8100310 Tietorakenteet ja algoritmit
Tentti 6. toukokuuta 2004
Henri Hansen

Kirjoita nimesi ja opiskelijanumerosi konseptipaperin vasempaan yläkulmaan. Jos olet korottamassa aiempaa arvosanaa, merkitse se kaikkiin konsepteihin. Jos olet suorittanut harjoitustyöt muulloin kuin vuoden 2004 keväällä, merkitse mukaan suoritusvuosi. Jos olet korottamassa, merkitse sekin paperiin. Vastaa **viiteen** kysymysryhmään. **HUOM: kaikki ryhmät eivät ole samanarvoisia, arvokkaammat ovat vaikeampia.**

1 Matriisien kertolasku ketjussa (6p)

Tehtävänä on laskea matriisitulo $A_1 A_2 \cdots A_n$. Matriisit ovat eri kokoisia. Oletetaan siis, että yksittäinen matriisien kertolasku lasketaan ns. alakoulualgoritmilla. Lisäksi oletetaan, että matriisien dimensiot ovat sopivat, siis että tulo $A_i A_{i+1}$ on aina hyvin määritelty.

Tiedetään, että $n \times m$-matriisin ja $m \times k$-matriisin tulon laskemiseksi tarvitaan $n \cdot m \cdot k$ kertolaskua ja tulos on $n \times k$ matriisi.

Esitä algoritmi, joka selvittää, mikä on annetun matriisiketjun optimaalinen laskujärjestys. (6p)

Opa: Esitä ensin ratkaisu rekursioyhtälön avulla ja siitä sitten, niinkuin on opetettu.

2 Analysointitehtävä (6p)

Tässä tehtävässä x mod y palauttaa x:n jakojäännöksen y:n suhteen.

Olkoon meillä algoritmi:

```
MODULAR EXP(a, b, n)
 c := 1
 d := 1
 olkoon ⟨b_k, b_{k-1}, ..., b_0⟩ b:n binaariesitys
 for i := k downto 0 do
    c := 2c
    d := d^2 mod n
    if b_i = 1 then
       c := c + 1
       d := d * a mod n
    endif
 endfor
 return d
```

Kyseinen algoritmi laskee, mitä on a^b mod n ja palauttaa sen. Palauta mieleesi *binääripotenssin* algoritmi. Sen oikeaksiosoittamisessa käytettiin invarianttia, jota hivenen muokkaamalla myös tämän algoritmin oikeaksiosoittaminen on helppoa. *Huom:* Muuttujan c arvoa ei käytetä d:n laskemiseen ja invarianttina sen arvo on sama kuin binääriluvun $\langle b_k, \ldots, b_{i+1} \rangle$.

a. Löydä muuttujia a, d, c ja n koskeva invariantti, joka annetun muuttujia c ja b koskevan invariantin kanssa takaa, että algoritmi on oikea ja perustele miksi se takaa oikeellisuuden. (3p)

b. Osoita invariantti oikeaksi invariantiksi. (3p)