Tietojenkäsittelyteoria, kevät 2000
Harjoitus 8, to 16.3. klo 10–12 sali MaD381

1. Sanotaan, että Monte Carlo -tyyppinen satunnaisalgoritmi A on *luotettava*, jos se annetulla syötteellä antaa oikean vastauksen todennäköisyydellä $p > 0$, ja todennäköisyydellä $q = 1 - p$ vastaa "en tiedä". Mikä on oikean vastauksen todennäköisyys, kun algoritmi A suoritetaan k kertaa peräkkäin? (Oletetaan, että suorituskerrat ovat toisistaan riippumattomia, ja toisto lopetetaan heti kun oikea vastaus on saatu.) Montako kertaa algoritmia tarvitsee enintään toistaa, jotta oikean vastauksen todennäköisyys saataisiin suuremmaksi kuin $1 - \epsilon$, jollakin annetulla $\epsilon > 0$?

2. Muodostetaan edellisen tehtävän algoritmin A pohjalta Las Vegas -tyyppinen algoritmi B, joka toistaa A:ta, kunnes saa oikean vastauksen (so. A vastaa jotakin muuta kuin "en tiedä"). Mikä on tarvittavien toistojen määrän odotusarvo?

3. Olkoon A jonkin päätösongelman ratkaiseva (so. 0/1-arvoinen) Monte Carlo -algoritmi, joka antaa oikean vastauksen todennäköisyydellä $p > 1/2$ ja väärän vastauksen todennäköisyydellä $q = 1 - p$. (Tällä kertaa algoritmi ei siis vastaa luotettavasti "en tiedä", vaan saattaa suorastaan valehdella.) Muodostetaan algoritmista A algoritmi B, joka toistaa A:ta $k = 2t - 1$ kertaa ja valitsee vastaukseksi sen, jonka A antoi useammin, so. vähintään t kertaa. Arvioi todennäköisyyttä, että B antaa väärän vastauksen, kun A:n eri suorituskerrat ovat toisistaan riippumattomia. Erityisesti: monellako A:n toistolla saadaan väärän vastauksen todennäköisyys pienemmäksi kuin jokin annettu $\epsilon > 0$?

4. Todista seuraavat hyppylistojen ominaisuudet:

   (a) n alkion hyppylistan alkioiden maksimikorkeus on "suurella todennäköisyydellä" enintään $2 \log_2 n$.

   (b) Kahden korkeutta h olevan alkion välissä on odotusarvoisesti $O(1)$ korkeutta $h - 1$ olevaa alkiota. (*Vihje:* Huomaa, että jos alkion x korkeus on vähintään $h - 1$, niin todennäköisyydellä $1/2$ sen korkeus on itse asiassa h tai suurempi.)

5. Todista binomijakauman "alahäntää" koskeva Chernoffin raja: kun $S \sim \mathrm{Bin}(n, p)$ ja $r \geq 0$, niin
$$Pr(S \leq np - r) \leq e^{-r^2/2np}.$$

6. Lausekalkyylin kaava φ on *disjunktiivisessa normaalimuodossa (dnf)*, jos se on muotoa
$$\varphi = \varphi_1 \vee \ldots \vee \varphi_m,$$
missä kukin termi φ_i on literaalien konjunktio
$$\varphi_i = \tilde{x}_{i1} \wedge \ldots \wedge \tilde{x}_{ir_i}.$$
(Tässä siis kukin $\tilde{x}_{ij}$ on joko muuttuja tai sellaisen negaatio.) Laadi satunnaisalgoritmi, joka arvioi monellako muuttujien totuusarvoasetuksella annettu dnf-muotoinen kaava φ tulee todeksi. (*Vihje:* Kukin kaavan termi φ_i määrittelee tietyn toteuttavien totuusarvoasetusten joukon S_i, ja koko kaavan φ toteuttavien asetusten joukko on näiden S_i-joukkojen yhdiste.) *Lisätieto:* Toteuttavien asetusten tarkan määrän laskeminen on ns. #P-täydellinen ongelma, siis luultavasti ei tehtävissä polynomisessa ajassa. (Funktio $f : \Sigma^* \to \mathrm{N}$ kuuluu luokkaan #P, jos jollakin epädeterministisellä polynomisessa ajassa toimivalla Turingin koneella M on $f(x) = M$:n syötteellä x hyväksyvien laskentojen määrä.)