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

2. domácí úlohy

Vzorové řešení

13.prosinec 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) $p_m(x) = \sum_{i=1}^{k} m_i x^{i+\ell}$, kde ℓ je pevně zvolené přirozené číslo,

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

   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.

   Řešení:

   (a) Snadno nahlédneme, že daný kód bude opět lineární, takže se bude jednat o kód $[n, k, d]_q$. Jediné, co zbývá určit je d. Jelikož kód je lineární, stačí zjistit maximální možný počet nul ve vektoru $[p_m(\alpha_1), p_m(\alpha_2), \ldots, p_m(\alpha_n)]$. Jelikož $p_m(x) = \sum_{i=1}^{k} m_i x^{i+\ell} = x^{\ell+1} \sum_{i=1}^{k} m_i x^{i-1}$, $p_m(x)$ má nejvýše $k-1$ nenulových kořenů. (0 je nejméně $l+1$ násobný kořen.) Tudíž pokud $\alpha_1, , \alpha_2, \ldots, \alpha_n$ jsou nenulové, pak $d = n - k + 1$, pokud některé z $\alpha_1, , \alpha_2, \ldots, \alpha_n$ je rovno nule, pak $d = n - k$.

   (b) Podobně jako v (a) se jedná o lineární kód $[n, k, d]_q$. Počet nul v $[p_m(\alpha_1), p_m(\alpha_2), \ldots, p_m(\alpha_n)]$ zavisí na volbě $\alpha_{1,}, \alpha_2, \ldots, \alpha_n$. Pokud α_i je kořen polynomu $p_m(x)$, pak α_i^2 je kořenem polynomu $p'_m(y) = \sum_{i=1}^{k} m_i y^i$. Polynom $p'_m(y)$ má nejvýše $k-1$ nenulových kořenů. Pokud tedy pro každé $i \neq j$, $\alpha_i^2 \neq \alpha_j^2$ a všechna α_i jsou nenulová, pak vektor $[p_m(\alpha_1), p_m(\alpha_2), \ldots, p_m(\alpha_n)]$ může obsahovat maximálně $k-1$ nul. Pro takovou volbu bude $d = n - k + 1$. Pokud jsou α_i vybrány nevhodně (například některý z nich je nula), pak bude d příslušně menší.

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.

   Řešení:

   (a) Ano, editovací vzdálenost je metrika. Důkaz ponecháme čtenáři.

   (b) Takové kódy s konstantím ratem a konstantní relativní vzdáleností existují. Klíčová věc je, kolik pro pevné slovo $x \in \Sigma^n$ existuje slov $y \in \Sigma^n$ takových, že $\Delta(x, y) \leq d$, kde $\Delta(x, y)$ je editovací vzdálenost x od y. Nechť $Vol_{q,edit}(x, d) = |\{y \in \Sigma^*; \Delta(x, y) \leq d\}|$. Zřejmě $Vol_{q,edit}(x, d) \leq \sum_{i=0}^{d} \binom{n}{i} \sum_{j=0}^{d} q^j \binom{n-i+j}{j} \leq q^d \left(\sum_{i=0}^{d} \binom{n+d}{i} \right)^2$. Pro konstantní $0 < \delta < 1$, $Vol_{q,edit}(0^n, \delta n) \leq q^{\delta n} 2^{2H(\delta/(1+\delta))(1+\delta)n}$. Uvažujme nyní po jednoduchost případ $q = 2$. Pokud δ je dostatečně malé takové, že $\delta + 2(1+\delta)H(\delta) < 1$, pak existuje kód s ratem $r = 1 - \delta - 2H(\delta)$. Můžeme totiž hladovým způsobem vybrat z $\{0, 1\}^n$ 2^{rn} slov x_i takových, že pro různé i a j, x_i a x_j jsou ve vzdálenosti alespoň δn. Těchto 2^{rn} slov tvoří kód s minimální vzdáleností $\delta n + 1$ opravující $\delta n/2$ chyb.

   Toto je za předpokladu, že nám kódová slova pro dvě různé velikosti n nemohou dát stejné slovo po δn změnách. Abychom tomu zabránili, budeme konstruovat kód pouze pro velikosti n_i takové, že $n_i < (1 - \delta) n_{i+1}$.

(c) Hammingova mez: kód na slovech délky n s minimální vzdáleností d musí obsahovat nejvýše $q^n/Vol_{q,edit}(0^n, d-1/2)$ slov. Gilbert-Varshamova mez je v podstatě problém (b).

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 $F_n[x] = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}; a_0, a_1, \ldots, a_{n-1} \in F\}$ 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.)

   Řešení:

   (a) Vzhledem k tomu, že zbytek při dělení je vždy nezáporný a menší než dělitel, indukcí snadno nahlédneme, že posloupnost $a_0, a_1, a_2, \ldots$ je nezáporná a striktně klesající, dokud se nenarazí na $a_t = 0$. Tudíž t je dobře definované. Dále pak se snadno ověří, že $nsd(a_i, a_{i+1}) = nsd(a_{i+1}, a_{i+2})$, pokud $a_{i+1} \neq 0$. Toto ověření je nutné udělat, mi ho však zde přeskočíme. Z toho vyplývá, že $nsd(a, b) = nsd(a_0, a_1) = nsd(a_{t-1}, a_t) = a_{t-1}$.

   (b) Opět lze indukcí snadno ověřit, že pro každé $i = 0, 1, \ldots$, existuje x_i a y_i takové, že $a_i = a_0x_i + a_1y_i$. To vyplývá z toho, že a_i lze získat z a_{i-2} postupným odečítáním a_{i-1}. Mez na velikost potřebných x_i a y_i vyplývá z toho, že pokud $y_i > a_o$ pak můžeme x_i zvětšit o a_1 a y_i zmenšit o a_0, při zachování požadovaných vztahů. Obdobně pro $-y_i > a_o$. To lze dělat tak dlouho, dokud nenastane $|y_i| < a_o$. Jelikož a_i je menší než a_1, x_i musí být také malé.

   (c) Pro p prvočíslo, všechna čísla m mezi 1 a $p-1$ jsou nesoudělná s p. Tudíž $nsd(m, p) = 1$. Podle předchozí části pak existuje m' takové, že $mm' = 1 (\bmod p)$. Tedy ke každému nenulovému prvku z $GF[p]$ lze nalézt inverzní prvek. Díky asociativitě, komutativitě a $1 \cdot 1 = 1$, $GF[p]^*$ musí být grupa. Detaily zde přeskočíme.

   (d) Postupuje se podle hintu a ukáže se (a), (b) a (c) také pro polynomy, přičemž se za velikost polynomů považuje jejich stupeň.

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 $GF[p]^{2k}$.)

   Řešení: Vychází z předešlého cvičení. Matice M_α obsahuje jako svůj i-tý řádek koeficienty polynomu $\overline{\alpha}_k x^{k+i-1} + \overline{\alpha}_{k-1} x^{k+i-2} + \cdots + \overline{\alpha}_1 x^i \bmod r(x)$, kde $r(x)$ je ireducibilní polynom stupně k používáný při násobení v $GF[p^k]$. Detaily ponecháme čtenáři.