Tézy predmetov rigorózneho konania – Aplikovaná informatika

Študijný odbor: *9.2.9 Aplikovaná informatika*
Skúška: *rigorózna (RNDr.)*
Zostavil: doc. Ing. Jarmila Škrinárová, PhD.
Schválil: prof. RNDr. Roman Nedela, DrSc.
Dátum: 28. 9. 2017

Predmety širšieho základu

Optimalizácia

- Optimalizácia – definícia úlohy, metódy riešenia.
- Úloha obchodného cestujúceho.
- Dopravná úloha.
- Sieťové úlohy – hľadanie najkratšej cesty.
- Hľadanie najdlhšej (kritickej) cesty – CPM.
- Systémy hromadnej obsluhy – základné pojmy, postup riešenia.
- Metóda lineárneho programovania: grafické riešenie, metóda Simplex.
- Problém optimalizácie batohu – zadanie, počet riešení, heuristické metódy.
- Školský rozvrh – zadanie, postup riešenia, priorita predmetov.

Odporúčaná literatúra

[1] RALSTON A.: Základy numerickej matematiky. Praha, Academia 1978.
[2] RIEČANOVÁ Z. a kol.: Numerické metódy a matematická štatistika. Bratislava, Alfa 1981.
[3] LAŠČIAK A. a kol: Optimálne programovanie. Bratislava, ALFA 1983.
[4] VITÁSEK E.: Numerické metody. SNTL Praha, 1987.
[5] BUCHANAN J., TURNER P.: Numerical Methods and Analysis. New York, McGrawHill, Inc. 1992.
[6] GRIVA I., NASH S.G.,SOFER: Linear and Nonlinear Optimization, 2nd ed., SIAM, Philadelphia, 2009.

Umelá inteligencia

- Hľadanie v grafoch, prediktátová logika 1. rádu vrátane rezolvenčného princípu.
- Reprezentácia poznatkov, riešenie úloh a plánovanie činnosti pomocou predikátovej logiky 1. rádu.
- Návrh expertných systémov s neurčitosťou, plausibilná inferencia, intenzionálny prístup, extenzionálny prístup, Bayesovská metóda, Dempster-Shaferova metóda, viachodnotová logika.
- Reprezentácia poznatkov, riešenie úloh a plánovanie činnosti pomocou fuzzy logiky, základné pojmy, vlastnosti základných operácií, t-normy, t-conormy.
- Mukaidonov fuzzy rezolučný princíp - dôkaz že formula je odvoditeľná z axióm vo fuzzy logike.
- Návrh fuzzy inferenčných systémov.

Odporúčaná literatúra:

[1] KUNCHEVA L. I. Fuzzy Classifier Design. A Springer Verlag Company, Germany, 2000.
[2] RUSSEL S., NORVIG P. Artificial Intelligence. A Modern Approach.. Prentice Hall, Second Edition, New Jersey, 2003.
[3] NEGNEVITSKY M. Artificial Intelligence : A Guide to Intelligent Systems. (2nd Edition). Addison Wesley, 2004.
[4] NILSSON, N. J. Artificial Intelligence: A New Synthesis. Morgan Kaufmann, 1998.
[5] MAŘÍK V. a kol. Umělá inteligence 1,2,3,4. Academia, Praha, 1993, 1995, 2001, 2003.

[6] Luger, G. F., Stubblefield, W.A.: Artificial Intelligence. Structures and Strategies for Complex Problem Solving. Addison-Wesley, 1999, 2004 alebo 2008.
[7] Návrat, P. A kol. Umelá inteligencia. Vydavateľstvo STU, 2015.
[8] Kolemen, J., Ftáčnik, M., Kalaš, I., Mikulecký, P.: Základy umelej inteligencie. ALFA, Bratislava, 1992.

Modelovanie a simulácia

- Spojité dynamické systémy - reprezentace lineárních, časově invariantních (LTI) spojitých systémů pomocí diferenciálních rovnic, Laplaceova transformace, přenosová funkce a kritérium stability LTI spojitých systémů.
- Modelování spojitých systémů a procesů - modelování obecně nelineárních diferenciálních rovnic pomocí integrátorů v prostředí Matlab Simulink, frekvenční charakteristiky spojitých LTI systémů.
- Diskrétní dynamické systémy - reprezentace lineárních, časově invariantních (LTI) diskrétních systémů pomocí diferenčních rovnic, z-transformace, přenosová funkce a kritérium stability LTI diskrétních systémů.
- Modelování diskrétních systémů a procesů - modelování obecně nelineárních diferenčních rovnic pomocí jednotkových zpoždění v prostředí Matlab Simulink, frekvenční charakteristiky diskrétních LTI systémů.
- Řazení dílčích subsystémů - sériové, paralelní řazení, záporná a kladná zpětná vazba, stabilizace systémů pomocí zpětných vazeb, řídicí technika.

Odporúčaná literatúra:
[1] Svítek M., Borka J., Vlček M.: Modelování systemů a procesů, skriptum ČVUT, 2001.
[2] Doňar B., Zaplatílek K.: Matlab pro začátečníky, BEN, 2003.
[3] Doňar B., Zaplatílek K.: Matlab - tvorba uživatelských aplikací, BEN, 2004.
[4] Doňar B., Zaplatílek K.: Matlab - začínáme se signály, BEN, 2006.

Softvérové systémy

- Softvér a vlastnosti softvérových produktov. Softvérové inžinierstvo. História softvérového inžinierstva. Zaradenie do kontextu informačných technológií vo svete a na Slovensku. Systematický prístup k vývoju softvéru. Ťažkosti s tvorbou softvéru a dôvody, ktoré k ťažkostiam pri tvorbe softvéru vedú.
- Životný cyklus softvérového systému (grafické vyjadrenie jednotlivých životných fáz cyklu). Metodiky a metódy tvorby softvéru a modely vývoja softvéru, prístupy k tvorbe softvéru. Tvorivý tím a jeho zloženie. Úlohy špecialistov v životnom cykle softvérového systému. Aspekty tvorby softvéru: technický aspekt, psychologický aspekt a aspekt riadenia (manažmentu) projektu. Softvérové procesy.
- Úvod do problematiky analýzy a návrhu softvérových systémov. Modelovanie softvérových systémov, dimenzie modelovania a klasifikácia modelov. Formalizmy pre reprezentáciu modelov (Unified Modeling Language, UML).
- Prístupy k analýze a návrhu: štruktúrovaný prístup, datovo-orientovaný prístup, objektovo-orientovaný prístup. Príklady použitia techník analýzy a návrhu (štruktúrovaný prístup). Príklad použitia techník analýzy a návrhu (objektovo-orientovaný prístup; Rational Unified Process). Porovnanie jednotlivých prístupov k analýze a návrhu.
- Implementácia softvérových systémov vo vybranom vytváracom prostredí. - základné charakteristiky, porovnanie rôznych prístupov. Testovanie softvérových systémov: statické a dynamické testovanie; techniky testovania, stratégie testovania. Prevádzka a údržba softvérových systémov.

Odporúčaná literatúra:
[1] Sommerville, I.: Software Engineering, Addison-Wesley Publ. Company, 7th Edition, 2005.

[2] Pressman, R.S. : Software Engineering: A Practicioner's approach. 6th Edition. McGraw Hill. 2005.
[3] Jalote, P.: An Integrated approach to Software engineering. 3rd Edition. Springer Verlag. 2005.
[4] Brooks, F.P.: The Mythical Man-Month. Anniversary Edition.Addison-Wesley. 1995.
[5] Booch, G., Jacobson, I., Rumbaugh, J.: The Unified Modeling Language User Guide. Addison Wesley, 1999.
[6] Booch, G., Jacobson, I., Rumbaugh, J.: The Unified Software Development Process. Addison Wesley, 1999.
[7] Richta, K., Sochor, J.: Softwarové inženýrství I. ČVUT Praha, Fakulta elektrotechnická. 1998.
[8] Paleta, P.: Co programátory ve škole neučí aneb Softwarové inženýrství v reálné praxi. Computer Press (in czech). 2003.
[9] Meilir Page-Jones: Základy objektově orientovaného návrhu v UML. Grada (in czech). 2001.

Zložitosť algoritmov a prekladače

- Výpočty podľa Minského.
- Výpočty podľa Markova.
- Nedeterministické Markovove algoritmy.
- Regulárne jazyky a konečné automaty.
- Časová zložitosť algoritmov (lineárne, kvadratické, atď.).
- Primitívna rekurzívnosť funkcií.
- Rekurzívnosť predikátov, špeciálne funkcie.
- Algoritmická riešiteľnosť, problém (samo)prípustnosti.
- Zložitosť P a NP, problémy SAT a 3-SAT.
- Programovací jazyk. Prekladač. Dôvody vzniku prekladačov. Proces prekladu.
- Lexikálna analýza, prehľadávanie. Tokeny, lexémy.
- Regulárne výrazy. Základné a rozšírené operácie. Deterministický a nedeterministický konečný automat. Transformácia regulárnych výrazov na deterministický konečný automat.
- Syntaktická analýza, parsovanie. Vzťah syntaktickej a lexikálnej analýzy. Terminály a neterminály. BNF a EBNF. Derivácia. Parsovací strom. Abstraktný syntaktický strom. Nejednoznačnosť gramatiky. Prednosť a asociatívnosť operátorov. Spracovanie chýb.
- Syntaktická analýza zhora nadol, zdola nahor. Recursive-descent parser. LL(1) parser. Množiny zač a nasl.
- Generátory prekladačov.

Odporúčaná literatúra:

[1] AHO A. V., SETHI R., ULLMAN J. D.: Compilers - Principles, Techniques, and Tools. Addison Wesley, 1986, ISBN: 978-0201100884.
[2] LOUDEN K. C.: Compiler Construction: Principles and Practice, Course Technology, 1997, ISBN: 978-0534939724.
[3] MAK R.: Writing Compilers and Interpreters: A Software Engineering Approach, Wiley, 2009, ISBN: 978-0470177075.
[4] KOLLÁR J.: Prekladače, Elfa, 2009, ISBN: 9788080861216.
[5] MARTIN J.C.: Introduction to Languages and the Theory of Computation 4th ed.. McGraw-Hill, New York, 2011.

Paralelné a distribuovane výpočty a distribuované operačné systémy

- Paralelné architektúry počítačov. Systémy so spoločnou pamäťou. Systémy s distribuovanou pamäťou. Systémy s virtuálnou spoločnou pamäťou.
- Paralelné programátorské modely. Model procesov a vlákien. Model zasielania správ.
- Komunikácia. Synchronizácia. Základné synchronizačné vzory (signalizácia, rendezvous, vzájomné vylučovanie, multiplex, bariéra) a problémy (producent-konzument, čitatelia-zapisovatelia, obedujúci filozofovia).
- Princíp semaforu.

- Granularita. Pozorovateľné zrýchlenie. Paralelná nadbytočnosť. Škálovateľnosť. Jednoduchý paralelizmus.
- Meranie výkonnosti paralelných programov: Zrýchlenie a efektívnosť. Amdahlovo pravidlo, Gustafsonovo pravidlo.
- Dekompozícia paralelných problémov vo vzťahu k paralelizmom.
- Programový model údajového paralelizmu.
- Metodika tvorby paralelných aplikácií podľa Fostera.
- Model PRAM (Parallel Random Access Machine).
- Sekvenčné a paralelné redukcie a prefixové redukcie.
- Modely riadenia zdrojov v dynamických výpočtových systémoch. Koncepcia elasticity v elastickom klastri.
- Rozvrhovanie a vyrovnávanie záťaže vo vysokovýkonných systémoch.
- Zelené počítanie, virtuálne stroje a ich konsolidácia vo vysokovýkonných systémoch.

Odporúčaná literatúra:

[1] KOLLÁR J.: Metódy a prostriedky pre výkonné paralelné výpočty. Elfa, 2003, ISBN: 9788089066704.
[2] ŠKRINÁROVÁ, J.: Elastický klaster. Banská Bystrica: Univerzita Mateja Bela, 2017, ISBN 978-80-557-0642-9, s. 108. (100%).
[3] BLIZŇÁK, M.: Paralelní procesy a programování. UTB Zlín. 2013.
[4] FOSTER, I.: Designing and Building Parallel Programs. Dostupné na: http://www.mcs.anl.gov/~itf/dbpp/
[5] BARBOSA, V.: An introduction to distributed algorithms. MIT Press, 1996.
[6] TEL, G.: Introduction to distributed algorithms. Cambridge : Cambridge University Press, 1994.
[7] ŠKRINÁROVÁ, J.: Elektronická podpora k paralelné a distribuované výpočty https://lms2.umb.sk/
[8] Beloglazov, A,. Abawajy, J., Buyya, R.: Energy-aware resource allocation heuristics for efficient management of data centers for Cloud computing. In Future Generation Computer Systems. 28, 2012. s. 755–768
[9] Blaise Barney: Introduction to Parallel Computing.

Povinne voliteľné predmety

Neurónové siete a fuzzy množiny

- Gradientové metódy učenia v dopredných neurónových sieťach, mechanizmus spätného šírenia chyby.
- ART neurónové siete, proces učenia.
- Všeobecný klasifikačný problém a rozklad množiny objektov na trénovaciu a testovaciu množinu.
- Evolučné stochastické optimalizačné algoritmy a proces učenia v dopredných neurónových sieťach.
- Charakteristika a návrh neuro-fuzzy-genetických systémov
- Fuzzy množiny a fuzzy logika – definícia základných pojmov a operácií, t-normy a t-konormy, základné rozdiely medzi „klasickou“ logikou a fuzzy logikou a tiež medzi „klasickými“ množinami a fuzzy množinami.
- Fuzzy odvodzovanie – zovšeobecnený modus ponens, fuzzy inferenčný systém (FIS), základné časti FIS a ich stručná charakteristika.
- Mamdaniho a Takagi-Sugenov FIS – základné rozdiely medzi uvedenými FIS, možnosti použitia daných systémov.
- Fuzzy clustering – základný princíp fuzzy zhlukovania, porovnanie rozdielov medzi „klasickým“ zhlukovaním a fuzzy zhlukovaním, možnosti použitia.

Odporúčaná literatúra:

[1] KVASNIČKA V. a kol. Úvod do teórie neurónových sietí. IRIS, Bratislava, 1997.
[2] HAYKIN S. S. Neural Networks: A Comprehensive Foundation. Prentice-Hall, 1999.
[3] MAŘÍK V. a kol. Umělá inteligence 1,2,3,4. Academia, Praha, 1993, 1995, 2001, 2003.
[4] OLEJ V. Modelovanie ekonomických procesov na báze výpočtovej inteligencie.Miloš Vognar - M&V, Hradec Králové, 2003.
[5] KOLESÁROVÁ, A., KOVÁČOVÁ M.: Fuzzy množiny a ich aplikácie, STU Bratislava, 2004, ISBN 80-227-2036.
[6] NAVARA, M., OLŠÁK, P.: Základy fuzzy množin. ČVUT Praha, 2002.
[7] ROSS, Timothy J. Fuzzy logic with engineering applications. John Wiley & Sons, 2009.

Informačná bezpečnosť

- Pojem informačná bezpečnosť. Otázky nevyhnutnosti ochrany údajov a informácií, prejavy škôd, činitele vplývajúce na informačnú bezpečnosť.
- Malware (klasické počítačové vírusy, červíky, trójske kone, dialery, spyware, adware, hoax, ale aj spam, ...) a čo najpodrobnejšie a najkomplexnejšie objasnenie tejto problematiku. Formulovanie odporúčaní a rád o tom, ako sa nestať distribútorom malware.
- Problematika prevádzkovej bezpečnosti. Prevádzkové procedúry, plánovanie kapacít zdrojov systému, zásady ochrany proti malware, procesy zálohovania a archivácie, aktivity správy sietí, bezpečná práca s médiami.
- Informačná bezpečnosť v počítačových sieťach. Autentifikácia komunikačných entít. Autentifikácia dátového zdroja. Autentifikácia spojenia. Riadenie prístupu. Zaistenie dôveryhodnosti. Zaistenie integrity. Hrozby na sieti, motívy útočníkov.
- Matematické základy kryptológie: Monoalfabetické a polyalfabetické šifry. Vernamova schéma, ideálna šifra, Shanonnova definícia bezpečnosti prenosu, Feistelove schémy, šifry GOST, DES, 3DES a Rijndael. Asymetrické šifry, RSA algoritmus, faktorizácia celých čísel, DSA. Šifry založené na eliptických krivkách.

Odporúčaná literatúra:

[1] Bell, D.E., LaPadula, L.J.: Secure computer system : Unified exposition and multics interpretation. Technical Report MTR-2997, Mitre Corp., Bedford Massachusetts, USA, 1976.
[2] Biba, K. J.: Integrity Considerations for Secure Computer Systems. The Mitre Corporation, 1977.
[3] Huraj, L.: Nebojme sa šifrovania, Bratislava : MPC BA, 2002. ISBN 80-8052-160-3
[4] Odehnal P., Zahradníček P.: Praktická sebeobrana proti virům, Grada, 1996
[5] Rychnovský, L.: Počítačová bezpečnost. Zpravodaj ÚVT MU. ISSN 1212-0901, 2005, roč. XVI, č. 1, s. 13-16.
[6] Szor, P.: The Art of Computer — Virus Research and Defense. Symantec, 2005.
[7] Ryabko, B., Fionov, A.: Basics of Contemporary Cryptography for IT Practitioners, World Scientific, Singapore, 2005.
[8] Menezes,A., Oorschot, Vanstone,S.: Handbook of applied cryptography, 5th edition, CRC Press, 2001.
[9] Singh, S.: Kniha kódu a šifer, Argo/Dokorán, Praha, 2007.
[10] Birkhoff, G., MacLane, S.: Prehlad modernej algebry. Alfa, Bratislava, 1979.
[11] Gallian,J.: Contemporary abstract algebra, 6th edition, Books Cole, 2009.

Informačné systémy

- Obecný popis systému - prvky, vazby, rozhraní, regularita rozhraní, identifikace, silné procesy, performační parametry (bezpečnost, spolehlivost, integrita, atd.), Petriho sítě.
- Teorie informace - definice informace/entropie, signály, míra informace ve zprávě, kódování, modulace, odstraňování neurčitosti, znalosti, fuzzy systémy, kvantové počítače, kybernetika.
- Datové modelování - logický datový model, fyzický datový model, normalizace, relační databáze, objektové databáze, datový registr, protokoly, ASN.1, standardy datových rozhraní (CEN, ISO).

- Návrh informačních systémů - metodika UML (Unified Modelling Languague), aktéři, případy užití, diagram tříd, sekvenční diagram, stavový diagram, humánní role v informačním systému.
- Technologie informačních systémů - procesní informační systémy, transakční informační systémy, architektury informačních systémů, claud computing, ubiquitous computing, telematické systémy, příklady realizace informačních systémů: e-Government, dopravní telematika, smart cities, atd.

Odporúčaná literatúra:
[1] Svítek M.: Víc než součet částí - systémový pohled na process lidského poznání, Academia, 2013.
[2] Kanisová H., Muller M.: UML srozumitelně, Computer Press, Brno 2004
[3] Šešera L., Mičovský A., Červeň J.: Data modelování v příkladech, Grada Publishing 2001
[4] Meilir Paga-Jones: Základy objektově orientovaného návrhu v UML, Grada 2001

Databázové systémy

- Koncepcia relačnej databázy. Relácia, primárne a cudzie kľúče, indexy. Normálne formy databáz.
- Relačná algebra. Operácie relačnej algebry: zjednotenie, prienik, rozdiel, projekcia, premenovanie, selekcia, spájanie (join). Tranzitívny uzáver relácie.
- Jazyk SQL ako implementácia relačnej algebry. DDL, DML a dopyty. Trojhodnotová logika. Rozdiely medzi relačnou algebrou a SQL.
- Použitie relačných databáz. OLTP prostredia vs. OLAP prostredia. . Thin client a thick client aplikácie. Transakcie.
- Relačná databáza ako jedna z alternatív organizácie dát. Výhody a nevýhody oproti textovým, binárnym súborom, Excel a Access súbormi, distribuovanými databázami, objektovými databázami, NoSql databázami.

Odporúčaná literatúra:
[1] Karol Matiaško, Monika Vajsová, Michal Zábovský, Matúš Chochlík, Databázové systémy a technológie, 2009, Online: http://www2.fiit.stuba.sk/DBS/lectures/lectures.shtml

Kódovanie

- Základy teórie informácie: Informácia, správa, abeceda, kódovanie, blokové a prefixové kódovanie. Informačný systém, miera informácie, komunikačný systém, prenosový kanál, šírka prenosového kanálu, šum.
- Kódovanie zdroja (kompresné metódy): Kompresia, stratové a bezstratové kompresné metódy. Run-length encoding. Tvorba prefixového kódu, pestované stromy, Huffmanov kód, optimalita Huffmanovho kódu, Huffmanove kódy pre nebinárne abecedy a pestované stromy vyššieho stupňa, algoritmus ZIP. Slovníkové metódy kompresie, Lempel-Ziv-Welch algoritmus, štandardné a skrátené slovníky pre LZW. Diskrétna Fourierova transformácia, diskrétna kosínusová transformácia, kompresie štandardu JFIF, algoritmus JPEG.
- Kódovanie prenosu: Vplyv šumu na prenos, Hammingova vzdialenosť, Hammingova váha slova, t-násobné chyby, chyby detegujúce kódovania, samoopravné kódovania, informačné a kontrolné (paritné) znaky, systematický kód, limity detekcie a možností opravy kódu, singleton bound, informačný pomer kódu, binárne paritné kódy, k-repeticné kódy. Lineárne kódovania, vektorové priestory, generujúca a kontrolná matica lineárneho kódu, triedy slov podľa kódu, syndróm slova, triedy slov podľa kódovania, štandardné dekódovanie s opravou, dekódovania a oprava podľa syndrómu, Hammingove kódy, Hammingove kódy s paritou, tvorba nových kódovaní úpravami generujúcej matice kódovania. Boolove algebry, polynomiálne kódy na Boolovými algebrami, syndróm slova, dekódovania a oprava podľa syndrómu, Reed-Muelerove kódovania. Okruhy polynómov nad konečnými poľami, polynomiálne kódy, syndróm slova, dekódovania a oprava podľa syndrómu, BCH kódovania, Reed-Solomonove kódy, Cyclic Redundancy Check.

Odporúčaná literatúra:

[1] J. Adámek, „Kódování“, SNTL, Praha, 1989.
[2] F. P. Preparata, R. T. Yeh, „Úvod do teórie diskrétnych algebraických štruktúr“, Alfa/SNTL, Bratislava, 1982.
[3] G. Birkhoff, S. MacLane, „Prehlad modernej algebry“, Alfa, Bratislava, 1979.
[4] J. Gallian, „Contemporary abstract algebra“, 6th edition, Books Cole, 2009.
[5] G.A. Jones & J.M. Jones, Information and Coding Theory, Springer Verlag, London, 2000.
[6] T. K. Moon, Error correction coding, Mathematical Methods and Algorithms, J. Wiley \& Sons, 2005.