

Cvičení - kapacita kanálu

Michal Kupsa, Štěpán Holub

V tomto cvičení uvažujeme pouze bezpaměťové kanály (vyjma bodu 4c). Připomeňme působení takového kanálu na náhodný vstup. Máme náhodnou veličinu S s hodnotami v A a její výstup pošleme kanálem Γ . Tím vznikne náhodná veličina $R = \Gamma(S)$, která reprezentuje výstup. Kanál a vstup zcela determinují rozložení R , ale také vzájemné rozložení R, S , konkrétně

$$\mathbb{P}(S = a, R = b) = \mathbb{P}(S = a) \cdot \mathbb{P}(\Gamma(a) = b),$$

t.j.

$$\mathbb{P}(R = b \mid S = a) = \mathbb{P}(\Gamma(a) = b), \quad \text{pokud } \mathbb{P}(S = a) > 0.$$

Bezpaměťový kanál budeme popisovat maticí příslušných pravděpodobností $\mathbb{P}(\Gamma(a) = b)_{(a,b) \in A \times B}$.

Připomeňme, že

$$I(X : Y) = \mathcal{H}(Y) - \mathcal{H}(Y \mid X)$$

$$\mathcal{H}(Y \mid X) = \sum_{a \in A} \mathbb{P}(X = a) \cdot \mathcal{H}(Y \mid X = a)$$

$$\mathcal{H}(Y \mid X = a) = - \sum_{b \in B} \mathbb{P}(Y = b \mid X = a) \cdot \log \mathbb{P}(Y = b \mid X = a).$$

1. Uvažujme kanál daný maticí

$$\Gamma \sim \begin{pmatrix} 0.5 & 0.5 \\ 0 & 1 \end{pmatrix}$$

s binární abecedou pro vstup i výstup.

- (a) Pro vstup S s uniformním rozdělením najděte sdružené rozdělení (S, R) , kde $R = \Gamma(S)$. Najděte rozdělení R .
- (b) Určete $\mathcal{H}(R \mid S)$, $\mathcal{H}(R)$ a $I(R : S)$. Co výsledek říká o $C(\Gamma)$?
- (c) Změňte S tak, aby $\mathcal{H}(R \mid S)$ bylo minimální. Jaké je v takovém případě $I(R : S)$? Říká to něco nového o $C(\Gamma)$?
- (d) Změňte S tak, aby $\mathcal{H}(R)$ bylo maximální. Jaké je v takovém případě $I(R : S)$? Říká to něco nového o $C(\Gamma)$?

2. Uvažujme kanál daný maticí

$$\Gamma \sim \begin{pmatrix} 0.5 & 0.25 & 0.25 \\ 0.5 & 0.25 & 0.25 \end{pmatrix}$$

z binární do ternární abecedy. Řešte otázky z předchozího bodu. Určete kapacitu kanálu a zdroj který ho maximalizuje.

3. Uvažujme kanál daný maticí

$$\Gamma \sim \begin{pmatrix} 0.5 & 0.25 & 0.25 \\ 0.25 & 0.5 & 0.25 \end{pmatrix}$$

z binární do ternární abecedy. Určete kapacitu kanálu a zdroj který ho maximalizuje.

4. Uvažujme kanál daný maticí

$$\Gamma \sim \begin{pmatrix} 0.5 & 0.5 & 0 & 0 \\ 0 & 0.5 & 0.5 & 0 \\ 0 & 0 & 0.5 & 0.5 \\ 0.5 & 0 & 0 & 0.5 \end{pmatrix}$$

z abecedy $A = \{a, b, c, d\}$ do sebe.

- (a) Navrhněte kódování $f : \{0, 1\} \rightarrow A$ a dekódování $\hat{f} : A \rightarrow \{0, 1\}$ tak, aby se z výstupu kanálu dalo s jistotou určit, zda byla poslána nula nebo jednička.
- (b) Pokud to lze, co to vypovídá o kapacitě kanálu?
- (c) Pokud zakódujeme A jako $\{00, 01, 10, 11\}$, lze Γ chápat jako dvojnásobné použití binárního kanálu. Ukažte, že Γ není bezpaměťový, tedy že ho nelze napsat jako Γ_0^2 pro žádné Γ_0 .

Řešení a komentář

Abeceda bude vždy sestávat z počátečních nezáporných přirozených čísel $0, 1, \dots, n-1$. Funkce h značí funkci definovanou předpisem $h(x) = -x \log x - (1-x) \log(1-x)$, tedy je to entropie náhodné veličiny s hodnotami v $\{0, 1\}$ takové, že $\mathbb{P}(X = 0) = x$. Budeme také psát $\mathcal{H}(p_1, p_2, \dots, p_n)$ pro pravděpodobnostní vektor. Takový zápis odpovídá entropii veličiny o příslušném rozdělení.

1. Označme $p_i = \mathbb{P}(S = i)$, $p := p_0$. Lze obecně dopočítat, v závislosti na těchto parametrech:

S	$P_{R S}$		$\mathcal{H}(R S = a)$	P_S	$P_{S,R}$		P_R
	0	1			0	1	
0	0.5	0.5	1	p	$0.5p$	$0.5p$	$0.5p$
1	0	1	0	$1-p$	0	$1-p$	$1-0.5p$

$$\mathcal{H}(R | S) = 1 \cdot p + 0 \cdot (1-p) = p$$

$$\mathcal{H}(R) = \mathcal{H}(0.5p, 1-0.5p) = h(0.5p)$$

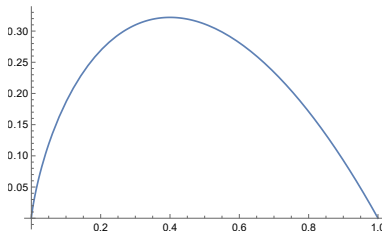
$$\mathcal{I}(S : R) = \mathcal{I}(p) := h(0.5p) - p$$

- (a) Pro vstup S s uniformním rozdělením,

$P_{R,S} :$	s	0	1
	0	1/4	1/4
	1	0	1/2
	P_R	0.25	0.75

- (b) Pro vstup S s uniformním rozdělením, $\mathcal{H}(R|S) = 0.5$, $\mathcal{H}(R) = h(0.25) \doteq 0.81$ a $\mathcal{I}(R : S) \doteq 0.31$. Z toho dostáváme, $C(\Gamma) \geq 0.31$.
- (c) $\mathcal{H}(R | S) = p$ bude minimální, pokud $p = 0$, neboli $\mathbb{P}(S = 0) = 0$, $\mathbb{P}(S = 1) = 1$. Obecně, dáváme maximální pravděpodobnost (tedy jedničku) tomu vstupu, jehož řádek v Γ má nejmenší entropii. Entropie toho řádku se tak stane entropií $\mathcal{H}(R | S)$. V našem případě platí $\mathcal{H}(R) = 0$, proto $\mathcal{I}(R : S) = 0$. Tedy $C(\Gamma) \geq 0$, ale to platí obecně.
- (d) $\mathcal{H}(R) = \mathcal{H}(0.5p, 1-0.5p)$. Zde se dá nastavit $p = 1$, t.j. $\mathbb{P}(S = 0) = 1$, $\mathbb{P}(S = 1) = 0$, abychom dostali uniformní rozdělení pro R . To má pak maximální entropii (ne vždy lze nastavit zdroj tak, aby byl výstup uniformní - srovnejte s dalšími příklady). Pro tuto volbu je $\mathcal{H}(R) = 1$, $\mathcal{H}(R | S) = 1$, $\mathcal{I}(R : S) = 0$. Tedy opět dostáváme triviální dolní odhad pro kapacitu $C(\Gamma) \geq 0$.

Tento příklad ukazuje, že při maximalizaci $I(R : S) = H(R) - H(R | S)$ nelze optimalizovat jeden ze činitelů bez ohledu na druhý. Graf funkce $I(p)$ vypadá takto:



Maximum se nabývá pro $p = 0.4$ a má hodnotu zhruba 0.322.

2. Kanál má všechny řádky stejné, čímž naznačuje, že mu vůbec nezáleží na vstupu. Výpočtem se ukáže, že opravdu nepřenáší žádnou informaci (pro žádný zdroj). Kromě výpočtů entropií můžeme přímo dokázat, že jsou vstup a výstup nezávislé. Platí

$$H(R | S) = H(0.5, 0.25, 0.25) \cdot p_0 + H(0.5, 0.25, 0.25) \cdot p_1 = H(0.5, 0.25, 0.25) = 1.5$$

$$H(R) = H(0.5, 0.25, 0.25) = 1.5$$

$$I(R : S) = 0.$$

Bez ohledu na vstup má výstup konstantní entropii i podmíněnou entropii a vzhledem k nulové vzájemné informaci je nezávislý na vstupu. Kapacita kanálu je nulová (zde již nejde o dolní odhad, protože nulovou vzájemnou informaci dostáváme pro jakýkoliv zdroj). Této kapacity přirozeně dosahuje jakékoliv rozdělení na vstupu.

Dá se ukázat, že nulovou kapacitu má kanál právě tehdy, když má všechny řádky totožné.

3. Řádky v Γ mají stejnou entropii (jsou jen propermutované), proto podmíněná entropie $H(R | S)$ nezávisí na zdroji S , konkrétně

$$\begin{aligned} H(R | S) &= H(0.5, 0.25, 0.25) \cdot p_0 + H(0.5, 0.25, 0.25) \cdot p_1 = \\ &= H(0.5, 0.25, 0.25) = 1.5 \end{aligned}$$

Dá se lehce nahlédnout, že je podmíněná entropie nezávislá na volbě zdroje právě tehdy když mají všechny řádky v Γ stejnou entropii (toho lze docílit i jinak, než jen permutací). Potom je maximalizace vzájemné informace totožná s maximalizací entropie výstupu R . V tomto případě,

$$P_R = (r_0, r_1, r_2) = (0.5p + 0.25(1 - p), 0.25p + 0.5(1 - p), 0.25).$$

Je vidět, že třetí složka nezávisí na zdroji. Intuice by měla radit, snažit se o co nejrovnoměrnější rozdělení na té části, na kterou máme vliv. To potvrzuje

následující obecný výpočet: Nejprve označme $r = r_0 + r_1$, potom

$$\begin{aligned}\mathcal{H}(R) &= -r_0 \log r_0 - r_1 \log r_1 - r_2 \log r_2 \\ &= r \left(-\frac{r_0}{r} \log r_0 - \frac{r_1}{r} \log r_1 \right) - r_2 \log r_2 \\ &= r \left(-\log r - \frac{r_0}{r} \log \frac{r_0}{r} - \frac{r_1}{r} \log \frac{r_1}{r} \right) - r_2 \log r_2 \\ &= r \mathcal{H} \left(\frac{r_0}{r}, \frac{r_1}{r} \right) - r \log r - r_2 \log r_2.\end{aligned}$$

Jelikož jsou $r = 0.75$ a $r_2 = 0.25$ konstanty, je třeba maximalizovat entropii $\mathcal{H}(\frac{r_0}{r}, \frac{r_1}{r})$. Ideální by bylo (nelze vždy), kdyby se jednalo o uniformní rozdělení, tedy $r_0 = r_1$. Toho v tomto případě lze dosáhnout, neboť rovnice

$$0.5p + 0.25(1 - p) = 0.25p + 0.5(1 - p)$$

má řešení. Konkrétně má řešení jediné, $p = 1/2$. Vzájemní informace (a zároveň entropie výstupu) bude největší v případě rovnoměrného rozdělení na vstupu, $\mathbb{P}(S = 0) = 0.5$ a $\mathbb{P}(S = 1) = 0.5$. Pro tento zdroj platí

$$C(\Gamma) = I(R : S) = \mathcal{H}(0.375, 0.375, 0.25) - \mathcal{H}(0.5, 0.25, 0.25) \doteq 0.06.$$

4. (a) Při požadavku na přesné dekódování se snažíme vybrat maximální množinu vstupů tak, aby se možné výstupy pro ně nepřekrývaly. Možné výstupy přečteme z Γ . Zde můžeme například volit $\{a, c\}$, protože a a c se nemohou zobrazit na stejný výstup. Kódování pak je

$$f(0) = a, f(1) = c, \quad \hat{f}(a) = 0, \hat{f}(b) = 0, \hat{f}(c) = 1, \hat{f}(d) = 1.$$

- (b) Pokud lze kanálem bezchybně přenést abecedu velikosti n , je kapacita kanálu rovna přinejmenším $\log n$. To lze ukázat tím, že budeme volit zdroj S rovnoměrně rozložený na vybraných písmenech, v našem případě a a c (nebo b a d). Vzhledem k dekódovatelnosti musí být $\mathcal{H}(S | R) = 0$ (S je funkcí R při zpětném dekódování). Z toho plyne

$$\log n = \mathcal{H}(S) = \mathcal{H}(S) - \mathcal{H}(S | R) = I(S : R).$$

Tedy kapacita kanálu je větší než $\log n$. V našem konkrétním případě tedy $C(\Gamma) \geq \log 2 = 1$. Zároveň se dá spočítat kapacita kanálu tak, jako v případě tři. Vyjde $C(\Gamma) = \log 2 = 1$.

- (c) Nechť

$$\Gamma' \sim \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Pak matice pravděpodobností pro průchod slov délky 2, vypadá následovně

$$\Gamma'_0 \Gamma'_1 \sim \begin{pmatrix} aa & ab & ba & bb \\ ac & ad & bc & bd \\ ca & cb & da & db \\ cc & cd & dc & dd \end{pmatrix}$$

. V prvním řádku např. vidíme, že $\mathbb{P}(\Gamma'(00) = 01) = \mathbb{P}(\Gamma'(00) = 10)$. To by pro původní kanál znamenalo, že $\mathbb{P}(\Gamma(a) = b) = \mathbb{P}(\Gamma(a) = c)$, což není pravda.

Obecně platí, že působení bezpaměťového kanálu na slova délky n , respektive rozložení možných výstupů, je možno zapsat maticí, která je tzv. *Kroneckerovým* či *tensorovým* součinem matic pro jednotlivé přenosy (takto lze definovat i kanál, který není časově invariantní). Tento součin je definovaný (na příkladu matice A typu 2×3 a matice B typu $m \times n$) jako matice

$$A \otimes B = \begin{pmatrix} a_{11} \cdot B & a_{12} \cdot B & a_{13} \cdot B \\ a_{21} \cdot B & a_{22} \cdot B & a_{23} \cdot B \end{pmatrix}$$

typu $2m \times 3n$. V případě matice Γ by matice

$$\begin{pmatrix} 0.5 & 0.5 \\ 0 & 0.5 \end{pmatrix} \quad \text{a} \quad \begin{pmatrix} 0 & 0 \\ 0.5 & 0 \end{pmatrix}$$

musely být násobkem téže matice. Matice Γ tedy není tensorově rozložitelná, a příslušný kanál tedy není bezpaměťový, ani když odstraníme podmínku časové invariance.