1 Uvod

2 Entropija

3 Informacija

4 Diskretni vir informacije

Definicija diskretnega kanala 18

Diskretni kanal je dinamičen naključen sistem, ki oddaja znake v diskretnem času na osnovi neke verjetnostne porazdelitve.

Opišemo ga lahko na 2 načina:

- **množica nizov**: vsakemu nizu z dolžino n iz množice nizov A^n pripada verjetnost $P(A^n)$
- **časovni proces**: sekvenca naključnih spremenljivk in verjetnost, da vir oddaja določeno sekvenco $P(x_1 , \dots , x_n)$

Ergodični viri 19

Vir je ergodičen, če je njegovo statistično povprečje enako časovnemu povprečju. Vsak niz Y dolžine m v nizu X dolžine n ima relativno pogostost enako $P(Y)$, ko $n \to \infty$.

Ergodični viri imajo en sam način delovanja.

Za vse ergodične vire velja **AEL**. Nize, ki jih vir oddaja lahko tako razdelimo v dve množici – tipično in atipično.

Tipični in atipični nizi 21

Število tipičnih nizov je enako $\boldsymbol{P = 2^{-nH}}$.

Kaj je lastnost Markovskih procesov? 22

Vir Markovova spada pod vire s spominom. Zadnji oddani znak je odvisen od predhodnega, torej je

$$\boldsymbol{P(X_n=x_j \mid X_1=x_k , \dots , X_{n-1}=x_i) = P(X_n=x_j \mid X_{n-1}=x_i) = q_{ij}}$$

Matrični zapis je v tem primeru

$$\boldsymbol{P_n = Q^T * P_{n-1}}$$

oziroma kadar imamo opravka z stacionarnimi viri

$$\boldsymbol{P = Q^T * P}$$

Entropija Markovega vira 23

Entropija vsakega stanja je enaka entropiji vrstice

$$\boldsymbol{H_i = - K * \sum_j q_{ij} * \log_d(q_{ij})}$$

Entropija Markovovega vira je torej

$$\boldsymbol{H = \sum_i p_i * H_i}$$

5 Kodiranje vira informacij

Kraftov izrek 27

Potreben in zadosten pogoj za obstoj trenutnega koda:

$$\boldsymbol{\sum_i b^{-ni} \leq 1}$$

b – velikost kodirne abecede

n_i – dolžine kodnih zamenjav

Velja tudi obratno: če dolžine zadoščajo neenačbi, je možno najti trenutni kod.

I. Shannonov teorem (kompresijski teorem) 27

Za diskretni stacionarni vir brez spomina velja:

Obstajajo kodi (**gospodarni**) kodi z enoznačno možnostjo dekodiranja, katerih povprečna dolžina $\tilde{n}$ je določena z:

$$\frac{H_1}{K * \log_d(b)} \leq \tilde{n} < \frac{H_1}{K * \log_d(b)} + 1$$

oziroma če je $K = 1$, $d = b = 2$:

$$H_1 \leq \tilde{n} < H_1 + 1$$

Entropija vira brez spomina za niz dolžine 1:

$$H_1 = -\sum_i p_i * \log(p_i)$$

Kadar s krajšimi kodami opišemo bolj verjetne vrednosti naključnih spremenljivk, govorimo o **podatkovni kompresiji**. Njena limita je **entropija**.

Optimalen kod je tisti izmed gospodarnih kodov, ki ima najmanjšo povprečno dolžino $\tilde{n}$.

Najmanjša dolžina $\tilde{n}$ je določena z:

$$\tilde{n} = \frac{H_1}{K * \log_d(b)}$$

iz tega sledi (če je $K = 1$, $d = b = 2$):

$$n_i = -\log_b(p_i)$$

kar imenujemo tudi **Shannonov kod**, saj določa optimalne dolžine kodnih zamenjav.

Shannon-Fanojev izrek 28

Shannonov kod ni vedno optimalen zaradi zaokroževalnih napak pri računanju posameznih dolžin kodnih zamenjav. **Shannon-Fanojev izrek** pravi, da se, če namesto posameznih znakov kodiramo bloke dolžine r, približamo spodnji meji za $\tilde{n}$.

Entropija blokov za vir brez spomina je enaka:

$$H(X_1, \ldots, X_r) = r * H_1$$

Če sedaj to ugotovitev vpeljemo v 1. Shannonov teorem o gospodarnih kodih:

$$\frac{r * H_1}{K * \log_d(b)} \leq \tilde{n}_r < \frac{r * H_1}{K * \log_d(b)} + 1$$

$$\frac{H_1}{K * \log_d(b)} \leq \frac{\tilde{n}_r}{r} < \frac{H_1}{K * \log_d(b)} + \frac{1}{r}$$

ker velja $\tilde{n} = \tilde{n}_r / r$

$$H_1 \leq \tilde{n} < H_1 + \frac{1}{r}$$

Iz tega sledaj sledi **Shannon-Fanojev izrek**:

$$\lim_{r \to \infty} \frac{\tilde{n}_r}{r} = \frac{H_1}{K * \log_d(b)}$$

oziroma če je $K = 1$ in $d = b = 2$

$$\lim_{r \to \infty} \tilde{n} = H_1$$

Gospodarnost kodov se povečuje s podalševanjem blokov znakov, ki jim prirejamo kodne zamenjave.

6 Komunikacijski kanal

Kako je definiran diskretni komunikacijski kanal? 33

Diskretni komunikacijski kanal je definiran s trojčkom $< U, P_k, V >$.

U – množica vhodnih znakov

V – množica izhodnih znakov

P_k – verjetnostna matrika kanala

Verjetnostna matrika kanala ima člene $\boldsymbol{a_{ij} = P(y_j \mid x_i) = p_{ij} / p_i}$.

Kapaciteta kanala 35

Definirana je kot $\boldsymbol{C = max\{ I(X ; Y) \}}$.

Zgornja meja je določena z $\boldsymbol{C_{max} = K * log_d(u)}$, spodnja meja pa je $\boldsymbol{C_{min} = 0}$.

u – število vrstic

Simetrični kanali imajo kapaciteto enako $\boldsymbol{C = K * log_d(v) + K * \sum_i r_i * log_d(r_i)}$.

r_i – verjetnosti v vrsticah

v – število stolpcev

Za določen binarni kanal povej kapaciteto kanala! 35

Če je simetričen, glej zgornjo enačbo. Če ni simetričen, je treba velik računat.

7 Kodiranje/dekodiranje kanala

Koliko napak lahko odkrijemo in koliko popravimo? ?

Odkrijemo lahko $\boldsymbol{E = d_{min} - 1}$.

Popravimo lahko $\boldsymbol{e = E / 2}$.

Pri čemer je d_{min} minimalna Hammingova razdalja.

Optimalno dekodiranje 43

Funkcija odločanja $g(y)$ lahko izbere x na dva načina

- Na osnovi **največje verjetnosti pravilne odločitve**

  $\boldsymbol{P (x \mid y) = max \{ P(x_i \mid y) \}}$

  Velja Bayesov teorem, zato je iskanje največje $P(x_i \mid y)$ enakovredno iskanju največje $P(y \mid x_i)$, s čimer pridemo do naslednjega načina.
- Na osnovi **največje aposteriorne verjetnosti**

  $\boldsymbol{P (y \mid x) = max \{ P(y_i \mid x) \}}$

  Če so vhodni vektorji enako verjetni $\boldsymbol{P(x_i) = 1 / M}$, sta obe funkciji odločanja enaki. Tedaj govorimo o **idealni funkciji odločanja**.

Bayesov teorem 43

$$\boldsymbol{P(x_i \mid y) = \frac{P(x_i) * P(y \mid x_i)}{P(y)}}$$

Torej je iskanje največje $P(x_i \mid y)$ enakovredno iskanju največje $P(y \mid x_i)$.

Idealna funkcija odločanja 43

Glej "Optimalno dekodiranje".

Hammingov pogoj 44

Hammingonov pogoj določa dolžino n kodnih zamenjav, ki omogočajo pri znanih M in e idealno funkcijo odločanja na strani dekodirnika (torej upošteva d_{min}):

$$\frac{2^n}{\sum_{i=0}^{e} \binom{n}{i}} \geq M$$

n – dolžina kodne zamenjave

e – povprečno število napak v kanalu

M – število različnih blokov ($M \leq b^k$)

II. Shannonov teorem (kanalski kodni teorem / eksistenčni teorem) 45

Govori o DK brez spomina in $C > 0$ ter o pogojih, pod katerimi je možno brez napak določiti poslano informacijo po kanalu s šumom.

$$0 < R < C$$

$$P^{max} \leq \delta + d^{-\rho n}$$

$$lim_{n \to \infty} P^{max} \rightarrow 0$$

$$M \leq d^{nR}$$

R – hitrost koda

C – kapaciteta kanala

n – dolžina koda

δ , ρ – poljubno majhni pozitivni števili

P^{max} – povprečje največjih verjetnosti napak kodov preko vseh $K(n , k)$

M – število kodnih zamenjav v množici K

d – osnova logaritma

Kaj je G in njena relacija z H? 54

G je generatorska matrika, s pomočjo katere lahko definiramo kodne zamenjave.

Relacijo med G in H opisuje $G * H^T = 0$. Iz te enačbe sledita relaciji

$H = [I_m \mid B] \rightarrow G = [B^T \mid I_k]$

$G = [I_k \mid A] \rightarrow H = [A^T \mid I_m]$

Velja tudi zveza med $g(p)$ in $h(p)$

$$g(p) * h(p) = p^n + 1$$

8 Kriptologija

9 Signali in sistemi

Kdaj je sistem linearen? 76

Linearni sistemi izpolnjujejo **princip superpozicije**. Če ga ne izpolnjuje, potem je sistem **nelinearen**.

Sistem je linearen, če velja

$$y(k) = \chi\{ \alpha_1 * x_1 (k) + \alpha_2 * x_2 (k) \} = \alpha_1 * y_1 (k) + \alpha_2 * y_2 (k)$$

pri čemer je

$$y_1 (k) = \chi\{ x_1 (k) \}$$

$$y_2 (k) = \chi\{ x_2 (k) \}$$

Kdaj je sistem časovno invarianten? 77

Za TI sisteme je značinlo, da se parametri s časom ne spreminjajo.

Če velja:

$$y(k) = \chi\{ x(k) \}$$

potem mora veljati tudi

$$y(k - n) = \chi\{ x(k - n) \}$$

Odziv na impulz 79

Sistem lahko določimo z odzivom na elementarni testni signal (enotin pulz $\delta(t)$).

Sistem je **kavzalen** ali **izvedljiv**, če njegov odziv ne prehiteva vhoda, ki ga povzroča, torej je $h(k) = 0 ; k < 0$.

Vhodni enotin pulz v času $i\ \delta(k - i)$ povzroči pri kavzalnem **TI** sistemu odziv v obliki skevence v času $i\ h(k - i)$. Pri **TV** sistemu bi povzročil $h(k , i)$.

Vzamemo poljubno sekvenco $x(k)$, ki vztopa v sistem in povzroči izhod $y(k)$. Zveza med vhodom $x(k)$, odzivom na enotin pulz $h(k)$ in $y(k)$:

$$x(k) = \sum_i x(i) * \delta(k - i) \quad \textbf{; vhod}$$

$$y(k) = \sum_i x(i) * h(k - i) \quad \textbf{; izhod}$$

Kako je definirana stabilnost? 82

Sistem je stabilen, če omejen vhod povzroči omejen izhod.

Pogoj za stabilnosti LTI sistema je:

$$\sum_i |h(i)| < \infty$$

10 Fourierova in Laplaceova transformacija

Dirichletovi pogoji 84

To so pogoji, katerim mora zadoščati periodična funkcija $f(t)$, da jo lahko razvijemo v **Fourierovo vrsto**.

1. Je enoznačna, za vsak t ima eno samo vrednost.
2. Je povsod končna, oz. če je kje neskončna, je tam integrabilna (npr. $\delta(t)$).
3. Je absolutno integrabilna v periodi oz. $\int_0^T |f(t)| * dt < \infty$.
4. V eni periodi ima končno število ekstremov.
5. Ima končno število nezveznosti v eni periodi.

Pri **Fourierovi transformaciji** so pogoji še ostrejši, saj imamo opravka z neskončnim intervalom

$$\int_{-\infty}^{\infty} |f(t)| * dt < \infty$$

Območje konvergence pri Laplaceu 86

Območje konvergence je pomembno pri inverzni Laplaceovi preslikavi.

Inverzni Laplaceov transform je enak

$$f(t) = \frac{1}{2*\pi*j} \int_{c-j\infty}^{c+j\infty} F(s) * e^{st} * ds$$

V tej enačbi mora c ležati v območju konvergence, kjer velja

$$\int_{-\infty}^{\infty} |f(t * e^{-\omega t})| * dt < \infty$$

11 Sistemska prenosna funkcija

Kaskadna in paralelna prenosna funkcija 89

Prenosno funkcijo lahko zapišemo v eni ali drugi obliki.

Kaskadna oblika:

$$H(s) = \frac{\prod_i (s - \beta_i)}{\prod_i (s - \alpha_i)}$$

α_i - pol

β_i - ničla

Paralelna oblika:

$$H(s) = \sum_i \frac{R_i}{(s - \alpha_i)}$$

α_i - pol

R_i - residuum pri polu α_i

Cauchyjev integralski teorem 91

Integral analitične (odvedljive) funkcije *f(z)* po krivulji *c* (sklenjena, ne gre skozi noben pol α_i) v z-ravnini je enak vsoti residuumov funkcije *f(z)* pri polih α_i znotraj *c*:

$$\int_c f(z) * dz = 2\pi j * \sum_i res\ f(z)\ pri\ polih\ \alpha_i$$

Poli α_i so znotraj *c*.

Uporabimo ga nad inverzno Laplaceovo transformacijo (residualna metoda).

12 Vzorčenje in Z-transformacija

III. Shannonov teorem (semplirni teorem) 95

Podaja spodnjo mejo vzorčenja.

Če je pasovno omejen signal *f(t)* sempliran s frekvenco $\omega_s \geq 2 * \omega_h$, potem semplirne vrednosti vsebujejo vso infromacijo iz zveznega signala. To pomeni, da lahko rekonstruiramo *f(t)* in *f(kT)* s formulo:

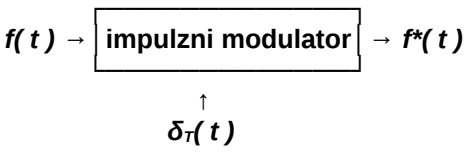
$$f(t) = \sum_k f(kT) * \frac{sin(\omega_s * (t - kT)/2)}{\omega_s * (t - kT)/2}$$

Minimalno semplirno frekvenco imenujemo tudi **Nyquistova frekvenca** za opazovani zvezni signal.

Idealna semplirna funkcija omogoča zapis semplirne funkcije.

$$\delta_T(t) = \sum_k \delta(t - kT)$$ (veriga enotinih pulzov)

Nariši impulzni modulator 96



Residualna metoda se uporablja za izračun inverzne Z transformacije.

Formula za pozitivne sekvece je

$$f(k) = Z^{-1}\{ F(z) \} = \sum res\{ F(z) * z^{k-1} \} \text{ pri polih } F(z) * z^{k-1} \text{ znotraj } c$$

Formula za negativne sekvece je

$$f(k) = Z^{-1}\{ F(z) \} = -\sum res\{ F(z) * z^{k-1} \} \text{ pri polih } F(z) * z^{k-1} \text{ znotraj } c$$