A BSc-képzés szakdolgozati témái

Valószínűségelméleti és Statisztika Tanszék

2018/2019

1. *Téma:* **Véletlen permutációk modellezése**
Témavezető: Arató Miklós
Rövid leírás: Szociológiai, pszichológiai kutatásokban igen gyakran fordulnak elő rangsorolási feladatok. A véletlen permutációkra az utóbbi években különböző modelleket javasoltak. A dolgozat bemutatná a véletlen permutációk különböző ábrázolási lehetőségeit és modelleit, továbbá néhány kapcsolódó feladatot szimulációkon keresztül is vizsgálna.
Ajánlott irodalom:
[1] M. A. Fligner and J. S. Verducci(eds.): *Probability Models and Statistical Analyses for Ranking Data* Springer-Verlag, New York (1993)
[2] Gladkich, Alexey and Peled, Ron: On the cycle structure of Mallows permutations,*Ann. Probab.*, Volume 46, no. 2 (2018) 1114-1169.
Szak: matematikus, alkalmazott matematikus

2. *Téma:* **Véletlen bolyongások véletlen gráfokon** (a téma már foglalt)
Témavezető: Backhausz Ágnes
Rövid leírás: Egy gráf szerkezetének jellemzésére az egyik lehetőség, hogy a gráf csúcsain értelmezett véletlen bolyongást vizsgáljuk. Erre a folyamatra egyrészt tekinthetünk úgy is, mint speciális Markov-láncra, vagy mint a számegyenesen definiált egyszerű szimmetrikus bolyongás általánosítására. Az átmenet-valószínűségeket is módosíthatjuk, mint például a Metropolis–Hastings-típusú (ahol a stacionárius eloszlást írjuk elő) vagy az öntaszító (ahol a korábban gyakrabban látogatott csúcsokba kisebb valószínűséggel lépünk) modellekben. Mindezeket a folyamatokat véletlen gráfokon (például Erdős–Rényi-gráf, preferential attachment gráfok) vizsgálva ezek struktúrájáról is nyerhetünk új információkat.
A feladat a kapcsolódó szakirodalom egy részének feldolgozása, a gráfokon való bolyongás és a Markov-láncok elmélete közötti összefüggések ismertetése a szakdolgozatban, valamint saját szimulációk készítése, ahol különböző típusú vagy eltérő paraméterekkel rendelkező véletlen gráfok között vizsgálhatók a hálózaton zajló véletlen bolyongás jellemzői (egyes csúcsokban töltött idő, keverési idő, stb.)
Ajánlott irodalom:
[1] N. Berestycki, E. Lubetzky, Y. Peres and A. Sly, Random walks on the random graph, Ann. Probab. 46 (2018), no. 1., 456–490.

[2] C. Cooper and A. Frieze, Random Walks on Random Graphs. In: Cheng M. (eds) Nano-Net. NanoNet 2008. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 3 (2009). Springer, Berlin, Heidelberg.
[3] D. A. Levin, Y. Peres, E. Wilmer, Markov chains and mixing times. American Mathematical Society, 2017.
Szak: alkalmazott matematikus, matematikus

3. *Téma:* **A mintanagyság meghatározásának módszerei**
Témavezető: Csiszár Villő
Rövid leírás: A szakdolgozatban a hallgató áttekinti, hogy milyen módszereket szokás a mintanagyság meghatározására alkalmazni a természettudományos kísérletekben, ahol a költségek gyakran behatárolják a lehetőségeket (kísérleti állatok). Ezután meg lehet vizsgálni, hogy a túl kis mintán végzett kutatások eredményeinek megbízhatóságával kapcsolatban milyen kétségek merülhetnek fel.
Ajánlott irodalom: K. S. Button et al.: Power failure: why small sample size undermines the reliability of neuroscience. Nature Reviews Neuroscience (2013).
Szak: alkalmazott matematikus, elemző.

4. *Téma:* **Véletlen permutációk modelljei**
Témavezető: Csiszár Villő
Rövid leírás: Hogyan állítja fel egy szavazó a választáson induló jelöltek sorrendjét? Hogyan keverednek össze a dossziék az irodában? Hanghatásokat hogyan rendezünk sorba erősségük szerint? A dolgozatban a véletlen permutációk kialakulásának számos modellje vizsgálható, a hallgató érdeklődésének megfelelően.
Ajánlott irodalom: J. I. Marden: Analyzing and modeling rank data. Chapman & Hall (1995).
Szak: mindegyik.

5. *Téma:* **A főkomponens-analízis és a Kosambi-Karhunen-Loéve tételkör gyakorlati alkalmazásai**
Témavezető:
Rövid leírás: Kornyik Miklós
Ajánlott irodalom:
Szak: A főkomponens-analízis és a Karhunen-Loéve elmélet a gyakorlatban (pl. neurobiológia, neurális hálózatok, szeizmológia, képfeldolgozás) széleskörűen elterjedt eszközök többdimenziós minták illetve idősorok elemzésére.

Sok esetben az adatsor zajjal terhelt jel és a cél az eredeti jel kinyerése. A hallgató feladata a PCA és/vagy KL sorfejtés elméletének megértése mellett annak gyakorlati példán való programozása (preferált "nyelv" MATLAB) és az eredmények értékelése. Idő függvényében más módszerekkel is össze lehet vetni az előzőeket.

[1] Oja, E. Principal components, minor components, and linear neural networks. Neural Networks, 1992,5.6:927–935
[2] Jorgensen, P. E., Song, M. S. Entropy encoding, Hilbert space, and Karhunen-Lo?ve transforms. Journal of Mathematical Physics, 2007, 48(10), 103503.
[3] Mudrova, M., and A. Prochazka. "Principal component analysis in image processing." Proceedings of the MATLAB Technical Computing Conference, Prague. 2005. alkalmazott matematikus

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:* **Véletlen fák aszimptotikus vizsgálata** (a téma már foglalt)
Témavezető: Rozner Bence
Rövid leírás: A nagyméretű hálózatok véletlen gráfokkal történő modellezése az utóbbi néhány évtizedben a matematika egyik intenzíven kutatott területe lett. Ezt elsősorban a gyakorlati alkalmazások szempontjából is fontos

hálózatok motiválják, mint például az internet, illetve szociológiai és biológia hálózatok.
A diszkrét lépésekben fejlődő véletlen fák különféle modelljei alkalmasak a genetikából jól ismert mutáció modellezésére. Az általános gráfokkal szemben, a véletlen fák esetében gyakran elemi valószínűségelméleti módszerek segítségével igazolhatók olyan mélyebb állítások, amelyek leírják a kérdéses struktúrák hosszútávú viselkedését.
A feladat a szakirodalomban ismert modellek egy részének áttekintése, és a kapcsolódó eredmények bemutatása, valamint saját szimulációk készítése.
Ajánlott irodalom:
[1] E. Hiesmayr, Ü. Işlak. *Asymptotic results on Hoppe trees and its variations.* arXiv preprint arXiv:1712.03572, 2017.
[2] K. Leckey, R. Neininger. *Asymptotic analysis of Hoppe trees.* Journal of Applied Probability, 2013, 50.1: 228-238.
[3] M. Rafler. *Hoppe trees, random recursive sets and their barycentre.* arXiv preprint arXiv:1207.1636, 2012.
Szak: alkalmazott matematikus, elemző

9. *Téma:* **A WIFI titkosítás matematikai alapjai**
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

10. *Téma:* **Az RSA kriptográfiai algoritmus paraméter-követelményeinek változása** (a téma már foglalt)
Témavezető: Szabó István
Rövid leírás: Miután Rivest, Shamir és Adleman publikálta az RSA algoritmust, nagyon gyorsan általánosan alkalmazásra került, és ma is jelentős szerepe van az internetes kommunikáció biztonsági megoldásaiban. A publikálás után jelentős kutatások indultak, publikációk sokasága jelent meg az alkalmazások támadási lehetőségeiről, ezek alapján a biztonsági szempontok folyamatos érvényesítése érdekében folyamatosan változtak az RSA paramétereivel szembeni követelmények, melyek érintették mind a paraméterek nagyságrendi elvárásait, mind a paraméterek véletlen választásának és tesztelésének eljárásait. A szakdolgozatban kerüljenek áttekintésre a kezdeti követelményektől a legújabb mértékadó szabványkövetelmények és néhány változás indokolása
Ajánlott irodalom:
[1] Rivest, Shamir és Adleman: A method for obtaining digital signatures and public-key cryptosystems, Comm.of ACM, 1978;
https://people.csail.mit.edu/rivest/Rsapaper.pdf
[2] NIST (National Institute of Standards and Technology) követelmények (pl. 800-56B, 800-57, 800-131A,...;
https://csrc.nist.gov/publications/sp800
[3] Matthieu Caneill, Jean-Loup Gilis: Attacks again the WiFi protocols WEP and WPA, 2010,
https://matthieu.io/dl/wifi-attacks-wep-wpa.pdf
[4] CCITT (Comité Consultatif Internationale de Télégraphique et Téléphonique) X:509, 11/1988 (C6 és C7 fejezet)
[5] SOG_IS (Senior Officials Group Information Systems Security) SOG-IS Crypto Working Group SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms (2018);
https://www.sogis.org/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-
[6] További saját forráskutatás
Szak: matematikus, alkalmazott matematikus

11. *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

12. *Téma:* **Sport-rekordok matematikai modelljei** (a téma már foglalt)
Témavezető: Zempléni András
Rövid leírás: A feladat az [1] cikk alapján feldolgozni a sport-rekordok elemzésére alkalmas módszereket. Ez valószínűségszámítási és statisztikai kérdések vizsgálatát egyaránt magában foglalja.
A dolgozatban a módszerek valós adatsorokra történő alkalmazására is sor kerül Ez utóbbi feladatot az R programnyelv segítségével elvégzett elemzéssel célszerű megoldani.
Ajánlott irodalom:
[1] Adam, M. B. and Tawn, J. A.: Modelling Record Times in Sport with Extreme Value Methods, Malaysian Journal of Mathematical Sciences 10(1): 1-21 (2016)
Szak: alkalmazott matematikus