Sada domácich úloh #4

1. Na prednáške sme si ukázali, že ak existujú ťažké funkcie, vieme z nich vytvoriť dobrý pseudonáhodný generátor. Ukážte, že to platí aj naopak – ak existuje dobrý PNG, tak E obsahuje ťažké funkcie. Presnejšie, dokážte, že ak existuje $S(\ell)$-PNG, tak existuje $f \in \mathsf{E}$ taká, že $\mathsf{H}_{\text{wrs}}(f)(n) \geq S(n)$. (Hint: Pre PNG G so seedom dĺžky ℓ vezmime len prvých $\ell + 1$ bitov; zistiť, či takýto reťazec G vygeneruje je ťažké; formálne: pre $|x| = \ell + 1$ nech $f(x) = 1$, ak $\exists z \in \{0,1\}^{\ell} : x$ je prefix $G(z)$.)

2. Dokážte, že $\mathsf{P}^{\mathsf{PP}} = \mathsf{P}^{\#\mathsf{P}}$ a teda $\mathsf{PH} \subseteq \mathsf{P}^{\mathsf{PP}}$. Pripomeňme, že PP je trieda jazykov, ktoré majú pravdepodobnostný polynomiálny algoritmus, ktorý slová v jazyku akceptuje pre aspoň polovicu hodov mincou. Inými slovami, existuje TS M bežiaci v polynomiálnom čase a polynóm p také, že

   $$x \in L \iff \Pr_r[M(x,r)] \geq \tfrac{1}{2} \iff \#\{r \in \{0,1\}^{p(|x|)} : M(x,r)\} \geq \tfrac{1}{2} \cdot 2^{p(|x|)}.$$

   (Na rozdiel od BPP, kde je pravdepodobnosť pre $x \in L \geq \frac{2}{3}$ a pre $x \notin L \leq \frac{1}{3}$, pri PP je to $\geq \frac{1}{2}$ vs. $< \frac{1}{2}$.)

3. AM je trieda jazykov, pre ktoré existuje deterministický TS V, bežiaci v polynomiálnom čase od x taký, že

   - ak $x \in L$, tak $\Pr_r[\exists \pi : V(x,r,\pi) = 1] \geq 2/3$ a
   - ak $x \notin L$, tak $\Pr_r[\exists \pi : V(x,r,\pi) = 1] \leq 1/3$

   (r a π sú polynomiálne dlhé).

   Takéto systémy sa volajú „Artur–Merlinove hry“: Merlin je múdry čarodejník, ktorý dokáže vyriešiť akýkoľvek ťažký problém, ale nie vždy sa mu dá veriť. Ak chce Artur zistiť, či vstup x patrí do jazyka $L \in \mathsf{AM}$,

   - hodí si mincou a vygeneruje náhodný reťazec r (polynomiálnej dĺžky) a ukáže ho Merlinovi;
   - Merlin mu prezradí dôkaz π_r pre tieto hody;
   - Artur skontroluje dôkaz π_r (ale už nehádže mincou).

   $L \in \mathsf{AM}$, ak pre $x \in L$ vo väčšine prípadov Merlin Artura presvedčí a pre $x \notin L$ Artur väčšinu dôkazov odmietne (aj keby ho chcel Merlin oklamať).

   Zjavne $\mathsf{NP} \subseteq \mathsf{AM}$. Dokážte, že $\mathsf{AM} \subseteq \mathsf{NP/poly}$, kde $\mathsf{NP/poly}$ môžeme definovať buď ako jazyky akceptované nedeterministickým TS s polynomiálnou radou v polynomiálnom čase, alebo ako jazyky, pre ktoré existuje polynomiálne dlhý certifikát, ktorý sa dá overiť neuniformným obvodom polynomiálnej veľkosti.

Bonus. (2 body) Dokážte, že ak $\overline{\text{3SAT}} \in \mathsf{AM}$ (t.j. ak doplnok k problému 3SAT patrí do triedy AM definovanej v predošlej úlohe), tak polynomiálna hierarchia skolabuje na 3. stupeň: $\mathsf{PH} = \Sigma_3^{\mathsf{P}}$. (Kvôli tomu neveríme, že by AM obsahovalo coNP, respektíve neveríme, že existuje randomizovaná redukcia $\overline{\text{3SAT}} \leq_r \text{3SAT}$.)