TIN 085 - Vybrané kapitoly z výpočetní složitosti I **zima 2006/2007**

1. domácí úlohy - opakování

do 24. října 2006

1. Bez použití Černovovy nerovnosti ukažte, jak se dá snížit chyba algoritmu z $1/3$ na 2^{-n}. (Hint: Snižte chybu nejprve na $1/4$ a pak použijte standartní kalkulaci.)

2. Nechť M je náhodná matice vzatá z uniformního rozdělení matic $n \times n$ nad tělesem $GF[2]$. Jaká je pravděpodobnost, že M je regulární (invertibilní)? Uveďte přesnou formuli a rozumné odhady na tuto pravděpodobnost pro $n \to \infty$. Udělejte to samé pro matice nad $GF[p]$. Co se děje s danou pravděpodobností, když $p \to \infty$?

3. Vezměme si celá čísla $0 < r < n$ a vyberme uniformě náhodně r vektorů $u_1, u_2, \ldots, u_r$ z $GF[2]^n = \{0,1\}^n$.

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

   (b) Označme písmenem B_ϵ množinu nenulových vektorů, jež jsou lineární kombinací $u_1, \ldots, u_r$ a jež mají Hammingovu váhu méně než ϵn, kde $0 < \epsilon < 1/2$ je zvolená konstanta. Jaká je očekávaná velikost množiny B_ϵ? (Hammingova váha je počet jedniček ve vektoru.)

   (Povšimněte si, že pokud všechny nenulové lineární kombinace vektorů u_i mají Hammingovu váhu větší nebo rovnu ϵn, tj. $B_\epsilon = \emptyset$, pak tyto vektory (lineární kombinace) tvoří *samoopravný kód* se vzdáleností ϵn, to jest kód schopný opravit $(\epsilon n - 1)/2$ chyb. Takový kód existuje pokud $r < (1 - H(\epsilon))n$, kde $H(\epsilon) = -\epsilon \log \epsilon - (1-\epsilon)\log(1-\epsilon)$. Rozmyslete si proč.)

4. Cílem tohoto cvičení je zopakovat, jak se konstruují konečná (komutativní) tělesa. Připomeňme si *Euklidův algoritmus*, pro hledání největšího společného dělitele dvou celých čísel a a b. Vstupem algoritmu je $a > b > 0$. Algoritmus definuje posloupnost $a_0, a_1, \ldots$ takto:

   - $a_0 = a$, $a_1 = b$ a
   - pro $i = 2, 3, \ldots$ nechť $a_i = a_{i-2} \bmod a_{i-1}$.

   Nechť t je nejmenší takové, že $a_t = 0$. Výstupem algoritmu je a_{t-1}.

   (a) Dokažte korektnost Euklidova algoritmu, to jest, že t je dobře definované a že výstupem je největší společný dělitel a a b.

   (b) Ukažte, že když $nsd(a,b) = c$, pak existují celá čísla x a y takové, že $|x| \leq b$, $|y| \leq a$ a $ax + by = c$.

   (c) Ukažte, že pro prvočíslo p, $GF[p] = \{0, 1, \ldots, p-1\}$ s počítáním modulo p je těleso. (Tedy především ukažte, že $GF[p]^* = GF[p] \setminus \{0\}$ tvoří grupu při násobení modulo p.)

   (d) Nechť F je konečné těleso a $F_n[x] = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}; a_0, a_1, \ldots, a_{n-1} \in F\}$ jsou polynomy nad F stupně nejvýše $n-1$. Nechť $r(x)$ je ireducibilní polynom stupně n. Ukažte, že $F_n[x]$ s počítáním modulo $r(x)$ je těleso. (Hint: Ukažte, že Euklidův algoritmus funguje i pro polynomy. Polynom je ireducibilní, když nelze zapsat jako součin jiných dvou.)