Bakalářské zkoušky (příklady otázek)

podzim 2012

1 Kryptografie, RSA

1. Vysvětlete termíny „asymetrická kryptografie“, „veřejný klíč“, „soukromý klíč“.
2. Vysvětlete, jak lze asymetrickou šifru využít k podepisování dokumentů.
3. Popište postup inicializace, šifrování a dešifrování algoritmem RSA.

2 Třídy složitosti

1. Definujte pojmy P, NP, NP-těžký a NP-úplný problém.
2. Uveďte tři příklady NP-úplných problémů.

3 Třídění Quick Sort

1. Napište pseudokód třídícího algoritmu Quick Sort.
2. Zdůvodněte, jaké jsou nejmenší a největší počty kroků a spotřeba paměti tohoto algoritmu pro n prvků.
3. Napište průměrnou časovou složitost tohoto algoritmu pro n prvků. Odvození není požadováno.

4 Procesory

1. Vysvětlete princip zřetězeného zpracování instrukcí procesorem. Kvantifikujte zhruba režii při zpoždění (pipeline stall) ve zřetězeném zpracování instrukcí. Jaké zrychlení lze očekávat při zřetězeném zpracování, pokud zpracování každé instrukce má k kroků ?
2. Vysvětlete důvod přítomnosti cache obsahu paměti v architektuře procesoru. Kvantifikujte zhruba režii při výpadku (cache miss) v přístupu k obsahu paměti. Vysvětlete pojmy „přímo mapovaná cache“ a „množinově asociativní cache“.

5 Stránkování

Uvažujte architekturu s podporou stránkování a délkou virtuální a fyzické adresy 32 bitů. Stránky mají velikost 4 kB, k překladu adres je použita dvouúrovňová stránkovací tabulka. Stránkovací tabulka první úrovně a stránkovací tabulka druhé úrovně mají stejný počet položek.

1. Nakreslete část obsahu stránkovací tabulky nutnou pro překlad virtuální adresy 123456_{16} na fyzickou adresu 123456_{16}.
2. Jaká je nejmenší nutná velikost stránkovacích tabulek, pokud je potřeba namapovat pouze tuto jedinou adresu a proč ? Velikosti uvádějte v počtu položek stránkovacích tabulek.
3. Které z následujících datových typů není vhodné na uvedenou virtuální adresu ukládat a proč ?

```
unsigned char
int32_t
int64_t
char [4096]
```

6 Synchronizace

1. Uvažujte třídu implementující semafor s následující signaturou:

   ```
   class Semaphore
   {
     Semaphore (int);
     void up ();
     void down ();
   };
   ```

   Popište sémantiku jednotlivých metod.

2. Máte k dispozici implementaci čítače:

   ```
   class Counter
   {
     private int value = 0;
     public int read () { return (value); };
     public void increment () { value ++; };
   };
   ```

   S použitím semaforu upravte implementaci tak, aby správně fungovala při současném volání z více vláken.

3. Diskutujte chování vámi upravené implementace při současném volání metody read z více vláken.

7 Transakce

1. Definujte pojem „transakce“ a vysvětlete vlastnosti ACID (atomicity, consistency, isolation, durability).
2. Uvažujte transakce T1: $R(X)R(Y)W(X)$ a T2: $R(X)R(Y)W(Y)$. Je rozvrh $R_1(X)R_2(X)R_1(Y)R_2(Y)W_1(X)W_2(Y)$ serializovatelný a proč ?

8 XSLT

1. Krátce popište princip fungování XSLT procesoru při zpracování XSLT skriptu.
2. Co vrátí prázdný XSLT skript a proč ?
3. Co bude výsledkem aplikace následujícího XSLT skriptu na XML dokument se seznamem zaměstnanců, z nichž každý má jako atribut rodné číslo a jako vnořené elementy jméno a příjmení ?

   ```
   <xsl:stylesheet>
     <xsl:template match="zamestnanec">
       <xsl:value-of select="@rodnecislo" />
       <xsl:apply-templates />
     </xsl:template>
   </xsl:stylesheet>
   ```

9 Predikátová logika

1. Zformulujte větu o kompaktnosti predikátové logiky. Uveďte hlavní body jejího důkazu.

10 Návrhové vzory

1. Vysvětlete, co to je návrhový vzor (design pattern). Jaké jsou základní součásti popisu návrhového vzoru ?
2. Vyberte si některý ze vzorů Visitor, Abstract Factory, Model-View-Controller a stručně jej popište.

11 Šablony a generika

```
template <class A> class B
{
  public:
    void f (A a) { ... }
}
```

```
public class B<A>
{
  public void f (A a) { ... }
}
```

1. Uvedené fragmenty kódu ilustrují šablony a generika. Vysvětlete, jaké typy uvedené fragmenty kódu definují.
2. Ilustrujte použití šablon nebo generik na definici rozhraní třídy, která implementuje FIFO frontu s metodami vložení posledního a vyjmutí prvního prvku.

12 DNS

1. Stručně popište princip překladu doménového jména na IP adresu systémem DNS.
2. Vysvětlete rozdíl mezi autoritativními a neautoritativními DNS servery. Co je primární a sekundární DNS server ?
3. Co jsou kořenové DNS servery a jak se předchází jejich přetížení ? Jak je v systému DNS zajištěna aktuálnost překladů ?

13 Rozklad polynomů

1. Definujte pojem „ireducibilní polynom“.
2. Ukažte, že každý polynom stupně alespoň 1 má jednoznačný rozklad na součin ireducibilních polynomů.
3. Najděte rozklad polynomu $x^3 + x$ na ireducibilní polynomy v $R[x]$.
4. Najděte rozklad polynomu $x^3 + x$ na ireducibilní polynomy v $C[x]$.

14 Derivace, Newtonova metoda

1. Definujte pojem „derivace funkce“.
2. Zjistěte, na kterých intervalech je funkce xe^{-x^2} rostoucí a klesající.
3. Popište Newtonovu metodu hledání nulového bodu funkce.

15 Primitivní funkce

1. Definujte pojem „primitivní funkce“.
2. Vyslovte větu o výpočtu primitivní funkce metodou per partes.
3. Najděte primitivní funkci k $x \sin(x)$.

16 Determinant

1. Definujte pojem „determinant“.
2. Dokažte, že $\det A = \det A^T$.
3. Jaký je vztah determinantu matice A a k ní inverzní matice A^{-1} ?

17 Soustavy lineárních rovnic

1. Dokažte, že elementární úpravy používané v Gausově eliminační metodě nemění řešení soustavy.
2. Spočítejte Gausovou eliminační metodou řešení soustavy dané touto rozšířenou maticí:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 4 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

18 Metrické prostory

1. Definujte pojmy „metrika“ a „metrický prostor“. Doplňte příklad metrického prostoru nad R^n s jinou než eukleidovskou metrikou.
2. Rozhodněte o následujících množinách, zda jsou otevřené a zda jsou uzavřené v metrickém prostoru reálných čísel s eukleidovskou metrikou. O jedné z těchto množin vaše tvrzení dokažte.
   - $\langle 0, 1 \rangle$
   - $(0, \infty)$
   - $(-\infty, \infty)$

19 Nezávislost jevů

1. Pravděpodobnost jevu A je $P(A)$, pravděpodobnost jevu B je $P(B)$. Vyjádřete pravděpodobnost $P(A \cap B)$ současného výskytu A a B, pokud víte, že A a B jsou nezávislé.
2. Rozšiřte předchozí vyjádření pro případ, kdy A a B jsou závislé. Stačí v tomto případě k vyjádření $P(A \cap B)$ znalost $P(A)$ a $P(B)$?
3. V experimentu se hází dvěma kostkami. Pro která $n \in \{2...12\}$ je jev „součet hodů obou kostek je n“ závislý na jevu „hod první kostky je 1“ ?

20 Základní pojmy teorie grafů

1. Definujte úplný graf K_n a úplný bipartitní graf $K_{m,n}$.
2. Pro jaká $m, n \in N$ je $K_{m,n}$ cestou ?
3. Pro jaká $n \in N$ je K_n rovinný ?
4. Pro jaká $m, n \in N$ je $K_{m,n}$ rovinný ?

   Odpovědi zdůvodněte.