Teorie kódování

Bezpečnostní kódy

Bezpečnostní kódy

Bezpečnostní kód = kód, který zabezpečuje informaci před šumem.

Redundance = nadbytečně přenášená informace.

Šum

1. záměna vyslaného znaku za jiný znak,
2. porucha synchronizace.

Kódy objevující chyby – kódy, u nichž umíme určit, že došlo k chybě, ale neumíme ji opravit.

Kódy opravující chyby – kódy, u nichž umíme určit, že došlo k chybě, a opravit ji.

Hammingova vzdálenost

Hammingova vzdálenost

$$\mathrm{d}(\alpha, \beta) = |\{i \in \hat{n} | a_i \neq b_i\}|$$

d je metrika: $\forall \alpha, \beta, \gamma \in \mathbb{A}^n$:

1. $\mathrm{d}(\alpha, \beta) \geq 0$
2. $\mathrm{d}(\alpha, \beta) = \mathrm{d}(\beta, \alpha)$
3. $\mathrm{d}(\alpha, \beta) = 0 \Leftrightarrow \alpha = \beta$
4. $\mathrm{d}(\alpha, \beta) \leq \mathrm{d}(\alpha, \gamma) + \mathrm{d}(\gamma, \beta)$

Minimální vzdálenost kódu

$$\mu(K) = \min\{\mathrm{d}(\alpha, \beta) | \alpha, \beta \in K,\ \alpha \neq \beta\}$$

Objevování a opravování chyb

Definice: Řekneme, že došlo k t-násobné chybě, liší-li se přijaté slovo β od vyslaného slova α v nejvýše t znacích.

Definice: Řekneme, že kód $K \subseteq \mathbb{A}^n$ objevuje t-násobné chyby, platí-li
$\forall \alpha \in K \; \forall \beta \in \mathbb{A}^n : 0 < \mathrm{d}(\alpha, \beta) \leq t \Rightarrow \beta \notin K$.

Věta: Kód K objevuje t-násobné chyby $\Leftrightarrow \mu(K) > t$.

Definice: Řekneme, že kód $K \subseteq \mathbb{A}^n$ opravuje t-násobné chyby, platí-li
$\forall \alpha \in K \; \forall \beta \in \mathbb{A}^n : \mathrm{d}(\alpha, \beta) \leq t \Rightarrow$
$\forall \alpha' \in K : \alpha' \neq \alpha \Rightarrow \mathrm{d}(\alpha', \beta) > \mathrm{d}(\alpha, \beta)$.

Věta: Kód K opravuje t-násobné chyby $\Leftrightarrow \mu(K) > 2t$.

Příklady bezpečnostních kódů

- Paritní kód
- Opakovací kód
- Kód „2 z 5“
- Koktavý kód
- Kód celkové kontroly parity
- Hammingův kód

Kódování a dekódování

Definice (Dekódování): Libovolné zobrazení $\delta : \mathbb{A}^n \to K$, které každému slovu délky n přiřadí kódové slovo, a přitom přijatá kódová slova nemění, tj. $\delta(\alpha) = \alpha$, $\forall \alpha \in K$.

Definice: Řekneme, že kód $K \subseteq \mathbb{A}^n$ má k informačních a $(n-k)$ kontrolních znaků $\Leftrightarrow$ existuje bijekce

$$\varphi : \mathbb{A}^k \to K.$$

Zobrazení φ se nazývá kódování informačních znaků.

Informační poměr $= \frac{k}{n}$

Systematický kód

Definice: Řekneme, že kód $K \subseteq \mathbb{A}^n$ je systematický $\Leftrightarrow$
$\exists k < n : (\forall \alpha = a_1 \dots a_k \in \mathbb{A}^k : \exists! \alpha' = a_{k+1} \dots a_n \in \mathbb{A}^{n-k} :$
$\alpha\alpha' \in K)$.
Kódování $\varphi : \mathbb{A}^k \to K$, definované předpisem $\varphi(\alpha) = \alpha\alpha'$, se nazývá systematické kódování informačních znaků.

Věta: Minimální vzdálenost $\mu(K)$ systematického kódu nemůže překročit počet $(n-k)$ kontrolních znaků o více než jeden, tj.

$$\mu(K) \leq n - k + 1 \qquad \text{(Singletonova nerovnost).}$$