A BSc-képzés szakdolgozati témái

Valószínűségelméleti és Statisztika Tanszék

2016/2017

1. *Téma:* **Véletlen gráfok és gráflimeszek**
Témavezető: Backhausz Ágnes
Rövid leírás: A nagy hálózatok elméleti szempontból történő kutatásának egyik legtöbbet vizsgált területe a gráfsorozatok konvergenciájának vizsgálata lett. Erre több különböző fogalom is született az utóbbi évtizedben. A megfelelő fogalmak megtalálása mellett ebben a témában azt a kérdést is több szempontból vizsgálták, hogy bizonyos módon sorsolt véletlen gráfok sorozata mikor konvergens (például 1 valószínűséggel). Természetesen ez is függ a gráfkonvergencia definíciójától.
A feladat egyrészt a véletlen gráfok konvergenciájáról szóló szakirodalom feldolgozása elsősorban a pozitív élsűrűségű esetre koncentrálva, amikor a sorozat határértéke egy $[0,1] \times [0,1]$-en értelmezett szimmetrikus, mérhető függvény lehet. A feladat másik része az [1] cikkben szereplő "randomly grown attachment" gráfmodell alaposabb vizsgálata, részben elméleti, részben számítógépes szimulációs módszerekkel. Ebben a modellben a gráfhoz az n. lépésben hozzávett csúcs $1 - i/n$ valószínűséggel kötődik hozzá a már létező i. csúcshoz, majd a régi csúcsok közötti további élek véletlenszerű behúzására is van lehetőség. Kérdés, hogy a konvergencia mennyire gyors (különböző gráftávolságokban értve), továbbá milyen további tulajdonságokkal rendelkezik ez a véletlengráf-sorozat, illetve a limeszobjektum.
Ajánlott irodalom:
[1] C. Borgs, J. Chayes, L. Lovász, V.T. Sós and K. Vesztergombi: Limits of randomly grown graph sequences, Eur. J. Combin. 32 (2011), 985-999.
[2] L. Lovász: Large networks and graph limits. American Mathematical Society, 2012.
[3] B. Szegedy and L. Lovász, Limits of dense graph sequences, J. Comb. Theory B 96 (2006), no. 6, 933–957.
Szak: alkalmazott matematikus, matematikus

2. *Téma:* **Az elágazó folyamatok és biológiai alkalmazásaik**
Témavezető: Backhausz Ágnes
Rövid leírás: Az elágazó folyamatok, melyek során minden egyed véletlen számú utódot hoz létre időről időre, különféle biológiai, evolúciós folyamatok gyakran használt modelljei közé tartoznak. Az egyedek különböző típusokra való felosztásával bizonyos genetikai jelenségek is modellezhetők így. A

feladat a kapcsolódó matematikai szakirodalom egy részének áttekintése, a kapcsolódó fogalmak és témakörök (pl. Crump–Mode–Jagers-folyamatok) ismertetése, valamint ehhez kapcsolódóan számítógépes szimulációk készítése.
Ajánlott irodalom:
[1] N. Champagnat, A. Lambert: Splitting trees with neutral Poissonian mutations I: Small families. Stochastic Processes and their Applications 122 (2012) no. 3., 1003–1033.
[2] P. Jagers, O. Nerman. The growth and composition of branching populations. Advances in Applied Probability, 16 (1984), no. 2., 221–259.
Szak: alkalmazott matematikus, matematikus

3. *Téma:* **Az MCMC algoritmus néhány alkalmazása** (a téma már foglalt)
Témavezető: Csiszár Villő
Rövid leírás: A Markov lánc Monte Carlo algoritmusokat számos területen alkalmazzák egy adott eloszlásból vett minta generálására. A szakdolgozat célja néhány valódi életbol vett alkalmazás bemutatása, esetleg rekonstruálása (programozás). Az alábbi ajánlott cikk kiindulásként szolgálhat.
Ajánlott irodalom:
[1] Persi Diaconis: The Markov Chain Monte Carlo revolution. *Bull. Amer. Math. Soc.* **(2009)**, 46, 179-205
Szak: alkalmazott matematikus, elemző

4. *Téma:* **Információelméleti mennyiségek axiomatikus jellemzése**
Témavezető: Csiszár Villő
Rövid leírás: Az információelméletben leggyakrabban használt mérőszámok (Shannon-entrópia, Rényi-entrópia, I-divergencia, stb) axiomatikus jellemzésének hatalmas irodalma van. Az ajánlott összefoglaló cikkből kiindulva kellene ezek közül néhányat áttekinteni.
Ajánlott irodalom:
[1] Csiszár Imre: Axiomatic characterizations of information measures. *Entropy* **2008**, 10, 261-273.
Szak: matematikus, alkalmazott matematikus

5. *Téma:* **Feleletválasztós tesztek kiértékelése** (a téma már foglalt)
Témavezető: Csiszár Villő
Rövid leírás: A szakdolgozat célja egy valós adatsor (online teszt a térképen való tájékozódási tudás felmérésére) elemzése. Az elemzéshez a fő eszköz az R-ben található **ltm** csomag lenne, mely különböző látens változó modelleket tud illeszteni. A dolgozat része természetesen az elmélet bemutatása is.
Ajánlott irodalom:

[1] Dimitris Rizopoulos: ltm: An R Package for Latent Variable Modeling and Item Response Theory Analyses. *Journal of Statistical Software* **2006**.
Szak: alkalmazott matematikus, elemző

6. *Téma:* **A Pólya-fele urnamodell** (a téma már foglalt)
Témavezető: Móri Tamás
Rövid leírás: A Pólya-fele urnamodell legegyszerűbb változatában egy urnából, amelyben néhány fehér és fekete golyó van, golyókat húzunk ki véletlenszerűen, és a kihúzott golyót visszatesszük további c ugyanolyan színű golyóval együtt. Kérdés az urna összetételének leírása az egymás utáni húzások során, illetve aszimptotika adása. Ennek az egyszerű modellnek nagyon sok általánosítása van, amelyeket különböző területeken alkalmaznak. A dolgozat ezeket mutatná be.
Ajánlott irodalom:
[1] N. L. Johnson, S. Kotz: *Urn Model and Their Application*, Wiley, 1977
Szak: matematikus, alkalmazott matematikus

7. *Téma:* **Statisztikai módszerek, alkalmazások**
Témavezető: Pröhle Tamás
Rövid leírás: A jelentkező hallgatók érdeklődésének megfelelő, szabadon választott statisztikai téma
Ajánlott irodalom: Tipikusan angol nyelvű cikkek
Szak: alkalmazott matematikus, elemző

8. *Téma:* **A WIFI titkosítás matematikai alapjai** (a téma már foglalt)
Témavezető: Szabó István
Rövid leírás: Az internetes kommunikáció biztonságának erősítése nagyon sokrétű matematikai és informatikai megközelítést igényel. Széleskörűen elterjedt alkalmazás a vezeték nélküli technológiák használata, amikor (általában nyilvános helyeken pl. repülőtér, hotel stb.) kialakított vezeték nélküli helyi hálózat segítségével saját számítógépünkkel kapcsolódhatunk a világhálóra. A WIFI biztonságáról, az alkalmazott protokollokról és kriptográfiai algoritmusok gyengeségeiről (pl. WEP: Wired Equivalent Privacy, vagy WPA: Wi-FI Protected Access,...) sok elemzés látott napvilágot, ezek áttekintése a szakdolgozat témája, különösen a matematikai támadó módszereket kell áttekinteni, valamint hogyan lehet védekezni a veszélyek ellen.
Ajánlott irodalom:
[1] Eric Tews: Attacks ont he WEP protocol, PhD Thesis, 2007.
`http://saluc.engr.uconn.edu/refs/stream_cipher/mantin01attackRC4.pdf`

[2] Buttyan Levente, Dóra László, Laczkó Péter: Mérési útmutató a "WIFI 1: Helyi hitelesítő eljárások elleni támadások" című méréshez,
http://saluc.engr.uconn.edu/refs/stream_cipher/mantin01attackRC4.pdf
[3] Erik Tews, Ralf-Philipp Weinmann, Andrei Pyshkin: Breaking 104 bit WEP in less than 60 seconds, 2007,
https://eprint.iacr.org/2007/120.pdf
[4] Matthieu Caneill, Jean-Loup Gilis: Attacks again the WiFi protocols WEP and WPA, 2010,
https://matthieu.io/dl/wifi-attacks-wep-wpa.pdf
Szak: matematikus, alkalmazott matematikus

9. *Téma:* **Az elliptikus görbéken alapuló titkosítás néhány matematikai kérdése** (a téma már foglalt)
Témavezető: Szabó István
Rövid leírás: Az internetes kommunikáció biztonságának erősítése nagyon sokrétű informatikai megközelítést és mély matematikai elemzéseket igényel. Nagyon dinamikusan fejlődik az elliptikus görbéken alapuló kriptográfiának mind a titkosítási -, mind a titkosításhoz szükséges aszimmetrikus kulcskialakítási -, mind az elektronikus aláírási algoritmusok területe. A téma feldolgozásában az elliptikus görbék támadási módszereire vonatkozó szakirodalomnak, az egyes módszerek hatékonyságára vonatkozó eredményeknek a rövid áttekintése szükséges, a módszerek hatékonyságából a biztonságos alkalmazáshoz szükséges javasolt algoritmusok, paraméterek felsorolásával.
Ajánlott irodalom:
[1] Aleksandar Jurisic, Alfred J. Menezes: Elliptic Curves and Cryptography,
http://www.cs.nthu.edu.tw/ cchen/CS4351/jurisic.pdf
[2] Certicom ECC Challenge,
https://www.certicom.com/pdfs/cert_ecc_challenge.pdf
[3] ECC challenge eredmények:
https://www.certicom.com/index.php/the-certicom-ecc-challenge
[4] Digital Signature Standard (DSS), FIPS PUB 186-3,2009:
http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
[5] Matthew Musson: Attacking the Elliptic Curve Discrete Logarithm Problem, PhD Thesis 2006.
Szak: alkalmazott matematikus, elemző

10. *Téma:* **Becslések torzításának csökkentése bootstrap segítségével**
Témavezető: Varga László
Rövid leírás: A bootstrap egy számításigényes statisztikai módszer különféle statisztikai feladatok – torzítás csökkentése, konfidencia intervallumok konstruálása, kvantilisek becslése, hipotézisek vizsgálata stb. – megoldására. A hallgató feladata bizonyos becslések torzításának csökkentése visszatevéses újramintavételezés többször ismételt alkalmazásával, az eredmények vizsgálata, alátámasztása alkalmasan választott szoftver segítségével.
Ajánlott irodalom:
[1] M. Chernick, R. LaBudde (2011), An introduction to bootstrap methods with applications to R, p. 1-11., 20-32.*John Wiley & Sons*
[2] P. Hall (1992), The bootstrap and Edgeworth Expansion, p. 30-53., *Springer*
Szak: alkalmazott matematikus

11. *Téma:* **Kupongyűjtés**
Témavezető: Varga László
Rövid leírás: A kupongyűjtési feladat egyike a valószínűségelmélet régi, klasszikus problémáinak. Az alapfeladat: vannak dobozok, amikben n-féle kupon közül egy szerepel. A kupongyűjtő addig vásárol újabb és újabb dobozokat, míg az összes fajta kupon meg nem lesz neki. Kérdés, hogy vajon várhatóan hányadik dobozban fogja megtalálni az utolsó fajta kupont; illetve mi az esélye, hogy ha m dobozt ($m \geq n$) vásárol, akkor ezekben mind az n-féle kupont meg lehet találni. A problémának számos kiterjesztése van, napjainkban is kedvelt kutatási terület, számos gyakorlati alkalmazással. A hallgató ezek közül szemezgethet.
Ajánlott irodalom:
[1] M. Ferrante, M. Saltalamacchia: The coupon collector's problem (2014), *Materials matemàtics*
[2] I. Adler, S. Ross: The coupon subset collection problem (2001), *Journal of Applied Probability*
Szak: matematikai elemző, alkalmazott matematikus

12. *Téma:* **Nemparaméteres sűrűségfüggvény-becslési eljárások**
Témavezető: Varga László
Rövid leírás: Egy adott, ismeretlen eloszlásból származó minta sűrűségfüggvényét leggyakrabban a hisztogrammal vagy a Parzen-Rosenblatt módszerrel szokás becsülni. A hallgató feladata a becslési módszerek és azok becsléselméleti tulajdonságainak áttekintése, valamint az **R** programnyelv témához

kapcsolódó package-einek felkutatása, majd saját és beépített függvényeket felhasználó szimulációk által az elméleti eredmények ellenőrzése.
Ajánlott irodalom:
[1] A. J. Izenman: Modern multivariate statistical techniques (2008), p. 75-107 *Springer*
[2] B. Silverman: Density estimation for statistics and data analysis (1986), *CRC Press*
Szak: elemző, alkalmazott matematikus

13. *Téma:* **Egyetlen szavazat ereje – power voting** (a téma már foglalt)
Témavezető: Varga László
Rövid leírás: Egy szavazat erejét annak a valószínűsége határozza meg, hogy az mennyivel nagyobb eséllyel fogja tudni a teljes szavazás végeredményét megváltoztatni. A hallgató feladata bizonyos, összetettebb választási modellek esetén a szavazat erejének becslése és a szavazás eredményének modellezése.
Ajánlott irodalom:
[1] N. Miller (2013): A priori voting power and the US Electoral College, *Springer*
[2] A. Gelman, G. King, J. Boscardin (1998): Estimating the probability of events that have never occurred: when is your vote decisive?, *Journal of the American Statistical Association*
[3] A. Gelman, J. Katz, F. Tuerlinckx (2002): The mathematics and statistics of voting power, *Statistical Science*
Szak: elemző, alkalmazott matematikus

14. *Téma:* **Labdarúgó-mérkőzések eredményeinek előrejelzése** (a téma már foglalt)
Témavezető: Varga László
Rövid leírás: A sakkban alkalmazott Élő-pontrendszer más sportágakban, így a labdarúgásban is kialakítható, aminek segítségével különböző matematikai modelleket lehet készíteni labdarúgó bajnokságok eredményeinek előrejelzésére. A hallgató feladata ezen modellek áttekintése és egy általa választott bajnokságra a legjobb kiválasztása múltbeli egymás elleni eredmények alapján, majd előrejelzés készítése egy teljes idényre vonatkozóan.
Ajánlott irodalom:
[1] J. Lasek, Z. Szlávik, S. Bhulai (2013): The predictive power of ranking systems in association football, *International Journal of Applied Pattern Recognition*

[2] A. Constantinou, N, Fenton, M. Neil (2012): pi-football: A Bayesian network model for forecasting Association Football match outcomes, *Knowledge-Based Systems*
[3] R. Stefani, R. Pollard et al (2007): Football rating systems for top-level competition: a critical survey, *Journal of Quantitative Analysis in Sports*
Szak: elemző, alkalmazott matematikus

15. *Téma:* **Kössünk biztosítást!**
Témavezető: Zempléni András
Rövid leírás: Számos ötlet felmerülhet, hogy mi az, ami váratlan kárt okoz és adott esetben egy fantáziadús biztosító megjelenhet az adott esemény bekövetkezése esetén kártérítést adó biztosítással.
A dolgozatban egy ilyen képzeletbeli biztosítás kidolgozása, árazása és a biztosító számára megjelenő kockázat modellezése lenne a feladat. Ez utóbbi feladatot az R programnyelv segítségével elvégzett szimulációval célszerű megoldani.
Ajánlott irodalom:
[1] Arató Miklós: Nem-élet biztosításmatematika. Eötvös kiadó, 2001.
Szak: elemző, alkalmazott matematikus