Kvázicsoportok realizációja projektív síkokban –

szakmai záró beszámoló

2021. október 27.

A kvázicsoport fogalma a csoport fogalmának nem-asszociatív általánosításának tekinthető. Az absztrakt kvázicsoportokhoz hozzárendelhetünk egy illeszkedési struktúrát, amely pontokból és egyeneseknek három osztályából áll. Ezeket az illeszkedési struktúrákat nevezzük 3-hálózatoknak. A kutatási projekt címében szereplő kvázicsoport realizáció valójában a megfelelő a 3-hálózatnak, vagy a duálisának a beágyazása a projektív síkba. A kutatásunk során értünk el eredményeket ezen a szűken vett területen, valamint általánosabban a véges absztrakt illeszkedési és algebrai struktúrák beágyazásaival kapcsolatos kérdésekben.

A projekt eredményeként **12 tudományos publikáció** született, és készült **2 szoftver csomag** a GAP komputeralgebra rendszerhez. A cikkek közül **3 jelent meg D1 szintű nemzetközi folyóiratban** (*Finite Fields and Their Applications, IEEE Transactions on Information Theory, Journal of Combinatorial Theory Series A*), további **3 pedig Q1 szintű folyóiratban** (*Discrete Mathematics, Designs Codes and Cryptography*).

Kvázicsoportok, csoportok és 3-hálózatok beágyazásai. Bogya Norberttel és Korchmáros Gáborral olyan duális 3-hálózat beágyazásokat vizsgáltunk, amik a ponthalmazon nem injektívek. Az ilyen beágyazások is eredményeznek algebrai geometriai szempontból érdekes vonalkonfigurációkat az algebrailag zárt K test feletti projektív síkban. Korábban Bartz és Yuzvinsky adtak ilyen konstrukciókat. Mi leírtunk két végtelen osztályt, osztályoztuk a 6 rendű duális 3-hálózatok beágyazásait, és adtunk példát egy olyan 18 rendű duális 3-hálózatra, aminek a pontjai nem címkézhetőek véges csoporttal. Szintén Korchmárossal közös munka nem-Abel féle csoportok grafikus reprezentációinak vizsgálata. A reprezentáció ebben az esetben egy Γ egyszerű gráffal történik, melynek az automorfizmuscsoportja izomorf G-vel, és aminek a csúcsain adott G-nek egy tranzitív Frobenius-csoport hatása. A cikkünkben a Higman-féle $A(f, f_0)$ 2-csoportról mutattuk meg, hogy rendelkezik ilyen típusú reprezentációval. Ezzel olyan végtelen osztályt találtunk, melyre teljesül Spiga tétele anélkül, hogy a Frobenius-komplementumra vonatkozó Spiga-korlát igaz lenne. Ehhez az alfejezethez tartozik még Kiss Rebekával írt cikkünk, amiben bizonyos paraméterekkel rendelkező ortogonális tömbök nem-létezését bizonyítottuk. Ortogonális tömbök a latin négyzetek általánosításának tekinthetők, amik pedig nem mások, mint véges kvázicsoportok művelettáblái. A vizsgált paraméterek lényeges információt szolgáltatnak korreláció-immun Boole-függvények minimális súlyára vonatkozóan. Ez utóbbiak kriptográfiai szempontból is fontos szerepet játszanak, mert segítségükkel a korrelációs támadásnak ellenálló S-dobozok készíthetők. Az eredményeinket algebrai és egészértékű programozási módszerek kombinálásával kaptuk, és ezzel kiegészítettük C. Carlet 2018-as cikkeiben ismertetett táblázatos értékeket.

- N. Bogya, G.P. Nagy: Light dual multinets of order six in the projective plane, Acta Mathematica Hungarica 159 : 2 pp. 520-536, 17 p. (2019), 2019 – Q2
- G. Korchmáros, G.P. Nagy: Group-labeled light dual multinets in the projective plane, Discrete Mathematics 341(8), 2121-2130, 2018 – Q1
- G. Korchmáros, G.P. Nagy: Graphical Frobenius representations of non-abelian groups, Ars Mathematica Contemporanea 20 : 1 pp. 89-102, 14 p. (2021), 2021 – Q2

- R. Kiss, G.P. Nagy: On the nonexistence of certain orthogonal arrays of strength four, Prikladnaya Diskretnaya Matematika 2021 : 52 pp. 65-68, 4 p. (2021), 2021 – Q4

Unitálok és más illeszkedési struktúrák beágyazásai. Egy n rendű absztrakt unitál alatt egy 2-$(n^3+1, n+1, 1)$ dizájnt értünk. A klasszikus Hermite-féle unitál rendje a q prímhatvány, a pontjai a $GF(q^2)$ feletti projektív sík Hermite-görbéjének pontjai $H_q : X^{q+1} + Y^{q+1} + Z^{q+1} = 0$, blokkjai pedig az egyenesekkel vett $q+1$-metszetei. Ilyen módon H_q mint absztrakt unitál természetes módon be van ágyazva $PG(2,q^2)$-be. Mezőfi Dáviddal kis rendű absztrakt unitálok gazdag osztályait tudtuk megkonstruálni a paramodifikációnak nevezett módszerünkkel. Ezek síkba történő beágyazásait a „teljes pontok" módszerével vizsgáltuk, amivel az esetek többségében ki tudtuk zárni, hogy az adott unitál beágyazható lenne a klasszikus síkba. A módszer alkalmazáskor olyan 4 rendű unitált tudtunk konstruálni, amibe beágyazható az 5 rendű nemklasszikus 3-hálózat. Unitálok beágyazásához kapcsolódóan sikerült egy nagyon szép eredményt bizonyítani Ree-féle unitálok nem-beágyazhatóságával kapcsolatosan. A legkisebb Ree-unitál beágyazásainak vizsgálatával elégséges feltételt adtunk arra, hogy q rendű Ree-unitál ne legyen beágyazható egy projektív síkba (desargues-i vagy sem). Ebből következik, hogy $q > 3$ esetben a Ree-unitál nem ágyazható be semmilyen test feletti síkba. A bizonyítás során elemi, de nem triviális számolások mellett a Ree-féle egyszerű csoportok maximális részcsoportjainak osztályozását használtuk fel. A számításokban nagyban támaszkodtunk a Mezőfivel közösen készített `UnitalSZ` GAP programcsomagunkra.

Két fontos beágyazási típusú eredményt értünk el Korchmárossal, Timpanellával, illetve Blokhuisal, Kovács Istvánnal és Szőnyi Tamással. Az egyik 3-dimenziós $U_3(q)$ Hermite-sokaságokban konstruál hemirendszereket. Utóbbiak fontosságát az adja, hogy belőlük erősen reguláris gráfokat, parciális általánosított négyzeteket, Q-antipodális asszociációs sémákat és más érdekes kombinatorikus struktúrákat lehet definiálni. Másrészről a $U_3(q)$-beli hemirendszerek kevesen vannak. Cikkünkben $U_3(q)$-ba ágyazott $q+1$ fokú maximális görbék felhasználásval készítünk olyan hemirendszereket, amiket invariánsan hagy a $PGU(4,q)$-nak egy $PSL(2,q) \times C_{(q+1)/2}$-vel izomorf részcsoportja. A feltételünk, hogy $q = 1 + 16a^2$ alakú Landau-prím. A másik dolgozatunkban egy klasszikus problémát vizsgáltunk: oválisok és hiperoválisok létezése nem Desargues-féle véges projektív síkokban. Ehhez teljesen leírtuk $PG(2,q)$ azon kúpszeleteit, amik oválisok maradnak a deriválási művelettel nyert Hall-féle síkon is. A bizonyítás kulcseleme egy Segre és Korchmáros nevéhez fűződő régi lemma volt kúpszeletbe írt perspektív háromszögekről.

- Dávid Mezőfi, Gábor P. Nagy: On the geometry of full points of abstract unitals, Designs Codes and Cryptography 87 : 12 pp. 2967-2978. , 12 p. (2019), 2019 – Q1
- Dávid Mezőfi, Gábor P. Nagy: New Steiner 2-designs from old ones by paramodifications, Discrete Applied Mathematics 288 pp. 114-122. , 9 p. (2021), 2021 – Q2
- Gábor P. Nagy: Embeddings of Ree unitals in a projective plane over a field, Finite Fields Appl. 74 (2021), Paper No. 101875, 11 pp., 2021 – D1
- Gábor Korchmáros, Gábor P. Nagy, Pietro Speziali: Hemisystems of the Hermitian Surface, Journal of Combinatorial Theory Series A 165 pp. 408-439. , 32 p. (2019), 2019 – D1
- Aart Blokhuis, István Kovács, Gábor P. Nagy, Tamás Szőnyi: Inherited conics in Hall planes, Discrete Mathematics 342 : 4 pp. 1098-1107. , 10 p. (2019), 2019 – Q1

- Dávid Mezőfi, Gábor P. Nagy: GAP Package UnitalSZ, Version 0.5, szoftver, 2018

Hermite-féle görbék és AG-kódjaik. Az unitálokkal kapcsolatosan említettük a H_q Hermite-görbéket. Ezek a $GF(q^2)$ véges test felett definiálva a maximális görbék legfontosabb osztályát adják. Maximális görbék felett értelmezett algebrai-geometriai (AG) kódok a hibajavító kódok jó paraméterekkel rendelkező osztálya. Ezen kódokat napjainkban különös figyelem övezi, mert potenciálisan felhasználhatók a posztkvantum kriptográfiában. Korchmárossal és Timpanellával a H_{q^3}-n értelmezett $C_\Omega(D,mT)$ differenciál-kódokat vizsgáltuk, ahol a T divizor a $GF(q^2)$-racionális affin pontok összege, míg D az összes többi $GF(q^6)$-racionális affin pont összege. Az m egész paraméter függvényében javítottunk a minimum távolságra adható becslésen, ezekről megmutattuk, hogy bizonyos esetekben jobbak az 1-pontos Hermite-kódok valódi értékeinél. Megmutattuk továbbá, hogy ha $m \leq q^3 - 2$, akkor a kód automorfizmuscsoportja izomorf $PGU(3,q)$-val. Sabira El Khalfaoui-val Hermite-kódok résztest részkódjait vizsgáltuk. Becsléseket adtunk a részkód dimenziójára, és bizonyos speciális esetekben a dimenzió pontos értékét is meghatároztuk. Kísérleti módszerekkel vizsgáltuk, hogy a résztest részkódok valódi dimenziói milyen eloszlásfüggvényekkel közelíthetők. Az tapasztaltuk, hogy a még kezelhető paraméter tartományban a szélsőérték eloszlás közelít legjobban. Az eredményeinkhez szükséges masszív számításokhoz készítettük a `HERmitian` GAP programcsomagot.

- Gábor Korchmáros; Gábor P. Nagy; Marco Timpanella: Codes and Gap Sequences of Hermitian Curves, IEEE Transactions on Information Theory, vol. 66, no. 6, pp. 3547-3554, June 2020, 2020 – D1
- Sabira El Khalfaoui, Gábor P. Nagy: On The Dimension of The Subfield Subcodes of 1-Point Hermitian Codes, Advances in Mathematics of Communications 15 : 2 pp. 219-226. , 8 p. (2021), 2021 – Q2
- Sabira El Khalfaoui, Gábor P. Nagy: Estimating the Dimension Of The Subfield Subcodes of Hermitian Codes, Acta Cybernetica 24 : 4 pp. 625-641. , 17 p. (2020), 2020 – Q4
- Sabira El Khalfaoui, Gábor P. Nagy: GAP package HERmitian, Version 0.1, szoftver, 2019