Válasz Wettl Ferencnek a "Loops and Groups" című doktori értekezésem bírálatára

Mindenek előtt szeretném megköszönni Wettl Ferenc alapos és gondos értékelését. Köszönet a számomra nagyon hasznos kérdéseiért is.

1. Kérdés:

Bár a loopelmélet messzire jutott a kiindulópontot jelentő problémáktól, ma vajon a kvázicsoportok/loopok algebrai vizsgálatában milyen irányú kutatásoktól vagy milyen típusú eredményektől lehet várni az elmélet még eredményesebb használhatóságát, például a kombinatorikai természetű kérdések megoldásában – ha ez egyáltalán reménytelinek látszik –, és saját kutatásai hogyan viszonyulnak ezekhez?

Válasz:

a) Először megemlíteném a loopok és a fizika kapcsolatát, pontosabban a "special grouplike loops", más néven "gyrocommutative gyrogroup"-ok kapcsolatát az Einstein-féle speciális relativitáselmélettel.

Kiderült, hogy az Einstein-féle sebesség-összeadás egy "gyrocommutative gyrogroup"-operáció, ami a hiperbolikus geometria Poincaré-féle gömb modelljének a kereteit alkotja, éppen úgy, ahogy a közönséges vektor-összeadás, ami egy kommutatív csoport művelet és az euklideszi geometria standard modelljének kereteit képezi.

A "special grouplike loop"-ok vizsgálata már eddig is új eredményekre vezetett a hiperbolikus geometriában, a relativitáselméletben, a kvantum információk és számításokban. Várhatóan a jelenlegi kutatások is további hasznosításokra adnak lehetőséget a fent vázolt területeken.

b) Másodszor beszélnünk kell a loopok/kvázicsoportok és a kriptográfia kapcsolatáról.

A kriptográfiában igen fontos probléma hatékony és biztonságos "hash" függvények konstrukciója.

Nemrégiben a kutatóknak nagyon magas elemszámú (2^{256}, 2^{334}, 2^{512}) kvázicsoportok konstruálásával sikerült hatékony "hash" függvényeket leírni.

Ebben a témában egy friss eredmény: a kvázicsoport-műveletet vektorértékű Boole-függvényként való reprezentációja a kvázicsoportok számos olyan új tulajdonságát adja meg, amelyek kriptográfiai "primitive"-ek meghatározására alkalmasak – ezek olyan kriptográfiai algoritmusok, amelyeket komputerbiztonsági rendszerek kiépítésére használnak.

Tudjuk, hogy a kvázicsoportok és a loopok szorzástáblája latin négyzet, a páronként ortogonális latin négyzetek hibajavító kódokként is használhatók.

Ezeken a területeken a kutatások nyomán újabb alkalmazások várhatók.

c) Végül a kombinatorikában a latin négyzetekhez kapcsolódó problémák, amelyek a loopok és kvázicsoportok vizsgálatával esetleg eredményesen megoldhatóak lesznek:

i) Az ortogonális latin négyzetekhez kapcsolódó egyik probléma a transzverzálisok keresése latin négyzetekben.

1. Sejtés: *Minden páratlan rendű latin négyzetnek van legalább egy transzverzálisa.*

2. Sejtés: *Minden n-edrendű latin négyzetnek van egy $n-1$ hosszúságú parciális transzverzálisa.*

Létezik néhány sejtés a latin négyzetben a transzverzálisok számára vonatkozóan is.

ii) Különböző csoportok és loopok szorzástáblájában a "critical set"-ek jellemzése.

iii) A szorzástáblák Hamming-távolságával kapcsolatos problémák.

Magamra vonatkozóan:

Eddig csak a loopok és szorzáscsoportjuk algebrai elméletével foglalkoztam, de nagyon örülök, hogy milyen széleskörű a felhasználhatóságuk. Jövőbeli terveim között szerepel a loopok szorzáscsoportja és a neki megfelelő latin négyzet tulajdonságai közötti kapcsolat vizsgálata.

2. Kérdés:

A dolgozatban használt technikák és eredmények szorosan kapcsolódnak a csoportelmélethez, aminek alapja a loopok szerkezetében megjelenő csoportok fontossága. Melyek a loopelmélet azon fontosnak tekinthető alapkérdései, amelyekről úgy tűnik, a támadások ellenére is ellenállnak a csoportelmélet felőli megközelítésnek? Másszóval: kérdésem arra vonatkozik, mik a csoportelméleti eszköztár korlátai?

Válasz: A dolgozatban vizsgált nilpotencia- és feloldhatósági és a belső permutációcsoportra vonatkozó problémák csoportelméleti megközelítése eddig csak ezen problémáknak a dolgozatban is leírt parciális megoldását adta. A teljes megoldás egyelőre ellenáll a csoportelméletnek, de lassan haladunk előre.

Nemrégiben hosszantartó ellenállás után csoportelméleti eszközökkel megoldották azt a korábbi sejtést, hogy a belső permutációcsoport nilpotenciája maga után vonja a loop feloldhatóságát és nilpotenciáját is. Ehhez az állításhoz kapcsolódó újabb sejtés, hogy a belső permutációcsoport nilpotenciája helyett a szorzáscsoport feloldhatóságához, így a loop feloldhatóságához elegendő a belső permutációcsoport szuperfeloldhatósága. Ennek megoldása csoportelméleti eszközökkel egyelőre várat magára.

Jelenleg a Moufang-loopok algebrai szerkezetét vizsgálom csoportelméleti eszközökkel, elsősorban a nucleus viselkedésével kapcsolatosan. Jónéhány éves sejtés, hogy a páratlan rendű Moufang-loopoknak mindig van nemtriviális nucleusa. A teljes megoldást ebben a kérdésben is a jövőben reméljük.

Csörgő Piroska