Blokové kódy a konvoluční kódy

Lineární blokové kódování je lineární zobrazení $\varphi : \mathbb{F}^b \to \mathbb{F}^c$. *Blokový kód* $\mathcal{C}$ s parametry (b, c) je potom množina všech kódových slov, tedy příslušný obraz $\mathbb{F}^b$, který je b-dimenzionálním podprostorem $\mathbb{F}^c$. Kód $\mathcal{C}$ sám o sobě určuje některé vlastnosti kódování, ale samozřejmě nedefinuje kódovací zobrazení φ, které můžeme nejlépe zadat *generující maticí* G, jejíž řádky $\{g_1, g_2, \ldots, g_b\}$ tvoří nějaká báze kódu. Volba báze tedy přiřazuje danému kódu určité kódování φ definované hodnotami $\varphi(e_i) = g_i$ a pro libovolné $u \in \mathbb{F}^b$ splňující $\varphi(u) = uG$.

> Pozn.: Parametry kódu se obvykle značí písmeny (n, k). V těchto přednáškách budeme používat (b, c) a písmena n a k ušetříme pro jiné účely.

Kódovaná zpráva je typicky delší než jeden blok, skládá se z více bloků. Zprávu tedy můžeme považovat za nekonečnou posloupnost bloků $u_0, u_1, \ldots$ (v případě konečné zprávy s konečným počtem nenulových bloků), která je zobrazena na posloupnost $v_0, v_1, \ldots$, kde $v_i = u_i G$. Je užitečné dovolit, aby byla zpráva indexována počínaje libovolným celým číslem z. To odpovídá situaci, kdy zpráva začíná jindy než v čase nula. Proto se z nazývá *zpoždění* zprávy. Zpráva začínající záporným číslem má „záporné zpoždění“, má začátek v minulosti. Zpráva ovšem musí mít začátek vždy, zprávy přicházející z „nekonečné minulosti“ neuvažujeme.

Klíčovým krokem je reprezentace posloupnosti $\mathbf{u} = (u_i)_{i=z}^{\infty}$, $z \in \mathbb{Z}$, pomocí její *generující řady*, tedy formální řady $\mathbf{u}(D) = \sum_{i=z}^{\infty} u_i D^i$. Později budeme automaticky předpokládat, že zpráva je dána svou řadou, a budeme proto řadu zjednodušeně značit jako $\mathbf{u}$, namísto $\mathbf{u}(D)$. Tato reprezentace poskytuje celou řadu užitečných nástrojů pro manipulaci s danou posloupností. Nejjednodušším z nich je fakt, že posloupnost začínající o jeden časový interval později než $\mathbf{u}$, je dána řadou $\mathbf{u}(D)D$.

> Pozn.: To také vysvětluje, proč se v teorii kódů používá formální proměnná D (na rozdíl od v algebře obvyklejšího x): proměnnou D lze totiž chápat jako „operátor zpoždění“, anglicky *delay*. Myšlenka reprezentace posloupnosti řadou se někdy v literatuře nazývá „Huffmanova D-transformace“.

Řady, které jsme definovali, se nazývají *formální Laurentovy řady*. Takové řady s indexy z množiny R a s formální proměnnou D se značí $R((D))$. Naše řada $\mathbf{u}(D)$ je tedy prvkem $\mathbb{F}^b((D))$, indexy jsou b-tice. Můžeme ji ale také chápat jako b-tici prvků $\mathbb{F}((D))$, tedy jako prvek $\mathbb{F}((D))^b$. Základní výhoda tohoto chápání spočívá v tom, že $\mathbb{F}((D))$ **je těleso** a celá (i nekonečná) zpráva se tak stává prvkem konečně dimenzionálního vektorového prostoru, stejně jako jeden blok blokového kódu.

*

Těleso $\mathbb{F}((D))$ zastřešuje struktury, se kterými budeme pracovat:

- Formální Laurentovy řady (nad tělesem $\mathbb{F}$ a s proměnnou D), tvoří těleso, které značíme $\mathbb{F}((D))$, s běžným násobením, které odpovídá konvoluci posloupností prvků $\mathbb{F}$:

  $$(\mathbf{u} \star \mathbf{v})_k = \sum_{i \in \mathbb{Z}} u_i \cdot v_{k-i}.$$

  Uvedená suma je pro každé k dobře definovaná, protože díky konečnému zpoždění obsahuje jen konečný počet nenulových členů. Inverzní prvek lze v tělese $\mathbb{F}((D))$ najít pomocí postupu známého jako „dlouhé dělení“.

- Těleso Laurentových formálních řad obsahuje podokruh formálních mocninných řad $\mathbb{F}[[D]]$, jehož prvky mají nezáporné zpoždění. Odpovídající posloupnosti se také nazývají *kauzální*. Invertibilní jsou v $\mathbb{F}[[D]]$ právě řady s nulovým zpožděním. (Dokažte.)
- V podokruhu $\mathbb{F}[D]$ polynomů jsou invertibilní pouze nenulové prvky tělesa $\mathbb{F}$. (Dokažte.)
- Laurentovy řady s konečným počtem nenulových koeficientů se nazývají *Laurentovy polynomy* nebo *řady konečné váhy* a značí se $\mathbb{F}[D, D^{-1}]$. Invertibilní jsou zde právě všechny (nenulové) monomy. (Dokažte.)
- Podobně značíme řady, které neobsahují žádné nenulové koeficienty s kladným indexem (a konečný počet nenulových koeficientů s indexem menším nebo rovným nule) symbolem $\mathbb{F}[D^{-1}]$. I tyto „záporné polynomy“ tvoří podokruh.
- Všimněte si, že analogické struktury $\mathbb{F}[[D^{-1}]]$ a $\mathbb{F}((D^{-1}))$, tedy řady tvaru $\sum_{i=z}^{\infty} u_i D^{-i}$, nejsou podmnožinou $\mathbb{F}((D))$.
- Důležitým podtělesem je těleso $\mathbb{F}(D)$ *racionálních funkcí*, tedy Laurentovy řady, které lze napsat jako podíl polynomů:

$$\mathbb{F}(D) = \left\{ \frac{\mathbf{p}}{\mathbf{q}} \;\middle|\; \mathbf{p} \in \mathbb{F}[D], 0 \neq \mathbf{q} \in \mathbb{F}[D] \right\}$$

- Racionální funkce, které jsou současně formálními řadami, se nazývají *realizovatelné*. To jsou právě ty funkce (ukažte!), které lze zapsat jako podíl polynomů $\mathbf{p}/\mathbf{q}$, kde absolutní člen polynomu $\mathbf{q}$ je nenulový.

Název „realizovatelné funkce“ a jejich význam pro konvoluční kódy spočívá v tom, že násobení řady realizovatelnou funkcí lze fyzicky realizovat obvodem podobným lineárnímu posuvnému registru se zpětnou vazbou (známým jako LFSR z ang. Linear Feedback Shift Register).

*

Vraťme se k naší generující matici blokového kódu G. Tato matice (tvaru $b \times c$) definuje nejen lineární zobrazení $\mathbb{F}^b \to \mathbb{F}^c$, ale také lineární zobrazení $\mathbb{F}((D))^b \to \mathbb{F}((D))^c$. Zavedené struktury tedy umožňují vyjádřit zakódování celé zprávy „najednou“. To samozřejmě není pro blokový kód příliš zajímavé, je to jen jiné (a asi zbytečně složité) vyjádření faktu, že se zpráva dělí na bloky a ty se kódují jeden po druhém. Můžeme však nyní snadno definovat konvoluční kód a konvoluční kódování jako zobecnění kódování blokového.

Definice.
- *Konvolučním kódem* s parametry (b, c) rozumíme podprostor $\mathcal{C} \subseteq \mathbb{F}((D))^c$ dimenze b, který má nějakou bázi v $\mathbb{F}(D)^c$.
- Matici $\mathbf{G}$, jejíž všechny indexy jsou realizovatelné funkce a jejíž řádky tvoří bázi $\mathcal{C}$, nazýváme *generující maticí* konvolučního kódu $\mathcal{C}$.
- Generující matice definuje vztahem $\varphi(\mathbf{u}) = \mathbf{uG}$ *konvoluční kódování*, což je lineární zobrazení $\varphi : \mathbb{F}((D))^b \to \mathbb{F}((D))^c$.

Poznámka ke značení: Spodní indexy budeme jako výše používat k označení času (pořadového čísla vstupu). Chceme-li zdůraznit, že vstup u_i není prvek $\mathbb{F}$ ale prvek $\mathbb{F}^b$, budeme psát $\vec{u}_i$. Pro j-tou složku $\vec{u} \in \mathbb{F}^b$ budeme používat značení $u^{(j)}$. Pro generující řady posloupností a pro odpovídající matice budeme používat tučné písmo. Viděli jsme, že řadu $\mathbf{u}$ můžeme chápat buď jako prvek $\mathbb{F}^b((D))$, nebo jako

prvek $\mathbb{F}((D))^b$. První případ odpovídá v našem značení zápisu

$$\mathbf{u} = \sum_{i=z}^{\infty} \overrightarrow{u}_i \, D^i,$$

v druhém případě je $\mathbf{u} = \left(\mathbf{u}^{(1)}, \mathbf{u}^{(2)}, \ldots, \mathbf{u}^{(b)}\right)$, kde

$$\mathbf{u}^{(j)} = \sum_{i=z}^{\infty} u_i^{(j)} D^i.$$