A bírálóbizottság értékelése

Gyarmati Katalin az MTA doktora fokozat elnyerése érdekében „Véges bináris sorozatok és rácsok pszeudovéletlensége” címmel nyújtotta be értekezését. A disszertáció angol nyelven készült (angol címe „Pseudorandomness of finite binary sequences and lattices”) és ez a dolgozat a jelöltnek a témában elért legfontosabb eredményeit tartalmazza. A disszertációban a szerző (részben társszerzőkkel közös) 6 cikkének eredményei részletesen bemutatásra kerülnek, de az utolsó fejezetben a szerző a témában írt további majd 20 dolgozatának eredményei is megemlítésre kerülnek.

A jelölt a disszertáció 2. fejezetében ismerteti a Blum-Blum-Shub pszeudovéletlen generátorra, illetve az ennek általánosításaként definiált hatványgenerátorokra vonatkozó kvantitatív eredményeit. A korábbi hasonló eredmények zöme bizonyítatlan hipotéziseken alapult (mint például az, hogy az egészek faktorizációja nehéz feladat), így fontos kiemelni, hogy a jelölt eredményei feltétel nélküliek. A bizonyításban egyebek mellett Bourgain 2005-ös exponenciális összegekre vonatkozó mély eredményének alkalmazására volt szükség.

A disszertáció 3. fejezetében a jelölt Mauduit-val közös eredményeit ismerteti, melyek Mauduit egy problémájának megoldásával kapcsolatosak. Egy $E_N \in \{-1,1\}\hat{}N$ véges pszeudovéletlen sorozat esetén $C_n(E_N)$ jelöli a sorozat n-ed rendű korrelációs mértékét. Mauduit 2003-ban vetette fel azt a kérdést, hogy adott $k, l \geq 2$ egészek esetén igaz-e, hogy minden $E_N \in \{-1,1\}\hat{}N$ sorozat esetén

$$C_{2k+1}(E_N) \cdot C_{2l}(E_N) \gg N$$

illetve, legalább

$$C_{2k+1}(E_N) \cdot C_{2l}(E_N) \gg N^{c(k,l)}$$

egy $0.5 < c(k,l) \leq 1$ konstanssal, ahol az indukált konstansok is csak k-tól és l-től függenek. A probléma megoldása irányába az első lépéseket a jelölt tette meg, mely eredményt Anantharam javította, végül pedig Mauduit-val közösen a jelölt pozitív választ adott a problémára $k \geq l$ esetén az erősebb formában, míg $k < l$ esetén a gyengébb formában. A bizonyításban részben a jelölt által korábban fejlesztett módszert használják.

A 4. fejezetben a jelölt Goubin, Mauduit és Sárközy Legendre szimbólumokat használó pszeudovéletlen sorozat-családjának f-bonyolultságára ad alsó becslést, ezzel Ahlswede, Kachatrian, Mauduit és Sárközy eredményét javítva. Így a legjobb alsó és felső becslés már csak egy konstans szorzóval tér el egymástól.

A dolgozat 5. fejezete a jelölt egy olyan tételét mutatja be, mely éles becslést ad pszeudovéletlen sorozatok rövid részsorozatainak korrelációjára abban az esetben, ha a sorozatok hossza legfeljebb $c_1 N^{\frac{1}{4}} \log N$, ahol N az eredeti sorozat hosszát jelöli.

A 6. és 7. fejezetben a jelölt Sárközy-vel és Stewarttal közös, pszeudovéletlen bináris rácsok l-ed rendű pszeudovéletlen mértékére vonatkozó eredményeit ismerteti. A jelölt társszerzőivel a korábban ismert kissé mesterkélt példák helyett egy „természetes” konstrukciót definiál, majd becsléseket ad a definiált bináris rács pszeudovéletlen mértékére.

Összefoglalva a jelölt a pszeudovéletlen sorozatok és rácsok elméletében számos új és mély tudományos eredményt ért el. Egyrészt új konstrukciókat javasolt, és ezek tulajdonságait vizsgálta, másrészt a bizonyítási módszereket újszerűen továbbfejlesztve és korábbi tételeket jelentősen élesítve nyert nemzetközileg elismert eredményeket.

A bizottság a jelölt téziseit elfogadja.