**MAT340 Tietojenkäsittelyteoria (5 ov)**
2. välikoe (kotikoe), 20.4.2000
Kuulustelija: Pekka Orponen

Tehtävien ratkaisemisen apuna saa käyttää mitä tahansa lähdemateriaalia; ratkaisut tulee kuitenkin laatia henkilökohtaisesti. Vastaukset palautetaan kuulustelijalle henkilökohtaisesti tai suljetussa kirjekuoressa huoneen MaD307 viereiseen postilaatikkoon *tiistaihin 9.5. klo 14 mennessä.*

1. Tarkastellaan Boolen funktioiden laskemista *kynnysporttien* (engl. threshold gate, perceptron) avulla. Kynnysfunktio $T_k^n : \{0,1\}^n \to \{0,1\}$ määritellään:

$$T_k^n(x_1, \ldots, x_n) = 1 \quad \text{joss vähintään } k \text{ kpl syötteistä } x_1, \ldots, x_n \text{ on } 1.$$

   *Kynnyspiiri* (engl. threshold circuit, multilayer perceptron) on kombinaatiopiiri, jonka portteina voi olla mielivaltaisia kynnysfunktioita $T_k^m$, $0 \leq k \leq m$. Todista seuraavat tulokset:

   (a) Jos syötteinä on käytettävissä sekä muuttujat $x_1, \ldots, x_n$ että niiden negaatiot $\bar{x}_1, \ldots, \bar{x}_n$, niin mikä tahansa muuttujien $x_1, \ldots, x_n$ monomi (literaalien konjunktio) voidaan laskea yhdellä kynnysportilla $T_k^m$, $0 \leq k \leq m \leq n$.

   (b) Mikä tahansa $n$ muuttujan Boolen funktio $f$ voidaan laskea $O(2^{n/2})$-porttisella kynnyspiirillä. (*Vihje:* Laske ensin kaikki muuttujien $x_1, \ldots, x_{\lfloor n/2 \rfloor}$ monomit. Tarkastele sitten funktion $f$ dnf-esitystä ja eri monomien esiintymistä siinä.)

   (c) Melkein kaikkien $n$ muuttujan Boolen funktioiden laskeminen kynnyspiireillä vaatii $\Omega(2^{n/2})$ porttia. (Vrt. Shannonin lause; täsmennä itse, mitä "melkein kaikki" tarkoittaa tässä yhteydessä.)

2. Olkoon $G = (V, E)$ tasaisen kaarijakauman mukaan generoitu $n$ solmun satunnaisverkko, so. $V = \{1, \ldots, n\}$, $\Pr(\{i, j\} \in E) = 1/2$ riippumattomasti kaikilla $i, j \in V$, $i \neq j$. Todista Kolmogorov-kompleksisuutta käyttäen mahdollisimman tiukka "suuren todennäköisyyden" yläraja verkon $G$ maksimaalisen klikin koolle.

3. Tarkastellaan seuraavaa vuorovaikutteisten todistussysteemien yleistystä. Kieli $L$ kuuluu luokkaan MIP$[k]$, $k \geq 0$, jos sillä on polynomisessa ajassa toimivan probabilistisen varmentajakoneen $V$ ja $k$ toisistaan riippumattoman todistusoraakkelin $P_1, \ldots, P_k$ muodostama *monitodistusjärjestelmä* (engl. multiprover interactive proof system), joka kaikilla $x \in \Sigma^*$ täyttää ehdot:

$$x \in L \quad \Rightarrow \quad \exists (P_1^*, \ldots, P_k^*) : \Pr((V, P_1^*, \ldots, P_k^*) \text{ hyväksyy } x\text{:n}) \geq 2/3,$$
$$x \notin L \quad \Rightarrow \quad \forall (P_1, \ldots, P_k) : \Pr((V, P_1, \ldots, P_k) \text{ hyväksyy } x\text{:n}) \leq 1/3.$$

KÄÄNNÄ

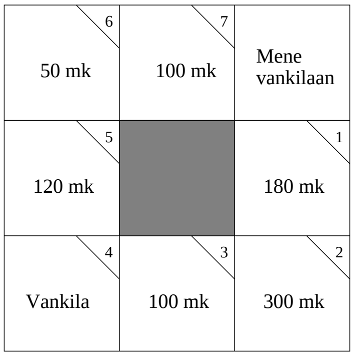
Näillä merkinnöillä on siis MIP[0] = BPP ja MIP[1] = IP = PSPACE. Merkitään edelleen $\mathrm{MIP} = \bigcup_{k\geq 0} \mathrm{MIP}[k]$. Todista seuraavat luokkien MIP ja PCP = PCP(poly, poly) suhdetta koskevat väitteet:

(a) MIP ⊆ PCP. (*Ohje:* Oraakkelien määrän lisäksi MIP- ja PCP-systeemeillä on se ero, että MIP-oraakkelit voivat "muistaa" aiemmat vastauksensa ja mukauttaa myöhemmän toimintansa niiden mukaan, kun taas PCP-oraakkelin vastaukset on kiinnitetty ennalta. Tämän tehtävän ideana on siis suunnitella koodaus, jolla $k$ adaptiivisen oraakkelin kysymys/vastausjonot voidaan koodata yhteen kiinteään oraakkeliin.)

(b) PCP ⊆ MIP[2]. (*Vihje:* Käytä toista MIP-oraakkelia PCP-oraakkelin koodaukseen ja toista oraakkelia sen varmistamiseen, että ensimmäinen oraakkeli ei muuttele vastauksiaan.)

*Lisätieto:* Edellisten tulosten nojalla on siis MIP = MIP[2] = PCP. Edelleen voidaan osoittaa (Babai, Fortnow, Lund 1991), että itse asiassa on MIP = NEXP.

4. Tarkastellaan oheisen kuvan esittämällä laudalla pelattavaa yksinkertaistettua Monopolipeliä:




Peliä pelataan noppien sijaan rahaa heittämällä siten, että kun rahanheiton tulos on "kruuna", pelaaja siirtyy yhden ruudun eteenpäin, ja kun tulos on klaava, hän siirtyy kaksi ruutua eteenpäin. Mallinna peli Markovin ketjuna ja määritä pelaajan eri ruuduille sijoittumistodennäköisyyksien tasapainojakauma äärettömän pitkässä pelissä. Määritä tämän jakauman ja lautaan merkittyjen eri ruutujen "vuokrien" perusteella, mikä on laudan paras ruutu (so. se, josta vastapelaaja pitkän ajan kuluessa joutuu odotusarvoisesti maksamaan eniten vuokraa).