## Konvoluční kódovač

Vytvořili jsme si aparát umožňující vyjádřit konvoluční kódový obraz celé (i nekonečné) vstupní zprávy najednou. Na kódovací proces se ale i nadále můžeme dívat jako na zařízení, které v daném čase (v $i$-tém časovém taktu) přijme vstup $\vec{u}_i$ a vrátí výstup $\vec{v}_i$. Rozdíl od blokového kódovače je v tom, že výstup není jednoznačně definován vstupem, záleží také na *stavu* kódovače. Chování konvolučního kódovače je tedy složitější než chování blokového kódovače, respektuje nicméně následující pravidla:

- Množina $\mathcal{S}$ stavů kódovače je konečná.
- Před začátkem zprávy je kódovač vždy ve stejném *počátečním stavu*.
- Stav kódovače se mění výhradně vstupem, a to deterministicky pomocí *přechodové funkce* $\delta : \mathcal{S} \times \mathbb{F}^b \to \mathcal{S}$. Je-li tedy $s_i$ stav kódovače v čase $i$, pak platí $s_{i+1} = \delta(s_i, u_i)$.
- Výstup $v_i$ je závislý výhradně na vstupu a stavu kódovače pomocí *výstupní funkce* $\lambda : \mathcal{S} \times \mathbb{F}^b \to \mathbb{F}^c$, neboli $v_i = \lambda(s_i, u_i)$.

V teorii systémů se takový kódovač nazývá *časově invariantní* systém, protože jeho chování nezáleží na konrétním čase, pouze na předchozích událostech. Označme $K(\mathbf{u})$ výstup kódovače na vstupu $\mathbf{u}$, kde vstup i výstup reprezentujeme generujícími funkcemi. Tedy

$$K\left(\sum_{i=z}^{\infty} \vec{u}_i\, D^i\right) = \sum_{i=z}^{\infty} \vec{v}_i\, D^i\,.$$

Předpoklad, že $K$ je časově invariantní (s fixním počátečním stavem) lze jednoduše zapsat jako

$$K(\mathbf{u}D) = K(\mathbf{u})D\,,$$

akce kódovače komutuje s akcí zdržení. (Časová invariance samozřejmě předpokládá, že počáteční stav kódovače je nezávislý na indexu, kterým posloupnost začíná.)

Konvoluční kódovač je ale navíc *lineární*, pro libovolné vstupy $\mathbf{u}$, $\mathbf{w}$ a $r \in \mathbb{F}$ platí

- $K(\mathbf{u} + \mathbf{w}) = K(\mathbf{u}) + K(\mathbf{w})$,
- $K(r\mathbf{u}) = rK(\mathbf{u})$.

Je-li $\mathbf{u} \in \mathbb{F}(D)^b$, tedy je-li to vektor racionálních funkcí, dostáváme (ukažte!) z definice lineární časově invariantní transformace vztah

$$K(\mathbf{u}) = \mathbf{u}\mathbf{G}. \tag{1}$$

kde $\mathbf{G}$ je matice, jejíž položka $\mathbf{g}_{i,j} = (\mathbf{G})_{i,j}$ je rovna $j$-té složce výstupu $\mathbf{v}$ na vstupu $\mathbf{e}_i = (0, \ldots, 0, 1, 0, \ldots 0) \in \mathbb{F}(D)^b$, tedy na zprávě s jedinou nenulovou hodnotou $u_0^{(i)} = 1$. Poznamenejme, že jsme tiše přešli od $\mathbb{F}^b(D)$ k $\mathbb{F}(D)^b$. U systémů s $b = c = 1$ se hodnota $K(1)$ se nazývá *odezva* systému. Je také přirozené dodefinovat hodnoty zobrazení spojitě, tj. tak, že vztah (1) platí pro všechny prvky $\mathbb{F}((u))$, nejen ty racionální.

Pro lineární časově invariantní systém lze, jak uvidíme později, bez újmy na obecnosti (tj. beze změny kódování) předpokládat, že jeho stavy tvoří vektorový prostor nad $\mathbb{F}$ a výstupní a přechodová funkce $(\delta, \lambda) : (s_i, u_i) \to (s_{i+1}, v_i)$ je lineární zobrazení mezi vektorovými prostory $\mathcal{S} \times \mathbb{F}^b \to \mathcal{S} \times \mathbb{F}^c$. Dimenze $m$ prostoru stavů se nazývá *stupeň* kódovače. Zobrazení $(\delta, \lambda)$ se obvykle reprezentuje čtyřmi maticemi $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ a $\mathcal{D}$, které dohromady tvoří matici $(\delta, \lambda)$ tak, že platí

$$s_{i+1} = s_i\mathcal{A} + u_i\mathcal{B}, \qquad\qquad v_i = s_i\mathcal{C} + u_i\mathcal{D}\,.$$

Přechodem ke generujícím řadám dostáváme (ověřte!)

$$\mathbf{s}\,D^{-1} = \mathbf{s}\,\mathcal{A} + \mathbf{u}\,\mathcal{B}, \qquad\qquad \mathbf{v} = \mathbf{s}\,\mathcal{C} + \mathbf{u}\,\mathcal{D}\,,$$

a tedy

$$\mathbf{s} = \mathbf{u}\,\mathcal{B}(D^{-1}\mathcal{I}_m - \mathcal{A})^{-1}, \qquad \mathbf{v} = \mathbf{u}\,(\mathcal{D} + \mathcal{B}(D^{-1}\mathcal{I}_m - \mathcal{A})^{-1}\mathcal{C})\,,$$

kde $\mathcal{I}_m$ je jednotková matice stupně $m$. Odtud dostáváme vztah s výše zmíněnou „maticí odezev"

$$\mathbf{G} = \mathcal{D} + \mathcal{B}(D^{-1}\mathcal{I}_m - \mathcal{A})^{-1}\mathcal{C}\,,$$

a vidíme zároveň, že je to matice (tvaru $b \times c$) nad tělesem racionálních funkcí $\mathbb{F}(D)$. Tuto matici nazýváme *generující maticí* daného kódování.

Můžeme se naopak ptát, zda libovolná taková matice je generující maticí nějakého kódovače. Pokud budou existovat 1/1 kódovače odpovídající funkcím $\mathbf{g}_{ij}$, bude možné sestavit kódovač pro $\mathbf{G}$ jako kombinaci takových elementárních kódovačů. Uvažme např. funkci $\mathbf{g} = 1/D$. Pak pro $\mathbf{u} = D$ máme $\mathbf{v} = \mathbf{ug} = 1$. Odpovídající kódovač má tedy v čase nula vrátit jedničku, pokud na vstupu v čase jedna bude jednička, jinak nulu. Je zřejmé, že takový kódovač nemůže existovat. S použitím naší terminologie vidíme, že řada $\mathbf{g}$, musí být kauzální, resp. realizovatelná (je totiž racionální). To ukazuje původ termínu realizovatelná funkce.

Chceme tedy nyní najít kódovač, který „realizuje" nějakou realizovatelnou racionální funkci. To bude kódovač $K$ s parametry $(1,1)$ a odezvou

$$K(1) = \frac{\mathbf{p}}{\mathbf{q}}\,,$$

kde

$$\mathbf{p} = p_0 + p_1 D + \cdots + p_m D^m, \qquad \mathbf{q} = 1 + q_1 D + \cdots + q_m D^m\,.$$

Poznamenejme, že předpoklad $q_0 = 1$ není na újmu obecnosti. Pro realizovatelnost racionální funkce jsme sice požadovali pouze, aby $q_0$ bylo nenulové, ale rozšíříme-li zlomek prvkem $q_0^{-1} \in \mathbb{F}$, dostaneme požadovaný tvar.

Nyní již můžeme formulovat následující zásadní větu.

**Věta.** *Nechť je $K$ konvoluční kódovač stupně $m$ s přechodovou funkcí*

$$(\vec{s}_i, u_i) \mapsto \vec{s}_{i+1} = \left( u_i - \sum_{j=1}^{m} q_j s_i^{(j)}, s_i^{(1)}, \ldots, s_i^{(m-1)} \right)$$

*a výstupní funkcí*

$$(\vec{s}_i, u_i) \mapsto \; p_0 u_i + \sum_{j=1}^{m} (p_j - p_0 q_j) s_i^{(j)} = p_0 s_{i+1}^{(1)} + \sum_{j=1}^{m} p_j s_i^{(j)}\,.$$

*Pak platí*

$$K(\mathbf{u}) = \mathbf{u} \cdot \frac{\mathbf{p}}{\mathbf{q}}\,.$$

*Důkaz.* Označme $\sigma_i = s_{i+1}^{(1)}$ a nechť $\mathbf{s}$ je generující řada posloupnosti $(\sigma_i)_{i=1}^{\infty}$. Z definic dostáváme

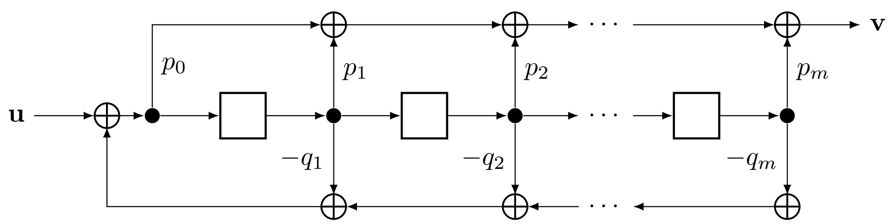
$$u_i = \sigma_i + \sum_{j=1}^{m} q_j \sigma_{i-j}, \qquad\qquad v_i = \sum_{j=0}^{m} p_j \sigma_{i-j},$$

pro všechna $i \in \mathbb{Z}$, tedy

$$\mathbf{u} = \mathbf{s} \cdot \mathbf{q}, \qquad\qquad \mathbf{v} = \mathbf{s} \cdot \mathbf{p},$$

z čehož tvrzení plyne. □

Násobení racionální funkcí $\mathbf{p}/\mathbf{q}$ je tedy realizováno následujícím obvodem:




Matice kódovače (příklad pro $m = 5$) jsou

$$\mathcal{A} = \begin{pmatrix} -q_1 & 1 & 0 & 0 & 0 \\ -q_2 & 0 & 1 & 0 & 0 \\ -q_3 & 0 & 0 & 1 & 0 \\ -q_4 & 0 & 0 & 0 & 1 \\ -q_5 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathcal{B} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathcal{C} = \begin{pmatrix} p_1 - p_0 q_1 \\ p_2 - p_0 q_2 \\ p_3 - p_0 q_3 \\ p_4 - p_0 q_4 \\ p_5 - p_0 q_5 \end{pmatrix}$$

$$\mathcal{D} = \begin{pmatrix} p_0 \end{pmatrix}$$

Kombinací takovýchto kódovačů pro jednotlivé indexy generující matice dostaneme fyzickou podobu kódovače příslušného kódu. Z hlediska velikosti kódovače je výhodné sloučit kódovače se stejným vstupem do kódovače se společnou zpětnou vazbou a $c$ výstupy. K tomu je třeba převést indexy v každém jednotlivém řádku na společného jmenovatele. Takto získámé tzv. *přímou formu* (nazývá se také „kontrolorova normální forma“) konvolučního kódovače dané generující matice sestávající z $b$ registrů.

Pro odpovídající generující matici

$$\mathbf{G} = \left( \frac{\mathbf{p}_{i,j}}{\mathbf{q}_i} \right)_{b \times c},$$

definujme *stupeň $i$-tého řádku* jako

$$\nu_i = \max\{\deg(\mathbf{p}_{i,1}), \deg(\mathbf{p}_{i,2}), \ldots, \deg(\mathbf{p}_{i,c}), \deg(\mathbf{q}_i)\}.$$

Součet

$$\nu = \sum_{i=1}^{b} \nu_i$$

nazýváme *vnější stupeň* matice $\mathbf{G}$, značíme $\operatorname{extdeg} \mathbf{G}$. Z definic plyne, že vnější stupeň matice je současně stupněm přímé formy kódovače.

Chceme-li vnější stupeň minimalizovat, hledáme pro daný kód $\mathcal{C}$ bázi s co nejmenšími stupni. Z definice je zřejmé, že stupně se nezvýší (a kód se nezmění) pokud položíme všechny jmenovatele rovny jedné, tedy pokud budeme uvažovat pouze matice nad $\mathbb{F}[D]$ (tedy kódovače bez zpětné vazby). Bez újmy na obecnosti také předpokládejme, že řádky jsou seřazeny tak, aby $\nu_1 \leq \nu_2 \leq \cdots \leq \nu_b$ a vektor $(\nu_1, \nu_2, \ldots, \nu_b)$ nazvěme vnější charakteristikou matice (resp. báze) $\mathbf{G}$. Následující tvrzení ukazuje, že vnější charakteristika báze s minimálním vnějším stupněm je pro daný kód určena jednoznačně.

*Lemma.* Nechť je $(\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_b)$ báze $\mathcal{C}$ s lexikograficky nejmenší vnější charakteristikou. Jinak řečeno, je to báze zvolená následujícím „hladovým“ postupem: za $\mathbf{g}_i$ volíme nějaký polynomiální vektor z $\mathcal{C} \setminus \langle \mathbf{g}_1, \ldots, \mathbf{g}_{i-1} \rangle$ s nejmenším možným stupněm $\nu_i$. Pak pro libovolnou bázi $(\mathbf{g}'_1, \mathbf{g}'_2, \ldots, \mathbf{g}'_b)$ kódu $\mathcal{C}$ s vnějším stupněm $(\nu'_1, \nu'_2, \ldots, \nu'_b)$ platí $(\nu_1, \nu_2, \ldots, \nu_b) \leq (\nu'_1, \nu'_2, \ldots, \nu'_b)$ (čímž je míněno, že platí $\nu_i \leq \nu'_i$ pro všechna $i = 1, 2, \ldots, b$).

*Důkaz.* Množina $\mathcal{C} \setminus \langle \mathbf{g}_1, \ldots, \mathbf{g}_{i-1} \rangle$ obsahuje alespoň jeden z vektorů $\mathbf{g}'_1$, $\mathbf{g}'_2, \ldots, \mathbf{g}'_i$, z čehož $\nu_i \leq \nu'_i$ plyne. □

Jednoznačně daná přirozená čísla $\nu_1, \nu_2, \ldots, \nu_b$ z předchozího tvrzení se nazývají *Forneyho indexy* kódu $\mathcal{C}$ a jejich součet $\nu$ se nazývá *stupeň kódu* $\mathcal{C}$, značíme $\deg \mathcal{C}$. Stupeň kódu je tedy roven nejmenšímu možnému vnějšímu stupni jeho generující matice, a tedy zároveň stupni přímé formy kódovače takovou maticí definovaného.