11. cvičení

Doplněk kódu. *(Toto tvrzení jsme použili na přednášce.)* Mějme vektorový prostor $\mathbb{Z}_p^n$ a nějaký jeho vektorový podprostor P generovaný maticí A, tzn. $P = \{x \mid \exists y : y^\intercal A = x\}$, neboli x je lineární kombinace řádků A. Ortogonální doplněk $P^\perp = \{x \mid Ax = 0\}$ neboli množina takových vektorů, které jsou kolmé na všechny vektory z P, tzn. platí $P^\perp = \{x \mid \forall x' \in P : x^\intercal x' = 0\}$.
Dokažte, že

$$\dim P + \dim P^\perp = n \ .$$

Hint: můžete použít fakt z lineární algebry, který říká, že pro matici A s n sloupci platí

$$\operatorname{rank}(A) + \dim(\ker(A)) = n \ .$$

Samoduální kód. Najděte příklad samoduálního kódu nad $\mathbb{Z}_2$ (t.j. $C = C^\perp$) délky alespoň 2.
Určete parametry následujícího kódu (nad $\mathbb{Z}_2$):
$C = \{(x_1; x_2; x_3; x_4; x_1 + x_2 + x_3; x_2 + x_3 + x_4; x_1 + x_4) \mid x_1, x_2, x_3, x_4 \in \mathbb{Z}_2\}$

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$K = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Rozmyslete, že G je generující matice (pro každý vektor $v \in \mathbb{Z}_2^4$, vG je kódové slovo) a K je kontrolní matice (pro každý vektor $w \in \mathbb{Z}_2^7$, $wK = (0, 0, 0)$ právě když $w \in C$). Slova považujeme ža řádkové vektory.

Generující a paritní matice. 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, pak $H = [-P^\intercal|I_{n-k}]$ je paritní matice C. (Předchozí příklad je v tomto tvaru.)

Hammingův kód. Na přednášce jsme řekli, že pro nalezení co největšího kódu s minimální vzdáleností 3 vezmeme paritní matici takovou, že obsahuje jako sloupce všechny binární zápisy čísel $1, \ldots, 2^r$, protože tyto sloupce jsou po dvou lineárně nezávislé.
Rozmyslete, že kód z předchozího příkladu je právě takový.
Dále zkuste pro $k = 4$ napsat paritní matici a pak generující matici takového kódu. (Ano, jsou velké...) Pak si vyzkoušejte kódování a dekódování, tedy zvolte nějakou zprávu správné (tedy jaké?) délky x, spočítejte součin xG, porušte nějaký jeden bit a zkuste zprávu dekódovat. (K dekódování Hammingových kódů si řekneme více na příští přednášce, ale zkusit to můžete :-))

Hadamardův kód. Velice zajímavý kód vznikne jako duál Hammingova kódu. Vezměte paritní matici Hammingova kódu (výše K) a uvažujte nad ní jako nad generující maticí. Jak dlouhé zprávy kóduje do jak dlouhých slov? Jaká je minimální vzdálenost tohoto kódu? (Cíl je, abyste nad tím začali přemýšlet; dostanu se k tomu na příští přednášce.)