Sylabus na štátnu skúšku blokového štúdia odboru Informatika z bloku Matematické metódy informatiky v školskom roku 2000/2001

27. novembra 2000

1 Teória kódovania a kryptológia

Základné pojmy teórie kódovania. Rovnomerné a blokové kódy. Rozdeliteľné a silne rozdeliteľné kódy. Kraftova-McMillanova nerovnosť. Cena kódu. Entropia. Kvázioptimálne kódy. Konštrukcia optimálneho kódu. Rozšírenia kódu. Kódovanie Markovovských zdrojov. Kódovanie s predpoveďou.

Model prenosového kanála. Typy chýb. Biely šum. Kódy odhaľujúce a opravujúce chyby — geometrické princípy. Obdĺžnikové kódy, Hammingov $(7,4)$-kód. Lineárne kódy. Konštrukcia, vlastnosti, kódovanie a dekódovanie. Dokonalé a kvázidokonalé kódy. Cyklické kódy. BCH kódy, konštrukcia, metódy kódovania a dekódovania.

Základné pojmy: otvorený, šifrovaný text, kľúč, šifrovanie, dešifrovanie, kryptoanalýza. Typy kryptoanalytických útokov. Klasické kryptosystémy a ich kryptoanalýza. Generátory presudonáhodných postupností. Stream ciphers. Blokové šifry. *DES.* Šifrovanie s verejnými kľúčmi. *RSA.* Aplikácie.

2 Výpočtová zložitosť

Turingove stroje, základné zložitostné triedy a vzťahy medzi nimi (Savitchova veta, Translačná lema, simulácie a hierarchie; existencia ťažkých problémov). Gap Theorem a Veta o zrýchľovaní. NP-úplnosť, Cookova veta a niektoré ďalšie (aj pre prax dôležité) NP-úplné problémy. Vzťah NP-úplných a NP-optimalizačných problémov. Aproximačné algoritmy pre NP-optimalizačné problémy; neaproximovateľnosť. Výpočty s orákulom a vzťah tried P a NP. Jednosmerné funkcie a šifrovanie. Pravdepodobnostné algoritmy a RSA šifrovací systém. $PSPACE$-úplné problémy.

3 Teória vypočítateľnosti

Funkcie a čiastočné funkcie; projekcie, skladanie funkcií, trojice číslovacích (párovacích) funkcií. Univerzálne funkcie a čiastočné funkcie. Primitívne rekurzívne, rekurzívne funkcie a čiastočne rekurzívne (vypočítateľné) funkcie (na množine $\mathbb{N}$). Primitívne rekurzívne, rekurzívne a rekurzívne spočítateľné množiny a predikáty a ich vlastnosti. Modely vypočítateľnosti (Turingove stroje a iné modely). Ekvivalentnosť modelov vypočítateľnosti. Churchova téza. Problém zastavenia a iné nerozhodnuteľné problémy. Kódovanie nečíselných oborov (oborov slov) do prirodzených čísel.

4 Kombinatorická analýza II.

Generujúce funkcie. Základné pojmy, operácie s g.f. Konvolúcia g.f. Použitie generujúcich funkcií na riešenie rekurentných vzťahov. Príklady: počet kostier vo vejári, Fibonacciho čísla, dobre uzátvorkované výrazy. Exponenciálne generujúce funkcie, operácie s nimi. Bernoulliho čísla.

Asymptotická analýza. Nekonečne malé a nekonečne veľké veličiny. Hardyho trieda logaritmicko-exponenciálnych funkcií. Notácia o, O, Ω, Θ, rádová rovnosť a asymptotická rovnosť. Narábanie s O. Asymptotické odhady odvodené pomocou radov. Metódy bootstrapping (asymptotická iterácia), traiding tails (odhady podstatných častí), Eulerova sumačná formula a jej použitie. Príklady.

5 Vybrané partie z logiky

1. **Výroková logika:** Jazyk logiky, formálne systémy logiky, výroková logika, veta o kompaktnosti, dôsledok vety o kompaktnosti, formálny systém výrokovej logiky, veta o dedukcii, základné teorémy výrokovej logiky, Postova veta, bezospornosť formálneho systému, veta o nahradení podformúl ekvivalentnými formulami, de Morganove pravidlá, veta o dôkaze rozborom prípadov, ekvivalentné vyjadrenie formúl d.n.f. a k.n.f., veta o substitúcii prvotných formúl, ekvivalentnosť pravidla modus ponens a pravidla rezu.

2. **Predikátová logika:** Jazyk a jeho sémantika, sémantika predikátovej logiky, substitúcia termov za premenné. Axiómy a pravidlá odvodenia predikátovej logiky, pravidlo zavedenia veľkého kvantifikátora, veta o uzávere, lema o distribúcii kvantifikátorov, veta o ekvivalencii, veta o variantoch, veta o dedukcii, veta o konštantách, zovšeobecnenie vety o dedukcii. Prenexný tvar formuly a Skolemov tvar formuly. Axiómy rovnosti, logika s rovnosťou, veta o korektnosti, bezospornosť predikátovej logiky, Gödelova veta, Henkinova veta, Lindenbaumova veta. Veta o kompaktnosti.

3. **Metóda rezolvent:** Skolemovské štandardné formy. Herbrandovské univerzum. Sémantický strom. Herbrandova veta I. a II. variant. Rezolvenčná metóda, substitúcia a unifikácia, unifikačná veta, úplnosť rezolvenčnej metódy, stratégia vymazávania, algoritmus pohltenia a jeho korektnosť.