Teorija informacij in sistemov, predavanje 6

Uroš Lotrič

Univerza v Ljubljani,
Fakulteta za računalništvo in informatiko

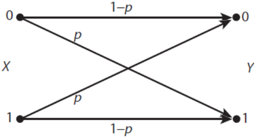
4.6 Kapaciteta kanala 1

- Shannonov najpomembnejši in najbolj presenetljiv rezultat je, da je zanesljiva komunikacija skozi nezanesljiv kanal, v katerem prihaja do napak, mogoča.
- **Kapaciteta kanala** je največja možna medsebojna informacija, ki jo lahko prenesemo od vhoda na izhod.

$$C = \max_{P(X)} I(X;Y)$$

4.6 Kapaciteta kanala 2

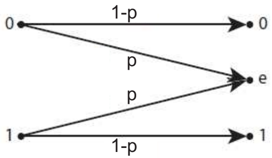
- Primer: binarni simetrični kanal



  - $C = \max_{P(X)} I(X;Y) = \max_{P(X)}(H(Y) - H(Y|X))$
  - $p(x_0) = \alpha, p(x_1) = 1 - \alpha$
  - $I(X;Y) = H(Y) - H(Y|X) = \ldots = H(Y) - H(p, 1-p)$
  - $\frac{dI(X;Y)}{d\alpha} = 0$ (naloga)
  - lahko sklep: C je max, ko je $H(Y) = 1$
  - $C = I(X;Y)|_{\alpha=1/2} = 1 - H(p, 1-p)$

4.6 Kapaciteta kanala 3

- Primer: binarni kanal z brisanjem



$$P_k = \begin{pmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{pmatrix} \quad .$$

- $p(x_0) = \alpha, p(x_1) = 1-\alpha$
- $p(y_0) = (1-p)\alpha, p(y_1) = p, p(y_2) = (1-p)(1-\alpha)$
- $I(X;Y) = (1-p)H(\alpha, 1-\alpha)$
- $dI(X;Y)/d\alpha = 0 \rightarrow \alpha = 1/2$
- $C = 1-p$

4.7 Shannonov drugi teorem 1

- Shannon je ugotovil, da nam združevanje znakov v nize daje več možnosti za doseganje zanesljivega prenosa.
- Naj bo M število različnih kodnih zamenjav, ki jih lahko oblikujemo z nizi dolžine n.
- **Hitrost koda** (prenosa) je definirana kot

$$R = \frac{\max H(X^n)}{n} = \frac{\log M}{n}$$

  Hitrost je največja takrat, ko so dovoljene kodne zamenjave na vhodu enako verjetne.
- Primer: binarno: Če je $M = 2^k$, $k \leq n$, je hitrost prenosa $R = \frac{k}{n}$.

4.7 Shannonov drugi teorem 2

- Shannonov teorem pravi, da je možna skoraj popolna komunikacija s hitrostjo, enako kapaciteti kanala.
- **Za $R \leq C$ obstaja kod, ki zagotavlja tako prevajanje informacije, da je verjetnost napake pri dekodiranju poljubno majhna. Za $R > C$, kod, ki bi omogočal prevajanje informacije s poljubno majhno verjetnostjo napake, ne obstaja.**
- Kdaj v teoremu namesto R nastopa H. Če so znaki neodvisni, je $\log H(X^n) = n \log H(X) \to R = H$.
- Lahko si pomagamo z znanimi enačbami: $C = \max_{P(X)} I(X;Y) = I(X;Y) + \varepsilon = H(X) - H(X|Y) + \varepsilon \to H(X|Y) = H(X) - C + \varepsilon$ — iz Y nedvoumno določimo X samo kadar je dvoumnost $H(X|Y) = 0$. Torej $H(X) = C - \varepsilon \leq C$.

4.7 Shannonov drugi teorem 3

- Pri razlagi ideje se omejimo na binarni simetrični kanal. Kapaciteta kanala je $C = 1 - H(p, 1-p)$
- Tako kot pri prvem teoremu tudi tu znake sestavljamo v nize dolžine n. Obstaja 2^n blokov na vhodu in na izhodu.
- Verjetnost za napako pri prenosu znaka je p. V bloku (nizu) je lahko napačnih np znakov. Blokov z np napakami je $\binom{n}{np} = \frac{n!}{(np)!(n-np)!}$
- Vzamemo Stirlingovo aproksimacijo $z! \approx z^z$ in dobimo $\log \binom{n}{np} = nH(p, 1-p)$
- Zaradi napak dobimo $\binom{n}{np} = 2^{nH}$ zelo sorodnih nizov.
- Če želimo rekonstrukcijo kljub napakam, se sorodni nizi različnih kodnih zamenjav ne smejo prekrivati med seboj. Torej lahko uporabljamo največ $M \leq 2^n / 2^{nH} = 2^{n(1-H)} = 2^{nC}$ različnih nizov.
- Torej je za $R \leq \frac{\log 2^{nC}}{n} = C$ možno najti kodne zamenjave, ki omogočajo zanesljivo komunikacijo.