

# A BSc- és MSc-képzés szakdolgozati témái

ELTE TTK, Valószínűségelméleti és Statisztika Tanszék

2011/2012

## BSc

### 1. Szabadon választható téma

*Témavezető:* A tanszék bármelyik oktatója, vagy (a tanszékvezető által jóváhagyott) külső szakember.

**A téma rövid leírása:** Ha egy hallgató tetszőleges valószínűségi számítási vagy statisztikai téma iránt érdeklődik, akkor témavezetőnek választhatja azt a szakembert, aki ehhez ért, és ebben segítséget tud neki nyújtani.

**Ajánlott irodalom:** a hallgató és a témavezető megállapodása alapján

**Ajánlott szakirányok:** mindegyik

### 2. Urnamodellek

*Témavezető:* Backhausz Ágnes

**A téma rövid leírása:** A legegyszerűbb Pólya-féle urnamodellben kezdetben adott számú fehér és piros golyó van. Minden lépésben húzunk egyet. Ha fehéret húzunk, még egy fehér, míg ha pirosat, még egy piros golyót teszünk az urnába. Az Ehrenfest-féle urnamodellben két urnánk van, itt a húzások után egyik urnából lehet a másikba helyezni a golyókat.

Mindkét modellt sokféleképpen általánosították. Például a Pólya–Eggenberger-féle urnamodellben a húzott golyó színétől függően adott számú fehér és piros golyót lehet az urnába helyezni vagy éppen kivenni.

Vizsgálni szokták, hogy adott számú lépés után milyen az eloszlása a különböző színű, illetve különböző urnákban elhelyezkező golyók számának, továbbá hogyan viselkedik a modell aszimptotikusan, a lépések számával végtelenhez tartva. A módszerek jöhetnek például a Markov-láncok vagy a martingálok elméletéből is.

A feladat minél több urnamodellre vonatkozó eredmény és módszer feldolgozása, valamint a különböző modellek összehasonlítása.

**Ajánlott irodalom:** Johnson, N. L., Kotz, S., *Urn models and their application*, John Wiley & Sons, New York (1977)

Mahmoud, H.M., *Polya urn models*, Chapman & Hall/CRC (2009)

**Ajánlott szakirányok:** matematikus, alkalmazott matematikus, matematikatanár

### 3. Lokális jelenségek véletlen gráfokban

Témavezető: Backhausz Ágnes

**A téma rövid leírása:** Diszkrét időben fejlődő véletlen gráfsorozatokot vizsgálunk. Minden lépésben egy új csúcst adunk a gráfhoz, amely egy-egy éllel csatlakozik néhány, véletlenszerűen kiválasztott régi csúcshoz. Tekinteni lehet minden  $d$  egész számra a  $d$  fokú csúcsok arányát. Több modellnél ez 1 valószínűséggel konvergál valamely  $c_d$  pozitív számhoz. Azokat a modelleket, melyekben  $c_d$  polinomiálisan csökken  $d$ -vel végtelenhez tartva (azaz  $c_d \sim d^{-\gamma}$ ), skálafüggetlen modelleknek nevezik, és gyakran használják nagy méretű hálózatok (internet, szociális hálók) modellezésére.

Bizonyos skálafüggetlen modellekben fellép a következő jelenség. Rögzítsünk egy csúcst, és tekintsük a  $d$  fokú csúcsok arányát ennek szomszédai között. Ez is konvergálhat egy valószínűséggel, viszont a határérték  $c_d$ -től különböző, sőt a polinomiális csökkenés kitevője is megváltozik.

A feladat a fenti jelenség elméleti hátterének összefoglalása és számítógépes szimulációja a különböző modellekben.

**Ajánlott irodalom:** R. Durrett, *Random graph dynamics*, Cambridge University Press, 2006

**Ajánlott szakirányok:** elemző, alkalmazott matematikus

### 4. Véletlen bolyongás csoportokon

Témavezető: Csiszár Villő

**A téma rövid leírása:** Jónéhány gyakorlati feladatban kell csoportokon való véletlen bolyongásokat vizsgálni, például az Ehrenfest urnamodellben (a csoport  $Z_2^d$ ), véletlenszám-generátorok elemzésénél (a csoport  $Z_p$ ), vagy a különböző kártyakeverési módszerek összehasonlításakor (a csoport  $S_n$ ). A tanulmányozandó kérdés, hogy a bolyongás milyen gyorsan jut el egy „teljesen véletlenszerű” állapotba. A témát Persi Diaconis igen jó stílusú és olvasmányos könyve alapján ajánlom, ezen kívül szimulációs vizsgálatokra is lehetőség nyílik.

**Ajánlott irodalom:** P. Diaconis: *Group Representations in Probability and Statistics* (1988), 3. és 4. fejezet

**Ajánlott szakirányok:** matematikus, alkalmazott matematikus, elemző

### 5. „Shrinkage” módszerek a lineáris regresszióban

Témavezető: Csiszár Villő

**A téma rövid leírása:** Ha egy mért változót bizonyos magyarázó változók lineáris függvényével szeretnénk közelíteni, a legkisebb négyzetek módszerét használhatjuk. Ez azonban nem mindig ad kielégítő eredményt, túl nagy lehet a predikciós hiba, instabilak a becsült paraméterek, illetve nehezen értelmezhető a modell. Ezen segíthetnek a „shrinkage” módszerek, mint például a ridge regresszió, vagy a lasso. A hallgató feladata a módszerek, algoritmusok ismertetése, illetve illusztrálásuk egy példa adatsoron.

**Ajánlott irodalom:** T. Hastie, R. Tibshirani, J.H. Friedman: The elements of statistical learning (2008), 3. fejezet

**Ajánlott szakirányok:** elemző, alkalmazott matematikus

## 6. Szindbád és a részben rendezett háremhölgyek

*Témavezető:* Csiszár Villő

**A téma rövid leírása:** A klasszikus feladatban Szindbádnak úgy kell a legszebbet kiválasztani az előtte elvonuló háremhölgyek közül, hogy csak az egymáshoz képesti szépségüket tudja megítélni. A legjobb stratégia ebben az esetben, ha  $n/e$  hölgyet elenged, majd kiválasztja az első olyat, aki az összes addiginál szebb. A szakdolgozatban azt a kérdést kell körüljárni, hogy mi a teendő, ha a hölgyek halmaza csak részben rendezett.

**Ajánlott irodalom:** R. Freij, J. Wastlund: Partially ordered secretaries (2010)

R. Kumar et al.: Hiring a secretary from a poset (2011)

B. Garrod, R. Morris: The secretary problem on an unknown poset (2011)

**Ajánlott szakirányok:** mindegyik

## 7. Optimális portfóliók kialakítása

*Témavezető:* Csiszár Villő

**A téma rövid leírása:** Markowitz 1952-ben alkotta meg az optimális portfóliókra vonatkozó elméletét. Ennek általánosításával lehetne a szakdolgozatban foglalkozni. Az egyik lehetőség annak az esetnek a vizsgálata, ha a részvények várható hozamáról nincs pontos információnk, csak valamilyen egyenlőtlenségeket tételezünk fel (pl. tudjuk, melyik részvénynek lesz a legnagyobb hozama, melyeknek lesz pozitív hozama, stb.).

**Ajánlott irodalom:** R. Almgren, N. Chriss: Optimal portfolios from ordering information (2004)

**Ajánlott szakirányok:** elemző, alkalmazott matematikus

## 8. Sock-modellek

**Ez a téma már foglalt**

*Témavezető:* Móri Tamás

**A téma rövid leírása:** Tekintsünk egy olyan rendszert, amelyet az idők folyamán véletlenszerű sokkok érnek, melyek következtében végül is tönkremegy. Mi mondható a rendszer élettartam-eloszlásának öregedő tulajdonságairól, ha különféle feltételeket teszünk a sokkok időbeli bekövetkezésének folyamatára, és a sokkok által okozott kár nagyságára. Ehhez előbb meg kell ismerkedni a megbízhatóságelméletben használatos öregedő eloszlások különféle osztályaival.

**Ajánlott irodalom:** Móri Tamás: *Élettartam-adatok elemzése*, Typotex Kft., Budapest, 2011

<http://www.interkonyv.hu/konyvek/%C3%89lettartamadatok%20elemz%C3%A9se>

R. E. Barlow, F. Proschan, *Statistical Theory of Reliability and Life Testing*, Holt, Rinehart and Winston, New York, 1975.

**Ajánlott szakirányok:** alkalmazott matematikus, matematikus

## 9. Biztosító kárkifizetési adatainak elemzése

**Ez a téma már foglalt**

*Témavezető:* Zempléni András

**A téma rövid leírása:** A vizsgálandó adatbázis több évre visszamenőleg tartalmazza számos háttérváltozó és a kárszám, kárösszeg értékeit. A feladat a tanult statisztikai módszerek, így elsősorban próbák, regressziós eljárások önálló alkalmazása, a kapott eredmények értékelése. Az elemzés célszerűen az R programnyelv segítségével történhet.

**Ajánlott irodalom:** Bolla–Krámlí: Statisztikai következtetések elmélete

**Ajánlott szakirányok:** elemző

## 10. Sportfogadások matematikai modellezése

**Ez a téma már foglalt**

*Témavezető:* Zempléni András

**A téma rövid leírása:** Különböző sportesemények eredményeinek modellezése és az eredmények összevetése az adott eseményekre vonatkozó oddsokkal. Alkalmazott módszerek: eloszlásillesztés, regresszió.

**Ajánlott irodalom:** Dixon, M.J., Coles, S.G: Modelling association football scores and inefficiencies in the football betting market (Applied Statistics, 1997)

**Ajánlott szakirányok:** mindegyik

## MSc

### 11. Szabadon választható téma

*Témavezető:* A tanszék bármelyik oktatója, vagy (a tanszékvezető által jóváhagyott) külső szakember.

**A téma rövid leírása:** Ha egy hallgató tetszőleges valószínűségszámítási vagy statisztikai téma iránt érdeklődik, akkor témavezetőnek választhatja azt a szakembert, aki ehhez ért, és ebben segítséget tud neki nyújtani.

**Ajánlott irodalom:** a hallgató és a témavezető megállapodása alapján

**Ajánlott szakirányok:** mindegyik

### 12. Valószínűségi módszerek

**Ez a téma már foglalt**

*Témavezető:* Móri Tamás

**A téma rövid leírása:** A matematika különféle ágaiban egyre nagyobb sikerrel alkalmaznak valószínűségszámításból kölcsönzött módszereket: Markov-, Csebisev-egyenlőtlenség, centrális határeloszlás-tétel, martingálok, Azuma- és McDiarmid-egyenlőtlenség, Lovász lokális lemmája, stb. Kiváló összefoglaló muvek is elérhetők. A szakdolgozat célja a módszerek áttekintése és illusztrálása, olyan példákon keresztül, amelyek különböznek a közismert monográfiákban és tankönyvekben szereplőktől.

**Ajánlott irodalom:** N. Alon, J. H. Spencer, *The Probabilistic Method*, Wiley, New York, 1991

J. M. Steele, *Probability Theory and Combinatorial Optimization*, SIAM, 1997

Lovász László: *Véletlen struktúrák és alkalmazásai*

<http://www.cs.elte.hu/~lovasz/random-2010.pdf>

**Ajánlott szakirányok:** alkalmazott matematikus, matematikus

### 13. Kétmintás statisztikai eljárások

**Ez a téma már foglalt**

*Témavezető:* Móri Tamás

**A téma rövid leírása:** A statisztikai hipotézisvizsgálat fontos feladata, amikor két független minta összehasonlítása által próbálunk következtetéseket levonni. A szakdolgozat célja, hogy az alapkursusokban szereplő próbák (Student-, Kolmogorov-Szmirnov-, Wilcoxon-próba) túl további érdekes eljárásokat keressen és írjon le, főként az élettartam adatok elemzése témakörből.

**Ajánlott irodalom:** Móri Tamás: *Élettartam-adatok elemzése*, Typotex Kft., Budapest, 2011

<http://www.interkonyv.hu/konyvek/%C3%89lettartam adatok%20elemz%C3%A9se>

D. R. Cox, D. Oakes, *Analysis of Survival Data*, Chapman and Hall, London, 1984

**Ajánlott szakirányok:** alkalmazott matematikus, matematikus

### 14. A mobil kommunikáció kriptográfiai biztonsága

*Témavezető:* Szabó István

**A téma rövid leírása:** A szakdolgozatban röviden át kell tekinteni a mobil (GSM) kommunikáció kriptográfiai algoritmusait (A5/1, A5/2, A5/3, A3, A8), a matematikai alapokat (shift regiszterek, illetve ezekből összeállított rendszerek periódusaira és statisztikai tulajdonságaira vonatkozó tételeket), az alkalmazott algoritmusokat és ismertetni, elemezni kell a szakirodalomban található legfontosabb eredményeket a használt algoritmusok biztonságáról.

**Ajánlott irodalom:** Alapokhoz:

Nemetz T.- Vajda I.: Algoritmikus adatvédelem,

Buttyán L. - Vajda I. : Kriptográfia és alkalmazásai, Typotex, 2004

Elemzéshez:

A. Biryokov, A. Shamir, D. Wagner: Real Time Cryptanalysis of A5/1 on a PC, Cryptome: <http://cryptome.org/a51-bsw.htm>

E. Barkan, E. Biham, N. Keller: Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication: <http://cryptome.org/gsm-crack-bbk.pdf>

**Ajánlott szakirányok:** alkalmazott matematikus, matematikus

## 15. Új kriptográfiai algoritmusok a hálózati kommunikációban

*Témavezető:* Szabó István

**A téma rövid leírása:** A hagyományos pont-pont titkosítás (ide tartoznak a Shannon modellen alapuló titkos kulcsú, valamint a nyilvános kulcsú titkosítások) lehetőségeihez képest a nagy hálózatokban teljesen új elvű, a lineáris hálózati kódoláson alapuló kriptográfiai lehetőségek jelentek meg (melyek egyrészt a C. Shannon információelméleti eredményein alapuló One-Time-Pad titkosítás, másrészt A. Shamir Secret Sharing módszere általánosításának tekinthetők). A szakdolgozat témája ezen információelméleti biztonságot garantáló új hálózati titkosítási módszerek eredményeinek áttekintése, az alkalmazhatósági feltételek további vizsgálata.

**Ajánlott irodalom:** Alapokhoz:

R.W.Yeung, S.Y.R.Li, N.Cai, Z.Zhang: "Network Coding Theory":

<http://iest2.ie.cuhk.edu.hk/~whyueung/publications/tutorial.pdf>

Elemzéshez:

R. Koetter, M. Médard: "An Algebraic Approach to Network Coding", IEEE ACM Trans., on Networking, Vo. 11, No 5, oct. 2003 (Interneten letölthető)

N.Cai, R. Yeung: "A Security Condition for Multi-Source Linear Network Coding": <http://iest2.ie.cuhk.edu.hk/~whyueung/publications/secure2.pdf>

Q. Guo, M. Luo, L. Li, Y Yang: "Secure Network Coding against Wiretapping and Byzantine attacks" (Interneten letölthető)

L. Lima, M. Médard, J. Barros: "Random Linear Network Coding: A free cipher?": <http://www.mit.edu/~medard/page2/papers08/lima-medard-barros.pdf>

**Ajánlott szakirányok:** alkalmazott matematikus, matematikus