EÖTVÖS LORÁND TUDOMÁNYEGYETEM
MATEMATIKAI INTÉZET

MATEMATIKUS MESTERKÉPZÉS

TÁRGYLEÍRÁSOK

Valószínűségelméleti és Statisztika Tanszék

BUDAPEST 2013

Tantárgy neve: Bevezetés az információelméletbe **(C46)**

Tantárgy heti óraszáma:	2+0
kreditértéke:	3+0
tantárgyfelelős neve:	Csiszár Villő
tanszéke:	Valószínűségelméleti és Statisztika Tanszék
számonkérés rendje:	kollokvium
előtanulmányi feltétel:	Valószínűségszámítás és statisztika (a matematikus és alkalmazott matematikus szakirányról érkezetteknél teljesítettnek tekintve)

Az elsajátítandó ismeretanyag rövid (néhány soros) leírása:

Forráskódolás változó hosszúságú és blokk-kódokkal. Entrópia és formális tulajdonságai. I-divergencia és formális tulajdonságai. Tipikus sorozatok. A zajos csatorna fogalma, csatornakódolási tételek. Csatornakapacitás és kiszámítási módjai. Forrás- és csatornakódolás lineáris kódokkal. Több felhasználós hírközlő rendszerek: korrelált források egyedi kódolása. Az additív Gauss-zajú csatorna.

Kötelező irodalom:

Ajánlott irodalom:

Csiszár – Körner: Information Theory: Coding Theorems for Discrete Memoryless Systems. Akadémiai Kiadó, 1981.

Cover – Thomas: Elements of Information Theory. Wiley, 1991.

Tantárgy neve: Diszkrét és folytonos paraméterű Markov-láncok (B16)

Tantárgy heti óraszáma:	2+0
kreditértéke:	2+0
tantárgyfelelős neve:	Prokaj Vilmos
tanszéke:	Valószínűségelméleti és Statisztika Tanszék
számonkérés rendje:	kollokvium
előtanulmányi feltétel:	Valószínűségszámítás és statisztika (gyenge előfeltétel) (a matematikus és alkalmazott matematikus szakirányról érkezetteknél teljesítettnek tekintve)

Az elsajátítandó ismeretanyag rövid (néhány soros) leírása:

Sztochasztikus folyamatok: Markov-tulajdonság, erős Markov-tulajdonság, homogenitás. Diszkrét paraméterű Markov-láncok: definíció, átmenetmátrix, az állapotok osztályozása. Periódus, visszatérőség. Az átmenetvalószínűségek konvergenciája. Stacionárius eloszlás. Nagy számok törvénye és centrális határeloszlás-tétel irreducibilis, pozitív rekurrens Markov-lánc funkcionáljára. Átmenetvalószínűségek tabu állapotokkal. Reguláris mérték, Doeblin hányados tétele. Megfordított Markov-lánc. Elnyelődési valószínűségek. Perron-Frobenius tételek. Folytonos paraméterű Markov-láncok: definíció, átmenetmátrix, derivált a nullában, infinitezimális generátor. Példák: Poisson folyamat, születési és halálozási folyamatok.

Kötelező irodalom:

Ajánlott irodalom:

Karlin – Taylor: Sztochasztikus folyamatok. Gondolat Kiadó, 1985.
Chung: Markov Chains With Stationary Transition Probabilities. Springer, 1967.
Isaacson – Madsen: Markov Chains: Theory and Applications. Wiley, 1976.

Tantárgy neve: Diszkrét paraméterű martingálok (B17)

Tantárgy heti óraszáma:	2+0
kreditértéke:	2+0
tantárgyfelelős neve:	Móri Tamás
tanszéke:	Valószínűségelméleti és Statisztika Tanszék
számonkérés rendje:	kollokvium
előtanulmányi feltétel:	Valószínűségszámítás és statisztika (a matematikus és alkalmazott matematikus szakirányról érkezetteknél teljesítettnek tekintve)

Az elsajátítandó ismeretanyag rövid (néhány soros) leírása:

Martingálok 1 valószínűségű és L_p-beli konvergenciája, reguláris martingálok.
Reguláris megállási idők, Wald-azonosság.
Négyzetesen integrálható martingálok konvergenciahalmaza.
Hilbert-tér értékű martingálok.
Centrális határeloszlás-tétel martingálokra.
Fordított martingál, *U*-statisztikák, felcserélhetőség.
Alkalmazások: Martingálok a pénzügyi matematikában, a Conway-algoritmus, optimális stratégiák nyereséges játékokban, elágazó folyamat kétféle típusú egyedekkel.

Kötelező irodalom:

Ajánlott irodalom:

Móri Tamás.: Diszkrét paraméterû martingálok. Typotex Kft., Budapest, 2011.
Y. S. Chow – H. Teicher: Probability Theory – Independence, Interchangeability, Martingales. Springer, New York, 1978.
J. Neveu: Discrete-Parameter Martingales. North-Holland, Amsterdam, 1975.

Tantárgy neve: Független növekményű folyamatok, határeloszlás-tételek (C47)

Tantárgy heti óraszáma:	2+0
kreditértéke:	3+0
tantárgyfelelős neve:	Prokaj Vilmos
tanszéke:	Valószínűségelméleti és Statisztika Tanszék
számonkérés rendje:	kollokvium
előtanulmányi feltétel:	Valószínűségszámítás és statisztika (a matematikus és alkalmazott matematikus szakirányról érkezetteknél teljesítettnek tekintve)

Az elsajátítandó ismeretanyag rövid (néhány soros) leírása:

Korlátlanul osztható eloszlás és karakterisztikus függvény. Poisson folyamat, összetett Poisson folyamat. Poisson pontfolyamat általános karakterisztikus mérték mellett. Pontfolyamat szerinti integrál. Lévy–Hincsin formula. Nem negatív és véges szórású korlátlanul osztható eloszlások karakterisztikus függvénye. Stabilis eloszlások karakterisztikus függvénye. Stabilis eloszlások generálása, farok-valószínűség nagyságrendje. Szériasorozatok határeloszlásai.

Kötelező irodalom:

Ajánlott irodalom:

Y. S. Chow – H. Teicher: Probability Theory: Independence, Interchangeability, Martingales. Springer, New York, 1978.

W. Feller: An Introduction to Probabilty Theory and its Applications, vol. 2. Wiley, New York, 1966.

Tantárgy neve: Kriptográfia **(C48)**

Tantárgy heti óraszáma: 2+0
kreditértéke: 3+0

tantárgyfelelős neve: Szabó István
tanszéke: Valószínűségelméleti és Statisztika
számonkérés rendje: C típusú kollokvium
előtanulmányi feltétel: Valószínűségszámítás és statisztika (a matematikus és alkalmazott matematikus szakirányról érkezetteknél teljesítettnek tekintve)

Az elsajátítandó ismeretanyag rövid (néhány soros) leírása:

Az informatikai adatvédelem alapjai: jogi környezet, veszélyek, szteganográfia-kriptográfia alapfogalmai
Adatvédelmi módszerek: algoritmusok és a biztonság garanciális /bizonyítási/ módszerei
- A kriptográfia története, történelmi hibák és kihasználásuk
- Információelméleti megközelítés (Shannon modell, egyértelműségi pont, OTP)
- Szimmetrikus (titkos) kulcsú rendszerek
- Stream ciphers: LFSR, lineáris ekvivalens fogalma, LFSR rendszerek, benne a GSM titkosítás (A5/1-A5/2), WLAN, BlueTooth titkosítás, statisztikai és algebrai követelmények a biztonságos stream-cipher rendszerekkel szemben
- Block ciphers: LUCIFER, DES, PES, IDEA, AES
- Aszimmetrikus (nyilvános) kulcsú (PKI) rendszerek

Egyirányú függvények, klasszikus matematikai problémákon alapuló algoritmusok, kulcsegyeztetők (Merkle-Hellmann, DLP-n alapuló), PKI kódolók (RSA, ECC), Hash függvények, elektronikus aláírási algoritmusok (RSA, DSA, ECDSA), elektronikus aláírási rendszerek (technológia, jogi-, szervezeti intézményi rendszer), egyéb protokollok (blind signature, secret sharing, …)
- Lineáris- és differenciál kriptoanalízis, faktorizációs módszerek, protokollhibák

Adatvédelmi rendszerek felépítése: primitívek, sémák, protokollok, alkalmazások (gyenge pontok és követelmények)
Nemzetközi és hazai szabványok és projektek (ISO/IEC, NIST, ANSI, FIPS, RFC, ETSI).
IT biztonsági módszertanok: MSZ ISO 15408: /Common Criteria/ 2008; /CEM/:2009; FIPS PUB 140-2:2001.

Kötelező irodalom:

Ajánlott irodalom:

Nemetz-Vajda: Algoritmusos adatvédelem.
Buttyán-Vajda: Kriptográfia és alkalmazásai.
Bruce Schneier: Applied Cryptography.
Alfred J. Menezes, Paul C. van Oorshchor, Scott A. Vanstone: Handbook of Applied Cryptography, CRC Press, 1997, online: http://www.cacr.math.uwaterloo.ca/hac/

Tantárgy neve: Statisztikai hipotézisvizsgálat (C49)

Tantárgy heti óraszáma:	2+0
kreditértéke:	3+0
tantárgyfelelős neve:	Csiszár Villő
tanszéke:	Valószínűségelméleti és Statisztika Tanszék
számonkérés rendje:	kollokvium
előtanulmányi feltétel:	Valószínűségszámítás és statisztika (a matematikus és alkalmazott matematikus szakirányról érkezetteknél teljesítettnek tekintve)

Az elsajátítandó ismeretanyag rövid (néhány soros) leírása:

Statisztikai hipotézisek, próbák, véletlenített próbák. Elsőfajú, másodfajú hiba, szint, terjedelem, erőfüggvény. Likelihood-hányados próba, Neyman-Pearson lemma. Az erő aszimptotikája. Egyoldali ellenhipotézis monoton likelihood-hányadosú osztályban. Kétodali ellenhipotézis exponenciális eloszláscsaládban. Hasonlóság, Neyman-struktúra. Hipotézis-vizsgálat zavaró paraméterek jelenlétében.
A klasszikus paraméteres próbák optimalitása. Aszimptotikus próbák. Általánosított likelihood-hányados próba, a khi-négyzet próbák levezetése.
A tapasztalati folyamat konvergenciája Brown-hídhoz. Gauss-folyamatok Karhunen-Loève sorfejtése. A klasszikus nemparaméteres próbák aszimptotikus elemzése.
Invariáns és Bayes-próbák.
A konfidenciahalmazok elméletének kapcsolata a hipotézisvizsgálattal.

Kötelező irodalom:

Ajánlott irodalom:

Móri Tamás: Statisztikai hipotézisvizsgálat. Typotex Kft., Budapest, 2011.
Bolla M.–Krámli A.: Statisztikai következtetések elmélete. Typotex Kiadó, Budapest, 2005.
A. A. Borovkov: Matematikai statisztika. Typotex Kiadó, Budapest, 1999.
E. L. Lehmann: Testing Statistical Hypotheses, 2nd Ed., Wiley, New York, 1986.

Tantárgy neve: Statisztikai programcsomagok 1 (B18)

Tantárgy heti óraszáma:	0+2
kreditértéke:	0+3
tantárgyfelelős neve:	Zempléni András
tanszéke:	Valószínűségelméleti és Statisztika Tanszék
számonkérés rendje:	gyakorlati jegy
előtanulmányi feltétel:	Valószínűségszámítás és statisztika (a matematikus és alkalmazott matematikus szakirányról érkezetteknél teljesítettnek tekintve)

Az elsajátítandó ismeretanyag rövid (néhány soros) leírása:

Az elemi, egydimenziós paraméterbecslés és hipotézisvizsgálat gyakorlati, számítógépes eszközeinek áttekintése. A leíró statisztikai módszerek. A várható érték és a szórás becslése. Hipotézisvizsgálat. Eloszlások. Eloszlásfüggvények előállítása, véletlen számok generálása, sűrűségfüggvények illesztése, becslése. Függés vizsgálata. Szórásanalízis. Regresszió. A statisztika különböző kategóriájú számítógépes eszközeinek megismerése: irodai programok, oktatási eszközök, zárt célprogramok, rugalmasan programozható szakértői környezetek.
Az óra számítógépes gyakorlat (EXCEL, Statistica, SPSS, SAS, R-project, MATLAB).

Kötelező irodalom:

http://www.cs.elte.hu/u/prohlet/jegyzetek/StPrcsom1

Ajánlott irodalom:

Mogyoródi J. - Michaletzky Gy. (szerk.): Matematikai statisztika. Egyetemi jegyzet. Nemzeti Tankönyvkiadó, Budapest, 1995.
Móri T.F., Szeidl L., Zempléni A.: Matematikai statisztika példatár, ELTE Eötvös Kiadó, Bp., 1997.
Móri F. T.- Székely J. G. (szerk.). Többváltozós statisztikai analízis, Műszaki Könyvkiadó, 1986, ISBN 963 10 6806 4
http://office.microsoft.com/en-us/excel/HP100908421033.aspx
http://www.statsoft.com/textbook/stathome.html
http://www.spss.com/stores/1/Training_Guides_C10.cfm
http://support.sas.com/documentation/onlinedoc/91pdf/sasdoc_91/insight_ug_9984.pdf
http://www.r-project.org/doc/bib/R-books.html
http://www.mathworks.com/access/helpdesk/help/pdf_doc/stats/stats.pdf

Tantárgy neve: Statisztikai programcsomagok 2 **(C50)**

Tantárgy heti óraszáma:	0+2
kreditértéke:	0+3
tantárgyfelelős neve:	Zempléni András
tanszéke:	Valószínűségelméleti és Statisztika Tanszék
számonkérés rendje:	gyakorlati jegy
előtanulmányi feltétel:	Többdimenziós statisztikai eljárások

Az elsajátítandó ismeretanyag rövid (néhány soros) leírása:

Többdimenziós statisztikai eljárások és számítógépes eszközeik megismerése és áttekintése. Dimenziócsökkentés. Főkomponens-, faktoranalízis és kanonikus korreláció. Diszkrét adatok feldolgozási módszerei. Bináris adatok feldolgozása, logisztikus regresszió. Skálázás, skálázáson alapuló módszerek. Korrespondencia-analízis. Csoportosítás. Klaszteranalízis és klasszifikáció. Élettartam-adatokat feldolgozó módszerek. Probit, logit és nemlineáris regresszió. Élettartam-táblák, Cox-regresszió.
Az óra számítógépes gyakorlat. Felhasznált eszközök EXCEL, Statistica, SPSS, SAS, R-project, MATLAB.

Kötelező irodalom:

http://www.cs.elte.hu/u/prohlet/jegyzetek/StPrcsom2

Ajánlott irodalom:

Móri F. T.- Székely J. G. (szerk.). Többváltozós statisztikai analízis, Műszaki Könyvkiadó, 1986, ISBN 963 10 6806 4
http://www.statsoft.com/textbook/stathome.html
http://www.spss.com/stores/1/Training_Guides_C10.cfm
http://support.sas.com/documentation/onlinedoc/91pdf/sasdoc_91/stat_ug_7313.pdf
http://www.r-project.org/doc/bib/R-books.html
http://www.mathworks.com/access/helpdesk/help/pdf_doc/stats/stats.pdf

Tantárgy neve: Többdimenziós statisztikai eljárások (B19)

Tantárgy heti óraszáma:	4+0
kreditértéke:	6+0
tantárgyfelelős neve:	Michaletzky György
tanszéke:	Valószínűségelméleti és Statisztika Tanszék
számonkérés rendje:	kollokvium
előtanulmányi feltétel:	Valószínűségszámítás és statisztika (a matematikus és alkalmazott matematikus szakirányról érkezetteknél teljesítettnek tekintve)

Az elsajátítandó ismeretanyag rövid (néhány soros) leírása:

A többdimenziós normális eloszlás paramétereinek becslése. Mátrixértékű eloszlások. A Wishart-eloszlás: sűrűségfüggvénye, determinánsa, inverzének várható értéke. Többdimenziós normális eloszlás paramétereire vonatkozó hipotézis vizsgálat. Függetlenségvizsgálat. Normalitásvizsgálat.
Lineáris regresszió.
A változók közötti kapcsolat mérése: korrelációs együttható, maximálkorreláció, parciális korreláció, kanonikus korreláció.
Főkomponensanalízis, faktoranalízis, szórásanalízis.
Diszkrét, többváltozós modellek, Kontingenciatáblák. Maximum-likelihood becslés loglineáris modellben. Kullback-Leibler-féle divergencia. Lineáris és exponenciális eloszláscsaládok. Az L-vetület numerikus meghatározása (Csiszár-féle módszer, Darroch-Ratcliff-eljárás).

Kötelező irodalom:

Ajánlott irodalom:

J. D. Jobson, Applied Multivariate Data Analysis, Vol. I-II. Springer Verlag, 1991, 1992.
Móri T. – Székely G. (szerk.) Többváltozós statisztikai módszerek, Műszaki Könyvkiadó, 1984.
C. R. Rao, Linear statistical inference and its applications, Wiley and sons, 1968.

Tantárgy neve: Valószínűségszámítás és statisztika (A12)

Tantárgy heti óraszáma:	3+2
kreditértéke:	3+3
tantárgyfelelős neve:	Móri Tamás
tanszéke:	Valószínűségelméleti és Statisztika Tanszék
számonkérés rendje:	kollokvium + gyakorlati jegy
előtanulmányi feltétel:	

Az elsajátítandó ismeretanyag rövid (néhány soros) leírása:

Mérték- és integrálelmélet elemei: Mérhető tér, mérhető leképezések. Mérték és integrál. Mértékek kiterjesztése.Lebesgue- és Lebesgue–Stieltjes-mérték. Mértéktartó leképezések. Előjeles mértékek és variációik. Abszolút folytonos és szinguláris mértékek. Mértékek differenciálása. Abszolút folytonos és szinguláris függvények. Mértékterek szorzata.
Valószínűségi mező, valószínűségi változó, eloszlásfüggvény, sűrűségfüggvény, várható érték, szórás, kovariancia, függetlenség.
Konvergenciafajták és kapcsolatuk: 1 valószínűségű, sztochasztikus, L_p-beli, gyenge. Egyenletes integrálhatóság.
Karakterisztikus függvény, centrális határeloszlás-tétel
Feltételes várható érték, feltételes valószínűség, reguláris feltételes eloszlás, feltételes sűrűségfüggvény.
Martingál, szubmartingál, konvergenciatétel, reguláris martingálok.
A nagy számok erős törvénye, független tagú sorok, 3-sor-tétel.
Statisztikai mező, elégségesség, teljesség.
Fisher-információ.
Cramér-Rao egyenlőtlenség, Blackwell-Rao tétel, becslési módszerek: tapasztalati becslések, momentum-módszer, maximum-likelihood becslés, Bayes-becslés.
Hipotézisvizsgálat, likelihood-hányados próba, aszimptotikus tulajdonságok.
Többdimenziós normális eloszlás, a paraméterek becslése
Lineáris modell, legkisebb négyzetes becslés. Lineáris hipotézis normális lineáris modellben.

Kötelező irodalom:

Ajánlott irodalom:

Petruska Gy.: Analízis II. kötet. Egyetemi jegyzet. ELTE Eötvös Kiadó, 1999.
Rényi A.: Valószínűségszámítás. Tankönyvkiadó, 1968.
J. Galambos: Advanced probability theory. Marcel Dekker, New York, 1995.
A. A. Borovkov: Matematikai statisztika . Typotex kiadó, Budapest, 1999.
Mogyoródi J. – Michaletzky Gy. (Szerk.): Matematikai statisztika. Egyetemi jegyzet. Nemzeti Tankönyvkiadó, Budapest, 1995.
Bolla M.–Krámli A.: Statisztikai következtetések elmélete. Typotex Kiadó, Budapest, 2005.