Požiadavky Algoritmy a datové struktury II, TIN061, ZS 2008/09

Vyhľadávanie vzorkov v reťazcoch, vyhľadávací stroj Aho-Corasicková: konštrukcia, dôkaz správnosti, zložitosť konštrukcie, zložitosť vyhľadávania; (možnosti realizácie vyhľadávacieho stroja). Algoritmy Rabin-Karp, Knuth-Morris-Pratt.

Toky v sieti, reziduálna sieť. Alg. Ford-Fulkerson a jeho správnosť, vzťah veľkosti toku a rezu, iné stratégie voľby cesty. Vrstvená sieť, Dinicov algoritmus, Goldbergov algoritmus, aplikácia na maximálne párovánie.

Rýchla Fourierova transformácia. Inverzná diskrétna Fourierova transformácia. Prevod na iteratívnu implementáciu, implementácia obvodom "butefly". Použitie na násobenie dlhých čísel.

Kombinačné obvody, miery ich zložitosti. Triediace siete, implementácia mergesortu. Paralelné sčítanie pomocou algoritmu carry look-ahead.

Triedy rozhodovacích problémov P, NP a NP-úplné, prevoditeľnosť a polynomiálna prevoditeľnosť, prevod CNFSat na Kliku, príklady dalších NP-úplných problémov.

Aproximačné algoritmy, pomerová a relatívna chyba; aproximačné schéma, polynomiálne, úplné. Aproximačný algoritmus pre Vrcholové pokrytie a pre problém Obchodného cestujúceho s trojuholníkovou nerovnosťou. Neexistencia aprox. alg. pre obecný problém Obchodného cestujúceho. Použitie aprox. schémy pre Súčet podmnožiny.

Rozšírený Euklidov algoritmus. Kryptografické protokoly: komutujúce šifry, verejné kryptografické systémy, elektronický podpis, (jednocestné) hašovacie funkcie, certifikačné autority. Šifra RSA.

Pravdepodobnostné algoritmy, idea Rabin-Millerovho testu prvočíselnosti.

Konvexný obal v rovine, lineárna zložitosť konštrukcie na predpripravených datách. Prevod Konvexného obalu na triedenie čísel. (Voronoiove diagramy, Fortunov algoritmus.)

Dynamické programovanie. Tabelácia, počítanie zdola. Problém najdlhšej spoločnej podpostupnosti.