Algoritminen matematiikka

Tentti 19.8.2016 (3h)

1. (a) Määrittele merkinnät $\mathcal{O}(g(n))$ ja $\Theta(g(n))$.
   (b) Kuuluuko funktio $\sum_{i=1}^{n} f(i)$ luokkaan $\mathcal{O}(f(n))$, kun
      i. $f(n) = 2^n$.
      ii. $f(n) = \log(n)$

2. (a) Tarkastellaan logaritmi-probleemaa, jossa syötteenä on luonnollinen luku a.
      i. Esitä algoritmi ja perustele sen kompleksisuus kun pitää laskea $\lfloor \log_k a \rfloor$, missä k on kiinnitetty kantaluku.
      ii. Olkoon $0 < a, b < m$. Mitä voidaan sanoa ongelman ratkaisevista algoritmeista tai niiden kompleksisuudesta kun pitää laskea $\log_b a \pmod m$ eli etsitään lukua $c \in \mathbb{Z}_m$, jolle $b^c \equiv a \pmod m$?
   (b) Esitä ehdollisen kompleksisuuden lemman todistus: Osoita, että jos $p \geq 2$ on kokonaisluku ja $g(n)$ on p-sileä sekä $f(n)$ on lopulta ei–vähenevä, niin silloin

$$f(n) = \mathcal{O}\big(g(n)\,;\, n \text{ on } p\text{:n potenssi}\big) \implies f(n) = \mathcal{O}\big(g(n)\big).$$

3. (a) Mikä on diskreetti Fourier-muunnos?
   (b) Perustele miten polynomien kertolasku voidaan laskea ajassa $\mathcal{O}(n \log n)$?

4. (a) Miten Las Vegas ja Monte Carlo -algoritmit eroavat toisistaan?
   (b) Esitä Miller-Rabinin alkulukutestin toimintaperiaate. Mikä on Miller-Rabinin testin kompleksisuus? Entä virhetodennäköisyys?