

Lineární kódy

Nad binární abecedou $\{0, 1\}$ a vzdálenostní funkcí jejích řetězců (typicky Hammingovskou metrikou) definujeme (n, k, d) -kód C následovně.

- $C \subseteq \{0, 1\}^n$
- vzdálenost mezi každými dvěma (různými) prvky v C je alespoň d
- $k = \log_2 |C|$

n je délka kódu, d je vzdálenost kódu, k je dimenze kódu

Příklad 1: Mějme (n, k, d) -kód pro liché d . Rozšířme všechna jeho slova o paritní bit (počítá paritu počtu jedniček). Určete parametry výsledného kódu. (speciálně pro $d = 1$)

Co by se stalo, pokud by d bylo sudé?

Příklad 2: Ukažte, že pro generující matici G a kontrolní matici K (nějakého binárního lineárního kódu) platí, že $GK = 0$.

Příklad 3: Dokažte, že pokud je generující matice G lineárního kódu C ve *standardním tvaru*, tzn. $G = [I_k | P]$ kde I_k je jednotková matice řádu k , potom

$$H = [-P^T | I_{n-k}]^T = \begin{bmatrix} -P \\ I_{n-k} \end{bmatrix}$$

je paritní matice C .

Příklad 4: Navrhněte binární kód velikosti 16, opravující jednu chybu. Navíc, chceme aby syndrom binárně kódoval pozici kterou je třeba opravit.