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

4. domácí úlohy - vánoční

do 10. ledna 2008

1. Uvažujme následující algoritmický problém: máme libovolnou posloupnost čísel $x_1, x_2, \ldots, x_n \in \{1, \ldots, n\}$. Navrhněte algoritmus, který by postupně dostával jednotlivé prvky této posloupnosti a na konci by vypsal, který prvek se v posloupnosti vyskytoval nejčastěji, pokud existuje prvek v $\{1, \ldots, n\}$, který se v posloupnosti vyskytuje alespoň $n/2$-krát. Pokud takový prvek neexistuje, výsledek algoritmu nás nezajímá. Jediné omezení na náš algoritmus je, že si může pamatovat pouze $O(\log^2 n)$ bitů informace, mezitím co dostává jednotlivé prvky vstupní posloupnosti.

2. *How to share a secret.* Představte si, že máte skupinu n bankovních úředníků a chcete mezi ně rozdělit kód k trezoru tak, aby libovolná skupina k z nich mohla kód společně zrekonstruovat, ale aby žádná skupina méně než k z nich kód zrekonstruovat nemohla a neměla by o něm žádnou informaci (to jest z jim dostupné informace by kód mohl být stále ještě cokoliv.) Vytvořte takové schéma. V prvním přiblížení tedy chceme funkci $f : \{1, \ldots, N\} \times \{1, \ldots, R\} \to \{1, \ldots, N\}^n$ takovou, že z libovolných k složek $f(x, r)$ můžeme jednoznačně určit x, ale pokud známe pouze $k - 1$ složek $f(x)$, x může být libovolné. Zde x je onen kód k trezoru a r je parametr, který bude zvolen náhodně a též bude utajen. Jak to souvisí se samoopravnými kódy?

3. Nechť n je kladné celé číslo. Zkonstruujme následující kód: nechť zpráva M je matice z $GF[2]^{n \times n}$. Její zakódování je M společně s paritou každého řádku, paritou každého sloupce a paritou těchto parit (tedy vektor/matice z $GF[2]^{(n+1)^2}$). Kolik chyb tento kód umí opravit? Jak chyby opravovat?