Kutatási jelentés

A kutatási tervnek megfelelően, eredményes kutatást folytattunk egyrészt a szűkebb értelemben vett információelmélet (ezen belül elsősorban az információelméleti titkosság), másrészt az információelméletnek a valószínűségszámításban és matematikai statisztikában való alkalmazása, valamint az információelméleti motiváltságú gráfelméleti problémák területén.

(i) Az információelméleti titkosság problémakörével több évre visszamenőleg folyamatosan foglalkozunk, fő eredményeinket a 2011-ben második kiadásban megjelent könyvünk (Csiszár-Körner: Information Theory etc., Cambridge University Press) új 17. fejezete tartalmazza.
Az itt összefoglalt eredményeink meghatározzák a több felhasználó számára generálható titkos kulcs maximális méretét (titkos kulcs kapacitás) olyan információelméleti modellekre, melyek korrelált forrásokat vagy több kimenetű (de egy bemenetű) csatornát használnak. A kutatást ezután több kimenetű csatornákra is kiterjesztettük, ilyen modellekre is adtunk alsó és felső korlátokat a titkos kulcsa kapacitásra, bár ezek az általános esetben nem bizonyultak egyenlőnek.
Egy másik titkossági probléma (oblivious transfer), hogy két információ egyikét kell eljuttatni a vevőhöz, annak választása szerint, de sem az adó nem szerezhet tudomást a vevő választásáról, sem a vevő a másik információról. Az oblivious transfer kapacitásra vonatkozó korábbi eredményünket a projekt során sikerült kiterjeszteni és kapcsolatot megállapítani a jól ismert „wiretap channel” problémával.

Ezen eredményeink az ún. oblivious transfer kapacitásról, valamint a több-bemenetű csatornák titkossági kapacitásáról, két cikkben kerültek publikálásra.

(ii) Statisztikai alkalmazások szempontjából fontos feladat a relatív entrópia és más konvex integrál funkcionálok minimalizálása momentum feltételek mellett.
Ezzel a problémával is több éve foglalkozunk, legáltalánosabb eredményeinket egy 2012-ben megjelent 52 oldalas cikkben publikáltuk. Ezek egyike az információs geometriai Pitagorasz tétel messzemenő általánosítása. További fő eredmény, hogy bár a minimumot elérő „valódi megoldás” nem mindig létezik, ilyenkor is létezik „általánosított megoldás”,

melyhez minden minimalizáló sorozat konvergál Bregman távolság szerint, és így egyúttal mértékben, lokális értelemben véve.
Említett eredményünket ezután sikerült a közgazdasági matematikában is alkalmazni, nevezetesen kockázatvizsgálatra „multiple priors” modellekben, ha a kockázati tényezőket jellemző ismeretlen eloszlásról az a plauzibilitási feltétel , hogy egy integrál funkcionál (amely az ismeretlen eloszlásnak egy alapeloszlástól vett eltérését méri) nem lép túl egy előírt korlátot.

(iii) Mértékkoncentráción azt a széles körben előforduló jelenséget értjük, hogy egy „nem túl kis” mértékű halmazt kissé felfújva (hozzávéve a „viszonylag közeli” pontokat) már „nagy” (a teljes térhez közeli) mértékű halmazt kapunk. A jelenség információelméleti hátterét a projekt egyik kutatója fedezte fel, azóta az információelméleti módszert az intenzíven kutatott témakör fő módszerei között tartják számon.
Rokon terület a logaritmikus Szoboljev egyenlőtlenségek elmélete, ahol már az alapprobléma megfogalmazásában is szerepel az entrópia. A munkatervnek megfelelően, ezeken a területeken is folytattuk korábbi kutatásainkat, a még kevésbé jól ismert nem független esetre koncentrálva. Fő eredményeink a szorzattér-beli relatív entrópiának a lokális specifikációk segítségével való becslésére vonatkoznak, ezen kívül bizonyítottunk új eredményeket logaritmikus Szoboljev egyenlőtlenségekről is.
A témával foglalkozó kutatónk korábbi eredményeiért 2012-ben nemzetközi díjat nyert (IEEE Information Theory Society, Shannon Award), melyet 2013-ban vett át és ez alkalomból plenáris előadást tartott a témáról.

(iv) A gráfelméletben fontos szerepük van információeméleti motiváltságú mértékszámoknak, mint pl. a Sperner kapacitás. A projekt keretében ilyen mértékszámok vizsgálatával foglalkoztunk.
Egyik fő irány a lokális kromatikus szám és ennek irányított gráfokra való általánosításának tanulmányozása volt. Publikált eredményeink többek között ezeknek egymással, a Sperner kapacitással, valamint geomeriai felületekre vonatkozó topológiai kérdésekkel való kapcsolatát állapították meg.
Említést érdemelnek a gráfok bizonyos típusú Hamilton útjaira, valamint az irányított végtelen gráfok ú.n. permutációs kapacitására vonatkozó eredményeink is.