Naključni vir brez spomina A oddaja N različnih znakov, vir brez spomina B pa N+1 različnih znakov. Verjetnosti prvih N znakov so pri obeh virih enake. Napišite povezavo med entropijama obeh virov in jo utemeljite.

$$A = \{x_1, \dots, x_N\}; \quad P_A = \{p_1, \dots, p_N\}; \quad \sum_{i=1}^{N} p_i = 1$$

$$B = \{x_1, \dots, x_N, x_{N+1}\}; \quad P_B = \{p_1, \dots, p_N, 0\}$$

$$H(B) = -\sum_{i=1}^{N} p_i \log p_i - \underbrace{0 \cdot \log 0}_{0} = H(A)$$

Opišite postopek kodiranja Huffmanovega koda

Huffmanov kod (s poljubno osnovo r):

- izračunamo potrebno število osnovnih znakov glede na r; po potrebi dodamo znake z verjetnostjo 0
- ponavljamo dokler ne dobimo samo enega znaka:
  - združujemo r znakov z najmanjšo verjetnostjo
  - ob vsaki združitvi dobimo nov znak z verjetnostjo, ki je vsota verjetnosti združenih znakov
- dodelimo kodne zamenjave:
  - začnemo v korenu kodnega drevesa in vsaki veji dodelimo eno od števil med 0 in r-1
  - to rekurzivno ponovimo za vsako vozlišče (sestavljen znak)
  - kodna zamenjava osnovnega znaka je sestavljena iz števil na vejah, ki jih zložimo od listov proti korenu.

V diskretni kanal brez spomina pošiljamo vrednosti naključne spremenljivke X in na njegovem izhodu pa opazujemo vrednosti naključne spremenljivke Y. Pokažite, da nam spremenljivka X pove o spremenljivki Y ravno toliko kot spremenljivka Y o spremenljivki X.

$$X \to \boxed{} \to Y$$

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

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

Napišite in razložite drugi Shannonov teorem. Napišite enačbe za količine, ki nastopajo v njem. Vse količine v enačbah označite.

Za R $\leq$ C obstaja kod, ki zagotavlja prenašanje informacije s poljubno majhno verjetnostjo napake.
Za R > C tak kod ne obstaja.

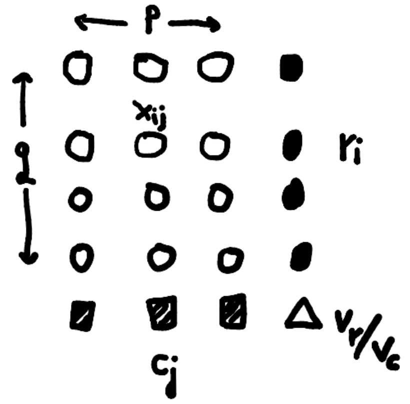
hitrost $\rightarrow$ $$R = \frac{\max H(X^n)}{n}$$ $\leftarrow$ entropija bloka n znakov; $\leftarrow$ število znakov v bloku

kapaciteta $\rightarrow$ $$C = \max_{P(x)} I(X;Y)$$ $\leftarrow$ medsebojna informacija; $\leftarrow$ vhodne verjetnosti

Največ koliko različnih kodnih zamenjav lahko tvorimo za linearni bločni kod, ki ima kodne zamenjave dolge n znakov, z njim pa želimo popraviti do f napak?

$$M \leq \frac{2^n}{\sum_{i=0}^{f} \binom{n}{i}}$$

Pravokotni kod tvorimo tako, da je vsota po vrsticah in stolpcih liha. Za kakšne kombinacije števila vrstic in stolpcev koda ne moremo tvoriti? Pokažite!



$$r_i = \bigoplus_{j=1}^{p} x_{ij} \oplus 1, \quad v_r = \bigoplus_{i=1}^{q} r_i = \bigoplus_{i=1}^{q}\left(\bigoplus_{j=1}^{p} x_{ij} \oplus 1\right)$$

$$c_j = \bigoplus_{i=1}^{q} x_{ij} \oplus 1, \quad v_c = \bigoplus_{j=1}^{p} c_j = \bigoplus_{j=1}^{p}\left(\bigoplus_{i=1}^{q} x_{ij} \oplus 1\right)$$

$$v_r \stackrel{?}{=} v_c$$

$$\bigoplus_{i=1}^{q}\bigoplus_{j=1}^{p} x_{ij} \oplus \bigoplus_{i=1}^{q} 1 \stackrel{?}{=} \bigoplus_{j=1}^{p}\bigoplus_{i=1}^{q} x_{ij} \oplus \bigoplus_{j=1}^{p} 1$$

$$q \bmod 2 = p \bmod 2$$

če to ne velja, koda ne moremo sestaviti.

Imamo množico virov brez spomina. Viri oddajajo do največ N znakov, pri čemer se viri razlikujejo po verjetnostih za oddane znake. Največ kolikšna je lahko razlika entropij dveh poljubnih virov?

Št. znakov	max. $H(x)$
1	0
N	$\log_b N$

$$\Delta H = \max H(x_1, \ldots, x_N) - H(x_1)$$
$$= \log_b N - 0 = \underline{\underline{\log_b N}}$$

Podan imamo generatorski polinom g(p) cikličnega koda. Opišite tvorbo generatorske matrike G in matrike za preverjanje sodosti H pri kodiranju na osnovi množenja

$$g(p) = p^m + g_{m-1} p^{m-1} + \ldots + g_1 p + 1$$

$$h(p) = (p^n + 1) : g(p) = 1 + h_1 p + \ldots + h_{k-1} p^{k-1} + p^k$$

$$G = \begin{array}{c} 1 \\ \\ \\ k \end{array} \begin{bmatrix} 1 & g_{m-1} & \cdots & g_1 & 1 & & & \emptyset \\ & 1 & g_{m-1} & \cdots & g_1 & 1 & & \\ & & & \vdots & & & & \\ \emptyset & & & 1 & g_{m-1} & \cdots & g_1 & 1 \end{bmatrix}$$
$$\begin{array}{cc} 1 & \qquad\qquad\qquad\qquad\qquad n \end{array}$$

$$H = \begin{bmatrix} 1 & h_1 & \cdots & h_{k-1} & 1 & & & \emptyset \\ & 1 & h_1 & \cdots & h_{k-1} & 1 & & \\ & & & \vdots & & & & \\ \emptyset & & & 1 & h_1 & \cdots & h_{k-1} & 1 \end{bmatrix}$$

Signal smo vzorčili s frekvenco vzorčenja, ki je vsaj dvakrat večja od najvišje frekvence v signalu. Napišite enačbo rekonstruiranega signala.

$$x(t) = \sum_{k=-\infty}^{\infty} x_k \frac{\sin\left(\pi \nu_s \left(t - \frac{k}{\nu_s}\right)\right)}{\pi \nu_s \left(t - \frac{k}{\nu_s}\right)}$$

A) Naključni vir brez spomina oddaja znake z verjetnostmi, ki jih v Matlabu zložimo v stolpični vektor p = [0.1; 0.22; 0.07; 0.42; 0.19]. Kateri ukaz izračuna nedoločenost vira?

a) H = - p' .* log2(p); b) H = - p .* log2(p'); c) H = - p .* log2(transpose(p));

d) H = - p' * log2(p); e) H = - p * log2(p'); f) H = - p * log2(transpose(p));

B) Z ukazom Y=fft(X) v Matlabu izračunamo diskretno Fourierevo transformacijo signala X. Spremenljivka X je vektor amplitud realnega signala po času vzorčenih s frekvenco Fs=8000. Signal smo vzorčili 1 sekundo. Kateri ukaz nam v spremenljivki P vrne moč pri frekvenčni komponenti f=1000? Frekvence so podane v Hz.

a) P = 2*Y(f)^2/length(Y)^2; b) P = 2*abs(Y(f))^2/length(Y)^2;

c) P = 2*abs(Y(f*Fs/length(Y)+1)^2/length(Y)^2; **(tukaj bi bil c prav če bi bil zaklepaj pred podpičjem, so trije oklepaji in 2 zaklepaja)**

d) P = 2*abs(Y(f*Fs/length(Y))^2/length(Y)^2;

e) P = Y(f); **f) Nič od naštetega.**

Znake, ki jih oddaja vir brez spomina X, združujemo v bloke dolžine M in jih kodiramo s Shannonovim algoritmom. Za največ koliko je lahko razmerje med povprečno dolžino kodnih zamenjav in številom znakov v bloku večje od entropije vira?

$$\underbrace{X \ldots X}_{M} = X^M$$

vir brez spomina

$$H(X^M) = M \cdot H(X)$$

Shannonov kod je gospodaren trenutni kod

$$H(X^M) \leq L_M < H(X^M) + 1$$

$$M \cdot H(X) \leq L_M < M \cdot H(X) + 1$$

$$H(X) \leq \frac{L_M}{M} < H(X) + \frac{1}{M}$$

$$\Delta H = H(X) + \frac{1}{M} - H(X) = \underline{\underline{\frac{1}{M}}}$$

Niz znakov smo z aritmetičnim kodom kodirali v desetiški interval. Opišite postopek dekodiranja desetiškega intervala v niz znakov.

Dekodiranje intervala [a,b) v niz n znakov

1. Začnemo z intervalom [0,1)
2. Izbrani interval razdelimo na n podintervalov, ki se ne prekrivajo; širine podintervalov ustrezajo verjetnostim za znake.
3. Izberemo interval, v katerem se nahaja interval [a,b)
4. Znak, ki ga predstavlja izbrani interval izpišemo
5. Če izpisani znak ni stop ali če število znakov ni enako številu znakov, ki jih moramo dekodirati, se vrnemo na korak 2.

Napišite in razložite enačbo za kapaciteto kanala.

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

X je naključna spremenljivka na vhodu v kanal
Y je naključna spremenljivka na izhodu iz kanala
I(*X*; *Y*) je medsebojna informacija
C je maksimalna medsebojna informacija, ki se lahko prenaša čez kanal. Ker se kanal ne spreminja, lahko maksimiramo samo po vhodnih verjetnostih *P*(*X*).

Pri nespremenljivem kanalu so prehodne verjetnosti p(yj/xi) fiksne => I(X;Y) = H(Y) – H(Y/X)

H(Y) so odvisne od vhodnih verjetnosti => dovolj je, če maksimiramo po vhodnih verjetnostih

H(Y/X) so fiksne

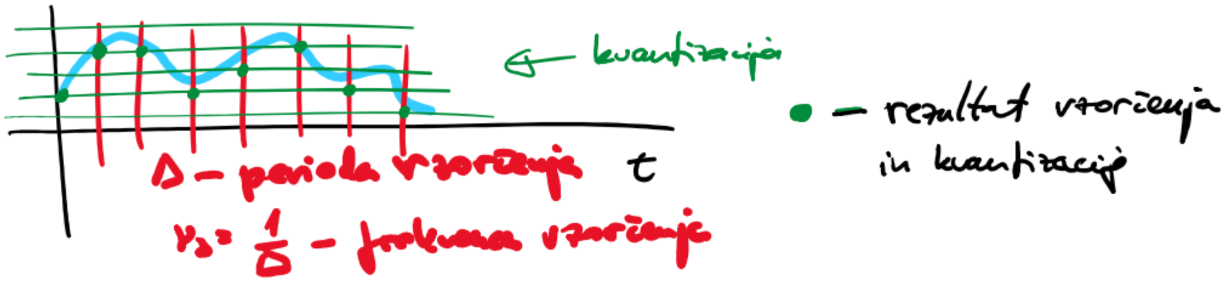
Sestavljamo linearni bločni kod z dolžinami kodnih zamenjav n. Največ koliko podatkovnih bitov k lahko vključimo v kodno zamenjavo, če želimo s kodom popravljati do f napak?

Nad Σ je vedno f

$$2^k \le \frac{2^n}{\sum_{i=0}^{f}\binom{n}{i}} \Rightarrow k = \left\lfloor \log_2 2^n - \log_2 \sum_{i=0}^{f}\binom{n}{i} \right\rfloor = n - \left\lceil \log_2 \sum_{i=0}^{f}\binom{n}{i} \right\rceil$$

Opišite postopke pri zajemanju meritev z računalnikom. Na kaj moramo biti pozorni?

- Vzorčenje: frekvenca vzorčenja mora biti vsaj dvakratnik najvišje frekvence v signal
- Kvantizacija: A/D pretvornik vrednosti predstavi z omejeno natančnostjo več bitov kot ima A/D prevornik, bolj natančno opiše vrednosti



Pokažite, da je ponavljajoči varnostni kod, ki je sestavljen iz enega podatkovnega bita in sodega števila varnostnih bitov, tudi sistematični ciklični kod. Določite generatorski polinom.

možne kodne zamenjave: $\begin{matrix} 0|\overbrace{0\ldots0}^{2q} \\ 1|1\ldots1 \end{matrix}\Big\}$ dva različna cikla ⇒ je ciklični kod

$1\ldots1$ → varnostni biti, $1|$ → podatkovni bit ⇒ so ločeni ⇒ kod je sistematičen

kod: $C(n, 1)$, $1 = k$

$m = n - k = n - 1 = 2q$

sistematični ciklični kod → kodiranje z deljenjem

$\vec{z} = (1) \Rightarrow$ kodna zamenjava za $z(p) = 1$:

$\vec{x} = (1|\underbrace{1\ldots1}_{m}) \Rightarrow x(p) = p^m + p^{m-1} + \ldots + p + 1 = \underbrace{z(p)}_{=1} \cdot p^m + r(p) \Rightarrow r(p) = p^{m-1} + p^{m-2} + \ldots + p + 1$

ostanek pri deljenju

$$p^m : \underbrace{p^m + g_{m-1}p^{m-1} + \ldots + g_1 p + 1}_{g(p)} = 1$$

$$r(p) = g_{m-1}p^{m-1} + \ldots + g_1 p + 1$$

mora biti enako

$$g_{m-1} = g_{m-2} = \ldots = g_1 = 1$$

$$\Downarrow$$

$$g(p) = p^{m = 2q} + p^{m-1} + p^{m-2} + \ldots + p + 1$$

A) Pri kodiranju LZW je potrebno pred začetkom postopka kodiranja/dekodiranja inicializirati slovar. Kot podatkovno strukturo za hrambo slovarja uporabimo običajno matriko. V prvem stolpcu matrike hranimo dolžino niza v posamezni vrstici, preostali stolpci hranijo ASCII kode znakov v nizu. V kolikor niz ne zasede celotne širine matrike, v preostale stolpce vstavimo ničle. Za začetek v slovar dodamo vse znake razširjene abecede ASCII. V slovarju naj bo prostora še za dodatnih 10 nizov dolžine 10. Kateri od spodnjih ukazov pravilno inicializira začetni slovar S?

a) S=[ones(1,256)'; zeros(1,10)',(0:255)'; zeros(1,10)', zeros(266,9)]
b) S=[ones(256,1), zeros(10,1)', (0:255), zeros(10,1), zeros(9,266)]
c) S=[ones(256,1) zeros(10,1); (0:255), zeros(10,1); zeros(266,9)]
d) S=[ones(1,256) zeros(1,10); (0:255), zeros(1,10); zeros(9,266)]'
e) S=[ones(256,1); zeros(10,1); (0:255); zeros(10,1); zeros(266,9)]'
f) Nič od naštetega.

B) V Matlabu simuliramo dekodiranje podatkov, ki so bili kodirani s Hammingovim kodom H(7,4). Spremenljivka H vsebuje matriko za preverjanje sodosti in je že podana. Definiran je tudi vrstični vektor y, ki vsebuje sprejete bite. Kateri izmed naslednjih ukazov pravilno izračuna sindrom s?

a) s = mod(y' * H', 2); b) s = mod(y' .* H, 2); c) s = mod(y' * H, 2);

d) s = mod(y .* H', 2); **e) s = mod(y * H', 2);** f) Nič od naštetega.

Opazujemo dva vira brez spomina, ki naključno oddajata različne znake z neničelnimi verjetnostmi. Prvi vir oddaja N znakov, drugi pa NN znakov. Maksimalno entropijo drugega vira izrazite z maksimalno entropijo prvega vira.

$H_{1max} = \log_b N \quad , \quad H_{2max} = \log_b N^N = N \cdot \log_b N = N \cdot H_{1max}$

H1max = log(b)N H2max = log(b) N^N = N*log(b)N = N*H1max (če ni pregledno)

Vir oddaja A znakov z neničelnimi verjetnostmi. Znake kodiramo z nesingularnim in enoličnim kodom. Kaj o ostalih lastnostih koda lahko sklepamo samo iz dolžin kodnih zamenjav? Odgovore podkrepite z enačbami.

vse kodne zamenjave enake dolge => enakomeren kod

$\sum_{i=1}^{A} r^{-l_i} \leq 1$ => izpolnjen potrebni pogoj za trenutnost koda

l_i ← dolžina i-te kodne zamenjave

r ← število znakov kodne abecede

Opišite postopek dekodiranja po algoritmu Lempel-Ziv-Welch.

```
preberi indeks k (kodno zamenjavo)
v slovarju poišči niz N, ki ustreza indeksu k
izpiši N
N_star = N
ponavljaj:
    preberi indeks k
    če je k v slovarju:
        v slovarju za indeks k poišči niz N
    drugače:
        N = [N_star, N_star(1)]
    izpiši N
    v slovar dodaj [N_star, N(1)]
    N_star = N
```

Opišite in razložite drugi Shannonov teorem.

$$R = \frac{\max H(X^m)}{m}$$

← entropija bloka

↑ število znakov v bloku

hitrost koda

Za R <= C (kapaciteta kanala) obstaja kod, ki zagotavlja prenašanje informacije, da je verjetnost napake pri dekodiranju poljubno majhna. Za R > C tak kod ne obstaja.

Naključni vir brez spomina oddaja znake, ki jih do ponora prenašamo po kanalu brez spomina. Količino informacije, ki jo prenesemo iz vira na ponor, izrazite s prehodnimi verjetnostmi obrnjenega kanala in z verjetnostmi sprejetih znakov na ponoru.

$X = \{x_1, \dots, x_n\}$, $P(X) = \{p(x_1), \dots, p(x_n)\}$

$Y = \{y_1, \dots, y_m\}$, $P(Y) = \{p(y_1), \dots, p(y_m)\}$ ← verjetnosti sprejetih znakov

$p(x_i|y_j)$ – prehodne verjetnosti

$$p(x_i) = \sum_{j=1}^{m} p(y_j) \cdot p(x_i|y_j)$$

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

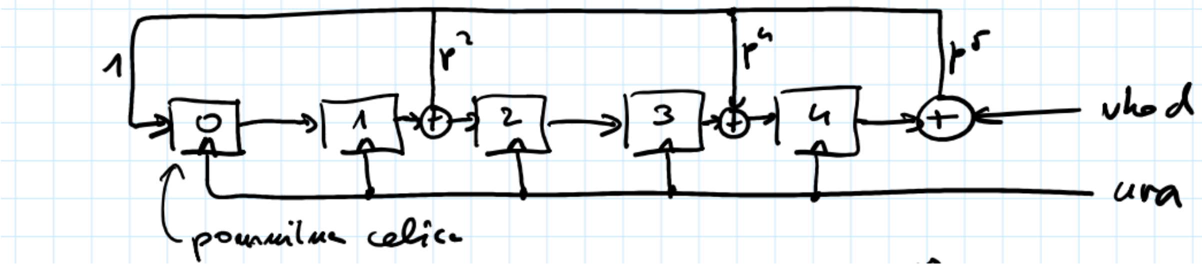
$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_b p(x_i)$$

$$H(X|Y) = \sum_{j=1}^{m} p(y_j) \cdot H(X|Y=y_j)$$

$$H(X|Y=y_j) = -\sum_{i=1}^{n} p(x_i|y_j) \log_b p(x_i|y_j)$$

Narišite shemo električnega vezja za generiranje kodnih zamenjav sistematičnega cikličnega koda z generatorskim polinomom $g(p) = p^5 + p^4 + p^2 + 1$.

$$g(p) = p^5 + p^4 + p^2 + 1$$



Pokažite, da s Fourierovo transformacijo prevedemo operacijo konvolucije v časovnem prostoru v navadno množenje v frekvenčnem prostoru.

Integrali so zgori neskončni in spodi minus neskončni, čudni t je tau τ.

$$f(t) = \int_{-\infty}^{\infty} x(t-\tau)\, y(\tau)\, d\tau \qquad F(\omega) = \int_{-\infty}^{\infty} f(t)\, e^{-i\omega t}\, dt$$

$$F(\omega) = \int_{-\infty}^{\infty} dt \cdot e^{-i\omega t} \int_{-\infty}^{\infty} d\tau \cdot x(t-\tau)\, y(\tau) =$$

$$= \int_{-\infty}^{\infty} dt \cdot x(t-\tau)\, e^{-i\omega(t-\tau)} \cdot \int_{-\infty}^{\infty} d\tau \cdot y(\tau)\, e^{-i\omega\tau}$$

$$t' = t - \tau$$
$$dt' = dt$$

$$= \underbrace{\int_{-\infty}^{\infty} dt'\, x(t')\, e^{-i\omega t'}}_{X(\omega)} \cdot \underbrace{\int_{-\infty}^{\infty} d\tau\, y(\tau)\, e^{-i\omega\tau}}_{Y(\omega)}$$

$$F(\omega) = X(\omega) \cdot Y(\omega)$$

Vir brez spomina oddaja N različnih znakov tako, da je entropija največja možna. Kolikšne so v tem primeru: največja lastna informacija, najmanjša lastna informacija in entropija?

ENTROPIJA JE NAJVEČJA, KO JE $p(x_i) = \frac{1}{m} \longrightarrow H(X) = I_{MIN} = I_{MAX} = \log_r m$

ŠT. ZNAKOV

Pri kodiranju se pogosto zgodi, da je povprečna dolžina kodnih zamenjav gospodarnega koda precej večja od entropije. Pokažite, da se z združevanjem znakov v bloke povprečna dolžina kodnih zamenjav lahko poljubno približa entropiji?

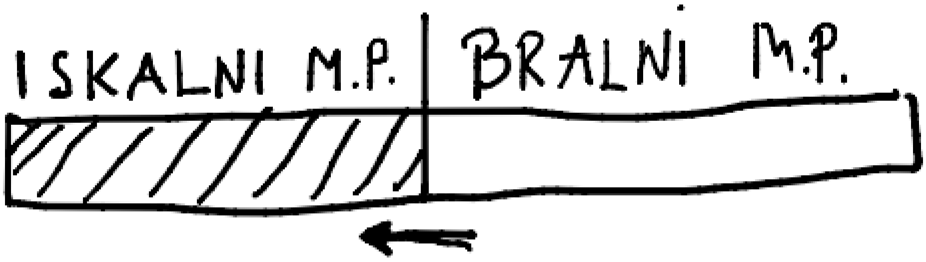
$$H(X^N) \leq L_N < H(X^N) + 1$$

$$N \cdot H(X) \leq L_N < N \cdot H(X) + 1$$

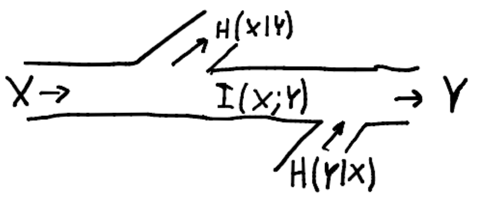
$$H(X) \leq \frac{L_N}{N} < H(X) + \frac{1}{N} \xrightarrow{\text{v limiti}} \lim_{N \to \infty} \frac{1}{N} = 0 \longrightarrow H(X) = \frac{L_N}{N}$$

Opišite kodiranje koda Lempel-Ziv 77

LZ77 – gre za kodiranje s slovarjem, kjer niz iz bralnega medpomnilnika primerjamo z nizom v iskalnem medpomnilniku. Vsak niz predstavimo kot trojček (odmik, dolžina, naslednji znak). Na začetku je slovar prazen. Če niza ne najdemo v slovarju (iskalni medpomnilnik), za odmik in dolžino nastavimo 0.



Vir brez spomina X oddaja v kanal N. Na izhodu kanala opazujemo spremenljivko Y. Napišite enačbo šuma v odvisnosti od verjetnosti znakov X in prehodnih verjetnosti kanala.



$$H(Y|X) = \sum_{i=1}^{m} p(x_i) \, H(Y|X=x_i)$$

$$H(Y|X=x_i) = -\sum_{j=1}^{m} p(y_j|x_i) \log_r p(y_j|x_i)$$

Koliko napak v sprejetem nizu lahko popravimo, če je Hammingova razdalja koda dH?

$$f_{MAX} = \left\lfloor \frac{d_H - 1}{2} \right\rfloor$$

Pokažite, da je pri trikotnem kodu vsota varnostnih bitov vedno 0!

Za vsak varnostni bit seštejemo vse bite podatkov v njegovi vrstici in v njegovem stolpcu. Vsak podatkovni bit tako nastopa pri enem varnostnem bitu v vrstici, pri nekem drugem varnostnemu bitu pa v stolpcu. Če seštejemo vse varnostne bite, smo vsak podatkovni bit šteli dvakrat. Vsota vseh varnostnih bitov je tako 0.

Napišite povezavo med generatorsko matriko G in matriko za preverjanje sodosti H pri sistematičnih linearnih bločnih kodih.

$G = [I_k | A]$, $H = [A^T | I_m]$ in $G = [A | I_k]$, $H = [I_m | A^T]$

Najmanj kolikšna mora biti perioda vzorčenja zveznega signala, da ga iz vzorcev lahko uspešno rekonstruiramo? Odgovor podkrepite s poenostavljanim ali pravim dokazom.

$\nu_S \geq 2 \cdot \nu_C$, ν_C je najvišja frekvenca v signalu. Perioda vzorčenja: $\Delta = \frac{1}{\nu_S}$

Zajeti signal poznamo samo na intervalu [0, T], zato se lahko delamo, da je periodičen in ga razvijemo v Fourierovo vrsto z osnovnim harmonikom $\nu_0 = \frac{1}{T}$.

Najvišja frekvenca je ν_C, torej v signalu nastopa $\frac{\nu_C}{\nu_0}$ harmonikov.

Za vsak harmonik imamo dva koeficienta (sin + cos), skupaj torej $2\frac{\nu_C}{\nu_0} = 2\nu_C T$ koeficientov.

Za izračun $2\nu_C T$ koeficientov rabimo ravno toliko točk v časovnem prostoru, ki so zajete v času T.

Iz tega sledi: $\nu_S = \frac{2\nu_C T}{T} = 2\nu_C$.

Vir brez spomina oddaja N znakov X= {x1, ..., XN} z verjetnostmi PX = {p1, ..., pN}. Napišite zvezo med lastno informacijo in entropijo vira.

$$H(X) = \sum_{i=1}^{N} p_i I_i \quad , \quad I_i = -\log_r p_i$$

Napišite Kraftovo neenakost in označite vse količine, ki v njej nastopajo. Kaj nam neenakost pove?

$$\sum_{i=1}^{n} r^{-l_i} \leq 1$$

n – število kodnih zamenjav
r – število znakov v kodirni abecedi
l_i – dolžina i-te kodne zamenjave
Potreben pogoj, da je kod trenutni – če neenačba velja, obstaja trenutni kod s takimi dolžinami kodnih zamenjav.

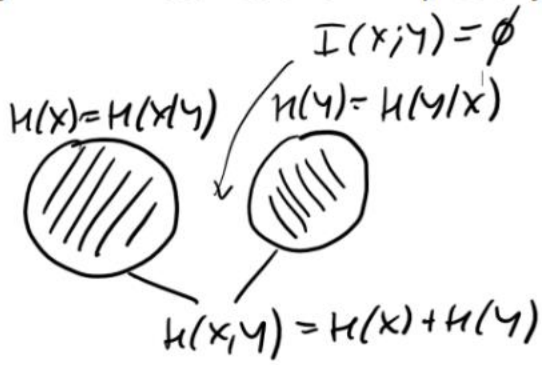
Opišite postopek dekodiranja koda Lempel-Ziv-Welch.

Začnemo z osnovnim slovarjem, ki ga dopolnjujemo.

```
preberi indeks k
v slovarju poišči niz N, ki ustreza indeksu k
izpiši N, N_star = N
ponavljaj:
   preberi indeks k
   če je k v slovarju:
      v slovarju za indeks k poišči niz N
   drugače:
      N = [N_star, N_star(1)]
   izpiši N, v slovar dodaj niz [N_star,N(1)]
   N_star = N
```

Opazujemo stohastično spremenljivko X = {x1, …, xN} z verjetnostmi PX = {p1, … pN} in stohastično spremenljivko Y = {y1, …, yM} z verjetnostmi PY = {q1, …, qM}. Verjetnost, da spremenljivka X zavzame vrednost xi, spremenljivka Y pa vrednost yj je enaka piqj. Narišite ustrezen Vennov diagram in na njem označite entropiji, pogojni entropiji, vezano entropijo in medsebojno informacijo.

$p_{ij} = p_i\, q_j$ → spremenljivki X in Y sta neodvisni → presek je prazna množica



Za varnostni kod izračunamo Hammingove razdalje med vsemi pari kodnih zamenjav. Izkaže se, da je povprečna razdalja d, najmanjša razdalja d-3, največja pa d+2. Koliko napak lahko odkrijemo s tem varnostnim kodom?

$d_H = d$-3 je najmanjša razdalja med vsemi pari kodnih zamenjav
$e = d_H$-1 = d-4 je število napak, ki jih lahko odkrijemo

Podan imamo generatorski polinom g(p), s katerim želimo tvoriti sistematični ciklični kod. Opišite postopek za tvorbo kodnih zamenjav.

Podatkovni blok ***z*** zapišemo s polinomom $z(p)$.
Nastavek $n(p) = z(p)p^m$ delimo z generatorskim polinomom $g(p)$.
Ostanek zgornjega deljenja r(p) prištejemo nastavku: $x(p) = n(p) + r(p)$.
Polinom $x(p)$ pretvorimo v kodno zamenjavo ***x***.

Napišite Shannon-Nyquistov teorem. Pokažite od kod pride zveza.

$$\nu_s \geq 2\nu_c$$

ν_s je frekvenca vzorčenja
νs_c je najvišja frekvenca v signalu

Vzemimo, da imamo zelo dolg zapis zveznega signala na intervalu $[0, T)$. Če signal z najvišjo frekvenco νc razvijemo v Fourierovo vrsto, je osnovna frekvenca enaka $\nu 0 = 1/T$, vseh harmonikov pa je $\nu c/\nu 0 = \nu c T$. Pri razvoju v Fourierovo vrsto vsak harmonik nastopa dvakrat (sin, cos), signal torej enolično določimo z $2\nu cT$ koeficienti. Za izračun $2\nu cT$ koeficientov potrebujemo vsaj toliko meritev v časovnem prostoru, zato mora biti frekvenca vzorčenja vsaj $\nu s = 2\nu cT/T = 2\ \nu\_c$.

A) **V Matlabu imamo podano matriko za preverjanje sodosti H, ki ima 3 vrstice in 7 stolpcev. Podan imamo tudi vrstični vektor s dolžine 3, ki predstavlja sindrom. Zanima nas, kateremu stolpcu matrike H je enak sindrom s. Kateri od spodnjih ukazov nam pravilno vrne številko (indeks) ujemajočega stolpca?**

a) find(sum(s==H)==3) b) find(sum(s==H')==3) c) find(sum(s'==H')==3)

d) find(sum(s'==H,1)==3) e) find(sum(s'==H,2)==3) f) Nič od naštetega.

B) V Matlabu v spremenljivki M hranimo matriko dimenzije 3x4 (3 vrstice, 4 stolpci). Kateri ukaz nam v spremenljivko T zapiše srednja dva stolpca matrike M?

a) T = M(2:3); b) T = M(:,1:2); c) T = M(2:3,:); **d) T = M(:,2:3);** e) T = M(1:2,:); f) Nič od naštetega.

Opazujemo dva vira brez spomina, ki naključno oddajata različne znake z neničelnimi verjetnostmi. Vir A oddaja N znakov, vir B pa N+M znakov. Kateri vir je lahko bolj nedoločen? Odgovor utemeljite z enačbami. N in M sta naravni števili.

max $H(A) = \log_r N$

max $H(B) = \log_r (N+M)$

$\log_r (N+M) > \log_r (N)$

vir B je lahko bolj nedoločen

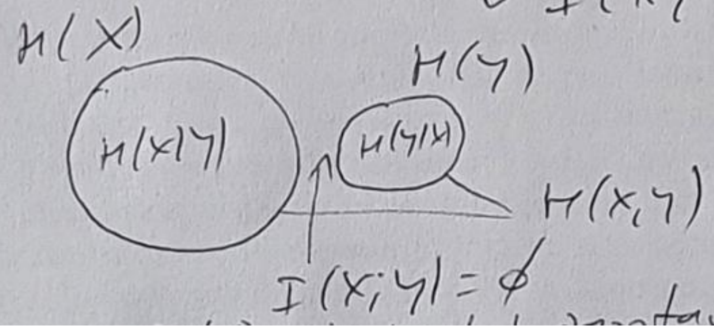
Opišite postopek kodiranja s Fanojevim kodom. Število znakov kodne abecede je večje od 1.

1. Znake razvrstimo po padajočih verjetnostih
2. Nato znake razdelimo v r čim bolj enako verjetnih skupin
3. Vsaki skupini priredimo enega od r znakov kodne abecede
4. Deljenje ponovimo na vsaki skupini dokler je potrebno

Opazujemo stohastično spremenljivko $X = \{x1, \dots, xN\}$ z verjetnostmi $PX = \{p1, \dots, pN\}$ in stohastično spremenljivko $Y = \{y1, \dots, yM\}$ z verjetnostmi $PY = \{q1, \dots, qM\}$, pi, $qj > 0$, $N > M$. Verjetnost, da spremenljivka X zavzame vrednost xi, spremenljivka Y pa vrednost yj je enaka $piqj$. Narišite ustrezen Vennov diagram in na njem označite entropiji, pogojni entropiji, vezano entropijo in medsebojno informacijo.

$p_{ij} = p(x_i, y_j) = p_i \cdot q_j$ → vira sta neodvisna

→ $I(X;Y) = 0$



Lihi pravokotni linearni bločni kod tvorimo tako, je vsota po vrsticah in stolpcih liha. Imamo $v \times s$ podatkovnih bitov, kjer je $v > 1$ označuje število vrstic in $s > 1$ število stolpcev. V katerih primerih ne moremo tvoriti lihega pravokotnega koda?

$$\begin{array}{cccc|c} z_{11} & z_{12} & \cdots & z_{1s} & s_{10} \\ z_{21} & & & & \vdots \\ \vdots & & & & \\ z_{v1} & \cdots & \cdots & z_{vs} & s_{v0} \\ \hline s_{01} & \cdots & \cdots & s_{0s} & s_{00} \end{array}$$

$s_{10} = z_{11} \oplus z_{12} \oplus \cdots \oplus z_{1s} \oplus 1$

$s_{v0} = z_{v1} \oplus z_{v2} \oplus \cdots \oplus z_{vs} \oplus 1$

$s_{01} = z_{11} \oplus z_{21} \oplus \cdots \oplus z_{v1} \oplus 1$

$s_{0s} = z_{1s} \oplus z_{2s} \oplus \cdots \oplus z_{vs} \oplus 1$

$$s_{00} = s_{10} \oplus \cdots \oplus s_{v0} \oplus 1 \stackrel{?}{=} s_{01} \oplus \cdots \oplus s_{0s} \oplus 1$$

$$= \underbrace{1 \oplus \cdots \oplus 1}_{v \text{ enic}} \stackrel{?}{=} \underbrace{1 \oplus \cdots \oplus 1}_{s \text{ enic}}$$

Lihega pravokotnega koda ne moremo tvoriti, če je v lih in s sod ali če je v sod in s lih.

Podana je periodična funkcija $x(t) = x(t + T)$, $T > 0$. Napišite razvoj funkcije v Fourierovo vrsto skupaj z enačbami za izračun koeficientov razvoja.

$$x(t) = \frac{1}{2}a_0 + \sum_{n=1}^{\infty} a_n \cos(n\omega_0 t) + \sum_{n=1}^{\infty} b_n \sin(n\omega_0 t)$$

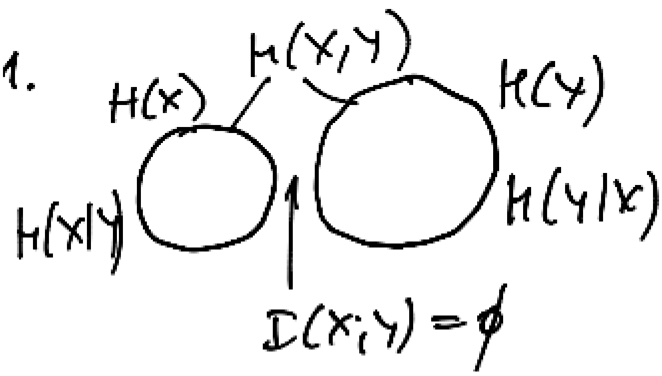
$$\omega_0 = \frac{2\pi}{T}$$

$$a_n = \frac{2}{T}\int_0^T x(t)\cos(n\omega_0 t), \quad n \geq 0$$

$$b_n = \frac{2}{T}\int_0^T x(t)\sin(n\omega_0 t), \quad n \geq 1$$

Opazujemo stohastično spremenljivko $X = \{x1, \ldots, xN\}$ z verjetnostmi $PX = \{p1, \ldots, pN\}$ in stohastično spremenljivko $Y = \{y1, \ldots, yM\}$ z verjetnostmi $PY = \{q1, \ldots, qM\}$, pri čemer velja $pi = N$ -1, $qj = M-1$ in $0 < N < M$. Spremenljivki v nekem trenutku zavzameta vrednosti xi in yj z verjetnostjo $piqj$. Narišite ustrezen Vennov diagram in na njem označite entropiji, pogojni entropiji, vezano entropijo in medsebojno informacijo.

1.



Vir brez spomina oddaja znake X = {$x1$, … , xN} z verjetnostmi PX = {$p1$, … , pN}, N > 0. Znake kodiramo z nesingularnim, enoznačnim in netrenutnim kodom z dolžinami kodnih zamenjav, lX = {$l1$, … , lN}. Kako lahko ugotovimo, ali je ta kod optimalen ali ne?

$X = \{x_1, \dots, x_N\}$
$P_X = \{p_1, \dots, p_N\}$
$l_X = \{l_1, \dots, l_N\}$

→ tvorimo Huffmanov kod, vzemimo, da so dolžine kodnih zamenjav $h_X = \{h_1, \dots, h_N\}$

$$L_H = \sum_{i=1}^{N} p_i \cdot h_i$$

Za netrenutni kod velja $L_K = \sum_{i=1}^{N} p_i \cdot l_i$

Če je $L_K = L_H$, je kod optimalen.

Z enačbami opišite postopek uporabe linearnega bločnega varnostnega koda: gradnje kodne zamenjave, prenosa čez kanal in uporabe varnostnega koda pri odkrivanju in popravljanju napak. Opišite generatorsko matriko in matriko za preverjanje sodosti ter podajte zvezo med njima. Vse uporabljene oznake na kratko opišite.

a. $\vec{z}$ – k znakov, ki jih želimo poslati čez kanal
b. $\vec{x}$ (kodna zamenjava) = $\vec{z}$*G ← generatorska matrika G = (   ) k
n
c. $\vec{y}$ = $\vec{x}$ + $\vec{e}$ ← napaka v kanalu
d. $\vec{s}$ = $\vec{y}$*H^T ← paritetna matrika H = ( ) k
n
e. $\vec{p}$ = f($\vec{s}$) ← iz sindroma določimo popravljalnik
f. $\vec{x}'$ = $\vec{y}$ + $\vec{p}$ ← iz niza $\vec{y}$ določimo najbližjo kodno zamenjavo
g. $\vec{z}$' ← iz kodne zamenjave $\vec{x}'$ določimo podatkovne bite; kar lahko narobe popravimo, je lahko $\vec{z}$' =/= $\vec{z}$

Pri kodiranju se pogosto zgodi, da je povprečna dolžina kodnih zamenjav gospodarnega koda precej večja od entropije. Pokažite, da z združevanjem znakov v bloke povprečna dolžina kodnih zamenjav lahko poljubno približa entropiji! Predpostavite, da so znaki v bloku medsebojno neodvisni.

$$X^m = \underbrace{X \cdot X \cdots X}_{m}, \quad H_r(X^m) = m \cdot H_r(X)$$

$$H_r(X^m) \leq L_m < H_r(X^m) + 1$$

$$m H_r(X) \leq L_m < m H_r(X) + 1$$

$$H_r(X) \leq \frac{L_m}{m} < H_r(X) + \frac{1}{m}$$

$$\lim_{m \to \infty} \frac{1}{m} \to 0 \Rightarrow \lim_{m \to \infty} \frac{L_m}{m} = H_r(X)$$

Potrdite ali ovrzite spodnji trditvi o Shannonovem kodu. a. Kod je gospodaren. b. Kod je trenuten. Odgovora utemeljite!

2. a) $l_i = \lceil -\log_r p_i \rceil$

$$-\log_r p_i \leq l_i < -\log_r p_i + 1$$

$$\sum_{i=1}^{m} p_i(-\log_r p_i) \leq \sum_{i=1}^{m} p_i l_i < \sum_{i=1}^{m} p_i(-\log_r p_i) + 1$$

$$H(X) \leq L < H(X) + 1 \rightarrow \text{kod } \underline{\text{je gospodaren}}$$

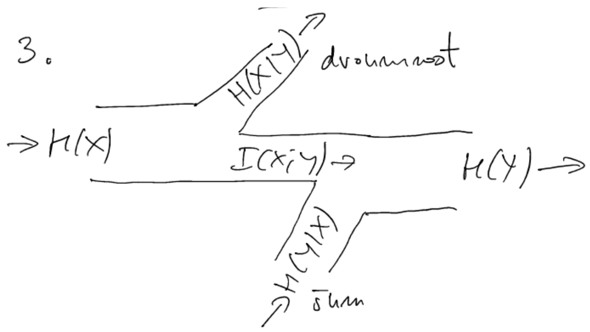
b) – s pretvorbo delnih vsot v bazo r poskrbimo, da so kodne zamenjave različne

– z razvrščanjem znakov po padajočih verjetnostih pred pretvarjanjem poskrbimo, da nobena kodna zamenjava ni predpona drugi.

→ kod <u>je trenuten</u>

Stohastični vir brez spomina oddaja $N > 0$ znakov v diskretni kanal brez spomina. Na izhodu iz kanala dobimo enake znake, vendar so njihove verjetnosti spremenjene. Narišite sliko prenosa informacije čez kanal in napišite enačbo dvoumnosti v odvisnosti od verjetnosti vhodnih znakov in prehodnih verjetnosti kanala.

3.



$X = \{x_1, \dots, x_r\}$

$P_X = \{p(x_1), \dots, p(x_r)\}$

$Y = \{y_1, \dots, y_s\}$

$P_Y = \{p(y_1), \dots, p(y_s)\}$

$$p(y_j) = \sum_{i=1}^{r} p(y_j|x_i)\, p(x_i)$$

$$p(x_i, y_j) = p(x_i, y_j)$$

$$p(y_j|x_i)\cdot p(x_i) = p(x_i|y_j)\cdot p(y_j)$$

$$p(x_i|y_j) = p(y_j|x_i)\cdot \frac{p(x_i)}{p(y_j)}$$

$$H(X|Y) = \sum_{j=1}^{s} p(y_j)\cdot H(X|Y=y_j)$$

$$H(X|Y=y_j) = \sum_{i=1}^{r} p(x_i|y_j) \log p(x_i|y_j)$$

Podan imamo generatorski polinom, s katerim želimo tvoriti sistematični ciklični kod. Opišite postopek za tvorbo generatorske matrike.

4. $st[g(p)] = m$, št. podatkov $= k$

Določimo kodne zamenjave za vseh k nizov, ki imajo samo eno enico. Kodne zamenjave določimo na osnovi deljenja. Iz kodnih zamenjav sestavimo matriko G tako, da je podmatrika velikosti $k \times k$ na levi identiteta.

$$G = \left(\begin{array}{cccc|c} 1 & 0 & \dots & 0 & \\ 0 & 1 & \dots & 0 & \\ 0 & 0 & 1 & 0 & \\ 0 & \dots & 0 & 1 & \end{array}\right) \Big\} k$$

$\underbrace{\quad}_{k}$ $\underbrace{\quad}_{m}$

identiteta

vsaka vrstica je ena kodna zamenjava

Podana je periodična funkcija $x(t) = x(t + T)$, $T > 0$. Napišite razvoj funkcije v Fourierovo vrsto in enačbe za izračun koeficientov razvoja.

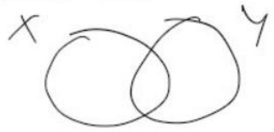
$$f(t) = \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos(n\omega_0 t) + \sum_{n=1}^{\infty} b_n \sin(n\omega_0 t)$$

$$\omega_0 = \frac{2\pi}{T}$$

$$a_n = \int_0^T f(t) \cos(n\omega_0 t)\, dt$$

$$b_n = \int_0^T f(t) \sin(n\omega_0 t)\, dt$$

Verjetnostni spremenljivki X in Y sta medsebojno odvisni. Kolikšno napako naredimo pri računanju skupne nedoločenosti, če predpostavimo, da sta spremenljivki neodvisni? Odgovor utemeljite!



neodvisni : $H_n(X,Y) = H(X) + H(Y)$

odvisni : $H_o(X,Y) = H(X) + H(Y|X)$

$$\Delta H = H_n(X,Y) - H_o(X,Y) = H(Y) - H(Y|X)$$

$$= \underline{\underline{I(X;Y)}}$$

Osnovno abecedo sestavlja n znakov, kodirno abecedo pa r znakov. Z neznanim nesingularnim in enoznačnim kodom so znake osnovne abecede pretvorili v kodne zamenjave. Vse, kar vemo o kodu, so dolžine kodnih zamenjav vseh znakov osnovne abecede. Napišite matematično zvezo, s katero enostavno preverimo, da kod ni trenuten?

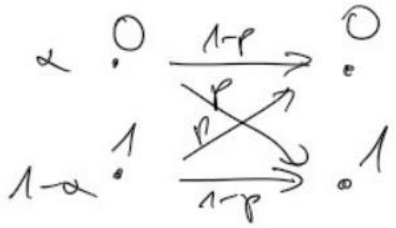
$A = \{a_1, \dots, a_n\}$

$L = \{l_1, \dots, l_n\}$

$B = \{b_1, \dots, b_r\}$

$$\sum_{i=1}^{n} r^{-l_i} > 1$$

Vir brez spomina oddaja znaka 0 in 1 v binarni simetrični kanal. Pri kakšnih verjetnostih za napako v kanalu je mogoča pravilna rekonstrukcija oddanih znakov?



$C = 1 - H(p, 1-p)$

$C = 1 \rightarrow H(p, 1-p) = 0$

$\hookrightarrow p = 0$

$\hookrightarrow p = 1$

Kakšna je pri cikličnih kodih povezava med matrikama G in H ter polinomoma g(p) in h(p) pri kodiranja na osnovi množenja? Pokažite na primeru C(7, 4), g(p) = p3+p+1.

$$g(p) = p^m + g_{m-1}p^{m-1} + \dots + g_1 p + 1$$
$$h(p) = 1 + h_1 p + \dots + h_{k-1}p^{k-1} + p^k$$

$$G = \begin{array}{c} \\ 1 \\ \\ \\ k \end{array}\left[\begin{array}{ccccccccc} 1 & g_{m-1} & \cdots & g_1 & 1 & & & \emptyset & \\ & 1 & g_{m-1} & \cdots & g_1 & 1 & & & \\ & \emptyset & & & \vdots & & & & \\ & & & & 1 & g_{m-1} & \cdots & g_1 & 1 \end{array}\right]^{n} \qquad H = \begin{array}{c} \\ 1 \\ \\ \\ m \end{array}\left[\begin{array}{ccccccccc} 1 & h_1 & \cdots & h_{k-1} & 1 & & & \emptyset & \\ & 1 & h_1 & \cdots & h_{k-1} & 1 & & & \\ & \emptyset & & & \vdots & & & & \\ & & & & 1 & h_1 & \cdots & h_{k-1} & 1 \end{array}\right]^{n}$$

$C(7,4)\quad g(p) = p^3+p+1\quad,\quad h(p) = p^7+1 : p^3+p+1 = p^4+p^2+p+1$

$$\cancel{p^7}+\cancel{p^5}+\cancel{p^4}$$
$$\cancel{p^5}+p^3+p^2$$
$$\cancel{p^4}+\cancel{p^2}+p$$

$$h(p) = 1+p+p^2+p^4$$

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Realni signal vzorčimo z računalnikom, nato pa zajete vzorce analiziramo v frekvenčnem prostoru. V katerem primeru izračunani spekter signala ne ustreza dejanskemu spektru? Za tak primer skicirajte izbrani dejanski spekter in ustrezni izračunani spekter.

Če je $\nu_s < 2\nu_c$ pride do prekrivanja frekvenc