Válasz Dr. Sándor Csaba bírálatára

Nagyon köszönöm Dr. Sándor Csabának az alapos és gondos bírálatot, a dolgozatom értékelésére fordított idejét és a pozitív véleményt. A bírálatban feltett fontos kérdésekre az alábbiakban válaszolok.

1. Kérdés: Milyen más mértékei vannak a ± 1 számokat tartalmazó véges sorozatok pszeudovéletlenségének?

Véges bináris sorozatok egyik legfontosabb és legtöbbet vizsgált pszeudovéletlen mértéke a lineáris bonyolultság. Ezt a mértéket a sorozatot generáló legrövidebb lineáris rekurzió hosszával definiálják. Elwyn Berlekamp egy régebbi algoritmusa alapján 1969-ben James Massey megadott egy egyszerűen számolható algoritmust, amely konkrét sorozat esetén kiszámolja a lineáris bonyolultság értékét. Azonban ez a módszer általában csak a posteriori tesztelésre alkalmas, azaz azután alkalmazható, ha a sorozat összes elemét már generáltuk.

A Christian Mauduit és Sárközy András által bevezetett mértékek egyik előnye, hogy azokkal már a sorozat generálása előtt, „a priori" biztosíthatjuk az erős pszeudovéletlen tulajdonságokat. Bizonyított tény, hogy amennyiben ezek a mértékek kicsik, akkor a konkrét sorozatok pszeudovéletlenségének tesztelésére használt statisztikák majdnem mindegyike legfeljebb minimális mértékben nagyobb az elvárhatónál. Rendkívül fontos az is, hogy bizonyos számelméleti konstrukciók esetén ezek a mértékek *bizonyítottan* kicsik, így szükségtelenné válik a sorozatok a posteriori tesztelése. Míg a lineáris bonyolultság csak egy tulajdonságot mér, ezekkel a mértékekkel tulajdonságok szélesebb köre vizsgálható. (Megjegyzem, ha a korrelációs mértékek kicsik, akkor abból Nina Brandstätter és Arne Winterhof eredménye alapján alsó becslést kapunk a lineáris bonyolultságra.)

Természetesen ezen mértékek mintájára számos más pszeudovéletlen mérték is definiálható, így például PhD értekezésemben bevezettem a szimmetria mértéket, amely a sorozatban található szimmetrikus részsorozatokat vizsgálja. Sziklai Balázs szakdolgozóm tovább általánosította ezt a mértéket. azonban az egyre újabb mértékek bevezetése során előfordulhat, hogy kezelhetetlen szituációba kerülünk. Például Kolmogorov egy tételéből következik, hogy ha túl sok követelményt írunk elő, akkor nagy valószínűséggel nincs

olyan sorozat, amely mindegyiknek eleget tesz. Így valóban fontos feladat az alapvető mértékek megtalálása. A legtöbb cikk az említett mértékekre szorítkozik.

2. Kérdés: Kapcsolódik-e szabadalom az értekezésben szereplő konstrukciókhoz? Van-e olyan szoftver, ami a szerző konstrukcióit használja?

Magyarországon nem kérhető szabadalom matematikai algoritmusra, sőt, tudomásom szerint az Európai Unióban sem. Az Egyesült Államokban kérhető szabadalom pszeudovéletlen generátorokra, azonban ez rendkívül költséges lenne. A kérdés második feléhez kapcsolódóan megemlítem, hogy a Kripto Kft., egy debreceni spin-off vállalkozás, Pethő Attilával és Sárközy Andrással közösen publikált lineáris rekurzión és Legendre szimbólumon alapuló konstrukciónkat hozzájárulásunkkal implementálta egy GVOP pályázat keretében 2006 vagy 2007-ben. Folláth János PhD értekezésében számos példa található hasonló elven működő pszeudovéletlenszám generátorok implementálására és tulajdonságaik, pl. lavina hatás, statisztikai vizsgálatára. Vannak arra utaló jelek, hogy a témakörben született főbb konstrukciókat több helyen is alkalmazzák, azonban a kriptográfia alkalmazásaiban - nyilvánvaló okokból - nem mindig hozzák nyilvánosságra, hogy milyen algoritmust használnak.

Budapest, 2014 május 5.

Gyarmati Katalin