

APLIKOVANÁ INFORMATIKA

6IOA001 štátna skúška – okruhy tém

1. Algoritmy a údajové štruktúry

- Štruktúry uložené v operačnej pamäti podporujúce viacrozmerné intervalové vyhľadávanie: quad strom, k-d strom.
- Vyhľadávacie stromy a ich implementácia: AVL strom, 2-3 strom, 2-4 strom, splay strom, treap, RB strom, AA strom, tango strom, znakové stromy.
- Pokročilé implementácie prioritného frontu: Fibonacciho halda, párovacia halda.
- Hešovací súbory: statický hešovací súbor, rozšíriteľné hešovanie, dynamické hešovanie, lineárne hešovanie.
- Efektívne triedenie dát v súboroch. Súvislý utriedený súbor a možnosti vyhľadávania dát v ňom.
- B-strom. Indexované utriedené štruktúry: B+ strom. Indexované neutriedené štruktúry: súbor s úplným indexom.
- Štruktúry uložené v súboroch podporujúce viacrozmerné intervalové vyhľadávanie: R-strom a jeho varianty.
- Vyhľadávanie reťazcov v texte: priamy algoritmus, Knuth – Morris – Pratt algoritmus, Karp – Rabin algoritmus.
- Komprimačné algoritmy: Shannon–Fano kódovanie, Huffmanovo kódovanie, LZ78 kódovanie, Lempel–Ziv-Welch kódovanie.
- Geometrické algoritmy: Voronoiové diagramy, Fortunov algoritmus, Delaunayova triangulácia.

2. Pokročilé databázové systémy

- Relačné DBS.
- Objekty v DBS.
- Jazyky a DBS (XML, JSON, SQL a PL/SQL).
- Transakčné spracovanie a paralelizmus v DBS.
- Výkonnosť databázových systémov (vyhľadávanie, indexovanie, prístupové metódy).
- Distribuované spracovanie dát.

3. Komunikačné technológie

- Vývoj v oblasti sieťových architektúr (klient/server a Peer-to-Peer) a vrstvomý model IP sietí.
- Protokol IPv6 a IPv4.
- Základy programovania sieťových aplikácií - TCP/IP sockety.
- Bezpečnosť IP sietí. Princípy, úlohy a funkcie zabezpečenia sietí (integrita, autenticita, šifrovanie). Bezpečnosť a zabezpečenie v TCP/IP architektúre.
- Multimediálna prevádzka a konvergované IP siete.
- Internet vecí (IoT) - definovanie základných pojmov a princípov.
- Vývojové trendy (SDN, network programmability).
- Virtualizácia a Cloud.
- Automatizácia a orchestrácia koncových zariadení.

4. Optimalizácia sietí

- Úloha návrhu štruktúry distribučného systému, model, prostriedky riešenia, úloha odberných dní.
- Úloha okružných jazd, úplná úloha návrhu distribučného systému, dekompozícia úlohy, model dopravnej siete.
- Verejné a súkromné obslužné systémy.
- Primárne a duálne heuristiky.
- Metaheuristiky.
- Harmonogramy dodávok a optimalizácia odberných dní.
- Riešenie úloh okružných jazd. Metódy riešenia úlohy obsluhy úsekov dopravnej siete. Špeciálne heuristiky pre riešenie úloh okružných jazd.
- Časové rozvrhy.

5. Architektúry informačných systémov

- Informačné systémy a systémová metodológia.
- Metodiky vývoja a riadenie projektov IS.
- Systems and software engineering, Norma ISO/IEC/IEEE 42010:2011.
- Biznis architektúra – analýza požiadaviek.
- Biznis architektúra - biznis procesy.
- Modelom riadená architektúra.
- Špecifikácia požiadaviek na IS.
- Softvérová architektúra.
- Finalizácia vývoja informačných systémov.
- Meranie výkonnosti informačných systémov.

6. Diskrétna simulácia

- Generátory náhodných čísel. Testovanie generátorov náhodných čísel. Generovanie náhodných veličín.
- Algoritmizácia simulačných modelov. Implementácia metódy plánovania udalostí a metódy snímania aktivít.
- Kombinovaná (diskrétno-spojité) simulácia. Animácia v simulácií.
- Agentovo orientované architektúry simulačných modelov. Architektúra ABASim.
- Distribuovaná simulácia. Konzervatívne metódy synchronizácie distribuovaných simulačných modelov. Optimistické metódy synchronizácie distribuovaných simulačných modelov.
- Pokročilé metódy, algoritmy a paradigmy využiteľné v modelovaní a simulácii - Petriho siete, BDI, atď.

7. Teória informácie

- Definícia pojmov informácie javu a entropie pokusu a ich vlastnosti.
- Podmienená entropia a spoločná informácia pokusov.
- Zdroje informácie a ich vlastnosti, entropia zdroja.
- Prefixové kódy, Kraftova nerovnosť, Huffmanove kódovanie a kompresia správ.

- Blokové kódy, kódy objavujúce a opravujúce chyby, príklady kódov EAN13, IBAN, rodné číslo.
- Lineárne kódy a ich vlastnosti, generujúca matica, kontrolná matica, syndróm slova, príklady lineárnych kódov objavujúcich a opravujúcich chyby, Hammingov kód.

8. Databázy a získavanie znalostí

- Reprezentácia znalostí.
- Algoritmy zoskupovania.
- Algoritmy klasifikácie.
- Rozhodovacie stromy.
- Rozhodovacie pravidlá, konverzia pravidiel do rozhodovacích stromov a späť.
- Orezávanie rozhodovacích stromov.
- Čistenie a transformácia dát, analýza chýb.
- Asociačné pravidla.

9. Kryptografia a bezpečnosť

- Význam kryptografie, všeobecný model šifrovacieho systému a základné typy útokov.
- Klasická kryptografia, monoalfabetické a polyalfabetické šifry a ich kryptoanalýza.
- Perfektná a výpočtová bezpečnosť kryptosystému, Vernamova šifra, generátory pravej náhodnej postupnosti.
- Prúdové šifry, generátory pseudonáhodných postupností a ich vlastnosti, RC4 generátor.
- Posuvné registre s lineárnou spätnou väzbou a ich vlastnosti, Geffeho generátor, Alternating step generátor, Shrinking generátor, GSM A5 generátor.
- Blokové šifry a ich vlastnosti, kryptosystémy Feistelovho typu DES a GOST, šifra IDEA, šifra Rijndael (AES).
- Jednocestné funkcie, diskrétny logaritmus, Diffie - Hellmanova výmena kľúčov.
- Asymetrická kryptografia, vlastnosti prvočísel, RSA – algoritmus.
- Hashovacie algoritmy a ich vlastnosti, narodeninový paradox, príklad algoritmov MD4 a MD5.
- Digitálny podpis, časové známky, problémy distribúcie verejného kľúča.