Pomocný text

Binární kódy

V této sérii se budeme zabývat binárními kódy, které se často používají v teorii kódování. Umožňují například zakódovat odesílanou zprávu tak, aby šla správně přečíst i v případě, že se během přenosu poškodí či pozmění. To se může hodit třeba při přenosu elektronických dat nebo při komunikaci s vesmírnými družicemi.

Binárním slovem délky $n \in \mathbb{N}$ rozumíme posloupnost délky n, která obsahuje pouze nuly a jedničky, například 0101 je binární slovo délky 4. Binárním kódem délky $n \in \mathbb{N}$ je pak libovolná neprázdná množina binárních slov délky n, například $\{0101, 1110, 1001\}$. Všimněte si, že každý binární kód délky n může obsahovat nejvýše 2^n slov.

Součet dvou binárních slov (stejné délky) definujeme po složkách, přičemž na každé složce sčítáme modulo 2 (provádíme vlastně operaci XOR, tedy $0+0=0$, $0+1=1+0=1$ a $1+1=0$). Platí tedy například $0101+0011=0110$, $1111+1101=0010$. Uvědomte si, že takto definované sčítání je asociativní a komutativní s neutrálním prvkem $\mathbf{0}$ (slovo ze samých nul) - pro libovolná slova u, v, w platí $(u+v)+w = u+(v+w)$, $u+v = u+v$ a $u+\mathbf{0} = \mathbf{0}+u$.

Binární kód nazveme lineární, pokud s každými dvěma slovy u, v obsahuje i slovo $u+v$. (Všimněte si, že každý binární lineární kód obsahuje slovo $\mathbf{0}$ - stačí vzít libovolné jeho slovo u a uvážit slovo $u+u$).

Binární lineární kód dále nazveme cyklický, pokud s každým slovem obsahuje i všechny jeho cyklické posuny. Například všechny cyklické posuny slova BRKOS jsou slova BRKOS, SBRKO, OSBRK, KOSBR a RKOSB. Pokud daný kód není lineární, nemůžeme mluvit o jeho cykličnosti. Příkladem binárního cyklického kódu je třeba kód $\{000, 101, 011, 110\}$ (ověřte si!).

Vzdáleností dvou slov stejné délky rozumíme počet pozic, na kterých se liší; vzdálenost slov 01010 a 11100 je tedy 3.

Aby Vám série šla lépe od ruky, vyřešíme si společně jednu úlohu.

Příklad 5.1. Ukažte, že v každém binárním lineárním kódu buď všechna slova začínají na 0, nebo polovina slov začíná na 0 a polovina na 1.

Řešení. Označme množinu všech slov z našeho kódu C, která začínají na 0, jako C_0 a množinu všech slov z C, která začínají na 1, jako C_1. Pokud $C_0 = C$, jsme hotovi protože všechna slova v našem kódu začínají na 0. V opačném případě existuje nějaké slovo $w \in C$, které začíná na 1. Uvažme nyní množinu $w + C_0 = \{w + u \mid u \in C_0\}$ všech slov, která vzniknou sečtením našeho slova w a slova začínajícího na 0. Protože je C lineární, platí $w + C_0 \subseteq C$; navíc sčítání funguje po složkách a $1+0=1$, takže $w + C_0 \subseteq C_1$. Ukážeme, že každému slovu $u \in C_0$ jednoznačně odpovídá slovo $w + u \in C_1$; pak budeme vědět, že množiny C_0 a C_1 jsou stejně velké (formálně: zobrazení $f : C_0 \to C_1$ dané předpisem

$f(u) = w + u$ je bijekce – vzájemně jednoznačné zobrazení). To je ale snadné, protože každému slovu $v \in C_1$ odpovídá slovo $w + v \in C_0$ (neboť $w + (w + v) = \mathbf{0} + v = v$) a naopak pro $x, y \in C_0$ z rovnosti $w + x = w + y$ vyplývá $x = w + (w + x) = w + (w + y) = y$. Tím je důkaz hotov.