BONYOLULTSÁGELMÉLET ÉS ALGEBRA

AZ OTKA K67870 PÁLYÁZAT ZÁRÓJELENTÉSE

A pályázat résztvevői az algebra és a bonyolultságelmélet határterületét kutatták. A pályázat időtartama alatt **43** publikáció született, jelentős részük magas színvonalú külföldi folyóiratban. Az elért eredményeket témánként és dolgozatonként taglaljuk.

Az ún. relációhomomorfizmus-problémák (Constraint Satisfaction Problem, röviden CSP) vizsgálata a nyolcvanas évek óta a számítástudomány egyik fő kérdése, de ezek a logikában és a gráfelméletben is központi szerepet játszanak. Egy rögzített R relációs struktúrára $CSP(R)$ inputja egy S, azonos típusú relációs struktúra, a kérdés pedig az, hogy létezik-e S-ből R-be homomorfizmus (azaz olyan leképezés, ami relációban álló elemeket relációban állókba képez).

A terület fő sejtése Feder és Vardi dichotómia sejtése, mely szerint minden CSP probléma vagy polinomiálisan eldönthető, vagy NP-teljes. Feder és Vardi belátták, hogy a CSP problémák osztályánál bővebb, másodrendű egzisztenciális formulákkal definiált úgynevezett Monotone Monadic Strict NP osztály minden problémája egy CSP problémával véletlen értelemben polinomiálisan ekvivalens. Kunnak [21] sikerült determinisztikus bizonyítást adnia ugyanerre, belátva, hogy a fenti osztályok polinomiálisan ekvivalensek. A bizonyítás kulcsa egy expander koncepció bevezetése hipergráfokra, majd ilyen korlátos fokszámú és rövid kör nélküli expanderek hatékony konstrukciója. Az expander gráfok az elmúlt évtizedben fontos szerepet játszottak a csoportelmélettől a számelméleten át a számítástudományig: gyakran a legfontosabb eredmények fő eszközeként. Hipergráfok esetében az expandereknek még nincs egységes elmélete, és túl sok alkalmazás sem ismert, így a bizonyításnak ez a része önálló érdeklődésre is számot tart.

Kun prágai társszerzőjével közösen kombinatorikus jellemzést ad az NP és MMSNP osztályokra [23], [24], [25]. Munkájuk rávilágít, hogy kombinatorikus problémák bizonyos intenzíven kutatott osztályainál nem várható a remélt dichotómia. Homomorfizmus dualitások segítségével jellemzik azokat az MMSNP problémákat, melyek a CSP osztályba esnek. Kapcsolódó munkájukban Kun és kanadai társszerzője véletlen módszerekkel belátják, hogy irányított gráfok duálisa exponenciálisan nagy is lehet.

Kun egy másik társszerzővel [27], [28] az ismert CSP dichotómia sejtés egy statisztikus ekvivalensét adja. Ezt felhasználva az irányítatlan gráfok dichotómiájára vonatkozó Hell–Nešetřil tétel egy teljesen új bizonyítását adják diszkrét Fourier analitikus eredményeket felhasználva. Összekötik a diszkrét Fourier analízis, a CSP problémák és a diszkrét kvadratikus dinamikai rendszerek elméletét. Munkájuk fontos híd a CSP problémákat algebrai illetve analitikus, számítástudományi oldalról vizsgálók közt: cikkükre már számos hivatkozás született.

A CSP problémák algebrai megközelítése a struktúra egy hatványából a struktúrába menő homomorfizmusok (ún. polimorfizmusok) vizsgálatán alapul. Az első ismert eredmény ezekről Greenwell és Lovász tétele, miszerint a teljes gráf minden polimorfizmusa csak egy koordinátától függ. Kun egy társszerzővel ezt kiterjeszti (triviális kivételektől eltekintve) a teljes gráf egy hatványának minden, a koordináták és a gráf permutációjára zárt részhalmazára [22].

Az elméleti számítástudomány egyik legünnepeltebb tétele (amiért 2001-ben Arora, Feige, Goldwasser, Lund, Lovász, Motwani, Safra, Sudan és Szegedy Gödel-díjat kaptak) az ún. PCP tétel (Probabilistically Checkable Proof rövidítése). Ez azt állítja, hogy CSP problémák nem csak hogy NP-teljesek lehetnek, de – például már a kételemű test feletti, lineáris egyenletrendszerek esetén – annak eldöntése is NP-nehéz, hogy van-e olyan kiértékelése a változóknak, ami az egyenletek 99 százalékát megoldja, vagy mindig csak legfeljebb 51 százalékuk oldható meg. CSP-k approximációjával kapcsolatos kérdések és dichotómia sejtések számítástudományi körökben hatalmas érdeklődésre tartanak számot. A legfontosabb algoritmus ilyen problémákra a lineáris program. Kun több társszerzővel közös cikkében belátta [26], hogy a lineáris programmal approximálható CSP problémák pontosan az ismert egy szélességű (width 1) osztály.

Horváth Gábor és Szabó Csaba több, néha társszerzőkkel is közös cikkeinek témája az egyenletek megoldhatóságának, valamint az ekvivalenciaprobléma bonyolultságának meghatározása különböző klasszikus algebrai struktúrák, elsősorban gyűrűk és csoportok felett.

Horváth Gábor és Szabó Csaba több társszerzővel közös cikkének [10] témája az ekvivalenciaprobléma. Egy G csoport feletti ekvivalenciaprobléma azt vizsgálja, miszerint egy egyenlőség minden G feletti helyettesítésre teljesül-e. Ismert, hogy nilpotens csoportokra és bizonyos feloldható csoportokra az ekvivalencia probléma polinom időben megoldható. Ebben a cikkben belátjuk, hogy minden véges, nem feloldható csoportra az ekvivalencia probléma bonyolultsága coNP-teljes.

A bizonyítás a gráfok k-színezésére való visszavezetésével történik, ahol k a G csoport elemszáma.

Horváth és Szabó egy társszerzővel közösen [14] egy egyenlet megoldhatóságának eldöntését vizsgálta függvényteljes algebrák felett. Egy gyengébb eredmény már létezett, mely szerint egy egyenletrendszer megoldhatóságának eldöntése NP-teljes ezen algebrák felett. A tétel általánosítása mellet igazolják, hogy egy egyenlet azonosság voltának ellenőrzése függvényteljes algebrák felett coNP-teljes.

Horváth Gábor [6] az ekvivalencia és egyenletmegoldhatóság problémák bonyolultságát vizsgálja nilpotens gyűrűkre és nilpotens csoportokra. Belátja, hogy ha R egy véges nilpotens gyűrű, akkor létezik egy olyan, csak R-től függő d pozitív egész szám, hogy bármely polinom értékkészlete megkapható azon helyettesítéseken, melyekben legfeljebb d változó értéke nem 0. Azonos tételt igazol nilpotens csoportokra. Ezen eredmény következménye, hogy nilpotens gyűrű vagy nilpotens csoport feletti ekvivalencia és egyenletmegoldhatóság problémák mindegyike polinomidőben megoldható.

Horváth Gábor és Szabó Csaba közös cikkükben [15] bebizonyítják, hogy az azonosságellenőrzés és egyenletmegoldhatóság problémák bonyolultságát nem határozza meg az algebra klónja. Belátják, hogy ezen problémák bonyolultsága az $\mathbf{A}_4$ alternáló csoportra P-beli; amennyiben azonban a csoportkommutátort is hozzávesszük az algebra alapműveleteihez, akkor az azonosságellenőrzés bonyolultsága coNP-teljessé, míg az egyenletmegoldhatóság bonyolultsága NP-teljessé változik.

Ezt követő közös cikkükben [16] definiálják az ekvivalencia és egyenletmegoldhatóság problémák kiterjesztett változatait, melyekben az algebra bővíthető új, kiszámolható műveletekkel. Véges csoportokra meghatározzák a kiterjesztett problémák bonyolultságát. Bebizonyítják, hogy a kiterjesztett ekvivalencia és egyenletmegoldhatóság P-beli véges nilpotens csoportokra. Továbbá a kiterjesztett ekvivalencia coNP-teljes, a kiterjesztett egyenletmegoldhatóság pedig NP-teljes minden véges, nem nilpotens csoportra.

Horváth [7]-ben a gyűrűk feletti ekvivalenciaproblémát vizsgálja. A gyűrűk felett az ekvivalenciaproblémának két változata van attól függően, hogy a bemeneti polinom milyen alakú. A szokásos ekvivalencia probléma esetén semmilyen megkötés nincs a bemeneti polinomra, míg a szigma ekvivalencia esetén a bemenő polinomot monomok összegeként kapjuk. Ross Willard sejtése szerint a szigma ekvivalencia bonyolultságát a gyűrű Jacobson radikálja szerinti faktor határozza meg: ha a Jacobson radikál szerinti faktor kommutatív, akkor a szigma ekvivalencia P-beli, ha a faktor nem kommutatív, akkor a szigma ekvivalencia coNP-teljes. Szabó és Vértesi igazolták a sejtés coNP-teljes részét [40]. [7]-ben Horváth igazolja a sejtést kommutatív gyűrűkre.

Pluhár Gabriella [36] egy kódelméleti tétel általánosításaként az alábbi problémát vizsgálta: egy egységnégyzetekből álló téglalapot szigetnek hívunk, ha a téglalap minden négyzetének magassága nagyobb az őt körülvevő négyzetek magasságánál, azaz, ha van olyan vízállás, amelynél ez a téglalap sziget a szokásos értelemben. Czédli Gábor bebizonyította, hogy egy $m \times n$-es négyzetrácson maximum $[(mn+m+n-1)/2]$ sziget van. A [36] cikk célja Czédli Gábor eredményének általánosítása: Pluhár becsléseket ad a szigetek maximális számára magasabb dimenziókban. Adott egy $m_1 \times m_2 \times \cdots \times m_d$ tégla. Ekkor jelölje $f(m_1, m_2, \ldots, m_d)$ a szigetek maximális számát. Megmutatja, hogy $\frac{(m_1+1)(m_2+1)\ldots(m_d+1)}{2^{d-1}} - 1 \geq f(m_1, m_2, \ldots, m_d) \geq \frac{m_1 m_2 \ldots m_d + \sum m_{j_1} m_{j_2} \ldots m_{j_{d-1}}}{2^{d-1}} - 1$, ahol az összegzés az $\{1, 2, \ldots, d\}$ halmaz $d-1$ elemű részhalmazain értelmezett. Egy másik dolgozatában [2] Pluhár két szegedi társszerzővel megoldja az előző feladatot háromszögrácsra is. Bebizonyítják, hogy a háromszög szigetek maximális számára egy n oldalú háromszögrácson a következő egyenlőtlenség teljesül: $\frac{n^2+3n}{5} \leq f(n) \leq \frac{3n^2+9n+2}{14}$.

A négyszerzős cikkben [1] a négyzet alakú szigetek maximális számára adnak becslést kettő- és több dimenzióban.

Pach Péter Pál társszerzőjével [30] ugyanezen probléma folytonos általánosítását vizsgálta. Egy $f\colon \mathbb{R}^2 \to \mathbb{R}$ függvényre azon H téglalapokat nevezzük szigetnek, amelyekre $\inf_H f$ nagyobb, mint f értéke a H egy környezetében. Szemléletesen tehát f a vízszint magassága, a szigetek pedig azok a téglalapok, amelyeket víz vesz körül. A szigetrendszerek laminárisak, vagyis két sziget vagy diszjunkt, vagy egyikük tartalmazza a másikat. Belátják, hogy egy maximális lamináris rendszer számossága megszámlálhatóan végtelen vagy kontinuum, és mindkét esethez megadnak konstrukciót is.

Pach, Pluhár, Ponrácz és Szabó tovább általánosítják a fenti kétdimenziós eredményt $\mathbb{R}^n$ egy tartományának összefüggő halmazokból álló S részhalmazrendszerére. [32]. Belátják, hogy egy megszámlálható maximális lamináris rendszer szigetrendszer. Igazolják, hogy egy maximális lamináris rendszer mérete (a lehetséges S halmazrendszerek egy széles osztályára) megszámlálható vagy kontinuum, és konstruálnak egy nem megszámlálható maximális lamináris rendszert, amihez nem létezik magasságfüggvény.

Pach Péter Pál és Szabó Csaba cikkükben [34] egy Günter Pilztől származó 18 éves kódelméleti eredetű problémát oldanak meg. Az eredeti probléma egy majdnemgyűrű-kód minimális távolságának meghatározása. A probléma ekvivalens a következővel: legyen $\underline{m}$ az első m

pozitív egészt tartalmazó halmaz, H pedig tetszőleges véges részhalmaza a természetes számoknak. A sejtés szerint az $\underline{m} \cdot H$ (multi)halmazban páratlan sokszor szereplő elemek száma legalább m. Pach és Szabó a korábban ismert legjobb $m/\log m$-es alsó becslést $m/\log^{0,223} m$-re javítja, és igazolja a sejtésnek azt a gyengébb változatát, amikor azt is megköveteljük, hogy H az első k természetes számból álljon valamely k-ra.

Horváth és Pongrácz [11] bekapcsolódtak az affinteljes algebrák elméletének vizsgálatába. Egy csoportban a konstans függvények és a csoportelemmel való balszorzások a részcsoportok bal mellékosztályait bal mellékosztályokba képezik. Csoportok bizonyos osztályairól belátják, hogy csak ezen függvények képeznek minden bal mellékosztályt bal mellékosztályba. Ilyen csoportok például a véges perfekt csoportok, a véges partícionálható csoportok, a primitív csoportok, vagy azon csoportok, melyek egy p prímre generálhatók a csoport p-ed rendű elemeivel. Egyéb csoportosztályokra mutatnak függvényeket, melyek nem a fenti alakúak, de szintén megőrzik a bal mellékosztályokat. Cikkükben főleg a reguláris csoporthatásokkal foglalkoztak. Belátták többek között, hogy a kommutatív csoportok az elemi Abel 2-csoportoktól eltekintve nem adnak affinteljes reguláris G-halmazt.

Pach Péter Pál [31]-ben megold egy kombinatorikus számelméleti kérdést, amely Pomerance és Schinzel *Multiplicative properties of sets of residues* című cikkében szerepel, a bizonyításban Rado és Ramsey tételeit használja. A kérdés az volt, hogy az $ab = c$ egyenletnek van-e nemtriviális monokromatikus megoldása a természetes számok tetszőleges k-színezése esetén. A szerző igazolja, hogy a válasz igenlő, sőt általánosabban, az $a_1 \dots a_k = b_1 \dots b_l$ egyenlet esetén is az.

Az alábbi probléma João Araújo és Friedrich Wehrung kérdése volt: melyek azok a ferdetestek, amelyek felett minden végtelen dimenziós vektortérre teljesül, hogy az altereiből álló metszetfélháló beágyazható az alterek generátumfélhálójába. Pongrácz András és társszerzője [17] belátták, hogy a testek ilyenek, és visszavezették a kérdést a megszámlálhatóan végtelen dimenziójú vektortér vizsgálatára. A kérdés véges dimenziós változatára pontos választ adtak általánosítva Reinhold Baer egy eredményét.

Számos algebrai kérdés – pl. a kongruenciahálók vizsgálata – visszavezethető olyan algebrai struktúrák tanulmányozására, amelyek csak egyváltozós műveleteket tartalmaznak. Ha a struktúra egyetlen egyváltozós műveletet tartalmaz, akkor monounáris algebráról beszélünk. Horváth Gábor, Kátai-Urbán Kamilla, Pach Péter Pál, Pluhár Gabriella, Pongrácz András és Szabó Csaba [8] kitevőaszimptotika erejéig meghatározták az n elemű monounáris algebrák számát. Ezt a rögzített méretű gyökeres fák számának segítségével becsülik meg.

Ennek kapcsán felmerült az adott méretű és adott mélységű fák vizsgálata. Ennek külön algebrai jelentése van: az $x^k = x^{k+1}$ azonosság által meghatárotzott varietásban szereplő n elemű algebrák számával egyezik meg. Pach Péter Pál, Pluhár Gabriella, Pongrácz András és Szabó Csaba [33] becslést adtak a k mélységű n pontú gyökeres fák $f_k(n)$ számára. Belátták, hogy $f_2(n)$ aszimptotikusan $\frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}$, és $\log f_k(n) = \frac{\pi^2}{6} \cdot \frac{n}{L_{k-2}(n)} \cdot \left(1 + O_k\left(\frac{L_{k-1}(n)}{L_{k-2}(n)}\right)\right)$ ha $k \geq 3$, ahol $L_k(x)$ a k-szor iterált logaritmusfüggvény $\log\log\cdots\log(x)$.

Horváth Gábor, Kátai-Urbán Kamilla, Pach Péter Pál, Pluhár Gabriella, Pongrácz András és Szabó Csaba [9] vizsgálták a félhálók iterált szemidirekt szorzatának varietását. Megadtak egy normálformát az n elemmel generált szabad algebra elemeire. Hatékony algoritmust konstruáltak a megadott normálforma meghatározására. Egy rekurzív képlet segítségével log-aszimptotikus becslést adtak a szabad spektrumra.

A k-darabonként tesztelhető nyelveknek nagy jelentősége van a formális nyelvek elméletében. Simon igazolta, hogy egy nyelv pontosan akkor darabonként tesztelhető, ha szintaktikus monoidja J-triviális, és azonosságbázist adott a $k = 1$ és a $k = 2$ esetekben. Blanchet-Sadri megadott egy azonosságbázist $k = 3$-ra, és igazolta, hogy $k \geq 4$ esetén nem létezik véges azonosságbázis. Kátai-Urbán Kamilla, Pach Péter Pál, Pluhár Gabriella, Pongrácz András és Szabó Csaba [19] normálformát adtak a $k = 2$ és $k = 3$ esetekhez tartozó varitások szabad algebrájának elemeire, és becslést adtak az n elemmel generált szabad algebra méretére.

Kátai-Urbán és Szabó közös cikkükben kis félcsoportvarietások szabadspektrumáról írnak [20]. Ahogy a véges egyszerű csoportok tekinthetők a véges csoportok építőköveinek, úgy a véges félcsoportok alapkövei a véges teljesen 0-egyszerű félcsoportok. Becslést adtak az összes olyan varietás szabad spektrumára, amit kombinatorikus teljesen 0-egyszerű félcsoportok generálnak. A becsléseket a kifejezésfüggvények számának vizsgálatával adták meg.

Pluhár és Szabó a kötegek varietásárának szabdspektrumát számolják ki [37]. Megmutatják, hogy a kötegek varietásának p_n sorozata kb. $\frac{1}{n^2} K^{2^{n+1}} \left(1 + O\left(\frac{1}{n}\right)\right)$, valamilyen K konstansra. Ebből adódik a képlet ezen varietás szabad spektrumára. Pluhár és Wood a valódi köteg varietásokban egy eddig ismeretlen méretű szabad algebrát találnak [38]: a szabad algebra méretének logaritmusa nagyságrendileg $n^k \log n$. Ez újdonság, hisz eddig csak polinomiális és exponenciális méretű szabad spektrumok voltak ismertek.

Vértesi Vera topológiával is, ezen belül kontakt struktúrabeli csomókkal foglalkozott. A 3 dimenziós euklideszi térben egy csomó Legendre féle, ha az (x, y) síktól vett előjeles távolsága megegyezik az (x, y) síkra vett vetületének meredekségével. Egy csomó transzverz, ha a fenti előjeles távolság szigorúan nagyobb mint a meredekség. Bármely csomó mind Legendre félévé, mind transzverz csomóvá tehető a tér egy izotópiájával. Azonban ha a vizsgált csomók osztályát leszűkítjük a csak Legendre féle illetve a csak transzverz csomókra, és csak az adott osztálybeli izotópiákat engedünk meg, akkor a sima csomók izotópiaosztályainak egy-egy finomítását kapjuk. Az alacsonydimenziós topológia egy sokat vizsgált problémája ezen finomítások megértése, például annak vizsgálata, hány különböző egy adott csomóval izotóp Legendre illetve transzverz csomó létezik. A kérdésre a válasz minden esetben végtelen, és ezt a Legendre csomók esetében a Thurston–Bennequin szám és a rotációs szám, a transzverz csomók esetében pedig az önhurkolódási szám bizonyítja. Bizonyos csomókra, mint például a triviális csomóra, a nyolcascsomóra és a tóruszcsomókra a fenti invariánsok egy teljes invariánsrendszert adnak, azaz amennyiben egy ilyen csomóval izotóp két Legendre (transzverz) csomó invariánsai megegyeznek, akkor ezen csomók már Legendre (transzverz) csomókon keresztül is izotópok. Ezen csomóosztályokat Legendre egyszerű illetve transzverzegyszerű csomóknak nevezzük. Vértesi Vera cikkeiben [42, 39] végtelen sok nem transzverz egyszerű csomót konstruál Heegaard Floer csomóinvariánsok segítségével.

Horváth Gábor [10] dolgozata a téma magyarországi népszerűsítéseként megjelent magyarul is [12]. Horváth két korábbi eredményének frissítését hasonló okokból publikálta magyarul [3, 13]. Pluhár Gabriella [38] dolgozatának eredménye magyarul [35]-ben jelent meg. Vértesi Vera egy korábbi eredményét szintén közölte magyarul [43].

Horváth Gábor 2008-ban számítástudományi PhD-jét ([4], University of Hertfordshire, Hatfield, Egyesült Királyság), 2010-ben a matematikus PhD-jét ([5], Eötvös Loránd Tudományegyetem, Budapest) védte meg. Kátai-Urbán Kamilla megvédte az Szegedi Tudományegyetemen [18], Vértesi Vera pedig az Eötvös Loránd Tudományegyetemen a matematika PhD-jét [41].