Úvod do kódovania – Úloha č. 3

Termín odovzdania 18. máj 2025, vo formáte pdf cez *Google Classroom*

(R) bude znamenať odkaz na knižku S. Romana, (G) P. Garretta a (H) R. Hilla; uvedené bude spravidla číslo príkladu/problému (kapitola.sekcia.problém), alebo číslo strany, kde sa o danej veci píše. Neočakávajú sa úplne kompletné a perfektné riešenia. Aj čiastkové riešenia s drobnými opomenutiami, logickými medzerami, či neporiadnym zápisom si môžu vyžadovať veľa práce a námahy a môžu dostať plný počet bodov. T.j. nemusíte týmito domácimi úlohami stráviť všetok svoj voľný čas počas nadchádzajúceho semestra. Na druhej strane, očakáva sa preukázanie výraznejších snáh, aby domáce úlohy splnili svoj účel – naučiť sa, resp. samostatne objaviť niečo netriviálne z preberaného materiálu.

Vždy je tu možnosť absolvovania konzultácií. Tiež môže pomôcť preskúmanie viacerých príkladov daného fenoménu pri hľadaní dôkazu všeobecného tvrdenia. Akceptované budú aj riešenia založené na počítačových simuláciách, pokiaľ budú primerane zdôvodnené a bude to v danom kontexte dávať zmysel.

Domáca úloha bude obsahovať príklady s celkovým ohodnotením prevyšujúcim 50 bodov, čo je maximum, ktoré sa v rámci jednej úlohy dá získať. To znamená, že si môžete zvoliť, ktorým príkladom sa budete venovať a ktoré nakoniec odovzdáte. Keďže sa dá očakávať, že nie všetky riešenia budú za plný počet bodov, má zmysel odovzdať príklady, ktorých celkové hodnotenie prevyšuje 50 bodov.

1. (5 bodov) Predpokladajme, že náhodne vyberieme M kódových slov z $V(n, \mathbb{Z}_2)$. Nájdite očakávanú minimálnu vzdialenosť medzi týmito slovami (očakávaná minimálna vzdialenosť je priemerom minimálnych vzdialeností pre všetky kódy veľkosti M vo $V(n, \mathbb{Z}_2)$).

Riešenie nemusí byť 'absolútne'. Očakáva sa, že použijete niektoré výsledky z prednášok, ktoré povedú k nejakým odhadom a tým demonštrujete, že rozumiete týmto výsledkom.

2. (5 bodov) Nech $B_q(n, M)$ označuje maximálnu vzdialenosť v ľubovoľnom kóde $\mathcal{C}$ obsahujúcom M slov v $GF(q)^n$. Nájdite nejaké zmysluplné súvislosti (rovnosti, nerovnosti) medzi funkciami $A_q(n, d)$ a $B_q(n, M)$.

3. (5 bodov) Nech $\mathcal{C} \subseteq (\mathbb{F}_q)^n$ je (n, M, d)-kód. Ak vyberieme k pozícií $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$ a zxmažeme symboly na týchto pozíciách v každom kódovom slove v $\mathcal{C}$, dostaneme $(n-k, M', d')$-kód $\widehat{\mathcal{C}}$.

a) Nájdite hornú hranicu pre k ako funkciu d, ktorá zaručí rovnosť $M = M'$.

b) Nájdite vzťahy medzi d a d' (napr. dolný/horný odhad) .

c) Nájdite (n, M, d)-kód $\mathcal{C}$ taký, že po vymazaní troch pozícií dostaneme $(n-3, M/2, d')$-kód.

d) Nájdite (n, M, d)-kód $\mathcal{C}$, pre ktorý existuje postupnosť troch zmazaní (povedzme na pozíciach i_1, i_2, i_3) s vlastnosťou, že postupné mazanie (najprv i_1, potom i_1 a i_2 a nakoniec i_1, i_2, i_3) dá tri kódy s klesajúcou dĺžkou aj klesajúcou minimálnou vzdialenosťou.

4. (5 bodov) Nájdite nejaké zmysluplné dolné a horné odhady minimálnej vzdialenosti v k-rozmernom lineárnom kóde $\mathcal{C} \subseteq (\mathbb{F}_2)^n$.

5. (5 bodov) Pre každý z nasledujúcich prípadov nájdite rozklad $(\mathbb{F}_q)^n$ na dve disjunktné podmnožiny $\mathcal{C}_1$ a $\mathcal{C}_2$ s vlastnosťami:

a) $d(\mathcal{C}_1) + d(\mathcal{C}_2) > n$

b) $d(\mathcal{C}_1) + d(\mathcal{C}_2) = n$

c) $d(\mathcal{C}_1) + d(\mathcal{C}_2) = 2$

Ak usúdite, že danom prípade taký rozklad neexistuje, zdôvodnite svoj úsudok.

6. (5 bodov) Nech $\mathcal{C} \subseteq (\mathbb{F}_q)^n$ je (n, M, d)-kód a Let $\overline{\mathcal{C}} = (\mathbb{F}_q)^n \setminus \mathcal{C}$ je k nemu komplementárny (n, M', d') kód. Existuje nejaký zmysluplný vzťah medzi d a d'? Ak zvolíte odpoveď 'áno', nájdite vzťah a zdôvodnite ho. Ak zvolíte odpoveď 'nie', poskytnite príklady poukazujúce na správnosť vašej voľby. Zmení sa odpoveď, ak navyše predpokladáme, že kód $\mathcal{C}$ je lineárny?

7. (5 bodov) a) Nech $\mathcal{C} \subseteq (\mathbb{F}_q)^n$ je (n, M, d)-kód, ktorého všeetky kódové slová majú párnu váhu. Ak je to možné, vylepšite Hammingov odhad pre tento kód.

b) Vylepšite Hamming odhad pre (n, M, d)-kód $\mathcal{C} \subseteq (\mathbb{F}_q)^n$ s vlastnosťou, že váhy každého z kódových slov sú deliteľné k, $1 < k < n$.

Riešenia nemusia byť 'absolútne'. Očakáva sa využitie niektorých výsledkov/myšlienok z prednášky na dosiahnutie zmysluplných odhadov, čím preukážete, že rozumiete daným výsledkom, resp. dokážete prispôsobiť danú myšlienku v novom kontexte.

8. (5 bodov) Rozhodnite, či neexistencia konečnej projektívnej roviny rádu 10 dáva protipríklad k tvrdeniu, že podmienky vo Vete 2.27 spolu s (2.24) a (2.25) udávajú nutné a postačujúce podmienky pre existenciu symetrického dizajnu. (Hill, str. 25 – 26)

9. (5 bodov) Vyriešte Úlohu 2.12 (str. 27 v Hillovi).

10. (5 bodov) Vyriešte Úlohu 5.8 (str. 54 v Hillovi).

11. (5 bodov) Vyriešte Úlohu 6.9 (str. 66 v Hillovi).

12. (5 bodov) Vyriešte Úlohu 7.10 (str. 79 v Hillovi).

13. (5 bodov) a) Automorfizmus kódu $\mathcal{C}$ dĺžky n je permutácia π v symetrickej grupe $\mathbb{S}_n$ spĺňajúca

$$\pi(u) = \pi(u_1, u_2, \ldots, u_n) = (u_{\pi(1)}, u_{\pi(2)}, \ldots, u_{\pi(n)}) \in \mathcal{C},$$

pre všetky $u \in \mathcal{C}$. Dokážte, že množina automorfizmov kódu $\mathcal{C}$ spolu s operáciou skladania tvorí podgrupu v $\mathbb{S}_n$.

b) Charakterizujte všetky binárne kódy, dĺžky n, ktorých grupa automorfizmov je celá $\mathbb{S}_n$.

c) Nech $\mathcal{C}$ je kód nepárnej dĺžky a $\mathcal{C}'$ je rozšírenie $\mathcal{C}$ popísané v dôkaze Vety 2.7 (str. 16 v Hillovi). Rozhodnite, či existuje vzťah medzi grupami automorfizmov kódov $\mathcal{C}$ a $\mathcal{C}'$. Toto je otázka s 'otvoreným koncom'; spíšte všetky pozorovania, na ktoré pridete, vrátane hypotéz a dokážte to, čo zvládnete dokázať.

14. (10 bodov) Spíšte dôkaz *Plotkinovho ohraničenia* podľa Úloh 2.20, 2.21 a 2.22 na str. 29 v Hillovi.

15. (10 bodov) Napíšte krátky súhrn (na stranu/dve) článku *The fabulous (11,5,2) biplane*. Vysvetlite o čom je tento článok, v čom sú jeho výsledky/popisované objekty význačné a prípadne pridajte aj nejaké osobné názory/poznámky/dojmy.

16. (10 bodov) Napíšte krátky súhrn (na stranu/dve) článku *The search for the finite projective plane of order 10*. Vysvetlite o čom je tento článok, v čom sú jeho výsledky/popisované objekty význačné a prípadne pridajte aj nejaké osobné názory/poznámky/dojmy.

17. (10 bodov) Napíšte krátky súhrn (na stranu/dve) článku *Optimal binary one-error-correcting codes of length 10 have 72 codewords*. Vysvetlite o čom je tento článok, v čom sú jeho výsledky/popisované objekty význačné a prípadne pridajte aj nejaké osobné názory/poznámky/dojmy.