Sylabus na štátnu skúšku zo spoločného základu v školskom roku 2000/2001 pre odbor Informatika [1]

28. novembra 2000

I. Matematika

1.1 Matematická analýza

1. Limita reálnej funkcie reálnej premennej. Nutná a postačujúca podmienka existencie limity funkcie v bode. Základné vety o limitách. Limita monotónnych funkcií a postupností.

2. Spojitosť funkcie. Základné vety o spojitých funkciách v bode. Spojité funkcie na množine a ich vlastnosti. [Rovnomerne spojité funkcie.]

3. Limita funkcie viac premenných. Limita zobrazenia z R^n do R^m. Spojitosť funkcie viac premenných. Spojitosť zobrazenia z R^n do R^m. Kompaktné a súvislé množiny. Vlastnosti spojitých zobrazení na kompaktných množinách.

4. Diferencovateľnosť funkcie jednej a viacerých premenných. Diferencovateľnosť zobrazenia z R^n do R^m. Súvis medzi diferencovateľnosťou a parciálnymi deriváciami. Spojitosť a diferencovateľnosť. Derivácia zloženého zobrazenia. Vety o strednej hodnote. Parciálne derivácie vyšších rádov, podmienky pre zámennosť ich derivovania. Taylorov vzorec. Extrémy funkcií. Nutné a postačujúce podmienky pre existenciu extrému.

5. Riemannov integrál. Základné vlastnosti R-integrálu. Nutná a postačujúca podmienka integrovateľnosti. Niektoré množiny R-integrovateľných funkcií. Veta o strednej hodnote. Metódy výpočtu R-integrálu. Newton-Leibnizov vzorec.

6. [Nevlastné integrály. Cauchyho-Bolzanova podmienka konvergenicie nevlastného integrálu. Kritériá konvergencie nevlastného integrálu.]

7. Číselné rady. Kritériá konvergencie. Absolútne a relatívne konvergentné rady.

8. Funkcionálne rady a postupnosti. Bodová a rovnomerná konvergencia. Kritériá pre rovnomernú konvergenciu postupností a radov funkcií. Vety o derivovaní a integrovaní rovnomerne konvergentných postupností a radov.

9. Mocninové rady. Abelova veta, polomer konvergencie. Vlastnosti mocninových radov v intervale konvergencie. Taylorov rad.

10. Lineárna diferenciálna rovnica 1. a n-tého rádu. Základné vlastnosti riešení. Lineárna diferenciálna rovnica 2. rádu s konštantnými koeficientami.

[1] Témy uzavreté v hranatých zátvorkách neboli (detailne alebo vôbec) v niektorom školskom roku odprednášané. Keďže tvoria neoddeliteľnú súčasť problematiky, je potrebné ich doštudovať z odbornej literatúry.

1.2 Algebra

Úvodné pojmy: základné pojmy z teórie množín, relácie, funkcie, binárne operácie. Pojem grupy, najzákladnejšie vlastnosti a príklady, pojem poľa, najzákladnejšie vlastnosti, príklady.

1. Vektorové priestory, lineárne zobrazenia: priestor, podpriestor, lineárna závislosť, báza a dimenzia. Steinitzova veta, súčty podpriestorov, lineárne zobrazenia, kompozícia lineárnych zobrazení, inverzné lineárne zobrazenia, matica lineárneho zobrazenia, jadro a obraz lineárneho zobrazenia.

2. Matice a riešenia lineárnych rovníc nad poľom F: matice, operácie s maticami (násobenie, sčítanie), elementárne riadkové operácie, trojuholníkový a redukovaný trojuholníkový tvar matice, systémy lineárnych rovníc nad poľom F, množina riešení homogénnych a nehomogénnych systémov lineárnych rovníc, existencia a tvary riešení.

3. Determinanty, determinant lineárneho zobrazenia a matice. Vlastnosti determinantov. Výpočty determinantov a ich použitie pri riešení lineárnych rovníc a hľadaní inverznej matice.

4. Euklidovské vektorové priestory, kvadratické formy: skalárny súčin, [matica skalárneho súčinu], vlastnosti skalárneho súčinu, dĺžka vektora, uhol medzi vektormi, ortonormálna báza euklidovského vektorového priestoru, ortogonálny doplnok, kvadratické formy, matica kvadratickej formy, kanonický tvar kvadratickej formy, Sylvestrov zákon zotrvačnosti. Kladne (semi-)definitné matice. Sylvestrova podmienka.

5. Podobnosť matíc, ortogonálna podobnosť matíc: matica lineárneho zobrazenia pri danej báze, definícia podobnosti matíc a vzťah k lineárnym zobrazeniam, kedy je matica podobná s diagonálnou maticou, ortogonálna podobnosť, charakteristický polynóm matice, vlastné čísla reálnej symetrickej matice.

6. Grupy: grupy, podgrupy, izomorfizmus a homomorfizmus grúp, cyklické grupy (s klasifikáciou) a ich podgrupy, grupy permutácií, rozklad grupy podľa podgrupy, Lagrangeova veta, homomorfizmus a izomorfizmus grúp, normálna podgrupa, faktorizácia grupy podľa podgrupy.

7. Okruhy: základné vlastnosti operácií v okruhoch, podokruh, ideál (hlavný, maximálny, prvoideál), faktorizácia okruhu podľa ideálu, vzťah medzi výsledkom faktorizácie a vlastnosťami ideálu, podľa ktorého sa faktorizuje, obor integrity a veta o podielovom poli.

8. Okruhy hlavných ideálov, existencia jednotky, najväčší spoločný deliteľ, vlastnosti deliteľnosti, ireducibilné prvky, veta o jednoznačnom rozklade.

9. Okruhy polynómov: pojem algebraického a transcendentného prvku pre daný okruh, okruh polynómov $R[x]$, okruh polynómov $F[x]$ nad poľom F ako okruh hlavných ideálov, veta o jednoznačnom rozklade polynómov nad daným poľom, substitučný homomorfizmus (veta o substitúcii), korene, viacnásobné korene, Hornerova schéma, derivácia, [Taylorov rozvoj].

10. Rozšírenia polí: jednoduché, viacnásobné a konečné rozšírenie poľa, vzťah medzi nimi, minimálny polynóm daného algebraického prvku, transcendentné rozšírenie.

11. [Teória konečných polí: charakteristika poľa, rozkladové pole daného polynómu nad daným poľom, veta o existencii a izomorfizmus rozkladových polí, konečné polia — veta o existencii a izomorfizme konečných polí.]

1.3 Diskrétna matematika

1. Výroky, logické operácie, formuly, výrokové funkcie, kvantifikácia výrokov, tautológie, matematický dôkaz, základné typy matematických dôkazov, logický dôsledok. Základné pojmy a označenia, intuitívny pojem množiny.

2. Operácie s množinami, zjednotenie, prienik, symetrická diferencia množín, množinové identity, karteziánsky súčin množín a jeho vlastnosti, relácie, relácie ekvivalencie a rozklad množiny, čiastočné usporiadanie a usporiadanie, zobrazenie. Mohutnosti množín. Ekvivalencia množín a kardinálne čísla, počítanie s kardinálnymi číslami, súčet, súčin a mocnina kardinálnych čísel, nerovnosti medzi kardinálnymi číslami. Cantorova-Bernsteinova veta a jej dôsledky. Cantorova veta a jej dôsledky. Konečné množiny. Nekonečné množiny. Aritmetika celých nezáporných čísel. Spočítateľné množiny, nespočítateľné množiny.

3. Základné pojmy kombinatoriky. Pravidlo súčtu a súčinu. Variácie a kombinácie s opakovaním a bez opakovania. Permutácie a permutácie s počtom cyklov danej dĺžky. Základné kombinatorické identity. Polynomická veta a jej dôsledky. Princíp zapojenia a vypojenia, jeho zovšeobecnenia a použitie. Počet surjektívnych zobrazení a počet predpísaných surjekcií na konečných množinách. Spernerova veta a jej použitie. Dirichletov princíp. Königova lema. Ramseyova veta. Ramseyove čísla. Systémy reprezentantov, Hallova veta, Hallov algoritmus, Königova veta pre binárne matice. Rozklady (partície) prirodzených čísel (usporiadané a neusporiadané). Metóda diagramov. Eulerova veta.

1.4 Kombinatorická analýza

Základne metódy výpočtu súm. Sumy a rekurentné vzťahy. Viacnásobné sumy. Konečný kalkul. Celočíselné funkcie (dolná a horná celá časť, div, mod). Sumy obsahujúce celé časti. Kombinačné čísla a ich vlastnosti. Binomická veta. Kombinatorické identity.

1.5 Teória grafov

1. Základy: stromy, lesy, bipartitné grafy, eulerovské grafy, cyklový priestor grafu.

2. Párenie: Königova teoréma a maximálnom párení, Hallova teoréma (o manželstvách) a ich dôsledky. Tuttova teoréma o 1-faktore a jej zovšeobecnenie. Petersenova teoréma o 1-faktore v kubických grafoch.

3. Súvislosť: charakterizácia dvoj- a trojsúvislých grafov, Mengerova teoréma a jej dôsledky, hranovo disjunktné kostry v grafe.

4. Planárne grafy: Reprezentácia grafov v rovine a v priestore, stereografická projekcia, Eulerova rovnosť, dualita v rovine, Kuratowského teoréma.

5. Farbenie: Heawoodova teoréma o 5 farbách, teoréma o 4 farbách, algoritmus postupného farbenia (greedy a.), Brooksova teoréma o hornom odhade chromatického čísla, Königova teoréma o hranovom farbení bipartitných grafov, Vizingova teoréma o hranových farbeniach. Zoznamové chromatické číslo (výberové číslo).

6. Hamiltonovské grafy: Diracova postačujúca podmienka, hamiltonovské kružnice a postupnosti stupňov, Chvátalova teoréma.

7. Toky v grafoch: Kirchhoffov zákon, Fordova a Fulkersonova teoréma o maximálnom toku a reze minimálnej kapacity, jej využitie. Fordov a Fulkersonov algoritmus na hľadanie maximálneho toku. Grupové toky, k-toky pre malé k, súvislosť s farbeniami.

8. Extremálne problémy, Turánova teoréma, Erdösova-Stonova teoréma, Ramseyova teoréma.

9. Náhodné grafy — základné pojmy a vlastnosti.

1.6 Logika pre informatikov

1. **Aritmetizácia**.

   - **Prirodzené čísla.** Reprezentácie prirodzených čísel: monadická, binárna, dyadická, párová.
   - **Primitívna rekurzia.** Rekurzia s mierou. Binárna a dyadická aritmetika.
   - **Zoznamy.** Triedenie zoznamov. Kombinatorické funkcie. Aritmetizácia pomocou zoznamov.
   - **Binárne stromy.** Binárne prehľadávacie stromy. Perfektne vyvážené stromy.
   - **Symbolické výrazy.** Aritmetické výrazy. Výroková logika.

2. **Úvod do logiky prvého rádu.**

   Tautológie. Výrokovologické vyplývanie a veta o kompaktnosti. Kvázitautológie. Logická platnosť a logické vyplývanie. Základná veta logiky prvého rádu. Gödelova veta o úplnosti pre tablový dokazovací systém. Peanova aritmetika.

1.7 Numerická matematika

Odhady nepresnosti výpočtov. Aproximácie funkcií polynómami. Interpolácia. Numerická kvadratúra. Metóda najmenších štvorcov. Newtonova metóda. Metóda regula falsi. [Systémy lineárnych algebraických rovníc. Gaussova eliminácia.] Numerické riešenie nelineárnych rovníc, systémy nelineárnych rovníc.

1.8 Pravdepodobnosť a matematická štatistika

Definícia a vlastnosti pravdepodobnosti. Pojem náhodnej premennej. Diskrétne a spojité náhodné premenné. Stredná hodnota náhodnej premennej a jej výpočet. Disperzia. Nezávislosť. Bernoulliho schéma. [Zákon veľkých čísel. Centrálna limitná veta.] Podmienená pravdepodobnosť. Bayesov vzorec. Definícia podmienenej pravdepodobnosti. Pojem náhodného výberu. Regresné priamky, koeficient korelácie. Testovanie štatistických hypotéz. Intervalové odhady.

II. Základy informatiky

2.1 Programovanie

Podprogramy, odovzdávanie parametrov, rekurzia. Metóda vyhľadávania s návratom (backtracking). Vstup a výstup, (štandardné) V/V súbory, textové a binárne súbory. Realizácia dátových štruktúr (zásobník, front, spájané zoznamy, stromy, vyhľadávacie stromy, grafy, množiny,...) Rôzne triediace algoritmy, vyhľadávanie. Objekty v jazyku Pascal (dedičnosť, zapúzdrenie, polymorfizmus).

2.2 Princípy tvorby software

Diagram dátových tokov. Entitno-relačný diagram a diagram tried. Štruktúrované metódy analýzy (Yourdonova metóda). Objektovo-orientované metódy analýzy (metóda OMT). Metóda riadenia projektov (metóda PRINCE).

2.3 Teória programovania

Programové schémy. Základné pojmy (štandardná schéma, interpretácia schém, vlastnosti schém). (Ne)rozhodnuteľnosť vlastností štandardných schém. Podtriedy štandardných schém s rozhodnuteľnými vlastnosťami (voľné, Janovove schémy). Porovnávanie a preklad tried schém — vzťahy medzi triedami štandardných a rekurzívnych schém. Čiastočne interpretované schémy.

Správnosť programov. Čiastočná a totálna správnosť programov. Invarianty a induktívne formuly. Metódy dokazovania čiastočnej a totálnej správnosti — indukčné techniky. Najslabšia vstupná a najsilnejšia výstupná podmienka. Systematický vývoj korektných programov.

Sémantika programov a jazykov. Význam programu. Princípy operačnej, denotačnej a axiomatickej sémantiky. Sémantické domény a ich konštrukcia. Formálna definícia (operačného a denotačného) významu imperatívnych a rekurzívnych programov. Porovnanie operačnej a denotačnej sémantiky imperatívnych a rekurzívnych programov. Korektnosť výpočtových pravidiel a kritériá ich korektnosti.

2.4 Princípy počítačov

Kódovanie informácií v počítači, Booleovské funkcie a ich realizácia pomocou DNF, minimalizácia DNF, návrh kombinačných a sekvenčných obvodov, digitálne systémy.

Základné princípy činnosti počítača von Neumannovského typu. Mikroinštrukčný súbor, množina registrov, ALU, spracovanie inštrukcií, ošetrenie prerušení, mikroprogramovanie, RISC versus CISC. Pamäť, operačná, pomocná, cache, virtuálna. I/O zariadenia, metódy I/O údajov, periférne zariadenia.

2.5 Operačné systémy

1. Význam používania jazyka assemblera. Assembler: typy inštrukcií, základné spôsoby adresovania (registrový mód, nepriamy registrový mód, autoinkrement, autodekrement, relatívny mód).

2. Makrá — definícia, rozvoj, volanie. Assembler — úlohy, jedno- a dvojprechodový assembler. Makroprocesor — úlohy, jedno- a dvojprechodový makroprocesor, makroassembler.

3. Štruktúra operačného systému, funkcie a služby operačného systému — systémové volania, základné prvky počítačového systému — procesy a súbory.

4. Procesy — vytváranie, hierarchia procesov, životný cyklus procesu, komunikácia medzi procesmi.

5. Synchronizácia procesov — časová závislosť procesov, vzájomné vylúčenie a spôsoby jeho dosiahnutia, klasické problémy synchronizácie procesov.

6. Uviaznutie — kritériá pre jeho vznik, metódy riešenia problému uviaznutia.

7. Správa procesov a procesora — plánovače a ich funkcie, algoritmy plánovania procesov.

8. Správa pamäte — funkcie, transformácia adries, modely reálnej pamäte (typy správy pamäte: holý počítač, jeden súvislý úsek, statické súvislé úseky, dynamické súvislé úseky, stránkovanie, segmentácia).

9. Správa pamäte — modely virtuálnej pamäte, stránkovanie — výpadok stránky, nahradzovacie algoritmy, stránkovanie na žiadosť a pracovná množina, niektoré problémy pri implementácii — zálohovanie inštrukcií, zamykanie stránok v pamäti, zdieľanie stránok.

10. Správa súborov — funkcie, súbory, adresáre (typy, organizácia, implementácia), správa voľného diskového priestoru, správa priestoru prideleného súboru (DOS, UNIX), zdieľané súbory (linky).

11. Správa zariadení — funkcie správy zariadení, technické charakteristiky periférnych zariadení (delenie V/V zariadení, pojem riadiaca jednotka, priamy prístup do pamäte), techniky prideľovania V/V zariadení, V/V software, správa diskových požiadaviek.

2.6 Databázové systémy

1. **Dátové modely.** Entitno-relačný model. [Bachmanove diagramy.] Relačný model.

2. **Architektúra DBMS a modelovanie reality.** Trojschémová architektúra (ANSI sparc).

3. **Relačný model.** Relačná algebra. Tabuľková a predikátová interpretácia relačnej algebry. Negácia, doménovo nezávislé a bezpečné formuly. Relačný kalkul (doménový). Relačný jazyk SQL. Programovanie v SQL. Iné dotazové jazyky (QBE, Datalog).

4. **Teória navrhovania relačných báz dát.** Funkčné závislosti, vyplývanie, Armstrongove axiómy, efektívne odvodenie. Normálne formy 3NF, BCNF. Algoritmy pre úpravu do normálnych foriem.

5. **Transakcie a spracovanie transakcií.** Sériovateľnosť, test sériovateľnosti. Zámky a zamykacie protokoly. Journal, commit a rollback. Optimistické a pesimistické riadenie transakcií, časové razítka.

6. **Bezpečnosť v databázových systémoch.** Autorizácia, metódy ochrany pred neoprávneným prístupom. Ochrana dát pred poškodením a zničením — backup.

7. **Fyzická organizácia.** Dvojúrovňový model pamäti a organizácie dát. Indexové súbory. B a B^*-stromy. Hašované súbory. Dotazy na čiastočnú zhodu. Realizácia relačných operácií. Kompresia dát (statické metódy, Ziv–Lempel).

2.7 Špecifikácia a verifikácia programov

Špecifikácia a verifikácia programov v Peanovej aritmetike. Odvodené induktívne princípy. Indukcia s mierou a štrukturálna indukcia. Ich redukcia do matematickej indukcie. Binárna a dyadická aritmetika, zoznamy, polia, stromy, symbolické výrazy.

2.8 Formálne jazyky a automaty

Regulárne jazyky. Deterministické a nedeterministické konečné automaty, regulárne gramatiky, regulárne výrazy, ekvivalencia popisov regulárnych jazykov, Nerodova veta, pumpovacia lema, uzáverové vlastnosti. Bezkontextové jazyky. Bezkontextové gramatiky, normálne tvary, nedeterministické zásobníkové automaty, ekvivalencia zásobníkových automatov a bezkontextových gramatík, uzáverové vlastnosti. Kontextové jazyky. Kontextové gramatiky, lineárne ohraničené automaty, ich ekvivalencia, uzáverové vlastnosti. Rekurzívne vyčísliteľné a rekurzívne jazyky. Turingove stroje, frázové gramatiky, ich ekvivalencia, uzáverové vlastnosti, univerzálny Turingov stroj, Turingova hypotéza. Nerozhodnuteľné problémy. Diagonalizácia, problém zastavenia, Postov problém, nerozhodnuteľné problémy pre bezkontextové jazyky, rozhodnuteľné problémy pre bezkontextové jazyky, metódy dokazovania nerozhodnuteľnosti.

2.9 Efektívne algoritmy

Problém slovníka (2–3 stromy). Union/Find-Set problém. Algoritmy pre hľadanie najkratších ciest a najlacnejšej kostry grafu. Princípy tvorby efektívnych algoritmov (vrátane konkrétnych aplikácií). Rozdeľuj a panuj. Dynamické programovanie. „Greedy“ algoritmy, vyváženosť a voľba vhodnej dátovej štruktúry. Triedy P a NP, polynomiálna redukovateľnosť, [Cookova veta] a NP-úplné problémy.

2.10 Algoritmy a dátové štruktúry

1. **Matematické základy.** Asymptotické označenia pre rast funkcií. Porovnanie funkcií na báze asymptotických označení. Iteratívna logaritmická funkcia ($\log^*$). Riešenie rekurencií substitúciou, iteratívne, rekurzívne stromy — master metóda.

2. **Algoritmy triedenia.** Elementárne, Heapsort, BottomUp Heapsort, Quicksort, znáhodnený Quicksort — analýza algoritmu. Halda, prioritná fronta. Dolný odhad pre triedenia porovnávaním.

3. **Lineárne triedenia.** Counting-sort, Radix-sort, Bucket-sort.

4. **Elementárne dátové štruktúry.** Elementárne dátové štruktúry, ich implementácia, zásobník, rad, zoznam, strom.

5. **Hašované tabuľky.** Tabuľky s priamou adresáciou. hašovanie so zreťazením, s otvorenou adresáciou, univerzálne hašovanie.

6. **Vyspelejšie dátové štruktúry.** Binárne prehľadávacie stromy a problém vyváženosti, červenočierne stromy.

7. **Vyspelejšie techniky tvorby algoritmov.** Dynamické programovanie, násobenie reťazca matíc; greedy algoritmy, knapsack problém, Huffmanovo kódovanie.