

Zkoušený dostane pět otázek z následujícího seznamu, tři z toho teoretické (u nich bude specifikováno, zda stačí formulovat pojmy či tvrzení nebo je třeba formulované dokázat) a dvě aplikační. U teoretických otázek jsou uvedena čísla tvrzení, na něž míří (úlohy bez čísla míří jen na pojmy), aplikační část testu sestává ze dvou úloh ze seznamu, které mohou být číselně i drobně formulačně modifikovány.

1. TEORETICKÉ OTÁZKY

- 1.1.** Vyslovte a dokažte Hammingovu nerovnost a definujte perfektní kódy. Uveďte netriviální příklad perfektního kódu. (1.3)
- 1.2.** Vysvětlete pojem vzdálenosti a nosnosti kódu. Vyslovte a dokažte Singletonův odhad. (1.4)
- 1.3.** Definujte schopnost kódu opravit chybu a popište ji pomocí vzdálenost kódu. Vyslovte a dokažte tvrzení o určení vzdálenost lineárního kódu z kontrolní matice. (2.3)
- 1.4.** Definujte MDS-kódy a zobecněné Reedovy-Solomonovy kódy. Vyslovte a dokažte tvrzení o duálních kódech k lineárním MDS-kódům. (3.3)
- 1.5.** Zaveďte pojmy lineární kód, generující a kontrolní matice. Co je standardní tvar generující matice?
- 1.6.** Definujte lineární MDS-kódy a vysvětlete, jak je charakterizovat pomocí generující matice. Vyslovte a dokažte tvrzení o nutných podmínkách pro parametry MDS-kódů. (3.4, 4.1)
- 1.7.** Zaveďte reziduální kódy a vyslovte a dokažte tvrzení o zaručené vzdálenosti reziduálních kódů pro MDS kódy. (4.3)
- 1.8.** Popište ireducibilní polynomy nad konečnými tělesy řádu q pomocí polynomu $x^{q^n} - x$. Své tvrzení dokažte. (5.4, 5.5)
- 1.9.** Kolik členů má ireducibilní rozklad cyklotomického polynomu Q_n nad konečným tělesem \mathbb{F}_q , pokud $\text{NSD}(q, n) = 1$? Tvrzení dokažte. (5.6)
- 1.10.** Popište všechny lineární cyklické kódy jako ideály okruhu $\mathbb{F}[x]_n$ a jako množiny $\mathcal{C}(f)$ a tvrzení dokažte. Jak vypadá generující a kontrolní matice lineárního cyklického kódu? (6.3, formulace 6.4)
- 1.11.** Zaveďte Reedovy-Solomonovy kódy a zobecněné Reedovy-Solomonovy kódy. Popište cyklické kódy jako množiny nul. Proč jsou reziduální kódy RS kódů cyklické? (7.1, 7.2, 7.3)
- 1.12.** Zaveďte okruhy booleovských funkcí a booleovských polynomů a popište jejich vztahy. Definujte binární Reedovy-Mullerovy kódy a ukažte jejich konstrukci pomocí booleovských polynomů.
- 1.13.** Co jsou Reedovy-Mullerovy kódy? Vyslovte a dokažte tvrzení o dimenzi a vzdálenosti RM-kódu. (8.2)
- 1.14.** Co jsou Reedovy-Mullerovy kódy? Vyslovte a dokažte tvrzení o dualitě RM-kódu. (8.3)
- 1.15.** Zkonstruujte lineární samoduální $[24, 12, 8]_2$ -kód a 3-perfektní $[23, 12, 7]_2$ -kód a uveďte a dokažte jejich základní vlastnosti. (9.6 a formulace 9.5)

- 1.16.** Vyslovte a dokažte tvrzení o existenci a jednoznačnosti binárního 3-perfektního kódu délky 23. (9.8, 9.9)
- 1.17.** Zaveďte pojem konvoluční kód a generující matice konvolučního kódu.
- 1.18.** Vysvětlete pojmy stupeň a Forneyho indexy konvolučního kódu a dokažte tvrzení, které říká, že jsou Forneyho indexy dobře definované. (10.3)
- 1.19.** Vysvětlete pojmy abstraktního a fyzického konvolučního kódovače. Co znamená realizace fyzického konvolučního kódovače obvodem?
- 1.20.** Zaveďte pojmy a zformulujte tvrzení o vztahu abstraktního a fyzického konvolučního kódovače. Načrtněte myšlenku důkazu. (11.3)
- 1.21.** Zaveďte pojmy vnitřní a vnější stupeň polynomiální matice. Co je základní a redukovaná polynomiální matice konvolučního kódu?
- 1.22.** Vysvětlete pojmy a vyslovte a dokažte tvrzení, které charakterizuje kanonické generující matice pomocí stupně generovaného konvolučního kódu. (12.5)
- 1.23.** Zaveďte pojem mřížový abstraktního konvolučního kódovače? Co je vrstva mřížová? Napište Viterbiho algoritmus pro hledání minimální cesty v mřížový abstraktního konvolučního kódovače.

2. APLIKAČNÍ ÚLOHY

- 2.1.** Určete všechny parametry a nějakou generující matici lineárního binárního kódu s kontrolní maticí $\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$.
- 2.2.** Určete nějakou generující a nějakou kontrolní matici Hammingova $[7, 4, 3]_2$ -kódu. Najděte nějaké slovo délky 7, které v kódu neleží a opravte ho na kódové.
- 2.3.** Určete nějakou kontrolní matici Hammingova $[15, 11, 3]_2$ -kódu. Najděte nějaké slovo délky 15, které v kódu neleží a opravte ho na kódové.
- 2.4.** Určete cyklotomické polynomy $Q_1, Q_3, (Q_5, Q_{15})$ nad tělesem \mathbb{F}_2 .
- 2.5.** Určete kolik existuje různých ireducibilních polynomů stupně a) 2, b) 3, c) 4, d) 5 nad tělesem \mathbb{F}_3 .
- 2.6.** Známe-li ireducibilní rozklad $x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ v oboru $\mathbb{F}_2[x]$, popište všechny binární cyklické kódy délky 7 a dimenze 4.
- 2.7.** Známe-li ireducibilní rozklad $x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ v oboru $\mathbb{F}_2[x]$, najděte generující a kontrolní matici binárního kódu $\mathcal{C}(x^3 + x^2 + 1)$.
- 2.8.** Je-li lineární binární MDS-kód \mathcal{C} délky n a dimenze k , určete parametry propíchnutí kódu \mathcal{C} v i souřadnicích pro každé $i < n - k + 1$.
- 2.9.** Najděte generující matici nějakého lineárního MDS kódu s parametry $[6, 2]$.
- 2.10.** Najděte kontrolní matici nějakého lineárního MDS kódu s parametry $[5, 4]$.
- 2.11.** Najděte kontrolní matici normovaného RS-kódu s parametry $[6, 3]_7$ a určete jeho vzdálenost.

2.12. Sestrojte pro dané k generující a kontrolní matici lineárního MDS-kódu dimenze k .

2.13. Sestrojte generující/kontrolní matici binárního Reed-Mullerova kódu $\mathcal{R}(4, 2)$ a určete jeho parametry.

2.14. Sestrojte generující/kontrolní matici binárního Reed-Mullerova kódu $\mathcal{R}(4, 1)$ a určete jeho parametry.

2.15. Rozhodněte, které z matic (a) $G = \begin{pmatrix} 1 + 2D & D + D^2 \\ D & 2D^2 \end{pmatrix}$,

(b) $G = \frac{1}{D} \begin{pmatrix} D + D^2 & 2D \end{pmatrix}$, (c) $G = \frac{1}{D} \begin{pmatrix} D + D^2 & 2D & 2 + D^2 \end{pmatrix}$ nad tělesem $\mathbb{F}_3(D)$ jsou generující matice konvolučního kódu a u těch, které jsou, určete stupeň kódu.

2.16. Určete stupeň a Forneyho indexy kódů nad tělesem \mathbb{F}_2 s generující maticí

(a) $G = \begin{pmatrix} \frac{1}{1+D} & D \\ D & D^2 \end{pmatrix}$,

(b) $G = \begin{pmatrix} \frac{1}{1+D^2} & \frac{1}{1+D} \end{pmatrix}$.

2.17. Pro fyzický konvoluční kódovač nad tělesem \mathbb{F}_3 s generující maticí $G = \begin{pmatrix} 1+2D \\ 2+D+D^2 \end{pmatrix}$ najděte jeho realizaci obvodem a spočítejte jeho popis jako abstraktního konvolučního kódovače.

2.18. Pro fyzický konvoluční kódovač nad tělesem \mathbb{F}_2 určete vnější stupeň $\text{extdeg}G$ a určete jeho popis jako abstraktního konvolučního kódovače, má-li generující maticí $G = \begin{pmatrix} \frac{1}{1+D} & \frac{D}{1+D^2} \end{pmatrix}$.

2.19. Pro matici $G = \begin{pmatrix} 1 & 0 & 1 \\ 1 & D^2 + D^3 & D \end{pmatrix}$ nad oborem $\mathbb{F}_2[D]$ spočítejte $\text{extdeg}(G)$ a $\text{intdeg}(G)$ a rozhodněte, zda je základní.

2.20. Pro matici $G = \begin{pmatrix} 1 & 0 & D \\ 0 & 1 + D^4 & 1 + D^2 \end{pmatrix}$ nad oborem $\mathbb{F}_2[D]$ spočítejte $\text{extdeg}(G)$ a $\text{intdeg}(G)$ a rozhodněte, zda je redukovaná.

2.21. Typ úlohy: Pro abstraktní konvoluční kódovač nakreslete jeho multigraf (nebo vrstvu mřížoví).

2.22. Typ úlohy: Pro abstraktní konvoluční kódovač dekódujte přijaté slovo Viterbiho algoritmem.