

1

Nechť \mathbf{C} je $[n, k, d]_2$ MDS kód, tedy $d = n - k + 1$. Uvažujme generující matici tohoto kódu ve standardním tvaru a označme jí $C = [I_k | A]$, kde A je matice z $\mathbb{F}_2^{k \times (n-k)}$. Matice A je díky tomu, že \mathbf{C} je MDS, typu $\mathbb{F}_2^{k \times (n-k)} = \mathbb{F}_2^{k \times (d-1)}$.

Pokud $k = 1$, tak matice C má pouze jeden řádek a aby byla splněna podmínka $d = n - 1 + 1$, tak v matici A (která je vlastně řádkový vektor) musí být samé 1 (tedy i v C). Což znamená, že tento kód je opět triviální a je to opakovací kód. Tedy $[n, 1, n]_2$ kód.

V řádcích C jsou kódová slova (prvky báze jsou také kódová slova), která musí splňovat, že jejich vzdálenost je d . Ale na prvních k prvcích je jejich vzdálenost pouze 1, kvůli tomu, že C obsahuje identickou matici, takže nezbyvá nic jiného, než že v matici A jsou samé jedničky, aby vzdálenost od nulového slova byla d . Pokud ale sečteme první 2 řádky matice C , tak z definice musí jejich součet být kódové slovo, ale to má právě 2 nenulové prvky, tedy $d \leq 2$.

Celkem tedy máme $1 \leq d \leq 2$. Takže $k = n - 1$ nebo $k = n$. Jediné možné binární MDS kódy jsou tedy

- $[n, 1, n]_2$
- $[n, n, 1]_2$
- $[n, n - 1, 2]_2$

My chceme ale 1-perfektní kódy, tedy $d > 2$. Tudíž jediný lineární kód co to splňuje je $[n, 1, n]_2$, což je 2 prvkový opakovací kód $\mathbf{C} = \{000 \dots 0, 111 \dots 1\}$. Tento kód můžeme jednoduše upravit na nelineární přičtením jakéholiv nenulového vektoru k oboum vektorům této množiny.

Nelineární zbytek???