

Teorija
Informacij
in sistemov,
predavanje
1

ULotric

Uvod

O predmetu

Literatura

1.1

Informacija

1.2

Entropija

Teorija Informacij in sistemov, predavanje 1

Uroš Lotrič

Univerza v Ljubljani,
Fakulteta za računalništvo in informatiko

- ▶ **Temelji informacijske znanosti:**
 - ▶ **entropija:** matematična teorija komunikacije, informacijska teorija, biti, kodi, pasovne širine
 - ▶ **kriptologija:** matematične metode za varovanje podatkov (entropija, kompleksnost)
 - ▶ **širjenje informacij:** elektromagnetno, frekvenčni pasovi, filtriranje, vzorčenje, premiki, rekonstrukcija
 - ▶ **Obdelava podatkov:** kako organizirati in modelirati podatke, da iz njih potegnemo največ
 - ▶ **ekonomija:** informacija se ne izrabí, lahko se jo razmnožuje, kako jo proizvajati, širiti, ceniti, ...

Obravnavanje informacije s tehničnega vidika

- ▶ poudarek na poglavjih 1-3 (+4)
- ▶ teoretične vsebine: izrek/dokaz
 - ▶ **povprečna zmogljivost** (enostavno opisovanje več dogodkov)
 - ▶ **optimalnost** (nižja cena, največje stiskanje, največja prenosna hitrost)
 - ▶ **kompleksnost** (ogromno podatkov - hitri algoritmi ali čim bolj zapleteni algoritmi, da je težje razbiti kodo)
 - ▶ **strukture** (vektorji, matrike, sistemi enačb, drevesa)
- ▶ za inženirje pomembnejši praktični vidiki: dotaknili se jih bomo kjer bo le mogoče

Kako narediti predmet?

- ▶ prof: Lotrič, asistenta: Ilc, Sluga
- ▶ končna ocena = izpit + sprotno delo = 50 % + 50 %
 - ▶ Izpit: 25 % pisni + 25 % ustni
 - ▶ Sprotno delo: 25 % domače naloge + 25 % kolokvija
- ▶ predavanja + tedenski kvizi
- ▶ kolokvija (ocena sprotnega dela), nadomestek za pisni in ustni izpit
- ▶ vaje niso obvezne, obiskovanje vam olajša delo na domačih nalogah

Teorija
Informacij
in sistemov,
predavanje
1

ULotric

Uvod

O predmetu

Literatura

1.1
Informacija

1.2
Entropija

Literatura

- ▶ Luenberger: Information science, Princeton, 2006 (bo v knjižnici)
- ▶ van der Lubbe: Information theory, Cambridge, 1997
- ▶ Dobnikar: Teorija informacij in sistemov, FE in FRI, 2009
- ▶ Pavešić: Informacija in kodi, FE in FRI, 1997

- ▶ Hartley (1928): prvi poskus matematične formulacije informacije.
 - ▶ vsak znak sporočila je izbran iz množice n različnih znakov, ki so med seboj enakovredni
 - ▶ več kot je različnih znakov, več moramo povedati, da opišemo izbrani znak (met kovanca proti metu kocke)
 - ▶ l znakov $\rightarrow n^l$ možnosti, l -krat toliko informacije kot en sam znak

$$f(n^l) = l \cdot f(n)$$

Edina funkcija, ki temu ustreza je $K \log_b(n)$

- ▶ Shannon (1948): vsi znaki niso enako verjetni. Manj verjetna sporočila nosijo več informacije kot bolj verjetna

- ▶ Definicija lastne informacije: $I = \log_b(1/p) = -\log_b(p)$
Enota: 2: bit, 3: trit, e: nit, 10: Hartley
- ▶ Dogovor: $\log = \log_2$, drugače od običajno $\log = \log_{10}$!!!
- ▶ Logaritmi in kalkulator:

$$\log_b x = \frac{\log_a x}{\log_a b}$$

- ▶ Odvod logaritma $d \ln(x)/dx = 1/x$
- ▶ Graf naravnega logaritma in tangenta $x - 1$ v točki $x = 1$
- ▶ Logaritem je monoton naraščajoča funkcija
 $\ln(x) \leq x - 1$
- ▶ Primer: pošten kovanec, padel je grb: $p = 1/2 \rightarrow I = 1$.
Sporočimo z enim znakom, ki ima lahko vrednost 0 ali 1.
- ▶ Aditivnost lastne informacije: pošten kovanec vržemo dvakrat, možni izdidi: CC, CG, GC, GG. Padli sta dve cifri (CC), $p = 1/4 \rightarrow I = 2$ bit.

- ▶ **Lastna informacija** opisuje dogodek, ki se je zgodil, **Entropija** je ocena za informacijo, ki jo lahko sprejmemo v prihodnosti.
- ▶ Je povprečna informacija, ki upošteva vse možne izide
- ▶ Je mera za nedoločenost dogodka
- ▶ Naključna spremenljivka X zavzame stanja $\{x_1, x_2\}$ z neko verjetnostjo $\{p, 1 - p\}$.
$$I_1 = -\log(p), I_2 = -\log(1 - p), \bar{I} = pI_1 + (1 - p)I_2.$$
$$H(X) = -p \log p - (1 - p) \log(1 - p)$$
- ▶ **graf odvisnosti** (zvezna, simetrična, maksimum, minimum)
- ▶ primer: kovanec, $p = 1/2$, $H(X) = 1$
- ▶ primer: pozimi vroče/mraz: $p = 1/16$, $H(X) = 0.238$
- ▶ primer: luna danes pade na zemljo da/ne:
 $p = 0$, $H(X) = 0$, $0 \log 0 = 0$

Diskretni vir informacije

- ▶ Diskretni vir informacije X je dinamični, naključni (stohastični) sistem, v katerem se dogodki $\{x_1, x_2, \dots, x_n\}$ zgodijo z verjetnostmi $\{p_1, p_2, \dots, p_n\}$.
- ▶ $\sum_{i=1}^n p_i = 1, \forall i; 0 \leq p_i \leq 1$
- ▶ Lastna informacija dogodka i :
 $I_i = \log(1/p_i) = -\log(p_i)$
- ▶ Entropija je povprečje vseh lastnih informacij:

$$H(X) = \sum_{i=1}^n p_i I_i = - \sum_{i=1}^n p_i \log p_i$$

- ▶ označevanje

$$H(X) = H(P) = H(x_1, \dots, x_n) = H(p_1, \dots, p_n)$$

Lastnosti entropije

- ▶ je zvezna funkcija
- ▶ je simetrična - vrstni red p_i ni pomemben: seštevanje je komutativno
- ▶ je večja od 0: $p_i \geq 0 \rightarrow -p_i \log p_i \geq 0 \rightarrow H(X) \geq 0$
- ▶ je navzgor omejena z $\log n$ (dokaz z uporabo tangente na logaritem)

Lastnosti entropije

- ▶ je aditivna, če sta dogodka neodvisna
 $H(X, Y) = H(X) + H(Y)$: če vzamemo
 $X = \{x_1, \dots, x_n\}, P_X = \{p_1, \dots, p_n\},$
 $Y = \{y_1, \dots, y_m\}, P_Y = \{q_1, \dots, q_n\},$
 $P_{X \times Y} = \{\dots p_{ij} \dots\}, p_{ij} = p_i q_j$ vstavimo v en. entropije
(dokaz)
- ▶ v splošnem velja $H(X, Y) \leq H(X) + H(Y)$. Več o tem kasneje.
- ▶ poseben primer: več zaporednih dogodkov enega neodvisnega vira (ergodičnost, statistično in časovno povprečje sta enaka):
 $X^l = X \times \dots \times X \rightarrow H(X^l) = lH(X)$