TIN 086 Vybrané kapitoly z výpočetní složitosti II **léto 2009/2010**

3. domácí úlohy

do zkoušky

Úloha 1. Dokažte, že každý jazyk, který má pravděpodobnostní důkazový systém (PCP) s ověřovatelem používajícím $r(n)$ náhodných bitů a čtoucím $q(n)$ pozic důkazu, má také PCP systém s ověřovatelem používajícím $r(n)$ náhodných bitů a čtoucím neadaptivně $2^{q(n)}$ pozic důkazu. Neadaptivně znamená, že pozice důkazu, které čte, nezávisí na tom, co z důkazu přečetl doposud.

Úloha 2. Ukažte, že PCP$(0, \log n)$ =P. Připomeňte si, že PCP$(0, poly(n))$ =NP.

Úloha 3. Množina vektorů $C \subseteq GF[2]^n$, kde $GF[2]$ je dvouprvkové těleso, se nazývá *lineární samoopravný kód schopný opravit t chyb*, pokud pro každé $u, v \in C$, $u + v \in C$ a různé vektory u a v se liší alespoň v $2t + 1$ pozicích. Vysvětlete tento název. Co lze říci o počtu jedniček ve vektorech v C.

Úloha 4. Ukažte, že pro všechna $1 \leq k \leq n/2$

$$\frac{2^{H(k/n)n}}{n+1} \leq \sum_{i=0}^{k} \binom{n}{i} \leq 2^{H(k/n)n}$$

kde pro $0 < x < 1$ je $H(x) = -x \log_2 x - (1-x)\log_2(1-x)$. *Hint:* Použijte binomickou větu na $\left(\frac{k}{n} + \frac{n-k}{n}\right)^n$.

Úloha 5. Vezměme si celá čísla $0 < r < n$ a konstantu $0 < \epsilon < 1/2$. Vyberme uniformě náhodně r vektorů $u_1, u_2, \ldots, u_r$ z $GF[2]^n$.

a) Jaká je pravděpodobnost, že $u_1, \ldots, u_r$ jsou lineárně nezávislé?

b) Jaká je pravděpodobnost, že vektor, jež je lineární kombinací vektorů $u_1, \ldots, u_r$ danou pevně zvolenými koeficienty $a_1, \ldots, a_k \in GF[2]$, obsahuje méně než ϵn jedniček.

c) Jaká je pravděpodobnost, že žádná z lineárních kombinací vektorů $u_1, \ldots, u_r$ neobsahuje méně než ϵn jedniček.

d) Pro jakou volbu r a ϵ, kde oba parametry jsou co možná největší, existují vektory $u_1, u_2, \ldots, u_r \in GF[2]^n$ takové, že generují vektorový prostor dimenze r a žádný z vektorů v tomto prostoru neobsahuje méně než ϵn jeniček. O jaký se jedná kód?