Tematické okruhy k magisterské státní zkoušce z předmětu Informační technologie

I. Matematické základy informatiky

1. Výpočetní složitost algoritmů. Techniky analýzy výpočetní složitosti algoritmů: analýza rekurzivních algoritmů, amortizovaná analýza, složitost algoritmů v průměrném případě.
2. Matematické modely algoritmů – Turingovy stroje a stroje RAM. Algoritmicky nerozhodnutelné problémy.
3. Třídy složitosti problémů. Třída PTIME a NPTIME, NP-úplné problémy. Další třídy složitosti (PSPACE, EXPTIME, EXPSPACE, polynomiální hierarchie, NLOGSPACE, LOGSPACE, ...).
4. Výpočetní modely pro paralelní a distribuované algoritmy. Výpočetní složitost paralelních algoritmů. Komunikační složitost.
5. Jazyk predikátové logiky prvního řádu. Práce s kvantifikátory a ekvivalentní transformace formulí.
6. Pojem relace, operace s relacemi, vlastnosti binárních homogenních relací. Relace ekvivalence a relace uspořádání a jejich aplikace.
7. Pojem operace a obecný pojem algebra. Algebry s jednou a dvěma binárními operacemi.
8. FCA – formální kontext, formální koncept, konceptuální svazy.
9. Asociační pravidla, hledání často se opakujících množin položek.
10. Metrické a topologické prostory – metriky a podobnosti. Jejich aplikace.
11. Shlukování. Typy shlukování, metody pro určení kvality shlukování, aplikace shlukování.
12. Náhodná veličina. Základní typy náhodných veličin. Funkce určující rozdělení náhodných veličin.
13. Vybraná rozdělení diskrétní a spojité náhodné veličiny - binomické, hypergeometrické, negativně binomické, Poissonovo, exponenciální, Weibullovo, normální rozdělení.
14. Popisná statistika. Číselné charakteristiky a vizualizace kategoriálních a kvantitativních proměnných.
15. Metody statistické indukce. Intervalové odhady. Princip testování hypotéz.

Okruhy pokrývají předměty Teoretická informatika, Pravděpodobnost a statistika, Matematika pro zpracování znalostí

II. Softwarové inženýrství

1. Význam testování, terminologie, testovací proces, Úrovně testování (V-model), Testovací techniky.
2. Architektonické styly.
3. Kvalitativní požadavky a jejich dosažení. Měření kvality návrhu.
4. Návrhové principy.
5. Návrhové vzory.
6. Co je to Secure Software Development Lifecycle (SSDLC)? Jaká jsou jeho specifika a využití?
7. Popište pět základních bezpečnostních vlastností, které se používají k zajištění bezpečnosti a spolehlivosti informačních systémů. Zkratka “CIAAN”, tedy “Confidentiality”, “Integrity”, “Availability”, “Authenticity” a “Non-repudiation”. Uveďte příklady softwarových požadavků, které z těchto vlastností vycházejí.

8. Penetrační testování software. Deskriptivní a preskriptivní rámce pro penetrační testování. Metody penetračního testování.

Okruhy pokývají předměty: Kvalita software

III. Databázové systémy

1. Relační datový model, SQL; funkční závislosti, dekompozice a normální formy.
2. Transakce, zotavení, log, ACID, operace COMMIT a ROLLBACK; problémy souběhu, řízení souběhu: zamykání, úroveň izolace v SQL.
3. Procedurální rozšíření SQL, PL/SQL, T-SQL, triggery, funkce, procedury, kurzory, hromadné operace.
4. Fyzická implementace databázových systémů: tabulky (halda, shlukovaná tabulka, hashovaná tabulka) a indexy (B-strom, bitmapový index), materializované pohledy, rozdělení dat.
5. Plán vykonávání dotazů, logické a fyzické operace, náhodné a sekvenční přístupy, ladění vykonávání dotazů.
6. Řádkování výsledku dotazu, komprimace tabulek a indexů, sloupcové a řádkové uložení tabulek.
7. CAP teorém, NoSQL DBS, BASE, replikace, MongoDB, CRUD operace.
8. Vícerozměrné datové struktury, podpora uložení prostorových dat v DBS.

Okruhy pokrývají předměty (Databázové systémy I, Databázové systémy II, Pokročilé databázové systémy)

IV. Počítačové systémy a sítě

1. Architektura univerzálních procesorů. Principy urychlování činnosti procesorů.
2. Základní vlastnosti monolitických počítačů a jejich typické integrované periférie. Možnosti použití.
3. Protokolová rodina TCP/IP.
4. Problémy směrování v počítačových sítích. Adresování v IP sítích.
5. Bezpečnost počítačových sítí s TCP/IP: útoky, paketové filtry, stavový firewall. Šifrování a autentizace, virtuální privátní sítě.
6. Paralelní výpočty a platformy: Flynnova taxonomie, SIMD, MIMD, SPMD. Paralelismus na úrovni instrukcí, datový a funkční paralelismus. Procesy a vlákna.
7. Systémy se sdílenou a distribuovanou pamětí: komunikace mezi procesy (souběh, uváznutí, vzájemné vyloučení). Komunikace pomocí zasílání zpráv. OpenMP, MPI.
8. Paralelní redukce a paralelní scan: principy fungování ve vybrané technologii a příklady užití
9. Konkurentní datové struktury: přehled, blokující a neblokující implementace

Okruhy pokrývají předměty Architektury počítačů a paralelních systémů, Počítačové sítě, Paralelní algoritmy I