Tietojenkäsittelyteoria, kevät 2000
Harjoitus 10, to 30.3. klo 10–12 sali MaD381

1. Esitä Lucasin testiin (luentojen s. 8.20) perustuva "NP-todistuspuu", joka vahvistaa että 11 on alkuluku.

2. [Siirtynyt harjoituksista 9.] Osoita, että jos NP $\subseteq$ BPP, niin NP $=$ R. (*Vihje:* SATin totuusarvoasetuksen oikeellisuuden voi tarkastaa.)

3. Sanotaan, että kieli A kuuluu luokkaan BPNP (kirjallisuudessa käytetään myös merkintää AM), jos on olemassa kieli $B \in NP$ ja polynomi $p(n)$, joilla:

   (i) jos $x \in A$, niin $\Pr_{|y|=p(|x|)}(\langle x, y\rangle \in B) \geq 2/3$;
   (ii) jos $x \notin A$, niin $\Pr_{|y|=p(|x|)}(\langle x, y\rangle \in B) \leq 1/3$.

   Osoita, että BPNP $\subseteq \Pi_2^p$. *Ohje:* Totea ensin, luentojen Lauseen 8.10 tapaan, että virhetodennäköisyys 1/3 voidaan pienentää luokkaan $2^{-q(n)}$, millä tahansa polynomilla $q(n)$. Seuraa sitten luentojen Lauseen 8.13 todistusta, käyttäen seuraavaa kielen A karakterisointia "ison" kielen B avulla:

   $$x \in A \iff (\forall\langle u_1, \ldots, u_{p(n)}\rangle, |u_i| = p(n))(\exists v, |v| = p(n))(\bigwedge_{i=1}^{p(n)} \langle x, v \oplus u_i\rangle \in B).$$

4. [Jatkoa edelliseen.] Osoita, että jos co-NP $\subseteq$ BPNP, niin PH $\subseteq$ BPNP. Päättele tästä, että jos verkkoisomorfiaongelma (kieli GISO) on NP-täydellinen, niin PH $= \Pi_2^p$.

5. Jäljittele kielen QBF vuorovaikutteista todistusprotokollaa, jolla

   (a) todistaja P vakuuttaa varmentajan V väitteen $\forall x \exists y((x \wedge y) \vee (\bar{x} \wedge \bar{y}))$ totuudesta;
   (b) todistaja P yrittää vakuuttaa varmentajan V väitteen $\exists y \forall x((x \wedge y) \vee (\bar{x} \wedge \bar{y}))$ totuudesta, mutta epäonnistuu.