

ALKALMAZOTT MATEMATIKUS MESTERSZAK: ZÁRÓVIZSGAKÉRDÉSEK

Összesen legalább 40 kreditnyi tárgyat kell választani.

Szakmai törzsanyag kérdései

Választandó: 3 témakörből legalább 15 kreditnyi tárgy.

1. Numerikus modellezés és közönséges differenciálegyenletek numerikus megoldási módszerei I. (kredit: 6) *Faragó István*

TÉMAKÖR: Alkalmazott analízis

- (a) Az egy lépéses numerikus módszerek és vizsgálatuk. (Euler típusú módszerek. Konzisztencia, stabilitás, konvergencia. Merev feladatok. A-stabilitás)
- (b) Runge–Kutta típusú módszerek és vizsgálatuk. (Explicit és implicit RK módszerek, konzisztencia rend, A-stabilitás.)

2. Nemlineáris funkcionálanalízis (kredit: 6) *Karátson János*

TÉMAKÖR: Alkalmazott analízis

- (a) Nemlineáris operátorok alapfogalmai. (Gâteaux- és Fréchet-derivált. Potenciáloperátorok, a potenciál fogalma és létezése. Monoton operátorok, konvex funkcionálok. Példa nemlineáris elliptikus operátorra.)
- (b) Nemlineáris operátoregyenletek megoldhatósága. (Variációs elv, funkcionál minimumának létezése. Kvadratikus funkcionál. Megoldhatóság nem potenciálos operátorra. Alkalmazás nemlineáris differenciálegyenletekre.)
- (c) Közelítő módszerek. (Ritz-Galjorkin-féle projekciós módszerek lineáris és nem lineáris operátorokra. Iterációs módszerek: gradiens-módszer Hilbert-térben, Newton-Kantorovics-módszer és változatai Banach-térben.)

3. Fourier-sorok (kredit: 6) *Fridli Sándor*

TÉMAKÖR: Alkalmazott analízis

- (a) Trigonometrikus rendszerek: ortogonalitás, teljesség. Riemann-Lebesgue-lemma. Fourier-sorok konvergenciája. Divergens Fourier-sorok, Fejér-mag, egység approximáció.
- (b) A diszkrét Fourier-transzformáció tulajdonságai. Gyors Fourier-transzformáció és alkalmazásai.
- (c) A Fourier transzformáció analitikus tulajdonságai. Speciális ortogonális rendszerek és alaptulajdonságaik.

4. Algoritmuselemzés I (kredit: 6) *Király Zoltán*

TÉMAKÖR: Algoritmuselemzés

- (a) Rendezés, számolás, dinamikus programozás. (Középső elem, gyorsrendezés, leszámoló és számjegyes rendezés. Mod m számítások, prímtesztelés, gyors Fourier transzformáció, Schönhage-Strassen szorzás. Dinamikus programozás alkalmazásai.)
- (b) Legrövidebb és diszjunkt utak. (Dijkstra algoritmus és alkalmazásai, Bellman-Ford, Johnson, Floyd és Suurballe-Tarjan algoritmusok. Diszjunkt utak keresése.)
- (c) Párosítások, folyamok, hálózati kódok. (Hopcroft-Karp algoritmus, stabil házasság és variációi. Dinitz algoritmus, többtermékes folyamok. Lineáris hálózati kódok.)
- (d) Közelítő és FPT algoritmusok. (Approximációs sémák. Közelítő algoritmus lefogó csúcshalmazra, metrikus utazó ügynökre, Steiner fára, hátizsák feladatra, halmazfedésre. Fix paraméterrel megoldható feladatok, kernelek, példák.)

5. **Bonyolultságelmélet** (kredit: 6) *Grolmusz Vince*

TÉMAKÖR: Algoritmuselmélet

- (a) Randomizált, illetve párhuzamos számítások (választható)
- (b) Algebrai és egyszerű döntési fák, zárkózottság
- (c) Kolmogorov bonyolultság
- (d) Boole hálózatok, alsó becslések kismélységű hálózatokra
- (e) Interaktív bizonyítások
- (f) Tárkorlátos számítások, polinomiális hierarchia, hierarchia-tételek

6. **Diszkrét és folytonos paraméterű Markov-láncok** (kredit: 3) *Prokaj Vilmos (Csiszár Villó)*

TÉMAKÖR: Sztochasztikus folyamatok

- (a) Alapfogalmak. Ergodikus Markov láncokra vonatkozó tételek. Stacionárius eloszlás és reguláris mérték, megfordított láncok.
- (b) Véges állapotterű Markov láncok, Perron–Frobenius-tételek. A konvergencia-sebesség becslése. MCMC-módszerek.
- (c) Folytonos paraméterű Markov láncok infinitezimális generátora. Születési-halálozási folyamatok. A Kolmogorov-féle differenciálegyenletek megoldhatósága.

7. **Sztochasztikus folyamatok** (kredit: 7) *Prokaj Vilmos*

TÉMAKÖR: Sztochasztikus folyamatok

- (a) Wiener folyamat: konstrukció, Donsker tétel, tükrözési elv, erős Markov tulajdonság. Maximum és a szintelérési idő eloszlása.
- (b) Sztochasztikus integrál, kvadratikus variáció, Ito formula, Lévy karakterizáció, Girsanov tétel.
- (c) Sztochasztikus differenciálegyenletek, erős és gyenge megoldás, eloszlásbeli és trajektóriánkénti unicitás. Tételek a megoldás létezéséről és unicitásáról.

8. **Stacionárius folyamatok** (kredit: 6) *Prokaj Vilmos*

TÉMAKÖR: Sztochasztikus folyamatok

- (a) Stacionárius folyamatok. Kovariancia függvény. Bochner-Hincsin-tétel. (Herglotz-tétel) Spektrálelőállítás.
- (b) Karhunen-Loeve-sorfejtés, Kotelnjikov-Shannon-tétel - a mintavételezés sűrűsége.
- (c) Wold-felbontás. Teljesen reguláris és szinguláris folyamatok.
- (d) Stacionárius folyamatok várható-értékének és kovariancia-függvényének becslése.

9. **Speciális sztochasztikus folyamatok** (kredit: 3) *Michaletzky György*

TÉMAKÖR: Sztochasztikus folyamatok

- (a) Felújítási folyamatok. A felújítási függvény, felújítási egyenlet. A megoldás egyértelműsége. A felújítási folyamat aszimptotikus viselkedése (1 valószínűségű konvergencia.). A felújítási függvény aszimptotikus viselkedése. A felújítási tétel. Speciális indítás esetén a pontos megoldás, illetve a hátralévő élettartam.
- (b) Elágazó folyamatok. Diszkrét paraméterű eset. A kihalás valószínűsége. A várható értékkel normalizált folyamat aszimptotikus viselkedése, a határérték várható értéke. Folytonos paraméterű eset. A populáció nagyságának időbeli alakulására vonatkozó differenciálegyenletek. A kihalás valószínűsége.

10. **Diszkrét matematika I.** (kredit: 6) *Lovász László (Sziklai Péter)*

TÉMAKÖR: Diszkrét matematika

- (a) Gráfelmélet: Párosításelmélet. Többszörös összefüggőség. Erősen reguláris gráfok. Regularitási lemma. Síkbarajzolhatóság, gráfminorok.
- (b) Leszámláló kombinatorika: Generátorfüggvények, inverziós formulák részben rendezett halmazokon, rekurziók. Mechanikus összegzés. Klasszikus gráfelméleti leszámolások, fák, feszítő fák száma.
- (c) Algebrai és véletlen módszerek: A lineáris algebrai módszer, extrémális halmazrendszerek. Véges testek, kombinatorikus Nullstellensatz. Várható érték és második momentum módszer. Véletlen gráfok, küszöbfüggvény.

11. **Diszkrét optimalizálás** (kredit: 7) *Frank András*

TÉMAKÖR: Operációkutatás

- (a) Gráfok a diszkrét optimalizálásban. (Legrövidebb utak: Konzervatív súlyozás, megengedett potenciál. Folyamok és áramok: Max-folyam/Min-vágás, Hoffman tétele. Párosítások: Kőnig és Egerváry tételei, a Berge-Tutte-formula, Edmonds-Gallai. Menger és Dilworth tételei. Algoritmusok: Magyar módszer, Edmonds párosítási algoritmus. Legolcsóbb fenők.)
- (b) Matroidok a diszkrét optimalizálásban. (Ekvivalens axiómarendszerek, rangfüggvény, szétbonthatóság. Matroidosztályok, a duális matroid. Mohó algoritmus. Metsettétel és Összeztétel.)

- (c) Lineáris programozás a diszkrét optimalizálásban. (Farkas-lemma és dualitástétel teljesen unimoduláris feltételi mátrixok esetén, alkalmazásokkal: irányított kínai postás, egyenletes színezés. Egész poliéderek Edmonds és Giles féle jellemzése.)

12. **Folytonos optimalizálás** (kredit: 7) *Bérczi Kristóf*

TÉMAKÖR: Operációkutatás

- (a) Konvex függvények, Első- és másodrendű optimalitási feltételek, Szeparáló hipersíkok, Poláris halmazok, Duális norma, Konjugált függvény
- (b) Konvex optimalizálás dualitáselmélete, Konvex program, Duális feladat, Lagrange-függvény, Gyenge és erős dualitás, Optimalitási feltételek, Karush-Kuhn-Tucker feltétel
- (c) Gradiens módszer, Bregman divergencia, Multiplikatív frissítés és mirror descent módszer

Differenciált szakmai anyag kérdései: alkalmazott analízis szakirány

Választandó: legalább 20 kreditnyi tárgy.

1. **Modellalkotás és természettudományos alkalmazások** (kredit: 6) *Izsák Ferenc*
 - (a) A diffúzió modellezése. Feltevés a diffúzióban szereplő fluxusról. Harmadfajú peremfeltétel levezetése. A modell matematikai tulajdonságai. Példák jelenségekre, amelyeket ezzel modellezünk.
 - (b) Áramlási feladatok modellezése egyszerű advekciónal. A megmaradási törvények általános alakja. A Navier–Stokes-egyenletek és az Euler-egyenletek levezetésének elve.
 - (c) Kémiai reakciók tömeghatás típusú modellje. Feltevések a modellben. A megfelelő kinetikai differenciálegyenlet-rendszer felírása, matematikai tulajdonságai.
2. **Elliptikus parciális differenciálegyenletek numerikus módszerei és alkalmazásai I.** (kredit: 6) *Karátson János*
 - (a) A véges differenciák módszere. (A módszer konstrukciója téglalapon, a lineáris rendszer tulajdonságai. Stabilitás és konvergencia. Általánosabb feladatok.)
 - (b) A végeselem-módszer. (A módszer elméleti alapjai, konstrukció 1 és magasabb dimenzióban. Nevezetes bázisfüggvények. A konvergencia és becslései, rendje.)
 - (c) A többrácsos (multigrid-)módszer. (A módszer alapelve. Simító iterációk, V- és W-ciklusok. A módszer konvergenciája.)
3. **Elliptikus parciális differenciálegyenletek numerikus módszerei és alkalmazásai II.** (kredit: 3) *Karátson János*
 - (a) Nem szimmetrikus elliptikus feladatok végeselemes megoldása, konvekció-diffúziós egyenletek, áramvonal-menti végeselem-módszer.
 - (b) Nyeregpont-feladatok, az áramlástan Stokes-feladat és végeselemes megoldása, Uzawa-iteráció.
 - (c) Nemlineáris elliptikus feladatok végeselemes megoldása: konstrukció, konvergencia, Newton-iteráció.
4. **Időfüggő parciális differenciálegyenletek numerikus módszerei és alkalmazásai I.** (kredit: 5) *Izsák Ferenc*
 - (a) Teljes diszkretizáció és szemidiszkretizáció. Az ezekkel kapott egylépéses sémák norma-konzisztenciájának és (feltételes) stabilitásának fogalma. A Lax-féle ekvivalenciatétel.
 - (b) Stabilitásvizsgálati módszerek: elégséges feltétel stabilitásra, vizsgálat Fourier-transzformációval és Gersgorin-tétellel. Nevezetes eredmények az diffúziós egyenletre vonatkozó explicit sémákra, explicit upwind és downwind sémák stabilitása állandó együtthatós áramlási feladatokra. A Crank-Nicolson-séma és tulajdonságai.

- (c) ADI típusú sémák és stabilitásuk. A Lax-Wendroff-séma. Probléma a peremfeltételekkel az advekción feladat esetében. A periodikus peremfeltételhez tartozó lépésmátrixok szerkezete.
5. **Időfüggő parciális differenciálegyenletek numerikus módszerei és alkalmazásai II.** (kredit: 5) *Izsák Ferenc*
- (a) Rendszerek és többlépéses sémák kapcsolata. Alkalmazás a hullámegyenlet numerikus megoldására, inicializáció, módosított Lax-tétel.
- (b) Megmaradási egyenletek megoldása. Fluxus, konzervatív séma fogalma. A Lax-Wendroff-tétel. Godunov-séma levezetése. Monoton, TVD sémák fogalma és kapcsolata.
6. **Dinamikai rendszerek és differenciálegyenletek I.** (kredit: 6) *Simon Péter*
- (a) Dinamikai rendszerek ekvivalenciái. Lineáris rendszerek topologikus osztályozása. Normálforma elmélet, a rezonancia fogalma.
- (b) Lokális vizsgálat egyensúlyi pontban. Hartman-Grobman tétel. Stabil és instabil sokaság tétel. Centrális sokaság és redukciós tétel.
- (c) Diszkrét dinamikai rendszer periodikus megoldásai. Periódus kettőződés. A kaotikus pálya fogalma. Szimbolikus dinamika alkalmazása kaotikus pálya létezésének bizonyítására. A logisztikus és a sátor leképezés.
7. **Dinamikai rendszerek és differenciálegyenletek II.** (kredit: 3) *Simon Péter*
- (a) Lokális bifurkáció fogalma és szükséges feltételei. Nyereg-csomó bifurkáció fogalma és elégséges feltétele.
- (b) Andronov-Hopf bifurkáció fogalma és elégséges feltétele.
- (c) Strukturális stabilitás, bifurkáció kodimenziója.
8. **Lineáris parciális differenciálegyenletek** (kredit: 6) *Simon László*
- (a) Szoboljev-terek: Fourier-transzformáció, kiterjesztési operátor, nyom operátor.
- (b) Lineáris elliptikus peremérték-feladatok gyenge megoldása, sajátérték-feladat. A peremérték-feladatok és sajátérték-feladatok variációs értelmezése.
- (c) Kezdeti-peremérték-feladatok lineáris hiperbolikus és parabolikus egyenletekre: a gyenge megoldás egyértelmősége, létezése: Fourier-módszer, Galjorkin-módszer.
9. **Numerikus modellezés és közöséges differenciálegyenletek numerikus megoldási módszerei II.** (kredit: 5) *Faragó István*
- (a) Lineáris többlépéses módszerek és vizsgálatuk. (Adams típusú módszerek, rend, stabilitás. BDF típusú módszerek és rendjük, abszolút stabilitási tartomány és A-stabilitás.)
- (b) Peremérték-feladatok numerikus megoldása. (a folytonos feladat megoldhatósága, belövéses módszer, véges differenciás módszer)

10. **Operátorfélcsoportok** (kredit: 6) *Bátkai András*

- (a) Motiváló példák (korlátos generátor, eltolás- és szorzás félcsoport, hővezetési egyenlet, stb.), alapfogalmak (generátor, rezolvens, Cauchy feladat, megoldásfogalmak), alaptulajdonságok és jóldefiniáltság, Laplace transzformáció.
- (b) Generálási tételek (Hille-Yosida, Lumer-Phillips), perturbációs tételek.
- (c) Spektrum és aszimptotika (spektráleképezés-tételek, stabilitásfogalmak, Datko-Pazy, Gearhart, Arendt-Batty-Ljubics-Vu, Lutz tételei).

Differenciált szakmai anyag kérdései: sztochasztika szakirány

Választandó: legalább 20 kreditnyi tárgy.

1. Idősorok elemzése 1 (kredit: 6) Márkus László

- (a) Stacionárius folyamatok alapfogalmi. Autokorreláció. Spektrálelőállítás, spektrálsűrűségfüggvény. Stacionárius folyamatok modelljei: autoregressziós (AR(p)), mozgóátlag (MA(q)), ARIMA(p,d,q), ARCH(p), GARCH(p,q), bilineáris, véletlen együtthetős AR, és a SETAR folyamatok, stacionaritása és a stacionárius eloszlás tulajdonságai. Sztochasztikus rekurziós egyenletek stacionárius megoldásának létezési feltétele Ljapunov-exponenssel, Kesten-Vervaat-Goldie tétel reguláris változású eloszlással bíró stacionárius megoldás létezéséről, alkalmazás ARCH(1)-re.
- (b) Idősorok becslélmélete: Az átlag és az autokovariancia függvény becslése, tulajdonságai és határeloszlása (ARCH eset is). Paraméterbecslés AR és MA folyamatra. Rendszelektió Akaike és Bayes információs kritériumok. A periodogram a diszkrét spektrum becslésére, Fisher-teszt. Spektrálsűrűségfüggvény becslése ablakolással, tulajdonságok. Előfehérítés módszere, CAT kritérium.

2. Pénzügyi folyamatok 1 (kredit: 3) Arató Miklós

- (a) Európai opció ára, piacok arbitrázsmentessége, teljessége, eszközárzás első és második alaptétele diszkrét idejű részvény-kötvény piacon. Teljesség, ármérce pár, "market price of risk" folyamat és a martingál mérték kapcsolatai. A Black-Scholes piac teljessége.
- (b) Amerikai opció ára diszkrét idejű kereskedésben. Példa nem teljes piacra, és eszközárak nem teljes diszkrét idejű piacon. A Black-Scholes formula mint a Cox-Ross-Rubinstein árazás határértéke. Több részvényes Black-Scholes modell teljessége.

3. Pénzügyi folyamatok 2 (kredit: 3) Arató Miklós

- (a) A Black-Scholes differenciálegyenlet, kapcsolat a Feynman-Kac formulával. PIDE az ugró folyamatok esetén, pszeudodifferenciál operátorral. Amerikai opció ára szintátlépéses megállítások mellett folytonos idejű kereskedésben. Összetett Poisson-folyamat. A Lévy-Itó felbontás. Exponenciális ugró diffúziós modellek: Merton, Kou, Bates.
- (b) Implikált és realizált volatilitás. Profit and Loss egyenlet. Az implikált volatilitás mosoly. Az implikált eloszlás és a Breeden-Litzenberger formula. Lokális volatilitás modellek (pl. CEV), Dupire egyenlete. Sztochasztikus volatilitás: Hull-White, Ornstein-Uhlenbeck, CIR, Heston. Ugró eszközármodellek. Szubordinátor, business time. Átskálázott Brown mozgás: Variance Gamma, és NIG modellek, tulajdonságaik.

4. Statisztikai becslélmélet (kredit: 4) Móri Tamás

- (a) A sűrűségfüggvény becslése. Cramér-Rao típusú egyenlőtlenségek: Chapman-Robbins, Bhattacharyya-határ. Valódi és általánosított Bayes-becslések, a Jeffrey-féle neminformatív a priori mérték.
- (b) Ekvivariáns becslések. A ML- és a Bayes-becslés ekvivarianciája. Folytonos eloszlásfüggvény ekvivariáns becslése. A Pitman-becslés és tulajdonságai. Véges sokaságból való mintavétel. Godambe és Joshi tételei. A Horvitz-Thompson becslés tulajdonságai.
- (c) L-statisztikák és határeloszlásuk. Legkisebb négyzetes becslés korrelált hibájú lineáris modellben. Optimális L-becslés eltolás- és skálaparaméteres családban. Aszimptotikusan optimális L-becslés az eltolásparaméterre. M-becslések, aszimptotikus normalitásuk. Robusztusság. A Huber-becslés minimax tulajdonsága. Az M- és az L-becslések ekvivalenciája.

5. **Statisztikai hipotézisvizsgálat** (kredit: 3) *Csiszár Villő*

- (a) Exponenciális eloszláscsalád. A Neyman-Pearson lemma általánosítása. Egy- és kétoldali ellenhipotézis vizsgálata. Neyman-struktúra, hipotézisvizsgálat zavaró paraméterek jelenlétében.
- (b) Az általánosított likelihood-hányados próba. Az empirikus folyamat konvergenciája a Szkorohod-térben. Karhunen-Loeve sorfejtés. Klasszikus nemparaméteres próbák. Konfidenciahalmazok. Kapcsolat a hipotézisvizsgálattal. Likelihoodra épülő aszimptotikus konfidenciahalmazok.

6. **Sztochasztikus analízis** (kredit: 6) *Prokaj Vilmos*

- (a) Kolmogorov kiterjesztési tétel. Folytonossági lemma, trajektóriák Hölder folytonossága. Gyenge konvergencia, Portmanteau tétel. Feszesség, Prohorov tétel. Donsker tétel.
- (b) Wiener folyamat tulajdonságai: Nagy számok erős törvénye, invariancia tulajdonságok, Wiener-folyamat null-halmaza, "sehol sem monotonitás", Dvoretzky-Erdős-Kakutani tétel, Paley-Wiener-Zygmund tétel, Iterált logaritmus tétel.
- (c) Doob-Meyer felbontás, Ito integrál, kvadratikus varáció, Ito formula.

7. **Többdimenziós statisztikai eljárások** (kredit: 6) *Michaletzky György*

- (a) A többdimenziós normális eloszlás paramétereinek becslése.
- (b) Főkomponensanalízis.
- (c) Faktoranalízis.
- (d) Diszkriminanciaanalízis.

8. **Életbiztosítás** (kredit: 3) *Kováts Antal*

- (a) A hagyományos és a modern életbiztosítási díjkalkulációs logika. Ezek különbségei.
- (b) A hagyományos életbiztosítások díjtartalékszámítása és az azokhoz kapcsolódó aktuáriusi számítások (visszavásárlás, díjmentesítés, nyereségszétosztás).

9. **Általános biztosításmatematika** (kredit: 3) *Arató Miklós*

- (a) Nevezetes kárszám- és káreloszlások.
- (b) Összetett eloszlások. Panjer rekurzió.

10. **Bevezetés az információelméletbe** (kredit: 3) *Csiszár Villő*

- (a) Entrópia, kölcsönös információ, relatív entrópia (divergencia). Veszteségmentes adattömörítés, a kódszóhosszakra (Kraft-egyenlőtlenség) és az átlagos kódszóhosszra vonatkozó korlátok. Kódolási módszerek és hatékonyságuk: Shannon kód, Shannon-Fano-Elias (alfabetikus) kód, aritmetikai kód, Huffman kód.
- (b) Sztochasztikus folyamatok (források) betűnkénti entrópiája. Tipikus sorozatok, információstabilis források (AEP: asymptotic equipartition property). Állandó hosszúságú blokk-kódok előírt hibavalószínűséggel, Fano egyenlőtlenség. Elérhető ráták. A hibaexponens i.i.d. forrás esetén (Rényi entrópia). Korrelált források kódolása: Slepian-Wolf tétel.
- (c) Zajos csatorna, szimmetrikus és gyengén szimmetrikus csatornák. Csatorna-kapacitás és kiszámítása (Arimoto-Blahut algoritmus). Csatornakódolási tétel, visszacsatolásos csatornák. Forrás- és csatornakódolás lineáris kódokkal. A Hamming-féle hibajavító kódok elemei. Differenciális entrópia, összevetés a diszkrét esettel. Gauss-csatorna.

Differenciált szakmai anyag kérdései: számítástudomány szakirány

Választandó: legalább 20 kreditnyi tárgy.

1. Adatbányászat (kredit: 6) *Lukács András*

- (a) Klasszifikáció modelljei I. (döntési fák, Bayes-módszerek, boosting)
- (b) Klasszifikáció modelljei II. (neurális hálózatok, lineáris szeparáción alapuló módszerek, kernel módszerek)
- (c) Gyakori mintázat kereső algoritmusok (Apriori, partíciós és Toivonen-algoritmus, FP-growth)
- (d) Klaszterező algoritmusok (particionáló, sűrűségalapú, hierarchikus módszerek)

2. WWW és hálózatok matematikája (kredit: 3) *ifj. Benczúr András*

- (a) PageRank és bolyongás gráfokon
- (b) Kleinberg linkgyűjtemény - meghatározó tartalom (hub-authority) algoritmus (HITS) és mátrixok szinguláris felbontása
- (c) Véletlengráf modellek: Barabási-Albert; Kleinberg kis világ modellje

3. Kriptológia (kredit: 6) *Sziklai Péter*

- (a) Titkosítás és pszeudovéletlenség (tökéletes biztonság ekvivalens definíciói, one-time pad, tökéletes biztonság korlátai, számítási biztonság definíciói, pszeudovéletlenség, konstrukciók lehallgatás és nyílt szövegű támadás ellen)
- (b) Üzenet autentikálás és hash-függvények (üzenetek integritása, üzenet autentikáló kódok (MAC) definíciója, konstrukciók, hash-függvények biztonsági kritériumai, születésnap támadás, Merkle-Damgard konstrukció)
- (c) Nyilvános kulcsú titkosítások (biztonság definíciók, RSA módszer, ElGamal titkosítás, kvadratikus maradékok és a Goldwasser-Micali titkosítás, Rabin titkosítás)

4. Algoritmusok és adatstruktúrák tervezése, elemzése és implementálása I (kredit: 6) *Király Zoltán*

- (a) Síkgráfokkal síkbarajzolása; favastagság $\leq k$ eldöntése
- (b) On-line és randomizált algoritmusok, min. vágások
- (c) Virtuális magánhálózatok; determináns-számítás gyűrűkben; Megiddo algoritmusai

5. Algoritmusok és adatstruktúrák tervezése, elemzése és implementálása II (kredit: 3) *Király Zoltán*

- (a) Unió-holvan adatstruktúrák; kupacok; vEB-struktúra
- (b) Szótárak, hash-elés
- (c) Geometriai adatstruktúrák; dinamikus fák

6. **Kódok és szimmetrikus struktúrák** (kredit: 3) *Szőnyi Tamás*

- (a) Perfekt kódok
- (b) MDS kódok
- (c) Négyzetes blokkrendszerek

7. **Adattömörítés** (kredit: 3) *Szabó István*

- (a) Fogalmak és korlátok stacionárius, egyértelműen felbontható (vesztésmentes) betűnkénti kódolásokra (prefix kód, Kraft-Fano egyenlőtlenség, átlagos kódhossz és kapcsolata az entrópiával, optimális kód, bináris Huffman kód, mennyire közelíti meg a bináris Huffman kód átlagos kódhossza az alsó korlátot, dinamikus kódolások)
- (b) Algoritmusok és aszimptotikus eredmények blokk kódolásokra és változó hosszúságú forráskódolásokra (blokk kódolás, aritmetikai kódolás, Lempel-Ziv kódolások fajtái (LZ77, LZ78, és javításai)), az értelmes írott szöveg entrópiája, meghatározásának módszerei
- (c) A veszteséges kódolások típusai, a kép és videó tömörítés elvi vázlata (a veszteséges tömörítés elvárásai, alapelvei, a JPEG és videó tömörítés főbb lépései)

Differenciált szakmai anyag kérdései: operációkutatás szakirány

Választandó: legalább 20 kreditnyi tárgy.

1. Egészértékű Programozás I. (kredit: 3) *Király Tamás*

- (a) Meyer tétele, Hilbert bázisok, teljes duális egészértékűség.
- (b) Heurisztikus algoritmusok az utazó ügynök feladatra, approximációs eredmények, Held–Karp-korlát, módszerek a kiszámolására.
- (c) Lagrange relaxáció, oszlopgenerálás.

2. Gráfelmélet (kredit: 3) *Frank András*

- (a) Leemelési tételek és alkalmazásaik.
- (b) A gráfelmélet min-max tételei.

3. Kombinatorikus algoritmusok I. (kredit: 6) *Jordán Tibor*

- (a) Gráfok bejárása, algoritmusok az összefüggőség tesztelésére, ritka tanúk, vágásekivalens fák.
- (b) Dinamikus programozás, gráfok favastagsága.
- (c) Merev gráfok és szerkezetek.

4. Lineáris optimalizálás (kredit: 3) *Bérczi Kristóf*

- (a) Érzékenységvizsgálat (lokális érzékenység, globális függés a korlátozó vektortól, duális megoldások halmaza, globális függés a költségfüggvénytől).
- (b) Nagyméretű lineáris programozási feladatok megoldása (oszlopgenerálás, vágósíkos eljárások, Dantzig-Wolfe dekompozíció, sztochasztikus programozás, Benders dekompozíció).
- (c) Affin skálázási algoritmus (belsőpontos módszerek alapötlete, affin skálázási algoritmus, konvergenca, inicializálás, hatékonyság).

5. Matroidelmélet (kredit: 3) *Frank András*

- (a) Matroidelméleti algoritmusok.
- (b) Matroidok gráfelméleti alkalmazásai (fedés és pakolás fákkal, fokszamkorlátos fák, forrás telepítés, merev gráfok, stb.).

6. Nemlineáris optimalizálás (kredit: 4) *Bérczi Kristóf*

- (a) Diszkrét konvex függvények, tulajdonságok (lokális-globális optimum, konvex kiterjesztés, konjugált), példák
- (b) M- és L-konvex halmazok, Szeparációs tételek, Fenchel dualitás
- (c) Algoritmusok diszkrét konvex függvényekre, M-konvex minimalizálás, L-konvex minimalizálás, M-konvex metszet

7. **Sztochasztikus optimalizálás** (kredit: 6) *Mádi-Nagy Gergely*

- (a) Sztochasztikus modellek áttekintése. A korlátok és célok különböző megfogalmazásai. Az adódó sztochasztikus programozási feladatok matematikai jellemzése. Logkonkáv mértékek alaptétele.
- (b) Sztochasztikus programozási feladatok megoldó módszerei. Speciális konvex programozási eljárások. Diszkrét momentum problémák. Valószínűségi korlátok kiértékelése.

8. **Ütemezéselmélet** (kredit: 3) *Jordán Tibor*

- (a) Egygépes feladatok.
- (b) Többgépes feladatok.
- (c) A shop modellek.

9. **Poliéderes kombinatorika** (kredit: 3) *Frank András*

- (a) Teljesen unimoduláris mátrixok jellemzése és gráfoptimalizálási alkalmazásai.
- (b) Teljesen duális egészértékűség (TDI-ség). A párosítás politóp poliéderes megadása és a leírás TDI-sége. A teljes párosítás politóp poliéderes leírása.
- (c) Polimatroidok és általánosításai. Szubmoduláris áramok. Alkalmazások gráfrányítási problémákra.

10. **Játékelmélet** (kredit: 3) *Király Tamás*

- (a) Kombinatorikus játékok: k-nim, Grundy-számozás, sövényvágó játék, Hex.
- (b) Stratégiai játékok: dominálás, Nash-egyensúly, Nash tétele. Kétszemélyes 0-összegű játékok, Neumann-tétel.
- (c) Kooperatív játékok: mag, Shapley-érték, konvex játékok. Stabil párosítások, felső körcsere algoritmus, taktikázás-biztosság.

11. **Egészértékű programozás II.** (kredit: 3) *Király Tamás*

- (a) Gomory-Chvátal-vágások. Vágások az utazó ügynök feladatra és a hátizsák-feladatra. Vágások felemelése.
- (b) Rácsok, redukált bázisok, LLL algoritmus.