PRÍMEK, POLIGNAC, POLYMATH

HARCOS GERGELY

1. Halászás a prímekre

A prímszámok rejtélyes viselkedése és a matematikában betöltött központi szerepe az ókori idők óta foglalkoztatja az embereket. Az elmúlt 10 évben több rendkívüli áttörést láttunk ezen a területen, amik korábban elérhetetlennek tűntek [10, 8, 32, 14, 6, 15, 7]. Ebben a cikkben az ikerprímsejtés körüli izgalmas fejleményekre koncentrálunk, hangsúlyozva a tételek mögötti alapgondolatokat.

Euklidész már az *Elemek* című művében (IX. könyv, 20. állítás) leírta a mindannyiunk által tanult bizonyítást, miszerint végtelen sok prímszám van. A szomszédos prímszámok közötti távolságok az első különbségtől eltekintve párosak, és talán már Euklidész megfigyelte, hogy ez a különbség gyakran 2, legalábbis a sorozat elején:

$$(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\ (41,43),\ (59,61),\ (71,73),\ \ldots$$

Az ilyen prímeket *ikerprímeknek* nevezzük, és azt sejtjük, hogy végtelen sok van belőlük:

Ikerprímsejtés. *A $p-p'=2$ egyenletnek végtelen sok megoldása van prímekben.*

Általánosabban, Polignac [19] azt sejtette, hogy minden páros szám végtelen sokszor előfordul két szomszédos prímszám közötti távolságként, ami motiválja a következő fogalmat.

1. definíció. A d pozitív egészt *Polignac-számnak* nevezzük, ha a $p-p'=d$ egyenletnek végtelen sok megoldása van prímekben. A Polignac-számok halmazát jelölje $\mathscr{D}$.

A definícióban nem követeljük meg, hogy p és p' szomszédos prímszámok legyenek. Polignac sejtéséből következik, hogy $\mathscr{D}$ a pozitív páros számok halmaza, de egészen tavalyig azt sem tudtuk, hogy $\mathscr{D}$ nem üres-e.

1. tétel (Zhang [32])**.** *Létezik Polignac-szám, azaz $\mathscr{D}\neq\emptyset$.*

A tétel bizonyítása a probléma egy újszerű megközelítésén alapul, amit eredetileg Goldston, Pintz, Yıldırım [8] fejlesztett ki Heath-Brown [12] egy korábbi

ötletére alapozva. A klasszikus megközelítésben egy konkrét d pozitív páros számról (pl. $d = 2$) igyekszünk kimutatni, hogy Polignac-szám, azaz hogy végtelen sok n pozitív egészre az n és az $n + d$ is prímszám. Felfoghatjuk ezt egyfajta prímhalászásnak, amiben két kézzel – amik adott távolságra vannak egymástól – próbálunk két prímet fogni úgy, hogy az egész számok különböző helyein próbálkozunk. A [8] cikk alapötlete, hogy a prímhalászást ne puszta kézzel, hanem halászhálóval – egy $\mathscr{H}$ véges halmaz eltoltjaival – végezzük. Ezáltal jobb esélyünk van arra, hogy két egymáshoz közeli prímet fogjunk, de cserébe azok távolsága már nem egy konkrét d lesz, hanem a $\mathscr{H}$-ban fellépő különbségek egyike. A [8] cikk központi észrevétele, hogy a prímszámoknak bizonyos maradékosztályokban való nagyon egyenletes eloszlása mellett a vázolt prímhalászás hatékonnyá tehető. Motohashi és Pintz [16] a szükséges hipotézist jelentősen gyengítette, és Zhang [32] ezt bizonyította bravúrosan.

Az 1. tétel szenzációs bejelentését követően Terence Tao vezetésével elindult a Polymath8 elnevezésű internetes kutatási projekt, amibe bárki szabadon bekapcsolódhatott, pl. magyar részről Pintz János mellett a szerző is részt vett benne. A projekt célja Yitang Zhang munkájának megértése, elemzése és a kvantitatív aspektusainak optimalizálása volt – ennek eredményeit a [20] cikk tartalmazza. Időközben – újabb drámai fordulatként – Heath-Brown fiatal tanítványa, James Maynard továbbfejlesztette a [8]-ban szereplő szitát – tehát hogy hol érdemes kivetni a hálót –, és ezáltal a [16]-ban megfogalmazott egyenletes eloszlási hipotézisre sem volt szüksége. Ily módon Maynard [14] új bizonyítást adott a Zhang-tételre, sőt azt is belátta, hogy kellően nagy halászhálóval akármilyen előírt véges számú prímet foghatunk, nem csak kettőt. Hasonló észrevételeket tett a blogján Tao is [29], majd a Polymath8 projekt folytatódott a Maynard–Tao-tétel továbbfejlesztésével [21].

2. Milyen hálóval halásszunk?

Az 1. tétel bizonyításának alapötlete a [8] cikkben szerepel:

1. ötlet. *Legyen $\mathscr{H} = \{h_1, \dots, h_k\}$ egy egész számokból álló k elemű halmaz. Próbáljunk végtelen sok n pozitív egészt találni úgy, hogy az $n + \mathscr{H} = \{n + h_1, \dots, n + h_k\}$ eltolt halmaz minél több prímet tartalmazzon.*

A szakirodalomban valóban a $\mathscr{H}$ jelölés terjedt el a fenti halmazra, ezért a halászháló metafora többszörösen helyénvalónak tűnik. A továbbiakban az elemeket nagyságrendi sorrendben számozzuk: $h_1 < \dots < h_k$. Persze rögtön látjuk, hogy nem minden k elemű halmaz felel meg egyaránt a prímhalászás céljára. Pl. a $k = 2$ esetben $\mathscr{H} = \{0, 1\}$ eleve rossz, mert n és $n+1$ közül az egyik mindig páros, tehát $n > 2$ esetén csak az egyikük lehet prím. A $\mathscr{H} = \{0, 2\}$ jobb ebből a szempontból, hiszen az ikerprímsejtés szerint n és $n + 2$ egyszerre prím végtelen sok n-re. Hasonlóan, a $k = 3$ esetben a 2 és a 3 szerinti maradékokat nézve látjuk, hogy $\mathscr{H} = \{0, 2, 3\}$ vagy $\mathscr{H} = \{0, 2, 4\}$ nem kifejezetten jó háló gyanánt, hiszen ezek eltoltjaiban legfeljebb csak két prím van, ha $n > 3$. Ellenben a $\mathscr{H} = \{0, 2, 6\}$ eltoltjaira nem tudunk semmiféle okot, ami megakadályozná, hogy mindhárom eleme prím legyen végtelen sokszor. Ez motiválja az alábbi fogalmat.

2. definíció. A $\mathscr{H} = \{h_1, \ldots, h_k\}$ egész számokból álló k elemű halmaz *megengedett,* ha semmilyen $m \geq 2$ egészre nézve nem tartalmaz teljes maradékrendszert.

Persze rögtön látjuk, hogy ha egy k elemű $\mathscr{H}$ halmaz tartalmaz teljes maradékrendszert valamilyen $m \geq 2$ egészre nézve, akkor $m \leq k$, vagyis $\mathscr{H}$ tartalmaz teljes maradékrendszert valamilyen $p \leq k$ prímszámra nézve is – nevezetesen az m bármely prímosztójára nézve. Tehát a fenti definícióban nem vesztünk semmit, ha feltesszük, hogy $m \leq k$ prímszám. Ez mutatja, hogy minden k-ra van megengedett k elemű halmaz, pl. a k utáni első k darab prímszám halmaza.

Az 1. ötletnek komoly támogatást ad Dickson [2] egy sejtése, illetve annak Hardytól és Littlewoodtól származó kvantitatív formája [11]:

Dickson–Hardy–Littlewood-sejtés. *Legyen $\mathscr{H}$ egy megengedett halmaz. Ekkor végtelen sok n pozitív egészre az $n + \mathscr{H}$ eltolt halmaz minden eleme prímszám.*

A sejtés persze nem mondja meg, az n-et miként válasszuk meg, hogy az $n + \mathscr{H}$ összes eleme, vagy akár csak két eleme prím legyen. A metaforánkkal élve: hiába van hálónk, ha nem tudjuk, hova vessük ki, tehát hol gazdag halban a víz. Pl. ha az n-et valamilyen nagy x körül az egyenletes eloszlás szerint véletlenszerűen választjuk, akkor az $n + \mathscr{H}$ halmazba átlagosan csak kb. $|\mathscr{H}|/\log x$ prímszám fog esni, mert ebben a tartományban átlagosan kb. $\log x$ távolságra vannak a prímszámok egymástól. Tehát ha x nagy, akkor ezen a naiv módon átlagosan közel nulla darab prímet fogunk kihalászni, nemhogy kettőt vagy többet. Itt és a továbbiakban $\log x$ a természetes logaritmust jelöli, az analitikus számelméletben megszokott módon. Az n ügyes megválasztásával, avagy a rossz n-ek „kiszitálásával" kell ellensúlyozni azt a tényt, hogy a prímszámok sorozata egyre ritkul. Ennek módja már Goldston, Pintz, Yıldırim [8] cikkében szerepel, de Zhang [32] bizonyította először, hogy így legalább két prímszám garantálható egy alkalmas megengedett halmaz végtelen sok eltoltjában. Maynard [14] még ügyesebben szitálja az n-et, ami által akár száz prímet is tud garantálni végtelen sok $n + \mathscr{H}$ alakú eltoltban.

2. tétel (Zhang [32])**.** *Létezik egy k pozitív egész az alábbi tulajdonsággal. Ha $\mathscr{H}$ egy k elemű megengedett halmaz, akkor végtelen sok n pozitív egészre az $n + \mathscr{H}$ eltolt halmazba legalább két prímszám esik.*

A tételből azonnal következik, hogy ha $\mathscr{H} = \{h_1, \ldots, h_k\}$ egy megfelelő halmaz, akkor a fellépő $h_j - h_i$ $(i < j)$ különbségek egyike Polignac-szám, hiszen $n + h_i$ és $n + h_j$ különbsége $h_j - h_i$. Tehát ha az a cél, hogy $\mathscr{D}$-ben minél kisebb elem létezését garantáljuk, akkor a tételbeli $\mathscr{H}$-t kell minél kisebb átmérőjűnek választani. Ehhez első lépésben a tételbeli k-t kell minimalizálni, majd ahhoz kell megtalálni a legjobb $\mathscr{H}$-t. Ilyen típusú optimalizálással telt a Polymath8 projekt jelentős része [20, 21]. Az alábbi táblázatban összefoglaljuk, hogy az 1-2. tételek numerikus variánsai miként fejlődtek.

A táblázat utolsó sora szerint van egy 50 elemű $\mathscr{H} \subset \{0, 2, \ldots, 246\}$ megengedett halmaz, aminek eltoltjaiban végtelen sokszor található két prímszám. Az 50 elem részletesen fel van sorolva a [21] cikk 76. oldalán. Tehát $\mathscr{D}$-ben mindenképpen van legfeljebb 246 nagyságú páros szám, de konkrét elemet megnevezni nem

forrás	$k =$	$\min \mathscr{D} \leq$
Zhang [32]	3.5×10^6	7×10^7
Polymath8a [20]	632	4680
Maynard [14]	105	600
Polymath8b [21]	50	246

tudunk. Ilyen konkrét elem megtalálása a jelenlegi módszerekkel reménytelennek tűnik: a probléma valószínűleg az ikerprímsejtéssel megegyező nehézségű. Mindazonáltal a $\mathscr{D}$-ről a fenti eredmények jóval többet elmondanak, amint az a következő fejezetből kiderül.

3. A Polignac-számok sűrűsége

Pintz János ismerte fel a 2. tétel azon következményét, hogy a Polignac-számok a természetes számok egy – csak a k-tól függő – pozitív hányadát elfoglalják, továbbá a szomszédos Polignac-számok közötti távolság korlátos. Az eredményt a közelmúltban finomította Granville, Kane, Koukoulopoulos, Lemke Oliver, és mi ebben a formában mondjuk ki és bizonyítjuk.

3. tétel (Pintz et al. [18, 9])**.** *Végtelen sok Polignac-szám létezik. Pontosabban:*

(a) *A $\mathscr{D} \subset \mathbb{N}$ halmaz aszimptotikus alsó sűrűsége*

$$\underline{d}(\mathscr{D}) \geq \frac{1}{k-1} \prod_{p \leq k} \left(1 - \frac{1}{p}\right),$$

ahol k mint a 2. tételben, és a szorzás a prímeken fut végig.

(b) *Létezik $m \in \mathbb{N}$ úgy, hogy minden $n \in \mathbb{N}$ esetén $\mathscr{D} \cap \{n, n+1, \ldots, n+m\} \neq \emptyset$.*

Bizonyítás. A jelzett becslés a k csökkentésével erősödik, ezért feltehető, hogy k a legkisebb egész, ami a 2. tételbeli állítást kielégíti. Ekkor persze $k \geq 2$, és a feltétel szerint létezik egy $k-1$ elemű $\mathscr{H} = \{h_1, \ldots, h_{k-1}\}$ megengedett halmaz, aminek $n + \mathscr{H}$ eltoltjában legfeljebb csak egy prímszám van, ha n kellően nagy. Legyen most $h > h_{k-1}$ olyan egész, amivel $\mathscr{H} \cup \{h\}$ egy k elemű megengedett halmaz, ekkor végtelen sok $n + \big(\mathscr{H} \cup \{h\}\big)$ eltoltban található két prímszám. A $\mathscr{H}$ tulajdonsága miatt szükségszerű, hogy valamilyen $1 \leq j \leq k-1$ indexre és végtelen sok n-re az $n + h_j$ és az $n + h$ egyszerre prím, vagyis $h - h_j \in \mathscr{D}$. A $h > h_{k-1}$ egészre tett feltevés csak annyi megkötést jelent, hogy ha egy $p \leq k$ prímszámra nézve $\mathscr{H}$ mod p már tartalmaz $p-1$ különböző maradékot, akkor h mod p is ezen $p-1$ maradékok egyike kell, hogy legyen. A kínai maradéktétel alapján tehát megadható $\prod_{p \leq k}(p-1)$ darab maradékosztály modulo $\prod_{p \leq k} p$ úgy, hogy ha $h > h_{k-1}$ ezek uniójából való, akkor a $h - h_1, \ldots, h - h_{k-1}$ különbségek egyike Polignac-szám. Innen már könnyű meggondolással következik az (a) és a (b) állítás, pl. az utóbbiban vehető $m := h_{k-1} - h_1 + \prod_{p \leq k} p$.

Ahogy a [9] cikk szerzői is megjegyzik, az (a) állításban vehető a már igazolt $k = 50$ érték [21], és ezzel a $\underline{d}(\mathscr{D}) > \frac{1}{354}$ becslést kapjuk a Polignac-számok aszimptotikus alsó sűrűségére. Tehát átlagosan minden 354 egymás utáni számra jut egy Polignac-szám, míg az első Polignac-szám legfeljebb 246. Ezzel szemben a szomszédos Polignac-számok közötti legnagyobb távolságra a fentihez hasonló formális érveléssel nem tudunk konkrét értéket szolgáltatni, aminek oka a következő. Adott M pozitív egészre van olyan $\mathscr{E} \subset \mathbb{N}$ halmaz, amiben az M végtelen sokszor fellép két szomszédos elem távolságaként, miközben bármely megengedett $\{h_1, h_2, h_3\}$ hármas esetén az $\mathscr{E}$ tartalmazza a $h_2 - h_1$, $h_3 - h_2$, $h_3 - h_1$ különbségek egyikét. Pl. $\mathscr{E}$-nek vehetjük azon természetes számok halmazát, amik modulo $3M$ kongruensek egy legfeljebb M abszolút értékű egész számmal. Tehát ha a 2. tételből csak annyit használunk fel, hogy minden k elemű megengedett $\mathscr{H}$ halmazra a $\mathscr{D}$ tartalmazza két $\mathscr{H}$-beli elem különbségét, akkor még $k = 3$ esetén is szóba jön a $\mathscr{D} = \mathscr{E}$ lehetőség, amikor is a (b) állítás csak $m \geq M$ mellett igaz.

4. A halászás művészete

Mint láttuk, a 2. tételből következik az 1. tétel, illetve sok egyéb értékes információ a Polignac-számok eloszlására vonatkozóan. A 2. tétel bizonyításának alapötlete szintén a [8] cikkben szerepel, és elnagyoltan annyit tesz, hogy megpróbáljuk előre megtippelni, hogy mely $n + \mathscr{H}$ alakú eltolt halmazokban várható az átlagosnál jóval több prímszám. Ezt jól csinálni egyfajta művészet, hiszen egyensúlyozni kell aközött, ami igaz és amit bizonyítani tudunk. Ha túl direkt módon választjuk ki a potenciálisan jó eltoltakat, akkor a várakozásunkat nem fogjuk tudni igazolni, ha pedig túl megengedőek vagyunk, akkor az eltoltakba nem esik majd elég prímszám. Formálisan az 1. ötlet egy valószínűségi finomításáról van szó:

2. ötlet. *Legyen $\mathscr{H} = \{h_1, \dots, h_k\}$ egy k elemű megengedett halmaz. Minden elég nagy $x > 0$ számra találjunk olyan valószínűségi mértéket az $x \leq n \leq 2x$ egészeken, amire nézve az $n + \mathscr{H} = \{n + h_1, \dots, n + h_k\}$ eltolt halmazba eső prímek számának várható értéke egynél nagyobb.*

A gyakorlatban ez annyit tesz, hogy olyan $\nu(n) \geq 0$ súlyokat keresünk, amikre bizonyíthatóan fennáll

$$\sum_{x \leq n \leq 2x} \nu(n) \sum_{i=1}^{k} 1_{n + h_i \text{ prím}} > \sum_{x \leq n \leq 2x} \nu(n). \tag{1}$$

Vegyük észre, hogy az egyenlőtlenség csak úgy teljesülhet, ha a jobb oldali összeg pozitív, és akkor ezzel az összeggel leosztva a $\nu(n)$ súlyok egy valószínűségi mértékké normálódnak. Az egyenlőtlenségből következik, hogy valamilyen $x \leq n \leq 2x$ egészre a belső összeg egynél nagyobb, tehát az $n + \mathscr{H}$ eltolt halmazba legalább két prímszám esik. Ha ez minden elég nagy $x > 0$ számra fennáll, akkor a 2. tételbeli állítás igaz a $\mathscr{H}$-ra.

A súlyokat úgy érdemes megválasztani, hogy $\nu(n)$ várhatóan akkor legyen nagy, amikor az $n + h_1, \dots, n + h_k$ számok között sok a prím, vagy legalábbis kevés

prímosztójuk van együttesen. A legnaivabb választást a már említett Dickson–Hardy–Littlewood-sejtés adja:

$$\nu(n) := 1_{n+h_1,\dots,n+h_k \text{ prím}}.$$

Ezek a súlyok a gyakorlatban nemigen használhatók, mert ha tudnánk, hogy az (1) jobb oldala minden elég nagy x-re pozitív, akkor rögtön a Dickson–Hardy–Littlewood-sejtést is igazoltuk volna. Vezessük be a

$$P(n) := (n+h_1)\dots(n+h_k)$$

jelölést, ekkor a [8]-beli súlyokhoz közelebb álló, de még mindig naiv változat a

$$\nu(n) := 1_{P(n) \text{ prímosztóinak száma legfeljebb } k+\ell},$$

ahol $0 \le \ell \le k$ egy szabadon választható paraméter. Ennek egy analitikus variánsa

$$\nu(n) := \sum_{d|P(n)} \mu(d) \log^{k+\ell}\left(\frac{P(n)}{d}\right), \tag{2}$$

ahol a $\mu(d)$ ún. *Möbius-függvény* a logikai-szitából jól ismert ± 1 súlyok megjelenése a prímszámok elméletében (vö. Eratosztenész-szita):

$$\mu(d) := \begin{cases} +1, & \text{ha } d \text{ páros sok különböző prímszám szorzata;} \\ -1, & \text{ha } d \text{ páratlan sok különböző prímszám szorzata;} \\ 0, & \text{ha } d \text{ nem négyzetmentes.} \end{cases}$$

Nem triviális, de a (2)-beli súlyokra teljesül

$$0 \le \nu(n) \le \log^{k+\ell}\big(P(n)\big),$$

továbbá $\nu(n)$ akkor és csak akkor pozitív, ha $P(n)$ különböző prímosztóinak száma legfeljebb $k+\ell$.

Goldston, Pintz, Yıldırım [8] és ezáltal Zhang [32] sikere nagy részben a (2)-beli naiv súlyok egy megfelelő finomításán múlik, ami lehetővé teszi az (1) két oldalának aszimptotikusan pontos kiszámítását. A finomítás Selberg [25] úttörő munkájának gyümölcse, amit a [8] merőben újszerű módon használ, bár a szerzők elismerik, hogy az ötlet részben Heath-Browntól [12] származik. A Selberg-szita abból indul ki, hogy ne az összes, hanem csak a $d \le R$ feltételt kielégítő négyzetmentes számokkal szitáljunk, ahol R egy szabadon választható „levágási paraméter". A $d \le R$ megszorítással a súlyok nemnegativitása már nehezen garantálható, ezért azokat még négyzetre is emeljük. A [8, 32] dolgozatokban konkrétan használt súlyfüggvény

$$\nu(n) := \left(\sum_{d|P(n)} \mu(d) \log_+^{k+\ell}\left(\frac{R}{d}\right)\right)^2, \tag{3}$$

ahol $R := x^{\theta/2}$ valamilyen rögzített $\theta > 0$ mellett. Itt $\log_+ t := \max(\log t, 0)$, tehát az összegben csak a $d \le R$ osztók vesznek részt. Ezeket a súlyokat érdemes megszorítani azokra az n-ekre, amikre $P(n)$ mentes a nagyon kicsi prímosztóktól. Ennek egyik oka, hogy az ilyen n-ekre az $n + h_1, \dots, n + h_k$ tényezők páronként relatív prímek, másrészt így az (1) két oldalának aszimptotikus kiszámításában a kis prímekből származó ún. lokális faktorok elhagyhatók. Mi a továbbiakban feltesszük, hogy $P(n)$ minden prímosztója legalább $\log\log\log x$, a többi n-re a $\nu(n)$-t nullának vesszük. A (3)-beli súlyfüggvény egy arányossági tényezőtől eltekintve nem más, mint

$$\nu(n) := \left(\sum_{d \mid P(n)} \mu(d) \left(1 - \frac{\log d}{\log R} \right)_+^{k+\ell} \right)^2, \tag{4}$$

ahol értelemszerűen $(1-t)_+ := \max(1-t, 0)$. Egy fontos általánosítást javasolt és vizsgált először Soundararajan [27, 28]:

$$\nu(n) := \left(\sum_{d \mid P(n)} \mu(d) g\left(\frac{\log d}{\log R} \right) \right)^2, \tag{5}$$

ahol $g : \mathbb{R} \to \mathbb{R}$ egy kellően sima függvény, ami a $[0, 1]$ intervallumon kívül nulla. Ezek az általánosabb súlyok lehetővé tették a [8, 32]-beli eredmények jelentős élesítését [5, 20], és megnyitották az utat az újabb felfedezések felé [14, 21].

5. Az átlagos kapás

Egy $\mathscr{H}$ megengedett halmazra az (1) bal és jobb oldalának hányadosa adja meg, hogy az $n + \mathscr{H}$ $(x \le n \le 2x)$ eltoltakba átlagosan hány prímszám esik, ha az átlagolást a $\nu(n)$ súlyokkal végezzük. Ez a hányados hatékonyan kiszámítható az (5) alakú súlyokra, feltéve, hogy a prímszámok bizonyos maradékosztályokban kellően egyenletesen oszlanak el. Az egyenletes eloszlás az (1) bal oldalának számítása közben merül fel, mégpedig a következőképpen. Az (5)-öt használva az (1) bal oldala

$$\sum_{i=1}^{k} \sum_{d,d' \le R} \mu(d)\mu(d') g\left(\frac{\log d}{\log R} \right) g\left(\frac{\log d'}{\log R} \right) \sum_{\substack{x \le n \le 2x \\ [d,d'] \mid P(n)}} 1_{n + h_i \text{ prím}},$$

ahol $[d, d']$ a d és a d' legkisebb közös többszöröse, tehát a $[d, d'] \mid P(n)$ reláció annyit tesz, hogy d és d' a $P(n)$ osztója. Pontosabban itt csalunk egy kicsit, de ez a lényeget nem érinti: a belső összegben csak azok az n-ek szerepelnek, amikre $P(n)$ minden prímosztója legalább $\log\log\log x$. A belső összeg olyan – nagyjából x és $2x$ közötti – prímek számát adja meg, amik modulo $q := [d, d']$ egy nem túl nagy számú adott maradékosztályba esnek. A külső összegzésben a négyzetmentes $d, d' \le R$ számok vesznek részt, ezért $q \le R^2 = x^\theta$ is négyzetmentes. A továbblépéshez célszerű feltenni, hogy az x és $2x$ közötti prímszámok maradékai a legtöbb szóba jövő q modulusra nézve nagyon egyenletesen oszlanak el:

***EH*(θ) hipotézis.** *Minden $A > 0$ számhoz található egy $C > 0$ konstans, hogy $x \geq 2$ esetén*

$$\sum_{\substack{q \leq x^{\theta} \\ q \text{ négyzetmentes}}} \max_{(a,q)=1} \left| \sum_{\substack{x \leq p \leq 2x \\ p \equiv a \pmod q}} 1 - \frac{1}{\varphi(q)} \int_x^{2x} \frac{dt}{\log t} \right| < C \frac{x}{\log^A x}.$$

Az egyenlőtlenségben szereplő integrál az x és $2x$ közötti prímek számát adja meg jó közelítéssel, $\varphi(q)$ a modulo q redukált maradékosztályok száma. A hipotézist a $\theta < 1/2$ értékekre Bombieri és Vinogradov igazolta egymástól függetlenül [1, 30], míg a $\theta < 1$ értékekre Elliott és Halberstam sejtette [3]. Mindezek után elmondhatjuk a számolás végeredményét, amit eredetileg Goldston, Pintz, Yıldırım [8] talált a $g(t) := (1-t)_+^{k+\ell}$ esetben (vö. (4)) és Soundararajan [27, 28] az általános esetben (vö. (5)).

4. tétel ([8, 27, 28])**.** *Legyen $\mathscr{H}$ egy k elemű megengedett halmaz. Legyen $g : \mathbb{R} \to \mathbb{R}$ egy k-szor folytonosan differenciálható függvény, ami a $[0,1]$ intervallumon kívül nulla. Az $EH(\theta)$ hipotézis mellett van olyan valószínűségi mérték az $x \leq n \leq 2x$ egészeken, amire nézve az $n + \mathscr{H}$ eltolt halmazba eső prímek számának várható értéke*

$$\frac{\theta}{2} \cdot \frac{k \displaystyle\int_0^1 g^{(k-1)}(t)^2 \frac{t^{k-2}}{(k-2)!}\, dt}{\displaystyle\int_0^1 g^{(k)}(t)^2 \frac{t^{k-1}}{(k-1)!}\, dt} + o(1).$$

A tételben $g^{(j)}$ a g függvény j. deriváltját jelöli, míg $o(1)$ egy nullához tartó mennyiség $x \to \infty$ mellett. Meglepő módon a fenti „átlagos prímkapás" mértéke nem éri el az egyet, de azt a k növelésével tetszőlegesen meg tudja közelíteni. Pontosabban az $EH(\theta)$ hipotézist egyelőre csak a $\theta < 1/2$ értékekre sikerült bizonyítani, míg [5, Theorem 16] szerint a második tört szuprémuma a lehetséges g-k felett kifejezhető a J_{k-2} Bessel-függvény első pozitív gyökéből mint

$$\sup_g \frac{k \displaystyle\int_0^1 g^{(k-1)}(t)^2 \frac{t^{k-2}}{(k-2)!}\, dt}{\displaystyle\int_0^1 g^{(k)}(t)^2 \frac{t^{k-1}}{(k-1)!}\, dt} = \frac{4k(k-1)}{j_{k-2,1}^2} \approx 4 - \frac{14.8461}{k^{2/3}}.$$

Mindenesetre a fenti tételből már következik, hogy ha $EH(\theta)$ fennáll bármilyen $\theta > 1/2$ értékre, akkor létezik a 2. tételt kielégítő k, tehát létezik Polignac-szám is. Például a [8] dolgozat fontos megállapítása, hogy az Elliott–Halberstam-sejtés mellett vehető $k = 6$, amikor is $\min \mathscr{D} \leq 16$.

6. Hogyan fogjunk több prímet?

A 4. tétel a határán van annak, hogy Polignac-szám létezése következzék belőle, ezért a megjelenésekor természetes kérdésként merült fel, hogy a benne szereplő várható érték megnövelhető-e valamiképpen. A szóban forgó várható érték a $o(1)$ hibatagot leszámítva két pozitív tényező szorzataként van megadva, ezért – ha kissé banálisak akarunk lenni – valamelyik tényezőt kell megnövelni úgy, hogy a másik tényező legfeljebb csak keveset változzék. A dolog azért bonyolultabb, mint hangzik, olyannyira, hogy a szakértők körében elterjedt volt a nézet, miszerint a meglévő eszközökkel ilyesfajta javítás nem várható. Mégis, a későbbi fejleményekben pontosan ez történt, mégpedig mindkét lehetséges irányban. Zhang [32] és Polymath8a [20] az első tényező megnövelésére koncentrált, míg Maynard [14] és Polymath8b [21] a második tényező megnövelésére.

Zhang [32] bizonyítása Motohashi és Pintz [16] egy fontos észrevételére épül: a 4. tételhez vezető számolásban nem vesztünk sokat, ha az $EH(\theta)$ hipotézist megszorítjuk azokra a négyzetmentes $q \le x^\theta$ számokra, amiknek minden prímosztója legfeljebb x^δ valamilyen $\delta > 0$ konstanssal. Az ilyen számokat x^δ-simáknak nevezzük, és sok előnyös tulajdonságuk van, pl. két egymás utáni osztójuknak a hányadosa legfeljebb x^δ, továbbá bármely osztójuk maga is x^δ-sima. Egy másik fontos észrevétel, hogy a számolásban csak azok az $a \bmod q$ maradékosztályok vesznek részt, amiket bármilyen $p \mid q$ prímosztó szerint redukálva a $h_j - h_i \bmod p$ $(i \ne j)$ maradékosztályok egyikét kapjuk. Zhang [32] az ily módon gyengített $EH(\theta, \delta)$ hipotézist igazolta valamilyen $\theta > 1/2$ és $\delta > 0$ paraméterekkel, és ebből adódott következésként a 2. tétel. A Polymath8a [20] projekt jelentősen bővítette a megfelelő (θ, δ) párok halmazát, minden ilyen párra csökkentette a megfelelő k értékét, és egyszerűsítette a bizonyítást. Pl. a θ felső határa Zhang [32] dolgozatában $1/2 + 1/584$, a Polymath8a [20] cikkben $1/2 + 7/300$.

Maynard [14] és Tao [29] az (5) helyett a

$$\nu(n) := \left(\sum_{d_1 \mid n+h_1} \dots \sum_{d_k \mid n+h_k} \mu(d_1) \dots \mu(d_k) f\left(\frac{\log d_1}{\log R}, \dots, \frac{\log d_k}{\log R} \right) \right)^2 \tag{6}$$

súlyokat használja, ahol $f : \mathbb{R}^k \to \mathbb{R}$ egy kellően sima függvény, ami a

$$\Delta_k := \{(t_1, \dots, t_k) \in \mathbb{R}^k : t_1, \dots, t_k \ge 0 \text{ és } t_1 + \dots + t_k \le 1\}$$

szimplexen kívül nulla. Ez a definíció jobban megfelel az eredeti célkitűzésnek, mert az $n + \mathscr{H}$ elemeiről külön-külön próbálja elérni, hogy kevés prímosztójuk legyen, nem csak a szorzatukat, a $P(n)$-t tartja szem előtt. Valójában az (5) a (6)-nak azon speciális esete, amikor $f(t_1, \dots, t_k)$ csak a változók összegétől függ, nevezetesen

$$f(t_1, \dots, t_k) = g(t_1 + \dots + t_k). \tag{7}$$

Ennek oka, hogy a megállapodásunk szerint csak olyan n-ekkel dolgozunk, amikre az $n + h_1, \dots, n + h_k$ számok páronként relatív prímek, vagyis a (6)-beli $d_1, \dots, d_k$ változók kölcsönösen egyértelműen meghatároznak egy $d \mid P(n)$ osztót a $d =$

$d_1 \dots d_k$ utasítással. Ezek után kimondhatjuk a 4. tétel megfelelőjét, ami a (6) súlyokkal való átlagolással következik. Először is bevezetünk egy jelölést a Δ_k szimplex $t_i = 0$ egyenlettel definiált lapjára:

$$\Delta_{k,i} := \{(t_1, \dots, t_k) \in \Delta_k : t_i = 0\}, \qquad i = 1, \dots, k.$$

5. tétel ([14, 29])**.** *Legyen $\mathscr{H}$ egy k elemű megengedett halmaz. Legyen $f : \mathbb{R}^k \to \mathbb{R}$ egy k-szor folytonosan differenciálható függvény, ami a Δ_k szimplexen kívül nulla. Az $EH(\theta)$ hipotézis mellett van olyan valószínűségi mérték az $x \le n \le 2x$ egészeken, amire nézve az $n + \mathscr{H}$ eltolt halmazba eső prímek számának várható értéke*

$$\frac{\theta}{2} \cdot \frac{\displaystyle\sum_{i=1}^{k} \int_{\Delta_{k,i}} \left(\frac{\partial^{k-1} f}{\partial t_1 \dots \partial t_{i-1} \partial t_{i+1} \dots \partial t_k} \right)^2}{\displaystyle\int_{\Delta_k} \left(\frac{\partial^k f}{\partial t_1 \dots \partial t_k} \right)^2} + o(1).$$

A (7) alakú függvényekre a fenti állítás a 4. tételbe megy át, mert a $t_1 + \dots + t_k = t$ affin hipersík a Δ_k-t egy $\frac{t^{k-1}}{(k-1)!}$ térfogatú $(k-1)$-szimplexben metszi, a $\Delta_{k,i}$-t pedig egy $\frac{t^{k-2}}{(k-2)!}$ térfogatú $(k-2)$-szimplexben. Általában véve is megmutatható [21, Lemma 41], hogy a tétel nem gyengül, ha szimmetrikus $f : \mathbb{R}^k \to \mathbb{R}$ függvényekre szorítkozunk: ilyenkor az $n + \mathscr{H}$ eltolt halmazba eső prímek számának várható értéke

$$\frac{\theta}{2} \cdot \frac{k \displaystyle\int_{\Delta_{k,k}} \left(\frac{\partial^{k-1} f}{\partial t_1 \dots \partial t_{k-1}} \right)^2}{\displaystyle\int_{\Delta_k} \left(\frac{\partial^k f}{\partial t_1 \dots \partial t_k} \right)^2} + o(1).$$

Mindezek fényében kézenfekvőnek tűnik egy f szimmetrikus polinomot keresni, amire a második tört 4-nél nagyobb, mert akkor alkalmas $\theta < 1/2$ értékkel új bizonyítást kapunk a 2. tételre. Más szóval, ha M_k jelöli a második tört szuprémumát a lehetséges f-ek felett, akkor $M_k > 4$ kimutatása a cél. A gyakorlatban célszerűbb az f helyett a nevezőben szereplő

$$F(t_1, \dots, t_k) := \frac{\partial^k f}{\partial t_1 \dots \partial t_k}$$

parciális deriváltat megadni, ami szintén szimmetrikus polinom. Maynard [14] az első két hatványösszeg, $t_1 + \dots + t_k$ és $t_1^2 + \dots + t_k^2$ polinomjaival kísérletezve talált egy 11-edfokú példát, amiből $M_{105} > 4$ következett. Polymath egy 23-adfokú F szimmetrikus polinommal demonstrálta az $M_{54} > 4$ egyenlőtlenséget [21, Theorem 23]. Másfelől belátható [21, Corollary 37], hogy M_k legfeljebb $\frac{k}{k-1} \log k$, amiért $M_{50} < 4$. Tehát a 2. tételben mindenképp vehető $k = 54$, de a $k = 50$ értékhez az 5. tétel nem elegendő. Ugyanakkor az 5. tételnek vannak olyan variánsai [21, Theorems 26 & 28], amikben $f : \mathbb{R}^k \to \mathbb{R}$ a Δ_k szimplexen kívül is lehet nullától

különböző: ezek segítségével a 2. tétel állítása a $k = 50$ értékre igazolható, és egy Elliott–Halberstam-típusú sejtés mellett $k = 3$ is megfelelő. Tehát bizonyításunk van arra, hogy $\min \mathscr{D} \leq 246$, és jó okunk van hinni abban, hogy $\min \mathscr{D} \leq 6$.

Mit ad az 5. tétel nagy k-ra? Már említettük az $M_k \leq \frac{k}{k-1} \log k$ felső becslést. A másik irányban Maynard [14] igazolta minden elég nagy k-ra, hogy $M_k \geq \log k - \log\log k - 2$. Valójában ez az alsó becslés minden $k \geq 2$ értékre teljesül [21, 48. oldal], és a $\log\log k$ helyett egy alkalmas abszolút konstanssal is igaz [21, Theorem 23]. Tehát a Bombieri–Vinogradov-tétel [1, 30] alapján kb. $\frac{1}{4} \log k$ darab prímet tudunk garantálni végtelen sok $n + \mathscr{H}$ eltoltban, és a Zhang-féle iránnyal kombinálva az $\frac{1}{4}$ együttható javítható $\frac{157}{600}$-ra [21, Theorem 6]. Ez a Dickson–Hardy–Littlewood-sejtés egy gyenge formája, és igen figyelemre méltó eredmény.

7. Történeti megjegyzések

A kis prímhézagok terén az egyik első fontos eredmény Erdős Páltól [4] származik: létezik egy $c < 1$ konstans úgy, hogy a

$$0 < p - p' < c \log p$$

egyenlőtlenségnek végtelen sok megoldása van prímekben. A $c < 1$ feltételnek az a jelentősége, hogy a prímszámtétel szerint az x körüli prímszámok átlagosan $\log x$ távolságra vannak egymástól, vagyis $c > 1$ esetén a fenti állítás egyszerű következmény, míg $c = 1$ esetén nem túl meglepő. A c-re többen próbáltak minél jobb értéket megadni, de az igazi áttörést Goldston, Pintz, Yıldırım [8] érte el, amikor sikerült belátniuk, hogy minden $c > 0$ konstans megfelelő. A [8]-ban kifejlesztett módszer fontos szerepet játszott Erdős két másik kedvenc problémájának megoldásában: van-e tetszőlegesen hosszú számtani sorozat a prímek között, illetve megjavítható-e a nagy prímhézagokra vonatkozó Rankin-becslés [23] egy végtelenhez tartó faktorral. Az elsőre ad választ a híres Green–Tao-tétel [10], a másodikat pedig néhány hónapja oldotta meg egymástól függetlenül Ford–Green–Konyagin–Tao [6] és Maynard [15]. A Rankin-becslés további javítását tartalmazza a napokban megjelent [7] preprint. A prímhézagokról és a kapcsolódó Landau-problémák történetéről részletes áttekintést nyújt a [17] dolgozat.

A Bombieri–Vinogradov-tétel [1, 30] két alappillére a Siegel–Walfisz-tétel [26, 31] és a Linnyik [13] által felfedezett ún. nagy szita egy letisztult formája. A nagy szita valószínűségszámítási jellegét az elsők között ismerte fel Rényi Alfréd [24], és a segítségével áttörést ért el az ikerprímsejtés és a hozzá szorosan kapcsolódó Goldbach-sejtés megközelítésében. Könnyen lehet, hogy már a Linnyik–Rényi-féle első verziókból következik az $EH(\theta)$ hipotézis valamilyen pozitív θ-val, legalábbis erre enged következtetni Bombieri egy megjegyzése [1, (1.12) alatt]. Mindez különösen érdekes az 5. tétel fényében, hiszen az itt szereplő várható érték bármilyen $\theta > 0$ mellett tetszőleges naggyá tehető a k és az $f : \mathbb{R}^k \to \mathbb{R}$ alkalmas megválasztásával.

A Polymath projekteket Timothy Gowers kezdeményezte 2009 elején a matematikai kutatás egy újfajta formájaként. A kutatás nyilvánosan, egy internetes

felületen keresztül történik, és bárki kötetlenül – akár névtelenül is – csatlakozhat. A prímhézagokra vonatkozó Polymath8 projekt egy intenzív évet ölelt fel 2013 nyarától 2014 nyaráig, és különösen sikeresnek mondható. Az Európai Matematikai Társulat (EMS) felkérésére több résztvevő – köztük a szerző is – leírta az idevágó személyes tapasztalatait, és ezek megjelentek az EMS Newsletter legfrissebb számában [22].

8. Köszönetnyilvánítás

A cikk a Fazekas Mihály Gimnáziumban, a Közép-európai Egyetemen és a Helvetic Algebraic Geometry Seminar-on tartott előadásaimra épül. Köszönöm a megtisztelő felkéréseket, ahogyan különböző grantok – OTKA K101855 és K104183, ERC AdG-228005 és AdG-321104 – támogatását is. Hálával tartozom Pintz Jánosnak, aki a kéziratot gondosan átnézte, és értékes megjegyzéseivel ellátta.

Irodalom

[1] E. Bombieri, On the large sieve, *Mathematika* **12** (1965), 201–225.

[2] L. E. Dickson, A new extension of Dirichlet's theorem on prime numbers, *Messenger of Math.* **33** (1904), 155–161.

[3] P. D. T. A. Elliott, H. Halberstam, A conjecture in prime number theory, In: *Symposia Mathematica*, Vol. IV (INDAM, Rome, 1968/69), 59–72, Academic Press, London, 1970.

[4] P. Erdős, The difference of consecutive primes, *Duke Math. J.* **6**, (1940), 438–441.

[5] B. Farkas, J. Pintz, Sz. Révész, On the optimal weight function in the Goldston-Pintz-Yıldırım method for finding small gaps between consecutive primes, In: *Number theory, analysis, and combinatorics*, 75–104, De Gruyter Proc. Math., De Gruyter, Berlin, 2014.

[6] K. Ford, B. Green, S. Konyagin, T. Tao, Large gaps between consecutive prime numbers, arXiv:1408.4505

[7] K. Ford, B. Green, S. Konyagin, J. Maynard, T. Tao, Long gaps between primes, arXiv:1412.5029

[8] D. A. Goldston, J. Pintz, C. Y. Yıldırım, Primes in tuples I, *Ann. of Math. (2)* **170** (2009), 819–862.

[9] A. Granville, D. M. Kane, D. Koukoulopoulos, R. J. Lemke Oliver, Best possible densities of Dickson m-tuples, as a consequence of Zhang-Maynard-Tao, arXiv:1410.8198

[10] B. Green, T. Tao, The primes contain arbitrarily long arithmetic progressions, *Ann. of Math. (2)* **167** (2008), 481–547.

[11] G. H. Hardy, J. E. Littlewood, Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes, *Acta Math.* **44** (1923), 1–70.

[12] D. R. Heath-Brown, Almost-prime k-tuples, *Mathematika* **44** (1997), 245–266.

[13] Y. V. Linnik, The large sieve (Russian), *Dokl. Akad. Nauk SSSR* **30** (1941), 292–294.

[14] J. Maynard, Small gaps between primes, *Ann. of Math. (2)*, **181** (2015), 383–413.

[15] J. Maynard, Large gaps between primes, arXiv:1408.5110

[16] Y. Motohashi, J. Pintz, A smoothed GPY sieve, *Bull. Lond. Math. Soc.* **40** (2008), 298–310.

[17] J. Pintz, Landau's problems on primes, *J. Théor. Nombres Bordeaux* **21** (2009), 357–404.

[18] J. Pintz, Polignac numbers, conjectures of Erdős on gaps between primes, arithmetic progressions in primes, and the bounded gap conjecture, arXiv:1305.6289

[19] M. A. de Polignac, Recherches nouvelles sur les nombres premiers, *Comptes rendus hebdomadaires des séances de l'Académie des sciences* **29** (1849), 397–401.

[20] D. H. J. Polymath, New equidistribution estimates of Zhang type, *Algebra & Number Theory* **8** (2014), 2067–2199.

[21] D. H. J. Polymath, Variants of the Selberg sieve, and bounded intervals containing many primes, *Res. Math. Sci.* **1** (2014), no. 12, 83 oldal

[22] D. H. J. Polymath, The "Bounded gaps between primes" Polymath project – A retrospective analysis, *EMS Newsletter*, no. 94, December 2014, 13–23.

[23] R. A. Rankin, The difference between consecutive prime numbers, *J. London Math. Soc.* **13** (1938), 242–244.

[24] A. Rényi, On the representation of an even number as the sum of a single prime and single almost-prime number (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **12**, (1948), 57–78.

[25] A. Selberg, Lectures on sieves, In: *Collected papers, Vol. II*, Springer-Verlag, Berlin, 1991.

[26] C. L. Siegel, Über die Classenzahl quadratischer Zahlkörper, *Acta Arith.* **1** (1935), 83–86.

[27] K. Soundararajan, Notes on Goldston-Pintz-Yıldırım, 2005, publikálatlan

[28] K. Soundararajan, Small gaps between prime numbers: the work of Goldston-Pintz-Yıldırım, *Bull. Amer. Math. Soc. (N.S.)* **44** (2007), 1–18.

[29] T. Tao, Polymath8b: Bounded intervals with many primes, after Maynard, 2013, blogbejegyzés, http://terrytao.wordpress.com/2013/11/19/polymath8b-bounded-intervals-with-many-primes-after-maynard/

[30] A. I. Vinogradov, The density hypothesis for Dirichet L-series (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **29** (1965), 903–934; Correction (Russian), *ibid.* **30** (1966), 719–720.

[31] A. Walfisz, Zur additiven Zahlentheorie. II., *Math. Z.* **40** (1936), 592–607.

[32] Y. Zhang, Bounded gaps between primes, *Ann. of Math. (2)* **179** (2014), 1121–1174.

Harcos Gergely

MTA Rényi Alfréd Matematikai Kutatóintézet,
1053 Budapest,
Reáltanoda u. 13–15.
gharcos@renyi.hu

Közép-európai Egyetem,
1051 Budapest,
Nádor u. 9.
harcosg@ceu.hu

A PROJEKTÍV TÉR REDUKTJAI

BODOR BERTALAN, KALINA KENDE

Jelölje P a megszámlálhatóan végtelen dimenziós alteret valamilyen $\mathbb{F}_q$ test fölött. Ebben a dolgozatban belátjuk, hogy ha G egy zárt részcsoportja a $\operatorname{Sym} P$ szimmetrikus csoportnak, ami tartalmazza $\operatorname{Aut} P$-t, akkor G-t tartalmazza a $\mathrm{P\Gamma L}(P)$ projektív szemilineáris csoport, vagy $G = \operatorname{Sym} P$.

1. Bevezető

A [4] és [2] cikkekben bizonyítják, hogy ha P egy véges dimenziós projektív tér valamilyen véges test fölött, és G egy részcsoportja $\operatorname{Sym}(P)$-nek (a P elemein ható teljes szimmetrikus csoportnak), ami tartalmazza P automorfizmuscsoportját, akkor $G \leq \mathrm{P\Gamma L}(P)$, $G = \operatorname{Sym}(P)$, vagy $G = \operatorname{Alt}(P)$ (a P elemein ható alternáló csoport). Ezekben a cikkekben a $\mathrm{PSL}(d, q)$ csoportot tartalmazó csoportokról szóló tételek kerültek kimondásra, amelyek egyszerű következménye az előbbi állítás. Mivel végtelen dimenzió esetén a PSL csoport nem értelmezhető, így ezen cikkek eredményeit nem lehet maradéktalanul általánosítani a végtelen dimenziós esetre. Az [1] cikkben alternatív bizonyítás található ugyanezen tételekre.

A [3] cikkben a racionális számtest feletti megszámlálhatóan végtelen dimenziós projektív tér esetén bizonyítják a maximalitást. Ehhez Jordan-csoportokat és más nem elemi eszközöket használnak.

Ebben a dolgozatban elemi eszközöket használva belátjuk, hogy az állítás a véges test feletti megszámlálhatóan végtelen dimenziós esetben is igaz. Végtelen halmaz esetén az alternáló csoportnak nincs természetes megfelelője, így ez esetben az állítás úgy szól, hogy ha P egy megszámlálhatóan végtelen dimenziós projektív tér egy véges test fölött, és $\operatorname{Aut}(P) \leq G \leq \operatorname{Sym}(P)$ egy *zárt* csoport, akkor $G \leq \mathrm{P\Gamma L}(P)$, vagy $G = \operatorname{Sym}(P)$. Itt a zártságot a pontonkénti konvegencia topológiája szerint értjük.

Egy megszámlálhatóan végtelen dimenziós projektív tér egy $\mathbb{F}_q$ véges test fölött mindig ω-kategorikus, azaz az elsőrendű elméletének pontosan egy megszámlálható modellje van izomorfia erejéig. Egy megszámlálható ω-kategorikus struktúránál megadható egy természetes bijekció a struktúra automorifizmuscsoportját tartalmazó zárt permutációcsoportok és az elsőrendben definiálható reduktjai között, ahol két reduktot ekvivalensnek tekintünk, ha egymásnak is reduktjai. Esetünkben az adódik, hogy P-nek pontosan $1 + d(k)$ reduktja van, ahol $q = p^k$, és p prím ($d(k)$ a k szám osztóinak számát jelöli).

1.1. Jelölések. Először bevezetünk néhány jelölést, amit a későbbiekben használni fogunk. Legyen G egy csoport, ami hat az Ω halmazon. Ekkor egy $S \subset \Omega$ esetén jelölje G_S az S halmaz elemenkénti stabilizátorát. Egy $\omega \in \Omega$ elem esetén jelölje $G(\omega)$ az ω elemnek a G csoport hatása szerinti orbitját.

Legyen V egy megszámlálhatóan végtelen dimenziós vektortér $\mathbb{F}_q$ felett. Ekkor a P projektív tér pontjaira tekinthetünk úgy, mint V egydimenziós altereire. Egy $v \in V \setminus 0$ vektor esetén jelölje $\tilde{v}$ a v vektor által kifeszített alteret, mint P elemét. Hasonlóan egy $X \subset V$ halmaz esetén jelölje $\tilde{X}$ az $\{\tilde{v} : v \in X\} \subset P$ halmazt. A következő lemma állításait gyakran fogjuk használni a későbbiekben, ezért ezeket itt külön is kimondjuk. Ezen állítások közvetlen következményei az előbbi definícióknak.

1.1. lemma. *Az előbbi jelöléseket használva a következők teljesülnek:*

(1) $G_S \supseteq G_{\{S\}}$.
(2) *Ha* $H \leq G$ *és* $\omega \in \Omega$, *akkor* $H(\omega) \subseteq G(\omega)$.
(3) *Tetszőleges* $S \subset P$ *részhalmazra és* $G \geq \operatorname{Aut} P$ *csoportra a* G_S *stabilizátor tranzitívan hat a* $P \setminus \langle S \rangle$ *halmazon.*
(4) *Tetszőleges* $S \subset \Omega$, $g \in G$ *és* $\omega \in \Omega$ *esetén* $\left|G_S(\omega)\right| = \left|G_{S^g}(\omega^g)\right|$.

2. Az Aut(P) csoport zárt szupercsoportjai

Ebben a fejezetben meghatározzuk a $\operatorname{Sym}(P)$ csoport azon zárt részcsoportjait, amik tartalmazzák az $\operatorname{Aut}(P)$ projektív lineáris csoportot. A zártságot itt a pontonkénti konvergencia topológiája szerint értjük. Ekkor egy $G \leq \operatorname{Sym}(P)$ csoport zártsága azzal ekvivalens, hogy ha $g \in \operatorname{Sym}(P)$, és a P projektív tér tetszőleges véges F részhalmazához létezik olyan $h \in G$, hogy $g|_F = h|_F$, akkor $g \in G$. Belátjuk, hogy ha egy $\operatorname{Aut}(P) \leq G \leq \operatorname{Sym}(P)$ csoport tartalmaz olyan transzformációt, ami nem szemiprojektív transzformáció (azaz nincs benne $\mathrm{P\Gamma L}(P)$-ben), akkor P tetszőleges S véges halmaza átvihető P egy projektív független elemekből álló részhalmazába egy G-beli elemmel.

2.1. lemma. *Tegyük fel, hogy* $\operatorname{Aut} P \leq G \leq \operatorname{Sym} P$, *és a* G *csoport* n*-tranzitívan hat* P*-n. Legyenek az* $a_1, a_2, \ldots, a_{n+1} \in P$ *elemek olyanok, hogy* $a_i \notin \langle a_j \mid j \neq i \rangle$ *valamilyen* $1 \leq i \leq n+1$ *esetén. Ekkor létezik olyan* $g \in G$ *elem, hogy az* $a_1^g, a_2^g, \ldots, a_{n+1}^g$ *elemek függetlenek.*

Bizonyítás. Legyen $S := \{a_1, \ldots, a_{n+1}\}$. Feltehető, hogy $i = n+1$. Legyen $S' := S \setminus \{a_{n+1}\}$. Ekkor a lemma feltétele szerint létezik olyan $h \in G$, hogy az S'^h halmaz független. Mivel $a_{n+1} \notin \langle S' \rangle$, ezért $\operatorname{Aut}(P)_{S'}(a_{n+1})$ végtelen, és így $\operatorname{Aut}(P)_{S'}(a_{n+1}) \subset G_{S'}(a_{n+1})$ is végtelen. A 1.1. lemma szerint azonban

$$\left|G_{S'^h}\left(a_{n+1}^h\right)\right| = \left|G_{S'}(a_{n+1})\right|,$$

így $G_{S'^h}\left(a_{n+1}^h\right)$ is végtelen. Ebből következik, hogy van olyan $k \in G_{S'}$ elem, amire $a_{n+1}^{hk} \notin \langle S'^h \rangle$. Ez azonban azt jelenti, hogy a $g = hk$ választás jó lesz, hiszen ekkor $S^g = S^{hk} = S'^h \cup \{a_{n+1}^k\}$, ami valóban egy független halmaz. ■

2.2. lemma. *Tegyük fel, hogy* $\operatorname{Aut} P \leq G \leq \operatorname{Sym} P$ *és a* G *csoport* n*-tranzitívan hat* P*-n. Tegyük fel továbbá, hogy* $S \subseteq V$*, ahol* $|S| = |\tilde{S}| = n$*. Ekkor a* $G_{\tilde{S}}$ *stabilizátor vagy tranzitív a* $P \setminus \tilde{S}$ *halmazon, vagy pontosan egy véges orbitja van, aminek hossza* $(q-1)^{n-1}$*.*

Bizonyítás. Mivel a G csoport n-tranzitív, ezért az állítást elég belátni független $S \subset V$ részhalmazokra. Legyen tehát $S = \{v_1, \ldots, v_n\}$, ahol a $v_1, \ldots, v_n$ vektorok (lineárisan) függetlenek. Legyen

$$A := \left\{ \sum_{i=1}^{n} \lambda_i v_i \mid \lambda_i \in \mathbb{F}_q \setminus 0 \right\} \quad \text{és} \quad B := V \setminus (A \cup S).$$

Azt állítjuk, hogy ekkor G tranzitívan hat a $\tilde{A}$ és a $\tilde{B}$ halmazon is. Ebből már következik a lemma állítása, hiszen $\tilde{A} \cup \tilde{B} = P \setminus \tilde{S}$, $|\tilde{A}| = \frac{|A|}{q-1} = \frac{(q-1)^n}{q-1} = (q-1)^{n-1}$, és a $\tilde{B}$ halmaz végtelen.

Először belátjuk, hogy G tranzitívan hat $\tilde{A}$-on. Ehhez elég belátni, hogy tetszőleges $u, v \in A$ vektorokhoz létezik olyan $\Gamma \in \operatorname{Aut}(V)$, hogy $v_i^\Gamma \in \langle v_i \rangle$ minden $1 \leq i \leq n$ esetén, és $u^\Gamma = v$. Legyenek tehát $u = \sum_{i=1}^n \lambda_i v_i \in A$ és $v = \sum_{i=1}^n \mu_i v_i \in A$ tetszőlegesek. Ekkor mivel $v_1, \ldots, v_n$ lineárisan függetlenek, ezért létezik olyan $\Gamma \in \operatorname{Aut}(V)$ lineáris transzformáció, amire $v_i^\Gamma = \frac{\mu_i}{\lambda_i} v_i$. Azt állítjuk, hogy ez a Γ jó választás, azaz $u^\Gamma = v$. Valóban, mivel Γ lineáris, ezért

$$u^\Gamma = \left(\sum_{i=1}^{n} \lambda_i v_i \right)^\Gamma = \sum_{i=1}^{n} \lambda_i v_i^\Gamma = \sum_{i=1}^{n} \mu_i v_i = v.$$

Most belátjuk, hogy G tranzitívan hat $\tilde{B}$-on is. Ehhez elég belátni, hogy ha $\tilde{a} \in \tilde{B}$, akkor az $\tilde{S} \cup \{a\}$ halmaz egy független halmazba képezhető valamilyen G-beli elemmel. Ebből már következik az állítás, hiszen $\operatorname{Aut}(P)$ (és így G is) tranzitívan hat a projektív független n-esek halmazán.

Ha $a \notin \langle S \rangle$, akkor $S \cup \{a\}$ független halmaz, így az $\tilde{S} \cup \{\tilde{a}\}$ halmaz is független. Tegyük fel most, hogy $a \in \langle S \rangle$. Ekkor $a = \sum_{i=1}^n \lambda_i v_i$ valamilyen $\lambda_i \in \mathbb{F}_q$-k esetén. Mivel $a \notin A$, ezért $\lambda_j = 0$ valamilyen $1 \leq j \leq n$-re. Ekkor $v_j \notin \langle v_i \mid i \neq j \rangle$, így $\tilde{v_j} \notin \langle \tilde{v_i} \mid i \neq j \rangle$. Ekkor azonban az 1.1. lemma szerint az $\tilde{S} \cup \{\tilde{a}\}$ halmaz átvihető egy független halmazba valamilyen G-beli elemmel, és ezt kellett bizonyítanunk. ■

2.3. lemma. *Tegyük fel, hogy* $\operatorname{Aut} P \leq G \leq \operatorname{Sym} P$*, és a* G *csoport* n*-tranzitívan hat* P*-n. Legyen továbbá* k *egy olyan egész szám, amire* $\frac{q^k-1}{q-1} \geq n$*. Ekkor minden* $S \subset P$*,* $|S| = n$ *halmazra a* G_S *stabilizátor minden* $P \setminus S$*-beli véges orbitja legfeljebb* $\frac{q^k-1}{q-1} - n$ *elemű.*

Bizonyítás. Legyen Q egy k dimenziós altere P-nek. Ekkor mivel $|Q| = \frac{q^k-1}{q-1} \geq n = |S|$, és a G csoport n-tranzitív, ezért feltehető, hogy $S \subset Q$. Ha $a \in P \setminus Q \subset P \setminus \langle S \rangle$, akkor az a elem G_S szerinti orbitja végtelen. Így Q tartalmazza G_S minden véges orbitját. Ebből következik, hogy minden $P \setminus S$-beli elem G_S szerinti orbitjának hossza legfeljebb $|Q \setminus S| = |Q| - n = \frac{q^k-1}{q-1} - n$. ■

2.4. lemma. *Minden $q, n \geq 3$ egészekhez létezik olyan k egész szám, amire*

$$(q-1)^{n-1} > \frac{q^{k+1}-1}{q-1} - n \geq 0$$

teljesül.

Bizonyítás. Ha $q = 3, 4$ és $n = 3, 4$, akkor az egyenlőtlenség teljesül $k = 1$ esetén. Tegyük fel most, hogy $q \geq 5$, vagy $q = 3, 4$ és $n \geq 5$. Legyen ekkor k a legkisebb olyan egész, amire $\frac{q^{k+1}-1}{q-1} \geq n$. Azt állítjuk, hogy erre a k-ra teljesülnek a lemmában felírt egyenlőtlenségek.

Mivel a k szám értékét minimálisnak választottuk, ezért $\frac{q^k-1}{q-1} < n$, amiből

$$nq + 1 > \frac{q^k-1}{q-1}q + 1 = \frac{q^{k+1}-1}{q-1} \geq n$$

adódik, így elég belátni, hogy $(nq+1) - n < (q-1)^{n-1}$. Ezt az állítást n szerinti teljes indukcióval bizonyítjuk. Ha $n = 5$ és $q = 3, 4$, akkor teljesül az egyenlőtlenség. Ha $n = 3$ és $q \geq 5$, akkor

$$(q-1)^2 > 4(q-1) - 1 \geq 3(q-1) + 1.$$

Az indukciós lépéshez tegyük fel, hogy már tudjuk, hogy

$$\big((n-1)q + 1\big) - (n-1) < (q-1)^{n-2},$$

ahol $n \geq 6$, vagy $n \geq 4$ és $q \geq 5$. Ekkor

$$(q-1)^{n-1} > (q-1)\big((n-1)(q-1)+1\big) > 2(n-1)(q-1) + 1 \geq n(q-1) + 1,$$

és ezt kellett bizonyítanunk. ■

2.5. lemma. *Legyen* $\mathrm{Aut}(P) \leq G \leq \mathrm{Sym}(P)$ *egy csoport. Ekkor* $G \leq \mathrm{P\Gamma L}(P)$ *vagy* G *3-tranzitív.*

Bizonyítás. Tegyük fel, hogy G nem 3-tranzitív. Belátjuk, hogy ekkor $G \leq \mathrm{P\Gamma L}(P)$. Mivel $\mathrm{Aut}(P)$ 2-tranzitív, ezért G is 2-tranzitív. Legyenek tehát $a, b \in P$ tetszőlegesek. Mivel G nem 3-tranzitív, ezért a 2.2. lemma szerint a $G_{a,b}$ stabilizátornak pontosan egy véges orbitja van $V \setminus \{a, b\}$-ben, aminek hossza $q-1$. Ha $c \notin \langle a, b\rangle$, akkor $G_{a,b}(c)$ végtelen, így ez a véges orbit benne van az $\langle a, b\rangle$ projektív altérben. Mivel azonban $\big|\langle a, b\rangle\big| = q+1$, ezért ez csak úgy lehetséges ha $G_{a,b}$ egyetlen véges orbitja $V \setminus \{a, b\}$-ben $\langle a, b\rangle \setminus \{a, b\}$. Ebből következik, hogy $c \in \langle a, b\rangle \setminus \{a, b\}$ pontosan akkor teljesül, ha $c \neq a, b$, és a $G_{a,b}(c)$ orbit véges.

Legyen most $g \in G$ tetszőleges. Legyenek továbbá $A, B, C \in P$ három egy egyenesre eső pont. Ekkor $C \in \langle A, B\rangle \setminus \{A, B\}$, és így az előbbiek szerint $\big|G_{A,B}(C)\big| < \infty$. Ebből következik (a 1.1. lemma szerint), hogy $G_{A^g,B^g}(C^g)$ is véges. Ez azonban azt jelenti, hogy $C^g \in \langle A^g, B^g\rangle \setminus \{A^g, B^g\}$, azaz az A^g, B^g, C^g pontok is egy egyenesre esnek. Azt kaptuk tehát, hogy a $g \in G$ transzformáció kollineáció (egyenestartó bijekció). Ekkor a projektív geometria alaptétele szerint $g \in \mathrm{P\Gamma L}(P)$. ■

Most belátjuk a dolgozat fő eredményét.

2.6. tétel. *Legyen $G \leq \mathrm{Sym}(P)$ egy zárt csoport. Ekkor $G \leq \mathrm{P\Gamma L}(P)$ vagy $G = \mathrm{Sym}(P)$.*

Bizonyítás. Ennél a bizonyításnál feltesszük, hogy $q \geq 3$. A $q = 2$ eset következik az $\mathbb{F}_2^\omega$ vektortér reduktjainak a klasszifikációjából. Tegyük fel, hogy $G \not\leq \mathrm{P\Gamma L}(P)$. Ekkor be kell látnunk, hogy $G = \mathrm{Sym}(P)$. Mivel $G \leq \mathrm{Sym}(P)$ zárt, ezért ehhez elég belátni, hogy G sűrű, azaz minden n-re n-tranzitív. Ezt n szerinti teljes indukcióval bizonyítjuk.

A 2.5. lemma szerint G 3-tranzitív. Az indukciós lépéshez tegyük fel, hogy a G csoport n-tranzitív, de nem $(n+1)$-tranzitív. Ekkor van olyan $S \subset P, |S| = n$, hogy G_S-nek legalább 2 orbitja van $P \setminus S$-en. Ekkor a 2.2. lemma szerint G_S-nek pontosan egy véges orbitja van $P \setminus S$-en, és ennek hossza $(q-1)^{n-1}$. A 2.3. lemma szerint azonban G_S-nek minden $V \setminus P$-beli véges orbitjának hossza legfeljebb $\frac{q^k-1}{q-1} - n$ minden olyan k-ra, amire $\frac{q^k-1}{q-1} - n \geq 0$. Tehát egy ilyen k-ra

$$(q-1)^{n-1} \leq \frac{q^k-1}{q-1} - n,$$

ami ellentmond a 2.4. lemmának, hiszen $n, q \geq 3$. ■

Legyen $q = p^k$ alakú, ahol p prím. Ekkor az $\mathrm{Aut}(\mathbb{F}_q) = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ csoport ciklikus, és a σ Frobenius-automorfizmus generálja. A $\mathrm{P\Gamma L}(P)$ csoport felírható $\mathrm{Aut}(P) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ alakban. Ebből következik, hogy a $\mathrm{P\Gamma L}(P)$ projektív szemilineáris csoportnak az $\mathrm{Aut}(P)$ csoportot tartalmazó részcsoportjai mind $\mathrm{P\Gamma L}_m(P) := \mathrm{Aut}(P) \rtimes \langle \sigma^m \rangle$ alakúak valamilyen $m|k$-ra. A $\mathrm{P\Gamma L}_m(P)$ csoportok mind véges sok $\mathrm{Aut}(P)$ szerinti mellékosztály uniói $\mathrm{P\Gamma L}(P)$-ben, így ezek a csoportok is zártak. Ezeket az észrevételeket használva a 2.6. tétel a következő formában is megfogalmazható.

2.7. tétel. *Legyen $G \leq \mathrm{Sym}(P)$ egy zárt csoport. Ekkor $G = \mathrm{P\Gamma L}_m(P)$ valamilyen $m|k$-re vagy $G = \mathrm{Sym}(P)$.*

A 2.7. tétel a követezőket jelenti a P struktúra reduktjaira vonatkozóan.

2.8. következmény. *P-nek pontosan $d(k)+1$ reduktja van, ahol $d(k)$ jelöli a k szám (pozitív) osztóinak számát. Speciálisan ha $q = p$ prím, akkor minden redukt triviális.*

Irodalom

[1] P. Bhattachabya, On groups containing the projective special linear group, *Arch. Math.,* **37** (1981), 295–299.

[2] W. M. Kantor, T. P. McDonough, On the maximality of $\mathrm{PSL}(d+1, q)$, $d \geq 2$, *J. London Math. Soc. (2),* **8** (1974), 426.

[3] I. Kaplan, P. Simon, *The affine and projective groups are maximal,* arXiv:1310.8157

[4] B. A. Pogorelov, Maximal subgroups of symmetric groups that are defined on projective spaces over finite fields, *Mat. Zametki,* **16** (1974), 91–100.

Bertalan Bodor, Kende Kalina: Closed supergroups of infinite dimensional projective linear groups

Let P be a countably infinite dimensional projective space over a finite prime field. In this paper we prove that $\mathrm{GL}\, P$ is maximal in $\mathrm{Sym}\, P$.

Bodor Bertalan
Eötvös Lóránd Tudományegyetem,
Algebra és Számelmélet Tanszék,
1117 Budapest,
Pázmány Péter sétány 1/c
bodorb@cs.elte.hu

Kalina Kende
Eötvös Lóránd Tudományegyetem,
Algebra és Számelmélet Tanszék,
1117 Budapest,
Pázmány Péter sétány 1/c
kkalina@cs.elte.hu

AZ $\mathbb{F}_2^\infty$ VEKTORTÉR REDUKTJAI

BODOR BERTALAN, KALINA KENDE

Klasszifikáljuk az $\mathbb{F}_2^\infty$ vektortér összes reduktját kölcsönös definiálhatóság erejéig.

1. Bevezetés

Az $\mathbb{F}_2^\infty$ vektortér univerzális abban az értelemben, hogy minden véges vagy megszámlálhatóan végtelen $\mathbb{F}_2$ feletti vektortér beágyazható $\mathbb{F}_2^\infty$-be. Ez a vektortér ω-kategorikus is: egy $\mathfrak{A}$ struktúrát ω-kategorikusnak nevezünk, ha megszámlálható, és elméletének minden megszámlálható modellje izomorf $\mathfrak{A}$-val. Az $\mathbb{F}_2^\infty$ vektortérre teljesül, hogy minden $\mathbb{F}_2^\infty$ két részalgebrája között menő φ izomorfizmus kiterjed $\mathbb{F}_2^\infty$ egy automorfizmusává. Ez a tulajdonság a homogenitás.

A megszámlálható struktúrák közül a homogén struktúrák állnak a legközelebb a véges struktúrákhoz. A homogén struktúrák elméletéből mi itt csak azokat az eredményeket ismertetjük röviden, amelyek közvetlenül kapcsolódnak a munkánkhoz. Sok és sokféle önmagában is érdeklődésre számot tartó struktúra tartozik közéjük: például a véletlen gráf, a véges testek feletti megszámlálhatóan végtelen dimenziós vektorterek, a racionális számok halmaza a szokásos rendezési relációval ellátva vagy a megszámlálható atommentes Boole-algebra. Kevésbé ismert, de egyszerűségük miatt fontos példa a Henson-gráfok családja, ezek azok a H_n megszámlálható homogén gráfok, amelyek nem tartalmaznak teljes K_n részgráfot [8], továbbá a homogén részbenrendezett halmaz, ami a véletlen gráfhoz hasonlóan megkapható véletlen konstrukcióként is [1]. A homogén struktúrák általános elméletének kidolgozása Fraïssé munkájával kezdődött [7], a Fraïssé-tétel karakterizálja azokat a véges struktúrákból álló osztályokat, amelyek előállnak, mint valamely homogén struktúra részstruktúráinak osztálya.

Egy struktúra egy reduktja alatt a struktúra alaphalmazán értelmezett relációk olyan halmazát értjük, amelyek mindegyikére igaz, hogy elsőrendű formulákkal definiálható a struktúrában. A reduktok halmazán értelmezhető egy kvázirendezés: $R_1 \lesssim R_2$ pontosan akkor, ha R_2 minden relációja definiálható R_1 feletti elsőrendű formulákkal. Két redukt kölcsönösen definiálható egymással, ha $R_1 \lesssim R_2$ és $R_2 \lesssim R_1$, azaz R_1 minden relációját definiálni lehet R_2 feletti elsőrendű formulákkal, és R_2 minden relációját definiálni lehet R_1 feletti elsőrendű formulákkal. Az 1. tétel fontos következménye, hogy ω-kategorikus struktúra minden reduktja is ω-kategorikus. Ez nem ω-kategorikus struktúrákra még akkor sem feltétlen igaz,

ha a struktúra nyelve véges, és csak relációkat tartalmaz. A [14]-ben megtalálható Lachlan egy ellenpéldájának leírása.

Egy redukt automorfizmuscsoportja pontosan azon permutációkból áll, amelyek megőrzik a redukt összes relációját, így speciálisan tartalmazza az eredeti struktúra automorfizmuscsoportját. Továbbá, egy redukt automorfizmuscsoportjára teljesül a következő zártsági feltétel: ha $g_1, g_2 \ldots \in \mathrm{Aut}(R)$ permutációk egy sorozata a redukt automorfizmuscsoportjából, amelyekre teljesül, hogy a struktúra minden a elemére van olyan j index és b_a elem, hogy minden $n > j$ indexre $g_n(a) = b_a$, akkor a $g_1, g_2 \ldots$ sorozat limesze, a $h(x) = b_x$ permutáció is benne van az automorfizmuscsoportban.

Azonban ω-kategorikus struktúrák esetén ennél erősebb is igaz: a struktúra automorfizmuscsoportját tartalmazó zárt részcsoportok bijekcióban állnak a reduktok kölcsönös definiálhatóságra vett ekvivalenciaosztályaival, így ω-kategorikus struktúrák esetén a reduktok klasszifikálása ekvivalens a struktúra automorfizmuscsoportját tartalmazó zárt részcsoportok osztályozásával. Mivel a véges testek fölötti legfeljebb megszámlálhatóan végtelen dimenziós vektorterek ω-kategorikusak, így $\mathbb{F}_2^\infty$ reduktjait vizsgálhatjuk az automorfizmuscsoportjaikon keresztül.

Számos ω-kategorikus homogén struktúrának sikerült osztályozni a reduktjait kölcsönös definiálhatóság erejéig. Kölcsönös definiálhatóság erejéig öt különböző reduktja van például a racionális számoknak a szokásos rendezésükkel ellátva [6], a véletlen gráfnak [14], a véletlen turnamentnek [2] és a véletlen poszetnek [12]. A klasszifikáció ismert a konstanssal ellátott Henson-gráfokra is [13]. A homogén rendezett gráfnak viszont már több mint 40 [3], a racionális számoknak a rendezéssel és egy konstanssal ellátva már 116 [10], a véletlen gráfnak egy konstanssal ellátva pedig már több mint 300 reduktja van. Ez utóbbira nem is ismert a teljes klasszifikáció. Ennek alapján megfogalmazható, hogy minél több eleme van a nyelvnek, várhatóan annál nagyobb lesz a reduktok száma, és ez egyszerűnek tűnő struktúrákra is meglepően nagy tud lenni.

Ezekben az eredményekben az a közös, hogy a vizsgált struktúrák nyelve minden esetben véges, és nem tartalmaz függvényjeleket. A legtöbb klasszifikáció ad hoc számolásokat használ, újabban Bodirsky és Pinsker munkája nyomán Ramsey-elméleti módszereket alkalmaztak sikerrel [4]. Az általunk vizsgált struktúrák ezzel szemben nem írhatóak le véges relációs nyelven. Így az eddig ismert módszerek nem működnek.

Az ω-kategorikus struktúrák elméletében fontos szerepet tölt be az alábbi tétel:

1. tétel (Engeler, Ryll–Nardzewski, Svenonius)**.** *Egy $\mathfrak{A}$ struktúra pontosan akkor ω-kategorikus, ha* $\mathrm{Aut}(\mathfrak{A})$ *oligomorf* [9].

Az 1. tétel egyszerű következménye az alábbi lemma:

2. lemma. *Legyen $\mathfrak{A}$ egy ω-kategorikus struktúra és R egy olyan reláció $\mathfrak{A}$ alaphalmazán, amelyet minden* $\mathrm{Aut}(\mathfrak{A})$*-beli permutáció megőriz. Ekkor R definiálható egy $\mathfrak{A}$ feletti elsőrendű formulával.*

Az $\mathbb{F}_2$ fölötti vektorterek struktúrája alapvetően különbözik az $\mathbb{F}_p$ fölötti vektorterekétől páratlan p prímekre. Ez elsősorban amiatt van, mert két nemnulla elem 2 karakterisztikában mindig független. Máshogyan fogalmazva, egy egy elem által generált részstruktúra az adott elemen kívül csak a 0-t tartalmazza.

Az $\mathbb{F}_2^\infty$ vektortér automorfizmuscsoportja a végtelen lineáris csoport amit $\mathrm{GL}(\infty,2)$-vel fogunk jelölni. Hasonlóan, $\mathrm{Aff}(\infty,2)$ jelöli az $\mathbb{F}_2$ feletti megszámlálhatóan végtelen dimenziós affin tér automorfizmuscsoportját. Az $\mathbb{F}_2^\infty$ elemein ható szimmetrikus csoportot $\mathrm{Sym}(\mathbb{F}_2^\infty)$-nel, a 0 elemnek a $\mathrm{Sym}(\mathbb{F}_2^\infty)$-beli stabilizátorát pedig $\mathrm{Sym}\left(\mathbb{F}_2^\infty\right)_0$-val fogjuk jelölni.

Egy $\mathrm{GL}(\infty,2) \leq G \leq \mathrm{Sym}(\mathbb{F}_2^\infty)$ csoport lezártját a pontonkénti konvergencia szerinti topológiában $\mathrm{Cl}\langle G\rangle$-vel jelöljük. A $\mathrm{Cl}\langle G\rangle$ csoportba tartozó permutációkat a következő módokon lehet karakterizálni:

- A φ permutáció akkor és csak akkor eleme $\mathrm{Cl}\langle G\rangle$-nek, ha $\mathbb{F}_2^\infty$ minden S részhalmazához létezik olyan ψ_S G-beli permutáció, amelyre φ és ψ_S megegyeznek az S halmazon.
- A φ permutáció akkor és csak akkor eleme $\mathrm{Cl}\langle G\rangle$-nek, ha létezik G-beli permutációknak olyan $\psi_1, \psi_2 \ldots$ sorozata, amelynek határértéke φ. Azaz minden $a \in \mathbb{F}_2^\infty$ elemre létezik j küszöbindex úgy, hogy minden $j < k$ indexre $\psi_k(a) = \varphi(a)$.

2. A 0-t megőrző reduktok

A $\mathrm{GL}(\infty,2)$ és a $\mathrm{Sym}\left(\mathbb{F}_2^\infty\right)_0$ csoport fixálja a 0-t. Ebben az alfejezetben belátjuk, hogy nincsen más, a 0-t fixáló $\mathrm{GL}(\infty,2) \leq G \leq \mathrm{Sym}(\mathbb{F}_2^\infty)$ zárt csoport. Ekvivalens átfogalmazásban: ha egy $\mathcal{R}$ redukt relációival definiálható a 0, akkor az a redukt vagy csak a 0-ból áll, vagy az összes, a vektortér felett definiálható reláció definiálható $\mathcal{R}$ relációival is.

3. lemma. *Legyen g olyan permutáció, amely nem eleme $\mathrm{GL}(\infty,2)$-nek, és fixálja a 0-t. Ekkor a $\left\langle \mathrm{GL}(\infty,2), g\right\rangle$ csoport és így az őt tartalmazó $\mathrm{Cl}\left(\mathrm{GL}(\infty,2), g\right)$ csoport is 3-tranzitívan hat az $\mathbb{F}_2^\infty \setminus \{0\}$ halmazon.*

Bizonyítás. Legyen a és b két tetszőleges nem nulla eleme $\mathbb{F}_2^\infty$-nek. Az a és a b elemek akkor és csak akkor lineárisan függetlenek, ha $a \neq b$. Most legyen c, d és e három páronként különböző nem nulla eleme $\mathbb{F}_2^\infty$-nek. Ezek akkor és csak akkor lineárisan függetlenek, ha $c + d \neq e$.

Mivel $\mathrm{GL}(\infty,2)$ tranzitívan hat a lineárisan független hármasokon, ezért elég megmutatnunk, hogy tetszőleges $j, k, l \in \mathbb{F}_2^\infty \setminus \{0\}$ páronként különböző elemekhez létezik $f \in \mathrm{Cl}\left(\mathrm{GL}(\infty,2), g\right)$ amire $f(j)$, $f(k)$ és $f(l)$ lineárisan függetlenek. Ha j, k és l egy lineárisan független rendszer, akkor f-et választhatjuk az identitásnak. Ha j, k és l lineárisan összefüggenek, akkor $j + k = l$. Mivel vannak olyan $a, b \in \mathbb{F}_2^\infty$ különböző elemek amikre $g(a + b) \neq g(a) + g(b)$, és $\mathrm{GL}(\infty,2)$ tranzitívan hat a $\mathbb{F}_2^\infty \setminus \{0\}$-beli elemekből álló lineárisan független párokon, léteznie kell olyan h $\mathrm{GL}(\infty,2)$-beli permutációnak amire $h(j) = a$ és $h(k) = b$. Az f függvényt választhatjuk $g \circ h$-nak. ■

4. lemma. *Legyen* $\mathrm{GL}(\infty,2) \leq G \leq \mathrm{Sym}\,(\mathbb{F}_2^\infty)_0$ *tetszőleges, a* 0*-t fixáló,* $\mathrm{GL}(\infty,2)$*-t tartalmazó zárt csoport. Legyenek továbbá* $a_1, a_2 \dots a_n$ *és* a_{n+1} *olyan* $\mathbb{F}_2^\infty \setminus \{0\}$*-beli páronként különböző elemek, amelyekre az* a_{n+1} *elemet nem tartalmazza a többi által generált* $\langle a_1, a_2 \dots a_n\rangle$ *altér. Ekkor ha a* G *csoport* n*-tranzitívan hat az* $\mathbb{F}_2^\infty \setminus \{0\}$ *halmazon, akkor tartalmaz olyan* h *permutációt, amelyre a* $h(a_1), h(a_2) \dots h(a_n)$, $h(a_{n+1})$ *elemek lineárisan független rendszert alkotnak.*

Bizonyítás. Mivel a G csoport n-tranzitívan hat az $\mathbb{F}_2^\infty \setminus \{0\}$ halmazon így választhatunk olyan G-beli h_1 permutációt, amelyre a $h_1(a_1), h_1(a_2) \dots h_1(a_n)$ elemek lineárisan függetlenek. Jelölje W a $\big\langle h_1(a_1), h_1(a_2) \dots h_1(a_n)\big\rangle$ generált alteret. A $h_1^{-1}(W)$ halmaz véges, mert egy véges dimenziós altér ősképe egy bijekcióra nézve, és 2 karakterisztikában a véges dimenziós alterek végesek. A lineáris leképezések független rendszereken való előírhatósága alapján az a_{n+1} elem pályája az $\{a_1, a_2 \dots a_n\}$ halmaz G-beli pontonkénti stabilizátorában végtelen elemszámú, így a $h_1(a_1)$ elem pályája a $\big\{h_1(a_1), h_1(a_2) \dots h_1(a_n)\big\}$ halmaz G-beli pontonkénti stabilizátorában is végtelen elemszámú. Tehát létezik olyan h_2 permutáció az $\{a_1, a_2 \dots a_n\}$ halmaz G-beli pontonkénti stabilizátorában, amelyre $h_2(a_{n+1})$ nem eleme $h_1^{-1}(W)$-nek. Ekkor a $h_1 \circ h_2$ permutáció megfelelő választás lesz h-nak. ■

5. lemma. *Legyen* $\mathrm{GL}(\infty,2) \leq G \leq \mathrm{Sym}\,(\mathbb{F}_2^\infty)_0$ *zárt csoport, amely* n*-tranzitívan hat az* $\mathbb{F}_2^\infty \setminus \{0\}$ *halmazon. Ekkor* $n \geq 3$ *esetén a* G *csoport hatása* $(n+1)$*-tranzitív is az* $\mathbb{F}_2^\infty \setminus \{0\}$ *halmazon.*

Bizonyítás. Elég megmutatnunk, hogy tetszőleges $a_1, a_2 \dots a_n, a_{n+1}$ páronként különböző $\mathbb{F}_2^\infty \setminus \{0\}$-beli elemekhez létezik olyan $h \in G$ permutáció, amelyre a $h(a_1)$, $h(a_2) \dots h(a_n), h(a_{n+1})$ elemek lineárisan függetlenek. Ennek bizonyítása azért elégséges, mert az $(n+1)$ elemű lineárisan független rendszereken a $\mathrm{GL}(\infty,2)$ csoport tranzitívan hat, így az őt tartalmazó G csoport is. Feltehetjük, hogy az $a_1, a_2 \dots a_n$ elemek lineárisan függetlenek, mivel a G csoport n-tranzitív.

Ha a_{n+1} nem eleme az $a_1, a_2 \dots a_n$ elemek által generált altérnek, készen vagyunk.

Ha a_{n+1} eleme az $a_1, a_2 \dots a_n$ elemek által generált altérnek, akkor a_{n+1} egyértelműen írható fel néhány a_j összegeként. Ha $a_{n+1} \neq \sum_{j=1}^n a_j$, akkor választhatunk olyan a_k elemet, amely lineárisan független a többi a_j elemtől, így alkalmazható a 4. lemma.

Ha $a_{n+1} = \sum_{j=1}^n a_j$ akkor a csoporthatás n-tranzitivitása miatt választhatunk egy h_1 permutációt G-ből úgy, hogy a $h_1(a_1), h_1(a_2) \dots h_1(a_{n-1})$ elemek lineárisan függetlenek legyenek, továbbá $h_1(a_n) = \sum_{j=1}^{n-1} h_1(a_j)$ is teljesüljön. Ha $h_1(a_{n+1})$ lineárisan független a többi elem képétől, akkor tudjuk alkalmazni a 4. lemmát. Ha pedig nem független, akkor felírható $h_1(a_{n+1}) = \sum_{j=1}^n \varepsilon_j h_1(a_j)$ alakban. Itt $\varepsilon_j \in \{0,1\}$ és legalább egy $\varepsilon_j = 0$, mert $h_1(a_{n+1}) \neq h_1(a_n)$, illetve legalább kettő $\varepsilon_j = 1$ kell, hogy legyen.

A $\big\{h_1(a_1), h_1(a_2) \dots h_1(a_{n-1})\big\}$ halmaz $\mathrm{GL}(\infty,2)$-beli stabilizátorába eső összes permutáció fixálja az összegüket, azaz a $h_1(a_n)$ elemet is. Tehát a $h_1(a_{n+1})$

elem pályája a $\{h_1(a_1), h_1(a_2)\dots h_1(a_{n-1})\}$ halmaz **stabilizátorára és nem pontonkénti stabilizátorára** nézve az $\mathrm{GL}(\infty,2)$ csoportban véges, mert része egy véges altérnek, de legalább két elemet tartalmaz, mert az egyelemű orbitok csak a $\{0\}$ és a $\{h(a_n)\}$. Legyen a h_2 permutáció a $\{h_1(a_1), h_1(a_2)\dots h_1(a_{n-1})\}$ stabilizátorának olyan eleme, amelyre $h_2\big(h_1(a_{n-1})\big) \neq h_1(a_{n-1})$; ekkor a $h_1^{-1}\big(h_2\big(h_1(a_j)\big)\big)$ elemeket a b_j szimbólumokkal jelölve, $b_1, b_2 \dots b_n$ lineárisan függetlenek, és $b_{n+1} \neq \sum_{j=1}^{n} b_j$. Ezt az esetet már korábban beláttuk. ■

6. tétel. *Legyen $g \in \mathrm{Sym}(\mathbb{F}_2^\infty)$ egy olyan permutáció, amelyik megőrzi a 0-t, és nem eleme $\mathrm{GL}(\infty,2)$-nek. Ekkor* $\mathrm{Cl}\big(\mathrm{GL}(\infty,2), g\big) = \mathrm{Sym}\,(\mathbb{F}_2^\infty)_0$.

Bizonyítás. $\mathrm{Sym}\,(\mathbb{F}_2^\infty)_0$ az egyetlen olyan zárt csoport, amely n-tranzitívan hat az $\mathbb{F}_2^\infty \setminus \{0\}$ halmazon minden $n \in \mathbb{N}$-re. A 3. lemmában beláttuk, hogy a $\mathrm{Cl}\big(\mathrm{GL}(\infty,2), g\big)$ csoport 3-tranzitív, a tétel állítása így teljes indukciót használva következik az 5. lemmából. ■

Ezzel befejeztük a 0-t megőrző reduktok osztályozását.

3. Az Aff$(\infty, 2)$ redukt

Most belátjuk, hogy amennyiben egy redukt nem fixálja a 0-t, akkor az csak az affin tér lehet az $\mathrm{Aff}(\infty,2)$ automorfizmuscsoporttal, vagy a struktúra nélküli halmaz a $\mathrm{Sym}(\mathbb{F}_2^\infty)$ automorfizmuscsoporttal. Mivel kettő karakterisztikában az affin terek egyenesei két pontból állnak, így a tér pontjainak bármely permutációja kollineáció. Ezért automorfizmus alatt olyan permutációkat értünk, amelyek a magasabb dimenziós altereket is a nekik megfelelő dimenziós alterekbe képezik.

Szükségünk lesz az eltolások csoportjára. Minden $\mathbb{F}_2^\infty$-beli a vektorhoz definiáljuk az a-val való eltolást a következőképpen: $t_a(x) = x + a$. Az eltolások csoportját T-vel fogjuk jelölni.

7. lemma. *Legyen f egy olyan $\mathrm{Sym}(\mathbb{F}_2^\infty)$-beli permutáció, amelyre igaz, hogy bármely három $a, b, c \in \mathbb{F}_2^\infty$ elemre az $f(a+b+c) = f(a)+f(b)+f(c)$ egyenlőség teljesül. Ekkor $f = t \circ h$ alakban előállítható, ahol $t \in \mathrm{T}$ egy eltolás, és $h \in \mathrm{GL}(\infty,2)$ egy vektortér-automorfizmus.*

Bizonyítás. Legyen t a $t(x) = x + f(0)$ eltolás, és $h(x) = t\big(f(x)\big) = f(x) + f(0)$. Ekkor a h permutáció megőrzi az összeadás műveletét, és fixálja a 0-t:

$$h(0) = f(0) + f(0) = 0,$$

$$h(a+b) = f(a+b+0) + f(0) = f(a) + f(b) + f(0) + f(0) = f(a) + f(b).$$

Tehát $h \in \mathrm{GL}(\infty,2)$ teljesül. Továbbá ekkor az $f(x) = \big(f(x) + f(0)\big) + f(0) = t\big(h(x)\big)$ azonosság is teljesül, azaz $f = t \circ h$. ■

A 7. lemma kimondásában szereplő $f(a+b+c) = f(a) + f(b) + f(c)$ képlet motiválja a következő négyváltozós reláció bevezetését:

$$R(a,b,c,d) \Leftrightarrow a+b+c = d.$$

Ez egy szimmetrikus reláció. Geometriai jelentése, hogy négy, páronként különböző elem pontosan akkor áll relációban egymással, ha egy kétdimenziós affin alteret alkotnak.

8. tétel. *A* $\mathrm{Cl}\big(\mathrm{GL}(\infty,2),\mathrm{T}\big)$ *csoport elemei karakterizálhatóak mint azok a permutációk, melyek megőrzik az* $R(a,b,c,d)$ *relációt. Tehát* f *pontosan akkor eleme a* $\mathrm{Cl}\big(\mathrm{GL}(\infty,2),\mathrm{T}\big)$ *csoportnak, ha* $f(a+b+c) = f(a)+f(b)+f(c)$ *teljesül minden* $a,b,c \in \mathbb{F}_2^\infty$ *elemre.*

Bizonyítás. Ha f eleme a $\big\langle \mathrm{GL}(\infty,2),\mathrm{T}\big\rangle$ csoportnak, akkor $f(a+b+c) = f(a) + f(b) + f(c)$ teljesül minden a, b, c $\mathbb{F}_2^\infty$-beli elemre, mert mind $\mathrm{GL}(\infty,2)$, mind T elemei megőrzik az R relációt.

Legyen f tetszőleges $\mathrm{Cl}\big(\mathrm{GL}(\infty,2),\mathrm{T}\big)$-beli permutáció. Ekkor f előáll mint egy $g_1, g_2 \ldots$ permutációsorozat limesze a pontonkénti konvergencia topológiájában, ahol minden g_j egy $\big\langle \mathrm{GL}(\infty,2),\mathrm{T}\big\rangle$-beli permutáció. Tehát minden $x \in \mathbb{F}_2^\infty$-hez létezik olyan n_x küszöbindex, hogy minden $j \geq n_x$ egészre igaz a $g_j(x) = f(x)$ egyenlőség. Legyenek az $a,b,c \in \mathbb{F}_2^\infty$ elemek fixek, és legyen $n_0 = \min\{n_a, n_b, n_c, n_{a+b+c}\}$, ekkor $f(a+b+c) = f(a)+f(b)+f(c)$ ekvivalens azzal, hogy $g_{n_0}(a+b+c) = g_{n_0}(a) + g_{n_0}(b) + g_{n_0}(c)$. Ez pedig igaz, mert $g_{n_0} \in \big\langle \mathrm{GL}(\infty,2),\mathrm{T}\big\rangle$. Tehát $f \in \mathrm{Cl}\big(\mathrm{GL}(\infty,2),\mathrm{T}\big)$-ből következik, hogy minden $a,b,c \in \mathbb{F}_2^\infty$ elemre $f(a+b+c) = f(a)+f(b)+f(c)$ igaz.

A másik irányú tartalmazás következik a 7. lemmából. ■

Tehát minden $\mathrm{Cl}\big(\mathrm{GL}(\infty,2),\mathrm{T}\big)$-beli f permutáció előáll mint $f = t \circ h$, ahol $t \in \mathrm{T}$ egy eltolás, és $h \in \mathrm{GL}(\infty,2)$ egy vektortér-automorfizmus. Így beláttuk, hogy $\mathrm{Aff}(\infty,2) = \mathrm{Cl}\big(\mathrm{GL}(\infty,2),\mathrm{T}\big)$, mivel a $\mathrm{Cl}\big(\mathrm{GL}(\infty,2),\mathrm{T}\big)$-beli permutációk affin automorfizmusok, és a 7. lemmából következik, hogy minden affin automorfizmus előáll $f = t \circ h$ alakban, ahol $t \in \mathrm{T}$ és $h \in \mathrm{GL}(\infty,2)$.

9. lemma. *Legyen* $\mathrm{GL}(\infty,2) \leq G \leq \mathrm{Sym}(\mathbb{F}_2^\infty)$ *olyan zárt csoport, amely nem fixálja a* 0*-t. Ekkor a* G *csoport* 3*-tranzitívan hat az* $\mathbb{F}_2^\infty$ *vektortéren.*

Bizonyítás. Elég megmutatnunk, hogy ha $a,b,c \in \mathbb{F}_2^\infty$ páronként különbőző elemek, akkor létezik olyan G-beli h permutáció, amelyre $h(a) = 0$. Ez azért elégséges, mert $\mathrm{GL}(\infty,2)$ tranzitívan hat az olyan $(0,x,y)$ rendezett hármasokon, amelyekre $x \neq y$, és a $\big(h(a),h(b),h(c)\big)$ elemek ilyen rendezett hármast alkotnak.

Tehát elég belátni, hogy G tranzitív az $\mathbb{F}_2^\infty$ vektortéren. A G csoport tartalmazza a $\mathrm{GL}(\infty,2)$ csoportot, és a $\mathrm{GL}(\infty,2)$ csoport tranzitívan hat a $\mathbb{F}_2^\infty \setminus \{0\}$ halmazon. Ezért G-nek legfeljebb két orbitja lehet a $\mathbb{F}_2^\infty$ vektortéren: a $\{0\}$ és a $\mathbb{F}_2^\infty \setminus \{0\}$ halmazok. Így G tranzitív kell, hogy legyen, mivel nem fixálja a 0-t. ■

10. lemma. *Legyen* $\mathrm{GL}(\infty,2) \leq G \leq \mathrm{Sym}(\mathbb{F}_2^\infty)$ *olyan zárt csoport, amely nem fixálja a* 0*-t. Ekkor a* G *csoport tranzitívan hat azokon az* (a,b,c,d) *rendezett négyeseken, amelyekre az* a*,* b*,* c *és* d *páronként különböző elemei a* $\mathbb{F}_2^\infty$ *vektortérnek, továbbá* $R(a,b,c,d)$ *is teljesül.*

Bizonyítás. A $\mathrm{GL}(\infty,2)$ csoport tranzitívan hat azokon az (a,b,c,d) négyeseken, amelyekre a, b, c és d a $\mathbb{F}_2^\infty \setminus \{0\}$ halmaznak páronként különböző elemei, és $a+b+c+d=0$ teljesül. Ez azért igaz, mert ebben az esetben az $\{a,b,c\}$ elemeknek lineárisan független rendszert kell alkotniuk. Ugyanis ha lineárisan összefüggőek lennének, akkor $d=a+b+c=a+b+(a+b)=0$ kellene, hogy legyen, viszont $d\neq 0$.

Továbbá a $\mathrm{GL}(\infty,2)$ csoport külön-külön tranzitívan hat az (a,b,c,d) rendezett négyesek azon négy részhalmazán, ahol a négy elem közül pontosan az egyik a 0, a másik három pedig különböző. Meg fogjuk mutatni, hogy $a=0$ esetén létezik olyan G-beli h permutáció, amelyre $0\notin\big\{h(a),h(b),h(c),h(d)\big\}$, továbbá $h(a)+h(b)+h(c)+h(d)=0$ teljesül. Analóg állítások igazak, ha valamelyik másik elem 0, ezzel a maradék eseteket is visszavezetjük az első bekezdésben bizonyítottra.

Legyen az (a,b,c,d) rendezett négyes olyan, amire $a=0$, továbbá $b+c=d$. Mivel a G csoport 3-tranzitív, a 9. lemma alapján ezért létezik olyan G-beli g permutáció, amelyre a $g(b)$, $g(c)$ és $g(d)$ elemek lineárisan független rendszert alkotnak.

Ha $g(0)=0$, akkor a 6. tétel szerint a 0 stabilizátorának a G csoportban $G_0=\mathrm{Sym}\,(\mathbb{F}_2^\infty)_0$-nak kell lennie. Így $G=\mathrm{Sym}\,(\mathbb{F}_2^\infty)$, mivel a G csoport nem fixálja a 0-t. Tehát ebben az esetben igaz a lemma állítása.

Ha $g(0)\neq 0$, és $g(b)$ nem eleme a $\big\langle g(c),g(d),g(0)\big\rangle$ generált altérnek, akkor a lineáris leképezések független rendszeren való előírhatósága alapján létezik olyan $\mathrm{GL}(\infty,2)$-beli h permutáció, amely stabilizálja a $g(c)$, $g(d)$ és $g(0)$ elemeket, viszont $h\big(g(b)\big)\neq g(b)$. Ekkor az $f=g^{-1}\circ h\circ g$ olyan permutáció lesz, amelyre $f(0)=0$, $f(c)=c$ és $f(d)=d$, de $f(b)\neq b$. Tehát az $f(b)$, $f(c)$ és $f(d)$ elemek lineárisan független rendszert alkotnak. A 6. tétel alapján ekkor is a 0 stabilizátora a G csoportban $G_0=\mathrm{Sym}\,(\mathbb{F}_2^\infty)_0$ kell, hogy legyen. Így $G=\mathrm{Sym}\,(\mathbb{F}_2^\infty)$, mivel a G csoport nem fixálja a 0-t.

A hátralévő eset az, amikor $g(0)\neq 0$, továbbá teljesül még az alábbi három feltétel is:

- $g(b)\in\big\langle g(c),g(d),g(0)\big\rangle$,
- $g(c)\in\big\langle g(b),g(d),g(0)\big\rangle$,
- $g(d)\in\big\langle g(b),g(c),g(0)\big\rangle$.

Indirekt tegyük fel, hogy $g(b)\neq g(c)+g(d)+g(0)$. Mivel $g(b)$, $g(c)$, $g(d)$ lineárisan függetlenek, és $g(b)\in\big\langle g(c),g(d),g(0)\big\rangle$ is teljesül, ezért vagy $g(b)=g(c)+g(0)$, vagy $g(b)=g(d)+g(0)$. Tegyük fel, hogy $g(b)=g(c)+g(0)$, ekkor a $\big\langle g(b),g(c),g(0)\big\rangle$ generált altér a $\big\{g(b),g(c),g(0),0\big\}$ kell, hogy álljon. Ez ellentmond annak, hogy $g(d)\in\big\langle g(b),g(c),g(0)\big\rangle$. A $g(b)=g(d)+g(0)$ lehetőség hasonlóan zárható ki. Így ellentmondásra jutottunk abból a feltevésből, hogy $g(b)\neq$

$g(c) + g(d) + g(0)$. Tehát a $g(b) + g(c) + g(d) + g(0) = 0$ egyenlőségnek teljesülnie kell. ■

11. tétel. *Legyen* $\mathrm{GL}(\infty, 2) \leq G \leq \mathrm{Sym}\,(\mathbb{F}_2^\infty)$ *olyan zárt csoport, amely nem fixálja a* 0*-t, és nem őrzi meg az* $R(a, b, c, d)$ *relációt sem. Ekkor* $G = \mathrm{Sym}\,(\mathbb{F}_2^\infty)$.

Bizonyítás. Mivel a G csoport nem őrzi meg az R relációt, így a 10. lemmát használva kapjuk, hogy a G csoport tranzitívan hat azokon az R-beli rendezett négyeseken, amelyek négy eleme páronként különböző. Így tudunk választani egy olyan g permutációt a G csoportból és hozzá olyan b és c elemeket az $\mathbb{F}_2^\infty \setminus \{0\}$ halmazból, melyekre $g(0) + g(b) + g(c) + g(b + c) \neq 0$ teljesül.

Ha a 0 eleme a $\big\{g(0), g(b), g(c), g(b + c)\big\}$ halmaznak, akkor a 10. lemma miatt feltehetjük, hogy $g(0) = 0$. Ekkor $g(b) + g(c) + g(b + c) \neq 0$, vagyis a $g(b)$, $g(c)$ és $g(b + c)$ elemek lineárisan függetlenek. A 6. tételt használva kapjuk, hogy $G_0 = \mathrm{Sym}\,(\mathbb{F}_2^\infty)_0$, tehát $G = \mathrm{Sym}\,(\mathbb{F}_2^\infty)$, mivel a G csoport nem őrzi meg a 0-t.

Most megvizsgáljuk azt az esetet, mikor 0 nem eleme a $\big\{g(0), g(b), g(c), g(b + c)\big\}$ halmaznak. Ekkor $g(0) + g(b) + g(c) + g(b + c) \neq 0$ miatt van legalább egy olyan x elem a $\{0, b, c, b + c\}$ halmazban, amelyre $g(x)$ nem eleme a $\Big\langle\big\{g(0), g(b), g(c), g(b + c)\big\} \setminus \big\{g(x)\big\}\Big\rangle$ halmaznak. Mivel a b, c és $b + c$ elemek szerepe szimmetrikus, így feltehetjük, hogy $x = b + c$ egy ilyen elem. Ekkor a lineáris leképezések lineárisan független rendszereken való előírhatósága alapján létezik olyan $\mathrm{GL}(\infty, 2)$-beli h permutáció, melyre $h\big(g(b + c)\big) \neq g(b + c)$, és az $y \in \{0, b, c\}$ elemekre $h\big(g(y)\big) = g(y)$ teljesül. Legyen $f = g^{-1} \circ h \circ g$. Ekkor $f(0) = 0$, $f(b) = b$ és $f(c) = c$ is teljesül, de $f(b + c) \neq b + c$. Használva a 6. tételt a 0 stabilizátorának a G csoportban $G_0 = \mathrm{Sym}\,(\mathbb{F}_2^\infty)_0$-nak kell lennie, amiből következik, hogy $G = \mathrm{Sym}\,(\mathbb{F}_2^\infty)$. ■

4. Összegzés

Ezzel befejeztük $\mathbb{F}_2^\infty$ reduktjainak klasszifikálását kölcsönös definiálhatóság erejéig.

12. tétel. *A* $\mathbb{F}_2^\infty$ *vektortérnek kölcsönös definiálhatóság erejéig pontosan a következő négy reduktja van:*

(1) *A vektortér* $\mathbb{F}_2^\infty$*, automorfizmuscsoportja* $\mathrm{GL}(\infty, 2)$*, ez pontosan azokból a permutációkból áll, melyek megőrzik a* 0 *konstansot és a* + *bináris műveletet.*

(2) *Az affin tér, automorfizmuscsoportja* $\mathrm{Aff}(\infty, 2)$*, ez pontosan azokból a permutációkból áll, melyek megőrzik az* R *négyváltozós relációt, azaz a kétdimenziós affin altereket.*

(3) *A struktúra egy* 0 *konstanssal, automorfizmuscsoportja* $\mathrm{Sym}\,(\mathbb{F}_2^\infty)_0$*, ez pontosan azokból a permutációkból áll, melyek megőrzik a* 0 *konstansot.*

(4) *A struktúra nélküli megszámlálhatóan végtelen halmaz, automorfizmuscsoportja* $\mathrm{Sym}\,(\mathbb{F}_2^\infty)$*, az összes permutáció az adott halmazon.*

Irodalom

[1] N. Ackerman, C. Freer, R. Patel, *Invariant measures concentrated on countable structures.* Preprint arXiv:1206.4011 [math.LO] (2012).

[2] J. H. Bennett, *The reducts of some infinite homogeneous graphs and tournaments.* Rutgers university, doktori értekezés (1997).

[3] M. Bodirsky, M. Pinsker, A. Pongrácz, *The 42 reducts of the random ordered graph,* beküldve (2013).

[4] M. Bodirsky, M. Pinsker, Reducts of Ramsey Structures, *Model Theoretic Methods in Finite Combinatorics,* American Mathematical Society, Contemporary Mathematics, **558** (2011), 489–519.

[5] P. J. Cameron, *Oligomorphic permutation groups.* London Mathematical Society Lecture Note Series, 152. Cambridge University Press (Cambridge, 1990).

[6] P. J. Cameron, Transitivity of permutation groups on unordered sets, *Mathematische Zeitschrift,* **148** (1976), 127–139.

[7] R. Fraïssé, Sur certaines relations qui généralisent l'order des nombres rationnels, *Comptes Rendus d' l'Académie des Sciences de Paris,* **237** (1953), 540–542.

[8] C. W. Henson, A family of countable homogeneous graphs, *Pacific Journal of Mathematics,* **38** (1971), 69–83.

[9] W. Hodges, *Model theory.* Encyclopedia of Mathematics and its Applications, 42. Cambridge University Press (Cambridge, 1993).

[10] M. Junker, M. Ziegler, The 116 reducts of $(Q, <, a)$, *J. Symbolic Logic,* **73** no. 3 (2008), 861–884.

[11] D. Macpherson, A survey of homogeneous structures, *Discrete Mathematics,* **311(15)** (2011), 1599–1634.

[12] P. P. Pach, M. Pinsker, G. Pluhár, A. Pongrácz, Cs. Szabó, Reducts of the random partial order, *Advances in Mathematics,* **267** (2014), pp. 94–120.

[13] A. Pongrácz, Reducts of the Henson graphs with a constant, *Annals of Pure and Applied Logic* (2013), accepted.

[14] S. Thomas, Reducts of the random graph, *Journal of Symbolic Logic,* **56(1)** (1991), 176–181.

Bertalan Bodor, Kende Kalina: First order definable reducts of the vectorspace $\mathbb{F}_2^\infty$

We classify the closed subgroups of the countable symmetric group which contain the automorphism group of $\mathbb{F}_2^\infty$, and thus also classify the structures which are first-order definable from $\mathbb{F}_2^\infty$ up to interdefinability.

Bodor Bertalan

Eötvös Lóránd Tudományegyetem,
Algebra és Számelmélet Tanszék,
1117 Budapest,
Pázmány Péter sétány 1/c
bodorb@cs.elte.hu

Kalina Kende

Eötvös Lóránd Tudományegyetem,
Algebra és Számelmélet Tanszék,
1117 Budapest,
Pázmány Péter sétány 1/c
kkalina@cs.elte.hu

AZ F_p^ω VEKTORTÉR REDUKTJAI PÁRATLAN PRÍMEK ESETÉN

BODOR BERTALAN, KALINA KENDE

Ebben a dolgozatban leírjuk az $\mathbb{F}_p$ feletti megszámlálhatóan végtelen dimenziós vektortér elsőrendben definiálható reduktjait, ahol $p \geq 3$ tetszőleges prím.

1. Bevezető

Legyen K egy tetszőleges véges test. Jelölje K^ω a K test feletti megszámlálhatóan végtelen dimenziós vektorteret. A lineáris leképezésekre vonatkozó kiterjesztési tulajdonság miatt igaz az, hogy K^ω bármely két véges altere közti izomorfizmus kiterjeszthető a teljes vektortér egy automorfizmusává. Ez a tulajdonság a homogenitás. Emellett ez a struktúra univerzális is abban az értelemben, hogy bármely véges vagy megszámlálhatóan végtelen K feletti vektortér beágyazható K^ω-ba. Szintén fontos tulajdonsága ennek a vektortérnek az ω-kategoricitás: egy struktúrát ω-kategorikusnak nevezünk, ha az elsőrendű elméletének pontosan egy megszámlálható modellje van izomorfia erejéig.

A megszámlálható, homogén, ω-kategorikus struktúrákat azért szokták gyakran vizsgálni, mert bizonyos értelemben a végtelen struktúrák közül ezek állnak legközelebb a véges struktúrákhoz. Ezek közé tartoznak például a véletlen gráf, a racionális számok halmaza a szokásos rendezési relációval ellátva és a megszámlálható atommentes Boole-algebra. Egy struktúra megértésénél fontos kérdés lehet, hogy a struktúrának mik az elsőrendben kifejezhető reduktjai, azaz milyen, esetleg gyengébb struktúrák adhatók meg a struktúra alaphalmazán elsőrendű definícióval. Egy megszámlálható ω-kategorikus struktúrával azért kényelmes dolgozni, mert ezen struktúráknál a struktúra reduktjai egyértelmű módon jellemezhetőek az automorfizmuscsoportjaikkal.

Már számos homogén, megszámlálható, ω-kategorikus struktúrára ismert a reduktok teljes klasszifikációja. Ezek közé tartoznak például a véletlen gráf [12], a véletlen hipergráf [13] és a véletlen részbenrendezett halmaz [10]. Ezekben az eredményekben az a közös, hogy a vizsgált struktúrák véges relációs nyelven homogén struktúrák. A legtöbb klasszifikáció ad hoc számolásokat használ, újabban Bodirsky és Pinsker munkája nyomán Ramsey-elméleti módszereket alkalmaztak sikerrel [4].

Ebben a dolgozatban a K^ω vektortér reduktjait vizsgáljuk abban az esetben, amikor $K = \mathbb{F}_p$, ahol $p \geq 3$ prím. A K^ω vektortér az eddig vizsgált struktúrákkal

szemben nem írható le véges relációs nyelven úgy, hogy homogén legyen, így ebben az esetben az eddig ismert módszerek nem működnek.

2. Reduktok

Egy $\mathfrak{A}$ struktúra reduktja egy olyan $\mathfrak{B}$ struktúra, aminek ugyanaz az alaphalmaza, mint $\mathfrak{A}$-nak, és a $\mathfrak{B}$ struktúra minden relációja és művelete kifejezhető az $\mathfrak{A}$ struktúra relációiból és műveleteiből valamilyen elsőrendű formula segítségével. Két reduktot ekvivalensnek tekintünk, ha egymásnak is reduktjai. Ha $\mathfrak{B}$ reduktja $\mathfrak{A}$-nak, akkor $\mathrm{Aut}(\mathfrak{A}) \subset \mathrm{Aut}(\mathfrak{B}) \subset \mathrm{Sym}(\mathfrak{A})$, továbbá könnyen ellenőrizhető az is, hogy $\mathrm{Aut}(\mathfrak{B})$ mindig zárt $\mathrm{Sym}(\mathfrak{A})$-ban. A zártságot a pontonkénti konvergencia topológiája szerint értjük. Ekkor egy $G \leq \mathrm{Sym}(\mathfrak{A})$ csoport zártsága azzal ekvivalens, hogy ha $g \in \mathrm{Sym}(\mathfrak{A})$, és az $\mathfrak{A}$ struktúra alaphalmazának tetszőleges véges F halmazához létezik olyan $h \in G$, amire $g|_F = h|_F$, akkor $g \in G$ is teljesül. Ha az $\mathfrak{A}$ struktúra ω-kategorikus, akkor ennek a megfordítása is igaz:

2.1. tétel. *Legyen $\mathfrak{A}$ egy megszámlálható, ω-kategorikus struktúra. Ekkor az $\mathfrak{A}$ alaphalmazán ható, $\mathrm{Aut}(\mathfrak{A})$-t tartalmazó zárt permutációcsoportok éppen az $\mathfrak{A}$ struktúra reduktjainak automorfizmuscsoportjai, továbbá két redukt automorfizmuscsoportja pontosan akkor egyezik meg, ha ekvivalensek.*

Ez azt jelenti, hogy egy ω-kategorikus struktúra reduktjai megfeleltethetőek az automorfizmuscsoportját tartalmazó zárt permutációcsoportoknak. Egy megszámlálható struktúra ω-kategoricitása könnyen ellenőrizhető a struktúra automorfizmuscsoportja segítségével.

2.2. tétel. *Egy megszámlálható $\mathfrak{A}$ struktúra pontosan akkor ω-kategorikus, ha az automorfizmuscsoportja $\mathrm{Aut}(\mathfrak{A})$ oligomorf, azaz minden $n \in \omega$ esetén véges sok n-orbitja van $\mathfrak{A}$-n.*

2.3. következmény. *Egy megszámlálható ω-kategorikus struktúra redukja is ω-kategorikus.*

Bizonyítás. Legyen $\mathfrak{A}$ egy megszámlálható struktúra, és $\mathfrak{B}$ ennek egy reduktja. Ekkor $\mathrm{Aut}(\mathfrak{B}) \supset \mathrm{Aut}(\mathfrak{A})$, így az $\mathrm{Aut}(\mathfrak{B})$ csoport minden n-orbitja az $\mathrm{Aut}(\mathfrak{A})$ csoport néhány n-orbitjának egyesítése. Ebből következik, hogy ha az $\mathfrak{A}$ struktúra automorfizmuscsoportja oligomorf, akkor ez minden reduktjára is igaz. A 2.2. tételt használva ebből azonnal következik az állítás. ■

2.4. állítás. *Legyen V megszámlálhatóan végtelen dimenziós vektortér egy véges test fölött. Ekkor V ω-kategorikus.*

Bizonyítás. A V struktúra megszámlálható, ezért alkalmazható a 2.2. tétel. Legyen $n \in \omega$ tetszőleges, és legyen U egy n dimenziós altere V-nek. Legyenek most $v_1, \ldots, v_n$ tetszőleges elemek. Ekkor $\dim\langle v_1, \ldots, v_n\rangle \leq n$, így létezik olyan $g \in \mathrm{Aut}\, V$ lineáris leképezés, amire $v_1^g, \ldots, v_n^g \in U$. Ez azt jelenti, hogy az U elemeiből alkotott rendezett n-esek reprezentálnak minden n-orbitot. U azonban véges dimenziós tér egy véges test fölött, tehát véges. Így U^n is véges, tehát az n-orbitok száma is véges. ■

2. bizonyítás. Ez az állítás közvetlenül a definícióból is bizonyítható. Jelöljük a V-hez tartozó alaptestet K-val. Tegyük fel most, hogy W egy megszámlálható modellje V elméletének. Ekkor mivel V vektortér, ezért V elmélete tartalmazza a vektortér axiómákat is. Ekkor azonban W elmélete is tartalmazza a vektortér axiómákat, így W is vektortér K fölött. Azt kell még belátnunk, hogy $\dim W = \omega$. $\dim W$ nem lehet véges, mert ha $\dim W$ véges lenne, akkor mivel K véges, ezért W is véges lenne, ami nem lehet. Tehát $\dim W$ végtelen. Ekkor azonban mivel K véges, ezért $\omega = |W| = \dim W$, és ezt kellett bizonyítanunk. ■

Ebben a dolgozatban azzal az esettel foglalkozunk, amikor az alaptest $K = \mathbb{F}_p$, ahol p egy páratlan prím. A dolgozat felépítése a következő: A 3. fejezetben azon zárt szupercsoportokat vizsgáljuk, amik a 0-t fixálják. Itt definiáljuk a $\sim_k$ ekvivalenciarelációkat, amik $p-1/k$ darab k elemű részre osztanak minden 1 dimenziós alteret. Kiderül, hogy a K^ω vektortér automorfizmuscsoportjának bármely G 0-t fixáló zárt szupercsoportjához van olyan k, hogy G hat a $\sim_k$-ekvivalenciaosztályok halmazán, és ez a hatás vagy (1) a teljes szimmetrikus csoport, vagy (2) a projektív lineáris csoport (és ekkor $k = p-1$). A 3.1. alfejezetben megadjuk az (1) esethez tartozó szupercsoportok teljes klasszifikációját. Végül a 3. fejezet eredményeit használva a 4. fejezetben bebizonyítjuk, hogy a vektortérnek pontosan 2 olyan reduktja van, ami a 0-t nem fixálja: ezek a végtelen dimenziós affin tér és a megszámlálhatóan végtelen halmaz (struktúra nélkül).

3. A vektortér 0-t fixáló reduktjai

Legyen $p \geq 3$ prím, és jelölje V a megszámlálhatóan végtelen dimenziós vektorteret $\mathbb{F}_p$ fölött. Ebben a fejezetben V automorfizmuscsoportjának azon zárt $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ szupercsoportjait vizsgáljuk, amelyek stabilizálják a 0-t. Ehhez először szükségünk lesz néhány definícióra. Tetszőleges $k \mid p-1$ esetén jelölje Γ_k az $\mathbb{F}_p$-beli k-adik egységgyökök által alkotott részcsoportot: $\Gamma_k = \{g \in \mathbb{F}_p \mid g^k = 1\}$. Nyilván $\Gamma_k \leq \mathbb{F}_p^\times$ és $|\Gamma_k| = k$.

3.1. definíció. Legyen $k \mid p-1$, $a, b \in V \setminus 0$. Ekkor legyen $a \sim_k b$ ha $a = \lambda b$ valamely $\lambda \in \Gamma_k$ esetén.

Mivel Γ_k csoport, $\sim_k$ ekvivalenciareláció. Valóban: $a \sim_k a$, mert $a = 1 \cdot a$. Ha $a \sim_k b$, akkor $a = \lambda b$ valamilyen $\lambda \in \Gamma_k$-ra, így $b = \lambda^{-1} a$, azaz $\sim_k$ szimmetrikus. Ha $a \sim_k b$ és $b \sim_k c$, akkor $a = \lambda b$ és $b = \mu c$ valamely $\lambda, \mu \in \Gamma_k$-ra. Mivel Γ_k csoport, ezért $\lambda\mu \in \Gamma_k$, így $a = \lambda\mu c$, tehát $a \sim_k c$ és így $\sim_k$ tranzitív is. A $\sim_k$ reláció az egydimenziós altereket $p-1/k$ darab k elemű osztályra osztja.

3.2. definíció. Legyen G egy tetszőleges csoport, ami hat $V \setminus 0$-n: $G \leq \mathrm{Sym}(V)$ és $a, b \in V \setminus 0$. Legyen $a \sim_G b$, ha $\langle a^g \rangle = \langle b^g \rangle$ minden $g \in G$ esetén.

Ekkor $\sim_G$ ekvivalenciareláció $V \setminus 0$-n. Egy $a \in V \setminus \{0\}$ esetén jelölje $\sim_G (a)$ az a vektor $\sim_G$-osztályát.

3.3. állítás. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *tetszőleges csoport. Ekkor* $\sim_G = \sim_k$ *valamilyen* $k \mid p-1$ *esetén.*

Bizonyítás. Ha $\mathrm{Aut}(V) \leq H \leq G \leq \mathrm{Sym}(V)_0$, akkor $\sim_G (a) \subseteq \sim_H (a)$, így $\sim_G (a) \subseteq \sim_{\mathrm{Aut}(V)} (a) = \langle a \rangle \setminus \{0\}$ teljesül. Legyen most $H_a = \{\lambda \in \mathbb{F}_p^\times \mid a \sim_G \lambda a\}$. Azt állítjuk, hogy H_a nem függ a választásától, azaz $a, b \in V \setminus \{0\}$ esetén $H_a = H_b$. Tegyük fel ugyanis, hogy $a \sim_G \lambda a$, de $b \nsim_G \lambda b$. Ekkor definíció szerint létezik olyan $h \in G$, hogy $\langle b^h \rangle \neq \langle \lambda b^h \rangle$. Legyen $g \in \mathrm{Aut}(V) \subset G$ egy olyan lineáris transzformáció, amelyre $a^g = b$. Ekkor $a^{gh} = b^h$ és $(\lambda a)^{gh} = (\lambda b^h)$, azaz $\langle a^{gh} \rangle \neq \langle \lambda a^{gh} \rangle$, ami ellentmond annak, hogy $a \sim_G \lambda a$. Jelöljük ezt a közös H_a halmazt Γ-val. Azt állítjuk, hogy Γ részcsoport $\mathbb{F}_p^\times$-ben. Mivel $\sim_G$ reflexív, $1 \in \Gamma$. A szimmetria miatt ha $\lambda \in \Gamma$, akkor $\lambda a \sim_G \lambda^{-1}(\lambda a)$-ból következik, hogy Γ zárt az inverzképzésre. Végül tegyük fel, hogy $\mu, \lambda \in \Gamma$, és $a \in V \setminus 0$ tetszőleges. Ekkor $a \sim_G \lambda a \sim_G \mu(\lambda a)$, így $a \sim_G \mu\lambda a$, így $\mu\lambda \in \Gamma$. Tehát Γ valóban részcsoportja $\mathbb{F}_p^\times$-nek, ami ciklikus, ezért ha $|\Gamma| = k$, akkor $k \mid p-1$ és $\Gamma = \Gamma_k$. Ebből pedig következik, hogy $u \sim_G v$ pontosan akkor teljesül, ha van olyan $\lambda \in \Gamma$, hogy $u = \lambda v$, azaz pontosan akkor, ha $u \sim_k v$, és ezt kellett bizonyítani. ■

A továbbiakban egy $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ csoport esetén jelölje k_G azt a $k \mid p-1$ értéket, amelyre $\sim_G = \sim_k$. A $\sim_G$ reláció definíciójából látható, hogy G megőrzi a $\sim_G$ relációt, így G hat a $\sim_G$-ekvivalenciaosztályok halmazán. Ha $k_G = p-1$, azaz a $\sim_G$-ekvivalenciaosztályok V egydimenziós alterei (a 0 nélkül), akkor a $\sim_G$-elvivalenciaosztályok egy megszámlálhatóan végtelen dimenziós $\mathbb{F}_p$ feletti projektív teret alkotnak az örökölt struktúrában. Most azt fogjuk belátni, hogy ha $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ egy zárt csoport, akkor G-re az alábbiak valamelyikre teljesül:

(1) $k_G = p-1$, és G a $P := (V \setminus 0)/\sim_G$ projektív téren a projektív lineáris transzformációk csoportjaként hat,

(2) G a szimmetrikus csoportként hat a $\sim_G$-ekvivalenciaosztályok halmazán.

Ezen állítás bizonyításához először belátjuk n szerinti indukcióval, hogy ha egy $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ csoportra nem teljesül a fenti (1) feltétel, akkor n tetszőleges pont beleképezhető egy G-beli elemmel V egy „elég kicsi" alterébe. Az alábbi észrevételt számos alkalommal fogjuk használni.

3.4. lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy csoport, és legyen* S *egy véges részhalmaza* V*-nek. Ekkor egy* $v \in V \setminus S$ *vektorra az alábbiak ekvivalensek:*

(1) $G_S(v)$ *végtelen.*

(2) $G_S(v)$ *tartalmaz olyan vektort, ami nincs benne az* $\langle S \rangle$ *altérben.*

(3) $G_S(v) \supset V \setminus \langle S \rangle$.

Bizonyítás. Az (1) → (2) irány nyilvánvaló, hiszen $\langle S \rangle$ véges. A (3) → (1) irány szintén nyilvánvaló, hiszen $V \setminus \langle S \rangle$ végtelen. Tegyük fel most, hogy v-re teljesül (2). Ekkor van olyan $u \in G_S(v)$ vektor, amit nem tartalmaz az $\langle S \rangle$ altér. Ekkor használva, hogy G_S tranzitív $V \setminus \langle S \rangle$-en, (3) adódik. ■

3.5. definíció. A továbbiakban egy $G \leq \mathrm{Sym}\,(V)_0$ csoport és egy $S \subset V$ részhalmaz esetén jelölje $A_k^G(S)$ azon $v \in V$ vektorok halmazát, amelyre $S \cup \{v\}$ beleképezhető egy G-beli elemmel V egy k dimenziós alterébe.

3.6. lemma. *Legyen $G \leq \mathrm{Sym}\,(V)_0$ egy csoport, és legyen $S \subset V$, $|S| = b$ egy tetszőleges részhalmaz. Ekkor az alábbiak valamelyike teljesül:*

- $\left|A_k^G(S)\right| = 0$,
- $\left|A_k^G(S)\right| = p^k$, *és van olyan* $g \in G$, *amire* $A_k^G(S)^g$ *egy* k *dimenziós altere* V*-nek.*
- $A_k^G(S) = V$.

Bizonyítás. Ha az S halmaz nem képezhető bele egy k dimenziós altérbe egy G-beli elemmel, akkor definíció szerint $A_k^G(S) = \emptyset$. Tegyük fel most, hogy nem ez a helyzet, és legyen ekkor $g \in G$ egy olyan transzformáció, amire S^g-t tartalmazza V egy U k-dimenziós altere. A definícióból könnyen látható, hogy $A_k^G(S) = \left(A_k^g(S^g)\right)^{g^{-1}}$, így elég belátni, hogy $\left|A_k^G(S^g)\right| = p^k$ vagy $A_k^G(S^g) = V$. Nyilván $U \subset A_k^G(S^g)$. Ha $U = A_k^G(S^g)$, akkor készen vagyunk, hiszen $|U| = p^k$, és U egy altér.

Ha nem, akkor $A_k^G(S^g)$ tartalmaz olyan v vektort, ami nincs benne U-ban, tehát $\langle S^g \rangle$-ben sincs benne. Ekkor a 3.4. lemma szerint

$$G_{S^g}(v) \supset V \setminus \langle S \rangle \supset V \setminus U,$$

így $A_k^G(S^g) \supset V \setminus U$. Azonban láttuk, hogy $A_k^G(S^g) \supset U$ is teljesül, így $A_k^G(S^g) = V$. ■

3.7. lemma. *Legyen $G \leq \mathrm{Sym}\,(V)_0$ egy csoport, és legyen $S \subset V$, $|S| = n$ egy tetszőleges részhalmaz. Tegyük fel továbbá, hogy egy $g \in G$ elemre teljesül, hogy $S^g \subset A_k^G(S)$. Ekkor $A_k^G(S) = A_k^G(S)^g$.*

Bizonyítás. Ha $A_k^G(S) = \emptyset$ vagy $A_k^G(S) = V$, akkor az állítás nyilvánvaló. Ha nem, akkor a 3.6. lemma szerint $\left|A_k^G(S)\right| = p^k$, és $A_k^G(S)^h$ egy k dimenziós altere V-nek valamilyen $h \in G$-re. Ez azonban azt jelenti, hogy tetszőleges $v \in A_k^G(S)$ esetén

$$v \in A_k^G\left(A_k^G(S)\right) \subset A_k^G(S^g) = A_k^G(S)^g,$$

hiszen $S^g \subset A_k^G(S)$. Tehát $A_k^G(S) \subset A_k^G(S)^g$, de $\left|A_k^G(S)\right| = \left|A_k^G(S)^g\right| = p^k$, így $A_k^G(S) = A_k^G(S)^g$ ■

A 3.7. lemmát általában abban az esetben fogjuk használni, amikor g egy lineáris transzformáció, és S lineárisan független elemekből áll. Ebben az esetben az állítás az alábbi formában is igaz.

3.8. következmény. *Legyen $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}\,(V)_0$ egy csoport, és legyen $S \subset V$. Tegyük fel továbbá, hogy $x_1, \ldots, x_m \in A_k^G(S)$ és $y_1, \ldots, y_m \in A_k^G(S)$ lineárisan független rendszerek. Ekkor tetszőleges $\lambda_1, \ldots, \lambda_m \in \mathbb{F}_p$ esetén*

$$\sum_{i=1}^{m} \lambda_i x_i \in A_k^G(S) \quad \textit{pontosan akkor, ha} \quad \sum_{i=1}^{m} \lambda_i y_i \in A_k^G(S).$$

Bizonyítás. Legyen $S := \{a_1, \dots, a_n\}$. Az általánosság megszorítása nélkül feltehető, hogy $y_1 = a_1, \dots, y_m = a_m$. Mivel $x_1, \dots, x_m$ lineárisan függetlenek, és $\dim\langle a_1, \dots, a_n, x_1, \dots, x_m\rangle \geq n$, ezért létezik olyan

$$\{i_{m+1}, \dots, i_n\} \subset \{1, 2, \dots, n\},$$

hogy $x_1, x_2, \dots, x_m, a_{i_{m+1}}, \dots, a_{i_n}$ lineárisan függetlenek. Ekkor létezik olyan $g \in \mathrm{Aut}(V) \subset G$ lineáris transzformáció, amire $a_j^g = x_j$, ha $1 \leq j \leq m$ és $a_j^g = a_{i_j}$. Ekkor $S^g \subset A_k^G(S)$ a feltétel szerint, így a 3.7. lemma szerint $A_k^G(S) = A_k^G(S)^g$. Mivel g lineáris, ezért ekkor $\sum_{i=1}^m \lambda_i a_i \in A_k^G(S)$ pontosan akkor teljesül, ha $\left(\sum_{i=1}^m \lambda_i a_i\right)^g \in A_k^G(S)$. Ismét a linearitást használva ez ekvivalens azzal, hogy $\sum_{i=1}^m \lambda_i a_i^g \in A_k^G(S)$, azaz $\sum_{i=1}^m \lambda_i x_i \in A_k^G(S)$, és ezt kellett bizonyítanunk. ■

A továbbiakban többször fogjuk használni az alábbi affin geometriai tényt, ezért most külön is kimondjuk.

3.9. lemma. *Legyen A egy véges dimenziós affin tér egy K test felett, ahol* $\mathrm{char}\, K \neq 2$. *Tegyük fel továbbá, hogy a $\emptyset \neq H \subset A$ halmazra teljesül a következő: ha $x, y \in H$, akkor $L(x, y) \subset H$, ahol $L(x, y)$ jelöli az x és y pontok által kifeszített egyenest. Ekkor H affin altere A-nak.*

Vegyük észre, hogy a 3.9. lemmában tényleg szükséges a $\mathrm{char}\, K \neq 2$ feltétel. Tegyük fel ugyanis, hogy $K = \mathbb{F}_2$, és legyen A tetszőleges affin altér $\mathbb{F}_2$ felett. Ekkor A tetszőleges részhalmazára teljesül a feltétel, hiszen ekkor tetszőleges $x, y \in A$ különböző pontok esetén $L(x, y) = \{x, y\}$.

3.10. lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}\,(V)_0$ *egy csoport, és legyen $S \subset V$, $|S| = n$ lineárisan független vektorok halmaza. Ekkor ha $A_k^G(S)$ tartalmaz egy 0-n nem átmenő affin egyenest, akkor $\left|A_k^G(S)\right| \geq p^{n-1} + 1$. Speciálisan $k < n$ esetén $A_k^G(S) = V$.*

Bizonyítás. Legyen $S = \{a_1, \dots, a_n\}$, és legyen L egy affin egyenes, ami nem megy át a 0-n, és $L \subset A_k^G(S)$. Legyen u, v két tetszőleges (különböző) pont L-en, ekkor $L = L(u, v)$. Mivel az L egyenes nem megy át a 0-n, ezért az u és v vekorok lineárisan függetlenek. Legyen most A az $a_1, \dots, a_n$ pontok által kifeszített affin altér V-ben, és legyen $H := A \cap A_k^G(S)$. Azt állítjuk, hogy a H halmazra teljesülnek a 3.9. lemma feltételei. Legyenek ugyanis $x, y \in H$ tetszőlegesek. Azt kell belátnunk, hogy $L(x, y) \subset A \cap A_k^G(S)$. Az $l(xy) \subset A$ tartalmazás triviális, mert A affin altér. Tehát már csak azt kell belátnunk, hogy az $L(x, y)$ egyenest tartalmazza $A_k^G(S)$.

Tegyük fel először, hogy az x és y vektorok lineárisan összefüggenek. Ekkor $y = \lambda x$ valamilyen $\lambda \in \mathbb{F}_p$-re, és így $0 \in L(x, y)$. Ekkor azonban $0 \in A$ is teljesül, mert A affin altér. Ez azonban lehetetlen, hiszen A minden eleme $\sum_{i=1}^n \lambda_i a_i$ alakú, ahol $\sum \lambda_i = 1$, ami nem lehet 0, mivel az $a_1, \dots, a_n$ vektorok lineárisan függetlenek.

Legyenek most x és y lineárisan függetlenek. Azt kell belátnunk, hogy minden $\lambda \in \mathbb{F}_p$-re $\lambda x + (1 - \lambda)y \in A_k^G(S)$. A 3.8. következmény miatt ehhez elég belátni, hogy vannak olyan x' és y' lineárisan független elemek $A_k^G(S)$-ben, amire $\lambda x' +$

$(1-\lambda)y' \in A_k^G(S)$ teljesül. Mivel $L = L(u,v) \subset A_k^G(S)$, ezért az $x' = u$ és az $y' = v$ választás megfelel.

Ezzel beláttuk, hogy a H halmazra teljesülnek a 3.9. lemma feltételei, így a 3.9. lemma szerint H affin altér. Mivel H tartalmazza az $a_1, \ldots, a_n$ vektorokat, ezért csak $H = A$ lehetséges. Azt kaptuk tehát, hogy az $a_1, \ldots, a_n$ vektorok által kifeszített affin alteret tartalmazza $A_k^G(S)$. Mivel ezek a vektorok lineárisan függetlenek, ezért affin függetlenek is, így ezen altér számossága p^{n-1}. Amint már láttuk, ez az altér nem tartalmazza a 0-t. A 0-t azonban mindig tartalmazza $A_k^G(S)$, ha nem üres, így $\left|A_k^G(S)\right| \geq p^{n-1}+1$. Végül ha $n \geq k+1$, akkor $\left|A_k^G(S)\right| > p^k$, és ekkor a 3.6. lemma szerint csak $A_k^G(S) = V$ lehetséges. ■

A következő állítás bizonyításához szükségünk lesz az alábbi technikai jellegű lemmára.

3.11. lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}\,(V)_0$ *egy csoport, és legyen* $S \subset V$, $|S| = n$ *lineárisan független vektorok halmaza. Tegyük fel továbbá, hogy az* $A_k^G(S)$ *halmaz tartalmaz egy*

$$v = \sum_{i=1}^{n} \lambda_i a_i \in A_k^G(G)$$

alakú vektort valamilyen λ_i*-kre, ahol a* λ_i *együtthatók közül legalább* 2 *nem* 0, *és nem mindegyik* -1.

Ekkor léteznek olyan $b_1, \ldots, b_n, w \in A_k^G(S)$ *vektorok, amelyekre* $b_1, \ldots, b_n$ *lineárisan függetlenek,* $w \notin \langle b_1 + b_2 + \ldots + b_n \rangle$, *és* $w \notin \langle b_i, b_j \rangle$ *semmilyen* i, j*-re.*

Bizonyítás. Ha a $b_i = a_i$, $v = w$ választás jó, akkor készen vagyunk. Tegyük fel ezért, hogy nem ez a helyzet. Ekkor $v = \lambda(a_1 + a_2 + \ldots + a_n)$ valamilyen $\lambda \neq -1$-re vagy $v \in \langle a_i, a_j \rangle$ valamilyen $1 \leq i < j \leq n$ indexekre. Tegyük fel először, hogy $v = \lambda(a_1 + a_2 + \ldots + a_n)$ valamilyen $\lambda \neq -1$-re. Ebben az esetben $a_1 = \frac{1}{\lambda}v - a_2 - \ldots - a_n$, így mivel $n \geq 3$ és $\frac{1}{\lambda} \neq -1$, ezért ekkor a $b_1 = v, b_2 = a_2, \ldots, b_n = a_n, w = a_1$ választás megfelel a feltételeinknek.

Maradt az az eset, amikor $v \in \langle a_i, a_j \rangle$ teljesül valamilyen $1 \leq i < j \leq n$-re. Ebben az esetben $v = \lambda a_i + \mu a_j$ alakú, ahol $\lambda, \mu \neq 0$. Mivel $n \geq 3$, ezért létezik egy $l \neq i, j$ index. Legyen ekkor $w = \lambda a_i + \mu a_j$. A 3.8. következmény szerint $w \in A_k^G(S)$. Legyen most $b_i = \lambda a_i + \mu a_j$, és legyen $b_m = a_m$, ha $m \neq i$. Ekkor $b_1, \ldots, b_n, w \in A_k^G(S)$, és mivel $\lambda \neq 0$, ezért a $b_1, \ldots, b_n$ vektorok lineárisan függetlenek, továbbá

$$w = \lambda a_i + \mu a_l = \lambda a_i + \mu a_j + \mu(a_l - a_j) = b_i + \mu b_l - \mu b_j.$$

Ezt azt jelenti, hogy a $b_1, \ldots, b_n, w$ vektorok ezen választása megfelel a feltételeinknek, hiszen $\mu \neq 0$, és $p \geq 3$ miatt $1 = \mu = -\mu$ nem lehetséges. ■

Tegyük fel, hogy $G \leq \mathrm{Sym}\,(V)_0$ egy olyan csoport, amire teljesül, hogy tetszőleges $a_1, \ldots, a_n$ nem nulla elemek beleképezhetőek egy k dimenziós W altérbe egy G-beli transzformációval valamilyen k-ra. Azt állítjuk, hogy ekkor $n \leq \frac{p^k-1}{k_G}$. Ekkor ugyanis az $a_1, \ldots, a_n$ vektorokkal együtt a $\sim_G (a_i)$ osztály minden eleme is beleképződik az altérbe. Mivel ezen osztályok diszjunktak, és $0 \in W$, a $\sim_G (a_i)$

osztályok elemszáma k_G, az $nk_G + 1 \leq |W| = p^k$ becslés adódik, azaz átrendezve $n \leq \frac{p^k-1}{k_G}$.

Azt kaptuk tehát, hogy $\frac{p^k-1}{k_G}$ egy olyan n lehetséges legnagyobb értéke, amire minden V-beli n-es beleképezhető V egy k dimenziós alterébe egy G-beli transzformációval. A továbbiakban majd belátjuk, hogy bizonyos feltételek mellett ez az érték „majdnem" el is érhető.

3.12. állítás. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy csoport, amire* $k_G < p-1$*; vagy* $k_G = p-1$ *és* G *hatása a* $P := (V \setminus 0)/\sim_G$ *projektív téren* nem *a projektív lineáris transzformációk csoportja. Tegyük fel továbbá, hogy az* $n \geq 3$*, és legyen* k *a legkisebb olyan egész szám, amire teljesül, hogy* $k \geq 2$ *és* $n \leq \frac{p^k-1}{k_G} - 1$*. Ekkor tetszőleges* $S \subset V$*,* $|S| = n$ *halmaz beleképezető* V *egy* k *dimenziós alterébe egy* G*-beli elemmel.*

Bizonyítás. Az állítást n szerinti teljes indukcióval bizonyítjuk. Tegyük fel először, hogy $n = 3$. Ekkor elég belátni, hogy 3 lineárisan független elem beleképezhető V egy 2 dimenziós alterébe egy G-beli elemmel.

1/a eset: $n = 3$ *és* $k_G = p-1$. Tekintsük ekkor G hatását a $P := (V \setminus 0)/\sim_G$ projektív téren. A feltétel szerint ez nem a projektív lineáris csoport, legyen tehát $g \in G$ egy olyan elem, aminek a hatása a P projektív téren nem projektivitás. A projektív geometria alaptétele szerint egy $\mathrm{Sym}(P)$-beli permutáció pontosan akkor projektivitás, ha tartja az egyenesket, így van olyan $L \subset P$ projektív egyenes, amire L^g nem projektív egyenes. Legyen U az L egyeneshez tartozó 2 dimenziós altér V-ben. Ekkor tehát $\dim\langle U^g\rangle \geq 3$, így vannak olyan $a, b, c \in U^g \subset V$ lineárisan független elemek, amikre $a^{g^{-1}}$, $b^{g^{-1}}$, $c^{g^{-1}}$ vektorokat tartalmazza az U 2 dimenziós altér. Mivel $\mathrm{Aut}(V)$ (és így G is) tranzitívan hat a V-beli lineárisan független hármasok halmazán, így tetszőleges lineáris független hármas beleképezhető egy 2 dimenziós altérbe.

1/b eset: $n = 3$ *és* $k_G < p-1$. Ekkor léteznek olyan $0 \neq a, b \in V$ elemek, amikre $\langle a\rangle = \langle b\rangle$, de $a \nsim_G b$. Ekkor tehát a^g, b^g lineárisan függetlenek valamilyen $g \in G$ esetén. Legyen c egy az a^g és b^g-től független vektor V-ben. Ekkor tehát az a^g, b^g, c lineárisan független vektorokat a $g^{-1} \in G$ transzformáció V egy 2 dimenziós alterébe képezi. Az $\mathrm{Aut}(V)$ csoport (és így G is) azonban tranzitívan hat a V-beli lineárisan független hármasok halmazán, így tetszőleges lineáris független hármas beleképezhető egy 2 dimenziós altérbe.

2. eset: $n > 3$. Tegyük fel most, hogy teljesül az állítás n-re. Belátjuk, hogy ekkor $n+1$-re is teljesül. Legyen k a legkisebb olyan egész, amire $k \geq 2$ és $n \leq \frac{p^k-1}{k_G} - 1$. Ha $n+1 > \frac{p^k-1}{k_G} - 1$, akkor készen vagyunk, hiszen ekkor a legkisebb olyan k' egész, amire $k' \geq 2$ és $n+1 \leq \frac{p^{k'}-1}{k_G} - 1$ is teljesül, az legalább $k+1$. Tegyük fel most, hogy $n+1 \leq \frac{p^k-1}{k_G} - 1$, azaz $n \leq \frac{p^k-1}{k_G} - 2$. Ekkor azt kell belátnunk, hogy tetszőleges $T \subset V, |T| = n+1$ esetén a T halmaz beleképezhető egy k dimenziós altérbe egy G-beli transzformációval.

Tegyük fel, hogy ez nem teljesül, és legyen ekkor T olyan ellenpélda, amire $\dim\langle T\rangle$ maximális.

2/a eset: $\dim\langle T\rangle \le n$. Ekkor van olyan $v \in T$, hogy $\langle T\setminus\{v\}\rangle = \langle T\rangle$. Az indukciós feltétel szerint van olyan $g \in G$, hogy $\big(T\setminus\{v\}\big)^g$-t tartalmazza V egy k dimenziós altere. Ekkor azonban v nem lehet benne ebben az altérben, így $v^g \notin \Big\langle \big(T\setminus\{v\}\big)^g \Big\rangle$, amiből a 3.4. lemma szerint $\Big|G_{(T\setminus\{v\})^g}(v^g)\Big| = \infty$, és így $\Big|G_{T\setminus\{v\}}(v)\Big| = \infty$ is teljesül. Ebből következik szintén a 3.4. lemma szerint, hogy van olyan $h \in G$, ami stabilizálja a $T\setminus\{v\}$ halmazt, de $v^h \notin \langle T\setminus\{v\}\rangle$. Ez azt jelenti, hogy $\dim\langle T^h\rangle = \dim\langle T, v^h\rangle > \dim\langle T\rangle$. Mivel $\dim\langle T\rangle$ maximális, ezért létezik olyan $h' \in G$ transzformáció, ami a T^h halmazt egy k dimenziós altérbe viszi. Ekkor azonban a $hh' \in G$ transzformáció egy legfeljebb k dimeziós altérbe viszi T-t, ami ellentmondás.

2/b eset: $\dim\langle T\rangle = n+1$. Legyen most $S := T\setminus\{v\}$ valamilyen $v \in T$-re. Ekkor $|S| = n$, és S lineárisan független rendszer. A feltétel szerint $v \notin A_k^G(S)$, így $A_k^G(S) \neq V$. A 3.6. lemma szerint ekkor $A_k^G(S) \le p^k$. Ha $u \in A_k^G(S)$, akkor az $A_k^G(S)$ halmaz definíciója szerint $G_S(u) \subset A_k^G(S)$, speciálisan $G_S(u)$ véges. Ekkor a 3.4. lemma szerint $u \in \langle S\rangle$. Tehát $A_k^G(S) \subset \langle S\rangle$. Három alesetet különböztetünk meg.

2/b/1 aleset: $\lambda a_i \in A_k^G(S)$ *valamilyen* $\lambda \notin \Gamma_{k_G}\cup\{0\}$ *és* $i = 1, 2, \dots, n$ *esetén.* Legyen

$$S_j := S\cup\{\lambda a_i\}\setminus\{a_j\}$$

minden $j \neq i$ esetén. Ekkor minden $j \neq i$-re $a_j \notin \langle S_j\rangle$, így a 3.4. lemma szerint $\big|G_{S_j}(a_j)\big| = \infty$. Mivel $\lambda \notin \Gamma_{k_G}\cup\{0\}$, ezért $0 \neq \lambda a_i \nsim a_i$, azaz létezik olyan $g \in G$ transzformáció, amire a_i^g és $(\lambda a_i)^g$ lineárisan függetlenek. Válasszuk meg ezt a g transzformációt úgy, hogy $\dim\Big\langle \big(S\cup\{\lambda a_i\}\big)^g\Big\rangle$ maximális legyen. Azt állítjuk, hogy ekkor $\dim\Big\langle \big(S\cup\{\lambda a_i\}\big)^g\Big\rangle = n+1$, azaz az $\big(S\cup\{\lambda a_i\}\big)^g$ halmaz elemei lineárisan függetlenek. Tegyük fel ugyanis, hogy $\dim\Big\langle \big(S\cup\{\lambda a_i\}\big)^g\Big\rangle \le n$. Ekkor mivel a_i^g és $(\lambda a_i)^g$ lineárisan függetlenek, ezért létezik olyan $j \neq i$, hogy $\langle S_j^g\rangle = \big\langle S_j\cup\{a_j\}\big\rangle = \Big\langle \big(S\cup\{\lambda a_i\}\big)^g\Big\rangle$. Ebből következik, hogy $G_{S_j}(a_j) = \infty$, és így $\big|G_{S_j^g}(a_j^g)\big| = \infty$. Ezért a 3.4. lemma szerint van olyan $h \in G$, hogy $\big(S_j^g\big)^h = S_j^g$, de $a_j^h \notin \langle S_j^g\rangle$. Ebből

$$\dim\Big\langle \big(S\cup\{\lambda a_i\}\big)^{gh}\Big\rangle = \dim\Big\langle \big(S\cup\{\lambda a_i\}\big)^g\Big\rangle + 1,$$

ami ellentmond $\dim\Big\langle \big(S\cup\{\lambda a_i\}\big)^g\Big\rangle$ maximalitásának. Tehát $\big(S\cup\{\lambda a_i\}\big)^g$ elemei lineárisan függetlenek. Megint a 3.4. lemmát használva adódik, hogy $\Big|G_{S^g}\big((\lambda a_i)^g\big)\Big| = \infty$, így $\big|G_S(\lambda a_i)\big| = \infty$. Ez azonban lehetetlen, hiszen $\lambda a_i \in A_k^G(S)$, így $G_S(\lambda a_i) \subset A_k^G(S)$, ami véges.

2/b/2 aleset: $v = \sum_{i=1}^n \lambda_i a_i \in A_k^G$ *valamilyen* λ_i*-kre, ahol a* λ_i *együtthatók közül legalább* 2 *nem* 0*, és nem mindegyik* -1. Ebben az esetben a 3.11. lemma szerint léteznek olyan $b_1, \dots, b_n, w \in A_k(S)$ elemek, amelyekre $b_1, \dots, b_n$ lineárisan függetlenek, $w \notin \langle b_1+b_2+\ldots+b_n\rangle$, és $w \notin \langle b_i, b_j\rangle$ semmilyen i, j-re. A 3.8. következményt

az $a_1, a_2, \ldots, a_n$ és $b_1, b_2, \ldots, b_n$ lineáris független rendszerekre alkalmazva adódik, hogy létezik olyan $w \in A_k(S)$ is, amire $w \notin \langle b_1 + b_2 + \ldots + b_n \rangle$ és $w \notin \langle b_i, b_j \rangle$. Rögzítsünk most egy ilyen tulajdonságú w-t. Ekkor $w = \sum_{i=1}^{n} \lambda_i a_i$ alakú, ahol a λ_i együtthatók közül legalább 3 nem 0, és nem mindegyik egyforma. Legyen tehát $1 \leq i < j \leq n$ olyan indexek, amire $\lambda_i \neq \lambda_j$. Legyen $\lambda := \lambda_i - \lambda_j \neq 0$. Legyen továbbá $a'_j = a_i, a'_i = a_j$ és $a'_l = a_l$ minden $i, j \neq l$ index esetén. Ekkor a 3.8. következményt az $a_1, a_2, \ldots, a_n$ és $a'_1, a'_2, \ldots, a'_n$ vektorrendszerekre alkalmazva azt kapjuk, hogy

$$A_k^G(S) \ni w' := \sum_{i=1}^{n} \lambda_i a'_i = \sum_{i=1}^{n} \lambda_i a_i + \lambda(a_j - a_i) = w + \lambda(a_j - a_i).$$

A feltevésünk szerint $w \notin \langle a_i, a_j \rangle$, így $w, a_i, a_j \in A_k^G(S)$ lineárisan függetlenek. Ekkor persze $w' = w + \lambda(a_j - a_i), a_i$ és a_j is lineárisan függetlenek. Alkalmazzuk most a 3.8. következményt a w, a_i, a_j és w', a_i, a_j vektorrendszerekre. Mivel $w + \lambda a_i + \lambda a_j = w' \in A_k^G(S)$, ezért ekkor

$$A_k^G(S) \ni w'' := w' + \lambda a_i + \lambda a_j = w + 2\lambda(a_i + a_j).$$

Ezt az eljárást folytatva adódik, hogy $w + s\lambda(a_j - a_i) \in A_k^G(S)$ minden $s \in \mathbb{F}_p$ esetén. Mivel $\lambda \neq 0$, ezért ezt azt jelenti, hogy

$$L := \{w + \mu(a_j - a_i) : \mu \in \mathbb{F}_p\} \subset A_k^G(S).$$

Mivel azonban w, a_1, a_2 lineárisan függetlenek, így L egy 0-n nem átmenő affin egyenes, így a 3.10. lemma szerint $\left|A_k(S)\right| \geq p^{n-1} + 1$. Azonban már láttuk, hogy $\left|A_k(S)\right| \leq p^k$, így $p^{n-1} < p^{n-1} + 1 \leq p^k$, azaz $n - 1 < k$. A k szám a definíciója alapján a legkisebb olyan pozitív egész, amire $k \geq 2$ és $n \leq \frac{p^k - 1}{k_G} - 1$ teljesülnek. Ez azt jelenti, hogy a $k' = n - 1$ választás „túl kicsi", azaz ekkor a $k' \geq 2$ és az $n \leq \frac{p^{k'} - 1}{k_G} - 1$ egyenlőtlenségek valamelyike nem teljesül. Mivel $n \geq 3$, így a $k' = n - 1 \geq 2$ egyenlőtlenség teljesül. Tehát

$$n > \frac{p^{k'} - 1}{k_G} - 1 = \frac{p^{n-1} - 1}{k_G} - 1 \geq$$

$$\geq \frac{p^{n-1} - 1}{p - 1} - 1 = \left(1 + p + p^2 + \ldots + p^{n-2}\right) - 1 \geq$$

$$\geq p + p^2(1 + p + \ldots + p^{n-4}) \geq 3 + (n - 3) = n,$$

hiszen $p \geq 3$, ami ellentmondás.

2/b/3 aleset: Minden $A_k^G(S)$-beli elem vagy $v = \lambda a_i$ alakú valamilyen $\lambda \in \Gamma_{k_G}$ és $1 \leq i \leq n$-re, vagy $v' = \lambda(a_1 + a_2 + \ldots + a_n)$ alakú, ahol $\lambda \in \{0, -1\}$. Ez a feltétel pontosan azt jelenti, hogy az $A_k^G(S)$ halmazt tartalmazza a

$$H := \{\lambda a_i : 1 \leq i \leq n,\ \lambda \in \Gamma_{k_G}\} \cup \{0, -a_1 - a_2 - \ldots - a_n\}$$

halmaz. Mivel $|\Gamma_{k_G}| = k_G$, ezért a H halmaz számossága $nk_G + 2$. Ekkor az $n \leq \frac{p^k-1}{k_G} + 2$ egyenlőtlenséget használva

$$\left|A_k^G(S)\right| \leq |H| = nk_G + 2 \leq p^k - 1 - 2k_G + 2 \leq p^k - 1 < p^k$$

adódik, ami ellentmondás, hiszen feltettük, hogy $A_k^G(S) = p^k$.

Tehát minden esetben ellentmondáshoz vezetett a feltevésünk, így valóban tetszőleges $T \subset V$, $|T| = n + 1$ halmaz beleképezhető egy k dimenziós altérbe egy G-beli transzformációval, és ezt kellett bizonyítanunk. ■

3.13. következmény. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}\,(V)_0$ *egy csoport, amire* $k_G < p - 1$*; vagy* $k_G = p - 1$ *és* G *hatása a* $P := (V \setminus 0)/\sim_G$ *projektív téren* nem *a projektív lineáris transzformációk csoportja. Legyen továbbá* $k \geq 2$ *tetszőleges egész. Ekkor tetszőleges* $S \subset V$, $|S| = \frac{p^k-1}{k_G} - 1$ *halmaz beleképezető* V *egy* k *dimenziós alterébe egy* G*-beli elemmel.*

Bizonyítás. Alkalmazzuk a 3.12. állítást $n := \frac{p^k-1}{k_G} - 1$ esetén. ■

3.14. állítás. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}\,(V)_0$ *egy csoport, amire* $k_G < p - 1$*; vagy* $k_G = p - 1$ *és* G *hatása a* $P := (V \setminus 0)/\sim_G$ *projektív téren* nem *a projektív lineáris transzformációk csoportja. Ekkor tetszőleges* $k \geq 2$ *pozitív egészre a* G *csoport* $\frac{p^k-1}{k_G} - 1$*-szeresen tranzitívan hat a* $\sim_G$*-ekvivalenciaosztályok halmazán.*

Bizonyítás. Legyen $k \geq 2$ és $n := \frac{p^k-1}{k_G} - 1$. Mivel $\mathrm{Aut}(V)$ (és így G is) tranzitívan hat a lineárisan független n-esek halmazán, ezért az állításhoz elég belátni, hogy tetszőleges n (különböző) ekvivalenciaosztály átvihető n független vektorhoz tartozó ekvivalenciaosztályba egy G-beli transzformációval. Ehhez elég belátni, hogy tetszőleges $a_1, \ldots, a_n$ páronként inekvivalens elemek átvihetők n lineárisan független elembe egy G-beli transzformációval.

Legyenek tehát $a_1, \ldots, a_n \in V \setminus 0$ páronként inekvivalens elemek, és $b_1, \ldots, b_n \in V \setminus 0$ lineárisan független elemek. A 3.13. következmény szerint ekkor léteznek olyan $g, h \in G$ transzformációk, amire az $\{a_1^g, \ldots, a_n^g\}$ és a $\{b_1^h, \ldots, b_n^h\}$ halmazt is tartalmazza V egy k dimenziós altere. Mivel $\mathrm{Aut}(V)$ (és így G is) tranzitívan hat V k dimenziós alterein, azért feltehető, hogy az előbbi két k dimenziós altér megegyezik. Jelöljük ezt az alteret U-val. Minden egydimenziós altér pontosan $\frac{p-1}{k_G}$ darab $\sim_G$-ekvivalenciaosztály és a $\{0\}$ uniója, így V minden k dimenziós altere $\frac{p^k-1}{p-1} \cdot \frac{p-1}{k_G} = \frac{p^k-1}{k_G}$ darab $\sim_G$-ekvivalenciaosztály és a $\{0\}$ uniója. A $\sim_G$ reláció definíciójából adódik, hogy az $\{a_1^g, \ldots, a_n^g\}$ és a $\{b_1^h, \ldots, b_n^h\}$ halmaz elemei páronként inekvivalensek. Ez azonban azt jelenti, hogy léteznek olyan $u, v \in U \setminus 0$ vektorok, hogy $\{a_1^g, \ldots, a_n^g, u\}$ és a $\{b_1^h, \ldots, b_n^h, v\}$ halmazok is az $U \setminus 0$ halmazbeli ekvivalenciaosztályok egy teljes reprezentációs rendszerét adják. Legyen most $\gamma \in \mathrm{Aut}(V) \subset G$ egy olyan lineáris transzformáció, ami fixálja az U alteret, mint halmazt, és az $u^\gamma = v$. Ekkor azonban az $a_1^{g\gamma}, \ldots, a_n^{g\gamma}$ vektorokhoz tartozó ekvivalenciaosztályok halmaza megegyezik a $b_1^h, \ldots, b_n^h$ vektorokhoz tartozó ekvivalenciaosztályok halmazával. Ez azt jelenti, hogy létezik az $1, 2, \ldots, n$ indexeknek egy olyan $\pi \in S_n$ permutációja, amire $a_i^{g\gamma} \sim_G b_{\pi(i)}^h$ minden $1 \leq i \leq n$-re. Ekkor

azonban $a_i^{g\gamma h^{-1}} \sim_G b_{\pi(i)}$. Speciálisan, léteznek olyan $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_p^\times$ számok, hogy $a_i^{g\gamma h^{-1}} = \lambda_i b_{\pi(i)}$ minden $1 \leq i \leq n$-re. A jobb oldalon álló vektorok azonban lineárisan függetlenek, hiszen a feltétel szerint $b_1, \ldots, b_n$ lineárisan függetlenek. Tehát a $g\gamma h^{-1} \in G$ transzformáció bizonyítja az állítást. ■

A fejezet főtételének bizonyításához szükségünk lesz még az alábbi lemmára.

3.15. lemma. *Tegyük fel, hogy $G \subset \mathrm{Sym}(H)$ egy zárt csoport, ahol $|H| = \omega$, és legyen $\sim$ egy ekvivalenciareláció H-n, amire minden $\sim$-ekvivalenciaosztály véges. Tegyük fel továbbá, hogy G kompatibilis a $\sim$ ekvivalenciarelációval, azaz $x \sim y$ pontosan akkor teljesül, ha $x^g \sim y^g$. Ekkor G hatása a $\sim$-ekvivalenciaosztályok halmazán is zárt.*

Bizonyítás. Legyen $g \in \mathrm{Sym}(H/\sim)$ tetszőleges, amire teljesül, hogy tetszőleges $F \subset H/\sim$ véges halmaz esetén van olyan $\tilde{h} \in G$, amire $\tilde{h}$ és g hatása megegyezik F-en. Be kell látnunk, hogy ekkor létezik olyan a $\tilde{g} \in G$ transzformáció is, amire $\tilde{g}$ és g hatása megegyezik az összes $\sim$-ekvivalenciaosztályok halmazán.

Egy $F \subset H/\sim$ esetén jelölje $\tilde{F}$ az F-beli ekvivalenciaosztályok unióját. Ekkor ha F véges, akkor $\tilde{F}$ is. Legyen $X_1, X_2, \ldots$ a $\sim_G$ ekvivalenciaosztályok egy felsorolása. Legyen $F_i := \{X_1, X_2, \ldots, X_n\}$. Ekkor az F_i halmazok végesek, $\emptyset = F_0 \subset F_1 \subset F_2 \subset F_3 \subset \ldots$, és $\bigcup_{i=0}^{\infty} F_i = H/\sim$. Mivel g bijekció, ezért $\bigcup_{i=0}^{\infty} F_i^g = H/\sim$ is teljesül. Ezekből következik az is, hogy

$$\bigcup_{i=1}^{\infty} X_i = \bigcup_{i=1}^{\infty} X_i^g = H.$$

Definiáljuk a T gyökeres fát a következőképpen. Jelölje T_n a T gyökeres fa n-edik szintjét. Ekkor minden n-re a T_n-en lévő csúcsok legyenek az olyan f függvények, amikre $D(f) = \tilde{F_n}$, és létezik olyan $\tilde{h} \in G$ függvény, amire $\tilde{h}|_{\tilde{F_i}} = h$, továbbá $\tilde{h}$ és g hatása megegyezik a $H/\sim$ halmazon. A T gráfban az $f_1 \in T_{n-1}$ és $f_2 \in T_n$ csúcsok között vezessen él, ha $f_2|_{\tilde{F_n}} = f_1$. Ekkor az egyetlen T_0-beli csúcs az üres függvény, jelöljük ezt most f_0-lal. Ez lesz a T gyökeres fa gyökere. A definícióból könnyen látható, hogy ebben a gráfban ha $f \in V(T_n)$, akkor f_0-ból pontosan egy út vezet f-be, nevezetesen

$$\big(f_0 = f|_{\tilde{F}_0}, f|_{\tilde{F}_1}, \ldots, f|_{\tilde{F}_{n-1}}, f\big).$$

A T gráf tehát valóban fa. Azt állítjuk, hogy létezik az f_0 csúcsból induló végtelen út T-ben. Ehhez a König-lemma feltételeit fogjuk ellenőrizni.

(1) *Létezik akármilyen hosszú f_0-ból induló út.* Ehhez elég belátni, hogy T_n nem üres minden n-re. Legyen tehát n tetszőleges, és legyen ekkor $\tilde{h}$ egy olyan függvény, amire $\tilde{h}$ és g hatása megegyezik F_n-en. A feltételeink szerint létezik ilyen $\tilde{h}$. Legyen most $\tilde{h}|_{\tilde{F_n}} = f$. Ekkor T_n definíciója szerint $f \in V(T_n)$.

(2) *Minden T-beli csúcs kifoka véges.* Ennél többet fogunk bizonyítani, belátjuk ugyanis, hogy T_n véges minden n-re. Tegyük fel, hogy $f \in T_n$. Ekkor $D(f) = \tilde{F_n} = \bigcup_{i=1}^{n} X_i$, és a feltétel szerint

$$R(f) \subset \bigcup_{i=1}^{n} X_i^f = \bigcup_{i=1}^{n} X_i^g.$$

Az $\bigcup_{i=1}^{n} X_i \to \bigcup_{i=1}^{n} X_i^g$ függvények száma azonban véges, hiszen az $X_1, \ldots, X_n, X_1^g, \ldots, X_n^g$ ekvivalenciaosztályok végesek, és ekkor az $\bigcup_{i=1}^{n} X_i$ és $\bigcup_{i=1}^{n} X_i$ halmazok is végesek.

Tehát a T gyökeres fára (ahol f_0 a gyökér) valóban teljesülnek a König-lemma feltételei. Ekkor a König-lemma szerint létezik az f_0 csúcsból induló végtelen út T-ben. Legyen ez $(f_0, f_1, \ldots)$. Ekkor $f_n \in T_n$, így $D(f_n) = \tilde{F}_n$, és $j > i$ esetén $f_j|_{\tilde{F}_i} = f_i$. Ebből következik, hogy $\bigcup_{i=0}^{\infty} f_i$ is függvény. Legyen ez f. Ekkor

$$D(f) = \bigcup_{i=0}^{\infty} D(f_i) = \bigcup_{i=0}^{\infty} D(f_i) = \bigcup_{i=0}^{\infty} X_i = H,$$

$$R(f) = \bigcup_{i=0}^{\infty} R(f_i) = \bigcup_{i=0}^{\infty} R(f_i) = \bigcup_{i=0}^{\infty} X_i^g = H.$$

Tegyük fel most, hogy $u \neq v \in H$. Ekkor van olyan n, hogy $u, v \in D(f_n) = \tilde{F}_n$. Legyen most $\tilde{h} \in G$ egy olyan függvény, amire $\tilde{h}|_{\tilde{F}_n} = f_n$. Ekkor mivel $\tilde{h}$ bijekció, ezért $u^{\tilde{h}} \neq v^{\tilde{h}}$, amiből $u^{f_n} \neq v^{f_n}$, és így $u^f \neq v^f$. Az f függvény tehát egy $H \to H$ bijekció.

Belátjuk most, hogy $f \in G$. Ehhez G zártsága miatt elég belátni, hogy H tetszőleges F véges részhalmazához létezik olyan $\tilde{h} \in G$ függvény, amire $\tilde{h}|_{\tilde{F}_n} = f_n = f|_{\tilde{F}_n}$. Legyen tehát F egy tetszőleges véges részhalmaza H-nak. Ekkor van olyan n, hogy $F \subset D(f_n) = \tilde{F}_n$, és ekkor az f_n függvény definíciója miatt létezik $\tilde{h} \in G$ függvény, amire $\tilde{h}|_{\tilde{F}_n} = f_n = f|_{\tilde{F}_n}$.

Azt állítjuk most, hogy a $\tilde{g} = f$ választás jó lesz, azaz f és g hatása megegyezik a $H/\sim$ halmazon. Legyen ugyanis $X_i \in H/\sim$ tetszőleges. Ekkor $j \geq i$ esetén az f_j függvények definíciója miatt $X_i^{f_j} = X_i^g$, és így $X_i^f = X_i^g$. ■

3.16. tétel. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy zárt csoport. Ekkor az alábbiak valamelyike teljesül:*

(1) $k_G = p - 1$, *és* G *a* $P := (V \setminus 0)/\sim_G$ *projektív téren a projektív lineáris transzformációk csoportjaként hat,*

(2) G *teljes szimmetrikus csoportként hat a* $\sim_G$*-ekvivalenciaosztályok halmazán.*

Bizonyítás. Tegyük fel, hogy a G csoportra nem teljesül az (1) feltétel. Be kell látni, hogy ekkor G szimmetrikus csoportként hat a $\sim_G$-ekvivalenciaosztályok halmazán.

Ha G-re nem teljesül az (1) feltétel, akkor a 3.7. állítás szerint a G csoport $\frac{p^k-1}{k_G} - 1$-szeresen tranzitív a $\sim_G$-ekvivalenciaosztályok halmazán minden $k \geq 2$-re. Mivel $\frac{p^k-1}{k_G} - 1$ érték tetszőleges nagy lehet, ezért ebből következik az is, hogy G minden n-re n-tranzitívan hat a $\sim_G$-ekvivalenciaosztályok halmazán, tehát G hatása sűrű a $\sim_G$-ekvivalenciaosztályok halmazán.

Be kell még látnunk, hogy ez a hatás zárt is. Ez a 3.15. lemma szerint teljesül, hiszen G kompatiblis a $\sim_G$ relációval, és minden $\sim_G$ ekvivalenciaosztály véges. ■

A későbbiekben még szükségünk lesz a 3.16. tétel állítására a $k_G = 1$ esetben, ezért ezt külön is kimondjuk.

3.17. következmény. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy zárt csoport, amire* $k_G = 1$. *Ekkor* $G = \mathrm{Sym}_0(V)$.

Bizonyítás. Mivel $p \geq 3$, ezért $k_G = 1 \neq p-1$, tehát ekkor a G csoportra 3.16. tételbeli (2) feltétel teljesül. $k_G = 1$ esetén definíció szerint a $\sim_G$ ekvivalenciaosztályok egyeleműek, tehát ekkor G a szimmetrikus csoportként hat $V \setminus 0$-n, azaz $G = \mathrm{Sym}_0(V)$. ■

3.1. Azon zárt csoportok leírása, amik a teljes szimmetrikus csoportként hatnak a $\sim_G$-ekvivalenciaosztályok halmazán.

Ebben a fejezetben megadjuk a klasszifikációját azon $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ zárt csoportoknak, amikre a 3.16. tétel (2) feltétele teljesül, azaz amikre G hatása a $\sim_G$-ekvivalenciaosztályok halmazán a teljes szimmetrikus csoport. Ezen csoportok leírásához szükségünk lesz a következő definíciókra.

3.18. definíció. Legyen $k \mid p-1$ tetszőleges. Ekkor egy $f : V \setminus 0 \to \Gamma_k$ függvényt *k-címkézés*nek hívunk, ha tetszőleges $u \in V \setminus 0$ és $\lambda \in \Gamma_k$ esetén $f(\lambda u) = \lambda f(u)$.

A definícióból könnyen látható, hogy a $V \setminus 0$ halmaz k-címkézései természetes módon megfeleltethetőek a $\sim_k$-ekvivalenciaosztályok egy reprezentánsrendszerével. Ebből speciálisan az is következik, hogy minden $k \mid p-1$-re van címkézése $V \setminus 0$-nak. A megfeleltetés a következő: ha adott egy f címkézés, akkor az 1 elem f szerinti ősképe egy reprezentánsrendszer. Megfordítva: ha adott egy X reprezentánsrendszere a $\sim_k$-ekvivalenciaosztályoknak, akkor minden $v \in V \setminus 0$ esetén legyen $f(v)$ értéke az az egyetlen λ, amire $v = \lambda v'$ alakú valamilyen $v' \in X$ esetén. A továbbiakban a $\{v \in V \setminus 0 : f(v) = 1\}$ halmazt jelöljük V^f-fel.

3.19. definíció. Legyen $k \mid p-1$ tetszőleges, és f egy k-címkézés $V \setminus 0$-n. Ekkor egy $g \in \mathrm{Sym}(V)_0$ permutációról azt mondjuk, hogy az f k-címkézéssel *kompatibilis*, ha g megőrzi a $\sim_k$ relációt, és $f(v^g) = f(v)$ minden $v \in V \setminus 0$-ra.

3.20. definíció. Legyen $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ egy csoport, legyen továbbá f egy tetszőleges k_G-címkézés $V \setminus 0$-n. Jelölje ekkor G_f azon $g \in G$ elemek részcsoportját, amik kompatibilisek f-fel.

3.21. definíció. Legyen $k \mid p-1$ tetszőleges, és f egy k-címkézés $V \setminus 0$-n. Ekkor egy $g \in \mathrm{Sym}\big((V \setminus 0)/\sim_k\big)$ elem esetén jelölje g^f azt az egyértelmű $\tilde{g} \in \mathrm{Sym}(V)_0$ elemet, amire $\tilde{g}$ kompatibilis az f k-címkézéssel, és g és $\tilde{g}$ hatása megegyezik a $\sim_k$-ekvivalenciaosztályok halmazán.

Egy $H \leq \mathrm{Sym}\big((V \setminus 0)/\sim_k\big)$ részcsoport esetén legyen $H^f = \{g^f : g \in H\}$.

A 3.22–3.26. lemmákban a címkézések segítségével leírjuk azon $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ zárt csoportok szerkezetét, amik a szimmetrikus csoportként hatnak a $\sim_{k_G}$-ekvivalenciaosztályok halmazán. Kiderül, hogy minden ilyen G előáll $G^* \cdot \left(\mathrm{Sym}\left((V \setminus 0)/\sim_{k_G}\right)^f\right)$ alakban, ahol a G^* azon G-beli elemek csoportja, amik minden $\sim_G$-ekvivalenciaosztályt (halmazként) stabilizálnak.

Ezután a 3.27–3.34. lemmákban leírjuk azon csoportokat, amik előállnak az előbbi G^* csoportként, és ezzel megkapjuk a teljes klasszifikációt is. Kiderül végül, hogy azon $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ zárt csoportok, amik a szimmetrikus csoportként hatnak a $\sim_k$-ekvivalenciaosztályok halmazán bijekcióban állnak a k fokú szimmetrikus csoport bizonyos tulajonságú (N, H) részcsoportpárjaival. Ez a bijekció nem fog függeni attól, hogy melyik címkézést használjuk, azonban a definíciójukban, és a későbbi bizonyításokban végig használni kell valamilyen k-címkézést.

Első lépésként bebizonyítjuk, hogy ha $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ egy zárt csoport, ami a szimmetrikus csoportként hat a $\sim_{k_G}$-ekvivalenciaosztályok halmazán, akkor $G_f = \left(\mathrm{Sym}\left((V \setminus 0)/\sim_{k_G}\right)^f\right)$.

3.22. lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy zárt csoport, és* f *egy* k_G *címkézés. Ekkor* G_f *is zárt.*

Bizonyítás. A definícióból látható, hogy $G_f = G \cap \left(\mathrm{Sym}\left((V \setminus 0)/\sim_{k_G}\right)^f\right)$, így elég belátni, hogy $\left(\mathrm{Sym}\left((V \setminus 0)/\sim_{k_G}\right)^f\right)$ zárt. Tegyük fel tehát, hogy $g \in \mathrm{Sym}(V)$, és minden $F \subset V$ véges halmazra van olyan $h \in \left(\mathrm{Sym}\left((V \setminus 0)/\sim_{k_G}\right)^f\right)$, hogy $g|_F = h|_F$. Be kell látnunk, hogy ekkor g is kompatibilis f-fel. Tegyük fel tehát, hogy $u \in V \setminus 0$. Legyen ekkor $F = \{u\}$. Erre alkalmazva az előbbi észrevételt $f(u) = f(u^h) = f(u^g)$. Mivel ez minden $u \in V \setminus 0$-ra teljesül, ezért g kompatibilis f-fel. ■

3.23. lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy zárt csoport, ami a szimmetrikus csoportként hat a* $\sim_{k_G}$*-ekvivalenciaosztályok halmazán, és* f *egy* k_G*-címkézés. Tegyük fel továbbá, hogy* G_f *tartalmaz egy olyan* g *elemet, amire a* $\{v \in V \setminus 0 : v \neq v^g\} \cap V^f$ *halmaz véges, nem üres, és elemei lineárisan függetlenek. Ekkor* $G_f = \left(\mathrm{Sym}\left((V \setminus 0)/\sim_{k_G}\right)^f\right)$.

Bizonyítás. Egy f k_G-címkézéssel kompatibilis permutáció hat a $V^f = \{v \in V \setminus 0 : f(v) = 1\}$ halmazon, továbbá egy f-fel kompatibilis g permutációt meghatároz a g permutációnak a $\sim_{k_G}$-ekvivalenciaoszályok halmazán való hatása, amit viszont meghatároz g hatása az V^f halmazon. Ez ezt jelenti, hogy a lemma állításához elég belátni, hogy $G_f|_{V^f} = \mathrm{Sym}(V^f)$. A 3.22. lemma szerint G_f zárt, így $G_f|_{V^f}$ is zárt. Ez azt jelenti, hogy a lemma állításához elég belátni, hogy a lemma feltételei mellett G_f hatása sűrű a V^f halmazon. Ehhez azt fogjuk bizonyítani, hogy G_f hatása a V^f halmazon tartalmaz minden transzpozíciót.

Legyen X egy tetszőleges végtelen, lineáris független elemekből álló halmaz, ami tartalmazza a $\{v \in V \setminus 0 : v \neq v^g\} \cap V^f$ halmazt. Legyen $\mathrm{Sym}^F(X)$ azon $h \in \mathrm{Sym}(X)$ elemek csoportja, amik véges sok kivétellel minden X-beli elemet fixen hagynak, legyen továbbá $\mathrm{Alt}^F(X)$ a páros permutációk csoportja $\mathrm{Sym}^F(X)$-ben.

Legyen $H := \mathrm{Sym}^F(X) \cap \big((G_f)_X\big)\big|_X$, azaz azon $h \in \mathrm{Sym}^F(X)$-ek halmaza, amiket identitásként kiterjesztve $V \setminus X$-re egy G_f-beli elemet kapunk. Azt állítjuk, hogy ekkor a H csoport normálosztó $\mathrm{Sym}^F(V^f)$-ben.

Legyen ugyanis $h \in H$, és $\gamma \in \mathrm{Sym}^F(X)$ tetszőleges. Ekkor γ kiterjed V egy automorfizmusává, jelöljük ezt a kiterjesztést is γ-val. Feltehető, hogy ez a kiterjesztés kompatibilis f-fel. Ekkor tehát $\gamma \in \mathrm{Aut}(V)_f \subset G_f$. Tekintsük ekkor a $\gamma h \gamma^{-1} \in \mathrm{Sym}(X)$ permutációt. Ekkor $\gamma h \gamma^{-1} \in \big((G_f)_X\big)\big|_X$, és ekkor $\gamma h \gamma^{-1} \in \big((G_f)_X\big)\big|_X \cap \mathrm{Sym}^F(X) = H$. Tehát valóban $H \lhd \mathrm{Sym}^F(X)$. Ismert, hogy ekkor $H = 1$ vagy $H \supset \mathrm{Alt}^F(X)$. A lemma feltétele szerint a $\{v \in V \setminus 0 : v \neq v^g\} \cap V^f \subset X$ halmaz nem üres, így $\mathrm{id} \neq g|_X \in H$. Tehát H nem lehet a triviális csoport.

Azt kaptuk tehát, hogy H tartalmazza $\mathrm{Alt}^F(X)$-et. Ekkor persze $\big((G_f)_X\big)\big|_X$ is tartalmazza $\mathrm{Alt}^F(X)$-et. Az $\mathrm{Alt}^F(X)$ alternáló csoport azonban sűrű $\mathrm{Sym}(X)$-ben. Azt állítjuk, hogy $\big((G_f)_X\big)\big|_X$ zárt is. Ehhez elég belátni, hogy $(G_f)_X$ zárt. Ez teljesül, hiszen a $G_f|_{V^f}$ csoportról láttuk, hogy zárt, és $X \subset V^f$. Ebből következik, hogy $\big((G_f)_X\big)\big|_X = \mathrm{Sym}(X)$. Speciálisan $\big((G_f)_X\big)\big|_X$ tartalmaz minden transzpozicíót. Ez azt jelenti, hogy minden $u, v \in X$ elemre $G_f|_{V^f}$ tartalmazza az (uv) transzpozíciót. Ekkor persze $G_f|_{V^f}$ bármely $u, v \in V^f$ lineárisan független elemekre tartalmazza az $u, v \in V^f$ transzpozíciót. Be kell még látnunk, hogy ez akkor is teljesül, ha $u, v \in V^f$ nem lineárisan függetlenek. Ebben az esetben legyen $w \in V^f \setminus \langle u, v\rangle$ egy tetszőleges vektor. Ekkor $(uw), (vw) \in G_f|_{V^f}$, amiből $(uv) = (uw)(vw)(uw) \in G_f|_{V^f}$. A $G_f|_{V^f}$ csoport tehát valóban tartalmaz minden transzpozíciót, és ezt kellett bizonyítanunk. ■

A következő állítás bizonyításához szükségünk lesz az alábbi jelölésre.

3.24. definíció. Legyen $k \mid p-1$, és legyen $g \in \mathrm{Sym}(V)_0$ egy tetszőleges elem, ami megőrzi a $\sim_k$-ekvivalenciarelációt. Legyen továbbá f egy tetszőleges k-címkézés $V \setminus 0$-n. Ekkor egy $v \in V \setminus 0$ esetén jelölje $\sigma_f(g, v)$ a

$$\lambda \mapsto f\big((\lambda \tilde{v})^g\big) : \Gamma_{k_G} \to \Gamma_k$$

leképezést, ahol $\tilde{v}$ jelöli az $\sim_G (v)$ ekvivalenciaosztály egyetlen olyan elemét, amire $f(v) = 1$ (azaz $\tilde{v} = \frac{v}{f(v)}$). Amennyiben ez nem okoz félreértést, a σ leképezésben az f címkézést nem írjuk ki.

A definícióból könnyen látható, hogy a $\sigma(g, v)$ leképezés mindig bijekció, és $v \sim_G v'$ esetén $\sigma(g, v) = \sigma(g, v')$. Ha a $g, h \in \mathrm{Sym}(V)_0$ elemek megőrzik a $\sim_k$ relációt, akkor tetszőleges $v \in V \setminus 0$ esetén $\sigma(gh, v) = \sigma(g, v)\sigma(h, v^g)$.

A következő állításban belátjuk, hogy a 3.23. lemma feltételei valójában automatikusan teljesülnek minden megfelelő G csoportra.

3.25. állítás. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy zárt csoport, ami a szimmetrikus csoportként hat a* $\sim_{k_G}$*-ekvivalenciaosztályok halmazán, és* f *egy* k_G *címkézés. Ekkor* $G_f = \big(\mathrm{Sym}\big((V \setminus 0)/\sim_{k_G}\big)\big)^f$.

Bizonyítás. Ezen állítás bizonyításához a 3.23. lemmát fogjuk használni. Legyenek $a_1, a_2, \ldots, a_p \in V_f$ tetszőleges lineárisan független elemek. A bizonyítás további részében az indexeket mod p értjük. Mivel G a szimmetrikus csoportként hat a $\sim_{k_G}$-ekvivalenciaosztályok halmazán, ezért van olyan $g \in G$, amire

$$\big(\sim_G (a_i)\big)^g = \sim_G (a_{i+1}) \quad \text{és} \quad b^g = b$$

minden $b \in (V \setminus 0)/\sim_{k_G} \setminus \big\{\sim_G (a_1), \sim_G (a_2), \ldots, \sim_G (a_p)\big\}$-re. Legyen $\sigma_i := \sigma(g, a_i)$, és legyen γ_i egy olyan lineáris transzformáció, amire $a_j^{\gamma_i} = a_{j+i}$ minden $j = 1, 2, \ldots, p$-re. Legyen továbbá $g_i := \gamma_i^{-1} a_i \gamma_i$. Ekkor persze az így kapott g_i-kre is teljesül, hogy $\big(\sim_G (a_j)\big)^{g_i} = \sim_G (a_{j+1})$, és $b^{g_i} = b$ minden $b \in (V \setminus 0)/\sim_{k_G} \setminus \big\{\sim_G (a_1), \sim_G (a_2), \ldots, \sim_G (a_p)\big\}$, azaz g_i és g hatása megegyezik $(V \setminus 0)/\sim_G$-n. Azt állítjuk, hogy $\sigma(g_i, a_j) = \sigma_{j-i}$. Valóban mivel γ_i lineáris, ezért tetszőleges $j = 1, 2, \ldots, p$ és $\lambda \in \Gamma_{k_G}$ esetén

$$f\big((\lambda a_j)^{g_i}\big) = f\big(\lambda a_j^{g_i}\big) = f(\lambda a_{j+i}) = \lambda,$$

így $\sigma(\gamma_i, a_j) = \mathrm{id}\,\Gamma_k$, amiből

$$\sigma(g_i, a_j) = \sigma(\gamma_{-i} g \gamma_i, a_j) = \sigma(\gamma_{-i}, a_j)\sigma\big(g\gamma_i, a_j^{\gamma_{-i}}\big) = \sigma\big(g\gamma_i, a_j^{\gamma_{-i}}\big) =$$

$$= \sigma(g\gamma_i, a_{j-i}) = \sigma(g, a_{j-i})\sigma\big(\gamma_i, a_{j-i}^{\gamma_i}\big) = \sigma_{j-i}\sigma(\gamma_i, a_j) = \sigma_{j-i}.$$

Legyen most $g' = g_0 g_1, \ldots, g_{k_G!-1} \in G$. Az így kapott g' hatása a $\sim_{k_G}$ ekvivalenciaosztályok halmazán megegyezik $g^{k!}$ hatásával, és tetszőleges $i = 1, 2, \ldots, p$-re

$$\sigma(g', a_i) = \sigma(g_0, a_i)\sigma\big(g_1, a_i^{g_0}\big)\sigma\big(g_2, a_i^{g_0 g_1}\big) \ldots \sigma\big(g_{k_G!-1}, a_i^{g_0 g_1, \ldots, g_{k_G!-2}}\big) =$$

$$= \sigma(g_0, a_i)\sigma(g_1, a_{i+1}) \ldots \sigma(g_{k_G!-1}, a_{i+k_G!-1}) = \sigma(g, a_i)^{k_G!} = \mathrm{id}\,\Gamma_{k_G},$$

hiszen $\big|\,\mathrm{Sym}(\Gamma_{k_G})\big| = k_G!$

Legyen $g'' = g'^{k_G!-1} \in G$. Azt állítjuk, hogy $g'' \in G_f$, azaz minden $u \in \mathrm{Sym}\,\big((V \setminus 0)/\sim_{k_G}$ esetén $\sigma(g, u) = \mathrm{id}\,\Gamma_{k_G}$. Tegyük fel először, hogy $u = \sim_G (a_i)$ valamilyen i-re. Ekkor

$$\sigma(g'', a_i) = \sigma(g', a_i)\sigma(g', a_i^{g'}) \ldots \sigma\big(g', a_i^{g'^{k_g!-1}}\big) =$$

$$= \sigma(g', a_i)\sigma(g', a_{i+k_G!}) \ldots \sigma\big(g', a_{i+(k_G!-1)k_G!}\big) = \mathrm{id}\,\Gamma_{k_G}.$$

Tegyük fel most, hogy u különbözik minden $\sim_G (a_i)$-től. Ekkor

$$\sigma(g'', u) = \sigma(g', u)\sigma(g', u^{g'}) \ldots \sigma\big(g', u^{g'^{k_g!-1}}\big) =$$

$$= \sigma(g', u)^{k_G!} = \mathrm{id}\,\Gamma_{k_G},$$

hiszen $\big|\,\mathrm{Sym}(\Gamma_{k_G})\big| = k_G!$.

A $g'' \in G_f$ permutáció hatása a $\sim_G$-ekvivalenciaosztályok halmazán megegyezik $g'^{k_G!}$ hatásával, ami pedig megegyezik $g^{(k_G!)^2}$ hatásával. Ebből következik, hogy

$a_i^{g''} \sim_G a_i^{g^{(k_G!)^2}} = a_{i+(k_G!)^2} \nsim_G a_i$, hiszen az $a_1, \dots, a_p$ elemek páronként inekvivalensek, és $k_G < p$ miatt $\left((k_G!)^2, p\right) = 1$, amiből $i \not\equiv i + (k_G!)^2 \bmod p$. Speciálisan $a_i^{g''} \neq a_i$. Ha egy $v \in V \setminus 0$ elem nincs benne a $\sim_G (a_i)$ ekvivalenciaosztályok egyikében sem, akkor $v^{g''} \sim_G v$. Ekkor azonban mivel $g'' \in G_f$, ezért $f(v^{g''}) = f(v)$ is teljesül, ami csak $v^{g''} = v$ esetén lehetséges. Tehát a $g'' \in G_f$ permutációra

$$\{v \in V \setminus 0 : \ v \neq v^g\} \cap V^f = \{a_1, \dots, a_p\}.$$

Ez a halmaz véges és nem üres, így a 3.23. lemma szerint

$$G_f = \left(\mathrm{Sym}\left((V \setminus 0)/\sim_{k_G}\right)\right)^f. \ \blacksquare$$

3.26. következmény. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy zárt csoport, ami a szimmetrikus csoportként hat a* $\sim_{k_G}$*-ekvivalenciaosztályok halmazán, és* f *egy* k_G*-címkézés. Ekkor* $G = G^* \cdot \left(\mathrm{Sym}\left((V \setminus 0)/\sim_{k_G}\right)\right)^f$ *alakú, ahol*

$$G^* = \left\{g \in G : \ g \text{ identitásként hat } (V \setminus 0)/\sim_{k_G} \text{-n}\right\}.$$

Bizonyítás. A „$\supset$” tartalmazás következik a 3.25. állításból. Tegyük fel most, hogy $g \in G$. Ekkor a 3.25. állítás szerint van olyan $g' \in G_f$, hogy g és g' hatása megegyezik a $\sim_G$-ekvivalenciaosztályok halmazán. Ekkor $g^* := gg'^{-1} \in G^*$, és $g = g^*g'$. ■

A 3.26. következményből következik az is, hogy a G^* csoport már meghatározza G-t, így elég a lehetséges G^* csoportokat klasszifikálni. A bizonyításból az is könnyen látható, hogy a $G = G^* \cdot \left(\mathrm{Sym}\left((V \setminus 0)/\sim_{k_G}\right)\right)^f$ szorzat valójában egy $G = G^* \rtimes \left(\mathrm{Sym}\left((V \setminus 0)/\sim_{k_G}\right)\right)^f$ szemidirekt szorzat.

Egy $k \mid p-1$ szám esetén jelöljük $\mathrm{Sym}_0^{(k)}(V)$-vel azon permutációk csoportját, amik megőrzik a $\sim_k$ relációt. Ekkor persze $\mathrm{Aut}(V) \leq \mathrm{Sym}_0^{(k)}(V)$ minden $k \mid p-1$-re, és egy $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ csoportra pontosan akkor teljesül $k_G = k$, ha $G \leq \mathrm{Sym}_0^{(k)}(V)$, de $G \not\leq \mathrm{Sym}_0^{(k')}(V)$ minden $k' < k$-ra. Legyen

$$\mathcal{S}^{(k)} = \left(\mathrm{Sym}_0^{(k)}(V)\right)^*,$$

azaz azon permutációk halmaza, amik minden $\sim_k$ ekvivalenciaosztályt önmagukra képeznek. Ekkor egy $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ csoportra $G^* = G \cap \mathcal{S}^{(k_G)}$.

Ha a g, h elemek az $\mathcal{S}^{(k)}$ részcsoportban vannak, akkor tetszőleges $v \in V \setminus 0$-ra $\sigma(gh, v) = \sigma(g, v)\sigma(h, v)$. Ezt azt jelenti, hogy a

$$\mathcal{S}^{(k)} \to \mathrm{Sym}(\Gamma), g \mapsto \sigma(g, u)$$

leképezés egy homomorfizmus minden $u \in V \setminus 0$ esetén. Azt állítjuk, hogy egy $g \in \mathcal{S}^{(k)}$ csoportbeli elemet meghatároznak a $\sigma(g, u)$ homomorfizmusnál vett képei. Valóban ha a $\sigma(\cdot, u)$ homomorfizmusok adottak, akkor egy $u \in V \setminus 0$ esetén $u^g = f(u)^{\sigma(g,u)} \frac{u}{f(u)}$. Ez azt jelenti, hogy az előbbi G^* csoport meghatározásához elég meghatározni, hogy egy G^*-beli elemnek mik lehetnek a képei a $\sigma(\cdot, u) : \ u \in V \setminus 0$ homomorfizmusoknál.

3.27. definíció. Legyen $G \leq \mathrm{Sym}_0^{(k)}(V)$ egy csoport és f egy k-címkézés. Ekkor egy $v \in V \setminus 0$ elemre legyen

$$H_v(G) := \{\sigma(g, v) : g \in G^*\}$$

és

$$N_v(G) := \{\sigma(g, v) : g \in G^*, \sigma(g, u) = \mathrm{id}\,\Gamma_k \text{ minden } u \nsim_k v\text{-re}\}.$$

A definícióból látható, hogy $N_v(G)$ és $H_v(G)$ részcsoportjai $\mathrm{Sym}(\Gamma_k)$-nak, és $N_v(G) \subset H_v(G)$.

3.28. lemma. *Legyen $G \leq \mathrm{Sym}_0^{(k)}(V)$ egy csoport és f egy k-címkézés. Ekkor ha G tartalmazza $\mathrm{Aut}(V)$-t, akkor az $N_v(G)$ és $H_v(G)$ csoportok nem függnek a v vektor választásától.*

Bizonyítás. Tegyük fel, hogy $\mathrm{Aut}(V) \leq G$. Az állítást nyilván elég belátni V^f-beli vektorokra. Tegyük fel tehát, hogy $u, v \in V^f$, és legyen $\gamma \in \mathrm{Aut}(V) \leq G$ egy lineáris transzformáció, amire $u^\gamma = v$.

Tegyük fel most, hogy egy σ permutáció benne van $H_u(G)$-ben. Ekkor van olyan $g \in G^*$, hogy $\sigma(g, u) = \sigma$. Ez esetben a $\gamma^{-1} \in G^*$ permutációra $\sigma(\gamma^{-1}g\gamma, v) = \sigma$. Tehát $H_u(G) \subset H_v(\mathrm{g})$. Hasonlóan $H_v(G) \subset H_u(G)$ is teljesül, így $H_u(G) = H_v(G)$.

Tegyük fel, hogy $\sigma \in N_u(G)$. Ekkor van olyan $g \in G^*$, hogy $\sigma(g, u) = \sigma$ és $\sigma(g, u') = \mathrm{id}\,\Gamma$ minden $u' \nsim_k u$ esetén. Ez esetben a $\gamma^{-1} \in G^*$ permutációra $\sigma(\gamma^{-1}g\gamma, v) = \sigma$ és $\sigma(\gamma^{-1}g\gamma, v') = \mathrm{id}\,\Gamma$ minden $v' \nsim_k v$ esetén, így $N_u(G) \subset N_v(G)$. Hasonlóan $N_v(G) \subset N_u(G)$. Tehát $N_u(G) = N_v(G)$. ■

3.29. lemma. *Legyen $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}_0^{(k)}(V)$ egy csoport és f egy k-címkézés. Ekkor $N(G) \triangleleft H(G)$.*

Bizonyítás. Legyenek $\sigma \in N(G), \sigma' \in H(G)$ tetszőlegesek, legyen továbbá $u \in V \setminus 0$ tetszőleges. Be kell látnunk, hogy $\sigma'^{-1}\sigma\sigma' \in N(G)$. A felírt tartalmazások szerint vannak olyan $g, h \in G^*$, hogy $\sigma(h, u) = \sigma', \sigma(g, u) = \sigma$ és $\sigma(g, u') = \mathrm{id}(G)$ minden $u' \nsim u$ esetén. Ekkor $h^{-1}gh \in G^*$ és $\sigma\big(h^{-1}gh, u\big) = \sigma'^{-1}\sigma\sigma'$. Ha $u' \nsim u$, akkor $\sigma\big(h^{-1}gh, u\big) = \sigma'^{-1}\,\mathrm{id}\,\Gamma_k\sigma' = \sigma'^{-1}\sigma' = \mathrm{id}\,\Gamma_k$. Ez éppen azt jelenti, hogy $\sigma'^{-1}\sigma\sigma' \in N(G)$. ■

A továbbiakban az $N_u(G)$ és $H_u(G)$ jelöléseknél néha el fogjuk hagyni az alsó indexeket, amennyiben $G \geq \mathrm{Aut}(V)$. Ezt a A 3.28. lemma miatt megtehetjük.

3.30. lemma. *Legyen $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}\,(V)_0$ egy zárt csoport, ami a szimmetrikus csoportként hat a $\sim_{k_G}$-ekvivalenciaosztályok halmazán. Ekkor az $N(G)$ és $H(G)$ részcsoportok a címkézéstől is függetlenek.*

Bizonyítás. Ebben a bizonyításban az $N(G)$ és $H(G)$ csoportoknál felső indexben jelezzük, hogy melyik k_G-címkézést használjuk a definíciójuknál. A $\mathcal{S}^{(k(G))}$ csoport nem függ a címkézéstől, így a $G^* = G \cap \mathcal{S}^{(k(G))}$ csoport sem. Egy rögzített f k_G-címkézésre, egy $g \in G^*$-beli elemre és egy $v \in V \setminus 0$ vektorra pontosan akkor teljesül $\sigma_f(g,u) = \mathrm{id}\,\Gamma_{k_G}$, ha g identitásként hat a $\sim_G (v)$ ekvivalenciaosztályon. Így ez a tény is független a címkézés megválasztásától. Ezeket használva a következő módon bizonyítható a lemma.

Legyenek f és f' két tetszőleges k_G-címkézés $V \setminus 0$-n. Legyen most f'' egy olyan címkézés, amelyik valamelyik k_G ekvivalenciaosztályon megegyezik f-fel és valamelyik ekvivalenciaosztályon megegyezik f'-vel. Legyen u tehát egy olyan elem, amire a $\sim_G (u)$ ekvivalenciaosztályon f és f'' megegyezik. Ekkor egy $g \in G^*$ elemre $\sigma_f(g,u) = \sigma_{f''}(g,u)$. Ebből következik, hogy $H^f(G) = H^f_u(G) = H^{f''}_u(G) = H^f(G)$. Tegyük fel most, hogy $\sigma \in N^f(G)$. Ekkor van olyan $g \in G^*$ transzformáció, amire $\sigma_f(g,u) = \sigma$ és $\sigma_f(g,u') = \mathrm{id}\,\Gamma_{k_G}$ minden $u' \nsim u$-ra. Ebből következik $\sigma_{k_G,f''}(g,u) = \sigma_{f''}(g,u) = \sigma$ és $\sigma_{f''}(g,u') = \mathrm{id}\,\Gamma_{k_G}$ minden $u' \nsim u$-ra, hiszen amint láttuk az, hogy $\sigma_f = \mathrm{id}\,\Gamma_{k_G}$ teljesül-e, nem függ a címkézés megválasztásától. Tehát $\sigma \in N^{f''}(G)$. Azt kaptuk tehát, hogy $N^f(G) \subset N^{f''}(G)$. Hasonlóan adódik a másik irányú tartalmazás is, így valójában $N^f(G) = N^{f''}(G)$.

Tehát $H^f(G) = H^{f''}(G)$ és $N^f(G) = N^{f''}(G)$. Hasonlóan bizonyíthatóak a $H^{f'}(G) = H^{f''}(G)$ és $N^{f'}(G) = N^{f''}(G)$ egyenlőségek is, így $H^f(G) = H^{f'}(G)$ és $N^f(G) = N^{f'}(G)$. ■

A Γ_k csoport hat saját magán a balról (vagy jobbról) szorzással. Ez a hatás hű, így adódik egy természetes $\Gamma_k \hookrightarrow \mathrm{Sym}(\Gamma_k)$ beágyazás.

3.31. lemma. *Legyen* $\mathrm{Aut}(V) \le G \le \mathrm{Sym}\,(V)_0$ *egy zárt csoport, ami a szimmetrikus csoportként hat a* $\sim_{k_G}$*-ekvivalenciaosztályok halmazán, és* f *egy* k_G*-címkézés. Ekkor* $\Gamma_{k_G} \le N(G)$.

Bizonyítás. Legyenek $u, v \in V^f, u \neq v$ tetszőlegesek. Legyen $\lambda \in \Gamma_{k_G}$ tetszőleges. Belátjuk, hogy $\lambda \in N(G)$.

Legyen f' az a címkézés, amire $f'(u') = f(u')$ minden $u' \nsim_G u$ esetén, és $f'(u') = \lambda u'$ minden $u' \sim_G u$ esetén. Legyen továbbá $g \in \mathrm{Sym}\left((V \setminus 0)/\sim_{k_G}\right)$ az a permutáció, ami kicseréli u és v ekvivalenciaosztályát. Ekkor $g^f g^{f'} \in G$ a 3.25. állítás szerint. Nyilván $g^f g^{f'} \in \mathcal{S}^{(k(G))}$, így $g^f g^{f'} \in G^* = G \cap \mathcal{S}^{(k(G))}$ is teljesül. Azt állítjuk, hogy ekkor $\sigma(g^f g^{f'}, v) = \lambda$ és $\sigma(g^f g^{f'}, v') = \mathrm{id}\,\Gamma_{k_G}$ minden $v' \nsim v$-re. Ezt elég bizonyítani, hiszen az $N(G)$ csoport definíciója szerint $\lambda \in N(G)$.

Tegyük fel, hogy $v' = \mu v$ valamilyen $\mu \in \Gamma_{k_G}$-re. Ekkor

$$v'^{g^f g^{f'}} = \left((\mu v)^{g^f}\right)^{g^{f'}} = (\mu u)^{g^{f'}} = \frac{f'(\mu u)}{f'(\mu v)}\mu v = \frac{\lambda\mu}{\mu}\mu v = \lambda\mu v.$$

Tegyük fel most, hogy $v' \nsim v$. Ebből $v'^{g^f} \nsim u$, és így $f(v'^{g^f g^{f'}}) = \left(f(v'^{g^f})^{g^{f'}}\right. = \left(f(v'^{g^f})^{g^f}\right. = f(v')$. Mivel $g^f g^{f'} \in G^*$, ezért $v'^{g^f g^{f'}} \sim_G v'$ is teljesül, így $v'^{g^f g^{f'}} = v'$, azaz $\sigma(g^f g^{f'}, v) = \mathrm{id}\,\Gamma_{k_G}$. ■

3.32. definíció. Legyen f egy tetszőleges k-címkézés valamilyen $k \mid p-1$-ra. Legyenek továbbá $\Gamma_k \leq N \triangleleft H \leq \mathrm{Sym}(\Gamma_k)$ tetszőleges csoportok.

Ekkor legyen $G_f^*(N,H)$ azon $g \in \mathrm{Sym}_0(V)$ elemek csoportja, ami stabilizál minden $\sim_k$-ekvivalenciaosztályt, a $\sigma_f(g,v) :\ v \in V \setminus 0$ elemek mind elemei H-nak, és a H/N faktorcsoportban megegyeznek.

Legyen $G_f(N,H) := G_f^*(N,H)\big(\mathrm{Sym}\left((V\setminus 0)/\sim_{k_G}\right)^f$.

A 3.27 és 3.32 definíciókból könnyen látható, hogy ha $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}_0^{(k)}(V)$ egy csoport, és f egy k-címkézés, akkor

$$N\big(G_f(N,H)\big) = N \quad \text{és} \quad H\big(G_f(N,H)\big) = H.$$

Ennek a megállapításnak egyszerű következménye, hogy a $G_f(N,H) \leq G_f(N',H')$ pontosan akkor teljesül, ha $N \leq N'$ és $H \leq H'$, továbbá hogy $G_f(N,H) = G_f(N',H')$ esetén $N = N'$ és $H = H'$ (azaz a $G_f(N,H)$ csoportok páronként különbözőek).

3.33. lemma. *Legyen f egy tetszőleges k-címkézés valamilyen $k \mid p-1$-ra. Legyenek továbbá $\Gamma_k \leq N \triangleleft H \leq \mathrm{Sym}(\Gamma_k)$ tetszőleges csoportok. Ekkor $G_f(N,H)$ tartalmazza $\mathrm{Aut}(V)$-t, $k_{G(N,H)} = k$, és $G_f(N,H)$ a teljes szimmetrikus csoportként hat a $\sim_k$-ekvivalenciaosztályok halmazán.*

Bizonyítás. A lemmában felsorolt állításokból csak az nem triviális, hogy $\mathrm{Aut}(V) \leq G_f(N,H)$. Mivel $\Gamma_k \leq N, H$, ezért $G_f(\Gamma_k,\Gamma_k) \leq G_f(N,H)$, így elég belátni, hogy $\mathrm{Aut}(V) \leq G_f(\Gamma_k,\Gamma_k)$. Legyen $\gamma \in \mathrm{Aut}(V)$ tetszőleges. Ekkor van olyan $g \in \mathrm{Sym}\left((V\setminus 0)/\sim_{k_G}\right)^f$, hogy $g' := \gamma g$ stabilizál minden $\sim_k$ ekvivalenciaoszályt. Mivel $\gamma \in \mathrm{Aut}(V)$, ezért $\sigma(g,u) \in \Gamma_k$ minden $u \in V \setminus 0$-ra. A g egy f-fel kompatibilis permutáció, így $\sigma(g,u) = \mathrm{id}\,\Gamma_k$. Ebből következik, hogy $\sigma(\gamma g,u) \in \Gamma_k$ minden $u \in V \setminus 0$-ra. Ez definíció szerint éppen azt jelenti, hogy $g' = \gamma g \in G_f^*(\Gamma_k,\Gamma_k)$, amiből

$$\gamma = {g'}^{-1} g \in G_f^*(\Gamma_k,\Gamma_k)\,\mathrm{Sym}\left((V\setminus 0)/\sim_{k_G}\right)^f = G_f(\Gamma_k,\Gamma_k).$$

Tehát valóban $\mathrm{Aut}(V) \leq G_f(\Gamma_k,\Gamma_k)$. ■

3.34. tétel. *Legyen $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}\,(V)_0$ egy zárt csoport, ami a szimmetrikus csoportként hat a $\sim_{k_G}$-ekvivalenciaosztályok halmazán, és f egy k_G-címkézés. Ekkor vannak olyan $\Gamma_{k_G} \leq N \triangleleft H \leq \mathrm{Sym}(\Gamma_{k_G})$ csoportok, hogy $G = G_f(N,H)$.*

Bizonyítás. Azt állítjuk az $N := N(G)$ és $H := H(G)$ választás jó lesz. Ekkor a 3.29. és a 3.31. lemmák szerint a $\Gamma_{k_G} \leq N \triangleleft H \leq \mathrm{Sym}(\Gamma_{k_G})$ tartalmazások teljesülnek. A 3.26. következmény szerint $G = G^*\big(\mathrm{Sym}\left((V\setminus 0)/\sim_{k_G}\right)^f$, így elég belátni, hogy $G^* = G_f^*(N,H)$.

Tegyük fel, hogy $g \in G^*$, és legyen v,w tetszőleges inekvivalens elemei $V \setminus 0$-nak. Ekkor $\sigma(g,v) \in H(G) = H$. Azt kell még belátni, hogy $\sigma(g,v)$ és $\sigma(g,w)$ képe megegyezik a H/N faktorcsoportban. Ehhez elég belátni, hogy $\sigma(g,v)\sigma(g,w)^{-1} \in N$. Legyen most $t \in \mathrm{Sym}\left((V\setminus 0)/\sim_{k_G}\right)$ az a transzpozíció, ami felcseréli v és

w ekvivalenciaosztályát. Tekintsük ekkor a $h = gt^f g^{-1}(t^{-1})^f = gt^f g^{-1} t^f$ kommutátort. Ez minden $\sim_G$-ekvivalenciaosztályt stabilizál, és

$$\sigma(h,v) = \sigma(g,v)\sigma(t^f,v)\sigma(g^{-1},w)\sigma(t^f,w) = \sigma(g,v)\sigma(g,w)^{-1},$$

továbbá minden $u \nsim_G v, w$ esetén

$$\sigma(h,u) = \sigma(g,u)\sigma(t^f,u)\sigma(g^{-1},u)\sigma(t^f,u) = \mathrm{id}(\Gamma_{k_G}).$$

Legyen most v rögzített és $w_1, w_2, \ldots$ a $V \setminus 0$ halmaz elemeinek egy felsorolása.

Legyen ekkor minden i-re $t_i \in \mathrm{Sym}\big((V \setminus 0)/\sim_{k_G}\big)$ az a transzpozíció, ami felcseréli w és w_i ekvivalenciaosztályát. Tekintsük ekkor a $h_i := t_i^f h (t_i^f)^{-1} = t_i^f h t_i^f$ permutációkat. Ekkor $h_i \in G^*$,

$$\sigma(h_i,v) = \sigma(t_i^f,v)\sigma(g,v)\sigma(g,w)^{-1}\sigma(t_i^f,v)^{-1} = \sigma(g,v)\sigma(g,w)^{-1},$$

és minden olyan u-ra, ami nem ekvivalens a v és w_i elemek egyikével sem

$$\sigma(h_i,u) = \sigma(t_i^f,u)\sigma(t_i^f,u^{t_i^f})\sigma(t_i^f,u^{t_i^f}) = \mathrm{id}(\Gamma_{k_G}).$$

Ekkor a $h_1, h_2, \ldots$ sorozat konvergens, és ennek a h határértékére h stabilizál minden $\sim_G$-ekvivalenciaosztályt, $\sigma(h,v) = \sigma(g,v)\sigma(g,w)^{-1}$ és $\sigma(h,u) = \mathrm{id}(\Gamma_{k_G})$ minden $u \nsim_G v$-re. Ebből következik, hogy $\sigma(g,v)\sigma(g,w)^{-1} \in N(H) := N$. Ezzel beláttuk, hogy $G^* \subset G_f^*(N,H)$.

Most belátjuk, hogy $G_f^*(N,H) \subset G^*$. Legyen U egy véges részhalmaza V-nek. Mivel G zárt, ezért az állításhoz elég belátni, hogy $G_f^*(N,H)\big|_U \subset G^*|_U$. A $G_f^*|_U$ hatást generálják a $g_{n,u} : n \in N,\ u \in U$ és a $g'(h) : h \in H$ elemek megszorításai U-ra, ahol a $g_{n,u}$ és $g'(h)$ elemek stabilizálnak minden $\sim_G$-ekvivalenciaosztályt, $\sigma\big(g'(h),v\big) = h$ minden $v \in U$-ra, $\sigma\big(g(n,v),v\big) = n$ és $\sigma\big(g(n,u),v\big) = \mathrm{id}(\Gamma_{k_G})$ minden $u \in U \setminus \sim_G (v)$-re. Az $N = N(G)$ csoport definíciójából következik, hogy a $g(n,u)\big|_U$ elemeket mind tartalamazza $G^*|_U$, így elég belátni, hogy tetszőleges $h \in H$ esetén $g'(h)\big|_U \in G^*|_U$. A H csoport definíciója miatt van olyan $g_0 \in G^*$ elem, amire $\sigma(g_0,v) = h$ valamilyen $v \in V \setminus 0$-ra. Láttuk, hogy $G^* \subset G_f^*(N,H)$. Ebből következik, hogy minden $u \in V \setminus 0$ esetén $\sigma(g_0,u) = hn_u$ valamilyen $n_u \in N$-re. Legyen U' a V^f egy olyan véges halmaz, amire $\bigcup_{v \in V^f} \sim_G (v)$ lefedi U-t, és tekintsük a $g_1 = g_0 \prod_{u \in U'} g^{-1}(n_u,u)$ permutációt. A $g(n_u,u)$ transzformációk páronként felcserélhetőek, így az előbbi szorzatnál mindegy, hogy milyen sorrendben szorozzuk össze az elemeket. Ekkor tetszőleges $u \in U$ esetén

$$\sigma(g_1,u) = \sigma(g_0,u)\sigma\big(g^{-1}(n_u,u)\big) = hn_u n_u^{-1} = h = \sigma(g',u),$$

így $g_1|_U = g'(h)\big|_U$, és ezt kellett bizonyítanunk. ■

3.35. következmény. *Ha $\Gamma_k \le N \lhd H \le \mathrm{Sym}\big(\Gamma_k(G)\big)$, akkor a $G_f(N,H)$ jelölés független az f címkézés megválasztásától.*

Bizonyítás. Legyen f és f' két tetszőleges k-címkézés. Ekkor $H\big(G_f(N,H)\big) = H$ és $N\big(G_f(N,H)\big) = N$. Ekkor azonban a 3.34. tételt alkalmazva a $G_f(N,H)$ csoportra és az f' címkézésre adódik, hogy $G_f(N,H) = G_{f'}(N,H)$. ■

4. A vektortér 0-t nem fixáló reduktjai

Legyen V továbbra is egy megszámlálhatóan végtelen dimenziós vektortér $\mathbb{F}_p$ fölött, ahol $p \geq 3$ prím. Ebben a fejezetben belátjuk, hogy ha V automorfizmuscsoportjának egy zárt szupercsoportjának van olyan eleme, ami nem tartja a 0-t, akkor V vagy az affin transzformációk csoportja, vagy a teljes szimmetrikus csoport. Ezen állítás bizonyításához használni fogjuk az előző fejezet eredményeit.

Jelölje $\mathrm{Aff}(V)$ az affin transzformációk csoportját V-ben. Egy $v \in V$ vektor esetén jelölje tr_v az $u \mapsto u + v$ eltolást V-n. Ekkor minden $g \in \mathrm{Aff}(V)$ egyértelműen felírható $g = g_0 \,\mathrm{tr}_u$ alakban, ahol $g_0 \in \mathrm{Aut}\, V$ és $u \in V$. Mivel $\mathrm{Aut}(\mathbb{F}_p)$ triviális, és $p \geq 3$, ezért az affin geometria alaptétele szerint egy $g \in \mathrm{Sym}(V)$ transzformáció pontosan akkor affin transzformáció, ha kollineáció, azaz g minden affin egyenest egyenesbe visz. Erre az észrevételre még szükségünk lesz a későbbiekben.

4.1. lemma. *Ha* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ *csoport, ami nem tartja a* 0*-t, akkor* G *tranzitívan hat* V*-n.*

Bizonyítás. $\mathrm{Aut}(V)$ tranzitívan hat $V \setminus 0$-n, és G-nek van olyan eleme, ami a 0-t egy $V \setminus 0$-beli vektorba képezi. Ebből következik, hogy G tranzitív. ■

A bizonyításhoz szükségünk lesz az alábbi jelölésre.

4.2. definíció. Legyen G egy csoport, ami hat V-n, és legyenek, $a, b \in V$ tetszőlegesek. Ekkor jelölje $F_G(a, b)$ az $\{a, b\}$ halmaz elemenkénti stabilizátorának véges orbitjainak unióját.

Ez a jelölés a következő módon függ össze a 3. fejezetbeli „$\sim_G$” jelöléssel.

4.3. lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ *egy csoport. Ekkor* $b \in F_G(0, a)$ *pontosan akkor teljesül, ha* $b \sim_{G_0} a$ *vagy* $b = 0$*.*

Bizonyítás. $b = 0$ esetén az állítás triviális, tegyük fel most, hogy $b \neq 0$.

Tegyük fel először, hogy $b \sim_{G_0} a$. Ekkor definíció szerint minden $g \in G_0$ esetén $b^g \in \langle a^g \rangle$, így minden $b \in (G_0)_v$ esetén $b^g \in \langle a \rangle$. Ekkor mivel $\langle a \rangle$ véges, így b orbitja is véges. Tehát $b \in F_G(0, a)$.

Tegyük fel most, hogy $b \nsim a$. Ekkor van olyan $g \in G_0$, hogy a^g, b^g lineárisan függetlenek. Legyen $h \in \mathrm{Aut}(V) \subset G_0$ egy olyan lineáris transzformáció, ami a^g-t a-ba viszi. Ekkor $gh \in (G_0)_a$ és $b^{gh} \notin \langle a \rangle$. Ekkor a 3.4. lemma szerint $(G_0)_a(b)$ végtelen, így $b \notin F_G(0, a)$. ■

4.4. következmény. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ *egy csoport, ami nem tartja a* 0*-t. Ekkor tetszőleges* $u, v \in V$ *különböző vektorok esetén* $\left|F_G(u, v)\right| = k_{G_0} + 1$*.*

Bizonyítás. A 4.1. lemma szerint G tranzitív, így az állítást elég belátni abban az esetben, amikor $u = 0$. A 4.3. lemma szerint azonban ekkor $F(u, v) = F(0, v) = \{w \in V : w \neq 0,\, w \sim_{G_0} v\} \cup \{0\}$, speciálisan $F(0, v) = k_{G_0} + 1$. ■

4.5. lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ *egy csoport, ami nem stabilizálja a* 0*-t. Ekkor tetszőleges* $a, b \in V, a \neq b$ *és* $u, v \in F_G(a,b), u \neq v$ *esetén* $F_G(u,v) = F_G(a,b)$.

Bizonyítás. A 4.1. lemma szerint G tranzitív, így feltehető, hogy $a = 0$. A 4.3. lemma szerint ekkor $c \in F(a,b)$ pontosan akkor teljesül, ha $c \sim_{G_0} b$. Tegyük fel most, hogy $u, v \in F_G(a,b), u \neq v$ és $w \notin F_G(a,b)$. Ekkor $u \sim_{G_0} b \sim_{G_0} v$ és $w \nsim_{G_0} b \sim_{G_0} u$. Ebből következik, hogy létezik olyan $g \in G_0$, hogy w^g és u^g lineárisan függetlenek. A $\sim_{G_0}$ reláció definíciója miatt $v^g \in \langle u^g \rangle$, így $w^g \notin \langle u \rangle = \langle u^g, v^g \rangle$. Így a 3.4. lemma szerint $(G_0)_{u^g, v^g}(w^g)$ végtelen. Ekkor $(G_0)_{u,v}(w)$ is végtelen, és így $G_{u,v}(w)$ is végtelen. Tehát $w \notin F_G(u,v)$. Beláttuk tehát, hogy $w \notin F_G(a,b)$ esetén $w \notin F_G(u,v)$. Ez azt jelenti, hogy $F_G(u,v) \subset F_G(a,b)$. A 4.4. következmény szerint azonban $\left|F_G(a,b)\right| = \left|F_G(u,v)\right| = k_{G_0} + 1$, így $F_G(u,v) = F_G(a,b)$. ■

4.6. lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ *egy zárt csoport, ami nem fixálja a* 0*-t. Ekkor* $k_{G_0} = 1$ *vagy* $k_{G_0} = p - 1$.

Bizonyítás. Tegyük fel, hogy $1 < k_{G_0} < p - 1$. Ez azt jelenti, hogy létezik olyan $\lambda \in \mathbb{F}_p \setminus \{0,1\}$, hogy $\lambda v \nsim_{G_0} v$. Ekkor a 4.3. lemma szerint $\lambda v \notin F_G(0,v)$. Azt állítjuk, hogy ekkor $0 \notin F_G(v, \lambda v)$. Tegyük fel ugyanis, hogy $0 \in F_G(v, \lambda v)$. Ebből a 4.5. lemma szerint $F(v, \lambda v) = F_G(0,v)$ kövekezik, amiből $\lambda v \in F_G(0,v)$, ami nem lehet. Mivel $1 < k_{G_0}$, ezért a 4.4. következmény szerint van olyan $u \in F_G(v, \lambda v)$, amire $u \neq v, \lambda v$. Az előbbiek szerint $u = 0$ nem lehetséges. Mivel $u \in F_G(v, \lambda v)$, ezért $G_{v, \lambda v}(u)$ véges, és így $(G_0)_{v, \lambda v}(u)$ is véges. Ekkor a 3.4. lemma szerint $u \in \langle v, \lambda v \rangle = \langle v \rangle$. Azt kaptuk tehát, hogy létezik olyan $\mu \in \mathbb{F}_p \setminus \{0, 1, \lambda\}$, hogy $\mu v = u \in F_G(v, \lambda v)$.

1. eset: $\mu v \nsim_{G_0} v$ *és* $\mu v \nsim_{G_0} \lambda v$. Ebben az esetben v, λv, μv páronként inekvivalens vektorok. A $G_0 = G \cap \mathrm{Sym}(V)_0$ csoport zárt, és tartalmazza $\mathrm{Aut}(V)$-t, így a 3.16. tétel szerint G_0 3-tranzitívan hat a $\sim_{G_0}$-ekvivalenciaosztályok halmazán. Speciálisan létezik olyan $g \in G_0$, amire a v^g, $(\lambda v)^g$, $(\mu v)^g$ vektorok lineárisan függetlenek. Ekkor a 3.4. lemma szerint $(G_0)_{v^g, (\lambda v)^g}(\mu g)$ végtelen, és így $(G_0)_{v, \lambda v}(\mu v)$ is végtelen, ami ellentmond annak, hogy $\mu v \in F_G(v, \lambda v)$. Tehát $\mu v \sim_{G_0} v$ vagy $\mu v \sim_{G_0} \lambda v$.

2. eset: $\mu v \sim_{G_0} v$. Ekkor a 4.4. következményt használva $\mu v \in F_G(v, \lambda v)$, amiből $\lambda v \in F_G(v, \mu v) = F_G(0,v)$, ami ellentmondás.

3. eset: $\mu v \sim_{G_0} \lambda v$. Ekkor megint a 4.4. következményt használva $\mu v \in F_G(v, \lambda v)$, amiből $v \in F_G(\lambda v, \mu v) = F_G(0, \lambda v)$ adódik, és így a 4.3. lemma szerint $\lambda v \sim_{G_0} v$, ami ellentmondás.

Minden esetben ellentmondást kaptunk, tehát $k_{G_0} = 1$ vagy $k_{G_0} = p - 1$. ■

A 4.4 és a 4.6. lemmák szerint, ha egy $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ csoport nem fixálja a 0-t, akkor tetszőleges $u, v \in V$, $u \neq v$ elemek esetén $\left|F(u,v)\right| = 2$ vagy $\left|F(u,v)\right| = p + 1$. Az előbbi esetben nyilván $F(u,v) = \{u, v\}$. Belátjuk, hogy az utóbbi esetben $F(u,v) = L(u,v)$, az u, v vektorokat összekötő affin egyenes. Ehhez először szükségünk lesz az alábbi lemmára.

4.7. lemma. *Legyen U egy 2 dimenziós vektortér $\mathbb{F}_p$ felett, és legyen $H \subset U, |H| = p$ egy olyan halmaz, amelynek elemei páronként lineárisan függetlenek, és kielégíti az alábbi feltételt:*

(1) *Tetszőleges $\lambda, \mu \in \mathbb{F}_p$ és $u, v, u', v' \in H$ esetén, ha $u \neq v, u' \neq v'$ és $\lambda u + \mu v \in H$, akkor $\lambda u' + \mu v' \in H$.*

Ekkor H egy affin egyenes U-ban.

Bizonyítás. A bizonyításban jelöljük I-vel azon $(\lambda, \mu) \in \mathbb{F}_p^2$ párok halmazát, amire $\lambda u + \mu v \in H$ valamelyik (az összes) különböző elemekből álló $(u, v) \in H^2$ esetén. Könnyen látható, hogy ekkor $(\lambda, \mu) \in I$ pontosan akkor teljesül, ha $(\mu, \lambda) \in I$ teljesül.

1. állítás. Ha $(\lambda, \mu) \in I$, ahol $\lambda, \mu \neq 0$, akkor $(\mu + 1, -\mu) \in I$. Legyenek ugyanis $a, b \in H, a \neq b$ tetszőlegesek. Tekintsük most a következő összefüggést.

$$\frac{1}{\lambda}(\lambda a + \mu b) - \frac{\mu}{\lambda} b = a \in H.$$

Mivel $\mu \neq 0$, ezért $\lambda a + \mu b \neq b$, és így $\left(\frac{1}{\lambda}, -\frac{\mu}{\lambda}\right) \in I$. Hasonlóan $\frac{1}{\lambda} a - \frac{\mu}{\lambda} b \neq a$, hiszen $\mu \neq 0$. Ekkor mivel $(\lambda, \mu) \in H$, ezért

$$H \ni \lambda \left(\frac{1}{\lambda} a - \frac{\mu}{\lambda} b \right) + \mu a = (\mu + 1)a - \mu b.$$

Ebből következik, hogy $(\mu + 1, -\mu) \in I$.

Most belátjuk a lemma állítását. Legyenek megint $a, b \in H, a \neq b$ tetszőlegesek. Ha $p = 3$ és $-a - b \in H$, akkor készen vagyunk, hiszen ekkor csak $H = \{a, b, -a - b\} = L(a, b)$ lehetséges. Tegyük fel ezért, hogy $p > 3$, vagy $p = 3$ és $-a - b \notin H$. Mivel $|H| = p$, ezért mindkét esetben azt kapjuk, hogy van olyan $(\lambda, \mu) \in I$ pár, amire $\lambda \neq 0$, $\mu \neq 0$ és a λ, μ elemek valamelyike nem -1. Mivel $(\lambda, \mu) \in I$ pontosan akkor teljesül, ha $(\mu, \lambda) \in I$, ezért feltehető, hogy $\mu \neq -1$. Ekkor az előbbiek szerint $(\mu + 1, -\mu) \in I$.

Legyen most M azon ν-k halmaza, amire $(\nu + 1, -\nu) \in I$ teljesül. Ekkor $0, -1, \mu \in M$, és a feltételeink szerint $\mu \neq 0, -1$. Ha $(\nu + 1, -\nu b) \in I$ és $\nu \neq 0, -1$, akkor az 1. állítás szerint $\big(\nu + 2, -(\nu + 1)\big) \in I$. Ebből következik, hogy $\mu, \mu + 1, \ldots, p - 2 \in M$. Ha $(\nu + 1, -\nu) \in I$ és $\nu \neq 0, -1$, akkor $(-\nu, 1 + \nu) \in I$, és ekkor az 1. állítás szerint $(-\nu + 1, \nu) \in I$ és így $\big(\nu, -(\nu - 1)\big) \in I$. Ebből következik, hogy $\mu, \mu - 1, \ldots, 2 \in M$. Ez azonban azt jelenti, hogy csak $M = \mathbb{F}_p$ lehetséges, és ekkor $I \supset \big\{(\nu + 1, -\nu) : \nu \in \mathbb{F}_p\big\}$, amiből

$$H \supset \big\{(\nu + 1)a - \nu b : \nu \in \mathbb{F}_p\big\} = L(a, b)$$

adódik. Az $L(a, b)$ egyenes számossága azonban p, így csak $H = L(a, b)$ lehetséges. ■

4.8. állítás. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ *egy zárt csoport, ami nem fixálja a* 0*-t. Ekkor ha* $k_{G_0} = p-1$*, akkor* $F_G(a,b) = L(a,b)$ *tetszőleges* $a, b \in V$ *különböző elemek esetén.*

Bizonyítás. Tegyük fel először, hogy $a, b \in V$ lineárisan összefüggenek. Ekkor ha $v \notin \langle a,b\rangle$, akkor a 3.4. lemma szerint $(G_0)_{a,b}(v)$ végtelen, és így $G_{a,b}(v)$ is végtelen, amiből következik, hogy $v \notin F_G(a,b)$. Tehát $F_G(a,b) \subset \langle a,b\rangle$. Ha a, b lineárisan összefüggenek, akkor $\big|\langle a,b\rangle\big| = \big|L(a,b)\big| = p$. A 4.4. következmény szerint az $F_G(a,b)$ halmaz is p elemű. Ez csak $F_G(a,b) = L(a,b)$ esetén lehetséges.

Tegyük fel most, hogy $a, b \in V$ lineárisan függetlenek. Legyen $U = \langle a,b\rangle$, ekkor $\dim U = 2$. Az előbbiekhez hasonlóan $v \notin \langle a,b\rangle$ esetén $v \notin F_G(a,b)$, így $F_G(a,b) \subset U$. Belátjuk, hogy ekkor az U 2 dimenziós altérre, és a $H := F_G(a,b)$ halmazra teljesülnek a 4.7. lemma feltételei. Ez elég, hiszen ekkor a 4.7. lemma szerint $H = F_G(a,b)$ egyenes, és ekkor ez az egyenes csak $L(a,b)$ lehet, hiszen $a, b \in F_G(a,b)$.

A 4.4. következmény szerint $|H| = \big|F_G(a,b)\big| = k_{G_0} + 1 = p$. Belátjuk most, hogy H nem tartalmaz két különböző lineárisan összefüggő vektort. Tegyük fel ugyanis, hogy $0 \neq u, \lambda u \in F(a,b)$, ahol $\lambda \neq 1$. Ekkor a 4.5. lemma szerint $F(a,b) = F(u,\lambda u)$, ami lehetetlen, hiszen az állításnak a már bizonyított előző esete szerint $F(u,\lambda u) = \langle u\rangle$, és ekkor $F(u,\lambda u)$ nem tartalmazhatna két lineárisan független vektort. Be kell még látni a 4.7. lemma (1) feltételét. Ehhez tegyük fel, hogy $u, v, u', v' \in H$ olyan vektorok, hogy $u \neq v$, $u' \neq v'$, és legyenek $\mu, \lambda \in \mathbb{F}_p$ olyan együtthatók, amelyekre $\lambda u + \mu v \in H$ teljesül. Be kell látnunk, hogy ekkor $\lambda u' + \mu v' \in H$. A 4.5. lemma szerint $F(a,b) = F(u,v) = F(u',v')$, így ezen állításhoz elég belátni, hogy $G_{u',v'}(\lambda u' + \mu v')$ véges. Legyen most $g \in \mathrm{Aut}(V) \subset G$ egy olyan lineáris transzformáció, amire $(u')^g = u$ és $(v')^g = v$. Ilyen létezik, hiszen az u, v és az u', v' is lineárisan független párok. Ekkor

$$\big|G_{u',v'}(\lambda u + \mu v)\big| = \Big|G_{(u')^g,(v')^g}\big((\lambda u' + \mu v')^g\big)\Big| = \big|G_{u,v}(\lambda u + \mu v)\big|,$$

ami véges, hiszen $\lambda u + \mu v \in H = F_G(a,b) = F_G(u,v)$. ■

4.9. tétel. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ *egy zárt csoport, ami nem fixálja a* 0*-t. Ekkor* $G = \mathrm{Aff}(V)$ *vagy* $G = \mathrm{Sym}(V)$*.*

Bizonyítás. A 4.6. lemma szerint $k_{G_0} = 1$ vagy $k_{G_0} = p-1$.

1. eset. $k_{G_0} = 1$. A $G_0 = G \cap \mathrm{Sym}_0(V)$ csoport zárt, így a 3.17. következmény szerint $G_0 = \mathrm{Sym}_0(V)$. A 4.1. lemma szerint azonban a G csoport tranzitívan hat V-n. Ez csak $G = \mathrm{Sym}(V)$ esetén lehetséges.

2. eset. $k_{G_0} = p-1$. Ekkor először belátjuk, hogy $G \leq \mathrm{Aff}(V)$. Ehhez elég belátni, hogy G minden eleme kollineáció. Legyen tehát $g \in G$ és $L = L(a,b)$ egy tetszőleges affin egyenes V-ben. Ekkor a 4.8. állítás szerint $L(a,b) = F_G(a,b)$. Az $F_G(a,b)$ halmaz definíciójából könnyen látható, hogy $\big(F_G(a,b)\big)^g = F_G(a^g,b^g)$, így $\big(L(a,b)\big)^g = F_G(a^g,b^g) = L(a^g,b^g)$. Tehát g valóban kollineáció. Tehát $G \leq \mathrm{Aff}(V)$.

Belátjuk most, hogy valójában $G = \mathrm{Aff}(V)$. Tegyük fel ugyanis, hogy $g \in G$ és g nem fixálja a 0-t. Ekkor $g = g_0\,\mathrm{tr}_v$ alakú valamilyen $g_0 \in \mathrm{Aut}(V)$-re és $v \in V \setminus 0$-ra. Ekkor $g_0 \in \mathrm{Aut}(V) \subset G$ miatt $\mathrm{tr}_v \in G$ is teljesül. Belátjuk, hogy ekkor már

G tartalmaz minden eltolást. Ez elég, hiszen az eltolások generálják $\mathrm{Aff}(V)$-t. Legyen tehát $w \in V \setminus 0$ tetszőleges. Legyen ekkor $h \in \mathrm{Aut}(V) \subset G$ egy olyan lineáris transzformáció, ami v-t w-be képezi. Ekkor tetszőleges $u \in V$ esetén

$$u^{h^{-1}\,\mathrm{tr}_v\,h} = \left(u^{h^{-1}} + v\right)^h = \left(u^{h^{-1}}\right)^h + v^h = u + v^h = u + w = u^{\mathrm{tr}_w},$$

így $G \ni h^{-1}\,\mathrm{tr}_v\,h = \mathrm{tr}_w$. ■

A 4.9. tétel azonnali következménye a következő tétel.

4.10. tétel. *Legyen $\mathfrak{A}$ a V struktúra egy reduktja, amiben a 0 nem definiálható. Ekkor $\mathfrak{A}$ vagy ekvivalens V-vel, mint egy megszámlálhatóan végtelen dimenziós affin térrel, vagy ekvivalens a megszámlálhatóan végtelen, struktúra nélküli halmazzal.*

Bizonyítás. Legyen $G := \mathrm{Aut}(\mathfrak{A})$. Legyen továbbá $\mathfrak{A}^0$ az a struktúra, amit $\mathfrak{A}$-ból kapunk úgy, hogy hozzávesszük a 0-t, mint konstanst. Mivel a 0 nem definiálható $\mathfrak{A}$-ban, ezért $\mathfrak{A}$ és $\mathfrak{A}^0$ nem ekvivalensek. Ekkor a 2.1. tétel szerint

$$G = \mathrm{Aut}(\mathfrak{A}) \neq \mathrm{Aut}\,\mathfrak{A}^0 = G \cap \mathrm{Sym}\,(V)_0.$$

Speciálisan $G \not\leq \mathrm{Sym}\,(V)_0$. A G csoport egy struktúra automorfizmuscsoportja, így zárt. Ekkor a 4.9. tétel szerint $G = \mathrm{Aff}(V)$ vagy $G = \mathrm{Sym}(V)$, amiből szintén a 2.1. tételt használva adódik a tétel állítása. ■

Irodalom

[1] M. Bodirsky, H. Chen, M. Pinsker, The reducts of equality up to primitive positive interdefinability, *Journal of Symbolic Logic,* **75(4)** (2010), 1249–1292.

[2] M. Bodirsky, M. Pinsker, Minimal functions on the random graph, *Israel Journal of Mathematics* (2010), to appear

[3] M. Bodirsky, M. Pinsker, T. Tsankov, Decidability of definability, *Journal of Symbolic Logic,* **78**, 1036–1054.

[4] M. Bodirsky, M. Pinsker, Reducts of Ramsey structures, *Model Theoretic Methods in Finite Combinatorics,* 558. Contemporary Mathematics, American Mathematical Society (2011), 489–519.

[5] P. J. Cameron, Transitivity of permutation groups on unordered sets, *Mathematische Zeitschrift,* **148** (1976), 127–139.

[6] W. Hodges, *Model theory,* Cambridge University Press (Cambridge, 1993).

[7] M. Junker, M. Ziegler, The 116 reducts of $(\mathbb{Q}; <; a)$, *Journal of Symbolic Logic,* **74(3)** (2008), 861–884.

[8] D. Macpherson, A survey of homogeneous structures, *Discrete Mathematics,* **311(15)** (2011), 1599–1634.

[9] P. P. Pach, M. Pinsker, A. Pongrácz, Cs. Szabó, A new transformation of partially ordered sets, *J. Comb. Theory A.,* **120(7)** (2013), 1450–1462.

[10] P. P. Pach, M. Pinsker, G. Pluhár, A. Pongrácz, Cs. Szabó, Reducts of the random partial order, *Advances in Mathematics* (2014), to appear.

[11] A. Pongrácz, Reducts of the Henson graphs with a constant, *Annals of Pure and Applied Logic* (2013), to appear

[12] S. Thomas, Reducts of the random graph, *Journal of Symbolic Logic,* **56(1)** (1991), 176–181.

[13] S. Thomas, Reducts of random hypergraphs, *Annals of Pure and Applied Logic,* **80(2)** (1996), 165–193.

Bertalan Bodor, Kende Kalina: On first order definable reducts of the vectorspace $\mathbb{F}_p^\infty$ for odd primes

Let V denote the countably infinte dimensional projective space over a field of size p, where p is a prime and let $\mathrm{PGL}(V)$ denote its group of automorphisms. We investigate the supergroups of $\mathrm{PGL}(V)$.

Bodor Bertalan
Eötvös Lóránd Tudományegyetem,
Algebra és Számelmélet Tanszék,
1117 Budapest,
Pázmány Péter sétány 1/c
bodorb@cs.elte.hu

Kalina Kende
Eötvös Lóránd Tudományegyetem,
Algebra és Számelmélet Tanszék,
1117 Budapest,
Pázmány Péter sétány 1/c
kkalina@cs.elte.hu

BOOLE-ALGEBRÁK FUNKCIONÁLIS REDUKTJAI

BODOR BERTALAN, KALINA KENDE

Bevezetjük a funkcionális redukt fogalmát, mint speciális reduktokat, illetve meghatározzuk bizonyos Boole-algebrák összes funkcionális reduktját.

1. Bevezetés

Jelölje $\mathfrak{Ba} = (B, \wedge, \vee, 0, 1, \neg)$ a megszámlálható atommentes Boole-algebrát. Izomorfia erejéig pontosan egy ilyen struktúra létezik. Könnyű ellenőrizni, hogy $\mathfrak{Ba}$ bármely két véges részalgebrája között menő izomorfizmus kiterjed $\mathfrak{Ba}$ egy automorfizmusává, továbbá minden véges vagy megszámlálhatóan végtelen Boole-algebra beágyazható $\mathfrak{Ba}$-ba. Azaz $\mathfrak{Ba}$ homogén és univerzális a Boole-algebrák osztályában.

1. definíció. Egy $\mathbf{A} = (A, f_1, \ldots, f_n)$ algebra egy funkcionális reduktján egy $(A, t_1, \ldots, t_n)$ algebrát értünk, ahol a t_i kifejezések előállnak az f_i-k iterált kompozícióiként, azaz a t_i műveletek az $\mathbf{A}$ algebra kifejezés-függvényei.

Például (B, Δ), ahol Δ a szimmetrikus differenciát jelöli, $\mathfrak{Ba}$ egy Abel-csoport reduktja. Ebben a dolgozatban $\mathfrak{Ba}$ funkcionális reduktjait klasszifikáljuk. Megmutatjuk, hogy lényegében 13 ilyen funkcionális redukt létezik, és jellemezzük ezen funkcionális reduktokat.

A $\mathfrak{Ba}$ algera ω-kategorikus. Egy $\mathfrak{A}$ struktúrát ω-kategorikusnak nevezünk, ha megszámlálható, és elméletének minden megszámlálható modellje izomorf $\mathfrak{A}$-val. Azaz, ha egy $\mathfrak{A}$ struktúrában ugyanazok az elsőrendű formulák igazak, mint $\mathfrak{Ba}$-ban, akkor $\mathfrak{A}$ izomorf kell, hogy legyen $\mathfrak{Ba}$-val. A $\mathfrak{Ba}$ struktúra előáll, mint a véges Boole-algebrák osztályának Fraïssé-limesze [7]. Sok és sokféle önmagában is érdeklődésre számot tartó (relációs) homogén struktúra ismert. Közéjük tartozik például a véletlen gráf, a véges testek feletti megszámlálhatóan végtelen dimenziós vektorterek, a racionális számok halmaza a szokásos rendezési relációval ellátva vagy a megszámlálható atommentes Boole-algebra. Kevésbé ismert, de egyszerűségük miatt fontos példa a Henson-gráfok családja, ezek azok a H_n megszámlálható homogén gráfok, amelyek nem tartalmaznak teljes K_n részgráfot [8], továbbá a homogén részbenrendezett halmaz, ami a véletlen gráfhoz hasonlóan megkapható véletlen konstrukcióként is [1]. A homogén struktúrák általános elméletének kidolgozása

Fraïssé munkájával kezdődött [7], a Fraïssé-tétel karakterizálja azokat a végesen generált struktúrákból álló osztályokat, amelyek előállnak, mint valamely homogén struktúra végesen generált részstruktúráinak osztálya.

Ebben a dolgozatban egy struktúra egy reduktja alatt a struktúra alaphalmazán értelmezett relációk olyan halmazát értjük, amelyek mindegyikére igaz, hogy elsőrendű formulákkal definiálható a struktúrában. A reduktok halmazán értelmezhető egy kvázirendezés: $R_1 \lesssim R_2$ pontosan akkor, ha R_2 minden relációja definiálható R_1 feletti elsőrendű formulákkal. Két redukt kölcsönösen definiálható egymással, ha $R_1 \lesssim R_2$ és $R_2 \lesssim R_1$, azaz R_1 minden relációját definiálni lehet R_2 feletti elsőrendű formulákkal, és R_2 minden relációját definiálni lehet R_1 feletti elsőrendű formulákkal. A 2. tétel fontos következménye, hogy ω-kategorikus struktúra minden reduktja is ω-kategorikus. Ez nem ω-kategorikus struktúrákra még akkor sem feltétlen igaz, ha a struktúra nyelve véges, és csak relációkat tartalmaz. A [14]-ben megtalálható Lachlan egy ellenpéldájának leírása.

Egy redukt automorfizmuscsoportja pontosan azon permutációkból áll, amelyek megőrzik a redukt összes relációját, így speciálisan tartalmazza az eredeti struktúra automorfizmuscsoportját. Továbbá, egy redukt automorfizmuscsoportjára teljesül a következő zártsági feltétel: ha $g_1, g_2, \ldots \in \mathrm{Aut}(R)$ permutációk egy sorozata a redukt automorfizmuscsoportjából, amelyekre teljesül, hogy a struktúra minden a elemére van olyan j index és b_a elem, hogy minden $n > j$ indexre $g_n(a) = b_a$, akkor a $g_1, g_2, \ldots$ sorozat határértéke, a $h(x) = b_x$ permutáció is benne van az automorfizmuscsoportban.

Azonban ω-kategorikus struktúrák esetén ennél erősebb is igaz: a struktúra automorfizmuscsoportját tartalmazó zárt részcsoportok bijekcióban állnak a reduktok kölcsönös definiálhatóságra vett ekvivalenciaosztályaival, így ω-kategorikus struktúrák esetén a reduktok klasszifikálása ekvivalens a struktúra automorfizmuscsoportját tartalmazó zárt részcsoportok osztályozásával.

Számos ω-kategorikus homogén struktúrának sikerült osztályozni a reduktjait kölcsönös definiálhatóság erejéig. Kölcsönös definiálhatóság erejéig öt különböző reduktja van például a racionális számoknak a szokásos rendezésükkel ellátva [6], a véletlen gráfnak [14], a véletlen turnamentnek [2] és a véletlen poszetnek [12]. A klasszifikáció ismert a konstanssal ellátott Henson-gráfokra is [13]. A homogén rendezett gráfnak viszont már több mint 40 [3], a racionális számoknak a rendezéssel és egy konstanssal ellátva már 116 [10], a véletlen gráfnak egy konstanssal ellátva pedig már több mint 300 reduktja van. Ez utóbbira nem is ismert a teljes klasszifikáció. Ennek alapján megfogalmazható, hogy minél több eleme van a nyelvnek, várhatóan annál nagyobb lesz a reduktok száma, és ez egyszerűnek tűnő struktúrákra is meglepően nagy tud lenni. Mivel a $\mathfrak{Ba}$ nyelve több jelet tartalmaz az itt felsorolt struktúrák nyelveinél, így itt is sok reduktra lehet számítani.

Az eddigi klasszifikációkban az a közös, hogy a vizsgált struktúrák nyelve minden esetben véges, és nem tartalmaz függvényjeleket. A legtöbb klasszifikáció ad hoc számolásokat használ, újabban Bodirsky és Pinsker munkája nyomán Ramsey-elméleti módszereket alkalmaztak sikerrel [4]. Az általunk vizsgált struktúrák ezzel szemben nem írhatóak le véges relációs nyelven. Így az eddig ismert módszerek nem működnek.

Az általunk vizsgált funkcionális reduktokon hasonlóan értelmezhető egy kvázirendezés: $\mathcal{C}_1 \lesssim \mathcal{C}_2$ pontosan akkor, ha $\mathcal{C}_2$ minden művelete definiálható $\mathcal{C}_1$ feletti elsőrendű formulákkal. Ezekre is igaz, hogy automorfizmuscsoportjuk zárt, és ω-kategorikus esetben ha két funkcionális redukt automorfizmuscsoportja megegyezik, akkor azok elsőrendű formulákkal kölcsönösen definiálhatóak egymásból. Azonban a funkcionális reduktok ekvivalenciaosztályai nem állnak bijekcióban a zárt csoportokkal: létezhetnek olyan zárt, a struktúra automorfizmuscsoportját tartalmazó csoportok, amelyek nem állnak elő funkcionális redukt automorfizmuscsoportjaként.

Egy algebra felett előfordulhat, hogy létezik olyan függvény, amely definiálható az algebra műveleteivel elsőrendű formulákkal, de nem kifejezésfüggvény. Ilyenre példa, ha egy háló alaphalmazát tekintjük, amelyen csak a $\wedge$ művelet adott: a $\vee$ művelet definiálható elsőrendű formulával: $a \vee b = c \Leftrightarrow (\forall d)\big((d \wedge a = a$ *és* $d \wedge b = b) \to d \wedge c = c\big)$, viszont nem kifejezésfüggvény. Tehát két különböző $\mathcal{C}_1$ és $\mathcal{C}_2$ funkcionális reduktnak lehet azonos automorfizmuscsoportja.

Az ω-kategorikus struktúrák elméletében fontos szerepet tölt be az alábbi tétel [9]:

2. tétel (Engeler, Ryll–Nardzewski, Svenonius)**.** *Egy $\mathfrak{A}$ struktúra pontosan akkor ω-kategorikus, ha* $\mathrm{Aut}(\mathfrak{A})$ *oligomorf.*

A 2. tétel egyszerű következményei az alábbiak:

3. következmény. *Legyen $\mathfrak{A}$ egy ω-kategorikus struktúra és R egy olyan reláció $\mathfrak{A}$ alaphalmazán, amelyet minden* $\mathrm{Aut}(\mathfrak{A})$*-beli permutáció megőriz. Ekkor R definiálható egy $\mathfrak{A}$ feletti elsőrendű formulával.*

4. következmény. *Legyen $\mathcal{C}, \mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_k$ néhány funkcionális reduktja $\mathfrak{Ba}$-nak. Ekkor a következő két feltétel ekvivalens:*

- $\mathrm{Aut}(\mathcal{C}_1) \cap \mathrm{Aut}(\mathcal{C}_2) \ldots \cap \mathrm{Aut}(\mathcal{C}_k) = \mathrm{Aut}(\mathcal{C})$.
- *$\mathcal{C}_1 \cup \mathcal{C}_2 \ldots \cup \mathcal{C}_k$ minden művelete definiálható $\mathcal{C}$-ből, és $\mathcal{C}$ minden művelete definiálható $\mathcal{C}_1 \cup \mathcal{C}_2 \ldots \cup \mathcal{C}_k$-ból.*

2. A nemlineáris funkcionális reduktok

A dolgozat további részében a $\mathfrak{Ba}$ megszámlálható atommentes Boole-algebra funkcionális reduktjait fogjuk klasszifikálni kölcsönös definiálhatóság erejéig. Mivel ez a sruktúra ω-kategorikus, így elegendő azon $\mathrm{Aut}(\mathfrak{Ba}) \leq G \leq \mathrm{Sym}(\mathfrak{Ba})$ csoportokat meghatározni, amelyek előállnak valamilyen funkcionális redukt automorfizmuscsoportjaként. A struktúrával mint Boole-gyűrűvel fogunk dolgozni; az elsőrendű kölcsönös definiálhatóság önmagában nem lenne elégséges, de a Boole-algebra és a Boole-gyűrű kifejezésfüggvényei megegyeznek, így ez megengedett.

Ebben a fejezetben a $\mathfrak{Ba}$ megszámlálható atommentes Boole-algebra nemlineáris funkcionális reduktjait klasszifikáljuk. Ehhez meghatározzuk a $\mathrm{Sym}(\mathfrak{Ba})$-nak az $\mathrm{Aut}(\mathfrak{Ba})$-t tartalmazó olyan zárt részcsoportjait, melyek megőriznek valamilyen nemlineáris kifejezésfüggvényt.

Legyen $f(x,y)$ egy kétváltozós kifejezésfüggvény. Ekkor $f(x,y)$ felírható az 1, x, y, xy monomok közül valahány összegeként, mivel minden Boole-gyűrű kommutatív, és minden elem idempotens a szorzásra nézve.

5. lemma. *Ha* $\mathrm{Aut}(\mathfrak{Ba}) \leq G \leq \mathrm{Sym}(\mathfrak{Ba})$ *megőriz valamilyen* $f(x,y)$ *nemlineáris kétváltozós kifejezésfüggvényt, akkor* $G = \mathrm{Aut}(\mathfrak{Ba})$.

Bizonyítás. Ha egy φ permutáció megőrzi az $xy = x \wedge y$ vagy az $xy + x + y = x \vee y$ műveletek valamelyikét, akkor φ automorfizmus. Ez azért igaz, mert minden hálót meghatároz önmagában egy is a $\wedge$ és a $\vee$ műveletek közül, és egy Boole-algebra háló ezekre a műveletekre.

- Legyen $f(x,y) = xy + x$, ekkor $f\big(x, f(x,y)\big) = x(xy+x) + x = xy$ miatt minden f-et megőrző permutáció automorfizmus, ugyanez igaz az $xy + y$ műveletre is.
- Legyen $g(x,y) = xy + x + 1$, ekkor $g(g(x,y),y) = (xy + x + 1)y + (xy + x + 1) + 1 = xy + x + y$ miatt minden g-t megőrző permutáció automorfizmus, ugyanez igaz az $xy + y + 1$ műveletre is.
- Legyen $h(x,y) = xy + 1$, ekkor $h\big(h(x,x), h(y,y)\big) = (xx+1)(yy+1) + 1 = xy + x + y$ miatt minden h-t megőrző permutáció automorfizmus.
- Végül legyen $k(x,y) = xy + x + y + 1$, ekkor $k\big(k(x,x), k(y,y)\big) = (x+1)(y+1) + (x+1) + (y+1) + 1 = xy$ miatt minden k-t megőrző permutáció is automorfizmus.

Ezzel a felsorolással az összes esetet ellenőriztük. ■

Ha f egy tetszőleges Boole-függvény, melynek aritása k, akkor

$$f(x_1, \ldots, x_k) = \sum_{\vec{\varepsilon} \in {}^k 2} \alpha_{\vec{\varepsilon}} \prod_{i=1}^{k} x_i^{\varepsilon_i}$$

alakban is felírható, ahol minden $\alpha_{\vec{\varepsilon}}$ értéke 0 vagy 1. A továbbiakban egy $\vec{\varepsilon}$ k hosszú $0-1$ vektorra $|\vec{\varepsilon}|$ jelöli $\sum_{i=1}^{k} \varepsilon_i$-t.

Jelölje továbbá $f_{x_i x_j}(x_1, \ldots, x_{k-1}) = f(x_1, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_k)$ amikor f-ben x_j helyébe x_i-t helyettesítünk. Amennyiben ez nem okoz félreértést, $f_{x_i x_j}$ helyett írhatunk f_{ij}-t. Szükségünk lesz az alábbi definícióra is:

6. definíció. A $\mathfrak{Ba}$ struktúra egy c elemével való eltoláson a $t_c(a) = a + c$ permutációt értjük. Az összes eltolás csoportját T-vel fogjuk jelölni: $T = \{t_c : c \in \mathfrak{Ba}\}$.

Most karakterizáljuk a háromváltozós nemlineáris kifejezésfüggvények lehetséges automorfizmuscsoportjait:

7. lemma. *Legyen* $f(x,y,z) = \alpha_7 xyz + \alpha_6 xy + \alpha_5 yz + \alpha_4 zx + \alpha_3 x + \alpha_2 y + \alpha_1 z + \alpha_0$ *egy nemlineáris háromváltozós kifejezésfüggvény. Ekkor minden olyan* φ *permutációra, amely eleme* $\mathrm{Aut}(f)$*-nek, a következő két lehetőség egyike teljesül:*

- φ *eleme* $\mathrm{Aut}(\mathfrak{Ba})$*-nak*
- φ *előáll egy* $\mathrm{Aut}(\mathfrak{Ba})$*-beli elemnek és egy nem-identikus eltolásnak a kompozíciójaként.*

Bizonyítás. Ha az f_{xy}, f_{yz}, f_{zx} függvények legalább egyike nemlineáris, akkor az 5. lemma miatt készen vagyunk.

- Ha $\alpha_7 = 1$ és $\alpha_6 = \alpha_5$ akkor f_{yz} nemlineáris. Az $\alpha_5 = \alpha_4$ és a $\alpha_4 = \alpha_6$ alesetek hasonlóak, és ezek közül legalább az egyik fennáll.
- Ha $\alpha_7 = 0$ és α_4, α_5, α_6 mindegyike 0, akkor bármely két változó azonosítása nemlineáris függvényt eredményez.
- Ha $\alpha_7 = 0$ és α_4, α_5, α_6 közül pontosan az egyik 1, feltehetjük, hogy α_4 az, akkor f_{yz} megfelel.
- Ha $\alpha_7 = 0$ és α_4, α_5, α_6 közül pontosan az egyik 0, feltehetjük, hogy α_4 az, akkor f_{xy} megfelel.
- Ha $\alpha_7 = 0$ és α_4, α_5, α_6 mindegyike 1, úgy $f(x,y,z) = xy + yz + zx + \alpha_3 x + \alpha_2 y + \alpha_1 z + \alpha_0$ alakú. Ekkor ha α_1, α_2, α_3 között az 1-esek száma 0 vagy 2, az $f(x+c, y+c, z+c) = xy + yz + zx + c + \alpha_3 x + \alpha_3 c + \alpha_2 y + \alpha_2 c + \alpha_1 z + \alpha_1 c + \alpha_0 = f(x,y,z) + (\alpha_1 + \alpha_2 + \alpha_3 + 1)c$ azonosság miatt minden $c \in \mathfrak{Ba}$ elemre a $t_c(a) = a + c$ eltolás megőrzi f-et. Legyen φ tetszőleges f-et megőrző permutáció. Definiáljuk a $\tilde{\varphi} = t_{\varphi(0)} \circ \varphi$ permutációt ($\tilde{\varphi}(x) = \varphi(x) + \varphi(0)$), megmutatjuk, hogy $\tilde{\varphi}$ eleme $\mathrm{Aut}(\mathfrak{Ba})$-nak. A $\tilde{\varphi}$ permutáció megőrzi f-et, és $\tilde{\varphi}(0) = 0$, így megőrzi a $g(x,y) = f(x,y,0)$ függvényt is, ami viszont egy nemlineáris kétváltozós kifejezésfüggvény, így $\tilde{\varphi} \in \mathrm{Aut}(\mathfrak{Ba})$ az 5. lemma miatt. A $t^{-1}_{\varphi(0)} \circ \tilde{\varphi} = \varphi$ egy a keresett típusú felbontása φ-nek.
- Ha pedig $\alpha_7 = 0$, és α_4, α_5, α_6 mindegyike 1, és α_1, α_2, α_3 között páratlan sok 1 van, akkor $f(a,a,a) = (f_{yz})_{xy}(a) = 0$ vagy $f(a,a,a) = 1$ minden $a \in \mathfrak{Ba}$-ra, ezért a $g(x,y) = f\big(x, y, f(x,x,x)\big)$ függvény egy nemlineáris kétváltozós kifejezésfüggvény, így minden az f-et, és így g-t is megőrző φ permutációra $\varphi \in \mathrm{Aut}(\mathfrak{Ba})$ az 5. lemma miatt. ■

Tehát ha $f(x,y,z) = xy + yz + zx + \alpha_3 x + \alpha_2 y + \alpha_1 z + \alpha_0$ alakú, ahol α_1, α_2, α_3 között az 1-esek száma 0 vagy 2, akkor az alábbi két feltétel ekvivalens:

- Egy φ permutáció megőrzi az f függvényt.
- Egy φ permutáció előáll $\varphi = t \circ \psi$ alakban, ahol t egy eltolás, és $\psi \in \mathrm{Aut}(\mathfrak{Ba})$.

Jelöljük M-mel a mediáns műveletét: $M(x,y,z) = xy + yz + zx$, továbbá jelölje $\mathrm{Aut}(M)$ a mediáns műveletét megőrző permutációk csoportját.

8. tétel. $\mathrm{Aut}(M) = T \rtimes \mathrm{Aut}(\mathfrak{Ba})$

Bizonyítás. Mivel $\mathrm{Aut}(M)$ minden eleme megőrzi $M(x,y,z) = xy + yz + xz$-et, így $\mathrm{Aut}(M)$ minden φ eleme előáll $\varphi = t \circ \psi$ alakban ($t \in T$ és $\psi \in \mathrm{Aut}(\mathfrak{Ba})$) a 7. lemma alapján. Továbbá $\mathrm{Aut}(\mathfrak{Ba})$ és T minden eleme megőrzi a mediánst, így $\mathrm{Aut}(M) = \big\langle \mathrm{Aut}(\mathfrak{Ba}), T \big\rangle$.

Az $\mathrm{Aut}(\mathfrak{Ba})$ és T csoportoknak egyetlen közös eleme van, az identitás, mert $\mathrm{Aut}(\mathfrak{Ba})$ minden eleme fixálja a 0-t, és az identitás az egyetlen 0-t fixáló eltolás. Be kell még látnunk, hogy T normálosztó, ehhez elég megmutatni, hogy tetszőleges $t_c \in T$ és $\varphi \in \mathrm{Aut}(\mathfrak{Ba})$ esetén $\varphi^{-1} \circ t_c \circ \varphi \in T$, amit az alábbi számolás bizonyít: $(\varphi^{-1} \circ t_c \circ \varphi)(x) = \varphi^{-1}\big(\varphi(x) + c\big) = (\varphi^{-1} \circ \varphi)(x) + \varphi^{-1}(c) = t_{\varphi^{-1}(c)}(x)$. ■

A háromnál több változós nemlineáris kifejezésfüggvények esetét vissza fogjuk vezetni a legfeljebb három változós esetre.

9. lemma. *Legyen f egy nemlineáris Boole-függvény, amelynek aritása k, és k legalább 4. Ekkor léteznek olyan $1 \leq i < j \leq k$ indexek melyekre f_{ij} is nemlineáris.*

Bizonyítás. Három alesetre bontunk:

- Ha van olyan $\vec{\varepsilon}$ amelyre $2 \leq |\vec{\varepsilon}| \leq k-2$ és $\alpha_{\vec{\varepsilon}} = 1$. Ekkor léteznek olyan $1 \leq i < j \leq k$ indexek, melyekre $\vec{\varepsilon}_i = \vec{\varepsilon}_j = 0$. Erre az $\vec{\varepsilon}$-ra az f_{ij} függvényben is teljesül $\alpha_{\vec{\varepsilon}} = 1$ (így f_{ij} is nemlineáris), mivel az x_i-nek x_j helyébe való behelyettesítése változatlanul hagyja azokat a monomokat, melyek sem x_i-t sem x_j-t nem tartalmazzák, és ilyenek nem képződnek más monomokból a behelyettesítés során.
- Ha az egyetlen legalább másodfokú tag az összes változó szorzata, akkor bármelyik $i,\ j$ pár megfelelő.
- Ha pedig minden legalább másodfokú monom foka legalább $k-1$, és van $(k-1)$-ed fokú monom, akkor legyen $\vec{\varepsilon}$ egy ilyen $(k-1)$-ed fokú monomhoz tartozó vektor. Legyenek továbbá $1 \leq i < j \leq k$ olyan indexek, melyekre $\vec{\varepsilon}_i = \vec{\varepsilon}_j = 1$. Ekkor az f-nek $\vec{\varepsilon}$-hez tartozó monomjából az f_{ij}-nek egy $(k-2)$-ed fokú monomja lesz, amelynek együtthatója nem lehet 0, mivel a helyettesítéssel csak f-nek a $(k-1)$-ed fokú monomjaiból képződhet $(k-2)$-ed fokú, és azok közül is csak a kiindulásiból. ■

Ennek alapján, ha f tetszőleges nemlineáris kifejezésfüggvény, akkor a 9. lemma miatt létezik olyan g nemlineáris kifejezésfüggvény, amely legfeljebb három változós, és $\mathrm{Aut}(\mathfrak{Ba}) \leq \mathrm{Aut}(f) \leq \mathrm{Aut}(g)$, tehát az 5. és a 7. lemmák alapján $\mathrm{Aut}(\mathfrak{Ba}) \leq \mathrm{Aut}(f) \leq \mathrm{Aut}(M)$. Most megmutatjuk, hogy valamelyik tartalmazás helyén egyenlőségnek kell állnia.

10. lemma. *Legyen f nemlineáris kifejezésfüggvény. Ekkor* $\mathrm{Aut}(f) = \mathrm{Aut}(\mathfrak{Ba})$ *vagy* $\mathrm{Aut}(f) = \mathrm{Aut}(M)$.

Bizonyítás. Legyen $G = \mathrm{Aut}(f)$. Mivel $\mathrm{Aut}(M) = T \rtimes \mathrm{Aut}(\mathfrak{Ba})$ és $\mathrm{Aut}(\mathfrak{Ba}) \leq G \leq \mathrm{Aut}(M)$, ezért G-t egyértelműen meghatározza a $T \cap G$ részcsoport. Legyen $c, d \in \mathfrak{Ba}$ olyan elemek, amelyek egy orbitra esnek $\mathrm{Aut}(\mathfrak{Ba})$ szerint. Tegyük fel, hogy $t_c \in G$, megmutatjuk, hogy ekkor $t_d \in G$ is fennáll. Legyen $\varphi \in \mathrm{Aut}(\mathfrak{Ba})$ olyan, hogy $\varphi(d) = c$ ekkor: $(\varphi^{-1} \circ t_c \circ \varphi)(x) = \varphi^{-1}\big(\varphi(x) + c\big) = (\varphi^{-1} \circ \varphi)(x) + \varphi^{-1}(c) = t_d(x)$. Mivel $\mathfrak{Ba}$-nak a nem 0 vagy 1 elemei azonos $\mathrm{Aut}(\mathfrak{Ba})$ szerinti orbitra esnek, és $t_c \in T \cap G$ egyszerre teljesül az összes azonos orbiton lévő c-re, így a $T \cap G$ részcsoport az alábbi négy egyike lehet (felhasználva, hogy $t_0 = \mathrm{id} \in G$):

- $T \cap G = \big\{t_c \mid c \in \{0\}\big\}$;
- $T \cap G = \big\{t_c \mid c \in \{0,1\}\big\}$;
- $T \cap G = \big\{t_c \mid c \in \mathfrak{Ba} \setminus \{1\}\big\}$;
- $T \cap G = \{t_c \mid c \in \mathfrak{Ba}\}$.

Ezek közül az első a $G = \mathrm{Aut}(\mathfrak{Ba})$, a negyedik a $G = \mathrm{Aut}(M)$ esetnek felel meg, a második és a harmadik lehetőségről pedig megmutatjuk, hogy nem állhatnak fenn.

A harmadik lehetőséget kizárja, hogy a $T \cap G = \{t_c \mid c \in \mathfrak{Ba} \setminus \{1\}\}$ halmaz nem is részcsoport: legyen $a \in \mathfrak{Ba} \setminus \{0,1\}$, ekkor t_a és t_{a+1} is eleme $T \cap G$-nek, így a kompozíciójuk $(t_{a+1} \circ t_a)(x) = x + a + a + 1 = t_1(x)$ is eleme kellene, hogy legyen.

A második lehetőség megad egy létező $\mathrm{Aut}(\mathfrak{Ba}) \leq G \leq \mathrm{Aut}(M)$ zárt csoportot, erről kell belátnunk, hogy nem áll elő funkcionális redukt automorfizmuscsoportjaként. Jelölje $\mathfrak{B}_2$ a kételemű Boole-algebrát. Legyen f olyan kifejezésfüggvény, melyet megőriz a t_1 permutáció. Ekkor az $f(x_1+1, x_2+1, \ldots, x_k+1) = f(x_1, x_2, \ldots, x_k)+1$ és az $f(x_1+0, x_2+0, \ldots, x_k+0) = f(x_1, x_2, \ldots, x_k)+0$ azonosságok is teljesülnek f-re, azaz az $f(x_1+c, x_2+c, \ldots, x_k+c) = f(x_1, x_2, \ldots, x_k)+c$ azonosság teljesül minden $c \in \mathfrak{B}_2$-re. Tehát ez az azonosság teljesül a $\mathfrak{B}_2$ által generált varietás minden algebrájában, így $\mathfrak{Ba}$-ban is. Így ha $G = \mathrm{Aut}(f)$ valamilyen f nemlineáris kifejezésfüggvényre, akkor $t_1 \in \mathrm{Aut}(f)$-ből következik, hogy $t_c \in \mathrm{Aut}(f)$ tetszőleges c-re. ■

A 3. következmény alapján így egy f nemlineáris kifejezésfüggvényre az alábbi két eset pontosan egyike teljesül:

- Az f művelet és a szorzás művelete kölcsönösen definiálható egymásból.
- Az f művelet és a mediáns művelete kölcsönösen definiálható egymásból.

Ezzel befejeztük a nemlineáris kifejezésfüggvényeket megőrző permutációk leírását.

3. A lineáris funkcionális reduktok

Ebben a fejezetben a lineáris funkcionális reduktokat fogjuk meghatározni, kölcsönös definiálhatóság erejéig.

Minden lineáris kifejezésfüggvény $l(x_1, x_2, \ldots, x_k) = x_1 + x_2 + \ldots + x_k + \alpha$ alakú, ahol $\alpha = 0$ vagy $\alpha = 1$.

Tekintsük az alábbi nyolc kifejezésfüggvényt:

(1) 0,
(2) 1,
(3) x,
(4) $\neg(x) = x + 1$,
(5) $+_0(x, y) = x + y$,
(6) $+_1(x, y) = x + y + 1$,
(7) $\Sigma(x, y, z) = x + y + z$,
(8) $\Sigma_1(x, y, z) = x + y + z + 1$.

Ezekre a lineáris függvényekre mostantól mint **kanonikus lineáris függvényekre** fogunk hivatkozni, annak ellenére, hogy a konstans 1 függvény nem lineáris:

$f(a+b) = 1 \neq 0 = f(a) + f(b)$. A továbbiakban szükségünk lesz ezeknek a függvényeknek az automorfizmuscsoportjaira, most ezek leírása következik.

1. csoport:

Az $f = 0$ esetben $\mathrm{Aut}(0)$ a 0 stabilizátora a $\mathrm{Sym}(\mathfrak{Ba})$ csoportban. Mivel $\mathrm{Aut}(0)$-hoz tetszőleges $\varphi \notin \mathrm{Aut}(0)$ a 0-t nem fixáló permutációt generátorként hozzávéve már az egész $\mathrm{Sym}(\mathfrak{Ba})$-et kapjuk, így ez a csoport maximális valódi részcsoportja $\mathrm{Sym}(\mathfrak{Ba})$-nek.

2. csoport:

Az $f = 1$ esetben $\mathrm{Aut}(1)$ az 1 stabilizátora a $\mathrm{Sym}(\mathfrak{Ba})$ csoportban. Az $\mathrm{Aut}(0)$ csoporthoz hasonlóan ez a csoport is maximális valódi részcsoportja $\mathrm{Sym}(\mathfrak{Ba})$-nek.

3. csoport:

Az $f(x) = x$ esetben $\mathrm{Aut}(x)$ maga a $\mathrm{Sym}(\mathfrak{Ba})$ csoport, amely természetesen tartalmazza az összes redukt automorfizmuscsoportját.

4. csoport:

Az $\neg(x) = x + 1$ esetben tekintsük $\mathfrak{Ba}$ egy tetszőleges $\mathfrak{I}$ maximális ideálját. Definiáljuk a következő két csoportot:

$\mathrm{Sym}_{\{\mathfrak{I}\}}(\mathfrak{Ba})$ jelölje a $\mathrm{Sym}(\mathfrak{I})$ csoportot, annak hatását kiterjesztve $\mathfrak{I}$-ről a teljes $\mathfrak{Ba}$-ra. Egy φ tetszőleges $\mathrm{Sym}(\mathfrak{I})$-beli permutáció hatását a következőképpen terjesszük ki: $\varphi(x) = \varphi(x)$ ha $x \in \mathfrak{I}$, illetve $\varphi(x) = \varphi(x+1) + 1$ ha $x \notin \mathfrak{I}$. Másképpen megfogalmazva, $\mathrm{Sym}_{\{\mathfrak{I}\}}(\mathfrak{Ba})$ az $\mathfrak{I}$ ideált mint halmazt fixáló permutációk csoportja $\mathrm{Sym}(\mathfrak{Ba})$-ban.

$Z_2^{\mathfrak{I}}$ pedig jelölje azt a csoportot, amely pontosan azokból a φ permutációkból áll, amelyekre teljesül, hogy minden $x \in \mathfrak{Ba}$ elemre $\varphi(x) = x$ vagy $\varphi(x) = x + 1$. Ez a $Z_2^{\mathfrak{I}}$ csoport az $\mathfrak{I}$ maximális ideál választásától függetlenül mindig ugyanaz, mert a definíciójában sehol sem szerepel $\mathfrak{I}$. A jelölést az indokolja, hogy $Z_2^{\mathfrak{I}}$ természetes módon izomorf a Z_2 csoport direkt hatványával, ahol az egyes direkttényezők $\mathfrak{I}$ elemeivel vannak indexelve.

Megmutatjuk, hogy $\mathrm{Aut}(\neg) = Z_2^{\mathfrak{I}} \rtimes \mathrm{Sym}_{\{\mathfrak{I}\}}(\mathfrak{Ba})$.

A $Z_2^{\mathfrak{I}}$ csoport normálosztó lesz $\mathrm{Aut}(\neg)$-ban: legyen $\varphi \in Z_2^{\mathfrak{I}}$ és $\psi \in \mathrm{Aut}(\neg)$ két permutáció, megmutatjuk, hogy $\psi^{-1}\varphi\psi$ is eleme $Z_2^{\mathfrak{I}}$-nek. Ez ekvivalens azzal, hogy minden $x \in \mathfrak{Ba}$ elemre $\psi^{-1}\varphi\psi(x)$ egyenlő x-szel vagy $(x+1)$-gyel. Két esetre bontunk:

- Ha $\varphi\big(\psi(x)\big) = \psi(x)$, akkor $\psi^{-1}\varphi\psi(x) = x$.
- Ha $\varphi\big(\psi(x)\big) = \psi(x) + 1$, akkor $\psi^{-1}\varphi\psi(x) = \psi^{-1}\big(\neg\psi(x)\big) = \neg\psi^{-1}\big(\psi(x)\big) = x + 1$.

Továbbá $Z_2^{\mathfrak{I}}$-nek és $\mathrm{Sym}_{\{\mathfrak{I}\}}(\mathfrak{Ba})$-nek a metszete csak az identikus permutációból áll, mivel $Z_2^{\mathfrak{I}}$-ben nincs olyan permutáció, amely $\mathfrak{I}$ valamely elemét egy másik, tőle különböző $\mathfrak{I}$-beli elembe vinné.

Ahhoz, hogy belássuk, hogy $\mathrm{Aut}(\neg)$ előáll a $Z_2^{\mathfrak{I}} \rtimes \mathrm{Sym}_{\{\mathfrak{I}\}}(\mathfrak{Ba})$ szemidirekt szorzatként, megmutatjuk még, hogy minden $\varphi \in \mathrm{Aut}(\neg)$ permutáció előáll egy $\mathrm{Sym}_{\{\mathfrak{I}\}}(\mathfrak{Ba})$-beli és egy $Z_2^{\mathfrak{I}}$-beli permutáció kompozíciójaként. Legyen $\varphi \in \mathrm{Aut}(\neg)$ tetszőleges permutáció, definiáljuk a $\tilde{\varphi}$ permutációt a következőképpen:

- Ha $x \in \mathfrak{I}$, akkor $\tilde{\varphi}(x)$ legyen $\varphi(x)$ és $\varphi(x)+1$ közül az, amelyik $\mathfrak{I}$-be esik.
- Ha $x \notin \mathfrak{I}$, akkor $\tilde{\varphi}(x)$ legyen $\varphi(x)$ és $\varphi(x)+1$ közül az, amelyik nem esik $\mathfrak{I}$-be.

Ekkor $\tilde{\varphi} \in \mathrm{Sym}_{\{\mathfrak{I}\}}(\mathfrak{Ba})$, és $\tilde{\varphi}^{-1} \circ \varphi \in Z_2^{\mathfrak{I}}$, és ezek kompozíciójaként φ előáll.

Tehát minden, a komplementer műveletét tartó permutáció úgy áll elő, hogy az $\{x, x+1\}$ párok halmazán tetszőlegesen hat, majd minden páron belül egymástól függetlenül vagy megcseréli a két elemet, vagy nem.

5. csoport:

A $+_0(x,y) = x+y$ esetben a funkcionális redukt egy vektortér: $\mathbb{F}_2^\infty$. Ennek automorfizmus-csoportja definíció szerint az általános lineáris csoport: $\mathrm{Aut}(+_0) = \mathrm{GL}(\infty, 2)$.

6. csoport:

A $+_1(x,y) = x+y+1$ esetben a redukt szintén egy vektortér, melynek műveletei nem azonosak a $+_0(x,y) = x+y$ vektortér műveleteivel (például $+_0$ nulleleme a 0, $+_1$ nulleleme az 1). Viszont kettejük között megadható egy izomorfizmus: a τ_1 eltolás, ugyanis $\tau_1\big(+_1(x,y)\big) = x+y+1+1 = x+1+y+1 = +_0\big(\tau_1(x), \tau_1(y)\big)$ és $\tau_1^{-1}\big(+_0(x,y)\big) = x+y+1 = +_1\big(\tau_1^{-1}(x), \tau_1^{-1}(y)\big)$. Ennek alapján vezessük be a következő jelölést: $\mathrm{Aut}(+_1) = \mathrm{GL}^1(\infty, 2)$. Izomorf struktúrák automorfizmuscsoportja is izomorf, azaz $\mathrm{Aut}(+_1) = \mathrm{GL}^1(\infty, 2) \cong \mathrm{GL}(\infty, 2) = \mathrm{Aut}(+_0)$.

7. csoport:

A $\Sigma(x,y,z) = x+y+z$ esetben a funkcionális redukt egy affin tér. Legyen $x, y, z, v \in \mathfrak{Ba}$ négy páronként különböző elem. Ezekre $\Sigma(x,y,z) = v$ akkor és csak akkor áll fenn, ha az x, y, z, v elemek egy kétdimenziós affin alteret alkotnak: $\Sigma(x,y,z) = v \Leftrightarrow x+y+z = v$, tehát az $\{x, y, z, v\}$ elemek a $\{0, y+x, z+x, v+x\}$ kétdimenziós lineáris altér x-szel való eltoltját alkotják.

Σ-t megőrzik (az x_0 műveletet is megőrző) $\mathrm{GL}(\infty, 2)$-beli permutációk és az eltolások is. Továbbá a T eltolások csoportja normálosztó $\mathrm{Aut}(\Sigma)$-ban, T és $\mathrm{GL}(\infty, 2)$ együtt generálják az egész $\mathrm{Aut}(\Sigma)$-t, és metszetük csak az identikus permutáció. Azaz az $\mathrm{Aut}(\Sigma)$ automorfizmuscsoport előáll mint a $T \rtimes \mathrm{Aut}(+_0)$ szemidirekt szorzat. Szimmetriaokokból $\mathrm{Aut}(\Sigma)$ mint a $T \rtimes \mathrm{Aut}(+_1)$ szemidirekt szorzat is felírható.

8. csoport:

Végül a $\Sigma_1(x,y,z) = x+y+z+1$ esetben Σ_1 segítségével definiálhatjuk a $\neg(x) = g(x,x,x)$ és a $\Sigma(x,y,z) = \Sigma_1\big(x,y,\neg(z)\big)$ műveleteket. Másrészt $\neg(x)$ és $\Sigma(x,y,z)$ segítségével is definiálhatjuk $\Sigma_1(x,y,z)$-t a következő módon: $\Sigma_1(x,y,z) = \Sigma\big(x,y,\neg(z)\big)$. Tehát a 4. következmény alapján $\mathrm{Aut}(\Sigma_1) = \mathrm{Aut}(\Sigma) \cap \mathrm{Aut}(\neg)$.

Mivel az eltolások megőrzik Σ_1-et, így T részcsoportja $\mathrm{Aut}(\Sigma_1)$-nek. Felhasználva, hogy $T \lhd \mathrm{Aut}(\Sigma)$, a T csoport normálosztó lesz $\mathrm{Aut}(\Sigma_1)$-ban is.

Az $\mathrm{Aut}(+_0) = \mathrm{GL}(\infty,2)$ csoportnak az $\mathrm{Aut}(\Sigma_1)$ csoportba eső része a komplementert tartó lineáris permutációkból áll. Belátjuk, hogy ezek pontosan az 1-et fixáló lineáris permutációk: legyen $\varphi \in \mathrm{Aut}(+_0)$ komplementertartó. Mivel φ fixálja a 0-t, így φ fixálja $\neg 0 = 1$-et is. Fordítva, ha $\varphi \in \mathrm{Aut}(+_0)$ megőrzi az 1-et, akkor megőrzi a komplementerséget is: $\varphi(x+1) = \varphi(x) + \varphi(1) = \varphi(x) + 1$. Az 1-et fixáló lineáris permutációk csoportja megegyezik az $\mathrm{Aut}(+_0) \cap \mathrm{Aut}(+_1)$ csoporttal.

Az előzőekből következik, hogy $\mathrm{Aut}(\Sigma_1) = \mathrm{Aut}(\Sigma) \cap \mathrm{Aut}(\neg) = (T \rtimes \mathrm{Aut}(+_0)) \cap \mathrm{Aut}(\neg) = T \rtimes \big(\mathrm{Aut}(+_0) \cap \mathrm{Aut}(\neg)\big) = T \rtimes \big(\mathrm{Aut}(+_0) \cap \mathrm{Aut}(+_1)\big)$.

11. lemma. *Minden l lineáris kifejezésfüggvényhez létezik pontosan egy f kanonikus lineáris függvény, amelyre teljesül, hogy l és f kölcsönösen definiálhatóak egymásból elsőrendű formulák segítségével.*

Bizonyítás. Legyen $l(x_1,x_2,\ldots,x_k) = x_1 + x_2 + \ldots + x_k + \alpha$.

Először belátjuk olyan f kanonikus lineáris függvény létezését, amelyre f és l kölcsönösen definiálható egymásból, az egyértelműség bizonyítását később végezzük el.

Minden olyan függvény, amelyre $k < 2$, szerepel a listában, így választhatjuk önmagukat a megfelelő f-nek.

Ha $k > 1$ páros szám, akkor az $f(x,y) = x+y+\alpha$ jó választás. Az egyik irányú definiálhatóságot $f(x,y) = l(x,y,y,\ldots,y)$ bizonyítja, a másik irányhoz definiáljuk az alábbi függvényeket rekurzívan: $l_2 = f(x_1,x_2)$ és $j > 2$-re $l_j(x_1,x_2,\ldots,l_j) = f\big(l(x_1,x_2,\ldots,x_{j-1}),x_j\big)$. Ekkor $l = l_k$.

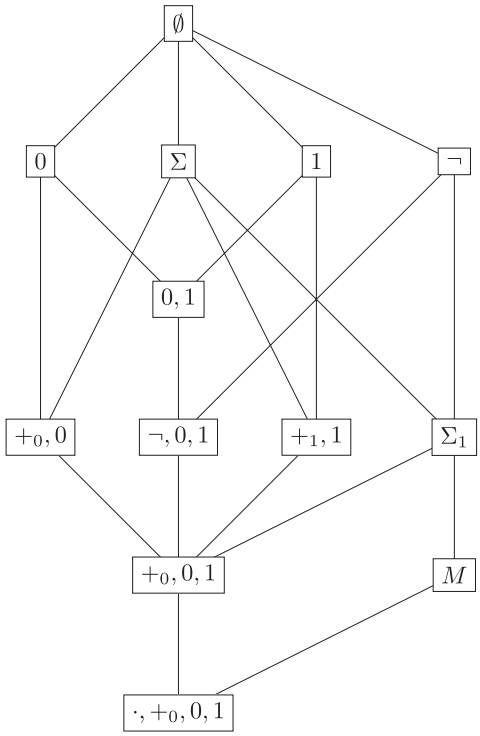
Ha pedig $k > 1$ páratlan szám akkor az $f(x,y,z) = x+y+z+\alpha$ jó választás. Az egyik irányú definiálhatóságot $f(x,y,z) = l(x,y,z,z,\ldots,z)$ bizonyítja, a másik irányhoz definiáljuk az alábbi függvényeket rekurzívan: $l_1 = f(x_1,x_2,x_3)$ és $j > 3$-ra

$$l_j(x_1,x_2,\ldots,x_{2j+1}) =$$
$$= f\big(l(x_1,x_2,\ldots,x_{2j-1}), f(x_{2j},x_{2j},x_{2j}), f(x_{2j+1},x_{2j+1},x_{2j+1})\big).$$

Ekkor $l = l_{(k-1)/2}$.

Be kell látnunk még a megfelelő f egyértelműségét. Ha lenne olyan l lineáris kifejezésfüggvény, amihez több olyan f kanonikus lineáris függvény is létezne, hogy l és f kölcsönösen definiálhatóak egymásból elsőrendű formulák segítségével, akkor ezek az f-ek is kölcsönösen definiálhatóak lennének egymásból, így megegyezne az automorfizmuscsoportjuk is. Ezért a 3. következmény alapján f egyértelműségét bizonyíthatjuk úgy, ha a listánk minden függvényének meghatározzuk az automorfizmuscsoportját, és ezek különbözőnek bizonyulnak.

A nyolc automorfizmuscsoportot jellemeztük ennek a lemmának a kimondása előtt, és különbözőnek bizonyultak. A fejezet további részében pontos tartalmazási viszonyaikat is meg fogjuk határozni, amiből szintén következik, hogy ez a nyolc csoport páronként különböző. ■



1. ábra. A funkcionális reduktok hálója, az automorfizmuscsoportok tartalmazás szerinti rendezésével

Célunk annak megmutatása, hogy a $\mathfrak{Ba}$ megszámlálható atommentes Boole-algebra funkcionális reduktjainak automorfizmuscsoportjai az 1. ábrán látható hálót alkotják a tartalmazásra nézve. Emlékezzünk rá,hogy ennek ismerete azért lehet hasznos, mert segítségével $\mathfrak{Ba}$ feletti kifejezésfüggvények tetszőleges $\mathcal{H}$ halmazára meg tudjuk határozni azokat a kifejezésfüggvényeket, amelyeket ki lehet fejezni $\mathcal{H}$-beli függvényekkel elsőrendű formulák segítségével. Ehhez csak annyit kell tennünk, hogy megkeressük a háló legbővebb olyan csoportját, amelynek minden eleme megőrzi az összes H-beli kifejezésfüggvényt: legyen ez a csoport G. Ekkor H-ból pontosan azok a kifejezésfüggvények fejezhetőek ki elsőrendű formulákkal, amelyeket G megőriz. Az egyes csoportok karakterizációi alapján ezek a kifejezésfüggvények egyszerűen leírhatóak.

Annak megmutatásához, hogy a háló tényleg így néz ki, először bebizonyítjuk a háló koatomjairól, hogy antiláncot alkotnak, majd leírjuk a belőlük metszetképzéssel megkapható elemeket. Legvégül megkeressük annak a két zárt csoportonak

a helyét a hálóban, amelyek nemlineáris függvények automorfizmuscsoportjaként állnak elő.

12. lemma. *A kanonikus lineáris függvények automorfizmuscsoportjaiból metszetképzéssel megkapható csoportok az 1. ábrán látható háló* $\big[\mathrm{Aut}(+_0,0,1),\mathrm{Aut}(\emptyset)\big]$ *intervallumát alkotják a tartalmazásra, mint rendezésre nézve.*

Bizonyítás. Először jellemezzük az adott intervallumban szereplő, eddig még nem leírt három csoportot:

9. csoport:

Az $\mathrm{Aut}(0,1)$ csoport a 0 és 1 elemek pontonkénti stabilizátora. Mivel tetszőleges φ az 1-et nem fixáló permutációt generátorelemként hozzávéve már a teljes $\mathrm{Aut}(0)$-t kapjuk, így $\mathrm{Aut}(0)$-nak maximális valódi részcsoportja. Hasonlóan maximális valódi részcsoportja $\mathrm{Aut}(1)$-nek is.

10. csoport:

Az $\mathrm{Aut}(\neg,0,1)$ csoport értelemszerűen az $\mathrm{Aut}(0)$, $\mathrm{Aut}(1)$ és $\mathrm{Aut}(\neg)$ csoportok metszete. Hasonlóan ahhoz, ahogy $\mathrm{Aut}(\neg)$ előáll a $Z_2^{\mathfrak{I}} \rtimes \mathrm{Sym}_{\{\mathfrak{I}\}}(\mathfrak{Ba})$ szemidirekt szorzatként, $\mathrm{Aut}(\neg,0,1)$ is felbontható: $\mathrm{Aut}(\neg,0,1) = \big(Z_2^{\mathfrak{I}}\big)_0 \rtimes \big(\mathrm{Sym}_{\{\mathfrak{I}\}}(\mathfrak{Ba})\big)_0$. Itt $\big(Z_2^{\mathfrak{I}}\big)_0$ és $\big(\mathrm{Sym}_{\{\mathfrak{I}\}}(\mathfrak{Ba})\big)_0$ a 0 stabilizátorait jelölik a $Z_2^{\mathfrak{I}}$ és a $\mathrm{Sym}_{\{\mathfrak{I}\}}(\mathfrak{Ba})$ csoportokban.

11. csoport:

Az $\mathrm{Aut}(+_0,0,1)$ csoport már előkerült $\mathrm{Aut}(\Sigma_1)$ szemidirekt szorzatként való jellemzésénél. Az 1-et fixáló, vagy ekvivalensen a komplementer műveletét megőrző lineáris permutációk csoportja.

Megmutatjuk, hogy az $\mathrm{Aut}(0)$, $\mathrm{Aut}(1)$, $\mathrm{Aut}(\Sigma)$ és $\mathrm{Aut}(\neg)$ csoportok antiláncot alkotnak.

- Legyenek $a,b \in \mathfrak{Ba} \setminus \{0,1\}$ tetszőleges elemek, melyek nem egymás komplementerei. Ekkor az $(a,a+1,b,1)$ ciklus eleme $\mathrm{Aut}(0)$-nak, jelöljük φ-vel.
  Ekkor $\varphi(1) = a \neq 1$ miatt $\mathrm{Aut}(0) \not\subseteq \mathrm{Aut}(1)$.
  $\varphi(\neg a) = b \neq a = \neg\varphi(a)$ miatt $\mathrm{Aut}(0) \not\subseteq \mathrm{Aut}(\neg)$.
  Illetve $\varphi\big(\Sigma(a,a+1,1)\big) = 0 \neq a+b+1 = \Sigma\big(\varphi(a),\varphi(a+1),\varphi(1)\big)$ miatt $\mathrm{Aut}(0) \not\subseteq \mathrm{Aut}(\Sigma)$.
- Hasonlóan bizonyítható, hogy $\mathrm{Aut}(1) \not\subseteq \mathrm{Aut}(0)$, $\mathrm{Aut}(1) \not\subseteq \mathrm{Aut}(\neg)$ és $\mathrm{Aut}(1) \not\subseteq \mathrm{Aut}(\Sigma)$.
- Most legyenek $a,b \in \mathfrak{Ba} \setminus \{0,1\}$ tetszőleges elemek, melyek nem egymás komplementerei. Ekkor az $(a,b,0,a+1,b+1,1)$ ciklus eleme $\mathrm{Aut}(\neg)$-nak, jelöljük φ-vel. Mivel φ sem a 0-t, sem az 1-et nem fixálja, így $\mathrm{Aut}(\neg) \not\subseteq \mathrm{Aut}(0)$ és $\mathrm{Aut}(\neg) \not\subseteq \mathrm{Aut}(1)$. Továbbá

  $$\varphi\big(\Sigma(a,b,0)\big) = a+b \neq a+b+1 = \Sigma\big(\varphi(a),\varphi(b),\varphi(0)\big)$$

  miatt $\mathrm{Aut}(\neg) \not\subseteq \mathrm{Aut}(\Sigma)$.

- Legyen $\tau_a(x) = x + a$ tetszőleges eltolás. Ekkor τ_a megőrzi Σ-t, viszont $a \neq 0$ esetén τ_a nem fixálja sem a 0-t, sem az 1-et, így $\mathrm{Aut}(\Sigma) \not\subseteq \mathrm{Aut}(0)$ és $\mathrm{Aut}(\Sigma) \not\subseteq \mathrm{Aut}(1)$. Legyen φ olyan $\mathrm{GL}(\infty, 2)$-beli permutáció, amely nem fixálja az 1-et, és így nem tartja a $\neg$ műveletet, mivel $\mathrm{GL}(\infty, 2)$ minden eleme fixálja a 0-t. Mivel $\mathrm{Aut}(+_0) = \mathrm{GL}(\infty, 2) \subset \mathrm{Aut}(\Sigma)$, így $\mathrm{Aut}(\Sigma) \not\subseteq \mathrm{Aut}(\neg)$.

Most az $\mathrm{Aut}(0)$, $\mathrm{Aut}(1)$, $\mathrm{Aut}(\Sigma)$, $\mathrm{Aut}(\neg)$ antilánc elemeiből képezhető metszeteket fogjuk meghatározni. A páronkénti metszetek:

- $\mathrm{Aut}\,0 \cap \mathrm{Aut}\,1 = \mathrm{Aut}\,0, 1$ a stabilizátorok definíciója alapján.
- $\mathrm{Aut}(0) \cap \mathrm{Aut}(\Sigma) = \mathrm{Aut}(+_0) = \mathrm{GL}(\infty, 2)$, a 4. következményt használva a $+_0(x, y) = \Sigma(x, y, 0)$, $0 = +_0(x, x)$ és $\Sigma(x, y, z) = +_0\big(x, +_0(y, x)\big)$ formulák miatt.
- $\mathrm{Aut}(0) \cap \mathrm{Aut}(\neg) = \mathrm{Aut}(\neg, 0, 1)$
- $\mathrm{Aut}(1) \cap \mathrm{Aut}(\Sigma) = \mathrm{Aut}(+_1) = \mathrm{GL}^1(\infty, 2)$ a 4. következményt használva az $+_1(x, y) = \Sigma(x, y, 1)$, $1 = +_1(x, x)$ és $\Sigma(x, y, z) = +_1\big(x, +_1(y, x)\big)$ formulák miatt.
- $\mathrm{Aut}(0) \cap \mathrm{Aut}(\neg) = \mathrm{Aut}(\neg, 0, 1)$.
- $\mathrm{Aut}(\Sigma) \cap \mathrm{Aut}(\neg) = \mathrm{Aut}(\Sigma_1)$ a 4. következményt használva a $\Sigma(x, y, z) = \Sigma_1\big(x, y, \Sigma_1(z, z, z)\big)$, $\neg x = \Sigma_1(x, x, x)$ és $\Sigma_1(x, y, z) = \Sigma(x, y, \neg z)$ formulák miatt.

A hármas metszetek:

- $\mathrm{Aut}(0) \cap \mathrm{Aut}(1) \cap \mathrm{Aut}(\Sigma) = \mathrm{Aut}(+_0, 1)$ a 4. következményt használva a $0 = +_0(x, x)$, $1 = 1$, $\Sigma(x, y, z) = +_0\big(x, +_0(y, x)\big)$, illetve $+_0(x, y) = \Sigma(x, y, 0)$ és $1 = 1$ formulák miatt.
- $\mathrm{Aut}(0) \cap \mathrm{Aut}(1) \cap \mathrm{Aut}(\neg) = \mathrm{Aut}(\neg, 0, 1)$.
- $\mathrm{Aut}(0) \cap \mathrm{Aut}(\Sigma) \cap \mathrm{Aut}(\neg) = \mathrm{Aut}(+_0, 1)$ a 4. következményt használva a $0 = +_0(x, x)$, $\Sigma(x, y, z) = +_0\big(x, +_0(y, x)\big)$, $\neg x = +_0(x, 1)$, illetve $+_0(x, y) = \Sigma(x, y, 0)$ és $\neg 0 = 1$ formulák miatt.
- $\mathrm{Aut}(1) \cap \mathrm{Aut}(\Sigma) \cap \mathrm{Aut}(\neg) = \mathrm{Aut}(+_0, 1)$ a 4. következményt használva az $1 = 1$, $\Sigma(x, y, z) = +_0\big(x, +_0(y, x)\big)$, $\neg x = +_0(x, 1)$, illetve $+_0(x, y) = \Sigma(x, y, \neg 1)$ és $1 = 1$ formulák miatt.

Végül az antilánc mind a négy elemének metszete:

- $\mathrm{Aut}(0) \cap \mathrm{Aut}(1) \cap \mathrm{Aut}(\Sigma) \cap \mathrm{Aut}(\neg) = \mathrm{Aut}(+_0, 1)$ a 4. következményt használva a $0 = +_0(x, x)$, $1 = 1$, $\Sigma(x, y, z) = +_0\big(x, +_0(y, x)\big)$, $\neg x = +_0(x, 1)$, illetve $+_0(x, y) = \Sigma(x, y, 0)$ és $\neg 0 = 1$ formulák miatt.

Ennek alapján minden kanonikus lineáris függvény automorfizmuscsoportja előáll, mint az $\mathrm{Aut}(0)$, $\mathrm{Aut}(1)$, $\mathrm{Aut}(\Sigma)$, $\mathrm{Aut}(\neg)$ antilánc valahány elemének metszete. Az $\mathrm{Aut}(x) = \mathrm{Sym}(\mathfrak{Ba})$ szimmetrikus csoport az üres metszetnek felel meg.

A kanonikus lineáris függvények automorfizmuscsoportjain kívül még három csoport kapható meg metszetként. Ezek $\mathrm{Aut}(0, 1) = \mathrm{Sym}_{(0,1)}(\mathfrak{Ba})$, ami a $\{0, 1\}$ hal-

maz pontonkénti stabilizátora a $\mathrm{Sym}(\mathfrak{Ba})$ csoportban, az $\mathrm{Aut}(\neg, 0, 1)$ csoport, illetve $\mathrm{Aut}(+_0, 1)$, ami az egy konstanssal ellátott vektortér automorfizmuscsoportja: $\mathrm{GL}(\infty, 2) \cap \mathrm{Sym}(\mathfrak{Ba})_1(\mathfrak{Ba})$. Ezek felsorolásunkban a 9., 10. és 11. csoportok. ■

4. A megszámlálható atommentes Boole-algebra funkcionális reduktjai

Ebben a fejezetben befejezzük a funkcionális reduktok kölcsönös definiálhatóság erejéig való klasszifikálását.

Az előző fejezetben meghatároztuk, hogy valahány $l_1, l_2, \ldots$ lineáris kifejezésfüggvényt megőrző permutációk milyen zárt részcsoportokat alkothatnak, ezek a zárt részcsoportok az 1. ábrán látható háló $\big[\{+, 0, 1\}, \emptyset\big]$ intervallumát alkotják a tartalmazásra mint rendezésre nézve. Ezt a hálót fogjuk most kiegészíteni a nemlineáris kifejezésfüggvények által meghatározott lehetséges automorfizmusokkal.

13. tétel. *A $\mathfrak{Ba}$ funkcionális reduktjai az 1. ábrán látható hálót alkotják, ahol a rendezés az automorfizmuscsoportok tartalmazása.*

Bizonyítás. A 10. lemma alapján egy f nemlineáris kifejezésfüggvényre vagy $\mathrm{Aut}(f) = \mathrm{Aut}(\mathfrak{Ba})$, vagy $\mathrm{Aut}(f) = \mathrm{Aut}(M)$. Mivel tudjuk, hogy $\mathrm{Aut}(\mathfrak{Ba})$ a háló minimális eleme, így csak $\mathrm{Aut}(M)$ helyét kell meghatároznunk a hálóban. $T \leq \mathrm{Aut}(M)$ miatt $\mathrm{Aut}(M) \not\subseteq \mathrm{Aut}(0)$ és $\mathrm{Aut}(M) \not\subseteq \mathrm{Aut}(1)$, így annyit kell még belátnunk, hogy $\mathrm{Aut}(M) \leq \mathrm{Aut}(\Sigma_1)$.

A 8. tétel miatt $\mathrm{Aut}(M) \leq \mathrm{Aut}(\Sigma_1)$ bizonyításához elég belátnunk, hogy az eltolások megőrzik Σ_1-et. Legyen $\tau_a(x) = x + a$ tetszőleges eltolás, ekkor

$$\tau_a\big(\Sigma_1(x, y, z)\big) = x + y + z + 1 + a = x + a + y + a + z + a + 1 =$$
$$= \Sigma_1\big(\tau_a(x), \tau_a(y), \tau_a(z)\big),$$

tehát az eltolások megőrzik a Σ_1 műveletet.

A szigorú tartalmazás belátásához kell mutatnunk olyan permutációt, amely megőrzi a Σ_1 műveletet, de nem tartja a mediánst. Ehhez elég mutatni olyan permutációt, ami fixálja a 0-t és az 1-et, továbbá tartja a $+_0$ műveletét, viszont nem Boole-algebra automorfizmus. Ilyen tulajdonságú permutáció létezik: ha $a, b \in \mathfrak{Ba}$ olyan elemek, melyekre $a < b$, akkor $a, b, 1$ lineárisan független elemek, így van olyan permutáció a lineáris csoportban, amely a-t és b-t megcseréli, az 1-et pedig fixálja. ■

Tehát tudjuk, hogy a $\mathfrak{Ba}$ funkcionális reduktjai az 1. ábrán látható hálót alkotják, ahol a rendezés az automorfizmuscsoportok tartalmazása. Ennél azonban több is igaz:

14. tétel. *Az 1. ábrán látható háló részhálója* $\mathrm{Sym}(\mathfrak{Ba})$ *részcsoporthálójának, azaz zárt részcsoportok hálóbeli egyesítése* $\mathrm{Sym}(\mathfrak{Ba})$ *általuk generált részcsoportjának felel meg.*

A 14. tétel nem teljesül minden homogén ω-kategorikus algebrai struktúrára.

Felmerül a kérdés, hogy tetszőleges Boole-algebrának mik a funkcionális reduktjai kölcsönös definiálhatóság erejéig.

Probléma. Legyen $\mathfrak{B}$ tetszőleges Boole-algebra. Ha $\mathfrak{B}$-nek legalább 16 eleme van, akkor ugyanazok a funkcionális reduktjai, mint a $\mathfrak{Ba}$ megszámlálható atommentes Boole-algebrának.

Ha a $\mathfrak{B}$ Boole-algebrának kevés eleme van, akkor olyan funkcionális reduktok is kölcsönösen definiálhatóak lehetnek egymásból, amelyek a $\mathfrak{Ba}$ megszámlálható atommentes Boole-algebra esetén nem. Például ha $\mathfrak{B}_2$ a kételemű Boole-algebra, akkor csak a 0 konstans segítségével definiálható az 1: $(x = 1) \Leftrightarrow (x \neq 0)$.

Amennyiben a fenti problémára a válasz igenlő, úgy annak bizonyításában jóval kisebb szerepet kell kapniuk az automorfizmuscsoportokat használó technikáknak.

Irodalom

[1] N. Ackerman, C. Freer, R. Patel, *Invariant measures concentrated on countable structures.* Preprint arXiv:1206.4011 [math.LO] (2012).

[2] J. H. Bennett, *The reducts of some infinite homogeneous graphs and tournaments.* Rutgers university, doktori értekezés (1997).

[3] M. Bodirsky, M. Pinsker, A. Pongrácz, *The 42 reducts of the random ordered graph,* beküldve (2013).

[4] M. Bodirsky, M. Pinsker, Reducts of Ramsey Structures, *Model Theoretic Methods in Finite Combinatorics,* American Mathematical Society, Contemporary Mathematics, **558** (2011), 489–519.

[5] P. J. Cameron, *Oligomorphic permutation groups.* London Mathematical Society Lecture Note Series, 152. Cambridge University Press (Cambridge, 1990).

[6] P. J. Cameron, Transitivity of permutation groups on unordered sets, *Mathematische Zeitschrift,* **148** (1976), 127–139.

[7] R. Fraïssé, Sur certaines relations qui généralisent l'order des nombres rationnels, *Comptes Rendus d' l'Académie des Sciences de Paris,* **237** (1953), 540–542.

[8] C. W. Henson, A family of countable homogeneous graphs, *Pacific Journal of Mathematics,* **38** (1971), 69–83.

[9] W. Hodges, *Model theory.* Encyclopedia of Mathematics and its Applications, 42. Cambridge University Press (Cambridge, 1993).

[10] M. Junker, M. Ziegler, The 116 reducts of $(Q, <, a)$, *J. Symbolic Logic,* **73** no. 3 (2008), 861–884.

[11] D. Macpherson, A survey of homogeneous structures, *Discrete Mathematics,* **311(15)** (2011), 1599–1634.

[12] P. P. Pach, M. Pinsker, G. Pluhár, A. Pongrácz, Cs. Szabó, Reducts of the random partial order, *Advances in Mathematics,* **267** (2014), pp. 94–120.

[13] A. Pongrácz, Reducts of the Henson graphs with a constant, *Annals of Pure and Applied Logic* (2013), accepted.

[14] S. Thomas, Reducts of the random graph, *Journal of Symbolic Logic,* **56(1)** (1991), 176–181.

Bertalan Bodor, Kende Kalina: Functional reducts of the countable homogeneous Boolean algebra

Let $\mathfrak{A} = (A, f_1, \dots f_n)$ be an algebra on the set A with operations $f_1, \dots, f_n$. A functional reduct of $\mathfrak{A}$ is a structure $\mathfrak{B} = (A, t_1, \dots, t_k)$ on the same set A and with operations $t_1, \dots, t_k$ such that every t_j is a term function of $\mathfrak{A}$. In this paper we classify the functional reducts of the homogeneous countable Boolean algebra. We show that there are 13 such reducts.

Bodor Bertalan

Eötvös Lóránd Tudományegyetem,
Algebra és Számelmélet Tanszék,
1117 Budapest,
Pázmány Péter sétány 1/c
bodorb@cs.elte.hu

Kalina Kende

Eötvös Lóránd Tudományegyetem,
Algebra és Számelmélet Tanszék,
1117 Budapest,
Pázmány Péter sétány 1/c
kkalina@cs.elte.hu