DEBRECENI EGYETEM
MATEMATIKAI INTÉZET

4032 Debrecen, Egyetem tér 1., ✉ 4010 Debrecen Pf. 12., 🖳 apinter@science.unideb.hu

Tel.: (52) 512-900 * Fax: (52) 512-728

Bírálói vélemény Gyarmati Katalin "Pszeudorandom finite binary sequences and lattices" című doktori munkájáról

A Szerző munkájában az kriptográfiában is jelentős alkalmazással bíró pszeudovéletlenséggel foglalkozik. A fogalomnak több megközelítése és definíciója van, leggyakoribb értelmezése bonyolultságelméleti fogalmakon alapszik, azonban éppen ezt a megközelítést kritizálják újabban, mert végtelen hosszú sorozatokkal foglalkozik, míg a gyakorlati alkalmazásokban csak véges sorozatok fordulnak elő.

Mauduit és Sárközy, 1997-ben az Acta Arithmeticában megjelent cikkükben vezették be a pszeudóvéletlenség új, konstruktív és kvalitatív megközelítését, amelyben véges bináris sorozatok pszeudóvéletlenségét definiálták, bevezetve egy úgynevezett pszeudóvéletlen mértéket. A Jelölt munkája ezt a területet gazdagítja érdekes és értékes eredményekkel.

A doktori munka 113 számozott oldalból áll, a bevezetés után hét fejezetben ismerteti az eredményeket, amelyet egy igen alapos, 108 tételből álló irodalomjegyzék egészít ki. A fejezetek tartalmazzák a Jelölt eredményeit, amelyet részben önállóan, részben a témakör neves kutatóival közösen nyert. Gyarmati Katalin a disszertáció 2.-7. fejezetében részletesen ismerteti bizonyos cikkeinek az eredményeit, a 8. fejezet pedig 18 cikk összefoglalója. A disszertáció 2. fejezetében hatványgenerátorra vonatkozó kvantitatív becsléseket ad, amelyek bizonyítása többek között Bourgain 2005-ös exponenciális összegekre vonatkozó becslésén múlik. A 3. fejezetben bináris sorozatok korrelációjával foglalkozik. A 4. fejezetben a Legendre-szimbólumot használó pszeudóvéletlen sorozatok úgynevezett f-bonyolultságára ad közel éles alsó becslést, így az alsó és a felső becslés most már csak egy konstans szorzóval tér el egymástól. Az alsó becslés bizonyítása karakterösszegekre, Weil tételére és egy átlagolásos ötlet újszerű alkalmazására épül. Az 5. fejezetben rövid sorozatok korrelációjával foglalkozik. Eredménye abban az esetben ad a rövid részsorozatok korrelációjára éles becslést, ha azoknak hossza c_1N^(1/4)logN-nél hosszabb. Mivel várhatóan a teljes sorozatban létezik olyan c_2 logN hosszú részsorozat, amely csupa egyesből áll, ezért nem remélhetjük, hogy egy erős pszeudovéletlen sorozat összes részsorozata erős pszeudovéletlen tulajdonságokkal rendelkezzék. Nyitott kérdés, hogy vajon becsülhető-e azon részsorozatok korrelációja, amelyek hosszúsága c_2 logN és c_1N^(1/4) logN közé esik. Ezen probléma nehézségét mutatja, hogy egy ehhez kapcsolódó probléma, a legkisebb kvadratikus nem-

maradék (mod p) becslése esetén is nagyon nagy hézag van Burgess felső becslése és megoldatlan sejtés között. Végül, a 6. és 7. fejezetekben a szerző a pszeudóvéletlenség több dimenziós általánosításaira vonatkozó eredményeit tekinti át.

A doktori munka valamennyi érdemi fejezete új tudományos eredményt tartalmaz, a szakterület és annak irodalmának alapos ismeretéről tanúskodik.

A tételek minősége, mélysége, a bizonyítások színvonala, a letisztult munka számomra világosan és meggyőzően mutatják, hogy a doktori munka elegendő az MTA doktori cím megszerzéséhez és a nyilvános védés kitűzését javasolom.

Kérdést nem fogalmazok meg a doktori munkával kapcsolatban.

Debrecen, 2014. március 20.

Pintér Ákos