KATEDRA INFORMATIKY
UNIVERZITA PALACKÉHO V OLOMOUCI
www.inf.upol.cz

Státní závěrečná zkouška, červen 2017

studijní program:	N1801 Informatika
studijní obor:	1801T001 Informatika
typ:	magisterský
forma:	prezenční

Státní závěrečná zkouška sestává z následujících částí:

- ústní zkouška
- obhajoba diplomové práce

Pro ústní zkoušku se stanovují následující okruhy. Z každého okruhu si student vylosuje 1 otázku (celkem 4 otázky).

1 Základní metody informatiky

Formální jazyky a jejich hierarchie. Regulární jazyky (definice, uzávěrové vlastnosti). Konečné automaty deterministické a nedeterministické. Regulární výrazy. Minimalizace konečného deterministického automatu. Pumping lemma. Bezkontextové jazyky a jejich vlastnosti (uzávěrové vlastnosti, jednoznačnost). Zásobníkové automaty a jejich modifikace.

Turingův stroj (TS), nedeterministický TS. Jazyk přijímaný TS, jazyk rozhodovaný TS, Church-Turingova teze. Částečně rekurzivní a rekurzivní jazyky, jazyky a rozhodovací problémy. Vztah rekurzivních a částečně rekurzivních jazyků. Složitost algoritmu (časová a paměťová). Třída P, třída NP, důvody jejich zavedení, jejich vzájemný vztah. NP-úplné problémy, příklady NP-úplných problémů, dokazovaní NP-úplnosti. Třída PSPACE, její vztah k třídám P a NP, PSPACE-úplné problémy. Třídy N a NL a NL-úplné problémy.

Výroková logika: jazyk, formule, pravdivostní ohodnocení, tautologie, tabulková metoda, sémantické vyplývání, normální formy formulí, úplné systémy spojek. Axiomatický systém výrokové logiky, syntaktické vyplývání. Věta o dedukci. Věty o korektnosti a úplnosti výrokové logiky. Predikátová logika: jazyk, termy a formule, struktury pro jazyk, ohodnocení termů a formulí. Axiomatický systém predikátové logiky, syntaktické vyplývání. Věty o korektnosti a úplnosti predikátové logiky.

Lineární datové struktury: seznam, zásobník, fronta. Metody třídění porovnáváním: insert sort, select sort, bubble sort, quick sort, merge sort, heap sort. Složitosti třídicích algoritmů. Grafy, stromy, základní pojmy a tvrzení. Vyhledávání v lineárních datových strukturách. Binární vyhledávací stromy, průchod a vyhledávání. Red-black stromy, AVL-stromy, B-stromy a jejich struktura, operace vyhledání, vložení a zrušení prvku. Hashování: hashovací funkce, organizace tabulek a způsoby řešení konfliktů.

Přehled a základní rysy programovacích paradigmat (funkcionální, procedurální, logické, objektové). Dynamický a statický typový systém. Prostředí, lexikální a dynamický rozsah platnosti. Správa paměti, garbage collector. Předávání argumentů procedurám, procedury vyšších řádů. Indukce a rekurze: princip a příklady.

Funkcionální programování: symbolické výrazy a vyhodnocovací proces jazyka Scheme. Seznamy a hierarchická data. Makra, typy maker, příklady použití. Líné vyhodnocování, přísliby a proudy. Aktuální pokračování a únikové funkce. Zásobníkový model vyhodnocování programů.

Objektové programování: třídy a objekty, zprávy a metody. Zapouzdření, polymorfismus, dědičnost. Metody objektů, jejich typy, způsoby ochrany. Vícenásobná dědičnost, rozhraní. Příklady objektově orientovaných jazyků.

Relační databázové systémy: relační model dat, základní pojmy (atributy, domény, ntice, relační schémata, relace). Operace relační algebry: množinové operace, projekce, selekce, dělení, spojení a jeho typy. Vzájemné vztahy relačních operací. Realizace operací relační algebry v jazyce SQL. Referenční integrita v relačním modelu dat. Funkční závislosti: definice, pravdivost v datech, modely, sémantické vyplývání, Armstrongova pravidla. Normalizace: Boyce-Coddova normální forma, normalizace dekompozicí a kompozicí schémat.

2 Teoretické základy informatiky

KMI/ALS1 Algoritmy a složitost 1

Složitost v průměrném případě: binární stromy, hašovací tabulky. Hašování, univerzální hašování, dokonalé hašování, Vyvážené stromy, B-stromy a jejich varianty, R-stromy a jejich varianty, digitální vyhledávání, trie, rozklad na singulární hodnoty a jeho výpočet, vlastnosti SVD, Pagerank – vlastnosti a výpočet.

KMI/ALS2 Algoritmy a složitost 2

Optimalizační problémy, aproximační algoritmy, základní pojmy a příklady. Třídy NPO a PO, NP-težké optimalizační problémy, příklady, vlastnosti. Problém pokrytí množiny (SET-COVER): aproximační algoritmy a jejich vlastnosti. Problém obchodního cestujícího a jeho varianty: aproximační algoritmy a jejich vlastnosti. Aproximační schémata a jejich příklady. Lineární programování: definice, varianty, obtížnost, princip duality. Metoda relaxace k lineárnímu programování: princip a příklad jejího použití. Pravděpodobnostní aproximační algoritmus: definice, algoritmus pro MAX-SAT, jeho vlastnosti a derandomizace.

KMI/TIK Teorie informace a kódování

Základní pojmy z pravděpodobnosti: pravděpodobnostní prostor a míra, podmíněná a sdružená pravděpodobnost, nezávislost jevů, Bayesova věta, náhodná proměnná, distribuční funkce a střední hodnota. Pojem entropie, jednoznačnost a základní vlastnosti. Podmíněná a sdružená entropie, pojem informace. Rozhodovací stromy, algoritmus ID3 s využitím podmíněné entropie, jiné klasifikační metody.

Kódování: základní pojmy, jednoznačně dekódovatelné kódy a test jednoznačné dekódovatelnosti, prefixové a blokové kódy. Kraftova a McMillanova věta. Optimální kódy a Shannonova věta. Huffmanův kód a jeho optimalita. Detekční a opravné kódy: příklady, Hammingova a minimální vzdálenost, podmínky detekce a opravy chyb, informační poměr, systematický kód. Binární lineární kódy: příklady, Hammingova a minimální váha, kontrolní matice. Hammingovy kódy: kódování a dekódování. Lineární kódy, základní pojmy, generující a kontrolní matice, kódování a dekódování.

KMI/PRKL Překladače

pro studenty, kteří nastoupili v ak. roce 2015/2016

KMI/PRKL1 Překladače 1

pro studenty, kteří nastoupili v ak. roce 2014/2015 a dříve

Základní struktura překladače, jednotlivé části překladače a fáze překladu. Lexikální analýza: základní pojmy (lexikální symboly – tokeny). Popis lexikálních symbolů regulárními gramatikami a regulárními výrazy. Konstrukce lexikálního analyzátoru konečným automatem. Konstrukce lexikálního analyzátoru s použitím generátoru lexikálních analyzátorů (lex, flex). Interní forma programu po lexikální analýze. Pumping lemma pro bezkontextové jazyky. Deterministická syntaktická analýza shora-dolů: Princip analýzy shora-dolů. Konstrukce zásobníkového automatu pro gramatiku LL(1). Výpočet množin First a Follow. Konstrukce syntaktického analyzátoru metodou rekurzivního sestupu. Transformace gramatiky pro odstranění kolizí v analyzátoru – odstranění levé rekurze, levá faktorizace, pohlcení řetězce. Deterministická syntaktická analýza zdola-nahoru: Princip analýzy zdola-nahoru. Konstrukce zásobníkového automatu pro gramatiky LALR(1) a SLR(1). Konstrukce syntaktického analyzátoru s použitím generátoru syntaktických analyzátorů (yacc, bison). Řešení kolizí v analyzátoru. Sémantická analýza: Atributová gramatika. Dědičné a syntetizované atributy, sémantická pravidla. L-atributové gramatiky a začlenění výpočtu atributů L-atributové gramatiky do syntaktického analyzátoru při analýze shora-dolů. S-atributové gramatiky a začlenění výpočtu atributů S-atributové gramatiky do syntaktického analyzátoru při analýze zdola-nahoru. Interní formy programu po sémantické analýze: AST, čtveřice. Tabulky symbolů.

3 Metody zpracování a modelování dat

KMI/KKD Kryptografie a komprese dat

pro studenty, kteří nastoupili v ak. roce 2014/2015 a dříve

Klasické šifry: afinní, Vigenerova a proudová šifra. Kryptoanalýza: typy útoků, redundance přirozeného jazyka, vzdálenost jednoznačnosti. Kryptoanalýza klasických šifer: frekvenční analýza, Kasiského a Friedmanův test. Perfektní šifrování: definice perfektní šifry, Shannonův teorém, Vernamova šifra. Symetrické šifry: DES, AES. Asymetrická šifra založená na zavazadlovém problému. Šifra RSA: popis algoritmu, bezpečnost, generování velkých prvočísel, testy prvočíselnosti. Statistické kompresní metody: Huffmanovo a aritmetické kódování. Třída slovníkových metod LZ77. Třída slovníkových metod LZ78. Ztrátová komprese obrazu JPEG.

KMI/KRY Kryptografie

pro studenty, kteří nastoupili v ak. roce 2015/2016

Základní pojmy z teorie čísel: Euklidův algoritmus, Bezoutova rovnost, zbytkové třídy, Eulerova funkce, Euler-Fermatova věta, Čínská věta o zbytcích, prvočíselná pole, rozšířená pole. Klasické šifry: posouvací, afinní, substituční, Vigenèrova a proudová šifra, linear feedback shift register. Redundance přirozeného jazyka, vzdálenost jednoznačnosti. Kryptoanalýza: typy útoků, frekvenční analýza, Kasiského a Friedmanův test. Perfektní šifrování: definice perfektní šifry, Shannonův teorém, Vernamova šifra. Symetrická šifra DES. Symetrická šifra AES. Bezpečná výměna klíče: motivace, Diffie-Hellmanova výměna klíče. Asymetrické šifrování: základní schéma, jednosměrná funkce, výhody, nevýhody, hybridní šifrování. Asymetrická šifra založená na zavazadlovém problému: popis šifry, důkaz korektnosti, bezpečnost. Šifra RSA: popis algoritmu, bezpečnost, generování velkých prvočísel, testy prvočíselnosti.

KMI/KOM Komprese dat

pro studenty, kteří nastoupili v ak. roce 2015/2016

Základní pojmy, taxonomie metod, míry komprese, typy modelů dat, Markovův model dat. Run-length encoding a Move-to-front kódování. Kódování čísel: unární kód, Eliasovy, Fibonacciho a Golombovy kódy. Tunstallův kód a Shannon-Fanovo kódování. Huffmanovo kódování se semi-adaptivním modelem. Huffmanovo kódování s adaptivním modelem. Aritmetické kódování. Kontextové kódování (PPM). Blokové třídění. Třída slovníkových metod LZ77. Třída slovníkových metod LZ78, reprezentace slovníku. Slovníková metoda LZW.

KMI/PDS Paralelní a distribuované systémy

Paralelní program, historie, atomické akce, synchronizace. Modely paralelních výpočtů, Flynnova klasifikace. Dokazování korektnosti programu, vyloučení interference (programová logika). Algoritmy kritické sekce (zámky, Petersonův aj.). Synchronizace bariérami (centralizovaná, symetrická). Semafory, jejich použití pro řešení synchr. problémů. Rozbor problému producent-konzument (správnost). Rozbor problému čtenáři-písaři (varianty a jejich řešení). Globální stav distribuovaného výpočtu (algoritmus snapshot). Logický čas (skalární, vektorový). Distribuované algoritmy vzájemného vyloučení a jejich složitost. Distribuované algoritmy pro detekci uváznutí.

KMI/ALS3 Algoritmy a složitost 3

pro studenty, kteří nastoupili v ak. roce 2014/2015 a dříve

Distribuovaný výpočetní model. Vlnové algoritmy. Algoritmy průchodu sítě. Algoritmus minimální kostry. Směrování s kompaktními tabulkami. Volba lídra. Byzantská dohoda. Složitost a výkonnost paralelních algoritmů. Zdvojování ukazatelů (paralelní výpočet sumy prefixu). Technika vyvážených stromů (paralelní výpočet sumy prefixu). Zřetězení (zatřiďování na 2-3 stromech). Akcelerující kaskády (výpočet maxima). Technika rozdělení (optimální zatřiďování). Paralelní vyhledávání a zatřiďování. Paralelní třídění (optimální algoritmus).

4 Okruh určený volbou povinně volitelných předmětů

Student si vylosuje otázku ze souboru předmětů, který si zvolí z níže uvedeného seznamu volitelných předmětů. Předměty ve zvoleném souboru musí mít v součtu alespoň 16 kreditů. Zvolené předměty student pošle e-mailem (nejpozději 14 dnů před zkouškou) zástupci vedoucího katedry pro studijní záležitosti.

KMI/ALGI Algoritmy v Internetu (4 kr.)
pro studenty, kteří nastoupili v ak. roce 2014/2015 a dříve

Protokol BGP: vnitřní a vnější směrování. Formální specifikace protokolu eBGP (algebry, grafy). Architektura a protokol vnitřního iBGP. Příklady oscilací směrování a možná řešení. Sítě peer-to-peer, první a druhá generace: Napster, Gnutella. Distribuované hašovací tabulky (Chord). Peer-to-peer systémy Pastry, SkipNet.

KMI/EVT Evoluční a výpočetní techniky (4 kr.)
pro studenty, kteří nastoupili v ak. roce 2014/2015 a dříve

Základní optimalizační algoritmy (horolezecký algoritmus, metoda zakázaného hledání, simulované žíhání). Genetické algoritmy (reprezentace, rekombinační operátory a jejich varianty). Messy GA. Věta o schématech,. Genetické programování (reprezentace, rekombinační operátory, modularita).

KMI/FUZ Fuzzy množiny (4 kr.)

Reziduované svazy a jejich základní vlastnosti, příklady reziduovaných svazů. Fuzzy množiny, jejich základní vlastnosti a operace s nimi. Fuzzy relace a jejich vlastnosti, fuzzy ekvivalence, fuzzy rovnosti. Extenzionalita fuzzy množin a fuzzy relací. Alfa řezy fuzzy množin a relací, vlastnosti zachovávající řezy, zavedení fuzzy množiny pomocí řezů. Princip rozšíření, zachování řezů v principu rozšíření. Fuzzy veličiny, fuzzy čísla, fuzzy intervaly. Fuzzy aritmetika pomocí řezů a pomocí principu rozšíření. Aplikace fuzzy množin: fuzzy regulátory a fuzzy automaty.

KMI/NLO Neklasické logiky (4 kr.)

Reziduované svazy a jejich vlastnosti, prelinearita, divisibilita, subdirektní reprezentace. Základy syntaxe a sémantiky výrokové BL logiky, schematická rozšíření. Věta o dedukci v BL logice. Věta o korektnosti výrokové BL logiky. Věta o úplnosti výrokové BL logiky (silná a slabá verze). Gödelova, Łukasiewiczova a Goguenova (produktová) logika. Standardní úplnost. Základy syntaxe predikátové BL logiky, vlastnosti kvantifikátorů. Základy sémantiky predikátové BL logiky, bezpečné interpretace. Věty o korektnosti a úplnosti predikátové BL logiky (přehledově). Užité pojmy: podalgebry, homomorfismy, direktní součiny, volné algebry, věta o varietách.

KMI/OOT Objektově orientované technologie (4 kr.)

Jazyk UML, diagramy tříd, vztahy mezi třídami asociace, agregace, kompozice, dědičnosti a závislosti. Jazyk OCL, omezující podmínky (invarianty) a jejich použití, operátory a operace jazyka OCL, kolekce a operace nad nimi, cykly, iterátory. Návrhové vzory a jejich účel, návrhové vzory vytvářející, návrhové vzory strukturální a návrhové vzory chování.

KMI/PPOG Počítačová grafika (5 kr.)
pro studenty, kteří nastoupili v ak. roce 2014/2015 a dříve

Bézierova metoda zobrazování křivek: Bézierovy křivky, racionální Bézierovy křivky. Bézierova metoda zobrazování ploch: čtyřúhelníkové a trojúhelníkové Bézierovy plochy, racionální Bézierovy plochy. NURBS: B-spline

bázové funkce, B-spline křivky, racionální B-sline křivky, NURBS křivky. Zobrazování těles a trojrozměrných dat: hraniční reprezentace, šablonování, konstruktivní geometrie, kódování voxelových modelů raw, run-length, octree, raytracing, global illumination, aproximace povrchu sítí trojúhelníků, Marching Cube algoritmus.

KMI/RDBS Relační databázové systémy (4 kr.)

Funkční závislosti: definice, pravdivost v datech, modely, sémantické vyplývání, kanonické modely, charakterizace sémantického vyplývání pomocí minimálních generátorů kanonických modelů, sémantické uzávěry množin atributů, algoritmy pro jejich výpočet (Closure, LinClosure). Funkční závislosti stanovená z dat: báze, redundance, nalezení mininální báze. Axiomatizace sémantického vyplývání funkčních závislostí: Armstrongova pravidla, důkazy, dokazatelnost, korektnost, úplnost.

KMI/TOI Topologie pro informatiky (5 kr.)

pro studenty, kteří nastoupili v ak. roce 2015/2016

Základy obecné topologie: topologické prostory, otevřené a uzavřené množiny, báze topologie a systémy generátorů. Podprostory, faktorprostory a součiny. Spojitá zobrazení a homeomorfismy. Kompaktní prostory. Vybrané aplikace obecné topologie: Stoneův teorém o reprezentaci Booleových algeber. Topologie datových typů, definovatelné a rozhodnutelné množiny, definovatelné funkce, definovatelnost velkého kvantifikátoru. Základy algebraické topologie: homotopická ekvivalence, singulární homologie, simpliciální homologie. Aplikace v analýze dat a asynchronních výpočtech.

KMI/AZO Analýza a zpracování obrazu (5 kr.)

pro studenty, kteří nastoupili v ak. roce 2014/2015 a dříve

Rekonstrukce obrazu: typy šumu, odstranění periodického šumu pomocí frekvenčních filtrů. Rekonstrukce obrazu: Wienerova filtrace. Popis a reprezentace obrazu: řetězové kódy, tvarová čísla, Fourierovy deskriptory. Matematická morfologie: operátory eroze, dilatace, uzavření a otevření.

KMI/BEPS Bezpečnost počítačových sítí (4 kr.)

Základy kryptografie: kontrolní součet, symetrická a asymetrická šifra, elektronický podpis, certifikace klíče. Bezpečnost TCP/IP, útoky a obrana. Autentizace a autorizace: faktory, heslo a metody jednorázových hesel, využití asymetrického šifrování, biometrika. Bezpečnost Ethernetu, útoky ve vztahu k IPv4 a IPv6 a obrana. Bezpečnost PPP a Wi-Fi, útoky a obrana. Filtrace IP a TCP/UDP, NAT, firewall a DMZ. Tunely a proxy: VPN, IPsec, aplikační proxy, brány a tunely. PKI: certifikát, žádost o něj a odvolání, CRL, zjišťování platnosti certifikátu, certifikační autorita. Aplikace PKI: elektronický podpis a obálka dat, bezpečná pošta (S/MIME). Šifrovaný protokol SSL/TLS: architektura, vytvoření spojení, aplikace. Šifrovaný protokol SSH: architektura, vytvoření spojení, autentizace, tunely.

KMI/FKA Fomální konceptuální analýza (4 kr.)

Formální kontext, formální koncept a konceptuální svaz. Galoisovy konexe, základní věta o konceptuálních svazech. Algoritmy pro výpočet konceptuálního svazu. Atributové implikace, jejich pravdivost, úplnost a báze. Armstrongovy axiomy, syntakticko-sémantická úplnost. Algoritmy pro výpočet atributových implikací.

KMI/SPA Síťové protokoly a algoritmy (5 kr.)

pro studenty, kteří nastoupili v ak. roce 2014/2015 a dříve

Protokol BGP: vnitřní a vnější směrování. Formální specifikace protokolu eBGP (algebry, grafy). Architektura a protokol vnitřního iBGP. Příklady oscilací směrování a možná řešení. Sítě peer-to-peer, první a druhá generace: Napster, Gnutella. Distribuované hašovací tabulky (Chord). Peer-to-peer systémy Pastry, SkipNet. Směrování v bezdrátových sítích. Řízení topologie. Shlukování a jeho aplikace.

KMI/ZZD Získávání znalostí z dat (4 kr.)

Explorační analýza dat. předzpracování dat: chybějící hodnoty, diskretizace, škálování. Asociační pravidla, základní pojmy, algoritmus Apriori. Shlukování: základní členění, míry (ne)podobnosti objektů a shluků. Teorie a metody hierarchického shlukování. Nehierarchické shlukování: Algoritmus shlukování k-means, fuzzy c-means, k-medoids. Shlukování založené na hustotě (DBSCAN), Sekvenční algoritmy. Klasifikace, rozhodovací stromy: růst a ořezávání. Redukce dimenze: Selekce atributů, PCA, Fisherův lineární diskriminant.

KMI/LGPR Logické programování (4 kr.)

Logické paradigma. Definitní programy: klauzule, fakta, pravidla a dotazy. Herbrandova struktura, herbrandův model, nejmenší herbrandův model a jeho nalezení. Sémantické vyplývání z definitních programů: substituce, aplikace substituce, uzavřené instance klausulí, korektní odpovědi. Rekursivní datové struktury a pravidla. Unifikace, nejobecnější unifikátor. Vztah deklarativní a procedurální sémantiky programu: korektní odpovědi, vypočtené odpovědi, korektnost, úplnost. Činnost zásobníku během výpočtu PROLOGu, backtracking, nalezení alternativních řešení. Řezy a negace, aritmetika, modifikace databáze. Expertní systém v PROLOGu.

KMI/LKFP Lambda kalkul a funkcionální programování (5 kr.)

Lambda-kalkul: lambda termy, redukce lambda termů, kombinátory. Normalizace, věta o pevném bodě. Programování v Haskellu: funkce, typy a typové třídy, pattern matching, stráže, funktory a monády.

KMI/MUSY Multimediální systémy (4 kr.)

pro studenty, kteří nastoupili v ak. roce 2014/2015 a dříve

Digitalizace analog. signálu, vzorkovací věta, filtrace. Reprezentace a formáty mult. dat. Barevné prostory. Komprese obrazu, JPEG. Komprese videa, standardy. Komprese zvuku, standardy. Komprese grafiky. Historie televize, kódování barev v televizním přenosu, televizní kanály. Pozemní digitální televize. Satelitní digitální televize. Televizní technologie ve světě.

KMI/MWEB Moderní webové technologie (4 kr.)

pro studenty, kteří nastoupili v ak. roce 2015/2016

CSS preprocesory: možnosti a využití. Pokročilé CSS: polyfill, flexbox model, gridlayout, critical CSS, OOCSS, BEM metodika. Adaptivní webdesign: principy a metody. HTML 5 API a element canvas: přehled, možnosti a použití. Search Engine Optimization: základní principy a metody. Šablonovací a ORM systémy. Google polymer, Angular.js, Node.js: stručná charakteristika a použití.

KMI/KOPR Konstrukce překladačů (4 kr.)

pro studenty, kteří nastoupili v ak. roce 2015/2016

KMI/PRKL2 Překladače 2 (4 kr.)

pro studenty, kteří nastoupili v ak. roce 2014/2015 a dříve

Základní struktura překladače, jednotlivé fáze překladu. Generování přechodného kódu: varianty syntaktických stromů, tříadresový kód, překlad výrazů, kontrola datových typů, ekvivalence typů a typová inference. Analýza toku dat a její použití. Lokální optimalizace, základní typy lokálních optimalizací. Globální optimalizace, základní typy globálních optimalizací. Generování cílového kódu, úloha přidělování registrů. Optimalizace generovaného kódu. Prostředí přeloženého programu: zásobník a alokování paměti, organizace haldy. Metody pro automatickou správu paměti: čítače referencí, algoritmus mark-sweep, kopírovací metody.

KMI/UNS Umělé neuronové sítě (4 kr.)

Neuronové sítě, principy. Jednoduchý model neuronu, McCulloch-Pits neuronové sítě. Perceptron, jeho vlastnosti, učení, lineární separabilita. Vícevrstvé neuronové sítě, jejich struktura a adaptace (backpropagation). Radial basis function sítě, topologie a učení. Asociativní sítě, Hopfieldova síť (struktura, adaptace, vybavování sítě), použití při optimalizaci obtížných úloh. Kompetiční neuronové sítě (struktura, učení), SOMs, counterpropagation.