TIN 085 - Vybrané kapitoly z výpočetní složitosti I **zima 2007/2008**

2. domácí úlohy

do 15. listopadu 2007

1. Uvažujme následující variantu Reed-Solomových kódů. Nechť $\alpha_{1,}, \alpha_2, \ldots, \alpha_n \in GF[q]$ jsou pevně zvolená. Pro zprávu $m = m_1 m_2 \cdots m_k \in GF[q]$ definujme polynom $p_m(x)$ jako

   (a) $p_m(x) = \sum_{i=1}^{k} m_{i-1} x^{i+\ell}$, kde ℓ je pevně zvolené přirozené číslo,

   (b) $p_m(x) = \sum_{i=1}^{k} m_{i-1} x^{2i}$,

   a kódem pro m je pak jako obvykle $[p_m(\alpha_1), p_m(\alpha_2), \ldots, p_m(\alpha_n)]$. Jaký kód dostane v případě a) a b)? Uveďte jeho parametry.

2. Zaveďme si následující *editovací vzdálenost*: slovo x má vzdálenost od slova y nejvýše d, pokud lze x z y získat tím, že nejprve nejvýše d symbolů z y vypustíme a poté tam až d symbolů libovolně přidáme. Vzdáleností x od y je pak nejmenší d takové, že x má od y vzdálenost nejvýše d.

   (a) Je editovací vzdálenost metrika? (Tedy splňuje symetričnost a trojúhelníkovou nerovnost?)

   Přirozeným způsobem můžeme zadefinovat samoopravné kódy pro editovací vzdálenost. (Řekneme, že kód $C \subseteq \Sigma^*$ opravuje d_n editovacích chyb, když pro každé $x \in C$ délky n, žádné slovo v C nemá editovací vzdálenost od x menší než d_n.)

   (a) Existují takové kódy s konstantní relativní vzdáleností a konstantním *ratem*? Pokud ano, tak nějaký navrhněte.

   (b) Jaký je ekvivalent objemové (Hammingovy) meze pro velikost takových binárních kódů a jaký pro Gilbert-Varshamovu mez.

3. 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.)

4. Nechť p a k jsou kladná celá čísla, kde p je prvočíslo. Ukažte, že pro každé $\alpha \in GF[p^k]$ existuje matice $M_\alpha \in GF[p]^{k \times k}$ taková, že pro všechna $\beta \in GF[p^k]$, když $\overline{\alpha}$ a $\overline{\beta}$ je přirozená vyjádření α a β jako vektory v $GF[p]^k$, pak $\overline{\beta} \cdot M_\alpha$ je vyjádření $\alpha \cdot \beta$ v $GF[p]^k$. Dále ukažte, že pro každé $\alpha \in GF[p^k]$ tvoří množina dvojic $\{[\overline{x}, \overline{x \cdot \alpha}]; \quad x \in GF[p^k]\}$ vektorový podprostor prostoru $GF[p]^{2k}$.