha a blokkrendszer nem-degenerált.

Ha 2×2-es főminort, azaz két különböző blokkot tekintünk, akkor a következő egyenlőtlenséget kapjuk.

Állítás 4.16 (Connor, Majumdar)

$$k + \lambda - r \leq |B \cap C| \leq r - k - \lambda + \frac{2\lambda k}{r}.$$

Bizonyítás. Az állítás előtti észrevétel szerint a B és C-hez tartozó főminor determinánsa nem-negatív. A főátlóban $r - \lambda + \lambda k/r - k$ áll, a másik két elem $\lambda k/r - |B \cap C|$, így egyrészt $r - \lambda + \lambda k/r - k \geq \lambda k/r - |B \cap C|$, másrészt $r - \lambda + \lambda k/r - k \geq -\lambda k/r + |B \cap C|$. Az első egyenlőtlenség adja a Majumdar (vagy Connor)-egyenlőtlenségbeli alsó becslést, a második a felsőt. ∎

Az egyenlőség esete is jellemezhető, erről szól a 4.4. Feladat.

A Connor-féle pozitív szemidefinitségi ötlet egy további következménye a Mann-egyenlőtlenség:

Állítás 4.17 (Mann) *Ha egy 2-struktúrában, melyre* $v > k$*, valamely blokk multiplicitása* m*, akkor* $b \geq mv$.

Bizonyítás. Ld. a 4.5. Feladatot. ∎

Nézzük meg most a Fisher-egyenlőtlenség egy további változatát, amely párhuzamossággal bíró blokkrendszerekre vonatkozik. Először lássunk egy önmagában is érdekes lineáris algebrai lemmát, a Block-lemmát. Mielőtt magára a lemmára térnénk, néhány definíció következik.

Definíció 4.18 Particionáljuk egy A mátrix sorait és oszlopait, legyen mondjuk $S = S_1 \cup \ldots S_{v_1}$ és $O = O_1 \cup \ldots \cup O_{b_1}$, ahol S és O a sorok illetve az oszlopok indexhalmaza. M_{ij} azt a mátrixot jelöli, amelynek sorai S_i-be, oszlopai O_j-be tartoznak. A felbontást *sor-taktikus*nak nevezzük, ha M_{ij} minden sorában az elemek összege ugyanannyi (mondjuk r_{ij}). Vezessük még be az $R = (r_{ij})$ mátrixot, ha a felbontás sor-taktikus volt. Hasonlóan definiáljuk azt, hogy a felbontás mikor *oszlop-taktikus*, és ebben az esetben az oszlopösszegek mátrixát jelölje C. Egy felbontást *taktikus*nak nevezünk, ha egyaránt sor – és oszlop-taktikus.

Lemma 4.19 (Block lemma) *Legyen A egy $v \times b$ mátrix, $S = S_1 \cup \ldots \cup S_{v_1}$ és $O = O_1 \cup \ldots \cup O_{b_1}$ a sorok illetve az oszlopok egy felbontása. Ha a felbontás sor-taktikus, akkor rang$(A)-$rang$(R) \leq b - b_1$. Ha a felbontás oszlop-taktikus, akkor rang$(A)-$rang$(C) \leq v - v_1$.*

Bizonyítás. Mondjuk az oszlop-taktikusságra vonatkozó állítást látjuk be. Ha $\mathcal{R}$ egy rang$(A) = r$ számú sorból álló független sorrendszer, akkor a fennmaradó $v-r$ sor nyilván legfeljebb $v-r$ pontosztályból tartalmaz sort. Eszerint legalább $v_1 - (v - r)$ teljes pontosztály van az $\mathcal{R}$-be eső sorok között. Ez persze lehet, hogy semmit nem ad, de akkor $v_1 - (v - r) \leq 0 \leq$rang$(C)$, azaz ekkor készen vagyunk. Tehát feltehetjük, hogy $v_1 - (v - r) > 0$ és tekintsük C megfelelő sorait (tehát azokat, amelyek teljes pont-osztálya $\mathcal{R}$-ben van. Tegyük fel, hogy ezen sorok valamely lineáris kombinációja nullvektor. Egy ilyen lineáris kombináció felemelhető A sorainak egy teljes pont-osztályokat tartalmazó lineáris kombinációjává (felhasználva, hogy a felbontás oszlop-taktikus). Ez viszont lehetetlen, hiszen ezek a sorok mind $\mathcal{R}$-ben voltak. Eszerint a szóbanforgó $v_1 - (v - r)$ sor lineárisan független, azaz rang$(C) \geq v_1 - (v - r)$. Ebből a (b)-beli egyenlőtlenség átrendezéssel adódik. ∎

Korollárium 4.20 *Ha A rangja v és a felbontás taktikus, akkor $0 \leq b_1 - v_1 \leq b - v$.*

Bizonyítás. Nyilván rang$(R) \leq v_1$. Eszerint a Block lemma miatt $v =$ rang $(A) \leq$ rang $(R) + b - b_1 \leq v_1 + b - b_1$, azaz $b - v \geq b_1 - v_1$. Hasonlóan kapjuk a $0 \leq b_1 - v_1$-et is az oszlop-taktikusság felhasználásával. ∎

Abban az esetben, ha A egy illeszkedési struktúra illeszkedési mátrixa, a taktikusságnak világos kombinatorikai jelentése van. Particionálnunk kell a pontokat és a blokkokat, és ha megszorítjuk az illeszkedést akármelyik pont és akármelyik blokk-osztályra, akkor a sor-taktikusság ezen megszorítás regularitásának, míg az oszlop- taktikusság a megszorítás uniformitásának felel meg (ld. 4.6. Feladat).

Emlékeztetünk arra, hogy a párhuzamosság, amelyet a Kirkman probléma után említettünk, speciális esete az ilyen taktikus felbontásnak: egyetlen pontosztály van, és minden pontra minden osztályból pontosan egy blokk illeszkedik. Ennél általánosabban, egy blokkrendszert *felbonthatóna*k nevezünk, ha illeszkedési mátrixának van olyan taktikus felbontása, amelyben egyetlen pontosztály van.

Felbontható, vagy párhuzamossággal rendelkező blokkrendszerekre pontosabbá tehetjük a Fisher-egyenlőtlenséget az alábbi módon.

Tétel 4.21 *Ha egy blokkrendszer felbontható, és a felbontásban x blokkosztály van, akkor $b \geq v + x - 1$. Speciálisan, ha a blokkrendszernek van párhuzamossága, akkor $b \geq v + r - 1$.*

Bizonyítás. Ez azonnal következik a Block lemmából, hisz esetünkben $v_1 = 1$, $b_1 = x$ és a felbontás taktikus. A párhuzamosság esetén még annyit kell észrevennünk, hogy egy ponton átmenő blokkok különböző osztályba kell tartozzanak, azaz $x = r$. ∎

Persze, a párhuzamosság létezése elegendő ugyan a taktikussághoz, azonban párhuzamosságot megadni gyakran nem is olyan egyszerű. A most következő állítások azt mutatják meg, hogyan lehet automorfizmusok segítségével az illeszkedési mátrix taktikus felbontásait származtatni.

Tétel 4.22 *Ha $G \leq$ Aut$(\mathbf{D})$, akkor G pont és blokk-orbitjai az illeszkedési mátrix egy taktikus felbontását adják.*

Bizonyítás. Ezt, és néhány olyan automorfizmusokról szóló állítás bizonyítását, amelyet az 1. fejezetben már láttunk, most egy feladat-sorozatban adjuk meg (ld. 4.6. Feladatot). ∎

Az említett feladat-sorozatban találhatjuk az alábbi hasznos tételt is.

Tétel 4.23 (Általánosított orbit-tétel) *Legyen $\mathbf{D}$ olyan 2-struktúra, amelynek v pontja, b blokkja van, és az illeszkedési mátrixának v a rangja. Ha $G \leq$ Aut$(\mathbf{D})$ olyan, melynek v_1 pontorbitja és b_1 blokkorbitja van, akkor $0 \leq b_1 - v_1 \leq b - v$.* ∎

Jegyezzük meg, hogy ez azonnal adja 1.22-t, a név is innen származik.

Mint említettük, párhuzamosságot nem is mindig könnyű definiálni egy blokkrendszerben, így nézzük meg, hogy a legegyszerűbb esetben, azaz Steiner hármasrendszerekre mit lehet erről mondani. Ekkor minden párhuzamossági osztály $v/3$ blokkot tartalmaz, és mivel $b = v(v-1)/6$, így az osztályok száma $(v-1)/2$. Ebből azonnal következik, hogy felbontható STS csak $v \equiv 3 \pmod 6$ esetén létezhet. Másrészről Ray-Chaudhuri és Wilson belátták, hogy minden ilyen v-re létezik is felbontható STS. Azt már maga Kirkman is tudta, hogy minden $v = 3^n$-re van ilyen felbontható STS. Ilyenek például a 3 elemű testre épített affin terek (a szokásos geometriai párhuzamossággal). Az első pillantásra meglepő, hogy a $\mathrm{PG}(n, 2)$ projektív terek is felbonthatóak, ha v-re tett szükséges feltétel teljesül, azaz, ha n páratlan. Ez pl. azt jelenti, hogy a $\mathrm{PG}(3, 2)$ a 15 iskoláslány probléma megoldását adja.
A bizonyítást ld. a 4.7. Feladatban.

4.1 Feladatok.

4.1., Biz. be a Fisher egyenlőtlenséget ill. a négyzetes blokkrendszerek tulajdonságait 4.6 alapján.
4.2., Számítsuk ki $\det(A)$-t, ha $A = \lambda J + \mathrm{diag}(r_1 - \lambda, ..., r_v - \lambda)$, és $r_i > \lambda$.
4.3., Ellenőrizzük a 4.13 Példát.
4.4., Jellemezzük az egyenlőség esetét a Connor, Majumdar egyenlőtlenségben.
4.5., Biz. be 4.17-et.
4.6., ** automorfizmus feladatsor **
4.7., Mutassuk meg, hogy $\mathrm{PG}(n, 2)$ pontosan akkor felbontható, ha n páratlan.

5 t-RENDSZEREK

Definíció 5.1 A $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ egyszerű illeszkedési struktúra $t-(v, k, \lambda)$ *rendszer*, ($v > k > 1$, $k \geq t \geq 1$), ha a pontok száma v, minden blokkra k pont illeszkedik és bármely t pont pontosan λ blokkban van benne. Ha az egyszerűséget elhagyjuk, vagyis lehetnek többszörös blokkok, akkor (uniform) $t-(v, k, \lambda)$ *struktúráról* fogunk beszélni.

A $t = 2$ visszadja a blokkrendszereket, $t = 1$-re pedig egyszerűen a reguláris, uniform hipergráfokat kapjuk.

Példa 5.2 1) Ha $\mathbf{B}$ a $\mathbf{P}$ halmaz összes k elemű részhalmaza, akkor a teljes k-uniform hipergráfot kapjuk, amely minden $t \leq k$-ra $t-(v, k, \lambda)$-rendszer, mégpedig $\lambda = \binom{v-t}{k-t}$-vel.
2) Az $\mathrm{AG}_2(n, 2)$ ($n \geq 3$) blokkrendszer $3-(2^n, 4, 1)$-rendszer is.

Mielőtt további példákat vagy eredményeket néznénk, megmutatjuk, hogy az illeszkedési struktúra egyszerűsége a definíció fontos része. Ha ezt nem kívánjuk meg, akkor sokkal könnyebben mennek a konstrukciók.

Tétel 5.3 *Tegyük fel, hogy $t < k < v - t$. Ekkor alkalmas λ-ra létezik olyan $t-(v, k, \lambda)$-struktúra, amelyben nem minden k pontú ponthalmaz blokk.*

Bizonyítás. Legyen M az a $\binom{v}{k} \times \binom{v}{t}$ mátrix, amelyben a sorokat illetve az oszlopokat a v elemű alaphalmaz k illetve t elemű részhalmazaival indexeltük, a (K, T) elem pedig pontosan akkor 1, ha $T \subset K$ különben 0. A feltétel szerint $\binom{v}{t} < \binom{v}{k}$ és így M sorai lineárisan összefüggők. Eszerint van olyan racionális koordinátájú $\mathbf{v}$ vektor, amelyre $\mathbf{v}M = \mathbf{0}$.
Persze feltehetjük, hogy $\mathbf{v}$ egész koordinátájú. Legyen $-m$ a $\mathbf{v}$ legkisebb koordinátája ($m > 0$). Ha $\mathbf{j}$ jelöli a csupa egyesből álló vektort és $\mathbf{w} = \mathbf{v} + m\mathbf{j}$, akkor $\mathbf{w}$ minden koordinátája nem-negatív egész és van olyan koordináta, amely 0. Továbbá

$$\mathbf{w}M = (\mathbf{v} + m\mathbf{j})M = m\mathbf{j}M = m\binom{v-t}{k-t}\mathbf{j}.$$

Ez az egyenlet pont azt adja amit akartunk: ha ugyanis $\mathcal{B}$ az alaphalmaz azon k elemű K részhalmazaiból áll, amelyekre $\mathbf{w}$ K-adik koordinátája pozitív, mégpedig az ilyen K-k multiplicitása $\mathbf{w}_K$, akkor egyenletünk azt mondja, hogy bármely t elemű részhalmaz pontosan $\lambda = m\binom{v-t}{k-t}$ darab $\mathcal{B}$-beli halmazban van benne (multiplicitással számolva). ∎

A helyzet meglehetősen különbözik ettől, ha nincsenek többszörös blokkok. Néhány sporadikus 5-rendszer ismert volt már régóta (ezek a Mathieu-csoportokhoz tartozó Witt-féle rendszerek, velük találkozunk később a Golay-kódoknál), de nem-triviális 6-rendszer sokáig nem volt ismert (semmilyen λ-ra). Mivel a példák sokszorosan tranzitív csoportokkal voltak kapcsolatban, a sokszorosan tranzitív csoportok nemlétezése bizonyításának egy lehetséges útjának látszott annak belátása, hogy 6-rendszerek nincsenek is. Ez azonban nem így van: először Magliveras és Leavitt konstruált 6-rendszereket, majd újabb és újabb rendszereket konstruáltak mások, így ez az út nem járható. (Jegyezzük meg, hogy a véges egyszerű csoportok osztályozásából kijön, hogy nincsenek 6-tranzitív csoportok, csak az alternáló és a szimmetrikus csoport.) Végül Teirlinck intézte el lényegében a kérdést, aki az alábbi tételt bizonyította.

Teirlinck tétele. *Adott t-re legyen*

$$\mu = \prod_{i=1}^{t}\left(\left[\{\binom{i}{n} \ : \ n=1,\ldots,i\}\right]\cdot[\{1,\ldots,i+1\}]\right).$$

Ekkor bármely $v \equiv t \pmod{\mu}$-re az X v-elemű alaphalmaz $(t+1)$-elemű részhalmazait $t-(v,t+1,\mu)$-rendszerekre particionálhatjuk. Speciálisan, $t-(v,t+1,\mu)$-rendszerek léteznek $v \equiv t \pmod{\mu}$, $\lambda \equiv 0 \pmod{\mu}$, és $v > \lambda + t$ esetén. ∎

A tételt nem bizonyítjuk, az messze meghaladná a jegyzet kereteit. A $[,]$ szimbólum a formulában a legkisebb közös többszöröst jelöli.

Most a Fisher-egyenlőtlenség t-rendszerekre való kiterjesztéseire térünk rá. Ezt a $t=4$ esetben Petrenjuk látta be, az általános eset bizonyítása Ray-Chaudhuri és Wilson érdeme.

Tétel 5.4 *Legyen $\mathbf{D}$ $t-(v,k,\lambda)$-rendszer, ahol $t=2s$ és $k \le v-s$. Ekkor $b \ge \binom{v}{s}$.*

Bizonyítás. Az incidencia-mátrix egy általánosítását fogjuk használni. A sorokat a blokkokkal, az oszlopokat az s pontú részhalmazokkal indexeljük, és egy (B,S) pozícióba pontosan akkor írunk 1-et, ha $S \subset B$. Ennek megfelelően legyen $\mathbf{r}_B$ az M B-edik sora, $\mathbf{e}_S$ pedig az a vektor, amelynek S-edik pozíciójában 1 áll, különben 0. Nyilván az $\mathbf{e}_S$-ek alkotják a $\binom{v}{s}$ dimenziós valós V vektortér természetes bázisát. Azt kellene belátnunk, hogy M sorai generátorrendszert alkotnak V-ben. Legyen $0 \le i \le s$-re

$$\mathbf{y}_i = \sum_{|B\cap S|=i}\mathbf{r}_B = \sum_{j=0}^{i}\sum_{|S'\cap S|=j}\ \sum_{S'\subset B, |B\cap S|=i}\mathbf{e}_{S'} =$$

$$\sum_{j=0}^{i}\binom{s-j}{i-j}\nu_{2s-j,s+i-j}\left(\sum_{|S'\cap S|=j}\mathbf{e}_{S'}\right),$$

ahol $\nu_{m,n}$ azon blokkok számát jelenti, amelyek egy adott M m pontú halmazt egy adott N n pontú részhalmazában metszenek. A szita-formula segítségével belátható, hogy $\nu_{m,n}$ nem függ az $N \subset M$ pártól (csak n-től és m-től), ha $n \le m \le t$ (ld. az 5.1. Feladatot). Legyen végül

$$\mathbf{x}_j = \sum_{|S'\cap S|=j}\mathbf{e}_{S'}.$$

Ezt a jelölést bevezetve a fenti egyenlőségek $s+1$ lineáris egyenletet adnak az $\mathbf{x}_j$-kre, melyeknek jobboldala éppen az $\mathbf{y}_j$. Ennek az egyenletrendszernek a mátrixa trianguláris mátrix, s a diagonális elemek, a $\nu_{2s-i,s}$ elemek nem nullák. Így az egyenletrendszer egyértelműen megoldható, vagy másképpen fogalmazva, az $\mathbf{x}_j$-k kifejezhetők az $\mathbf{y}_j$-k lineáris kombinációjaként. Speciálisan $x_s = \mathbf{e}_S$ is előáll az $\mathbf{y}_j$-k kombinációjaként, vagyis az $\mathbf{y}_j$-k tényleg generátorrendszert alkotnak. ∎

Természetesen, ha $t=2s+1$, akkor ugyanez az egyenlőtlenség érvényes, hiszen egy t-rendszer egyben $(t-1)$-rendszer is.

Ray-Chaudhuri és Wilson a duális eredményt is belátták.

Tétel 5.5 (Ray-Chaudhuri, Wilson) *Legyen $s \le k \le v-s$ és legyen $\mathbf{B}$ egy V v pontú halmaz k elemű részhalmazainak olyan családja, melyre $|B \cap B'|$ legfeljebb s értéket vesz fel, ha $B \ne B' \in \mathbf{B}$. Ekkor $\mathbf{B} \le \binom{v}{s}$.* ∎

Ezt a változatot nem bizonyítjuk, legfőképpen azért, mert az Extremális Kombinatorika előadásban szokott szerepelni, továbbá megtalálható a Babai–Frankl könyvben is, ahol további variánsait (pl. mod p) is elolvashatja az érdeklődő olvasó.

5.1 Feladatok

5.1., Mutassuk meg, hogy az 5.4 bizonyításában szereplő $\nu_{m,n}$ valóban csak m-től és n-től függ.

5.2., Mutassuk meg, hogy t-rendszerben a $t+1$ pontot elkerülő blokkok száma nem függ a pontoktól.

5.3., Legyen $\Omega = \{0,1\}^n$. Tekintsük az $\Omega \mapsto \mathbf{R}$. függvényeket. $I \subset \{1,\ldots,n\}$-re legyen $f(I) := f(v_I)$, ahol $v_I \in \Omega$ az I incidencia-vektora. Legyen $x_I := \prod_{i\in I} x_i$. Ekkor

a) $x_I(J)=1$, ha $I \subseteq J$, 0 különben.

b) Legyen $f:\Omega \to \mathbf{R}$ függvény. Tegyük fel, hogy $f(I)\neq 0$, ha $|I|\leq r$. Ekkor

$$\{x_I f \ :\ |I| \leq r\}$$

lineárisan független.

c) Legyen $L=\{\ell_1,\dots,\ell_s\}$, $V=\{1,\dots,v\}$, $\mathbf{B}=\{A_1,\dots,A_m\}$, ahol $|A_1|\leq \dots |A_m|$, v_i pedig jelölje A_i incidencia-vektorát ($i=1,\dots,m$-re). Legyen

$$f_i(x)=\prod_{k=1}^{s}((v_i,x)-\ell_k), \quad (x\in\Omega).$$

Ekkor az

$$\{f_1,\dots,f_m, x_I(\sum_{j=1}^{m} x_j - k)\ :\ I\subseteq\{1,\dots,v\}, |I|\leq s-1\}$$

függvények lineárisan függetlenek.

d) Lássuk be az 5.5 Tételt!

5.4., Idézzük fel a Ray-Chaudhuri–Wilson tétel nem-uniform változatának bizonyítását (elsőben szerepelt!)!

[Legyen $\mathcal{F}$ egy hipergráf n ponton, $L=\{\ell_1,\dots,\ell_s\}$ nemnegatí v, n-nél kisebb egészek halmaza. Ha bármely két különböző $A,B\in\mathcal{F}$-re $|A\cap B|\in L$, akkor

$$|\mathcal{F}|\leq\sum_{k=0}^{s}\binom{n}{k}.$$

6 NÉGYZETES BLOKKRENDSZEREK

Idézzük fel, hogy egy blokkrendszer pontosan akkor négyzetes, ha a blokkok száma azonos a pontokéval ($b=v$). Láttuk, hogy ez egyenértékű azzal, hogy $r=k$, és azzal is, hogy bármely két blokk metszete λ pontú. Célunk az lesz, hogy négyzetes blokkrendszerek paraméterei közötti további összefüggéseket találjunk. Emlékeztetünk arra, hogy a **??** Lemma miatt blokkrendszer M incidencia-mátrixára $\det(MM^T)=rk(r-\lambda)^{v-1}$. Esetünkben $k=r$, így ($\det(M)=\det(M^T)$-t is használva) azt kapjuk, hogy

$$(\det(M))^2=(k-\lambda)^{v-1}k^2.$$

Korollárium 6.1 *Ha létezik négyzetes $2-(v,k,\lambda)$-rendszer, akkor $(k-\lambda)^{v-1}$ négyzetszám.* ∎

Definíció 6.2 Négyzetes $2-(v,k,\lambda)$-rendszerekre az $n=(k-\lambda)$ mennyiséget a blokkrendszer *rend*jének nevezzük. A későbbiekben az n mindig ezt fogja jelenteni (négyzetes blokkrendszerekre).

Állítás 6.3 *Legyen* $\mathbf{D}$ *négyzetes $2-(v,k,\lambda)$-rendszer ($1<k<v-1$). Ekkor*

$$4n-1\leq v\leq n^2+n+1.$$

Bizonyítás. Tudjuk, hogy $(v-1)\lambda=r(k-1)$, ami esetünkben a $v=1+k(k-1)/\lambda=\lambda+2n-1+n(n-1)/\lambda$ összefüggést adja. (Ha $n=1$, akkor ebből $r=k=v-1$ adódna, így feltehetjük, hogy $n>1$.) Ebből

$$\lambda=\frac{1}{2}(v-2n\pm\sqrt{(v-2n)^2-4n(n-1)});$$

az egyenlet két megoldása (λ,λ') $\mathbf{D}$-nek illetve komplementumának felel meg. Mivel $\lambda,\lambda'\geq 1$, így $v-2n-2\geq\sqrt{(v-2n)^2-4n(n-1)}$, amit négyzetre emelve azt kapjuk, hogy $v\leq n^2+n+1$. Egyenletünk diszkriminánsa is pozitív, amiből $(v-2n)^2-4n(n-1)\geq 0$ adódik. Így $(v-2n)^2\geq(2n-1)^2-1$, és $v\geq 2n$-et is figyelembe véve ez a $v-2n\geq 2n-1$ egyenlőtlenséget adja. ∎

A szereplő korlátok élesek végtelen sok n-re. A felső becslést a projektív síkok, az alsót az ú.n. Hadamard-féle blokkrendszerek valósítják meg. Ezekről nemsokára többet is megtudunk.

Most rátérünk egy jóval mélyebb tétel igazolására. Ez mindmáig az egyetlen általános szükséges feltétel négyzetes blokkrendszerek létezésére. A 10-edrendű sík nemlétezése mutatja, hogy ez a feltétel sajnos nem elegendő. Mielőtt a bizonyításra rátérnénk, lássunk egy Lagrange-tól eredő elemi számelméleti lemmát, valamint egy elemi azonosságot.

Lemma 6.4 (Lagrange) *Minden pozitív egész szám előáll négy négyzetszám összegeként.* ∎

Ezen kívül szükségünk lesz az alábbi elemi számelméleti azonosságra is:

$$(b_1^2+b_2^2+b_3^2+b_4^2)(x_1^2+x_2^2+x_3^2+x_4^2) = y_1^2+y_2^2+y_3^2+y_4^2 \tag{10}$$

ahol

$$\begin{aligned} y_1 &= b_1x_1 - b_2x_2 - b_3x_3 - b_4x_4;\\ y_2 &= b_2x_1 + b_1x_2 - b_4x_3 + b_3x_4;\\ y_3 &= b_3x_1 + b_4x_2 + b_1x_3 - b_2x_4;\\ y_4 &= b_4x_1 - b_3x_2 + b_2x_3 + b_1x_4. \end{aligned}$$

Az azonosság szemléletes tartalma az, hogy két kvaternió szorzatának normája megegyezik a normák szorzatával. Ez azt is jelenti, hogy az $x \to y$ lineáris transzformáció (azaz a $b_1 + b_2i + b_3j + b_4k$-val való szorzás) nem szinguláris. Mivel a b-k alkotta mátrix elemei egészek, így inverz mátrixa is racionális elemű. Erre az észrevételre szükségünk lesz a bizonyítás során.

Tétel 6.5 (Bruck–Chowla–Ryser) *Tegyük fel, hogy v páratlan és létezik négyzetes $2-(v,k,\lambda)$-rendszer. Ekkor a*

$$z^2 = (k-\lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2$$

diofantoszi egyenletnek van nem-triviális egész megoldása.

Bizonyítás. Soroljuk fel a pontokat: $p_1,\dots,p_v$ és a blokkokat: $B_1,\dots,B_v$ és legyen M az ennek megfelelő incidencia-mátrix. Az $MM^T = nI + \lambda J$ mátrixegyenletet lineáris kifejezésekre vonatkozó azonosság formájában fogjuk felírni. Ehhez vezessük be az

$$L_i = \sum_{j=1}^{v} m_{ji}x_j, \quad (i = 1,\dots,v)$$

kifejezéseket. Ezekre az

$$L_1^2+\dots+L_v^2 = n(x_1^2+\dots+x_v^2) + \lambda(x_1+\dots+x_v)^2 \tag{11}$$

azonosság érvényes. Ehhez azt kell észrevenni, hogy minden ${x_i}^2$ k-szor fordul elő a baloldalon, mert a p_i pontra k blokk illeszkedik, és hasonlóan az x_ix_j szorzat 2λ-szor fordul elő, mert a p_i,p_j pontokra λ blokk illeszkedik. Ezt az azonosságot fogjuk redukálni, a 6.4 Lemma és az utána említett azonosság segítségével.

Mivel v páratlan, két esetet különböztetünk meg: $v \equiv 1 \pmod 4$ és $v \equiv 3 \pmod 4$.

1.eset: $v \equiv 1 \pmod 4$.

Négyesével írjuk fel a 6.4 Lemma és a (10) azonosság alapján az $n(x_i^2 + x_{i+1}^2+x_{i+2}^2+x_{i+3}^2)$ kifejezéseket négy négyzetszám összegeként. Legyen mondjuk $n = b_1^2+\dots+b_4^2$ és

$$(b_1^2+b_2^2+b_3^2+b_4^2)(x_i^2+x_{i+1}^2+x_{i+2}^2+x_{i+3}^2) = y_i^2+y_{i+1}^2+y_{i+2}^2+y_{i+3}^2.$$

A rövidség kedvéért írjunk $x_1+\dots+x_v$ helyett w-t. Ekkor az

$$L_1^2+\dots+L_v^2 = y_1^2+\dots+y_{v-1}^2 + nx_v^2 + \lambda w^2 \tag{12}$$

azonossághoz jutunk, ahol minden kifejezés az x-ek függvénye. Mivel a (10) azonosság mátrixos alakjában szereplő $x \to y$ hozzárendelés kölcsönösen egyértelmű, így az előző egyenlőséget tekinthetjük az y-ok (és x_v) kifejezésének, mégpedig minden szereplő kifejezés homogén és az együtthatók racionálisak. Olyan (racionális együtthatós) kifejezését fogjuk y_1-nek ebbe az azonosságba helyettesíteni, amely "rövidíti" azt. Nézzük meg, hogy L_1-ben, mint $y_1,\dots,y_{v-1}$, x_v homogén lineáris kifejezésében mi y_1 együtthatója. Ha ez nem 1, akkor fejezzük ki y_1-et az $L_1 = y_1$ egyenletből. Természetesen a megoldás $y_1 =$(a többi változó racionális együtthatós homogén lineáris kifejezése) alakban írható. Ha ezt behelyettesítjük (12)-be, akkor az

$$L_2^2+\dots+L_v^2 = y_2^2+\dots+y_{v-1}^2 + nx_v^2 + \lambda w^2 \tag{13}$$

egyenletet kapjuk, amelyben továbbra is minden az $y_2,\dots y_{v-1},x_v$ homogén lineáris kifejezése. Ha véletlen y_1 együtthatója 1 volt L_1-ben, akkor az $L_1 = y_1$ helyett az $L_1 = -y_1$ egyenletet oldjuk meg és helyettesítjük vissza (12)-be. Természetesen így is (13)-hoz jutunk.

A megrövidített egyenletre ezt az eljárást ismételjük: rendre megoldjuk az $L_2 = \pm y_2$, …, $L_{v-1} = \pm y_{v-1}$ egyenletek valamelyikét y_2, majd …, y_{v-1}-re. Ezeket a racionális együtthatós homogén lineáris kifejezéseket rendre visszahelyettesítve végül az

$$L_v^2 = nx_v^2 + \lambda w^2$$

egyenlethez jutunk, ahol most már L_v és w csupán x_v-től függ, mégpedig homogén módon, továbbá racionális együtthatósan, azaz L_v és w az x_v változó racionális számszorosa. Leosztva x_v^2-tel és felszorozva a nevezők legkisebb közös többszörösével valóban a $z^2 = nx^2 + \lambda y^2$ egy nem-triviális egész megoldásához jutunk.

2.eset: $v \equiv 3 \pmod 4$.

Először is vezessünk be egy x_{v+1} új változót és adjunk hozzá (11) mindkét oldalához nx_{v+1}^2-et. Így az alábbi egyenletet kapjuk:

$$L_1^2 + \ldots + L_v^2 + nx_{v+1}^2 = n(x_1^2 + \ldots + x_v^2 + x_{v+1}^2) + \lambda(x_1 + \ldots + x_v)^2. \quad (14)$$

Ez pontosan olyan, mint az 1. esetben kezelt egyenlet. Az ottani eljárást megismételve az

$$nx_{v+1}^2 = y_{v+1}^2 + \lambda w^2$$

egyenlethez jutunk, amiből az $nx^2 = z^2 + \lambda y^2$ egyenlet egy nem-triviális megoldását kapjuk. Ez most is pont az, ami kellett, mert $v \equiv 3 \pmod 4$ miatt $(-1)^{(v-1)/2} = -1$. ∎

A $\lambda = 1$ esetben (azaz projektív síkokra) nagyon könnyen kezelhető a Bruck–Chowla–Ryser feltétel. Ezt az eredményt korábban bizonyította Bruck és Ryser. Mielőtt a tételt kimondanánk, egy számelméleti állítást lássunk (ld. Turán Számelmélet jegyzet).

Lemma 6.6 *Egy pozitív egész szám pontosan akkor írható fel legfeljebb két négyzetszám összegeként, ha minden $4k+3$ alakú prímosztója páros kitevőn szerepel.* ∎

Tétel 6.7 *Ha létezik n-edrendű projektív sík és $n \equiv 1$ vagy $2 \pmod 4$, akkor n felírható két négyzetszám összegeként.*

Bizonyítás. Jegyezzük meg, hogy $v = n^2 + n + 1$ mindig páratlan, és $n \equiv 1$ vagy $2 \pmod 4$ pontosan akkor, ha $v \equiv 3 \pmod 4$. Ekkor a Bruck–Chowla–Ryser tétel azt mondja, hogy az $nx^2 = y^2 + z^2$ egyenletnek van nem-triviális megoldása. Mivel a jobboldalon a $4k+3$ alakú prímosztók páros kitevőn szerepelnek az előző lemma miatt, így ugyanez igaz n-re is, vagyis n is két négyzetszám összege. ∎

Megjegyzés 6.8 Mivel $n = 6$ nem két négyzetszám összege, így nem létezik 6-odrendű projektív sík. Persze ezt már Euler is "tudta", hisz nincs 6-odrendű ortogonális Latin négyzetpár. Az $n = 10$ mindmáig az egyetlen olyan érték, amely teljesíti a Bruck–Chowla–Ryser tétel feltételeit, mégsem létezik 10-edrendű projektív sík. Ezt a nyolcvanas évek végén igazolta számítógéppel Lam, Swiercz és Thiel.

A következőkben az lesz a célunk, hogy a $\mathrm{PG}_{n-1}(n,q)$ projektív tereket, mint négyzetes blokkrendszereket karakterizáljuk. A bizonyításokat elhagyjuk, a 6.1–3 Feladatokban az érdeklődő olvasó maga is megteheti.

A projektív terek jellemzéséhez először az "egyenes" fogalmát fogjuk bevezetni.

Definíció 6.9 Legyen p és q két különböző pontja a $\mathbf{D}$ blokkrendszernek. A két pont által meghatározott e_{pq} *egyenes* a két pontot tartalmazó blokkok metszete, azaz

$$e_{pq} = \bigcap_{p,q \in B \in \mathbf{B}} B.$$

Jegyezzük meg, hogy Steiner-rendszerekben maguk a blokkok az egyenesek. A következő állítás azt mutatja, hogy ezek az egyenesek jól definiáltak.

Állítás 6.10 *Blokkrendszerben egy egyenes bármely pontpárja egyértelműen meghatározza az egyenest.* ∎

Állítás 6.11 *Egy L egyenes méretére érvényes a $2 \le |L| \le (b-\lambda)/(r-\lambda)$ egyenlőtlenség. Továbbá $|L| = (b-\lambda)/(r-\lambda)$ pontosan akkor ha minden blokk metszi L-et.* ∎

Természetesen a projektív terekben ez a helyzet, minden hipersík metsz minden egyenest. Ha felidézzük a projektív tereket definiáló axiómákat, akkor sejthetjük, hogy valamiképpen a sík fogalmát is érdemes megfognunk. Ez a következőképpen történik.

Definíció 6.12 Legyen p, q, r a $\mathbf{D}$ blokkrendszer három olyan pontja, amelyek nincsenek egy egyenesen (azaz $r \notin e_{pq}$). A Π_{pqr} *sík* nem más, mint a három pontot tartalmazó blokkok metszete. (Ha ilyen nincs, akkor legyen a Π_{pqr} sík a teljes ponthalmaz.)

A $\mathrm{PG}_{n-1}(n,q)$ blokkrendszernek az az egyik jellemző tulajdonsága, hogy bármely három nem egy egyenesen fekvő pont egyértelműen meghatároz egy síkot. Ezt általában nem várhatjuk, csak 3-rendszerek esetében.

Tétel 6.13 (Dembowski–Wagner) *Ha $\mathbf{D}$ nem-triviális négyzetes $2-(v,k,\lambda)$-rendszer, akkor a következő állítások egyenértékűek:*

(a) $\mathbf{D} = PG_{n-1}(n,q)$ *valamely $n \ge 2$-re és q prímhatványra, vagy $\mathbf{D}$ projektív sík;*

(b) minden egyenes metsz minden blokkot;

(c) minden egyenes $(b-\lambda)(r-\lambda)$ pontú;

(d) minden sík ugyanannyi blokkban van benne. ∎

Korollárium 6.14 *Ha egy $\lambda > 1$ paraméterű négyzetes blokkrendszernek van a síkokon tranzitív automorfizmuscsoportja, akkor izomorf a $PG_{n-1}(n, q)$-val valamilyen $n > 2$-re.* ∎

Megjegyzés 6.15 A Dembowski–Wagner tételhez hasonló eredmények ismertek az affin terekre is, ezek kimondásától is eltekintünk.

Említsük meg azt, hogy a projektív terek jellemzéséhez a paraméterek ismeretén túl további feltétel is kell, amint azt az alábbi tétel mutatja.

Tétel 6.16 (Kantor) *Legyen q prímhatvány és $n > 2$ egész. Ekkor létezik olyan blokkrendszer, melynek paraméterei ugyanazok, mint $PG_{n-1}(n, q)$ paraméterei, mégsem izomorf vele.*

Bizonyítás. Ld. a 6.4. feladatot. ∎

A projektív síkok esete nem véletlenül maradt ki a tételből. Ismert például, hogy a 2,3,4,5,7 és 8-adrendű síkok izomorfia erejéig egyfélék, így ekkor nem is igaz a megfelelő tétel. Általában a véges geometriák egyik fontos megoldatlan problémája, hogy vannak-e más prímrendű síkok, mint a $\mathrm{PG}(2, p)$ síkok. Erről szinte semmi nem ismert. Ha viszont q prímhatvány és $q > 8$, akkor mindig vannak nem testre épített síkok is. $q = 9$-re pontosan ismerik is ezek számát: négy sík van. Ezt is a 10-edrendű síknál megismert Lam, Swiercz, Thiel trió látta be számítógéppel.

Természetes más megszorításokat tenni a blokkrendszerünkre, például az automorfizmuscsoportra. Ilyenek az alábbi tételek.

Tétel 6.17 (Kantor) *Legyen $\mathbf{D}$ olyan blokkrendszer, melynek paraméterei ugyanazok, mint $PG_{n-1}(n, q)$-é ($n > 2$). Ekkor $\mathbf{D} = PG_{n-1}(n, q)$ pontosan akkor, ha $Aut(\mathbf{D})$ 2-tranzitív a pontokon.* ∎

Tétel 6.18 (Ostrom–Wagner) *Egy projektív sík pontosan akkor izomorf a testre épített $PG(2, q)$ síkkal, ha automorfizmuscsoportja kétszeresen tranzitív a pontokon.* ∎

Megjegyzés 6.19 Olyan blokkrendszer, amelynek paraméterei $\mathrm{PG}_1(3, 2)$-ével megegyeznek, pontosan 80 van. Olyan blokkrendszer, melynek paraméterei megegyeznek $\mathrm{PG}_2(3, 2)$-ével 5 darab van.

6.1 HADAMARD-FÉLE BLOKKRENDSZEREK

A négyzetes blokkrendszerek egy másik fontos (végtelen) családja az Hadamard-féle blokkrendszerek családja.

Definíció 6.20 A négyzetes $2-(4\lambda+3, 2\lambda+1, \lambda)$ blokkrendszereket *Hadamard-féle blokkrendszer*nek hívjuk.

Definíció 6.21 Egy $n \times n$-es H mátrixot *Hadamard-mátrix*nak nevezünk, ha minden eleme ± 1 és $HH^T = nI$.

Természetesen $HH^T = nI$-ből $H^T H = nI$ is következik. Az elnevezés onnan származik, hogy Hadamard bizonyította az alábbi determináns-egyenlőtlenséget:

Ha egy $n \times n$-es mátrix elemeire $|a_{ij}| \leq 1$ teljesül, akkor $det(A) \leq n^{n/2}$ és egyenlőtlenség pontosan akkor áll, ha a mátrix Hadamard-féle.

Az állítás elég szemléletes, hisz $\det(A)$ a mátrix sorai által kifeszített parallelotóp térfogata. Minden sorvektor hossza legfeljebb $\sqrt{n}$ és a parallelotóp térfogata legfeljebb az élek hosszának szorzata. Az is látszik, hogy az egyenlőséghez szükséges, hogy minden élhossz $\sqrt{n}$ legyen, valamint hogy a sorok ortogonálisak legyenek egymásra.

Példa 6.22 A $\mathrm{PG}_{n-1}(n, 2)$ projektív tér Hadamard-féle blokkrendszer.

Példa 6.23 Az alábbi mátrixok

$$(1)\,, \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{és} \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Hadamard-mátrixok.

A példában szereplő első két mátrixot kivéve az Hadamard-mátrixok mérete néggyel osztható. Ehhez vegyük észre, hogy Hadamard-mátrix bármely sorát vagy oszlopát végigszorozhatjuk (-1)-gyel anélkül, hogy elrontanánk a $HH^T = nI$ egyenlőséget. Eszerint feltehető, hogy az Hadamard-mátrix első sora és oszlopa csupa $+1$-ből áll. Ugyanígy a sorok vagy oszlopok cseréje sem befolyásolja az Hadamard tulajdonságot, így azt is feltehetjük, hogy a második sorban (ha van ilyen) először $+1$-ek, majd -1-ek következnek. Mivel ez a sor ortogonális a csupa egyesből álló első sorra, így máris kapjuk, hogy $n = 2m$ és a második sor elején m darab $+1$-es és utána m darab -1-es szerepel. Ha van egy további sor, akkor legyen x az egyesek száma az első m pozícióban, y pedig az egyesek száma a második m pozícióban. Mivel a sor ortogonális az elsőre kapjuk, hogy $x + y = m$. A második sorral vett skaláris szorzat pedig $x + (-1)(m - x) - y + (m - y) = 0$. Ebből $x = y$ adódik, azaz $m = 2x$, vagyis n valóban osztható 4-gyel. Ezzel beláttuk az alábbi tételt:

Tétel 6.24 *Hadamard-mátrix rendje 1,2 vagy osztható 4-gyel.* ∎

Fontos megoldatlan sejtés, hogy minden néggyel osztható n-re létezik Hadamard-mátrix. Néhány direkt illetve rekurzív konstrukciót mi is látni fogunk. Pillanatnyilag a legkisebb olyan n, amelyre nem ismert $n \times n$-es Hadamard-mátrix $n = 428$.

A most következő tétel azt mutatja, hogy a fent definiált dolgok nem véletlenül kapták ugyanazt a nevet.

Tétel 6.25 *Pontosan akkor létezik $4n \times 4n$-es Hadamard-mátrix, ha van négyzetes $2-(4n-1, 2n-1, n-1)$ blokkrendszer.*

Bizonyítás. A 6.24 tétel előtti okoskodás szerint feltehető, hogy az első sor és oszlop csupa $+1$-ből áll. Töröljük ezt a sort és oszlopot és a maradékban a -1 helyett írjunk 0-t. Könnyen verifikálható, hogy így négyzetes blokkrendszer illeszkedési mátrixát kapjuk. A másik irányt a konstrukció megfordításával láthatjuk be. (ld. 6.5. Feladat). ∎

Jegyezzük meg, hogy izomorf Hadamard-féle blokkrendszerek ekvivalens mátrixokból származnak, de visszafelé ez nem igaz. A most következő rekurzív konstrukció nagyon egyszerű.

Állítás 6.26 *Ha H_n $n \times n$-es Hadamard-mátrix, H_m $m \times m$-es Hadamard-mátrix, akkor $H_n \otimes H_m$ is Hadamard-mátrix.*

Bizonyítás. Csupán a tenzorszorzat fogalmát kell felidézni (ld. 6.6. Feladat). ∎

Elindulva egy 2×2-es Hadamard-mátrixból és ezt önmagával tenzorszorozva minden 2-hatványra kapunk Hadamard-mátrixot. Ez a Sylvester-konstrukció, melyről könnyű látni, hogy a neki megfelelő Hadamard blokkrendszer éppen a $\mathrm{PG}(n,2)$ projektív tér (ld. 6.7. Feladat).

Most lássunk egy véges testeket használó direkt konstrukciót.

Példa 6.27 Legyen $q \equiv 3 \pmod 4$ prímhatvány. Legyen F a q elemű véges test ($\mathrm{GF}(q)$), és S a nem-nulla négyzetelemek halmaza ("kvadratikus maradékok"). Definiáljuk a $\mathbf{D} = (\mathbf{P}, \mathbf{B})$ blokkrendszert a következőképpen:

Legyen $\mathbf{P} = F$, $\mathbf{B} = \{S + x \ : \ x \in F\}$. Ezt *Paley-féle* blokkrendszernek nevezik.

Nem magától értetődő, de megmutatható (ld. 6.8. Feladat), hogy így blokkrendszert kapunk. A paraméterek: $v = q$, $k = (q-1)/2$, $\lambda = (q-3)/4$. (Ez utóbbi az, aminek a meghatározása nem triviális.)

Mivel 12 az a legkisebb rend, amelyre nem lehet a Sylvester konstrukcióval Hadamard-mátrixot gyártani, így erre az esetre konkrétan megadjuk a Paley-konstrukcióval kapható Hadamard-mátrixot.

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\
1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\
1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\
1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\
1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 \\
1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1
\end{pmatrix}.$$

Mielőtt rátérnénk a bisíkok ismertetésére, jegyezzük meg, hogy az Hadamard-féle blokkrendszerek mutatják, hogy a 6.3 Állításban az alsó becslés végtelen sokszor pontos.

6.2 BISÍKOK

Mindezidáig $\lambda = 1$ az egyetlen olyan rögzített λ, amelyre végtelen sok ilyen λ-jú négyzetes blokkrendszert ismerünk. A következő esetben, azaz ha $\lambda = 2$, már csak néhány példát ismerünk. Egy $\lambda = 2$ paraméterű négyzetes blokkrendszert *bisík*nak szoktak nevezni. $k = 3, 4, 5$-re pontosan egy ilyen bisík létezik. $k = 6$-ra pontosan három, $k = 9$-re négy, míg $k = 11$-re csak annyit tudunk, hogy legalább négy nem-izomorf bisík van. $k = 13$-ra pedig csak két nem-izomorf bisíkot ismerünk. Ez a teljes listája a ma ismert összes bisíknak, sem azt nem tudjuk, hogy van-e végtelen sok, sem azt, hogy olyan rendekre, amelyekre aritmetikailag létezhet bisík, arra létezik-e. Természetesen az általános négyzetes blokkrendszerekre vonatkozó szükséges feltételek itt is érvényesek, és a következőt adják.

Korollárium 6.28 *Ha $k \equiv 2$ vagy $3 \pmod 4$, akkor $n = k - 2$ négyzetszám kell legyen. Ha $k \equiv 0$ vagy $1 \pmod 4$, akkor az*

$$x^2 = ((k-2)y^2 + (-1)^{k(k-1)/4} 2z^2$$

diofantoszi egyenletnek létezik nem-triviális egész megoldása. ∎

Korollárium 6.29 *Ha $n(= k-2) \leq 11$, akkor $n = 1, 2, 3, 4, 7, 9$ vagy 11.*

A bizonyítást ld. a 6.9. Feladatban. ∎

Lássunk most egy elemi, de igen hasznos módszert bisíkok vizsgálatára. A módszer Hussaintól származik, és a bisíkok létezését egyszerű szerkezetű gráf-családok létezésére vezeti vissza.

Legyen tehát **B** bisík, p egy pontja, B pedig egy p-n át nem menő blokk. Definiálunk egy $\Gamma(p)$ gráfot a következőképpen: legyenek a pontok B pontjai, az $x, y \in B$ pontokat pedig kössük össze éllel, ha az x, y pontokon átmenő (B-től különböző) blokk tartalmazza p-t. Mivel két ponton pontosan két blokk megy át, így valóban egy egyszerű gráfot definiáltunk B pontjain. Ha ezeket a $\Gamma(p)$ gráfokat az összes $p \notin B$-re tekintjük, akkor a bisík *Hussain gráfjait* kapjuk. Ezek az alábbi tulajdonságokkal rendelkeznek:

Tétel 6.30 *Ha* **D** *olyan bisík, melynek blokkmérete k, akkor egy rögzített B blokkhoz tartozó Hussain gráfok rendszere (mely az összes $p \notin B$-re van definiálva, és így $(k-1)(k-2)/2$ gráfból áll) eleget tesz az alábbiaknak:*

1. *valamennyi gráf másodfokú reguláris,*
2. *két különböző gráfnak pontosan két közös éle van.*

Bizonyítás. Tekintsük egy gráf egy x pontját. Ez akkor van az $y \in B$ ponttal összekötve, ha x, y és p egy blokkban vannak. Mivel x-en és p-n pontosan két blokk megy át, így adott x-hez pontosan két y szomszédot találunk. Ha két különböző gráfot (pl. a p és q pontokhoz tartozókat) tekintünk, akkor ezeknek a közös élei a p, q pontokat tartalmazó két blokknak B-vel való metszéspontjai alkotta élek lesznek. ∎

Megfordítva, könnyű azt is belátni, hogy ha k csúcson meg tudunk adni $(k-1)((k-2)/2$ olyan gráfot, amelyek teljesítik a fenti tétel két feltételét, akkor azok bisíkot határoznak meg (ld. 6.10. Feladat).

A következő $k = 4$-re megadott Hussain-gráf rendszer mutatja a 2-rendű bisík létezését. Az egyértelműséget is könnyű látni ezen a módon (ld. 6.11. Feladat),

a szóbanforgó bisík a Fano-sík komplementere. $k = 5$-re a $\lambda = 2$-höz tartozó Hadamard-blokkrendszer egyben bisík is. Az unicitás igazolása és a Hussain gráfok rendszerének felrajzolása a 6.12. Feladat, a gráfokat azért mi is megadjuk:

$k = 6$-ra Hussain megmutatta, hogy pontosan három nem-izomorf Hussain gráf rendszer van. A szóbanforgó bisíkok konstrukciójára az erősen reguláris gráfok és blokkrendszerek kapcsolatáról szóló részben visszatérünk.

6.3 Feladatok.

6.1., Lássuk be 6.9-at.
6.2., Lássuk be 6.10-et.
6.3., Lássuk be 6.12-et.
6.4., Lássuk be 6.16-et.
6.5., Ha létezik Hadamard-féle blokkrendszer, akkor létezik Hadamard-mátrix is, és megfordítva.
6.6., Két Hadamard mátrix tenzorszorzata (másszóval Kronecker-szorzata) is az.
6.7., Mutassuk meg, hogy a kételemű Hadamard-mátrix önmagával vett tenzorszorzatának megfelelő Hadamard blokkrendszer izomorf PG$(n, 2)$-vel.
6.8., Lássuk be, hogy a Paley konstrukció Hadamard-mátrixot ad.
6.9., Bisíkokra $n \leq 11$-ből $n = 1, 2, 3, 4, 7, 9$ vagy 11.
6.10., Hussain gráfokból bisíkot kapunk.
6.11., $k = 4$ egyértelműség Hussain gráfokkal.
6.12., $k = 5$ egyértelműség Hussain gráfokkal.

7 BLOKKRENDSZEREK KONSTRUKCIÓJA MÁS BLOKKRENDSZEREKBŐL

Definíció 7.1 *(A derivált rendszer)* Legyen p a $\mathbf{D} = (\mathbf{P}, \mathbf{B}, \in)$ $t-(v,k,\lambda)$-rendszer egy pontja és legyen $\mathbf{P}_p = \mathbf{P} \setminus \{p\}$, $\mathbf{B}_p = \{L \in \mathbf{B} \ : \ p \in L\}$. Ekkor $\mathbf{D}_p = (\mathbf{P}_p, \mathbf{B}_p, \in)$ $(t-1)-(v-1,k-1,\lambda)$-rendszer lesz (az ellenőrzést ld. 7.1. feladatban). Ezt hívjuk $\mathbf{D}$ p pontra vonatkozó *derivált rendszer*ének.

Definíció 7.2 *(A pont-reziduális rendszer)* Legyen p a $\mathbf{D} = (\mathbf{P}, \mathbf{B}, \in)$ $t-(v,k,\lambda)$-rendszer egy pontja és legyen $\mathbf{P}^p = \mathbf{P} \setminus \{p\}$, $\mathbf{B}^p = \{L \in \mathbf{B} \ : \ p \notin L\}$. Ekkor $\mathbf{D}^p = (\mathbf{P}^p, \mathbf{B}^p, \in)$ $(t-1)-(v-1,k,\lambda')$-rendszer lesz, ahol $\lambda' = \lambda(v-k)/(k-t+1)$ (az ellenőrzést ld. 7.2. Feladatban). Ezt hívjuk $\mathbf{D}$ p pontra vonatkozó *pont-reziduális rendszer*ének.

Definíció 7.3 *(A blokk-reziduális rendszer)* Legyen B a $\mathbf{D} = (\mathbf{P}, \mathbf{B}, \in)$ négyzetes blokkrendszer egy blokkja és legyen ${}^B\mathbf{P} = \mathbf{P} \setminus B$, ${}^B\mathbf{B} = \mathbf{B} \setminus \{B\}$. Ekkor ${}^B\mathbf{D} = ({}^B\mathbf{P}, {}^B\mathbf{B}, \in)$ is $2-(v',k',\lambda)$ blokkrendszer lesz, ahol $v' = v-k$, $k' = k-\lambda$ (a további paraméterek $r' = r$, $b' = b-1$, az ellenőrzést ld. 7.3. Feladatban). Ezt hívjuk $\mathbf{D}$ B blokkra vonatkozó *blokk-reziduális rendszer*ének.

Ezek a konstrukciók nem nagyon hasznosak, mert nagyobb rendszerből készítenek kisebbet. Sokkal érdekesebb, hogy vajon ezek megfordíthatók-e. Mielőtt erre rátérnénk, lássunk néhány példát.

Példa 7.4 $\mathrm{PG}_1(n,q)$ derivált rendszere egy $q^n + \ldots + q$ pontú q-uniform, reguláris hipergráf. A pont-reziduális rendszer $(q+1)$-uniform hipergráf, amely szintén reguláris (mi a pontok foka? ld. 7.4. Feladatot).

$\mathrm{AG}_2(n,2)$ derivált rendszere $\mathrm{PG}_1(n-1,2)$, a pont-reziduális rendszer pedig egy blokkrendszer $2-(2^{n-1}, 4, 2^{n-1}-2)$ paraméterekkel. (ld. 7.5. Feladat.)

Példa 7.5 A $\mathrm{PG}_{n-1}(n,q)$ blokkreziduálisa éppen $\mathrm{AG}_{n-1}(n,q)$. Ez a motiváló példa a blokkreziduális konstrukcióra.

Ha egy blokkrendszer keletkezhet valami másik blokkrendszer blokkreziduálisaként, akkor $k + \lambda - r = 0$ teljesül rá. Egy ennek a feltételnek eleget tevő blokkrendszert *kvázireziduális*nak szoktak nevezni. A fő kérdés természetesen az, hogy mikor lesz egy kvázireziduális blokkrendszer valaminek a reziduálisa. Erről részletesebben a 8. Fejezetben lesz szó.

A legérdekesebb a deriválás megfordítása: Ha adott egy $t-(v,k,\lambda)$-rendszer, található-e olyan $(t+1)-(v+1,k+1,\lambda)$-rendszer, amelynek ő a deriváltja.

Definíció 7.6 Ha $\mathbf{D}$ derivált rendszere (valamely pontjára) $\mathbf{E}$, akkor $\mathbf{D}$-t az $\mathbf{E}$ *bővítésének* nevezzük. Ha $\mathbf{E}$-nek van bővítése, akkor *bővíthetőnek* nevezzük.

Állítás 7.7 *Ha egy $t-(v,k,\lambda)$-rendszer bővíthető, akkor $k+1$ osztja $b(v+1)$-et.*

Bizonyítás. A bővítésben egy pont foka éppen b, egy blokk mérete $k+1$, a pontok száma pedig $(v+1)$ ahonnan az állítás 1.15 szerint azonnal adódik. ∎

Az affin síkok mindig eleget tesznek a bővíthetőségi feltételnek, a projektív síkok azonban általában nem.

Állítás 7.8 *Ha egy n-edrendű projektív sík bővíthető, akkor $n = 2, 4$.*

Bizonyítás. Az előző oszthatósági feltételből $n+2$ osztója kell legyen $(n^2+n+1)(n^2+n+2)$-nek. Kis számolással kapjuk, hogy ekkor $n+2$ osztója 12-nek, azaz $n = 2, 4$, vagy 10. Mivel 10-edrendű projektív sík nem létezik, a bizonyítást befejeztük. ∎

Az $n = 2$ eset elég egyszerű: ekkor a Fano-sík egyben Hadamard-féle blokkrendszer, így bővíthető is (ld. majd a 7.10 állítást). Azt is beláthatjuk, hogy a bővítés egyértelmű.

Az affin síkok és a $\mathrm{PG}(2,4)$ projektív sík bővítésére a Golay kódokról szóló 10. fejezetben részletesebben visszatérünk.

Általánosságban négyzetes blokkrendszerek bővítéséről a következő mondható.

Tétel 7.9 (Cameron) *Ha egy nem-triviális négyzetes $2-(v,k,\lambda)$ blokkrendszer bővíthető, akkor az alábbi lehetőségek valamelyike teljesül:*

(a) $v = 4\lambda + 3$, $k = 2\lambda + 1$, *azaz a blokkrendszer Hadamard-féle.*

(b) $v = (\lambda+2)(\lambda^2+4\lambda+2)$, $k = \lambda^2 + 3\lambda + 1$,

(c) $v = 495$, $k = 39$, $\lambda = 3$.

Bizonyítás. Mivel a bizonyítás elég hosszú, röviden összefoglaljuk a lényegét: először a bővíthetőségből származó oszthatósági feltételt nézzük meg, majd definiálunk egy segéd-blokkrendszert, amelyből egy további oszthatósági feltételt kapunk. Végül erre a segéd-blokkrendszerre a Fisher-egyenlőtlenséget alkalmazva korlátozzuk a lehetséges paraméter-értékeket.

Legyen $\mathbf{D}$ az eredeti, $\mathbf{D}^*$ a bővített blokkrendszer. Ez utóbbi egy $3-(v+1, k+1, \lambda)$-rendszer, így blokkjainak száma $b^* = v(v+1)/(k+1)$ (ld. 1.15 Köv.). Mivel $\mathbf{D}$ négyzetes, így $v = (k^2-k+\lambda)/\lambda$, amit behelyettesítve

$$b^* = \frac{(k^2-k+\lambda)(k^2-k+2\lambda)}{\lambda^2(k+1)}$$

adódik, s ebből a $k+1|(k^2-k+\lambda)(k^2-k+2\lambda)$ oszthatósági feltételt kapjuk. Mindkét oldalt modulo $(k+1)$ tekintve ebből az derül ki, hogy

$$k+1 \text{ osztja } 2(\lambda+1)(\lambda+2)\text{-t.}$$

Definiáljunk egy újabb **D'** blokkrendszert $\mathbf{D}^*$ segítségével. Ehhez jegyezzük meg, hogy $\mathbf{D}^*$-ban két blokk vagy 0, vagy pontosan $\lambda+1$ pontban metszi egymást. Valóban, ha két blokk metszi egymást akkor a metszésponthoz tartozó derivált rendszer négyzetes $2-(v,k,\lambda)$-rendszer lesz, azaz ebben két blokk pontosan λ pontban metszi egymást (ld. 4.4). (Említsük meg, hogy nem okvetlenül kapjuk vissza **D**-t!).

Rögzítsük $\mathbf{D}^*$ egy Y blokkját. A **D'** illeszkedési struktúra pontjai az Y-ra nem illeszkedő pontok, a blokkok pedig az Y-t nem metsző $\mathbf{D}^*$-beli blokkok. Megmutatjuk, hogy ez blokkrendszer lesz. Azt kell belátnunk, hogy két különböző ponton (A és B) mindig ugyanannyi blokk megy át. Ehhez számoljuk meg a **D'**-ből "kimaradó" blokkokat, vagyis a (Q,X) párokat, ahol Q az Y egy pontja X pedig az A,B,Q-t tartalmazó $\mathbf{D}^*$-beli blokk. Ez egyrészt az A,B-n átmenő blokkok száma szorozva $(\lambda+1)$-gyel, másrészt viszont X-et $(k+1)$-féleképpen választhatjuk, és A,B,X-en λ blokk megy (amelyek automatikusan metszik Y-t). Így $m(\lambda+1)=(k+1)\lambda$. Ebből $m=\lambda(k+1)/(\lambda+1)$, azaz **D'**-ben két ponton $k-m=(k-\lambda)/(\lambda+1)$ blokk megy át. (Ehhez még arra kell emlékeznünk, hogy a bővítésben két pontra annyi blokk illeszkedik, mint ahány blokk egy ponton megy át **D**-ben.) Ráadásként az is kiderült, hogy

$$(\lambda+1) \quad \text{osztja} \quad (k+1)\text{-et.}$$

Megkaptuk a beígért két oszthatósági feltételt, még egy egyenlőtlenséget írunk fel **D** paramétereire a Fisher-egyenlőtlenség segítségével. Ha **D'** degenerált, azaz egyetlen blokkja van, akkor $v=2k+1$. A $v=(k^2-k+\lambda)/\lambda$ összefüggésből $k=2\lambda+1$ adódik, azaz **D** Hadamard-féle blokkrendszer. Ha $v>2k+1$, akkor $\mathbf{D}'$ nem-degenerált, azaz alkalmazható rá a Fisher-egyenlőtlenség, azaz

$$\frac{k-\lambda}{\lambda+1}\cdot\frac{(v-k)(v-k-1)}{(k+1)k}\geq v-k.$$

(Itt a bal oldalon megint használtuk a blokkok számát megadó 1.15 Állítást.) Behelyettesítve $v=(k^2-k+\lambda)/\lambda$-t, azt kapjuk, hogy

$$(k-\lambda)(k\lambda-1)\geq\lambda(\lambda+1)(k+1).$$

Kis számolással ebből az adódik, hogy

$$k+1\geq(\lambda+1)(\lambda+2).$$

Most felhasználjuk, hogy $\lambda+1$ osztja $(k+1)$-et, mondjuk $k+1=s(\lambda+1)$. Visszaemlékezve az első oszthatósági feltételre látjuk, hogy s osztja $2(\lambda+2)$-t.

A legutolsó egyenlőtlenség szerint viszont $s\geq\lambda+2$, azaz két lehetőségünk van $s=\lambda+2$ vagy $s=2(\lambda+2)$. Ha $s=\lambda+2$, akkor $k=\lambda^2+3\lambda+1$, és ez éppen a (b) eset a bizonyításban. A másik esetben kicsit tovább is tudunk menni.

Ha $s=2(\lambda+2)$, akkor $k=2\lambda^2+6\lambda+3$. Mivel **D** négyzetes, így λ osztja $k(k-1)$-et, amiből kis számolással (mod λ), $\lambda|6$ következik. Ha $\lambda=1$, akkor a paraméterek 10-edrendű projektív sík paraméterei, ami viszont nem létezik. (Az igazsághoz tartozik, hogy azt, hogy nincs bővíthető projektív sík, jóval hamarabb belátták, mint azt, hogy egyáltalán nincs 10-edrendű projektív sík.) A $\lambda=2,6$ esetekben v páros, de nem négyzetszám lenne, ami 6.1 szerint lehetetlen. Egyedül a $\lambda=3$, $k=39$, $v=495$ eset marad, ami a (c) lehetőség a tételben. ∎

Végezetül megemlítjük, hogy a (b) esetben Bagchi egy 1988-as eredménye szerint $\lambda\neq2$.

A bizonyításból Hadamard-féle blokkrendszerek bővítéséről is kiolvashatunk érdekes információkat.

Tétel 7.10 *Az Hadamard-féle blokkrendszereknek egyértelmű bővítése van.*

Bizonyítás. Azt a Cameron-tétel bizonyításából kiolvashatjuk, hogy a bővítésben a blokkok komplementumait kell hozzávenni a blokkok halmazához, ami pont azt jelenti, hogy a bővítés egyértelmű. Képletben a $\mathbf{D}=(\mathbf{P},\mathbf{B})$-ből a $\mathbf{D}^*=(\mathbf{P}\cup\{\infty\},\mathbf{B}^*)$ bővítést kapjuk, ahol

$$\mathbf{B}^*=\{B\cup\{\infty\},\mathbf{P}\setminus B\ :\ B\in\mathbf{B}\}.$$

Így csak azt kell ellenőriznünk, hogy ezen a módon tényleg 3-rendszer keletkezik. Magyarán szólva azt kell kiszámolnunk, hogy az eredeti Hadamard-blokkrendszerben három ponthoz hány olyan blokk van, amely nem megy át rajtuk. Az 5.1. Feladatban általában is megmutattuk, hogy egy t-rendszerben a $t+1$ pontot elkerülő blokkok száma csak a t-rendszer paramétereitől, valamint a $t+1$ ponton átmenő blokkok számától függ. A konkrét esetben, ha c_3 jelöli a mindhárom ponton átmenő blokkok számát, c_0 az elkerülő blokkokét, akkor a szita-formula segítségével azt kapjuk, hogy

$$c_0=b-3r+3\lambda-c_3.$$

Behelyettesítve $b=4\lambda+3$-at, $r=2\lambda+1$-et azonnal adódik, hogy $c_0+c_3=\lambda$, de c_0+c_3 éppen a bővítésben a három ponton átmenő blokkok száma. ∎

Még egy további érdekes blokkrendszer család van, amelynek elemei bővíthetők, ez az affin síkok családja. Az $\mathrm{AG}(2,q)$ affin sík bővítése az ú.n. *inverzív sík*, amelyet a következőképpen lehet elképzelni. Vegyünk a 3-dimenziós $\mathrm{AG}(3,q)$ térben egy elliptikus másodrendű felületet. Intuitíve "gömböt" érdemes elképzelni. Ennek q^2+1 pontja van. Legyenek a blokkok ennek a gömbnek a síkmetszetei (persze az egypontú metszeteket nem tekintjük). Minden ilyen síkmetszet "kör" (vagyis irreducibilis kúpszelet), azaz a blokkok $q+1$ pontúak. Három ponton átmegy egy és csak egy sík, a neki megfelelő blokk lesz a három ponton átmenő blokk. Két további érdekes megjegyzés: Thas megmutatta, hogy $\mathrm{AG}(2,q)$ bővítése egyértelmű. Másrészt viszont nem ismert olyan nem testre épített affin sík, amely bővíthető lenne. Az esetleg ismeretlen fogalmakról az 1.1 szakaszban olvashatunk.

7.1 NÉGYZETES BLOKKRENDSZEREK POLARITÁSAI

Ebben a rövid szakaszban azt vizsgáljuk meg, hogy egy négyzetes blokkrendszer polaritásának hány autokonjugált pontja lehet. Emlékeztetünk arra, hogy polaritásnak bijektív, illeszkedéstartó, pontot blokkba, blokkot pontba vivő leképezést neveztünk. Polaritás persze csak akkor létezhet, ha a blokkrendszer izomorf a duálisával.

Mint azt az első fejezetben már láttuk, a blokkrendszernek pontosan akkor van polaritása, ha van szimmetrikus illeszkedési mátrixa. Legyen A egy ilyen szimmetrikus illeszkedési mátrix ($A=A^T$). Ebben az esetben a 2-struktúrákat leíró mátrix-egyenlet az alábbi alakot ölti:

$$A^2=\lambda J+\mathrm{diag}(\deg(p_i)-\lambda).$$

Mivel $\det(A^2-xI)=\det((A-\sqrt{x}I)(A+\sqrt{x}I))=\det(A-\sqrt{x}I)\cdot\det(A+\sqrt{x}I)$, azonnal láthatjuk az alábbi észrevételt.

Állítás 7.11 *Az A szimmetrikus illeszkedési mátrix sajátértékei éppen a $\lambda J+$ diag$(\deg(p_i)-\lambda)$ mátrix sajátértékeinek négyzetgyökei.* ∎

Blokkrendszerekre viszont lényegében már meghatároztuk a sajátértékeket (ld. 4.3 Köv.), az eredményt most csak megismételjük.

Állítás 7.12 *Legyen A a $\mathbf{D}$ négyzetes blokkrendszer illeszkedési mátrixa. Ekkor AA^T sajátértékei k^2 (1 multiplicitással), valamint $n=k-\lambda$, $v-1$ multiplicitással.* ∎

Definíció 7.13 Legyen σ a $\mathbf{D}$ négyzetes blokkrendszer polaritása. A p pontot (B blokkot) *autokonjugált*nak nevezzük, ha illeszkedik a p^σ blokkra (B^σ pontra).

Könnyen látható, hogy ez pontosan azt jelenti, hogy az A mátrix p ponthoz tartozó diagonális eleme 1, vagyis az autokonjugált pontok száma megegyezik A nyomával, $\mathrm{tr}(A)$-val. Mivel a nyom másrészt a sajátértékek összege, beláthatjuk a következő állítást.

Tétel 7.14 *Legyen $\mathbf{D}$ négyzetes (v,k,λ)-blokkrendszer, σ egy polaritása. σ autokonjugált pontjainak száma*

$$k+s\sqrt{n}-(v-1-s)\sqrt{n},\quad \textit{alakú, ahol}\quad \frac{1}{2}(v-1-\frac{k}{\sqrt{n}})\le s\le v-1.$$

Bizonyítás. 7.11 miatt A sajátértékei csupán k, $-k$ $\sqrt{n}$ és $-\sqrt{n}$ lehetnek, mivel A^2 sajátértékei k^2 és n. k^2 multiplicitása 1, és $\mathbf{j}$ sajátvektora A-nak mégpedig k sajátértékkel, így $\mathbf{j}$ multiplicitása 1, és $-k$ nem sajátértéke A-nak. Ha $\sqrt{n}$ multiplicitása s, akkor $-\sqrt{n}$ multiplicitása $v-1-s$, amiből az egyenlőtlenség jön. Az s-re vonatkozó feltételekből $s\le v-1$ triviális, a másik pedig abból következik, hogy az autokonjugált pontok száma nem-negatív. ∎

Korollárium 7.15 *1) Ha n nem négyzet, akkor v páratlan és a polaritásnak k fixpontja van.*

2) Ha σ-nak nincs autokonjugált pontja, akkor n négyzet és $\sqrt{n}$ osztja λ-t.

Bizonyítás. Az eddigiek alapján feladatnak hagyjuk (ld. 7.6. Feladat.). ∎

Jegyezzük meg, hogy q-adrendű projektív síkokra ebből következik, hogy minden polaritásnak van autokonjugált pontja, továbbá, hogy nem négyzetrendű sík polaritásának $q+1$ autokonjugált pontja van. Projektív síkokra mindig ez a helyzet, legalább $q+1$ autokonjugált pont van. A másik egyenlőtlenség is lényegesen javítható projektív síkokra, legfeljebb $q\sqrt{q}+1$ autokonjugált pont van. Mindkét extrém eset elő is fordul (legalábbis az ismert síkokon).

7.2 Feladatok.

7.1., Ellenőrizzük, hogy a derivált blokkrendszer valóban blokkrendszer.

7.2., Ellenőrizzük, hogy a pont-reziduális blokkrendszer valóban blokkrendszer.

7.3., Ellenőrizzük, hogy a blokk-reziduális blokkrendszer valóban blokkrendszer.

7.4., Mi $\mathrm{PG}(n,q)$ derivált rendszere ill. pont-reziduális rendszere; mik a pontok foka, stb.

7.5., $\mathrm{AG}_2(n,2)$ deriváltja $\mathrm{PG}_1(n-1,2)$. Mi a pont-reziduális rendszere?

7.6., Lássuk be Köv. 7.15-öt.

7.7., Felhasználva azt, hogy az (x_1, x_2, x_3) pontnak megfeleltetve az $[x_1, x_2, x_3]$ egyenest a $\mathrm{PG}(2,q)$ projektív sík egy polaritását kapjuk, (ha q páratlan), konstruáljuk olyan q^2+q+1 pontú gráfot, amelyben nincsen négyszög és $(q^2+q-1)(q+1)/2$ éle van.

(Megjegyzés: Füredi belátta, hogy ennél nem is lehet több.)

8 ERŐSEN REGULÁRIS GRÁFOK

Ebben a fejezetben további magyarázat nélkül használjuk a szokásos gráfelméleti terminológiát. Az előforduló gráfok hurok és többszörös él nélküliek, ezt a továbbiakban nem hangsúlyozzuk külön.

Jelölés 8.1. Ha x csúcsa a G gráfnak, akkor $G(x)$-szel fogjuk jelölni az x-szel összekötött csúcsok halmazát (az x-et magát nem beleértve).

Definíció 8.1 A Γ gráfot (n,k,λ,μ) *paraméterű erősen reguláris* gráfnak nevezzük, ha a csúcsok száma n, a gráf k-adfokú reguláris, két összekötött pont közös szomszédainak száma λ, két összekötetlen ponté pedig μ.

Állítás 8.2 *Ha létezik (n,k,λ,μ) paraméterű erősen reguláris gráf, akkor*

$$k(k-\lambda-1) = (n-k-1)\mu.$$

Bizonyítás. Rögzítsünk egy x csúcsot és számoljuk meg kétféleképpen az $\{y,z\}$ éleket, ahol y össze van kötve x-szel, z pedig nincs. ∎

Állítás 8.3 *Erősen reguláris gráf komplementere is erősen reguláris.*

Bizonyítás. Legyen Γ egy (n,k,λ,μ) paraméterű erősen reguláris gráf. Nyilván $\bar{\Gamma}$-nak is n csúcsa van, $(n-1-k)$-adfokú reguláris. A $\bar{\lambda}$ meghatározásához azt kell megszámolnunk, hogy Γ-ban két nem szomszédos ponthoz hány olyan csúcsot találunk, amelyek egyikkel sincsenek összekötve. Ez $(n-k-2)-(k-\mu) = n-2k+\mu-2$, ami valóban nem függ a csúcsok választásától. Hasonlóan kapjuk, hogy $\bar{\mu} = n-2k+\lambda$. ∎

Megjegyzés 8.4 Ez újabb szükséges feltételt ad: t.i. $n \geq 2k-\mu+2$ és $n \geq 2k-\lambda$ kell legyen.

Hasonlóan a blokkrendszerekhez itt is az lesz a fő kérdés, hogy egyrészt a paraméterekre minél több megszorítást találjunk, másrészt pedig a szükséges feltételek szűrőjén átment paraméter-halmazokra konstruáljunk is erősen reguláris gráfot.

Mielőtt folytatnánk a szükséges feltételek keresését, lássunk néhány példát:

Példa 8.5 A $T(m)$ *trianguláris gráf* ($m \geq 4$): csúcsai egy m elemű halmaz 2-elemű részhalmazai, két ilyet összekötünk, ha nem diszjunktak. Az előző ábrán is látható *Petersen gráf* $T(5)$ komplementere. $T(m)$ erősen reguláris, paraméterei

$$n = m(m-1)/2, \quad k = 2(m-2), \quad \lambda = m-2, \quad \mu = 4.$$

Példa 8.6 Az $L_2(m)$ *négyzetháló gráf* nem más, mint $K_m \oplus K_m$, azaz csúcsai a (v, v') párok, ahol $v, v' \in V$, ($|V| = m$) és két különböző csúcsot pontosan akkor kötünk össze, ha valamelyik koordinátában megegyeznek. $L_2(m)$ is erősen reguláris, paraméterei

$$n = m^2, \quad k = 2(m-1), \quad \lambda = m-2, \quad \mu = 2.$$

Ezeket a gráfokat úgy is lerajzolhatjuk, hogy csak a tartalmazott klikkeket rajzoljuk le egy vonallal, és úgy képzeljük, hogy egy folyamatos vonalon belül bármely két pont össze van kötve. Az ábra $L_2(4)$-et és $T(6)$-ot mutatja:

Jegyezzük meg, hogy a 7.2 Következményben $u = 2, 3$-ra éppen $L_2(3)$ és $T(6)$ komplementere szerepel.

Példa 8.7 r darab diszjunkt m pontú teljes gráf (K_m) uniója erősen reguláris, a paraméterek:

$$n = rm, \quad k = m-1, \quad \lambda = m-2, \quad \mu = 0.$$

Ezt a gráfot rK_m-mel fogjuk jelölni. $\mu = 0$-ra minden erősen reguláris gráf ilyen (alkalmas r, m-re, ld. 8.5. Feladat). Ugyancsak erősen reguláris rK_m komplementere, azaz az r osztályú teljes Turán-gráf (az osztályok mérete m). Az rK_2 speciális esetben a gráfot *létrá*nak, komplementerét *koktél parti gráf*nak szokás nevezni és ezt a komplementert $CP(r)$-rel jelöljük.

További példák még később is szerepelni fognak, most azonban térjünk rá a szükséges feltételek vizsgálatára.

Legyen A a Γ adjacencia-mátrixa. Csak emlékeztetőül: $a_{ij} = 1$ ha az i-edik és j-edik csúcs szomszédok, különben 0. Idézzük fel azt is, hogy A^s-ben az (i, j) elem az i-edik és j-edik csúcs közti s hosszúságú utakat számolja (ld. 8.6. Feladatot is).

Ha Γ (n, k, λ, μ) paraméterű erősen reguláris gráf, akkor A^2 nagyon egyszerű szerkezetű: a főátlóban k-k állnak, a főátlón kívül pedig λ-k illetve μ-k, aszerint, hogy a két pont össze volt-e kötve Γ-ban. Ha I jelöli az egységmátrixot, J pedig a csupa egyesből álló mátrixot, akkor tehát

$$A^2 = kI + \lambda A + \mu(J - I - A). \tag{15}$$

A gráf regularitása is felírható mátrixosan:

$$AJ = JA = kJ. \tag{16}$$

Érdemes megemlíteni, hogy ezek az egyenletek pontosan leírják az erősen reguláris gráfokat, azaz ha egy gráf adjacencia-mátrixa eleget tesz ezeknek az egyenleteknek, akkor az erősen reguláris.

Lineáris algebrából tudjuk, hogy felcserélhető szimmetrikus mátrixok egyszerre diagonalizálhatók (egy ortogonális mátrixszal). Ilyenek esetünkben A és J. A csupa egyesből álló $\mathbf{j}$ vektor A-nak és J-nek is sajátvektora, a megfelelő sajátértékek k és n. Alkalmazva $\mathbf{j}$-re (15)-öt azt kapjuk, hogy

$$k(k - \lambda - 1) = (n - k - 1)\mu,$$

amit más módon már beláttunk 8.1-ban. Vegyük A egy további sajátvektorát, ami másik ϱ sajátértékhez tartozik. Egy ilyen $\mathbf{v}$ sajátvektor $\mathbf{j}$-re merőleges, így J-nek is sajátvektora, 0 sajátértékkel. Alkalmazva (15)-öt $\mathbf{v}$-re azt kapjuk, hogy

$$\varrho^2 = (k - \mu) + (\lambda - \mu)\varrho. \tag{17}$$

Ez az egyenlőség másodfokú egyenletet ad ϱ-ra. A két gyököt r-rel és s-sel fogjuk jelölni, mégpedig úgy, hogy $r > s$ legyen. Eszerint

$$r, s = \frac{1}{2}\left(\lambda - \mu \pm \sqrt{(\lambda - \mu)^2 + 4(k - \mu)}\right). \tag{18}$$

Említsük meg azt is, hogy ez az okoskodás használható akkor is, ha a k sajátérték multiplicitása nem 1. Ha ugyanis k multiplicitása legalább kettő, akkor $\mathbf{v}$-t tudnánk $\mathbf{j}$-re ortogonálisan választani a k sajátértékhez tartozó sajátaltérben, vagyis akkor k is kielégíti a (17) egyenletet. Jegyezzük meg, hogy ez csak $\mu = 0$ vagy k esetén lehet, további információkat a 8.7 Feladat tartalmaz. Ez azonban a továbbiakat nem befolyásolja. Ha r és s multiplicitását f-fel és g-vel jelöljük, akkor ezekre az

$$n = f + g + 1, \quad 0 = \mathrm{Trace}(A) = k + fr + gs.$$

egyenletrendszert írhatjuk föl. Ez az $r = k$ esetben is érvényes, ekkor k multiplicitása $1 + f$ lesz. Mivel $k = \lambda = \mu$ nem lehetséges, így az egyenletrendszer egyértelműen megoldható. Mivel f, g természetes számok, beláttuk az alábbi tételt.

Tétel 8.8 (Integralitási feltétel) *Az*

$$f, g = \frac{1}{2}\left(n - 1 \pm \frac{(n-1)(\mu-\lambda) - 2k}{\sqrt{(\mu-\lambda)^2 + 4(k-\mu)}}\right)$$

számok nem-negatív egészek. ∎

Mielőtt az integralitási feltétel következményeivel foglalkoznánk, lássunk néhány újabb példát erősen reguláris gráfra.

Példa 8.9 A most következő példával nem először és nem utoljára találkozunk. A $P(q)$ *Paley gráf* csúcsai a $\mathrm{GF}(q)$ véges test elemei, $q \equiv 1 \pmod 4$. Két csúcsot összekötünk, ha különbségük nemnulla négyzetelem. Mivel -1 négyzetelem, ha $q \equiv 1 \pmod 4$, így ez egyszerű irányítatlan gráf lesz. Nem teljesen magátólértetődő (ld. 8.8. Feladat), hogy erősen reguláris. A paraméterek

$$n = q, \quad k = (q-1)/2, \quad \lambda = (q-5)/4, \quad \mu = (q-1)/4.$$

A most következő konstrukció permutáció-csoportokkal van kapcsolatban.

Példa 8.10 Legyen G tranzitív permutációcsoport a V jegyhalmazon. Ekkor G a természetes módon (komponensenként) hat $V \times V$-n, azaz $(x, y)^g = (x^g, y^g)$. Ennél a hatásnál a diagonális persze orbit. Ha G 2-tranzitív, akkor a diagonálison kívüli elemek egy orbitban vannak. Általában, a $V \times V$-n az orbitok számát a permutációcsoport *rang*jának szokták nevezni. (Tehát G 2-tranzitív, ha rangja 2.) Tegyük fel, hogy G 3 rangú, azaz a diagonálison kívül pontosan két további orbit van: O_1 és O_2. Tegyük fel továbbá, hogy G páros rendű, és legyen $\tau \in G$ egy involúció (másodrendű elem). Legyen $x \in V$ olyan, hogy $x\tau \neq x$, és persze $(x\tau)\tau = x$ (ilyen elem van). Tekintsük az (x, y); $y = x\tau$ párt. Legyen ez mondjuk O_1-ben. Ekkor G O_1-en való tranzitivitása miatt O_1 minden párjára van olyan elem, amely felcseréli a pár tagjait, azaz O_1 szimmetrikus a diagonálisra. Ekkor viszont tekinthetjük azt a Γ gráfot, amelynek élei azon $\{x, y\}$ párok, ahol $(x, y) \in O_1$. Γ regularitása egyszerűen G V-n való tranzitivitásából, az erősen regularitás meg abból következik, hogy összekötött pontpár átvihető tetszőleges összekötöttbe (mert O_1 orbit). Hasonlóan okoskodhatunk összekötetlen pontpárokra is, mert O_2 orbit. Az ilyen gráfokat 3 rangú gráfoknak hívják.

MESE. A 3 rangú permutációcsoportok ismertek (modulo egyszerű csoportok karakterizációja). Sajnos azonban a legtöbb erősen reguláris gráf NEM 3 rangú. Ennek ellenére több olyan eredmény ismert, amelyet csoportelméleszek találtak 3 rangú csoportokra, de valójában erősen reguláris gráfokra vonatkoznak.

Lássunk még néhány sporadikus konstrukciót is. Semmiképpen sem törekszünk teljességre, a legjellegzetesebb konstrukciós ötleteket azonban igyekszünk érzékeltetni.

Példa 8.11 A *Clebsch gráf* csúcsai az $\{1, 2, 3, 4, 5\}$ halmaz páros sok elemű részhalmazai. Két ilyet összekötünk, ha szimmetrikus differenciájuk 4 elemű. Ellenőrizhető (ld. 8.9. Feladat), hogy a Clebsch gráf $(16, 5, 0, 2)$ paraméterű erősen reguláris gráf.

Példa 8.12 A *Gewirtz gráf* egy $(56, 10, 0, 2)$ paraméterű erősen reguláris gráf lesz (ld. 8.10. Feladat). A csúcsok halmaza $V = \{\infty\} \cup \mathcal{P} \cup \mathcal{Q}$, ahol $\mathcal{P}$ az $Alt(6)$ alternáló csoport 3-Sylow részcsoportjainak halmaza, $\mathcal{Q}$ pedig $Alt(6)$ involúcióinak halmaza. Élek: ∞-t pontosan a $\mathcal{P}$ elemeivel kötjük össze, $P \in Syl_3(Alt(6))$ és q akkor és csak akkor legyenek összekötve, ha q normalizálja P-t (azaz $q^{-1}Pq = P$), végezetül két involúciót $q_1, q_2 \in \mathcal{Q}$-t pontosan akkor kötünk össze, ha szorzatuk negyedrendű (azaz $|q_1q_2| = 4$). Hogy a dolgot konkrétabban lássuk, azonosítsuk a 3-Sylow részcsoportokat orbitjaikkal (ez tehát a 6 elemű alaphalmaz két 3-elemű halmazra való partícióját jelenti), és hasonlóan az involúciókat is tekintsük mint transzpozíció-párokat. Ennek segítségével hosszadalmasan, de mechanikusan ellenőrizhető, hogy az involúció normalizálja-e a Sylow részcsoportot. Például a

$$\{\{1, 2, 3\}, \{4, 5, 6\}\} \text{ és } q = (12)(45)$$

össze vannak kötve, hiszen $q^{-1}(123)q = (132) = (123)(123)$, és hasonlóan a Sylow-részcsoport többi elemére is. Involúciók esetén pl. $(12)(34)$ és $(23)(56)$ össze van kötve, mert szorzatuk $(1342)(56)$ negyedrendű.

Ez a konstrukció Simstől származik.

A Gewirtz gráf egy másik konstrukciója a negyedrendű projektív sík bővítésekor használatos hiperoválís-osztályokat (azaz $\mathrm{PSL}(3, q)$ orbitjait a hiperoválisokon, ld. 10.2 szakasz) használja. A csúcsok egy osztály hiperoválisai (tehát 56 csúcs van), és két hiperoválist összekötünk, ha diszjunktak.

Folytassuk a szükséges feltételekkel kapcsolatos vizsgálódásainkat. Mivel az

$$f, g = \frac{1}{2}\left(n - 1 \pm \frac{(n-1)(\mu-\lambda) - 2k}{\sqrt{(\mu-\lambda)^2 + 4(k-\mu)}}\right)$$

egészek, így két lehetőségünk van: a zárójelen belüli tört számlálója nulla, azaz $(n-1)(\mu-\lambda) = 2k$, vagy a gyökjel alatt négyzetszám áll és még néhány oszthatósági feltétel is teljesül. Az első esetben $n = 1 + 2k/(\mu - \lambda) > 1 + k$, azaz csak $\mu = \lambda + 1$ lehet, továbbá $n = 2k + 1$. A 8.1 feltétel szerint ebből $k(k - \mu) = k\mu$ jön, vagyis $k = 2\mu$, $n = 2k + 1 = 4\mu + 1$. Az ilyen gráfokat szokták *konferencia gráfok*nak is hívni. Erre az esetre van Lint és Seidel egy további, a Bruck–Chowla–Ryser tételre (ld. 6.5) emlékeztető, szükséges feltételt is belátott:

Tétel 8.13 (van Lint, Seidel) *Konferencia gráfban, azaz egy $(n-1)(\mu-\lambda) = 2k$-nak eleget tevő erősen reguláris gráfban, n két négyzetszám összege kell legyen.*

A tételt nem bizonyítjuk.

Jegyezzük meg, hogy például a Paley gráfok (ld. 8.9) ilyenek, így konferencia gráf létezik, ha n mod 4 eggyel kongruens prímhatvány. További példák is ismertek, pl. $n = 45, 225$ esetén.

A második esetben a gyökjel alatti kifejezés négyzetszám, mondjuk $(\mu - \lambda)^2 + 4(k - \mu) = u^2$. Továbbá u osztja $(n-1)(\mu-\lambda) - 2k$-t, végül a hányados ugyanolyan paritású, mint $n - 1$. Ez az "általános eset". Ennek egy nagyon fontos következménye, hogy az r, s sajátértékek is egészek, hiszen ugyanez a kifejezés áll a gyök alatt r és s kifejezésében (ld. (18)), továbbá $\lambda - \mu$ és a gyök alatt álló kifejezés egyszerre páros vagy páratlan, azaz ha a gyökvonás eredménye egész, akkor r, s már automatikusan egész számok.

Korollárium 8.14 *Ha egy erősen reguláris gráf nem konferencia gráf, akkor az r, s sajátértékek egészek.* ∎

Jegyezzük meg, hogy abban az esetben, ha n négyzetszám, akkor a $(n - 1)(\mu - \lambda) = 2k$-nek eleget tevő gráfok a második esetbe is beletartoznak. A $P(9)$ Paley gráf (amely izomorf az $L_2(3)$ négyzetháló gráffal) ilyen példa.

Az eddigiekben azt láttuk, hogy az erősen reguláris gráf paraméterei meghatározzák a sajátértékeket és azok multiplicitását. A fordított esetben az nyilvánvaló, hogy a sajátértékek meghatározzák a paramétereket (ne feledjük, hogy k is sajátérték!), hiszen ők a $\varrho^2 = (k - \mu) + (\lambda - \mu)\varrho$ másodfokú egyenlet gyökei, s így $r + s = \lambda - \mu$, $rs = -(k - \mu)$, ahonnan $\lambda = k + r + s + rs$, $\mu = k + rs$, végül n-et 8.1-mal határozhatjuk meg. Eszerint a sajátértékek meghatározzák f-et és g-t is.

Általában csupán a multiplicitások ismerete nem elegendő a paraméterek meghatározásához, de vannak olyan speciális esetek amikor valamit tudunk mondani (persze még egy adat szükséges). A következő eredményt először Wielandt bizonyította 3 rangú gráfokra. Mielőtt a tételt kimondanánk, lássunk egy fontos lineáris algebrai tételt, amelyet a bizonyítás használ.

Perron–Frobenius tétel. *Legyen A nem-negatív mátrix. Ekkor A-nak van olyan sajátvektora, melynek minden koordinátája pozitív. Ha k az ehhez tartozó sajátérték, akkor minden további ϱ sajátértékre $|\varrho| \leq k$ teljesül.*

Tétel 8.15 (Wielandt) *Legyen Γ erősen reguláris gráf $n = 2m$ csúcson és tegyük fel, hogy a sajátértékek multiplicitása $1, m - 1$ és m. Ekkor vagy Γ vagy komplementere a létra gráf (ld. 8.6 Példa), vagy Γ vagy komplementere az alábbi paraméterű: $n = 4s^2 + 4s + 2$, $k = s(2s + 1)$, $\lambda = s^2 - 1$, $\mu = s^2$ (valamilyen pozitív egész s-re).*

Bizonyítás. Mivel a komplementer gráf foka $2m - k - 1$, így esetleg áttérve a komplementerre feltehetjük, hogy $k < m$. Nézzük Γ adjacencia-mátrixát A-t, valamint A^2-et és A^3-t és számítsuk ki a nyomukat. Ez egyfelől a diagonális elemek összege, másfelől a sajátértékeké, amiből három egyenletet fogunk kapni. A diagonális elemei 0-k, A^2-é k-k, míg A^3-ben a diagonális elemek a ponton átmenő háromszögek száma, így $k\lambda$. Tehát:

$$k + (m - 1)r + ms = 0,$$
$$k^2 + (m - 1)r^2 + ms^2 = 2mk,$$
$$k^3 + (m - 1)r^3 + ms^3 = 2mk\lambda.$$

A Perron–Frobenius tétel esetünkben azt adja, hogy $|r| \leq k$. Az első egyenlet szerint $k \equiv r \pmod m$, azaz $r = k$ vagy $r = k - m$. Az első esetben $s = -k$, $2mk^2 = 2mk$, vagyis $k = 1$ és a gráf a létra vagy komplementere (ld. 8.11. Feladat). A második esetben $k = m-1-s$, $r = -1-s$ és a második egyenletből az is következik, hogy $m = 2s^2 + 2s + 1$, végül λ értékét a harmadik egyenlet adja meg. ∎

A Wielandt-tétel második esete is előfordul, $s = 1$ esetén pl. a Petersen gráfot (és csak azt, ld. 8.12. Feladat) kapjuk. Delsarte és Goethals, valamint Turyn példái mutatják, hogy abban az esetben, ha $2s+1$ prímhatvány, vannak ilyen paraméterű gráfok.

Folytassuk a szükséges feltételek tanulmányozását: először lássunk egy gyakran használt elemi lemmát, amely arról szól, hogy pozitív definit mátrixok Gram-mátrixként előállíthatók.

Lemma 8.16 (Delsarte, Goethals, Seidel) *Legyen $A = (a_{ij})$ pozitív szemidefinit valós $n \times n$-es, d rangú mátrix. Ekkor vannak olyan $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbf{R}^d$ vektorok, melyekre $a_{ij} = (\mathbf{v}_i, \mathbf{v}_j)$ $(i, j = 1, \ldots n)$.*

Bizonyítás. A "főtengelytranszformáció" miatt található olyan nem-szinguláris valós P mátrix, amellyel

$$PAP^T = \begin{pmatrix} I_d & O \\ O & O \end{pmatrix}.$$

Ha P inverzét Q-val jelöljük, akkor

$$A = Q \begin{pmatrix} I_d & O \\ O & O \end{pmatrix} Q^T = Q_1 I_d Q_1^T,$$

ahol Q_1 az az $n \times d$-es mátrix, mely Q első d oszlopát tartalmazza. A $\mathbf{v}_1, \ldots, \mathbf{v}_n$ vektorok egyszerűen a Q_1 sorai lesznek. ∎

A most következő tétellel, illetve a hozzá kapcsolódó kérdésekkel kapcsolatban ld. Babai–Frankl könyvének 1.2 szakaszát.

Tétel 8.17 *Legyen Γ erősen reguláris gráf, melyre mind Γ, mind $\bar{\Gamma}$ összefüggő. Ha Γ adjacencia-mátrixának van $f(>1)$ multiplicitású sajátértéke, akkor $n \leq f(f+3)/2$.*

Bizonyítás. Az A adjacencia-mátrixának három saját altere van. Ezeken a saját altereken a I, A és $J - I - A$ mátrixok skalárral való szorzások. Megfordítva, ha egy mátrixnak ez a három altér saját altere, akkor az a fenti három mátrixnak lineáris kombinációja. Tekintsük azt az E mátrixot, amely az f dimenziós saját altéren 1, a másik kettőn 0. Legyen ez az E mondjuk $E = \alpha I + \beta A + \gamma(J - I - A)$. Ekkor E pozitív szemidefinit, így az előző lemma alapján találunk egy $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subset \mathbf{R}^f$ vektorrendszert, amelynek ez a Gram-mátrixa, azaz $e_{ij} = (\mathbf{v}_i, \mathbf{v}_j)$. Ebből meg tudjuk határozni a $\mathbf{v}_i$ vektorok hosszát és az egymással bezárt szögeket. Így $(\mathbf{v}_i, \mathbf{v}_i) = \alpha$, mert az E mátrix főátlójában α-k állnak. Hasonlóan a $\mathbf{v}_i$ és $\mathbf{v}_j$ vektorok által bezárt szög cosinusa vagy γ/α vagy β/α, mert a főátlón kívüli elemek (azaz $(\mathbf{v}_i, \mathbf{v}_j)$), mind β-k vagy γ-k és a cosinus kiszámolásához a vektorok abszolút értékeivel osztanunk kell. Természetesen eloszthatjuk a vektorokat $\sqrt{\alpha}$-val, és így egységnyi abszolút értékű vektorokból álló olyan S vektor-halmazunk lesz, amelyben bármely kettő kétféle szög valamelyikét zárja be. Még azt is vegyük észre, hogy a vektorok páronként különbözőek, mert mind Γ, mind $\bar{\Gamma}$ összefüggő (részletesen ld. a 8.19. Feladatot).

A bizonyítás befejező része egyszerűen ilyen vektorhalmazokról szól. Minden $\mathbf{v} \in S$-re definiáljuk az $f_{\mathbf{v}}$ függvényt az alábbi módon:

$$f_{\mathbf{v}}(\mathbf{x}) = \frac{((\mathbf{v}, \mathbf{x}) - \beta)((\mathbf{v}, \mathbf{x}) - \gamma)}{(1 - \beta)(1 - \gamma).}$$

Persze $f_{\mathbf{v}}$ az egységnyi abszolút értékű vektorokon van értelmezve. Ha ezt $\mathbf{x}$ koordinátáival felírjuk, akkor másodfokú polinomot kapunk. Másrészt az $f_{\mathbf{v}}$ függvények lineárisan függetlenek, ha ugyanis egy ilyen $f_{\mathbf{v}}$-be az S egy $\mathbf{w}$ elemét helyettesítjük, akkor azt kapjuk, hogy

$$f_{\mathbf{v}}(\mathbf{w}) = \begin{cases} 1 & \text{ha } \mathbf{v} = \mathbf{w}, \\ 0 & \text{ha } \mathbf{v} \neq \mathbf{w}. \end{cases}$$

Ha tehát egy $\sum_{v \in S} \lambda_v f_{\mathbf{v}}$ lineáris kombináció $\mathbf{0}$, akkor $\mathbf{w}$ behelyettesítésével látjuk, hogy $\lambda_w = 0$, vagyis az $f_{\mathbf{v}}$-k valóban függetlenek. Másfelől ezek benne vannak abban a vektortérben amelyet az f darab lineáris és $f(f+1)/2$ homogén másodfokú függvény feszít ki. Konstansokat nem kell figyelembe venni, mert $x_1^2 + \ldots + x_f^2 = 1$, azaz a konstans lecserélhető másodfokúra. Más függvény viszont nem ad azonosan 0-t az egységnyi abszolút értékű vektorokra megszorítva. Eszerint valóban

$$n = |S| = f + \frac{1}{2} f(f+1) = \frac{1}{2} f(f+3). \quad ∎$$

A bizonyítás lelke az olyan vektorok számának becslése, amelyek csak két szöget határoznak meg. Delsarte, Goethals és Seidel a használt becslést "abszolút korlát"-nak nevezte, mert a becslés nem függ a meghatározott szögek nagyságától.

Egy további korlát a *Krein feltétel*, ezt először (Krein egy eredményét felhasználva) 3 rangú gráfokra bizonyította Scott.

Tétel 8.18 (Krein-feltételek) *Legyen Γ erősen reguláris gráf, melyre mind Γ, mind $\bar{\Gamma}$ összefüggő. Ha Γ adjacencia-mátrixának sajétértékei k, r, s, akkor*

(a) $(r+1)(k+r+2rs) \leq (k+r)(s+1)^2$,

(b) $(s+1)(k+s+2rs) \leq (k+s)(r+1)^2$.

A bizonyítás nagyon számolós, így most elhagyjuk. ∎

Még egy további szükséges feltételt említünk erősen reguláris gráfok létezésére, a bizonyítást teljesen elhagyjuk.

Tétel 8.19 ("Karom korlát") *Ha $\mu \neq s^2$, $\mu \neq s(s+1)$, akkor $2(r+1) \leq s(s+1)(\mu+1)$.* ∎

Igen gyakran az a helyzet, hogy egy erősen reguláris gráfot meghatároznak paraméterei. Erre már több konkrét példát láttunk eddig is, most ezt a négyzetháló gráfokra fogjuk megmutatni. A megfelelő állítást a trianguláris gráfok esetére a következő fejezetben bizonyítjuk, mert ezt majd ott használjuk a Hall–Connor tétel bizonyításában.

Tétel 8.20 *Legyen Γ egy $(n^2, 2(n-1), n-2, 2)$ paraméterű erősen reguláris gráf. Ekkor $n > 4$-re Γ izomorf az $L_2(n)$ négyzetháló gráffal.*

Bizonyítás. Válasszuk ki Γ egy x pontját és tekintsük a $\Gamma(x)$ gráfot. Ez egy $2(n-1)$ csúcsú $(n-2)$-edfokú reguláris gráf. Vegyünk ebben a gráfban két nem összekötött csúcsot, y-t és z-t. Jelöljük m-mel ezek $\Gamma(x)$-beli közös szomszédainak számát. Nyilván $m \leq 1$. Mivel $\deg(y) = \deg(z) = n-2$, így $n-2-m$ olyan csúcs van amely csak y-nal van összekötve, de z-vel nincs, és megfordítva. Eszerint viszont marad $2(n-1) - 2 - m - 2(n-2-m) = m$ olyan csúcs, amely sem y-nal, sem z-vel nincs összekötve.

Tekintsük először $m = 1$ esetet. Jelölje w azt a pontot, amelyik sem y-nal, sem z-vel nincs összekötve. Ekkor w-nek és y-nak csak egy közös szomszédja lehet. Hasonlóan w-nek és z-nek is. Másrészt minden w-től különböző pont vagy y-nal vagy z-vel össze van kötve, ami csak úgy lehet, ha $n-2 \leq 2$.

Így $n > 4$-re csak $m = 0$ fordulhat elő. Ez magyarul azt jelenti, hogy $\overline{\Gamma(x)}$ nem tartalmaz háromszöget. $\overline{\Gamma(x)}$ egy $(n-1)$-reguláris gráf $2(n-1)$ ponton, így a Turán-tétel szerint csak akkor lehet háromszögmentes, ha teljes páros gráf. Az eredeti $\Gamma(x)$-re ez azt jelenti, hogy ő két diszjunkt klikk uniója.

Vegyük hozzá x-et a $\Gamma(x)$-beli két klikkhez. Így minden ponton két klikk megy át, azaz összesen $2n^2/n = 2n$ ilyen n pontú klikkünk van, melyek egymást nulla vagy egy pontban metszik. Három ilyen klikk közül mindig van két diszjunkt, mert ellenkező esetben a két klikk közös pontjához tartozó $\Gamma(x)$ gráf két diszjunkt klikkje között menne a harmadik klikk valamelyik éle. Ez azt jelenti, hogy egy rögzített klikket metsző klikkek páronként diszjunktak és lefedik az összes pontot. Ebből azonnal adódik, hogy a klikkek két osztályba sorolhatók és a gráf $L_2(n)$. ∎

Jegyezzük meg, hogy $n = 2, 3$-ra közvetlenül láthatjuk az állítást, míg $n = 4$-re van ellenpélda, az ú.n. Shrikhande-gráf, ld. 8.33.

8.1 ERŐSEN REGULÁRIS GRÁFOK ÉS BLOKKRENDSZEREK

Tétel 8.21 *Legyen Γ olyan erősen reguláris gráf, amelyre $\lambda = \mu$. Ekkor Γ adjacenciamátrixa A tekinthető egy négyzetes $2-(n, k, \lambda)$ blokkrendszer incidencia mátrixának.*

Bizonyítás. Mivel $A = A^T$, így

$$A^2 = AA^T = (k-\lambda)I + \lambda J,$$

és ez a mátrixegyenlet pontosan azt fogalmazza meg, hogy A négyzetes blokkrendszer illeszkedési mátrixa. ∎

Tétel 8.22 *Legyen Γ olyan erősen reguláris gráf, amelyre $\mu = \lambda+2$, és legyen A a Γ adjacencia-mátrixa. Ekkor $B = A + I$ egy négyzetes $2-(n, k+1, \lambda+2)$ blokkrendszer incidencia mátrixa.*

Bizonyítás. Most is $B = B^T$, azaz

$$BB^T = B^2 = (A+I)^2 = A^2 + 2A + I = (k-\lambda-2)I - 2A + (\lambda+2)J + 2A + I,$$

és mivel ez nem más, mint $(k-\lambda-1)I + (\lambda+2)J$, az állítás adódik. ∎

Jegyezzük meg, hogy ezeket az észrevételeket megfogalmazhattuk volna a polaritások nyelvén is, hiszen a kapott blokkrendszerek illeszkedési mátrixa automatikusan szimmetrikus lesz.

Tétel 8.23 *Akkor és csak akkor létezik olyan négyzetes (v, k, λ) blokkrendszer, melynek van olyan polaritása, ahol semelyik pont sem illeszkedik a hozzárendelt blokkra, ha van (v, k, λ, λ) paraméterű erősen reguláris gráf.*

Akkor és csak akkor létezik olyan négyzetes (v, k, λ) blokkrendszer, amelynek van olyan polaritása, ahol mindegyik pont illeszkedik a hozzárendelt blokkra, ha van $(v, k-1, \lambda-2, \lambda)$ paraméterű erősen reguláris gráf.

A bizonyítást ld. a 8.13. Feladatban. ∎

Tétel 8.24 *Rögzített λ-ra csak véges sok $\mu = \lambda$-nak eleget tevő erősen reguláris gráf létezik.*

Bizonyítás. Egy ilyen gráf nem lehet konferencia gráf, azaz a 8.8 Integralitási feltétel szerint $k = \lambda + u^2$ kell legyen valamilyen u-ra, amely osztja λ-t. Mivel eszerint $u \leq \lambda$, így $k \leq \lambda(\lambda+1)$ és $v \leq \lambda^2(\lambda+2)$. ∎

Jegyezzük meg, hogy a bizonyításban adott felső becslések élesek, ha λ prímhatvány, akkor vannak is ilyen gráfok.

A másik esetben, amikor $\mu = \lambda + 2$ nem ismert hasonló végességi eredmény, még $\lambda = 0$-ra sem, pedig ebben az esetben csak három gráfot ismerünk.

Nézzük, hogyan hozhatók kapcsolatba bisíkokkal ezek az erősen reguláris gráfok. Az $L_2(4)$ gráf és a Shrikhande-gráf $(16, 6, 2, 2)$ paraméterű gráfok, így ezek (nem-izomorf) negyedrendű ($k = 6$-os) bisíkokat adnak. Másrészt a Clebsch-gráf $(16, 5, 0, 2)$ paraméterű, így ő is negyedrendű bisíkot ad meg. Más negyedrendű bisík nincs is.

A Gewirtz-gráf $(56, 10, 0, 2)$ paraméterű erősen reguláris gráf így 9-edrendű bisíkot határoz meg. Ismert, hogy pontosan 4 nem-izomorf 9-edrendű bisík van.

Egy másik olyan témakör, ahol a blokkrendszerek elméletében erősen reguláris gráfokat használunk, a kvázi-reziduális blokkrendszerek. Idézzük fel, hogy egy négyzetes blokkrendszer reziduálisa a belőle egy blokk (és annak összes pontjai) törlésével kapható blokkrendszer. Természetesen az eljárás prototípusa az, ahogy projektív síkból affin síkot nyerünk. Ha egy blokkrendszer valaminek a reziduálisa, akkor paramétereire teljesül az $r = k + \lambda$ összefüggés.

Definíció 8.25 Egy blokkrendszert *kvázi-reziduális*nak nevezünk, ha paramétereire $r = k + \lambda$.

Természetesen a fő kérdés az, hogy vajon egy kvázi-reziduális blokkrendszer reziduálisa-e valami más blokkrendszernek. Könnyű megmutatni, hogy $\lambda = 1$ esetén kvázi-reziduális blokkrendszer csak az affin sík lehet, az pedig projektív sík reziduálisa. $\lambda = 2$-re is igaz ez (ez a Hall–Connor tétel, amelyet rövidesen bizonyítunk). $\lambda = 3$-ra azonban már nem igaz, hogy minden kvázi-reziduális blokkrendszer reziduális volna. Az alábbi Bhattacharyától származó példa ellenpélda: a pontok halmaza $\{1, \ldots, 16\}$, a blokkokat pedig az alábbi táblázat tartalmazza.

$$
\begin{array}{lll}
B_1 = \{1,2,7,8,14,15\} & B_9 = \{4,5,7,8,12,15\} & B_{17} = \{1,2,3,11,12,15\} \\
B_2 = \{3,5,7,8,11,13\} & B_{10} = \{2,4,9,10,11,13\} & B_{18} = \{2,6,7,9,14,16\} \\
B_3 = \{2,3,8,9,13,16\} & B_{11} = \{3,6,7,10,11,14\} & B_{19} = \{1,4,5,13,14,16\} \\
B_4 = \{3,5,8,9,12,14\} & B_{12} = \{1,2,3,4,5,6\} & B_{20} = \{2,5,6,11,12,16\} \\
B_5 = \{1,6,7,9,12,13\} & B_{13} = \{1,4,7,8,11,16\} & B_{21} = \{1,3,9,10,15,16\} \\
B_6 = \{2,5,7,10,13,15\} & B_{14} = \{2,4,8,10,12,14\} & B_{22} = \{4,6,8,9,11,15\} \\
B_7 = \{3,4,7,10,12,16\} & B_{15} = \{5,6,8,10,15,16\} & B_{23} = \{1,5,9,10,11,14\} \\
B_8 = \{3,4,6,13,14,15\} & B_{16} = \{1,6,8,10,12,13\} & B_{24} = \{11,12,13,14,15,16\}
\end{array}
$$

Ekkor **D** egy $(16, 6, 3)$ blokkrendszer, amely kvázireziduális. Jegyezzük meg, hogy annak, hogy egy ilyen blokkrendszer nem lehet négyzetes blokkrendszer blokkreziduálisa a triviális oka az, ha két blokk egymást több, mint λ pontban metszi. Esetünkben ezek a blokkok B_5 és B_{16}, melyek 4 pontban metszik egymást.

A jelen jegyzetben csak a $\lambda = 2$ esetet vizsgáljuk meg részletesen, azonban általános λ-ra a helyzet nem annyira elszomorító, mint azt Bhattacharya-féle példa alapján gondolhatnánk. Nevezetesen Bose, Shrikhande és Singhi belátták az alábbi szép aszimptotikus eredményt.

Tétel 8.26 (Bose, Shrikhande, Singhi) *Van olyan λ-tól függő $g(\lambda)$, hogy $k > g(\lambda)$ esetén minden kvázireziduális blokkrendszer reziduális.*

Konkrétan $g(3) = 76$-ot adták meg, különben pedig $\lambda \geq 10$-re λ^4, $4 \leq \lambda \leq 9$-re λ^5 nagyságrendű $g(\lambda)$-t. Részletesen ld. az eredeti cikket [6].

A $\lambda = 2$ eset részletes vizsgálatát kezdjük az alábbi észrevétellel:

Tétel 8.27 *Legyen* **D** *kvázi-reziduális blokkrendszer, melyre $\lambda = 2$. Ekkor*

$$v = \frac{k(k+1)}{2}, \quad r = k+2, \quad \lambda = 2, \quad b = \frac{(k+1)(k+2)}{2}.$$

Továbbá két különböző blokknak 1 vagy 2 közös pontja van.

Bizonyítás. A paraméterek meghatározása triviális (ld. 3.2), csak a blokkok metszetére vonatkozó állítást kell igazolnunk. Legyen B rögzített blokk és jelölje n_i a B-t i pontban metsző blokkok számát $(i = 0, \ldots k)$. Ekkor a variancia-trükköt (négyzetes leszámlálást) alkalmazva kapjuk, hogy

$$\sum_i n_i = \frac{1}{2}(k+1)(k+2) - 1,$$

$$\sum_i i n_i = k(r-1) = k(k+1),$$

$$\sum_i i(i-1)n_i = k(k-1)(\lambda - 1) = k(k-1).$$

Átrendezéssel azt kapjuk, hogy

$$\sum_i (i-1)(i-2)n_i = 0.$$

Ebből az látszik, hogy $i \neq 1, 2$-re $n_i = 0$, amint bizonyítani akartuk. (A harmadik egyenletből az is következik, hogy $n_2 = k(k-1)/2$ és így $n_1 = 2k$.) ∎

A most következő definíció a négyzetes blokkrendszer általánosítása. Emlékeztetünk arra, hogy négyzetes (más szóhasználattal szimmetrikus) blokkrendszerben bármely két blokk metszete λ volt.

Definíció 8.28 Egy blokkrendszer *kváziszimmetrikus*, ha létezik két egész szám μ_1 és μ_2, hogy bármely két blokk μ_1 vagy μ_2 pontban metszi egymást. Ezeket a blokkrendszer *metszési számainak* nevezzük.

Ezzel a definícióval az előző állítás azt mondja, hogy $\lambda = 2$ paraméterű kvázireziduális blokkrendszer kváziszimmetrikus és $\mu_1 = 1$, $\mu_2 = 2$. A kváziszimmetrikus blokkrendszerek azért érdekesek, mert erősen reguláris gráfot tudunk definiálni segítségükkel.

Tétel 8.29 *Legyen* **D** *kváziszimmetrikus blokkrendszer μ_1, μ_2 paraméterekkel. Legyen a Γ gráf csúcsainak halmaza* **D** *blokkjainak halmaza és kössünk össze két blokkot, ha metszetük μ_2 elemű. Ekkor Γ erősen reguláris.*

Bizonyítás. Azt akarjuk belátni, hogy A^2 az A, I, J kombinációja. Legyen M a **D** incidencia-mátrixa és tegyük fel, hogy $\mu_2 > \mu_1$ (áttérhetünk a komplementerre). Ekkor a Γ gráf A adjacenciamátrixa nem más, mint

$$A = \frac{1}{\mu_2 - \mu_1}(M^T M - \mu_1 J - (k - \mu_1)I).$$

Mivel $MM^T = nI + \lambda J$, ahol $n = r - \lambda$, így

$$\begin{aligned}(M^t M)^2 &= M^t(nI + \lambda J)M \\ &= nM^t M + \lambda k^2 J.\end{aligned}$$

Ilymódon

$$\begin{aligned}(\mu_2 - \mu_1)^2 A^2 &= (M^t M)^2 + \mu_1^2 bJ + (k - \mu_1)^2 I - \mu_1(M^t MJ + JM^t M) \\ &\quad -2(k - \mu_1)M^t M + 2\mu_1(k - \mu_1)J.\end{aligned}$$

Felhasználva, hogy

$$\begin{aligned}M^t MJ &= rkJ = JM^t M; \\ (M^t M)^2 &= nM^t M + \lambda k^2 J, \\ \text{és} \qquad M^t M &= (\mu_2 - \mu_1)A + \mu_1 J + (k - \mu_1)I,\end{aligned}$$

azt találjuk, hogy A^2 előáll az erősen reguláris gráfoknál megszokott alakban, vagyis

$$A^2 = \alpha I + \beta A + \gamma J.$$

Tehát Γ valóban erősen reguláris. ∎

A tételben szereplő Γ gráfot a blokkrendszer *blokkgráfjá*nak szokás hívni.

Korollárium 8.30 *Steiner-rendszer blokkgráfja erősen reguláris.* ∎

Tétel 8.31 (Hall–Connor) *$\lambda = 2$ paraméterű kvázireziduális blokkrendszer reziduális, ha $k \neq 6$.*

Bizonyítás. Azt már láttuk, hogy egy ilyen blokkrendszer blokkgráfja erősen reguláris, mert a blokkok 1 vagy 2 pontban metszik egymást. Tekintsük azt a gráfot, ahol két blokkot pontosan akkor kötünk össze, ha metszetük egypontú. Ennek a paraméterei $v = r(r-1)/2$, $k = 2(r-2)$, $\lambda = r - 2$, $\mu = 4$. A v, k-ra vonatkozó állítást a 8.27 Tétel bizonyításának a végén láttuk, a λ-t, μ-t az előző tételből lehet kiolvasni (ld. 8.14. Feladat). Ezek éppen a $T(r)$ trianguláris gráf paraméterei, és ebből $r \neq 8$ esetén következik is, hogy a gráf izomorf $T(r)$-rel. Eszerint viszont megindexelhetjük a blokkokat az $S = \{1, \ldots, r\}$ halmaz kételemű részhalmazaival úgy, hogy két blokk pontosan akkor metszi

egymást 1 pontban, ha a megfelelő kételemű halmazok is egy pontban metszik egymást. Bővítsük **D**-t S elemeivel és tegyük hozzá a blokkokhoz S-et és minden blokkhoz az őt megindexelő kételemű halmazt. Az eddig elmondottakból könnyű látni, hogy így négyzetes blokkrendszert kapunk $\lambda = 2$-vel és az S-re vonatkozó blokkreziduális éppen **D**. ∎

Megjegyzés. A $k \neq 6$ megszorítás nem szükséges. Connor ugyanis megmutatta, hogy nincsen $2-(21, 6, 2)$ paraméterű blokkrendszer.

Hogy a bizonyítás teljes legyen, lássuk be, hogy a trianguláris gráfokat paramétereik meghatározzák.

Tétel 8.32 *Legyen Γ egy*

$$(\binom{r}{2}, 2(r-2), r-2, 4)$$

paraméterű erősen reguláris gráf. Ekkor Γ izomorf a trianguláris gráffal, ha $r > 8$.

Bizonyítás. A bizonyítás nagyjából az $L_2(n)$ gráfokra vonatkozó bizonyítást követi, így csak vázoljuk (részletesen ld. a 8.18. Feladatot). Vegyünk egy x pontot, és tekintsük a $\Gamma(x)$-et. Ez egy $2(r-2)$ csúcsú, $(r-2)$-edfokú reguláris gráf. Legyen y, z ennek két össze nem kötött pontja. Először megmutatjuk, hogy y, z közös szomszédainak m száma $\Gamma(x)$-ben csak 3 vagy 2 lehet. Nyilván $m \leq 3$, hisz x közös szomszéd Γ-ban. Olyan csúcs amely y-nal (ill. z-vel) össze van kötve $\Gamma(x)$-ben, de z-vel (ill. y-nal) nincs, pontosan $r - 2 - m$ van. Így $\Gamma(x)$-ben $m - 2$ olyan csúcs van, amely sem y-nal, sem z-vel nincs összekötve. Tehát $2 \leq m$. Ha $m = 3$ volna, akkor tekintsük azt a w pontot, amely sem y-nal, sem z-vel nincs összekötve. Mivel minden w-vel összekötött csúcs y-nal vagy z-vel össze van kötve, így $r - 2 \leq 3 + 3$, ellentmondás.

Eszerint $m = 2$ mindig, azaz $\Delta = \bar{\Gamma}(x)$ nem tartalmaz háromszöget. Azt se nehéz látni, hogy Δ páros gráf, részletesen ld. 8.18. Feladat.

Ez azt jelenti, hogy minden x-re $\Gamma(x)$ két nagy ($r - 2$ méretű) klikket tartalmaz. Vegyük hozzá ezekhez az x-et. Így minden csúcs benne van pontosan két "nagy" klikkben, melyeknek mérete $r - 1$. Ugyanez az okoskodás mutatja, hogy minden él benne van egy nagy klikkben. A nagy klikkek száma $2\binom{r}{2}/(r-1) = r$. Mivel bármely két nagy klikknek legfeljebb egy közös csúcsa van, így pontosan egy van. Ha a "nagy" klikkeket pontoknak, a csúcsokat blokkoknak tekintünk, akkor egy 2-$(r, 2, 1)$ blokkrendszert kapunk, amely nem lehet más, mint az összes pár alkotta blokkrendszer, ami megadja az izomorfizmust Γ és a trianguláris gráf között. ∎

Jegyezzük meg, hogy igazából elegendő az $r \neq 8$ feltétel is, az $r \leq 7$ esetek elintézhetők (ld. 8.15. Feladat).

Minden bisík legalább egy reziduális blokkrendszert határoz meg, s ahhoz a blokkrendszerhez tartozik egy blokkgráf. Noha a gráfok egy végtelen családhoz tartoznak, bisíkok, mint láttuk csak a $k = 3, 4, 5, 6, 9, 11$ és 13 értékekre ismertek. A $k = 5$-ös bisík Hadamard-féle, blokkgráfja a Petersen-gráf.

Még egy olyan nevezetes blokkrendszer-osztály van, amely kváziszimmetrikus. Nevezetesen ha egy **D** 3-rendszer bővítése egy **E** négyzetes blokkrendszernek, akkor ilyen (ld. 8.16. Feladat). Ha visszaemlékszünk, akkor a Cameron tétel (7.9) bizonyítása ezt az észrevételt használta.

Ebben a szakaszban több olyan tételt is láttunk, hogy bizonyos gráfokat a paramétereik meghatároznak. Azonban az is tipikus volt, hogy bizonyos kivételes paraméterekre ez nem volt igaz. Most egy olyan konstrukciót lássunk, amely mind a négyzetháló, mind a trianguláris gráf esetében alkalmas a kivételes példák előállítására.

A konstrukció az ú. n. *switching*: Legyen Y a Γ gráf csúcsainak egy halmaza. Ha két pont egyike Y-beli, másika nincs Y-ban, akkor cseréljük meg összekötöttségüket (ha tehát él volt köztük, akkor ne legyen, ha viszont nem volt, akkor kössük őket össze). Ne változtassunk semmit azon párok esetén, ahol mindkét csúcs Y-beli, vagy egyik sem.

Nyilvánvaló, hogy az Y-ra vonatkozó switching azonos a $V(\Gamma)\setminus Y$-ra vonatkozóval, továbbá ha előbb Y_1-re majd Y_2-re végezzük el a switchinget, akkor az ugyanaz, mintha $Y_1 \triangle Y_2$-re végeznénk el egyszerre. Ilymódon a switching ekvivalenciarelációt hoz létre. A switching-et lényegében Seidel vezette be, és vizsgálta először szisztematikusan. A motiváció az ú. n. 2-gráfok témaköre volt, melyet G. Higman talált ki a Co_3 sporadikus egyszerű csoport 2-tranzitív hatásának vizsgálatára. Később Seidel, Taylor és mások vizsgálták behatóan. A 2-gráfok k-reguláris gráfok (mint $1-(n, 2, k)$-rendszerek) bővítésével vannak kapcsolatban, bővebben ld. a 8.31. Feladatsort.

Példa 8.33 Lássuk, hogyan kaphatjuk meg az ú. n. *Shrikhande gráfot.* Ezt az $L_2(4)$ négyzetháló gráfból kaphatjuk meg switching segítségével, ha Y-nak a négy diagonális pontot választjuk. A Shrikhande gráf paraméterei ugyanazok, mint az $L_2(4)$-é.

Példa 8.34 Most a $T(8)$ trianguláris gráfból induljunk ki. Mivel a trianguláris gráfok csúcsai egy nyolcelemű halmaz kételemű részhalmazai, az Y halmaz pontjait tekinthetjük egy a nyolc ponton értelmezett gráfnak is, ha minden párt egy élnek gondolunk. Ilymódon Y-nak az alábbi három gráf választható:

(1) egy 1-faktor (négy diszjunkt él);

(2) egy nyolc hosszú kör, végül

(3) egy diszjunkt ötszög és háromszög.

Mindegyik esetben a $T(8)$-éval azonos (28,12,6,4) paraméterű erősen reguláris gráfot kapunk.

A fenti példák mutatják, hogy $L_2(4)$ és $T(8)$ esetén nem véletlenül nem működött a karakterizációs tételek bizonyítása.

Fejezzük be ezt a fejezetet egy a témakörre nézve tipikus tétellel.

Tétel 8.35 (Seidel) *Azon erősen reguláris gráfok, melyeknek legkisebb sajátértéke -2, a következők:*

(a) $T(m)$ trianguláris gráf, $m \geq 5$;

(b) $L_2(m)$ négyzetháló gráf, $m \geq 3$;

(c) $CP(m)$ koktélparti gráf, $m \geq 2$;

(d) a Petersen-gráf;

(e) a Clebsch-gráf komplementere;

(f) a Schläfli-gráf komplementere;

(g) a Shrikhande-gráf;

(h) a három Chang-gráf.

A tételben szereplő gráfokat egy kivétellel már ismerjük, ez a kivétel a Schläfli gráf, mellyel a következő szakaszban a szélmalom-tételben fogunk megismerkedni.

8.2 ERŐSEN REGULÁRIS GRÁFOKKAL KAPCSOLATOS GRÁFOS TÉTELEK

Tétel 8.36 ("Szélmalom tétel") *Legyen Γ olyan nem-üres gráf, amelyre az alábbi megszorítás teljesül:*

(*) Bármely $\{x, y\}$ él benne van olyan $\{x, y, z\}$ háromszögben, amely azt tudja, hogy minden további csúcs x, y, z közül pontosan eggyel van összekötve.

Ekkor Γ az alábbi gráfok valamelyike:

(a) egy csúcsról lelógó háromszögek uniója ("szélmalom"),

(b) három speciális gráf valamelyike, ahol a csúcsok száma 9, 15 illetve 27.

Bizonyítás. Feltehetjük, hogy Γ-nak nincs olyan csúcsa, amely minden további csúccsal össze lenne kötve, mert akkor szélmalmunk kell legyen.

Ez a kiinduló észrevétel az általános esetben is: legyen x a legnagyobb fokú csúcs. Az $\{x\} \cup \Gamma(x)$ által feszített részgráf szélmalom. Máris következik, hogy x foka páros, azaz $\deg(x) = 2u$ $(u \geq 1)$. Ha $u = 1$, akkor minden csúcs foka 2, és a gráf diszjunkt körök uniója. A feltételek miatt ez csak úgy lehet, ha egyetlen háromszögünk van, amit viszont fentebb kizártunk. Tehát $u \geq 2$. Sorszámozzuk meg az x-ről lelógó háromszögeket: $T_1, \ldots, T_u$, és legyen $T_i = \{x, y_{i,0}, y_{i,1}\}$, $(i = 1, \ldots, u)$.

Tekintsünk most egy olyan $z \neq x$ csúcsot, amely nincs összekötve x-szel. A (*) feltétel szerint z az $y_{i,0}$ és $y_{i,1}$ közül pontosan az egyikkel van összekötve minden $i = 1, \ldots, u$-ra. Így a z pontot jellemezhetjük egy u hosszú 0–1 vektorral, amelynek i-edik koordinátája ε, ha z az $y_{i,\varepsilon}$-nal van összekötve. Jelöljük ezt a vektort $\mathbf{v}(z)$-vel. Ezeknek a $\mathbf{v}(z)$ vektoroknak az alábbi tulajdonságai vannak (z mindig x-szel össze nem kötött csúcsot jelöl):

(1) Ha z és z' szomszédos, akkor $\mathbf{v}(z)$ és $\mathbf{v}(z')$ pontosan egy pozícióban egyezik meg.

(2) Ha z és z' nem szomszédos, de van olyan közös szomszédjuk, amely nincs összekötve x-szel, akkor $\mathbf{v}(z)$ és $\mathbf{v}(z')$ pontosan két pozícióban nem egyezik meg.

(3) Ha z és z' nem szomszédos és minden közös szomszédjuk össze van kötve x-szel, akkor $\mathbf{v}(z)$ és $\mathbf{v}(z')$ megegyezik.

Lássuk mondjuk (1) bizonyítását: Ebben az esetben a z és z' össze vannak kötve, így z, z' benne vannak egy olyan háromszögben, amelynek valamelyik csúcsával Γ minden pontja össze van kötve, így x is. Mivel x sem z-vel, sem z'-vel nincs összekötve, így a háromszög harmadik csúcsa kell x valamelyik szomszédja, mondjuk $y_{i,\varepsilon}$ legyen. z-nek és z'-nek nem lehet több közös szomszédja, hiszen az a $z, z', y_{i,\varepsilon}$ háromszög két csúcsával is össze lenne kötve. Ez viszont pontosan azt jelenti, hogy $\mathbf{v}(z)$ és $\mathbf{v}(z')$ pontosan az i-edik pozícióban egyezik meg.

Teljesen hasonlóan bizonyítható (2) és (3) is (ld. 8. 1–2. Feladatokat).

Tegyük fel, hogy $u \geq 3$. Válasszunk egy $z \notin \Gamma(x)$ pontot. Ekkor z a $\Gamma(x)$-nek pontosan u pontjával van összekötve, és ezek a szomszédok egymással nincsenek összekötve. Mivel z szomszédai is valahány z-ről "lelógó" háromszöget alkotnak, így $\deg(z) = 2u$ és z-nek pontosan u olyan szomszédja van, amelyek nincsenek $\Gamma(x)$-ben. Válasszunk ezek közül egyet, mondjuk z'-t. Megismételve ezt az eljárást z'-re, válasszuk ki annak egy (z-től különböző) z'' szonszédját, ami nincs $\Gamma(x)$-ben. Az (1) bizonyításában használt gondolatmenet (vagy maga (1)) azonnal adja, hogy z és z'' nem lehetnek összekötve. Végül válasszunk egy negyedik z''' pontot, amely z''-vel van összekötve. A z, z', z'', z''' út szomszédos pontjaihoz tartozó vektorok pontosan egy koordinátában egyeznek meg. Legyenek ezek a koordináták az i-edik z, z' esetén, a j-edik z', z'' esetén, végül a k-adik z'', z''' esetén. Jegyezzük meg, hogy itt i, j, k különbözőek. Mivel (1), (2), (3) az összes lehetőséget kimerítik és a z-hez és z'''-höz rendelt vektor csupán ezen három koordinátában egyezik meg, így csak $u = 3$ vagy $u - 2 = 3$ lehet.

Összefoglalva tehát csak $u = 2, 3, 5$ lehet.

Mindhárom esetben elegendő információnk van ahhoz, hogy rekonstruáljuk (egyértelműen) a gráfot. Először is jegyezzük meg, hogy a gráfok $2u$-adfokú regulárisak, mint azt már lényegében láttuk a bizonyítás során. $u = 2$-re a gráf $K_3 \times K_3$, vagyis a csúcsok egy 3×3-as mátrix elemei, és két csúcsot pontosan akkor kötünk össze, ha egy sorban vagy egy oszlopban vannak. $u = 3$-ra a csúcsok egy 6-elemű halmaz kételemű részhalmazai, két csúcs pontosan akkor szomszédos, ha a megfelelő halmazok diszjunktak. Természetesen nemcsak azt kell ellenőriznünk, hogy ezek a gráfok kielégítik a feltételt, hanem az egyértelműséget is (ld. 8.3 Feladat). Végezetül az $u = 5$ esetben annyit jegyzünk meg, hogy a $\mathbf{v}(z)$ vektorok pontosan azok a vektorok lesznek, amelyekben páros sok 1-es szerepel. Eszerint gráfunk 1+10+16=27 pontú lesz. Ezt a gráfot *Schläfli gráf* nak nevezzük (ld. 8.4 Feladat). ∎

A szereplő kivételes gráfok mind regulárisak, sőt ennél több is teljesül: a (*) feltételben szereplő háromszög egyértelmű, azaz minden él pontosan egy háromszögben van benne. Hasonlóan azt is láttuk a bizonyítás során, hogy két össze nem kötött pontnak pontosan u közös szomszédja van.

Eszerint a 8.36 tétel azt mondja, hogy $(6u - 3, 2u, 1, u)$ paraméterű erősen reguláris gráfok csak az $u = 2, 3, 5$ esetben léteznek és a gráfok egyértelműek. Valóban, ez a korábbi ismereteinkből következik.

Nézzük, mit ad a 8.8 feltétel a szélmalom-tétel következményére. A gráfokra $n = 6u - 3$, $k = 2u$, $\lambda = 1$, $\mu = u$ volt. 8.8 szerint

$$3u - 2 \mp \frac{(3u-1)(u-2)}{u+1}$$

nem-negatív egész kell legyen. Ebből könnyen látszik, hogy $u + 1$ osztja 12-t, azaz $u = 2, 3, 5$ vagy 11 lehet. Az első három eset, mint tudjuk elő is fordul, a negyediket az abszolút korlát (ld. 8.17) zárja ki.

Egy szintén erősen reguláris gráfokkal kapcsolatos kérdést old meg az alábbi tétel:

Tétel 8.37 ("Friendship theorem") *Tegyük fel, hogy egy n emberből álló közösségben bármely két embernek pontosan egy közös barátja van. Ekkor n páratlan, és valamennyi $n \geq 3$ páratlan számra van is ilyen gráf: a v_1 ember mindenkinek a barátja, a többiek közül pedig v_{2i} és v_{2i+1} barátok (minden i-re) és más nem.*

Bizonyítás. Legyen G a gráfunk, és minden $x \in G$-re tekintsük az x szomszédainak $G(x)$ halmazát. Ha u és v két különböző pont, akkor ezeket pontosan egy $G(x)$ fogja tartalmazni, mégpedig a közös szomszédjukhoz tartozó. Így $(V(G), \{G(x) : x \in V(G)\}$ lineáris tér, melyre $v = b$. Ha ez a lineáris tér degenerált, akkor van egy $|V(G)| - 1$ pontú halmaz (ez lesz $G(v_1)$), a többi halmaz kételemű, ami azt jelenti, hogy a v_1-et és a belőle kiinduló éleket törölve egy diszjunkt élekből álló gráfot kapunk. Ez pontosan az, amit a tétel állít. Ha a lineáris tér projektív sík, akkor a G adjacencia-mátrixa ennek egy olyan szimmetrikus illeszkedési mátrixa lenne, amelynek főátlójában csupa nulla állna. Más szóval ez egy olyan polaritást jelentene, aminek nincs autokonjugált pontja (v. ö. a 7.1 szakaszt). A 7.15 Korollárium miatt ez nem lehetséges. ∎

A tétel először Wilf egy 1971-es dolgozatában szerepel G. Higmanra, mint forrásra való hivatkozással. Valószínűleg az igazi forrás Erdős, Rényi és T. Sós 1966-os "On a problem of graph theory" c. dolgozata, amely hasonló, sőt némileg általánosabb extremális kérdésekkel foglalkozik (*Studia Sci. Math. Hung.* **1** (1966), 215–235). Az említett dolgozat néhány állítását feladatként is megtalálhatjuk a jelen fejezet végén.

Zárjuk ezt a fejezetet egy különösen szép gráffal, mellyel valószínűleg gráfelméletből már találkoztunk 5 bőségű r-reguláris gráfoknál. Ez az előbb említett Erdős–Rényi–T. Sós dolgozat kérdéséhez is szorosan kapcsolódik.

Tétel 8.38 *5 bőségű r reguláris gráfnak legalább r^2+1 csúcsa van. Ha itt egyenlőség van, akkor $r = 2, 3, 7$ vagy 57 lehet.*

Bizonyítás. Tekintsünk egy csúcsot. Ennek r szomszédja van, amelyek mind különbözőek. Mivel a gráf 5 bőségű, ezen szonszédok szomszédai is páronként különbözőek, vagyis valóban van $1+r+r(r-1) = r^2+1$ csúcs legalább. Két összekötött csúcsnak nyilván nincs közös szomszédja, mert akkor lenne háromszög. Ha viszont két összekötetlen pontot tekintünk, akkor az előző okoskodásban az egyenlőség azt jelenti, hogy a másik csúcs ennek másodszomszédja. Akkor viszont az első csúcsnak pontosan egy olyan szomszédja van, amelynek a második csúcs szomszédja. Tehát a gráf erősen reguláris, paraméterei: $n = r^2+1$, $k = r$, $\lambda = 0$, $\mu = 1$. Az integralitási feltétel azonnal adja, hogy $r = 2, 3, 7$ vagy 57 lehet csak. ∎

Az $r = 57$ eset mind a mai napig megoldatlan, $r = 2$-re az ötszög, $r = 3$-ra a Petersen gráf az (egyértelmű) megoldás. $r = 7$-re a következő ú. n. *Hoffmann–Singleton gráf*: azonosítsuk PG$(3,2)$ egyeneseit egy 7 elemű halmaz rendezetlen hármasaival olymódon, hogy két egyenes pontosan akkor legyen metsző, ha a megfelelő hármasoknak pontosan egy közös eleme van. A $\mathcal{H}$ gráf csúcsai a PG$(3,2)$ 15 pontja és 35 egyenese (azaz a gráfunk tényleg 50 pontú). A pontok páronként nem illeszkednek, egy pont akkor illeszkedik egy egyenesre, ha PG$(3,2)$-ben rajta van, két egyenes pedig akkor van összekötve, ha a nekik megfeleltetett hármasok diszjunktak. A 8.20. Feladatban ellenőrizhetjük, hogy így tényleg $(950, 7, 0, 1)$ paraméterű erősen reguláris gráfot kaptunk.

8.3 Feladatok

8.1., Biz. be a (2) tulajdonságot a Szélmalom tételben.

8.2., Biz. be a (3) tulajdonságot a Szélmalom tételben.

8.3., $u = 2, 3$-ra a szélmalom tételbeli kivételes gráfok egyértelműek.

8.4., A Schläfli-gráf (ld. Szélmalom tételt, 8.36) egyértelmű.

8.5., $\mu = 0$ esetén $G = rK_m$.

8.6., Az A adjacencia-mátrixra A^s elemei a szóbanforgó pontokat összekötő s hosszú séták számát adják.

8.7., Mely gráfokra teljesül $k = r$?

8.8., A $P(q)$ Paley-gráfok erősen regulárisak.

8.9., A 8.12-ben megadott Clebsch-gráf $(16, 5, 0, 2)$ paraméterű erősen reguláris gráf.

8.10., A 8.13-ban megadott Gewirtz-gráf $(56, 10, 0, 2)$ paraméterű erősen reguláris gráf.

8.11., 8.16 (Wielandt) bizonyításában $r = k$, $s = -k$ esetén a gráf a létra, vagy annak komplementuma.

8.12., Wielandt tételben a 2. esetben $s = 1$ esetén a Petersen-gráfot (és csak azt) kapjuk.

8.13., Lássuk be az erősen reguláris gráfok és blokkrendszerek kapcsolatának polaritásos alakját.

8.14., A Hall–Connor tételben ellenőrizzük λ és μ értékét.

8.15., $r \leq 7$-re a trianguláris gráf egyértelmű.

8.16., Négyzetes blokkrendszer bővítése kváziszimmetrikus.

8.17., Mutassuk meg, hogy egy gráf akkor és csak akkor erősen reguláris, ha adjacencia-mátrixát a vektor ortogonális kiegészítőjére megszorítva a megszorításnak pontosan két sajátértéke van.

8.18., 8.32 bizonyításában a $\bar{\Gamma}$ páros.

(Útmutatás 1.: mutassuk meg, hogy nincs benne páratlan kör;

Útmutatás 2.: A Turán tétel $|E(G)| \leq \alpha(G)\tau(G)$ alakjában mutassuk meg, hogy $\alpha(G) = n$ kell legyen!)

8.19., Az abszolút korlát bizonyításában a keletkező vektorok páronként különbözőek.

8.20., Hoffmann–Singleton gráf: biz. be, hogy azonosíthatjuk PG$(3,2)$ egyeneseit egy 7 elemű halmaz rendezetlen hármasaival olymódon, hogy két egyenes pontosan akkor legyen metsző, ha a megfelelő hármasoknak pontosan egy közös eleme van.

8.21. Mutassuk meg, hogy a Hoffmann-Singleton gráf erősen reguláris.

8.22. Mit mondhatunk 6 bőségű, és a lehető legkevesebb csúcsot tartalmazó erősen reguláris gráfról?

8.23. Bizonyítsuk be, hogy adott r-re és g-re van r-reguláris g bőségű gráf.

8.24. Egy r-reguláris g bőségű gráfnak legalább

$$1 + r + r(r-1) + \ldots + r(r-1)^{(g-3)/2}$$

csúcsa van, ha g páratlan, legalább

$$2(1 + (r-1) + \ldots + (r-1)^{(g-2)/2}$$

csúcsa, ha g páros.

8.25. Van olyan r-reguláris g bőségű gráf, amelynek legfeljebb

$$r(r-1)^g/(r-2)$$

csúcsa van.

8.26. Tegyük fel, hogy egy n csúcsú gráfban a maximális fok $n-2$, az átmérő 2. Mutassuk meg, hogy az élek száma legalább $2n-4$. Keressünk is ilyen gráfokat.

8.27. Az előző feladatban mi a helyzet, ha a maximális fok $n-3$ vagy $n-4$.

8.28.* Megint csak a 8.26-nak megfelelő a kérdés: ha $n \geq 13$ és a maximális fok $n-\ell$, $5 \leq \ell \leq (n+2)/2$, akkor az élek száma legalább $2n-4$.

8.29. Bizonyítsuk be, hogy a Shrikhande gráf (ld. 8.33) erősen reguláris.

8.30. Bizonyítsuk be, hogy a Chang gráfok (ld. 8.34) erősen regulárisak.

8.31. Nevezzünk *reguláris 2-gráf* nak egy X halmaz 3 elemű részhalmazainak egy olyan $\mathcal{B}$ halmazát nevezzük, hga bármely négyelemű $Y \subset X$-re páros sok $\mathcal{B}$-beli halmaz része Y-nak. Egy 2-gráf *reguláris*, ha $2-(n,3,\lambda)$-rendszer valamely λ-ra. Triviális példák az össze háromelemű részhalmaz alkotta 2-gráf, valamint az üres.

(a) Ha Γ egy gráf az $X = V(\Gamma)$-n, akkor azon 3 elemű halmazok $\mathcal{B}$ halmaza, melyeken Γ-nak páratlan sok éle feszül, 2-gráfot alkotnak.

(b) minden 2-gráf előáll az (a)-beli konstrukcióval.

(c) két gráf pontosan akkor adja az (a)-beli konstrukcióval ugyanazt a 2-gráfot, ha switching segítségével egymásba vihetők.

8.32. Keressünk olyan Y ponthalmazt, amelyre vonatkozó switching a $T(5)$-öt átviszi a Petersen gráfba.

8.33. Mutassuk meg, hogy $L_2(4)$, a Shrikhande-gráf és a Clebsch-gráf ugyanazon $2-(16,6,2)$ bisík különböző polaritásaink feleltethető meg.

9 DIFFERENCIA HALMAZOK

Mielőtt a differencia halmazok elméletébe belemerülnénk, lássuk azt a példát, amellyel elkezdődött a differencia halmazok története. Tekintsük a $\mathrm{PG}(2,q)$ projektív síkot. Ennek pontjai egy háromdimenziós $\mathrm{GF}(q)$ feletti vektortér 1-dimenziós alterei, az egyenesek pedig a 2-dimenziós alterek. Ilyen három dimenziós vektortér például a $\mathrm{GF}(q^3)$ véges test. Pontok tehát a nem-nulla testelemek ekvivalencia-osztályai, ahol $x \sim y$, ha létezik $0 \neq \lambda \in \mathrm{GF}(q)$, amelyre $\lambda x = y$. Három pont x, y, z akkor van egy egyenesen, ha alkalmas $\lambda, \mu, \nu \in \mathrm{GF}(q)$ elemekre $\lambda x + \mu y = \nu z$, vagy más szavakkal két pont által meghatározott egyenes pontjai a két pont $\mathrm{GF}(q)$-beli együtthatós lineáris kombinációi. Vegyük a $\mathrm{GF}(q^3)$ test multiplikatív csoportjának egy ω generátorelemét (algebrából tudjuk, hogy véges test multiplikatív csoportjá ciklikus), és tekintsük a $T_\omega : x \to x\omega$ leképezést. Ez bijekció és persze kompatibilis a $\sim$ relációval, így a projektív sík pontjain is bijekció. Természetesen a $\mathrm{GF}(q)$ feletti lineáris függést sem befolyásolja a T_ω alkalmazása, azaz egy egyenesbe eső ponthármas egy egyenesbe eső hármasba megy, és viszont. Ez magyarul azt jelenti, hogy T_ω kollineáció. Mivel ω generátorelem, T_ω a pontokat egyetlen ciklusban permutálja. Tekintsünk egy egyenest, mondjuk az $L = \{1 = \omega^0, \omega^{i_1}, \ldots, \omega^{i_q}\}$ egyenest. Mi lesz az LT_ω egyenes? Nem más, mint az $\{\omega, \omega^{i_1+1}, \ldots, \omega^{i_q+1}\}$, halmaz. Hasonlóan az LT_ω^j halmaz is egyenes, ami nem más, mint $\{\omega^j, \omega^{i_1+j}, \ldots, \omega^{i_q+j}\}$. Az 1.20 Tétel miatt T_ω-nak és valamennyi hatványának ugyanannyi fixpontja van az egyeneseken, mint a pontokon, így T_ω nemcsak a pontokat, hanem az egyeneseket is egy orbitban permutálja. Ez azt jelenti, hogy LT_ω^j alakban minden egyenest megkapunk.

Nézzük meg, mit jelent ez az L-beli elemek kitevőire! Mivel két ponton át megy egyenes, minden i-re létezik olyan j, hogy az $1, \omega^i$ pontok rajta vannak az LT_ω^j egyenesen. Ez azt jelenti, hogy van olyan i_1, i_2 kitevő, melyre $i_1 + j = 0$, $i_2 + j = i$, azaz $i_1 - i_2 = i$. Másrészt pontosan egy ilyen i_1, i_2 pár van, hiszen ha kettő lenne, akkor két különböző j-t is lehetne találni, vagyis az 1 és ω^i pontokon két különböző egyenes menne. Így tehát egy egyenes pontjainak kitevői a mod (q^2+q+1) additív csoportban olyan $(q+1)$ elemű D halmazt alkotnak, hogy bármely nem-nulla csoportelem pontosan egyféleképpen áll elő két D-beli elem különbségeként. Innen ered a *differencia halmaz* elnevezés. Ez az észrevétel a projektív síkok egy nagyon szép ciklikus reprezentációját teszi lehetővé (ld. a 9.1–2. Feladatokat). Jegyezzük meg, hogy megfigyelésünk ekvivalens azzal, hogy a testre épített síkok illeszkedési mátrixa ciklikus alakra hozható.

Természetesen a fenti eljárás megismételhető $\mathrm{PG}(2,q)$ helyett az n dimenziós $\mathrm{PG}(n,q)$ projektív térre is. Ezt Singer vette észre a harmincas években és eredménye a differencia halmazok vizsgálatának kiindulópontja lett.

Ezt a szituációt fogjuk kicsit általánosabban négyzetes blokkrendszerekre megvizsgálni.

Idézzük emlékezetünkbe az 1. fejezetből a Burnside-lemmát, valamint azokat a tételeket (1.20, 1.22), amelyek négyzetes illeszkedési struktúrák automorfizmusainak pontokon és blokkokon való hatásáról szólnak. Ezek többek között azt is maguk után vonják, hogy ha egy automorfizmuscsoport egy négyzetes (és nem-szinguláris incidencia mátrixú) illeszkedési struktúra pontjain regulárisan hat, akkor a blokkokon is automatikusan reguláris. Mi ilyen blokkrendszereket fogunk részletesebben szemügyre venni.

Definíció 9.1 Legyen G (additívan írt) véges Abel-csoport. A $D \subset G$ részhalmazt (v, k, λ) *differencia halmaz*nak nevezzük, ha $|G| = v$, $|D| = k$, és minden $0 \neq g \in G$-re pontosan λ db olyan $d, d' \in D$ pár van, melyre $d - d' = g$.

Definíció 9.2 Legyen G a $\mathbf{D}$ négyzetes blokkrendszer olyan automorfizmuscsoportja, amely reguláris a pontokon (és így 1.22 miatt a blokkokon is). Egy ilyen G-t *Singer-csoport*nak nevezünk.

Tétel 9.3 *Legyen $k < v$, G pedig v elemű véges Abel-csoport. Pontosan akkor létezik $D \subset G$ (v, k, λ) differencia halmaz, ha létezik olyan $\mathbf{D}$ négyzetes $2-(v, k, \lambda)$ blokkrendszer, amelynek G Singer-csoportja.*

Bizonyítás. Legyen $D \subset G$ differencia halmaz. Definiáljuk a

$$\mathbf{D}(D) = (\mathbf{P}(D), \mathbf{B}(D), \in)$$

blokkrendszert a következőképpen: $\mathbf{P}(D) = G$, $\mathbf{B}(D) = \{D + g : g \in G\}$. Azonnal látható, hogy $\mathbf{D}(D)$ négyzetes $2-(v, k, \lambda)$ blokkrendszer és a G-vel izomorf $\{\tau_g : x \to x + g \ : \ g \in G\}$ csoport valóban reguláris a pontokon.

Megfordítva tegyük fel, hogy $\mathbf{D}$ négyzetes blokkrendszer a G Singer-csoporttal. Mivel G reguláris a pontokon, válasszunk ki egy p alappontot és minden más pontot azonosítsunk azzal a $g \in G$ csoportelemmel, amely p-t ebbe a pontba viszi. Egy B alapblokk pontjaihoz ilymódon tartozó csoportelemek egy D differencia halmazt alkotnak a G csoportban. Legyen ugyanis $0 \neq g \in G$. A p és p^g pontok λ darab blokkban vannak benne. Mivel G a blokkokon is reguláris, ezeket felírhatjuk $B^{g_1}, \ldots, B^{g_\lambda}$ alakban. A p^g pont pontosan akkor van benne ezekben a blokkokban, ha $p \in (B^{g_j})^{g^{-1}} = B^{g_j - g}$. A p alappont viszont akkor van benne a $B^{g_j - g}$ blokkban, ha $p^{g - g_j} \in B$. Ez viszont éppen azt jelenti, hogy g λ-féleképpen áll elő D-beli elemek különbségeként. ∎

Jegyezzük meg, hogy G Abelségét csak arra használtuk, hogy ne kelljen figyelni az összeadások sorrendjére, a tétel nem-Abel G-re is igaz (ld. 9.3. Feladat).

Példa 9.4 A mod 7 additív csoportban $D = \{0, 1, 3\}$ differencia halmaz, a megfelelő blokkrendszer a Fano-sík. A mod 11 additív csoportban a $D = \{1, 3, 4, 5, 9\}$ differencia halmaz, a megfelelő blokkrendszer Hadamard-féle (ez a Paley-konstrukció, ld. 6.27).

A bevezetőben projektív síkokra látott Singer-konstrukciót tételként is megfogalmazzuk.

Tétel 9.5 (Singer) *A mod v additív csoportban, ahol $v = (q^{n+1} - 1)/(q - 1)$ létezik differencia halmaz a $k = (q^n - 1)/(q - 1)$, $\lambda = (q^{n-1} - 1)/(q - 1)$ paraméterekkel.* ∎

Természetesnek tűnik a kérdés, hogy mennyire egy–egyértelmű a kapcsolat a blokkrendszer, a Singer-csoport és a differencia halmaz között. Két differencia halmazt *izomorf*nak szoktak hívni, ha a megfelelő $\mathbf{D}(D)$ blokkrendszerek izomorfak. Ebből még az sem következik, hogy a megfelelő csoportok izomorfak (ld. 9.4. Feladat). Ugyanazon csoport két differencia halmaza *ekvivalens*, ha van olyan csoport-automorfizmus, amely egyiket a másikba viszi. Kibler adott példát azonos csoportban izomorf, de nem ekvivalens differencia halmazokra. Érdemes megemlíteni, hogy ciklikus csoportok esetén mindmáig megoldatlan, hogy vannak-e izomorf, de nem ekvivalens differencia halmazok.

A differencia halmazok konstrukcióit nem szaporítjuk, több végtelen család ismert (McFarland, Spence, Hall és mások konstruáltak ilyeneket), mi csak egy már látott családra és annak közvetlen általánosításaira szorítkozunk.

Tétel 9.6 *A $GF(q)$ test additív csoportjában, ha $q \equiv 3 \pmod 4$, a kvadratikus maradékok differencia halmazt alkotnak. Ha $q = 4t^2 + 1$, t páratlan, akkor a negyedik hatványmaradékok differencia halmazt alkotnak.* ∎

A 9.5–6. Feladatokban keressük meg a 9.6 Tételbeli differencia halmazok paramétereit, míg a 9.7–8. Feladatok további konstrukciókat tartalmaznak.

Legyen $D \subset G$ differencia halmaz. A fő kérdés az, hogy tudunk-e további automorfizmusokat találni $\mathbf{D}(D)$-ben a G elemeivel való eltolásokon kívül. Nézzük először a Fano-sík példáját: itt $G = C_7$,a pontok a mod 7 maradékosztályok, a blokkok $D = \{1, 2, 4\}$ eltoltjai és a 2-vel való szorzás ilyen automorfizmus lesz, (ami ráadásul D-t önmagába viszi. Az egyszerűség kedvéért mi csak azzal az esettel foglalkozunk, amikor G Abel-csoport. A Fano-sík esetében az ‘extra’ automorfizmus egy a csoport rendjével való szorzás volt. Általában is ilyenszerű automorfizmusok létezését tudjuk garantálni. Lássuk ugyanezt precízen:

Definíció 9.7 *(M. Hall)* Legyen $D \subset G$ differencia halmaz, G (additívan írt) Abel-csoport, t egy $|G|$-hez relatív prím természetes szám. t-t (numerikus) *multiplikátor*nak nevezzük, ha a t-vel való szorzás a $\mathbf{D}(D)$ blokkrendszer automorfizmusát indukálja.

Megjegyzés 9.8 Szoktak nem-Abel (vagy nem ciklikus) csoportokat is tekinteni, ekkor a multiplikátorok nem természetes számok, hanem G olyan automorfizmusai, amelyek a $\mathbf{D}(D)$ blokkrendszer automorfizmusát indukálják. Ha Abel-csoport esetén az automorfizmus egy t elemmel való szorzás, akkor t-t *numerikus multiplikátor*nak szokták nevezni. Mi azonban csak ilyen numerikus multiplikátorokkal foglalkozunk, így a numerikus jelzőt is elhagyjuk. Jegyezzük meg, hogy ciklikus csoportok esetén minden multiplikátor numerikus.

Marshall Hall volt az első, aki ú. n. multiplikátor-tételeket bizonyított. Ezek olyan tételek, amelyek valamely, csupán a blokkrendszer (ill. a differenciahalmaz) paramétereiből előállított számról garantálják, hogy ő numerikus multiplikátor. A multiplikátor-tételek differencia halmazok nem-létezésének bizonyítására használhatók fel, valamint differencia-halmazok megkonstruálására ill. egyértelműségük igazolására. Ehhez segít az alábbi két észrevétel.

Tétel 9.9 *1) Minden multiplikátor fixálja D valamely eltoltját.*

2) Ha G Abel és $(v, k) = 1$*, akkor van olyan eltoltja a D differencia halmaznak, amelyet minden multiplikátor fixál.*

Bizonyítás. 1) Minden multiplikátor fixálja a 0 elemet (az alappontot), így 1.20-ből adódóan egy blokkot is. $\mathbf{D}(D)$ blokkjai pedig éppen D eltoltjai.

2) Legyen α a D differencia halmaz összes elemének összege. Mivel $(v, k) = 1$, k-val tudunk osztani G-ben. Tekintsük a $D' = D - \alpha/k$ eltoltat. A D' elemeinek összege 0, míg $D' + g$-é kg. Mivel a multiplikátor automorfizmus, olyan eltoltat, melyben az elemek összege 0, ugyanilyenbe visz. A fenti észrevétel alapján azonban ilyen csak maga a D' van, hisz $kg = 0$-ból $g = 0$ következik. ∎

Most már látjuk, hogy ha ismerünk néhány multiplikátort, akkor ezt a minden multiplikátor által fixált blokkot (eltoltat) megprróbálhatjuk felírni. Azt talán jegyezzük meg, hogy a $(v, k) = 1$ feltétel nem hagyható el, az $\langle a, b, c, d\rangle$ által generált elemi Abel 2-csoportban a $\{0, a, b, c, d, a + b + c + d\}$ halmaz $(16, 6, 2)$ differencia-halmaz, de egyetlen eltoltját sem fixálja valamennyi multiplikátor (persze itt a multiplikátorok nem numerikusak).

Mielőtt belátnánk M. Hall és H.J. Ryser multiplikátor tételét, idézzük fel a csoportgyűrű fogalmát. Legyen G (ezúttal multiplikatívan írt!) csoport. A $\mathbf{Z}[G]$ csoportgyűrű elemei a $\sum_{g\in G} a_g g$ alakú formális összegek, ahol $a_g \in \mathbf{Z}$. A szorzás és összeadás műveleteket a természetes módon értelmezzük $\mathbf{Z}[G]$-n.

Jelölés. Ha $A = \sum_{g\in G} a_g g \in \mathbf{Z}[G]$, akkor legyen $A^{(t)} = \sum_{g\in G} a_g g^t$ (azaz szemléletesen ez a "tagonkénti hatványozás".

Ha $X \subset G$, akkor $\bar{X}$ jelöli a csoportgyűrű $\sum_{g\in X} g$ elemét.

Lemma 9.10 *Legyen D differenciahalmaz a G Abel-csoportban, valamint* $X \subset G$*. A* $\bar{X}\bar{D}^{(-1)}$ *szorzatban a* $g \in G$ *csoportelem* a_g *együtthatója éppen* $|X \cap (D + g)|$ *(ahol persze* $D + g$ *nem a csoportgyűrű eleme, hanem D eltoltja, mely a megfelelő blokkrendszer blokkja).*

Bizonyítás. A szóbanforgó együttható azt számolja, hogy $x - d$ alakban hányszor áll elő g, ahol $x \in X$, $d \in D$. ∎

Lemma 9.11 *Ha egy négyzetes* $2 - (v, k, \lambda)$*-rendszer valamely k pontú S ponthalmaza minden blokkot legalább* λ *pontban metsz, akkor maga is blokk.*

Bizonyítás. Először gondoljuk meg, hogy van olyan blokk, amely λ-nál több pontot tartalmaz S-ből. Ha ugyanis minden blokk λ pontban metszené S-et, akkor $x \in S$-re leszámolva az (y, B) párokat, ahol $x \in B$, $x \neq y \in S \cap B$, azt kapnánk, hogy $k(\lambda - 1) = \lambda(k - 1)$.

Vegyük azt a B blokkot, amely a lehető legtöbb pontot tartalmazza a mi S ponthalmazunkból. Feltehetjük tehát, hogy $|S \cap B| > \lambda$. Ha $S \neq B$, akkor legyen $x \in B \setminus S$. Az illeszkedő (p, B') ($p \in S \cap B'$, $x \in B'$, $B' \neq B$) párok kétféle leszámlálásával kapjuk, hogy $(k - 1)\lambda \leq \lambda k - |S \cap B|$. Felhasználva, hogy $|S \cap B| > \lambda$ ez nem lehetséges, vagyis csak $S = B$ lehetett. ∎

Tétel 9.12 (M. Hall, H. J. Ryser, első multiplikátor tétel) *Legyen* $D \subset G$ *differencia halmaz a G Abel-csoportban, és legyen p az* $n = k - \lambda$ *olyan prímosztója, amely relatív prím* $v = |G|$*-hez. Ha* $p > \lambda$*, akkor p multiplikátora D-nek.*

Bizonyítás. Ez az egyszerű és elegáns bizonyítás Alexander Pott-tól származik.

Jelöljük $\bar{D}$-vel a $\mathbf{Z}G$ csoportgyűrű $\bar{D} = \sum_{d\in D} d$ elemét. A D pontosan akkor differenciahalmaz, ha a $\bar{D}\bar{D}^{(-1)} = \lambda\bar{G} + (k - \lambda)\bar{1}$ (Itt 1 a G csoport semleges eleme). A $\bar{D}^{(p)} = \bar{X}$ valamely $X \subset G$-re. Azt szeretnénk megmutatni, hogy $X = D + g$-vel valamely $g \in G$-re. Ehhez az előző lemma szerint azt kéne belátni, hogy X minden blokkot legalább λ pontban metsz, ami az utolsó előtti lemma miatt azt jelenti, hogy $\bar{X}\bar{D}^{(-1)}$-ben minden együttható legalább λ.

A trükk az, hogy áttérünk a $\mathrm{GF}(p)[G]$ csoportgyűrűre. Mint megjegyeztük, ez nyilván homomorfizmus, nem történik más, csak az együtthatókat modulo p tekintjük. Ekkor viszont a p-edik hatványra emelés az együtthatókat nem változtatja, azaz $\bar{D}^p$ helyett írhatunk $\bar{D}^{(p)}$-t.

Tekintsük tehát a $\bar{X}\bar{D}^{(-1)}\bar{D}^{(p)}\bar{D}^{(-1)} = \bar{D}^p\bar{D}^{(-1)}$ szorzatot $\mathrm{GF}(p)[G]$-ben. Leválasztva egy $\bar{D}$ tényezőt, $\bar{D}^{p-1}(\bar{D}\bar{D}^{(-1)})$-et kapunk. A zárójelben szereplő tag $\lambda\bar{G} + (k - \lambda)\bar{1}$, de az utolsó tag 0 mod p. Így a $\bar{D}^p\bar{D}^{(-1)}$ szorzat $\mathrm{GF}(p)[G]$-ben $\lambda\bar{D}^{p-1}\bar{G}$. A csoportgyűrű egy A elemét viszont nagyon könnyű megszorozni

$\bar{G}$-vel, az eredmény az A-beli együtthatók összege szorozva $\bar{G}$-vel. Eszerint $\bar{D}\bar{G} = k\bar{G}$, $\bar{D}^2\bar{G} = k^2\bar{G}$, s. í. t., $\bar{D}^{p-1}\bar{G} = k^{p-1}\bar{G}$. Mivel p nem osztja k-t, a kis Fermat tétel miatt $k^{p-1} = 1$ (modulo p), azaz $\bar{D}^p\bar{D}^{(-1)} = \lambda\bar{G}$ a $\mathrm{GF}(p)[G]$-ben.

Visszatérve a $\mathbf{Z}[G]$ csoportgyűrűre ez azt jelenti, hogy $\bar{X}\bar{D}^{(-1)}$-ben minden együttható legalább λ (itt használjuk, hogy $\lambda < p$, ami a tételt megelőző lemmák miatt elég. ∎

Történetileg M. Hall először a $\lambda = 1$ esetre (azaz projektív síkok esetére, és ciklikus Singer-csoportra) látta be a tételt. A $p > \lambda$ feltételt az ismert bizonyítások lényegesen kihasználják, de mindenki azt sejti, hogy ez csupán technikai nehézség, valójában $k-\lambda$ minden v-hez relatív prím prímosztója multiplikátor. Ennek a **multiplikátor-sejtés**nek a bizonyítására sok erőfeszítés történt, s ezek eredményeként több komplikáltnak tűnő, de jól használható multiplikátor-tételt ismerünk. Ezekkel bizonyos λ-nál kisebb p-kről is kimutatható, hogy multiplikátorok, a $p > \lambda$ feltételt azonban mindmáig nem sikerült teljesen eliminálni. Az általunk ismertetett Pott féle bizonyítás tipikus abban az értelemben, hogy szinte valamennyi bizonyítás a csoportgyűrűt használja (M. Hall eredeti bizonyítása is). A Pott-féle bizonyítás jó arra is, hogy legalább érzékeltethessük a differencia halmazoknál tipikus bizonyítási eljárásokat. Általában az történik, hogy a csoportgyűrűbeli egyenletre, mint amilyen esetünkben a

$$\bar{D}\bar{D}^{(-1)} = \lambda\bar{G} + (k-\lambda)\bar{1}$$

egyenlet, a G csoport karaktereit alkalmazzuk. G Abel-csoport lévén ezek a komplex egységgyökök multiplikatív csoportjába vivő homomorfizmusok, így az alapegyenletből egy alkalmas körosztási test algebrai egészei közötti egyenlet adódik. Erről az egyenletről algebrai számelméleti módszerekkel gyakran lehet mondani valamit, és abból többször tudunk információt nyerni magáról az eredeti egyenletről.

Lássuk az eddigi eredmények néhány alkalmazását differencia-halmazok nemlétezésének bizonyítására ill. differencia-halmazok konstrukciójára.

Példa 9.13 1) Keressünk $(37, 9, 2)$ differencia halmazt. Ekkor a csoport ciklikus, $n = 7$. Így 7 multiplikátor. Mivel van olyan D differencia halmaz, amelyet a 7-tel való szorzás fixen hagy, és feltehetjük, hogy $1 \in D$, így $D = \{1, 7, 7^2, \ldots\}$. Ez tényleg differencia halmaz, és persze lényegében egyértelmű.

2) Keressünk $(23, 11, 5)$ ill. $(21, 5, 1)$ differencia halmazt. Ld. a 9.11. Feladatot.

3) Nem létezik $(31, 10, 3)$ differencia halmaz. Valóban a 7 multiplikátor és a 7 által fixált halmaznak (7 hatványai) több, mint tíz eleme lenne.

4) Nem létezik ciklikus $(111, 11, 1)$ differencia halmaz. Mind 2, mind 5 multiplikátor lenne ugyanis, részletesen ld. a 9.12. Feladatot.

Állítás 9.14 *Nem létezik ciklikus projektív sík, ha rendje osztható* 6*-tal.*

Bizonyítás. Valóban, $2, 3$ multiplikátorok lennének, és lenne olyan D differencia halmaz, amelyre $D = 2D = 3D$. Ekkor viszont c, $2c$, $3c$ mind D-beli lenne, ami nem lehet, mert $3c - 2c = 2c - c$. ∎

Mielőtt a multiplikátor-tétel(ek) alkalmazásait néznénk meg, lássunk két további ilyen tételt.

Tétel 9.15 (második multiplikátor-tétel, Menon; Arasu–Xiang) *Legyen D (v, k, λ) differencia halmaz a v^* exponensű G véges Abel-csoportban. Legyen t egy a v-hez relatív prím egész szám, és legyen n_1 osztója $n = k - \lambda$-nak. Legyen $n_1 = p_1^{e_1} \ldots p_s^{e_s}$ az n_1 törzstényezős felbontása és végül legyen $n_2 = n_1/(v, n_1)$. A p_i prímtényezőkhöz definiáljuk a q_i számokat a következőképp:*

$$q_i = \begin{cases} p_i & \text{ha } p_i \text{ nem osztja } v\text{-t} \\ l_i & \text{ha } v^* = p_i^r u_i,\ (p_i, u_i).\ \text{Itt } l_i \text{ olyan egész,} \\ & \text{melyre } (l_i, p_i) = 1, \text{ és } l_i \equiv p_i^f \pmod{u_i}. \end{cases}$$

Tegyük fel, hogy minden i-re van olyan f_i egész szám és s_i multiplikátor, melyre $s_i q_i^{f_i} \equiv t \pmod{v^*}$. Ha $n_2 > \lambda$ vagy ha a $\mathbf{Z}[G]$-beli $FF^{(-1)} = (n/n_2)^2$ egyenletnek csak a triviális $F = (n/n_2)g$ megoldásai vannak ($g \in G$), akkor t multiplikátor. ∎

Azt mindenképpen érdemes megjegyezni, hogy ebből az ijesztően hangzó tételből az első multiplikátor tétel azonnal következik. Érdemes ennek a tételnek egy egyszerűbb alakját is megfogalmazni (történetileg persze ez keletkezett elő ször: ciklikus csoportokra Hall, általánosabban Menon igazolta).

Tétel 9.16 (Menon, Hall) *Legyen D Abel-féle (v, k, λ) differencia-halmaz és legyen $m > \lambda$ olyan osztója n-nek, amely relatív prím v-hez. Legyen továbbá t olyan v-hez relatív prím egész, amely teljesíti a következő feltételt: minden $p|m$ prímre van olyan f, amelyre $t \equiv p^f \pmod{v^*}$, ahol v^* a G exponense. Ekkor t (numerikus) multiplikátor.*

Ezek a tételek elsősorban a nem-ciklikus esetben hasznosak, így most mi itt megállunk.

9.1 Feladatok

9.1., Nevezzük egy q^2+q+1 oldalú szabályos sokszög egy rész k-szögét teljesen szabálytalannak, ha a csúcsai között fellépő távolságok mind különbözők. Mutassuk meg, hogy $k \leq q+1$ és $k = q+1$ esetén a teljesen szabálytalan részsokszög elforgatottjai egy projektív sík egyenesei lesznek.

9.2., Mutassuk meg, hogy a előző feladatban definiált teljesen szabálytalan részsokszög differencia-halmaznak felel meg a (q^2+q+1)-edrendű ciklikus csoportban.

9.3., Terjesszük ki 9.3-at a nem-Abel esetre.

9.4., ** példa nem izomorf csoportokra, amelyek uazt a blokkrendszert adják **

9.5., A négyzetelemek alkotta differenciahalmaz paraméterei.

9.6., A negyedik hatványok alkotta differenciahalmaz paraméterei.

9.7., McFarland konstrukció

9.8., $C_2 \times C_4 \times C_4 \times C_3$-ban a

$$(0000), (0001), (0002), (0020), (0101), (0031), (0132), (0200), (0212), (0220)$$
$$(0221), (0302), (1012), (1101), (1132), (1201), (1211), (1222), (1231)(1322)$$

elemek $(96, 20, 4)$ differencia halmazt alkotnak.

9.9., Legyen $q = s^2$, s prímhatvány. Mutassuk meg, hogy egy ciklikus q-adrendű projektív síknak van s-edrendű részsíkja (méghozzá egy ilyent a ciklizálás szerinti (s^2-s+1)-edik pontok adnak.

9.10., Tükrözzük a 9.1 Feladatbeli teljesen szabálytalan részsokszöget az eredeti (q^2+q+1)-szög egy tengelyére. Mutassuk meg, hogy az így kapott halmaznak nincs három kollineáris pontja.

9.11., Keressünk $(23, 11, 5)$ differencia halmazt és ciklikus $(21, 5, 1)$ differencia-halmazt.

9.12., Nincs ciklikus $(111, 11, 1)$ differencia halmaz.

9.13., Mit ad az 1.24 tétel projektív síkok polaritásaira?

10 LINEÁRIS KÓDOK

Az algebrai kódelmélet a következő feladattal foglalkozik: tegyük fel, hogy egy üzenetet el szeretnénk juttatni egyik helyről a másikra. Az a csatorna azonban, amin az üzenetet továbbítjuk, zajos: nem pontosan ugyanaz az üzenet érkezik meg, mint amit elküldtünk. Ahhoz, hogy a fogadó ki tudja találni az eredeti üzenetet, azt redundánssá tesszük, s így remélhetőleg még az elromlott információból is kitalálható az eredeti. Számítógépeknél gyakran használják a "paritás-ellenőrző bit"-et: az üzenet egy 0-1 sorozat, s a végére aszerint írunk 0-t vagy 1-et, hogy az üzenetben páros vagy páratlan sok egyes volt. Általában az üzenetet (rögzített hosszú) vektoroknak tekintjük (valamely véges test felett). Tipikus esetben a test a kételemű GF(2), de más testek is szóba jöhetnek (pl. ha színeket akarunk kódolni képpontokban). A küldő tehát kiindul egy $\mathbf{m}$ üzenetből, ezt valamilyen módon (redundánsan) kódolja egy GF(q) feletti n hosszú $\mathbf{v}$ vektorrá. A fogadó $\mathbf{v}$ helyett egy $\mathbf{w}$ vektort kap. Természetesen a két fél megállapodik a kódolási eljárásban, így a fogadó tudja, hogy mik az értelmes üzenetek (pl. betűk). Ezután megkeresi azt az értelmes üzenetet, amely a $\mathbf{w}$-ből a legkevesebb változtatással kapható, és ezt tekinti a küldött üzenetnek. Ezt a lépést *dekódolás*nak nevezzük. Az eljárás precíz leírásához szükségünk van néhány definícióra.

A jelen jegyzetben nem célunk a kódelmélet bemutatása, elsősorban a Golay-kódok, és a belőlük kapható Witt-féle blokkrendszerek bemutatása a célunk. Ennek megfelelően csak egy-egy kódot fogunk bemutatni, és a dekódolási algoritmusok leírását (amelyek pedig a gyakorlati alkalmazások szempontjából sorsdöntő jelentőségűek) teljesen mellőzzük.

Definíció 10.1 A GF(q) test feletti n dimenziós $V(n,q)$ vektortér két elemének *Hamming távolságá*n a két vektor különböző koordinátáinak számát értjük. Egy vektor *súly*a a nullvektortól mért távolsága. A $V(n,q)$ részhalmazait *kód*nak, lineáris altereit *lineáris kód*nak nevezzük. A kódhoz tartozó vektorokat *kódszavak*nak nevezzük. Az altér dimenziója a kód *dimenzió*ja, n-et a kód *hosszá*nak hívjuk. A C kód *minimális súlya* a legkisebb súlyú nullvektorról különböző C-beli elem súlya. Lehetne definiálni a C kód *minimális távolságá*t is, mint a különböző vektorok közötti távolságok minimumát, de lináris kódokra ez persze megegyezik a kód minimális súlyával. Ha tehát C éppen k-dimenziós altér, és C minimális súlya d, akkor C-t $[n,k,d]$ kódnak nevezzük. Ha a kód nem lineáris, akkor a k dimenzió helyett a kódszavak számát tüntetjük fel, a minimális súly helyett pedig a minimális távolságot, így ilyenkor (n,M,d)-kódról beszélünk. Persze lineáris kódra $M=q^k$ volna.

Egy C kód e hibát képes (a természetes módon a legnagyobb valószínűség elve alapján) javítani, ha $2e<d$. Az *e-hibajavító* tulajdonságot úgy is megfo-

galmazhatjuk, hogy a kódszavak köré írt e sugarú gömbök diszjunktak legyenek.

Ebből máris megkaphatjuk az első nem-triviális egyenlőtlenséget a kód paraméterei között, ez a *Hamming-korlát*:

Tétel 10.2 *Ha egy GF(q) test feletti (n, M, d) kód e hibát javít, akkor*

$$M \sum_{i=0}^{e} \binom{n}{i} (q-1)^i \le q^n.$$

Bizonyítás. A bal oldalon levő összeg az e sugarú gömbben levő vektorok számát adja meg. ∎

Azokat a kódokat, amelyekre a 10.2 Tételben egyenlőség teljesül, *perfekt*nek nevezzük. Ilyenkor tehát a kódszavak köré rajzolt e sugarú gömbök egyrétűen és hézagtalanul kitöltik az n dimenziós GF(q) feletti vektorteret. Mivel a perfekt kódok a lehető legjobb kódok, így fontos minél több ilyet ismerni. Erre a kérdésre nemsokára visszatérünk.

A gyakorlatban a kódolással két célunk van, egyrészt minél jobb hibajavító képességet elérni, másrészt mindezt nem túl nagy kódhosszal. Vegyük észre, hogy a C kód dimenziója a továbbítható üzenetek számával van kapcsolatban, tehát k-t állandónak tekinthetjük. A minimális súly ugyancsak (általában műszaki feltételekből számítható) konstans, így fix k (vagy M) és d mellett a lehető legkisebb n-et szeretnénk elérni.

Mielőtt a lineáris kódok vizsgálatára térnénk, lássunk egy "jó" nem-lineáris kódot.

Legyen H_n egy n-edrendű Hadamard-mátrix. Cseréljük ki a -1-eket 0-ra H_n-ben és $-H_n$-ben. Ezen két mátrix sorai $2n$ darab n hosszú $0-1$ vektort adnak meg. Legyen a H Hadamard-kód ezen $2n$ vektor halmaza. Mivel egy Hadamard-mátrix két sora pontosan $n/2$ pozícióban tér el, könnyű látni, hogy ezen a módon egy $n/2$ minimális távolságú kódot kapunk (a részleteket ld. a 10.1. Feladatban). Ez a kód azért érdekes, mert az $n = 32$ esetben éppen ezt használta 1969-ben a Mariner Mars-szonda. Látható, hogy ebben az alkalmazásban a nagy hibajavító képesség volt lényeges, hisz pl. a dekódolás a Földön történt, ami gyakorlatilag nem jelentett időbeli korlátozást. Hasonló jellegű, nagy minimális távolságú nem-lineáris kódot kaphatunk a Paley-mátrixból is (ld. 10.2. Feladat.)

Természetes kérdés, hogy hogyan adhatunk meg lineáris kódokat? Elegendő, ha C egy bázisát adjuk meg. Ha ennek a bázisnak az elemeit egy

mátrix soraiba írjuk, akkor így a C kód egy *generátormátrixát* kapjuk. Eszerint a G generátormátrixból a kódszavakat (C elemeit) a sorok lineáris kombinációjaként kapjuk meg. Érdemes megemlíteni, hogy alkalmas bázist választva mindig elérhetjük, hogy a generátormátrix első k oszlopában egységmátrix legyen. Generátormátrixszal adott lineáris kódok esetén a kódolás nagyon egyszerű, a kódolandó (k hosszú!!) üzenetet egyszerűen megszorozzuk a G mátrixszal. Ha tehát el akarjuk dönteni, hogy egy $\mathbf{w} \in V(n, q)$ vektor hozzátartozik-e a C kódhoz, akkor a $\mathbf{w} = \mathbf{x}G$ egyenletet kellene megoldanunk. Ezt egyszerűbben is megtehetjük, ha ismerjük C ortogonális kiegészítőjét.

Definíció 10.3 Vezessük be $V(n, q) = V$-n a szokásos skaláris szorzást, azaz az $\mathbf{x} = (x_1, \ldots, x_n)$ és $\mathbf{y} = (y_1, \ldots, y_n)$ vektorok skaláris szorzata legyen $\mathbf{xy} = \sum_{i=1}^{n} x_i y_i$. A C kód *duális*a a $C^\perp = \{\mathbf{w} \in V \ : \ \mathbf{wx} = 0, \ \forall \ \mathbf{x} \in C\}$ kód. Ha H a $C^\perp$ duális kód egy generátormátrixa, akkor H-t a C kód *paritásellenőrző* mátrixának nevezzük.

Ez azt jelenti, hogy H sorai ortogonálisak a kódszavakra, azaz C elemei éppen azok az $\mathbf{x}$ vektorok, amelyekre $H\mathbf{x}^T = 0$ teljesül. Azt is könnyű látni, hogy (lineáris) $[n, k, d]$ kód duálisa lineáris $[n, n-k, d']$ kód, alkalmas d'-re. Ha egy kód generátormátrixa a kanonikus $(I_k \ A)$ alakban van adva, akkor a paritásellenőrző mátrix felírható $(-A^T \ I_{n-k})$ alakban. Itt szokás szerint I_n az $n \times n$-es egységmátrixot jelöli.

Lássuk először a világ legegszerűbb sok hibát javító kódját, az ismétléskódot ("Hát maga megbolondult, hát maga megbolondult, hogy mindent kétszer mond, hogy mindent kétszer mond...").

Definíció 10.4 $[n, 1, n]$ *ismétlés-kód*nak nevezzük az $(1, \ldots, 1)$ által generált (egydimenziós) lineáris kódot.

Definíció 10.5 Legyen $n = (q^k - 1)/(q - 1)$. Az $[n, n-k]$ *Hamming-kód* olyan kód melynek paritásellenőrző mátrixában az oszlopok éppen a GF(q) test feletti k hosszú nemnulla oszlopvektorok, méghozzá, úgy, hogy két oszlop ne legyen egymás konstansszorosa. (Úgy is mondhatnánk, hogy az oszlopok a PG$(k-1, q)$ pontjai(nak egy-egy reprezentánsa).)

A legegyszerűbb ilyen kód a $q = 2$, $k = 3$ esetnek megfelelő bináris $[7, 4]$ Hamming-kód. Ekkor a paritásellenőrző mátrix a

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Általában a bináris $(q = 2)$ esetben a paritásellenőrző mátrix oszlopai pontosan az $1, 2, \ldots, 2^{k-1}$ számok kettes számrendszerben felírt alakjai.

Tétel 10.6 *A Hamming-kódok perfektek (minimális súlyuk 3).*

Bizonyítás. Az 1 sugarú gömb mérete $1 + n(q-1) = 1 + (q^k - 1) = q^k$, $M = q^{n-k}$, azaz a 10.2 Tételben valóban egyenlőség van. ∎

Alapvetően fontos észrevétel, hogy a H paritásellenőrző mátrixból ki tudjuk olvasni a kód minimális távolságát.

Állítás 10.7 *A C kód minimális távolsága pontosan akkor d, ha a paritásellenőrző mátrix bármely $d-1$ oszlopa független, de van d olyan oszlop, amelyek lineárisan összefüggők.*

Bizonyítás. A kód egy d súlyú vektora éppen d oszlopra ad meg lineáris összefüggést. ∎

Az alábbi következmény fontos korlátot mond a minimális súlyra.

Tétel 10.8 (Singleton-korlát) *Ha C lineáris $[n, k, d]$ kód, akkor $d \leq n - k + 1$.*

Bizonyítás. Mivel a paritásellenőrző mátrix mérete $(n-k) \times n$, így rangja legfeljebb $(n-k)$, azaz $(n-k)$-nál több oszlop nem lehet független. ∎

Definíció 10.9 *Ha a C kódra $d = n - k + 1$, akkor a kódot* M.D.S. *kódnak (Maximum Distance Separable) nevezzük.*

Állítás 10.10 *M.D.S. kód duálisa is M.D.S.*

Bizonyítás. A duális kód hossza n, dimenziója $n-k$, így azt kell belátnunk, hogy minimális súlya $k+1$. Legyen H a kód paritásellenőrző mátrixa, amely egyben az ortogonális kód generátormátrixa. Legyenek $\mathbf{h}_1, \ldots, \mathbf{h}_k$ a generátormátrix sorai. Kellene, hogy $\lambda_1 \mathbf{h}_1 + \ldots + \lambda_k \mathbf{h}_k$ súlya nagyobb, mint k. Először ezt magukra a $\mathbf{h}_i$-kre lássuk be: ha $\mathbf{h}_i$ súlya legfeljebb k, akkor a legalább $n-k$ olyan oszlop van H-ban, ahol 0 áll az i-edik sorban. Ekkor viszont a megfelelő $(n-k) \times (n-k)$-as részmátrix determinánsa 0, azaz az oszlopok összefüggőek, ellentmondás. Tetszőleges lineáris kombinációra úgy térhetünk át, hogy a H-t lecseréljük egy olyan mátrixra, amelyben a lineáris kombináció éppen egy sor. Eszerint $C^\perp$ minimális súlya legalább $k+1$, akkor viszont a Singleton-korlát szerint egyenlőség kell álljon. ∎

Jegyezzük meg, hogy a Singleton-korlát úgy is írható, hogy $n \geq d + k - 1$, azaz a 10.3 definícióban bevezetett $M(d, k; q)$-ra

$$M(d, k; q) \geq d + k - 1$$

teljesül és egyenlőség éppen az M.D.S. kódokra áll.

Definíció 10.11 Jelöljük tehát a lehető legrövidebb, d minimális súlyú és k dimenziós lineáris kód hosszát $M(d, k; q)$-val. (Ez a jelölés nem standard, de a jelen fejezetben mi ezt használjuk.)

Lássunk példát M.D.S. kódokra. Legyen a C kód paritásellenőrző mátrixa a

$$H = \begin{pmatrix} t_1 & t_2 & \ldots & t_n \\ t_1^2 & t_2^2 & \ldots & t_n^2 \\ \ldots & & & \\ t_1^r & t_2^r & \ldots & t_n^r \end{pmatrix},$$

ahol a t_i elemek a GF(q) test páronként különböző nem-nulla elemei. Ha ennek a mátrixnak $r+1$ oszlopát kiválasztjuk, akkor azok lineárisan függetlenek (hiszen a megfelelő aldeterminíns Vandermonde típusú), így a H által meghatározott kód n hosszú, $k = n - r$ dimenziós és a fenti állítás miatt minimális súlya $d = r + 1$, vagyis valóban M.D.S.

Ezeknek a kódoknak (az ú.n. *Reed–Solomon* kódoknak) is igen jelentős gyakorlati alkalmazásai vannak, a közismert CD-lejátszók ezt használják, persze némileg megcsavarva (a $q = 2^8$, $(n, k, d) = (32, 28, 5)$, és $(28, 24, 5)$ választással).

Ismerkedjünk meg végül egy nagyon fontos kódosztállyal, a *ciklikus kódok* osztályával.

Definíció 10.12 A C kódot *ciklikus*nak nevezzük, ha $(c_0, \ldots, c_n) \in C$-ből $(c_n, c_0, \ldots, c_{n-1}) \in C$ következik.

Ezek a kódok legkényelmesebben polinomokkal írhatók le, a $(c_0, \ldots, c_n)$-nek feleltessük meg a $c(x) = \sum_{i=0}^n c_i x^i$ polinomot. A ciklikus eltolás a következőképpen írható le a polinomok nyelvén: szorozzunk x-szel, majd az eredményt redukáljuk modulo $(x^n - 1)$. Eszerint minden polinomot érdemes a GF$(q)[x]/(x^n - 1)$ faktorgyűrű elemének tekinteni. A szavak tehát ezen polinomgyűrű elemei, a kódok pedig polinomok bizonyos halmazai. Mivel a szóbanforgó polinomok halmaza vektortér is, a lineáris kódok is természetesen láthatóak ebben a reprezentációban.

Tétel 10.13 *Egy C lineáris kód pontosan akkor ciklikus, ha a megfelelő polinomhalmaz ideál a GF$(q)[x]/(x^n - 1)$ faktorgyűrűben.*

Bizonyítás. Ez egyszerűen amiatt van, hogy tetszőleges polinommal való szorzás visszavezethető az x-szel való szorzásra és a vektortér-műveletekre. ∎

Mivel a GF$(q)[x]/(x^n - 1)$ gyűrű főideálgyűrű, minden C ciklikus kódhoz találhatunk egy $g(x)$ *generátor polinomot*, amely nem más, mint a legkisebb fokú C-beli (pl. egy főegyütthatós) polinom. Ez a generátor-polinom egyértelmű, és osztója kell legyen $(x^n - 1)$-nek, különben ugyanis $g(x)$ és $(x^n - 1)$

legnagyobb közös osztója alacsonyabb fokú C-beli polinom lenne. A $g(x)$ együtthatóiból könnyen felírhatjuk a kód generátormátrixát is, ha $g(x) = \sum_{i=0}^{n-k} g_i x^i$, akkor

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{n-k-1} & g_{n-k} & 0 & \dots & 0 \\ 0 & 0 & \dots & & & & \dots & 0 \\ 0 & 0 & \dots & & g_0 & g_1 & \dots & g_{n-k} \end{pmatrix}$$

lesz a generátormátrix. A paritásellenőrző mátrix megfelelője a $h(x) = (x^n - 1)/g(x)$ *paritásellenőrző* polinom, a C kódszavai éppen azok a polinomok, amelyeket $h(x)$-szel megszorozva 0-t kapunk a $\mathrm{GF}(q)[x]/(x^n-1)$ gyűrűben. Feladatként (10.3. Feladat) érdemes felírni a paritásellenőrző mátrixot is. Az eddig elmondottak alapján ciklikus kódok konstruálásához az $x^n - 1$ polinom faktorizációját lenne jó ismerni. Ha tehát $x^n - 1$ gyökeit nézem $\mathrm{GF}(q)$ egy bővítésében, akkor olyan gyökhalmazokat kell tekinteni, amelyek a testbővítés automorfizmusaira nézve invariánsak. Ha a gyököket a bővítés egy primitív elemének hatványaival írjuk fel, akkor ez pontosan azt jelenti, hogy a kitevők a q-val való szorzásra zártak legyenek.

Az egyik legegyszerűbb eset, ha $n = q - 1$, amikor nincs bővítés. Ekkor pl. vehetjük egy primitív elem első d hatványát. Így a már látott Reed-Solomon kódokat kapjuk vissza.

Egy másik egyszerű eset a *kvadratikus maradék kódok* esete. Tegyük fel, hogy n páratlan prím, és q kvadratikus maradék mod n. (A $q = 2$ esetről ld. a 10.4. Feladatot.) Legyen α egy primitív n-edik egységgyök $\mathrm{GF}(q)$ egy olyan bővítésében, amely az összes n-edik egységgyököt tartalmazza. Legyen

$$g_0(x) = \prod_{i=1}^{n-1}(x - \alpha^{i^2}), \quad g_1(x) = \prod_{j \neq i^2}(x - \alpha^j).$$

Ekkor mind g_0, mind g_1 $\mathrm{GF}(q)$-beli együtthatós polinomok (ehhez kell az, hogy q kvadratikus maradék mod n), továbbá

$$x^n - 1 = (x-1)g_0(x)g_1(x).$$

A $C = ((g_0(x))$ kódot hívják *kvadratikus maradék* kódnak. Ezeket a kódokat sokat vizsgálták (ld. pl. van Lint [**?**], Par. 6.9.), mi majd csak egy speciális esetben térünk vissza rájuk a Golay-kódokkal kapcsolatban. Egy példát mindenképpen érdemes említeni: ha $q = 2$, $n = 7$, akkor

$$x^7 - 1 = (x-1)(x^3+x+1)(x^3+x^2+1),$$

s a $g_0(x) = (x^3 + x + 1)$ által generált kvadratikus maradék kód korábbi jó ismerősünk, a (perfekt) $[7,4,3]$ Hamming-kód.

10.1 A GOLAY-KÓDOK

Mielőtt rátérnénk a Golay-kódok konstrukciójára, lássunk egy nagyon egyszerű eljárást, amellyel kódokat hosszabbá tehetünk. Ez nem más, mint a paritásellenőrző bit általánosítása.

Definíció 10.14 Ha C egy n hosszú kód a $\mathrm{GF}(q)$ ábécé felett, akkor a $\bar{C}$ *kibővített* kód a

$$\bar{C} = \{(c_1, c_2, \dots, c_n, c_{n+1}) \ : \ (c_1, c_2, \dots, c_n) \in C, \sum_{i=1}^{n+1} c_i = 0\}$$

kódszavakból áll.

A legegyszerűbb a konstrukció a bináris esetben, ekkor tényleg a paritásellenőrző bit hozzábiggyesztéséről van szó. Világos, hogy ha C minimális távolsága d, amely páratlan, akkor $\bar{C}$-é $d+1$ lesz. Szintén a bináris esetben világos, hogy a paritásellenőrző mátrix minden sorát egy 0-val kell kibővíteni, és egy új csupa egyesből álló sort kell még hozzácsapni (ld. részletesebben a 10.5. Feladatot).

Példa 10.15 Ha a bináris $[7,4,3]$ Hamming-kódból indulunk ki, akkor egy $[8,4,4]$ kódot kapunk.

Ezek után már meg tudjuk konstruálni a bináris Golay-kódokat. Induljunk ki a H bináris $[7,4]$ Hamming-kódból, melynek paritásellenőrző mátrixa a

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

mátrix. Könnyű látni, hogy H éppen a $\mathbf{0}$ szóból, az $(1,1,0,1,0,0,0)$ szó hét ciklikus eltoljtából, valamint ezen szavak komplementumaiból áll. Legyen H^* az a kód, amelyet H-ból a szavak megfordításával nyerünk, és legyen $\bar{H}^*$ ennek kibővítettje. Könnyen ellenőrizhető, hogy $\bar{H}$ és $\bar{H}^*$ 8 hosszú, 4 dimenziós kódok és $\bar{H} \cap \bar{H}^* = \{\mathbf{0}, \mathbf{1}\}$. Idézzük fel, hogy mindkét kód minimális súlya 4, valamint hogy önduálisak (10.15).

Legyen $\bar{C}$ az alábbi 24 hosszú kód:

$$\bar{C} = \{(\mathbf{a}+\mathbf{x}, \mathbf{b}+\mathbf{x}, \mathbf{a}+\mathbf{b}+\mathbf{x}) \ : \ \mathbf{a}, \mathbf{b} \in \bar{H}, \mathbf{x} \in \bar{H}^*\}.$$

Ha $\mathbf{a}, \mathbf{b}$ a $\bar{H}$, $\mathbf{x}$ pedig a $\bar{H}^*$ egy bázisát futja be, akkor így $\bar{C}$ egy bázisát kapjuk, azaz $\bar{C}$ egy $[24,12]$ kód. A felsorolt vektorok páronként ortogonálisak (hiszen minden nyolcas darabjukban páros sok egyes van), így $\bar{C}$ önduális. A fenti bázisvektorok mindegyikének súlya 4-gyel osztható, így $\bar{C}$ minden kódszavára ugyanez igaz, hiszen két kódszó összegében az egyesek helyének szimmetrikus differenciájának megfelelő pozíciókban lesznek egyesek, ennek mérete két néggyel osztható szám összege mínusz a metszet méretének kétszerese, de a metszet mérete az öndualitás miatt páros.

Most már az lesz a célunk, hogy megmutassuk, hogy $\bar{C}$ minimális súlya 8. Ehhez csak azt kell lássuk, hogy 4 súlyú szó nem lehet $\bar{C}$-ben. Indirekte legyen $\mathbf{c} = (\mathbf{a}+\mathbf{x}, \mathbf{b}+\mathbf{x}, \mathbf{a}+\mathbf{b}+\mathbf{x})$ egy 4 súlyú szó. Mindhárom nyolcas blokkba kerülő szórész súlya páros, így valamelyik nyolcas rész $\mathbf{0}$ kellene legyen. Mivel $\bar{H} \cap \bar{H}^* = \{\mathbf{0}, \mathbf{1}\}$, azt kapjuk, hogy $\mathbf{x} = \mathbf{0}$ (vagy $\mathbf{x} = \mathbf{1}$.) Ha $\mathbf{x} = \mathbf{0}$, akkor mindhárom nyolcas részben a $\bar{H}$ egy-egy szavát kapjuk. Mivel ezen részek súlya 0 vagy legalább négy és közülük legfeljebb egy lehet nullvektor, kapjuk, hogy $\mathbf{c}$ súlya legalább 8, ami ellentmondás.

A bináris *Golay-kód* ezek után az utolsó koordináta törlésével keletkezik $\bar{C}$-ből, ez tehát egy 23 hosszú, 12 dimenziós kód, a minimális súly pedig 7.

Tétel 10.16 *A* $[23, 12, 7]$ *bináris Golay-kódok perfektek.*

Bizonyítás. Ld. a 10.6. Feladatot. ∎

Megjegyzés 10.17 S. L. Snover 1973-ban belátta, hogy bármely (nem feltétlen lineáris) $(23, 2^{12}, 7)$ kód ekvivalens C-vel.

Lássuk a Golay-kódok néhány további előállítását!
Legyen G az alábbi mátrix:

$$\begin{array}{c}
\begin{matrix} \infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{matrix} \\
\begin{pmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}
\end{array}$$

A mátrix oszlopait az $\ell_\infty, \ell_0, \ell_1, \ldots \ell_{10}$ valamint $r_\infty, r_0, r_1, \ldots r_{10}$ szimbólumokkal fogjuk jelölni. Fontos észrevétel, hogy a jobboldalon lévő mátrix ciklikus mátrix, melyben az egyesek a mod 11 kvadratikus maradékoknak megfelelő helyen vannak (azaz ez a mátrix a Paley-féle blokkrendszer incidenciamátrixa).

A 10.7–8. feladat-sorozat azt mutatja, hogy hogyan lehet lényegében az előző konstrukcióban belátott tulajdonságokat igazolni, ha ebből a generátormátrixos megadásból indulunk ki.
Legyen $q = 2$, $n = 23$. Ekkor

$$x^{23} - 1 = (x-1)(x^{11}+x^9+x^7+x^6+x^5+x+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1).$$

Az első tényező éppen a kvadratikus maradék kódot generálja. Az ilyen kódokra érvényes általános tételekből következik, hogy a minimális távolságra $d \geq 7$ teljesül. Mivel a 3 sugarú gömb $\sum_{i=o}^{3} \binom{23}{i} = 2^{11}$ szót tartalmaz, és a kód dimenziója 12 (hisz a generátorpolinom foka 11), így a kódszavak körüli (diszjunkt) 3 sugarú gömbök lefedik a teljes 23 dimenziós vektorteret. Ez azt jelenti, hogy a kód perfekt és ugyanazok a paraméterei, mint a bináris Golay-kódnak. Snover már idézett tétele (10.17) szerint akkor viszont ez a kód izomorf a Golay-kóddal.

Lássuk, hogy a Golay-kódok milyen kapcsolatban vannak a blokkrendszerekkel!

Definíció 10.18 *Ha egy n hosszú C kódra A_i jelöli az i súlyú kódszavak számát, akkor az*

$$A(z) = \sum_{i=0}^{n} A_i z^i$$

polinomot a C súlypolinomjának nevezzük.

A most következő MacWilliams-től származó azonosság segít kiszámítani $C^\perp$ súlypolinomját.

Tétel 10.19 (MacWilliams) *Legyen C egy $[n, k]$ kód a* GF(q) *test felett, $C^\perp$ pedig a duálisa. A súlypolinomokat jelölje rendre $A(z)$ és $B(z)$. Ekkor*

$$B(z) = q^{-k}(1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right).$$

Először is számítsuk ki a kibővített Golay-kód súlypolinomját. Tudjuk, hogy a minimális távolság 8, továbbá, hogy minden kódszó súlya 4-gyel osztható, így a súlypolinom $A(z) = 1 + Az^8 + Bz^{12} + Az^{16} + z^{24}$ alakú. Ehhez csak azt kell észrevennünk, hogy a csupa 1 vektor benne van a kódban, s így a 8 súlyú kódszavak száma azonos a 16 súlyúakéval. Még azt is tudjuk, hogy $2 + 2A + B = 2^{12}$, hiszen ez éppen a kódszavak száma. Mivel a Golay-kód önduális, alkalmazva McWilliams tételét egy második összefüggést kapunk A és B között, amiből majd meghatározhatjuk a súlypolinomot.

$$A(z) = 2^{-12}(1+z)^{24} A\left(\frac{1-z}{1+z}\right),$$

vagyis

$$1 + Az^8 + Bz^{12} + Az^{16} + z^{24} = 2^{-12}((1+z)^{24} + A(1-z)^8(1+z)^{16} + B(1-z)^{12}(1+z)^{12} + A(1-z)^{16}(1+z)^8 + (1-z)^{24}.$$

Itt a bal oldalon z^2 együtthatója 0, míg ugyanez a jobb oldalon

$$2^{-12}(2\binom{24}{2} + 2A(16 \cdot 8 + \binom{8}{2} + \binom{16}{2} - 12B).$$

A két egyenletből álló rendszert megoldva $A = 759$ adódik. Ennek segítségével már könnyű belátni a Golay-kódok alábbi igen fontos tulajdonságát:

Tétel 10.20 *A kibővített Golay-kód 8 súlyú szavai egy* $5-(24,8,1)$ *Steiner-rendszer blokkjai.*

Bizonyítás. Két 8 súlyú kódszó legfeljebb 4 pozícióban lehet azonos. Ha ugyanis ennél több azonos koordináta volna, akkor a két szó összege legfeljebb 6 súlyú volna. Ez azt jelenti, hogy ha megadunk 5 pozíciót, akkor legfeljebb egy olyan 8 súlyú kódszó van, amelyben ezeken a helyeken egyes áll. Ilyen ötöst $\binom{24}{5}$-féleképpen tudunk kiválasztani, s egy blokkot (nyolc súlyú szót) $\binom{8}{5}$ ötösnél számolunk. Így legfeljebb $\binom{24}{5}/\binom{8}{5} = 759$ blokkunk lehet, de fentebb láttuk, hogy pontosan ennyi van. Ez viszont azt jelenti, hogy minden adott koordináta-ötöshöz egy és csak egy olyan nyolc súlyú szó van, amely itt egyeseket tartalmaz. ∎

A Tételben szereplő Steiner-rendszert szokás 24 pontú *Witt-féle* blokkrendszernek nevezni. Ennek derivált-rendszere egy $4-(23,7,1)$ blokkrendszer, ha pedig tovább deriválunk, akkor egy $3-(22,6,1)$ Steiner-rendszert kapunk. (Ezeket is szokás (23 ill. 22 pontú) Witt-féle blokkrendszereknek nevezni.) Ha még egyszer deriválunk, akkor egy $2-(21,5,1)$-rendszert kapunk, ami nem más mint egy negyedrendű projektív sík. Mivel a szóbanforgó projektív sík izomorfia erejéig egyértelmű, így csak a PG$(2,4)$ testre épített sík lehet. Erre a megfigyelésre építve is meg lehet konstruálni a Witt-féle blokkrendszereket, amint azt a következő szakaszban vázolni is fogjuk. Érdemes megemlíteni, hogy a projektív síkok bővíthetőségének feltételéből azt kaptuk (ld. 7.8 Állítás), hogy a sík rendje 2 vagy 4 kell legyen. A Fano-sík bővítésével az Hadamard-mátrixoknál már megismerkedtünk, a negyedrendű esetben pedig itt látjuk a bővítést.

Most nézzük meg, hogy hogyan lehet a *ternér Golay kódokat* ehhez hasonló módon előállítani. Tekintsük a modulo 5 maradékosztálytest kvadratikus

maradékai segítségével definiált Paley-mátrixot, azaz a

$$S_5 = \begin{pmatrix} 0 & + & - & - & + \\ + & 0 & + & - & - \\ - & + & 0 & + & - \\ - & - & + & 0 & + \\ + & - & - & + & 0 \end{pmatrix}$$

mátrixot. $+$ ill. $-$ természetesen +1-et és –1-et jelöl, melyet a modulo 3 test elemének tekintünk. Legyen C az a ternér (GF(3) felett definiált) kód, melynek generátormátrixa

$$G = \begin{pmatrix} & 1 \; 1 \; 1 \; 1 \; 1 \\ I_6 & S_5 \end{pmatrix}.$$

Ez a kód természetesen 11 hosszú és 6 dimenziós. A most következő tulajdonságokat nem bizonyítjuk, feladatként (9–10. Feladatok) az olvasóra hagyjuk. Kibővített kódja $\bar{C}$ önduális, így benne a kódszavak súlya 3-mal osztható. $\bar{G}$ generátormátrixát úgy kapjuk G-ből, hogy egy

$$(0, -1, -1, -1, -1, -1)^T$$

oszlopot adunk G-hez. $\bar{G}$ sorai 6 súlyúak, így két oszlop kombinációja legalább 4, és így a hárommal való oszthatóság miatt legalább hat súlyú. Ebből kideríthető, hogy $\bar{C}$ minimális súlya 6, tehát C-é 5. Könnyen ellenőrizhető, hogy a C kód perfekt. A kapott kódot *ternér Golay-kód*nak nevezzük.

Megjegyzés 10.21 Tetszőleges $(11, 3^6, 5)$ kód ekvivalens a ternér Golay-kóddal.

Az eddigiekben megismerkedtünk néhány perfekt kóddal (Hamming-kódok, Golay-kódok). Mivel a perfekt kódok bizonyos értelemben a lehető legjobb kódok, kívánatos lenne minél több ilyen kódot ismerni (különösen, ha azt is figyelembe vesszük, hogy a Hamming- kódok csak egy hibát javítanak). Sajnos ebben az értelemben a helyzet rossz, lényegében az összes perfekt kóddal megismerkedtünk.

Tétel 10.22 (van Lint, Tietäväinen) *e-hibajavító perfekt kódok csak a Golay-kódok vagy az ismétlés-kódok, ha $e > 1$.*

Ha $e = 1$, akkor a kódszavak száma megegyezik a Hamming-kódéval, de a kód nem feltétlen kell lineáris legyen (egy példát mutatunk a 11. Feladatban, [?] 7.7.4). Persze, ha a kód lineáris, akkor az csak a Hamming-kód lehet (ld. 10.12. Feladat).

10.2 A WITT-FÉLE BLOKKRENDSZEREK

Ebben a fejezetben kicsit szemügyre vesszük a címben jelzett Witt-féle blokkrendszereket, melyekkel a Golay kódok kapcsán már megismerkedtünk. Az egyszerűség kedvéért a nagy Mathieu-csoportokhoz tartozó Witt-rendszereket ismertetjük vázlatosan. Ez azt jelenti, hogy bizonyítás szinte egyáltalán nem lesz ebben a fejezetben.

Állítás 10.23 $\mathrm{PGL}(3,4)$ *tranzitív a hiperoválisokon. A* $\mathrm{PG}(2,4)$ *síkban 168 hiperovális van. Egy ponton 48, két ponton 12, három ponton 3 hiperovális megy át, négy pont pedig egyértelműen egészíthető ki hiperoválissá.*

Az egyszerűség kedvéért jelölje G a $\mathrm{PGL}(3,4)$-et, S pedig $\mathrm{PSL}(3,4)$-et.

Állítás 10.24 *S a hiperoválisokat három (56 hosszú) orbitban permutálja.*

Láttuk, hogy egy háromszög pontosan három hiperoválisban van benne, ez a három hiperovális különböző orbitban van. A szóbanforgó hiperovális-orbitokat a most említett tulajdonság karakterizálja: ha hiperoválisok egy halmazában bármely két hiperovális legfeljebb két pontban metszi egymást, akkor legfeljebb 56 hiperovális lehet. Egyenlőség pontosan akkor áll, ha a hiperovális-halmaz egy S-orbit.

Szükségünk lesz G ill. S hatására másodrendű (Fano) részsíkokon is.

Állítás 10.25 *A Fano-részsíkok száma 360, ezeket S három (120 hosszú) orbitban permutálja.*

Ahhoz, hogy ezekből az orbitokból tényleg össze tudjuk rakni a Witt-féle blokkrendszereket, még további tulajdonságok kellenek, mi csak magát a konstrukciót mondjuk el. Jelölje a három hiperovális-orbitot H_1, H_2, H_3, a három részsík-orbitot R_1, R_2, R_3. Alkalmasan választott indexeléssel a konstrukció az alábbi:

A W_{24} blokkrendszer:
pontok: $\mathrm{PG}(2,4)$ pontjai és $\infty_1, \infty_2, \infty_3$.
blokkok:

$\mathrm{PG}(2,4)$ egyenesei hozzávéve $\infty_1, \infty_2, \infty_3$-et.

H_i elemei hozzávéve ∞_j, ∞_k-t (i, j, k az $1, 2, 3$ egy permutációja)

R_i elemei hozzávéve ∞_i-t ($i = 1, 2, 3$)

$\{(g \cup h) \setminus (g \cap h)\}$ g, h egyenes.

A legfontosabb tény erről a blokkrendszerről az alábbi.

Tétel 10.26 *W_{24} automorfizmus-csoportja az M_{24} Mathieu-csoport, amely a pontokon 5-tranzitív. (M_{24}-ben 3 pont stabilizátora S).*

Hasonló konstrukció adható a kis Mathieu-csoportokhoz tartozó Witt-rendszerekre is. Ehhez néhány megjegyzés: $\mathrm{AG}(2,3)$-on minden négyszög parallelogramma. Minden háromszög pontosan három négyszögben van benne. Van egy olyan 72 elemű U részcsoportja az $\mathrm{AGL}(2,3)$ affin csoportnak, amely a négyszögeket három orbitban permutálja, és itt is minden háromszöget tartalmazó három négyszög különböző U-orbitban van benne. Persze ez az U a pontokon szigorúan kétszeresen tranzitív. Jelöljük a négyszög-orbitokat N_1, N_2 és N_3-mal. Mivel minden négyszög parallelogramma, ezért minden négyszögnek pontosan egy nem ideális átlóspontja van. Ezeken U szintén három orbitot létesít: N_1^*, N_2^* és N_3^*. Természetesen a jelölést úgy érdemes választani, hogy N_i^* az N_i-beli négyszögekből álljon, kibővítve átlóspontjukkal.

A W_{12} blokkrendszer:
pontok: $\mathrm{AG}(2,3)$ pontjai és $\infty_1, \infty_2, \infty_3$.
blokkok:

$\mathrm{PG}(2,4)$ egyenesei hozzávéve $\infty_1, \infty_2, \infty_3$-et.

N_i elemei hozzávéve ∞_j, ∞_k-t (i, j, k az $1, 2, 3$ egy permutációja)

N_i^* elemei hozzávéve ∞_i-t ($i = 1, 2, 3$)

$\{(g \cup h)\}$ g, h párhuzamos egyenesek.

A legfontosabb tény erről a blokkrendszerről az alábbi.

Tétel 10.27 *W_{12} automorfizmus-csoportja az M_{12} Mathieu-csoport, amely a pontokon szigorúan 5-tranzitív.*

Egy további megjegyzés, amely mutatja, hogy a geometria olykor csoportelméleti állításokat is megvilágít. Vegyünk egy unitér polaritását $\mathrm{PG}(2,4)$-nek (ld. az 1.1 szakaszt). Ennek autokonjugált pontjai egy $\mathrm{AG}(2,3)$ affin síkot alkotnak. Ráadásul az is megmutatható, hogy a W_{24} nyoma ezen az affin síkon éppen W_{12} lesz, amiből következik, hogy M_{12} részcsoportja M_{24}-nek.
A Witt-féle blokkrendszerekből sok érdekes erősen reguláris gráf is származtatható.

Példa 10.28 (1) A $HS(100)$ gráf: csúcsai W_{22} pontjai (22 pont), W_{22} blokkjai (77 pont), és egy ∞ szimbólum. ∞-t összekötjuk a 22 ponttal, és pont-blokk akkor és csak akkor lesz összekötve éllel, ha ők a W_{22}-ben illeszkedtek. Paraméterei: $(100, 22, 0, 6)$.

(2) $HS(77$: a W_{22} blokkgráfja. Paraméterei: $(77, 16, 0, 4)$.

(3) A Gewirtz gráf: pontjai egy hiperovális-orbit elemei. Összekötés: diszjunktság. Paraméterei: $(56, 10, 0, 2)$.

10.3 Feladatok

10.1., A Hadamard-kód min. távolsága $n/2$

10.2., Legyen S a Paley-mátrix és tekintsük a $\mathbf{0}, \mathbf{1}$ sorokat, valamint az $(S+I+J)/2$ és $(-S+I+J)/2$ mátrixokat. Ennek sorait tekintsük egy kód szavainak.

Mutassuk meg, hogy így $(n, 2(n+1), (n-1)/2)$ paraméterű (nem-lineáris) kódot kapunk.

10.3., Írjuk fel ciklikus kód paritás ellenőrző mátrixát.

10.4., Mikor lesz a 2 kvadratikus maradék mod p?

10.5., Írjuk fel egy kód kibővítettjének paritás ellenőrző mátrixát a $q = 2$ esetben.

10.6., Biz. be 10.16-ot.

10.7., Golay-kód tulajdonságai:

paraméterei $[24, 12, 8]$, önduális, minden kódszó súlya 4-gyel osztható, $\mathbf{1} \in G_{24}$.

10.8., G_{24} invariáns az

$$(\ell_\infty r_\infty)(\ell_0 r_0)(\ell_1 r_{10})(\ell_2 r_9)\ldots(\ell_{10} r_1)$$

permutációra.

G_{24} súlyeloszlása: 0 – 1, 8 – 759, 12 – 2576, 16 – 759, 24 – 1 (persze a jelölés súly – szavak száma).

10.9., ternér Golay kód tulajdonságai: önduális, minimális távolsága 6.

10.10., A ternér Golay kód perfekt.

10.11., ** példa perfekt nem-lineáris kódra **

10.12., 1–hibajavító perfekt lineáris kód csak a Hamming-kód lehet.

10.13., Lássuk be a W_{24} konstrukciója előtt említett állításokat.

10.14., Konstruáljuk meg az U részcsoportot. (PSU$(3,4)$!!)

10.15., Ellenőrizzük a W_{22}-höz tartozó erősen reguláris gráfok paramétereit.

IRODALOM

References

[1] L. Babai and P. Frankl. Linear algebra methods in combinatorics Chicago Univ. Press, 1992.

[2] S. Bagchi and B. Bagchi. *Designs from pairs of finite fields I. A cyclic unital* ($U(6)$ *and other regular Steiner 2-designs.* Technical Report 10/87, Indian Statistical Institute, 1987.

[3] Th. Beth, D. Jungnickel, and H. Lenz. *Design Theory.* Wissenschaftsverlag, 1985.

[4] K. N. Bhattacharya. On a new symmetrical balanced incomplete block design. *Bull. Calcutta Math. Soc.*, 36:91–106, 1944.

[5] R. C. Bose. Strongly regular graphs, partial geometries and partial balanced designs. *Pacific J. Math.*, 13:389–419, 1963.

[6] R. C. Bose, S. S. Shrikhande, N. M. Singhi. 1977.

[7] P. J. Cameron. Extending symmetric designs. *J. Comb. Th.*, A 14:215–220, 1973.

[8] P. J. Cameron. Strongly regular graphs. In L. W. Beineke and R. J. Wilson, editors, *Selected topics in graph theory*, pages 337–360, Academic Press, 1978.

[9] P. J. Cameron and J. H. van Lint. *Graphs, Codes and Designs.* Volume 43 of *Lecture Note Series*, London Math. Soc., 1980.

[10] L. C. Chang. Association schemes of partially balanced block design with parameters $v = 28$, $n_1 = 12$, $n_2 = 15$ and $p^2_{11} = 4$. *Sci. Record*, 4:12–18, 1959.

[11] A. Gewirtz. Graphs with maximal even girth. *Can. J. Math.*, 21:915–934, 1970.

[12] A. Gewirtz. The uniqueness of g(2,2,10,56). *Trans. New York Acad. Sci.*, 31:656–675, 1969.

[13] M. Jr Hall. *Combinatorial Theory.* Blaisdell, Waltham, 1967.

[14] M. Jr Hall. Cyclic projective planes. *Duke J. Math.*, 14:1079–1090, 1947.

[15] M. Jr Hall and W. S. Connor. An embedding theorem for balanced incomplete block designs. *Can. J. Math.*, 6:35–41, 1954.

[16] A. J. Hoffman and R. R. Singleton. On Moore graphs with diameters 2 and 3. *IBM J. Res. Develop.*, 4:497–504, 1960.

[17] D. R. Hughes and F. C. Piper. *Design Theory.* Cambridge University Press, 1985.

[18] W. M. Kantor. Note on symmetric designs and projective spaces. *Math. Z.*, 122:61–62, 1971.

[19] F. Kárteszi *Bevezetés a véges geometriákba.* Akadémiai Kiadó, Budapest, 1973.

[20] C. W. H. Lam, L. Thiel, and S. Swiercz. The non-existence of finite projective planes of order 10. *Can. J. Math.*, XLI(6):1117–1123, 1989.

[21] E. S. Lander. *Symmetric designs: an algebraic approach. London Math. Soc. Lecture Notes*, Cambridge University Press, 1974.

[22] F. Radó, B. Orbán *A geometria mai szemmel* Dacia, Cluj, 1982.

[23] C. J. Salwach and J. A. Mezzaroba. The four biplanes with $k = 9$. *J. Combinatorial Theory*, A 24:141–145, 1978.

[24] J. J. Seidel. Strongly regular graphs. In B. Bollobás, editor, *Surveys in Combinatorics*, pages 157–180, London Math. Soc. Lecture Note Series 38, Cambridge, 1979.

[25] J. J. Seidel. Strongly regular graphs of L_2-type and of triangular type. *Indag. Math.*, 29(2):189–196, 1967.

[26] J. H. van Lint. Non-embeddable quasi-residual designs. *Proc. Kon. Nederl. Akad. Wetensch.*, (A) 81:269–275, 1978.

[27] J. H. van Lint and J. J. Seidel. Equilateral point sets in elliptic geometry. *Indag. Math.*, 28:335–348, 1969.

[28] J. H. van Lint. Coding theory Springer GTM, 198*.

[29] J. H. van Lint and R. M. Wilson. A course in Discrete Mathematics Cambridge Univ. Press, 1992.