Sveučilište u Zagrebu
**Fakultet elektrotehnike i računarstva**

Međuispit iz predmeta **TEORIJA INFORMACIJE**, 28. studenog 2013.

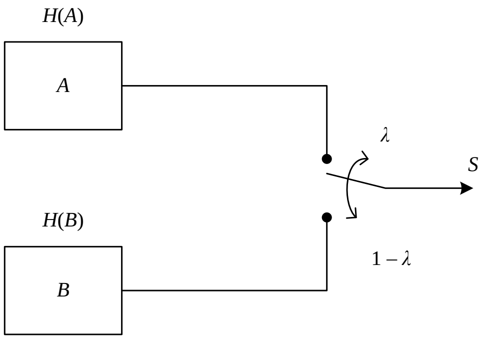
**Napomena:**

Svaki točno riješen zadatak boduje se s najviše 7 bodova. Svaki zadatak potrebno je rješavati na zasebnom listu papira. U svakom potpitanju jasno istaknite konačni odgovor. Svaka izračunata veličina mora imati točnu brojčanu vrijednost i po potrebi mjernu jedinicu.
U zadacima koji su razdvojeni na više dijelova (tzv. I. dio, II. dio,…) ne postoji nikakva povezanost između navedenih dijelova.

Trajanje ispita: 150 minuta.

## ZADACI

**Zadatak – 1:** (I. dio) **{4 boda}** Dva izvorišta, $A$ i $B$, čije su entropije $H(A)$, odnosno $H(B)$ povezana su na preklopnik kako je to predočeno na slici. Preklopnik slučajno odabire izvorište $A$ s vjerojatnšću $\lambda$, odnosno izvorište $B$ s vjerojatnošću $1 - \lambda$. Odredite entropiju skupa simbola $S$ na izlazu preklopnika u ovisnosti o $H(A)$, $H(B)$ i $\lambda$.




(II. dio) **{3 boda}** Zadane su dvije nezavisne slučajne varijable $X$ i $Y$. Varijabla $X$ poprima vrijednosti iz skupa $\{1, 2, 3, …, 8\}$ s jednakom vjerojatnošću. Varijabla $Y$ poprima bilo koju pozitivnu vrijednost $k$ ($k \in \mathrm{N}$) s vjerojatnošću $p(Y = k) = 2^{-k}$, $k = 1, 2, 3, …$

Odredite: $H(X)$, $H(Y)$ i $H(X, Y)$. **Napomena:** $\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$ za $|x| < 1$.

*Rješenje*:

(I. dio)

Neka $p_{i,A}$ i $n_A$ označavaju vjerojatnost pojavljivanja $i$-tog simbola na izvorištu $A$, odnosno broj simbola izvorišta $A$. Za izvorište $B$ koristi se označavanje $p_{i,B}$ i $n_B$, odnosno slična notacija se koristi za $S$, tj. $p_{i,S}$ i $n_S = n_A + n_B$.

Koristeći definiciju entropije dobivamo:

$$
\begin{aligned}
H(S) &= -\sum_{i=1}^{n_S} p_{i,S}\log_2\left(p_{i,S}\right) \\
&= -\sum_{i=1}^{n_A} \lambda p_{i,A}\log_2\left(\lambda p_{i,A}\right) - \sum_{i=1}^{n_B} (1-\lambda) p_{i,B}\log_2\left((1-\lambda) p_{i,B}\right) \\
&= -\lambda \sum_{i=1}^{n_A} p_{i,A}\left(\log_2 p_{i,A} + \log_2\lambda\right) - (1-\lambda)\sum_{i=1}^{n_B} p_{i,B}\left(\log_2 p_{i,B} + \log_2(1-\lambda)\right) \\
&= \lambda H(A) + (1-\lambda)H(B) - \lambda\log_2\lambda - (1-\lambda)\log_2(1-\lambda) \\
&= \lambda H(A) + (1-\lambda)H(B) + H(\lambda)
\end{aligned}
$$

(II. dio)

$H(X) = \log_2(8) = 3$ bit/simbol

$$H(Y) = -\sum_{j=1}^{m} p(y_j)\log_2 p(y_j) = -\sum_{j=1}^{\infty}\left(\frac{1}{2}\right)^j \log_2\left(\frac{1}{2}\right)^j = \sum_{j=1}^{\infty} j\left(\frac{1}{2}\right)^j = \text{...rješenje dano niže...}$$

Ako izraz

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$$

deriviramo (obje strane), a potom pomnožimo s $x$, dobit ćemo

$$\sum_{k=0}^{\infty} k\cdot x^k = \frac{x}{(1-x)^2} \quad \text{što je isto kao} \quad \sum_{k=1}^{\infty} k\cdot x^k = \frac{x}{(1-x)^2}$$

Dakle,

$H(Y) = 2$ bit/simbol.

Slučajne varijable $X$ i $Y$ međusobno su nezavisne → $I(X; Y) = 0$, tj. $H(X, Y) = H(X) + H(Y) = 5$ bit/simbol.

**Zadatak – 2:** (I. dio) **{4 boda}** Diskretno bezmemorijsko izvorište, $X$, generira beskonačan niz simbola iz skupa $\{a, b\}$ s vjerojatnostima pojavljivanja $p(a) = p$ i $p(b) = 1 - p$, $(0 < p < 1)$. Neka je nad takvim skupom simbola provedeno kodiranje kako je to predočeno u sljedećoj tablici:

| kôd A | | kôd B | | kôd C | |
|---|---|---|---|---|---|
| Simboli | kodne riječi | simboli | kodne riječi | Simboli | kodne riječi |
| *aa* | 1 | *aa* | 0001 | *a* | 0 |
| *ab* | 01 | *ab* | 001 | *b* | 1 |
| *b* | 00 | *ba* | 01 | | |
| | | *bb* | 1 | | |

Odredite:

i) srednju duljinu kodne riječi (bit/simbol) za svaki od navedenih kodova.
ii) za koje vrijednosti *p* je kôd A efikasniji od koda B.

(II. dio) **{3 boda}** Izvorište *X* generira *K* simbola s vjerojatnostima pojavljivanja $p_1 \geq p_2 \geq ... \geq p_K$ . Odredite najveći *q* za koji je $p_1 < q$ i $l_1 > 1$, gdje je, općenito gledano, $l_i$ duljina kodne riječi binarnog Huffmanovog koda pridružena simbolu $x_i$.

*Rješenje*:

(I. dio)

i)

Kôd A pridružuje <u>različite</u> duljine kodnih riječi različitim duljinama izvorišnih simbola. Neka $s_k$ predstavlja izvorišne simbole (jedan ili više njih grupiranih) kojima su pridjeljene različite kodne riječi. Općenito, srednju duljinu kodne riječi po simbolu (bit/simbol) možemo dobiti tako što podijelimo srednju duljinu kodne riječi po izvorišnim simbolima $s_k$ sa srednjim brojem simbola po $s_k$, tj.

$$L = \frac{\sum_{\forall s_k} p(s_k) \cdot l(s_k)}{\sum_{\forall s_k} p(s_k) \cdot n(s_k)}$$

Za kôd A:

$$L_A = \frac{\sum_{\forall s_k} p(s_k) \cdot l(s_k)}{\sum_{\forall s_k} p(s_k) \cdot n(s_k)} = \frac{p(aa) \cdot l(aa) + p(ab) \cdot l(ab) + p(b) \cdot l(b)}{p(aa) \cdot n(aa) + p(ab) \cdot n(ab) + p(b) \cdot n(b)} = \frac{p^2 \cdot 1 + p(1-p) \cdot 2 + (1-p) \cdot 2}{p^2 \cdot 2 + p(1-p) \cdot 2 + (1-p) \cdot 1} =$$

$$= \cdots = \frac{2-p^2}{1+p} \ \frac{\text{bit}}{\text{simbol}}$$

Po istoj analogiji za kôd B dobivamo:

$$L_B = \frac{\sum_{\forall s_k} p(s_k) \cdot l(s_k)}{\sum_{\forall s_k} p(s_k) \cdot n(s_k)} = \cdots = \frac{1+3p}{2} \ \frac{\text{bit}}{\text{simbol}}$$

Konačno, za kôd C dobivamo:

$$L_C = \frac{\sum_{\forall s_k} p(s_k) \cdot l(s_k)}{\sum_{\forall s_k} p(s_k) \cdot n(s_k)} = \cdots = 1 \frac{\text{bit}}{\text{simbol}}$$

ii)

Iz uvjeta zadatka ($\varepsilon_A > \varepsilon_B$) dobivamo $L_A < L_B$, tj. $\frac{2-p^2}{1+p} < \frac{1+3p}{2}$

odnosno

$$p^2 + \frac{4}{5}p - \frac{3}{5} > 0$$

Rješavanjem navedene nejednadžbe dobivamo:

$$p_{1/2} = -\frac{2}{5} \mp \frac{1}{2}\sqrt{\frac{16}{25} + \frac{12}{5}} = -\frac{2}{5} \mp \sqrt{\frac{19}{25}} = -\frac{2}{5} \mp \frac{\sqrt{19}}{5} = \frac{1}{5}\left(\mp\sqrt{19} - 2\right)$$

tj. nul-točke funkcije su:

$$p_1 = \frac{1}{5}\left(-\sqrt{19} - 2\right) \approx -1{,}2718$$

$$p_2 = \frac{1}{5}\left(\sqrt{19} - 2\right) \approx 0{,}4718$$

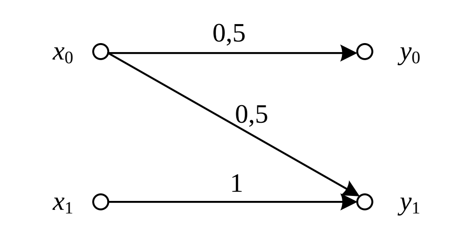
Također, $p$ mora biti pozitivno i u granicama između 0 i 1. Važno je uočiti da parabola $p^2 + \frac{4}{5}p - \frac{3}{5} > 0$ ima vrijednosti manje od nule za $0 \le p \le p_2$. **Dakle, kôd A je efikasniji od koda B ako je** $\frac{1}{5}\left(\sqrt{19} - 2\right) < p \le 1$**.**

(II. dio)

Iz uvjeta zadatka ( $p_1 \ge p_2 \ge ... \ge p_K$ i $l_1 > 1$) nameće se činjenica da bi prvo trebali provjeriti slučaj za koji je $K = 3$. Nadalje, neka su dana tri simbola $x_1$, $x_2$ i $x_3$ s vjerojatnostima pojavljivanja $p_1$, $p_2$ i $p_3$ ( $p_1 \ge p_2 \ge p_3$). Promatrajmo slučaj u kojem duljina kodne riječi za simbol $x_1$ iznosi 1 bit. To znači da je $x_1$ kodiran u posljednjem koraku algoritma.

Vrijedi sljedeće: $1 = p_1 + p_2 + p_3 \le 3p_1$, tj. $p_1 \ge 1/3$. Dokazali smo da je $l_1 = 1$ za $p_1 \ge 1/3$, odnosno, ako je $p_1 < 1/3$ tada je $l_1 > 1$. Pitanje koje se još nameće je: Je li $q = 1/3$ ili postoji li možda $q > 1/3$ za koji je $l_1 > 1$. Lako uviđamo da za $p_1 = p_2 = p_3 = 1/3$ nije moguće konstruirati Huffmanov binarni kôd za koji je $l_1 > 1$. **Dakle, najveći *q* je 1/3 za bilo koji *K*.**

**Zadatak – 3:** Zadan je diskretni bezmemorijski kanal.




Odredite:

i) **{5 bodova}** kapacitet zadanog diskretnog bezmemorijskog kanala.
ii) **{2 boda}** entropiju $H(X)$.

*Rješenje*:

i)

Krenimo od poznate formule za kapacitet diskretnog komunikacijskog kanala

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

Nadalje, $I(X;Y)=H(Y) - H(Y|X)$ te neka su $p_0$ i $p_1$ (= $1- p_0$) vjerojatnosti pojavljivanja ulaznog skupa simbola $X$. Neka je $[p(Y|X)]$ matrica uvjetnih prijelaza kanala: $[p(Y \mid X)] = \begin{bmatrix} 0,5 & 0,5 \\ 0 & 1 \end{bmatrix}$.

Matrica združenih vjerojatnosti je: $[p(X,Y)] = \begin{bmatrix} 0,5p_0 & 0,5p_0 \\ 0 & p_1 \end{bmatrix} = \begin{bmatrix} 0,5p_0 & 0,5p_0 \\ 0 & 1-p_0 \end{bmatrix}$, odnosno $[p(Y)] = \begin{bmatrix} \frac{p_0}{2} & \frac{2-p_0}{2} \end{bmatrix}$.

$$H(Y \mid X) = -\left\{2 \cdot \frac{p_0}{2} \log_2 \frac{1}{2}\right\} = p_0$$

$$H(Y) = -\left\{\frac{p_0}{2}\log_2 \frac{p_0}{2} + \frac{2-p_0}{2}\log_2\left(\frac{2-p_0}{2}\right)\right\} = \ldots = -\left\{\frac{1}{2}\left[p_0 \log_2 p_0 + (2-p_0)\log_2(2-p_0)\right] - 1\right\}$$

$$I(X;Y) = H(Y) - H(Y \mid X) = -\frac{1}{2}\left[p_0 \log_2 p_0 + (2-p_0)\log_2(2-p_0)\right] + 1 - p_0$$

Nadalje, $C = \max_{\{p(x_i)\}} I(X;Y)$ te dobivamo

$$\frac{dI(X;Y)}{dp_0} = -\frac{1}{2\ln 2}\{\ln p_0 + 1 - \ln(2-p_0) - 1\} - 1 = -\frac{1}{2\ln 2}\ln\frac{p_0}{2-p_0} - 1 = 0 \text{ odnosno}$$

$$\frac{1}{2\ln 2}\ln\frac{2-p_0}{p_0} = 1$$

$$\ln\frac{2-p_0}{p_0} = \ln 4$$

tj. $p_0 = \frac{2}{5} \rightarrow p_1 = \frac{3}{5}$

**Konačno, C ≈ 0,322 bit/simbol.**

ii)

$H(2/5, 3/5) \approx 0,971$ bit/simbol

**Zadatak – 4:** (I. dio) **{4 boda}** Skup simbola $X = \{x_1, x_2, x_3, x_4\}$, s vjerojatnostima pojavljivanja 0,25; 0,25; $p$ i $(0{,}5 - p)$, slijedno gledano, kodiran je prefiksnim Huffmanovim kodom. Također vrijedi $0 < p < 0{,}5$. Odredite za koje vrijednosti $p$ srednja duljina kodne riječi iznosi 2 bit/simbol.

(II. dio) **{1 bod}** Koristeći algoritam LZ77 kodirajte poruku *abaaabaab** uzimajući pritom da je maksimalna duljina posmičnog prozora i prozora za kodiranje 5, odnosno 4 simbola. **Napomena:** * označava kraj poruke.

(III. dio) **{2 boda}** Diskretno bezmemorijsko izvorište generira simbole iz skupa simbola $X = \{A, B\}$ s vjerojatnostima pojavljivanja $p(A) = 0{,}99$ i $p(B) = 0{,}01$. Aritmetičkim kodom kodirana je poruka $\underbrace{AA...A}_{n\,\text{puta}}B$ te je dobiven podinterval [0,36603; 0,36973) koji jednoznačno definira poruku. Odredite koliko simbola $A$ se nalazi u poruci. **Napomena:** Postojeći redoslijed simbola u skupu $X$ iskoristite za stvaranje kumulativnih podskupova pri čemu je simbol $A$ najbliži nuli.

*Rješenje*:

(I. dio)

1. Ako je $0 < p < 0{,}25$ tada simboli imju sljedeći redoslijed pri kodiranju (gledano od najvećeg do najmanjeg po vjerojatnosti):

| $x_i$ | $p(x_i)$ |
|---|---|
| $x_4$ | $0{,}5 - p$ |
| $x_1$ | 0,25 |
| $x_2$ | 0,25 |
| $x_3$ | $p$ |

Ako je $p(x_3) + p(x_2) \leq p(x_4)$, tj. ako je $p \leq 0{,}125$ tada su duljine kodnih riječi $l(x_4)=1$ bit/simbol, $l(x_1)=2$ bit/simbol, $l(x_2)= l(x_3) = 3$ bit/simbol.

Nadalje, pronađimo za koji $p$ ($p \leq 0{,}125$) je srednja duljina kodne riječi $L = 2$ bit/simbol. Dobivamo sljedeće:

$$(0{,}5 - p) \cdot 1 + 0{,}25 \cdot 2 + 0{,}25 \cdot 3 + p \cdot 3 = 2 \rightarrow p = 0{,}125 \quad (1)$$

Ako je $0{,}125 < p < 0{,}25$, tada je $p(x_3) + p(x_2) > p(x_4)$ pa duljine kodnih riječi iznose: $l(x_4) = 2$ bit/simbol, $l(x_1) = 2$ bit/simbol, $l(x_2) = 2$ bit/simbol, $l(x_3) = 2$ bit/simbol, tj.

$L = 2$ bit/simbol za $0{,}125 < p < 0{,}25$ (2)

Također, za $p = 0{,}25$ srednja duljina kodne riječi iznosi 2 bit/simbol. (3)

2. Ako je $0{,}25 < p < 0{,}5$ tada simboli imju sljedeći redoslijed pri kodiranju (gledano od najvećeg do najmanjeg po vjerojatnosti):

| $x_i$ | $p(x_i)$ |
|---|---|
| $x_3$ | $p$ |
| $x_1$ | 0,25 |
| $x_2$ | 0,25 |
| $x_4$ | $0,5 - p$ |

Ako je $p(x_4) + p(x_2) > p(x_3)$, tj. ako je $p < 0,375$ tada su duljine kodnih riječi $l(x_3) = 2$ bit/simbol, $l(x_1) = 2$ bit/simbol, $l(x_2) = 2$ bit/simbol, $l(x_4) = 2$ bit/simbol, tj.

$L = 2$ bit/simbol za $0,25 < p < 0,375$ (4)

Ako je $p(x_4) + p(x_2) \leq p(x_3)$, tj. ako je $p \geq 0,375$ tada su duljine kodnih riječi $l(x_3) = 1$ bit/simbol, $l(x_1) = 2$ bit/simbol, $l(x_2) = 3$ bit/simbol, $l(x_4) = 3$ bit/simbol. Nadalje, pronađimo za koji $p$ ($p \geq 0,375$) je srednja duljina kodne riječi $L = 2$ bit/simbol. Dobivamo sljedeće:

$$p \cdot 1 + 0,25 \cdot 2 + 0,25 \cdot 3 + (0,5 - p) \cdot 3 = 2 \rightarrow p = 0,375 \quad (5)$$

Konačno, ako ujedinimo sve uvjete (označene u zagradama "(...)") dobivamo da je srednja duljina kodne riječi $L = 2$ bit/simbol za $p \in [0,125; 0,375]$.

(II. dio)

(0, 0, *a*), (0, 0, *b*), (2, 1, *a*), (4, 3, *a*) i (3, 1, *)

(III. dio)

Odredimo kumulativne podskupove:

| $x_i$ | $p(x_i)$ | Kumulativni podskupovi $[D_s; G_s)$ |
|---|---|---|
| $A$ | 0,99 | [0; 0,99) |
| $B$ | 0,01 | [0,99; 1) |

Polazno je $D = 0$ i $G = 1$ te za proračun podintervala koristimo sljedeće formule:

$D' = D + (G - D) \cdot D_s$

$G' = D + (G - D) \cdot G_s$

Lako se uočava da je $n$-ti simbol $A$ određen sljedećim podintervalom:

$D' = 0$

$G' = 0,99^n$

odnosno, prije kodiranja simbola $B$ donja i gornja granica su $D = 0$, odnosno $G = 0,99^n$.

Za simbol $B$ dobivamo:

$$D' = 0{,}99^n \cdot 0{,}99 = 0{,}99^{n+1}$$

$$G' = 0{,}99^n \cdot 1 = 0{,}99^n$$

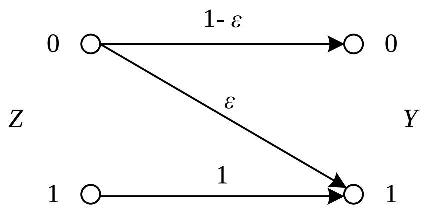
što jasno određuje interval [0,36603; 0,36973).

Iz $0{,}99^{n+1} = 0{,}36603$ ili $0{,}99^n = 0{,}36973$ dobivamo da je **$n$ = 99, tj. broj simbola *A* u poruci je 99.**

**Zadatak – 5:** Zadano je diskretno bezmemorijsko izvorište, $X$, koje generira simbole iz skupa $\{-1, 0, 1\}$. Neka je definirana sljedeća funkcija:

$$\mu(a) = \begin{cases} 0, \text{ za } a \le 0 \\ 1, \text{ za } a > 0 \end{cases}$$

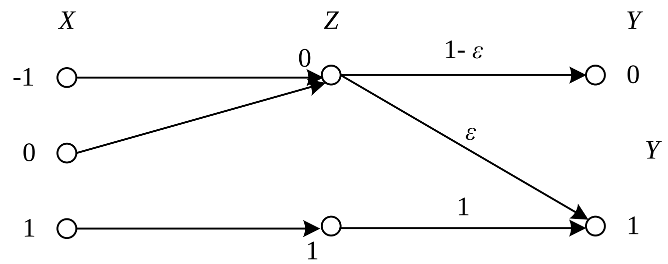
Slučajana varijabla $Z = \mu(X)$ se prenosi sljedećim kanalom:




i) **{1 bod}** Skicirajte komunikacijski kanal $X \rightarrow Z \rightarrow Y$.
ii) **{2 boda}** Za koje će sve razdiobe od $X$ entropija od $Z$ biti maksimalna?
iii) **{3 boda}** Za koji $\varepsilon$ ($0 \le \varepsilon \le 1$) je kapacitet kanala $X \rightarrow Z \rightarrow Y$ minimalan?
iv) **{1 bod}** Izračunajte $I(X; Y)$ uzimajući da je $\varepsilon = 0{,}5$ i da $X$ ima jednoliku razdiobu.

*Rješenje*:

i)




ii)

Neka su vjerojatnosti pojavljivanja izvorišnog skupa simbola sljedeće: $p_{-1}=p(x = -1)$, $p_0=p(x = 0)$ i $p_1=p(x = 1)$.

Iz $\left[p(Z \mid X)\right]=\begin{bmatrix}1 & 0\\ 1 & 0\\ 0 & 1\end{bmatrix}$ i $\left[p(X,Z)\right]=\begin{bmatrix}p_{-1} & 0\\ p_0 & 0\\ 0 & p_1\end{bmatrix}$ dobivamo da je $\left[p(Z)\right]=\left[p_{-1}+p_0 \quad p_1\right]$.

Uočavamo da se maksimum entropije $H(Z)$ = 1 bit /simbol dobiva ako je $\boldsymbol{p_{-1}+p_0=0{,}5}$ **i** $\boldsymbol{p_1=0{,}5}$**.**

iii)

Kapacitet diskretnog komunikacijskog kanala određuje se iz:

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

gdje je $I(X;Y)=H(Y)-H(Y|X)=H(X)-H(X|Y)$.

Odredimo ukupnu matricu (ulaz – izlaz) uvjetnih prijelaza zadanog komunikacijskog sustava, tj.:

$$\left[p(Y \mid X)\right]=\begin{bmatrix}1 & 0\\ 1 & 0\\ 0 & 1\end{bmatrix}\cdot\begin{bmatrix}1-\varepsilon & \varepsilon\\ 0 & 1\end{bmatrix}=\begin{bmatrix}1-\varepsilon & \varepsilon\\ 1-\varepsilon & \varepsilon\\ 0 & 1\end{bmatrix}.$$

Uočavamo, iz matrice $[p(Y|X)]$ i slike (dio zadatka i)) da za $\varepsilon$ = 1 izlazne vjerojatnosti za skup simbola $Y$ = {0, 1} poprimaju vrijednosti 0, odnosno 1. Što upućuje da je $H(Y)$=0, odnosno iz $[p(Y|X)]$ za $\varepsilon$ = 1 da je $H(Y|X)$=0. Dakle, prema formuli za kapacitet dobivamo da je ***C*** **= 0 ili *C* = 0 bit/simbol.**

iv)

$I(X;Y)$ = 0,25163 bit/simbol