

Kombinatorika a grafy 1

Cvičení #11 – Samoopravné kódy

Čtvrtá (poslední) sada domácích úkolů

Deadline: **5. 1. 2022** (v 9:00). Předestírám, že po Novém roce mi pravděpodobně opravy a odpovědi budou trvat dlouho. Pokud ještě potřebujete body na zápočet, důrazně doporučuji poslat řešení co nejdříve, během Vánoc bych se k nim rozhodně měl dostat, čili budete mít slušnou šanci si je případně i opravit a zápočet na začátku zkouškového už mít v SISu.

Řešení ve formátu PDF pošlete mailem na matej@kam.mff.cuni.cz. Ideálně L^AT_EX, můžete ale použít cokoli jiného (exportovaného do PDF) včetně scanu ručního řešení. Moc vás ale prosím o dobře čitelná řešení.

1. Dokažte, že pro každé $n \in \mathbb{N}$ existuje $N \in \mathbb{N}$ takové, že každá množina N bodů v rovině obsahuje buď n bodů na přímce, anebo n bodů v obecné poloze (tj. žádné tři z nich neleží na přímce).
2. Necht' C je kód s parametry $(n, k, 2t + 1)_2$ nad abecedou $\{0, 1\}$. Z něj vytvoříme kód C' tak, že na konec každého kódového slova $x \in C$ ještě přidáme nulu nebo jedničku podle toho, zda x obsahuje sudý či lichý počet jedniček. (Tedy počet jedniček každého slova v C' je potom sudý.) Rozhodněte, jaké má parametry kód C' .

Příklady

1. Dokažte, že Hammingova vzdálenost je skutečně metrika.
2. Necht' C je kód obsahující všechna binární slova délky $n \geq 2$, která obsahují sudý počet jedniček. Určete parametry tohoto kódu a ověřte, že je lineární.
3.
 - (a) Dokažte, že pro každý kód C s parametry $(4, k, 3)_3$ (tj. kód délky 4 nad ternární abecedou, který umí opravit jednu chybu) platí $|C| \leq 9$.
 - (b) Zkonstruujte kód C s parametry $(4, k, 2)_3$ (tj. kód délky 4 nad ternární abecedou, který umí rozpoznat, že došlo k jedné chybě) s $|C| \geq 20$.

4. **Ze života.** Označme $\Sigma = \{0, 1, 2, 3, 4\}$. Paní Nováková posílá svého syna Pepíčka každé ráno na nákup do místního hokynářství, kde prodává její kamarádka paní Baštýřová. Vždy Pepíčkovi řekne, že má koupit a ananasů, b banánů, c chlebů, d balení droždí a e energetických nápojů Monster, přičemž $a, b, c, d, e \in \Sigma$. Pepíček je však pravděpodobně budoucí profesor matematiky, jelikož cestou většinu pokynů zapomene a v hokynářství si vždy vzpomene na právě dvě věci, které měl koupit. (Tj. například správně řekne paní Baštýřové, že měl vzít c chlebů a e energetických nápojů Monster a zbytek že zapomněl.)

Vedle ženy v domácnosti resp. prodavačky v hokynářství jsou ovšem paní Nováková a paní Baštýřová také členky supertajné konspirace. Jako takové spolu potřebují supertajně komunikovat, konkrétně paní Nováková potřebuje každý den poslat paní Baštýřové nějaký řetězec délky 2 nad abecedou Σ . Jejich první nápad byl, že chce-li paní Nováková poslat řetězec ab , řekne Pepíčkovi, aby koupil a ananasů a b banánů. Jak jsme si však řekli výše, tohle nebude fungovat, jelikož Pepíček si nemusí zapamatovat zrovna tyto dva údaje. Pomožte paní Novákové a Baštýřové vymyslet lepší protokol. Přesněji řečeno, pro každý řetězec $ab \in \Sigma^2$ najděte řetězec $c_{ab}d_{ab}e_{ab} \in \Sigma^3$ tak, aby když paní Nováková pošle Pepíčka pro a ananasů, b banánů, c_{ab} chlebů, d_{ab} balení droždí a e_{ab} energetických nápojů Monster, tak paní Baštýřová byla schopna zrekonstruovat zprávu ab z libovolných dvou údajů, na které si Pepíček vzpomene.

Formálně tedy najděte 25 slov z Σ^5 takových, že postupně začínají všemi možnými dvojicemi symbolů a z každé dvojice pozic lze vždy zrekonstruovat první dvě pozice (a tedy celé slovo). Určete parametry vašeho kódu.