

## ENTROPIJA:

$$H(X) = -\sum p_i \log(p_i) \text{ [bit]}$$

Primer:

X\Y	B	Č	pi
B	9/21	5/21	2/3=14/21
Č	5/21	2/21	1/3=7/21
p'j	2/3	1/3	1

$$H(X) = \rightarrow + \rightarrow = H(2/3, 1/3)$$

$$H(Y) = \downarrow + \downarrow = H(2/3, 2/3)$$

$$H(Y|X=b) = H(9/21 * 21/14, 5/21 * 21/14)$$

$$H(Y|X=\check{c}) = H(5/21 * 21/7, 2/21 * 21/7)$$

$$H(Y|X) = 2/3 * H(Y|X=b) + 1/3 * H(Y|X=\check{c})$$

**VEZANA ENTROPIJA** (to spodaj)

$$H(X, Y) = H(X) + H(Y|X)$$

$$= H(Y) + H(X|Y)$$

## POVPR. ŠT. BIN. VPR:

$$n = \sum p_i * n_i \text{ (} n_i = \text{št. Vpr)}$$

## ZVEZNA ENTROPIJA:

$$H(X) = -\int p(x) * \log(x) dx$$

-ploščina na grafu p(x) je 1

$$-0 * \log 0 = 0$$

## POVPR. LASTNA INF. = ENTROPIJA

$$I(X) = E\{I(X_i)\} = H(X)$$

## LASTNA INFORMACIJA ZNAKA:

$$I(x_i) = -\log(p_i)$$

## POVPR. MEDSEBOJNA INF:

(koliko inf. o dogodku X zvezo od Y)

$$I(X; Y) = H(X) - H(X|Y)$$

$$= H(Y) - H(Y|X)$$

$$H(X, Y) = H(X) + H(Y) - I(X; Y) \text{ (povezava)}$$

## RAZDALJA MED

## PORAZDELITVAMA

p...ocena, q...dejanska

$$D(p||q) = \sum p_{ij} * \log(p_{ij}/q_{ij})$$

-delimo celice na istem mestu iz dveh tab

## VIR INFORMACIJ

### 1) VIR BREZ SPOMINA

-njegova vrednost je neodvisna od tega

kaj se je dogajalo prej

$$H(x_1, \dots, x_n) = n * H(x_1)$$

-nedoločeno je enaka za en dogodek \*

toliko kot jih je

$$\text{Npr: } H(u) = 1,15b \dots H(u, u) = 2,30b$$

$mi = p_i * n$  ← značilno št. ponovitev =

tolikokrat se pojavi znak mi

$pz = 2^{-(n * H(x_i))}$  ← verjetnost za najbolj

značilne dogodke (tiste z največjo

verjetnostjo)

$$Nz = 2^{(n * H(x_i))} \leftarrow \text{število}$$

tipičnih/značilnih dogodkov

Npr: met goljuf. Kovanca: cifra: 0,2, gl.: 0,8

-entropija meta kovanca:  $H(0.2, 0.8) = 0,72b$

-znač. št. cifer v 15metih:

$$mz = p * n = 0,2 * 15 = 3$$

-verjetnost za znač. Dogodek:  $pz = 2^{-(n * H)}$

$$= 2^{-(15 * 0,72)}$$

-število značilnih dogodkov

## 2) MARKOVOV VIR – s spominom

$$[0, 4/5, 1/5]$$

$$Q = [1/2, 1/2, 0]$$

$$[1/2, 2/5, 1/10]$$

-novo stanje je odv. od prejšnjega

-imamo matriko prehodnih verjetnosti Q

Abeceda:  $X = \{a, b, c\}$

a) **SPREMINJANJE VERJETNOSTI** če je

$$P_0 = [1/3, 1/3, 1/3]^T$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}^T = \begin{bmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{bmatrix}$$

$$P_1 = Q^T * P_0$$

$$P_2 = Q^T * P_1 \dots$$

b) **DOLOČITEV STAC. VERJETNOSTI**

$$p = Q^T * p$$

$$[p_1] [0, 1/2, 1/2] [p_1]$$

$$[p_2] [4/5, 1/2, 2/5] [p_2]$$

$$[p_3] [1/5, 0, 1/10] [p_3]$$

Narediš enačbe + vzameš:  $p_1 + p_2 + p_3 = 1$

c) **ENTROPIJA VIRA BREZ SPOMINA**

(ki ima iste verjetnosti kot ta naš s

spominom)

$$H_b = H(1/3, 16/27, 2/27) \leftarrow \text{te vrednosti}$$

smo v b) dobili za  $p_1, p_2, p_3$

d) **ENTROPIJA MARKOVVEGA VIRA**

$$H_m = \sum p_i * H_i \text{ po } i\text{-ju, } H_i = -\sum q_{ij} * \log(q_{ij}) \text{ po } j$$

$$H_1 = H(0, 4/5, 1/5), H_2 = H(1/2, 1/2, 0) \text{ in še } H_3$$

$$H_m = 1/3 * H_1 + 16/27 * H_2 + 2/27 * H_3$$

e) **SKUPNA INF. DVEH ODD. ZNAKOV**

$$H(x_1, x_2) = H(x_1) + H(x_2|x_1) + H_m$$

$$\leftarrow H_b$$

## KODIRANJE - SHANNONOV KOD

a) **Je Shannonov kod optimalen?**

Veljati mora:  $H \leq \bar{n} \leq H + 1$

$$\bar{n} = \sum p_i * n_i \leftarrow \text{povpr. Dolž. Kod. Zamen.}$$

$$n_i = \lceil -\log(p_i) \rceil \text{ (navzgor zaokr.)}$$

Npr:  $P = \{1/2, 1/4, 1/8, 1/8\}$

$$n_1 = \lceil -\log(1/2) \rceil = 1, n_2 = 2, n_3 = 3$$

$$\bar{n} = 1/2 * 1 + 1/4 * 2 + 2 * 1/8 * 3 = 1,75$$

TOREJ JE OPTIMALEN

b) **Ali obstaja kod z dolžinami**

**zamenjav**  $\{1, 3, 3, 3, 3, 3\}$ ?  $B = \{0, 1\}$

b je torej 2

Da, če velja:  $\sum b^{(-n_i)} \leq 1 \dots$  če to

velja obstaja TRENUTEN kod

Npr:  $2^{(-1)} + 5 * 2^{(-3)} > 1 \dots$  ne obst

c) **Določanje Shannonov. koda**

$A = \{a, e, i, o, u\}$ ,  $P = \{0.3, 0.15, 0.10,$

$0.24, 0.21\}$ ,  $B = \{0, 1\}$

A	pi	Pi	ni	Zamen.
A	0,3	0	2	00
O	0,24	0,3	3	010
U	0,21	0,54	3	100
E	0,15	0,75	3	110
i	0,10	0,90	5	1110

$$n_i = \lceil -\log(p_i) \rceil$$

Pi pretvorimo v binarno

$$0,75(d) = ?(b) \rightarrow 0,75 * 2 = 1,50$$

$$0,50 * 2 = 1,00$$

$$0,00 * 2 = 0,00$$

$$0,75(d) = 0,100000 \dots (b) \rightarrow 3 \text{ znaki}$$

zaradi  $n_i = 3$ !!

## HUFFMANOV KOD

Združimo 2 najmanj verjetni

možnosti in seštejemo njuni verj.

Včasih dodamo še verjetnost 0.

## UČINKOVITOST KODA

$$\tau = H_b / \bar{n} = H_d / (\bar{n} * \log d) \dots d \text{ je}$$

nova osnova, npr 3

$$H = H(0.3, 0.15, 1.10,$$

$$0.24, 0.21) = 2,23 \text{ bit}$$

$$\bar{n} = 0,3 * 2 + 0,15 * 3 + \dots = 2,55$$

Potem pa samo deliš.

Če imamo  $B = \{1, 2, 3\}$  izračunamo

$\tau$  tako:  $\tau = H / \bar{n}$ , kjer je H izračunan

pri osnovi logaritma 3!

## DISKRETNi KOMUNIKAC.

### KANAL

Če je simetričen so vrstice

verjetnostne matrike kanala  $P_k$

samo različne razporeditve števil,

isto stolpci.

Npr:  $P_x = \{0.5, 0.4, 0.1\}$ , X-vh, Y-

izh

a) **Verjetnosti izhodnih znakov**

$$p' = P_k^A * P_x \dots P_x \text{ so verj. vh.}$$

znakov Rezultat:  $[0.39, 0.2, 0.41]$

b) **Povpr. Inf.vh. znakov H(X)**

$$H(X) = H(0.5, 0.4, 0.1)$$

c) **Povpr. Inf. izh. Znakov H(Y)**

$$H(Y) = H(0.39, 0.2, 0.41)$$

d) **Povpr. inf. potrebna za določitev izhoda znaka ko poznamo vhodnega**

$H(Y|X) = H(0.2, 0.1, 0.7) \leftarrow$  ni važno pri simetričnem katero komb. vzamemo

e) **Povpr. Inf ki se izgubi pri prenosu enega znaka  $H(X|Y)$ ?**

$H(X) + H(Y|X) = H(X, Y) = H(Y) + H(X|Y)$   
Rez:  $H(X|Y) = H(X) + H(Y|X) - H(Y)$

f) **Nedoločenost kanala  $H(X, Y)$**

$H(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$  (velja za sim)

g) **Povpr. Prenešana inf na znak**

$I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$  (velja za sim)

h) **KAPACITETA KANALA**

za simetričnega:  
 $C = \max\{H(p^1, \dots, p^v)\} - H(r_1, \dots, r_v)$   
Npr:  $C = \log 3 - H(0.2, 0.1, 0.7)$   
Log 3 zato ker imamo 3 elemente v eni vrstici

**DOPIŠI TO KAPACITETO ZA NESIMETRIČNE**

**VARNOSTNO KODIRANJE – LIN. BLOČNI KODI - L(n,k)**

$n = \text{št. znakov}, m = \text{št. var. bitov}, k = \text{št. podatkovnih bitov/osnovni bloki}$   
 $n = m + k$   
 $e = \text{številko napak}$   
KODNE ZAMENJAVE:  $z * G = x$

Naloga1: **Blok želimo var.kodirati z  $m=2,3,4,5$ biti. Kok dolgi morajo biti osn. bloki k da lahko odkr. In popravimo  $e=1$  ali  $e=2$  napaki?**  
 **$e=1$ :**  $2^m - 1 \geq n \dots$  vstaviš  $m=2$  in dobiš  $n=3$ . k pa dobiš z:  $k=n-m$ .  
 **$e=2$ :**  $2(2^m - 1) \geq n(n+1)$   
k ne sme pridet = 0  
Hitrost koda:  $r = k/n$

Naloga2: **3 inf.znakom(z) dodamo 3 var.znake s katerimi preverjamjo sodost med pari inf.znaki. x so kodne zamenjave.**

a) **En.za prev.sodosti:**  
 $4 = z_1 + z_1, x_5 = z_1 + z_3, x_6 = z_1 + z_3$   
-izdelamo tabelo:  $z_1, z_2, z_3, x_1, \dots, x_6$   
b) **Matrika za preverjanje sodosti H m vrstic=3, n stolpcev = 6**

VELJA:  $Hx^T = 0$ ,  
 $x_4 + x_1 + x_2 = 0 \quad [1 \ 1 \ 0 \ | \ 1 \ 0 \ 0]$   
 $x_1 + x_3 + x_5 = 0 \quad [1 \ 0 \ 1 \ | \ 0 \ 1 \ 0]$

c) **Gener. matrika: k vrstic, n stolpcev**  
VELJA:  $H = (A^T | I) \rightarrow G = (I | A)$  in  
 $H = (I | B) \rightarrow G = (B^T | I)$

$[1 \ 0 \ 0 \ | \ 1 \ 1 \ 0]$   
 $[0 \ 1 \ 0 \ | \ 1 \ 0 \ 1] = G$   
 $[0 \ 0 \ 1 \ | \ 0 \ 0 \ 1]$

d) **Hammingova razdalja koda dH**

-v tabelo vpisujemo 3, 34, 343... gledamo koliko se vrstica x-ov razlikuje od prejšnje  
 $dH_{min} = \text{najmanjša št jo dobimo... torej } \exists$   
e) **Koliko napak lahko odkrijemo in popr?**  
ODKRIJEMO:  $e_o = dH_{min} - 1$   
POPRAVIMO:  $e_p = \lfloor dH_{min} / 2 \rfloor$

**STANDARDNA TABELA**

$s = y * H^T$  ali  $s^T = H * y^T$

Popravl.	Kod.zam	sindrom
0 0 0	<b>0 0 0</b>	0 0
0 0 1	0 0 1	1 1 0
0 1 0	0 1 0	1 0 1
1 0 0	1 0 0	0 1 1

000, 111 sta možni kod zamenjavi pri napaki 000. Potem pa samo spremenimo za napake na 1 mestu. **Sindrom izračunamo po  $s^T = H * y^T$**  in dobimo tabelo:

y	s
0 0 0	$H * (0 \ 0 \ 0)^T = 0 \ 0$
0 0 1	0 1
0 1 0	1 0
0 1 1...	1 1

Potem pogledamo vrstico kodne zamenjave (npr (001) in (110) in vzamemo za y tisto ki ima manj enic in pogledamo kater sindrom je to.  
a) **Sprejet je bil vektor  $y=(011)$ , ali lahko popravimo napako na prvem mestu če je pršlo do nje? Pa na drugem?**  
-pogledamo v kodne.zamenjave (011) in v popravljajniku najdemo na levi (100)  
 $x^T = y + p \dots (011) + (100) = (111) \dots$  to pa je res kodna zamenjava ki obstaja! Torej ja.

**HAMMINGOV KOD H(n,k)**

$n = 2^m - 1, m \geq 2, e = 1$ , mat.za prev.sodosti H ima v stolpcih zapisana št.  $1-2^{m-1}$  (vsa raznen 0). H: m vrstic, n stolpcev. Tisti ki majo samo eno 1 v stolpcu so var.bit. Ostali so z-ji.  
a) **Najdi kodno zamenjavo za (0001) npr.**  
-to so  $z_1, z_2, z_3, z_4$ . Zmnožiš H in  $(x_1, x_2, x_3, 0, 0, 0, 1)^T$  in dobiš  $(x_1 + 1, x_2 + 1, x_3 + 0)$  npr. Te 1, 1, 0 so pa ostali x-i. Zdaj samo skupaj sestaviš z-je od prej in te nove x-e.

b) **Pri prenosu vektorja x je prišlo do napake e. Jo lahko popravimo?**  
-seš x in e. dobiš y.  
-izrač. sindrom po:  $s^T = H * y^T$   
-pogledaš koliko je sindrom desetiško -na tem desetiškem mestu lahko popr.

**CIKLIČNI KOD – C(n,k)**

**PREMIK  $x(p)$  ZA i MEST V LEVO:**  
 **$-(p^i * x(p)) : (p^{n+1})$**  in pogledaš ost.

a) **Določanje gen. polinom, polinom  $h(p)$ , gen.matr, mat. za prev.sodost, kodne zam. za  $n=3 \rightarrow 3$  podatkov.bit**  
 $\rightarrow (p^3 + 1) = (p + 1)(p^2 + p + 1)$

V tem primeru 4 možnosti:

1)  $g(p) = 1 \rightarrow m = 0 \rightarrow C(3, 3) \rightarrow G = 3 \times 3$ , id  
 **$h(p) = (p^{n+1}) / g(p)$** ,  $H = 0$  tukaj  
Kod.zam: 000, 100, 010, 001, 111

2)  $g(p) = p + 1 \rightarrow m = 1 \rightarrow C(3, 2)$   
 $G = [110]$ ,  $H = [111]$ , zaradi  
[011]  $h(p) = p^2 + p + 1$ ,  
ampak vpises iz D proti L  
KOD.ZAM:  $x = z * G$  ali  $x = z(p) * g(p)$   
Te z-ji so pa od k podatkov bitov..tu 2

3)  $g(p) = p^2 + p + 1 \rightarrow m = 2 \rightarrow C(3, 1)$   
 $G = [111]$  od  $g(p)$ ,  $h(p) = p + 1 \rightarrow$   
 $H = [110]$  ker le 1 podatkov. bit  
[011] sta kodni zam.  $Z = 0$  ali 1

4)  $g(p) = p^3 + 1$ ..ni podatkov.bitov  
 $G = 0$ ,  $h(p) = 1$ ,  $H = 3 \times 3$  identiteta  
Kod zamenjave:  $z(p) * 0 = 0 \dots x = (000)$

made by fidek

