Samoopravné kódy - zkoušená látka

- definice: (lineární) blokový kód; délka, dimenze, (minimální) Hammingova vzdálenost kódu, (minimální) váha (kódového slova / kódu), hustota (neboli nosnost, neboli informační poměr) kódu
- definice: relativní vzdálenost, $\alpha(\delta)$ - asymptoticky nejlepší informační hustota pro danou relativní vzdálenost
- definice: generující a kontrolní matice lineárního kódu
- věta: minimální váha je rovna minimální vzdálenosti
- vztah počtu opravitelných a rozeznatelných chyb k minimální vzdálenosti
- definice: (q-ární) Hammingovy kódy
- definice: duální kód, samoortogonální a samoduální kódy
- věta: Singletonův odhad (pro lineární i nelineární kódy), asymptotická verze
- definice: MDS (maximum distance separable) kódy
- věta: Hammingův odhad (pro q-ární kódy). Asymptotická verze.
- definice: perfektní kódy
- odvození váhového polynomu perfektního kódu
- definice: t–(v, k, λ) design, incidenční matice M
- určení počtu bloků a stupně vrcholů designu
- definice: čtvercový design (2–(v, k, λ) design, kde počet bloků je v)
- věta: symetrie čtvercových designů (čtvercová incidenční matice M je 2–(v, k, λ) design, právě když M^{T} je 2–(v, k, λ) design)
- definice $\mathcal{G}_{24}$: rozšířený Golayův kód $(24, 12, 8)$ (pomocí dvanáctistěnu)
- definice $\mathcal{G}_{23}$: Golayův kód $(23, 12, 7)$ (propíchnutý $\mathcal{G}_{24}$)
- věta: $\mathcal{G}_{24}$ je samoduální
- věta: $\mathcal{G}_{24}$ má váhu 8 (metoda důkazu)
- odvození matice $\mathcal{G}_{24}$ v kanonickém tvaru, přítomnost 2–$(11, 5, 2)$ designu (jeho jednoznačnost bez důkazu)
- definice: cyklický kód jako ideál v okruhu polynomů (a proč to znamená cykličnost v běžném smyslu)
- věta: vztah generující a kontrolní matice cyklického kódu
- věta: rozklad $x^n - 1$ nad $\mathbb{F}_{q^s}$
- věta: vztah mezi uspořádáním kódů inkluzí a dělitelností generujících polynomů
- souvislost mezi ideálem a společnými kořeny v rozkladovém nadtělese
- definice: Reedovy-Solomonovy kódy (zobecněné a konvenční)
- věta: vztah mezi generující a kontrolní maticí RS kódu (speciální případ: normalizované RS kódy)
- věta: RS kódy jsou MDS
- definice: residuální kódy, zaručená vzdálenost
- věta: odhad dimenze residuálního kódu
- definice: BCH kód
- věta: generující polynom BCH kódu
- definice: QR-kódy
- věta: podmínka na prvočíselnou délku QR-kódu
- věta: kdy je rozšířený QR kód samoduální
- věta: odhad (liché) váhy QR kódu
- definice: Reedovy-Mullerovy kódy

- věta: korespondence booleovských funkcí a booleovských polynomů (algebraická normální forma booleovské funkce a její jednoznačnost)
- věta: afinní podprostory jako incidenční množiny booleovských monomů
- věta: dimenze RM kódu
- věta: minimální váha RM kódu (pomocí induktivní katenční charakterizace)
- věta: korespondence mezi vektory minimální váhy a afinními podprostory maximální kodimenze
- věta: RM-kód je generován vektory minimální váhy
- dekódování RM-kódu většinovou logikou
- definice: Hadamardovy matice
- konstrukce Hadamardových matic: Sylvestrovy matice, Paleyho konstrukce
- věta: Plotkinův odhad (binární verze)
- věta: Gilbert-Varšamovova nerovnost (existence kódu); asymptotická verze
- definice: vzájemná informace náhodných veličin, kapacita kanálu
- binární symetrický kanál, výpočet kapacity
- věta: Shannonova věta (důkaz pro BSC)
- inverzní Shannonova věta (důkaz pro BSC)
- definice: dobrá třída kódů
- definice: Justesenovy kódy