Szakmai beszámoló
zárójelentés

„Információelmélet és alkalmazásai”
OTKA „K 46376”

A kutatási program alapkutatást irányzott elő egyrészt a szűkebb értelemben vett információelmélet (Shannon elmélet), másrészt az információelméleti módszerek alkalmazása területén, a valószínűségszámításban, matematikai statisztikában és gráfelméletben.

A programban külön pontként szerepelt az információmennyiségek formális tulajdonságainak vizsgálata, elsősorban az u.n. információs geometria, az idevágó eredményekről a statisztikai alkalmazások között számolok be (c. pont).

a) A Shannon elméletben elsősorban a bizonyítható titkosság témakörével foglalkoztunk.

   Itt fő probléma a titkos kulcs kapacitás, az elérhető maximális sebesség, mellyel titkos kulcs generálható két szeparált felhasználó számára, nyilvános kommunikáció segítségével, természetesen olyan modellt feltételezve, amely biztosít „korrelált véletlenhez” való hozzáférést. A problémát általánosítottuk több felhasználó esetére és mind forrás, mind csatorna típusú modellek széles osztályára meghatároztuk a titkos kulcs kapacitást. Nemzetközi konferenciákon több előadás, két megjelent folyóiratcikk.

   Vizsgáltuk az „oblivious transfer” fontos kriptográfiai fogalommal kapcsolatos kapacitás-problémát is. Bizonyos modellekre (pl. törléses csatorna) meghatároztuk a kapacitást, más esetekre alsó és felső korlátokat adtunk. Nemzetközi konferencián előadva, folyóiratpublikáció előkészületben.

   A Shannon-elmélet témakörhöz sorolható egy kvantum-információelméleti probléma megoldása is (publikáció megjelent). Ide tartozik még egy megjelent és egy sajtó alatt lévő összefoglaló cikk.

b) A valószínűségszámítás jelenleg intenzíven kutatott „measure concentration” témakörének egyik hatékony módszere a Marton Katalin által bevezetett információelméleti módszer.

   A projekt keretében ezzel mértékkoncentrációt bizonyítottunk különböző távolságok esetén, Markov láncokra és általánosabb folyamatokra. Új logaritmikus Szoboljev egyenlőtlenséget bizonyítottunk gyengén függő valószínűségi változókra. Távolság-divergencia egyenlőtlenségeket bizonyítottunk kontraktív Markov láncokra, ennek segítségével ilyen egyenlőtlenségeket lehet bizonyítani Gibbs mértékekre. Több előadás nemzetközi konferenciákon, egy folyóiratpublikáció megjelent, kettő előkészületben.

c) Foglalkoztunk modell-választási problémákkal, információelméleti alapú módszert használva, egyrészt az u.n. kontextus fa becslésével (a korábbi irodalomtól eltérőleg nem véges emlékezetű folyamatokat is megengedve), másrészt Markov mezők alapkörnyezetének becslésével. Mindkét esetben igazoltuk a használt módszer konzisztens voltát, az első esetben azt is, hogy a becsült fa lineáris időben kiszámítható. Előadások nemzetközi konferenciákon, két megjelent folyóiratcikk, előadássorozat nyári iskolán.

   Az információs geometriával kapcsolatos korábbi vizsgálódásainkat folytatva, exponenciális eloszláscsaládokra megadatuk az általánosított maximum likelihood becslés létezésének szükséges és elégséges feltételét, és a becslés pontos jellemzését. Eredményeinket kiterjesztettük általános entrópiafunkcionálok minimalizálására és az exponenciális családok megfelelő általánosításaira. A korábbi hasonló vizsgálatokkal szemben regularitási feltételekre nem volt szükség. Több nemzetközi konferencián előadva, két megjelent és egy előkészületben lévő cikk.

d) Az gráfelméleti problémák közül főleg gráfszinezéseket és (részben új) információelméletileg értelmezhető gráfparamétereket vizsgáltunk.

   Topológiai módszerrel új alsó becsléseket adtunk a lokális kromatikus számra és a cirkuláris kromatikus számra, melyek több fontos esetben pontosak; több sejtést bebizonyítottunk, pl. hogy Kneser gráfok cirkuláris kromatikus száma egyenlő a kromatikus számmal. Gráfok különböző osztályaira megmutattuk, hogy optimális szinezésnél minden olyan teljesen tarka páros gráf megjelenik, melynek csúcsszáma a gráf kromatikus számával egyenlő; új eredményeket bizonyítottunk az u.n. necklace bisection problémára is. Nemzetközi konferenciákon több előadás, négy megjelent cikk.

   Gráfokra bevezettünk egy gráfkapacitás jellegű új paramétert, segítségével új becslést adtunk egy Körner és Malvenuto által korábban vizsgált problémára; publikáció megjelent. Vizsgáltuk az előbbi gráfparaméter egy általánosítását végtelen gráfokra, több esetre meghatároztuk az értékét és megmutattuk, hogy a Shannon kapacitás speciális esetként értelmezhető. Publikáció benyújtva.