Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Teorija informacij in sistemov

Andrej Dobnikar

Ljubljana, marec 2009

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

621.391(075.8)
519.72(075.8)

DOBNIKAR, Andrej
Teorija informacij in sistemov / Andrej Dobnikar ; [izdajatelj] Fakulteta za računalništvo in informatiko. - 1. izd. - Ljubljana : Založba FE in FRI, 2009

ISBN 978-961-6209-71-7 (Fakulteta za računalništvo in informatiko)

244409600

Recenzenta: dr. Uroš Lotrič, dr. Branko Šter
Založnik: Založba FE in FRI, Ljubljana
Izdajatelj: Fakuleta za računalništvo in informatiko, Ljubljana
Urednik: mag. Peter Šega

Natisnil: Fakulteta za računalništvo in informatiko, Ljubljana
Naklada: 200 izvodov
1. izdaja

Kazalo

Poglavje 1

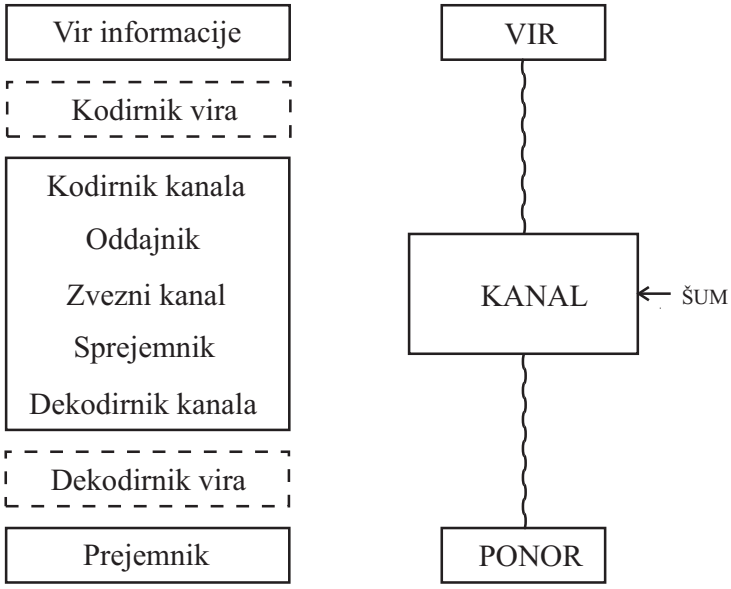
Uvod

Informacija je osnovna veličina, na osnovi katere je mogoče graditi znanje in ustvarjati nove vrednote. Na osnovi informacije je definirana osnovna enota (bit), ki je najmanjši podatek, ki ga lahko hrani računalniški pomnilnik. Vendar pa informacija ni sama sebi namen, ustvarjena je zato, da jo sprejme uporabnik, ki mu je namenjena. To pa zahteva njeno potovanje, največkrat po prenosnem mediju (kanalu), ki vnaša šum. Zato je potrebno kodiranje, najprej za kompresijo podatkov in nato še zaradi odpornosti na šum. Velikokrat informacijo zapišemo tudi v šifrirni obliki, zato da ni čitljiva nepooblaščeni osebi. S temi lastnostmi smo opisali pot informacije od izvora do ponora in vse čeri, ki jo na poti spremljajo. Pri podrobnejšemu opisu te poti se srečamo s postopki kodiranja vira informacij, ki nas seznanijo s spodnjo mejo podatkovne kompresije in s praktičnimi postopki kodiranja. Seznanimo se s komunikacijskim kanalom in varnostnim kodiranjem/dekodiranjem, kjer obstaja pomemben pogoj (kanalski teorem), ki mora biti izpolnjen pri prenosu skozi kanal, da zagotavlja kvalitetno dekodiranje na strani ponora informacije (prenos brez napak). Na problem šifriranja in dešifriranja je mogoče gledati tudi kvalitativno s pomočjo informacijske teorije. Nosilec informacij po poti od izvora k ponoru so signali, ki jih je skupaj s njihovimi preslikavami mogoče opisovati v jeziku matematičnih transformacij, kot so Fourierjeva, Laplaceova in Z- transformacija. Pri opisovanju prenosnih funkcij na poti signalov se soočamo z različnimi kategorijami sistemov, od katerih so najzanimivejši zaradi svoje preprostosti linearni in časovno neodvisni sistemi. Z njimi je mogoče na osnovi superpozicije določati izhodne funkcije za poljubne vhode, če je le poznan odziv na enotino (delta) funkcijo. Pri bolj kompliciranih sistemih, ki so časovno odvisni (in torej dinamični) pa ločimo med sistemi s končno globino pomnilnika in sistemi z neskončnim pomnilnikom (tudi rekurzivni sistemi). Pri njih običajno opisujemo delovanje z diferenčnimi enačbami, ki jih klasično rešujemo lahko z matematično indukcijo, konvolucijo ali pa s pomočjo Z transformacije. Slednja omogoča dokazati teorem vzorčenja, ki zahteva opazovanje signalov z dvakratno ali večjo frekvenco od najvišje frekvence v signalu (kar sledi iz Fourierjeve vrste), če naj pri takšnem diskretiziranju signalov ne pride do izgube informacije. Poleg tega je s pomočjo Z - transformacije mogoče reševati diferenčne enačbe, predvsem kadar zaradi kompleksnosti indukcija ali konvolucija nista primerni. Delo Teorija informacij in sistemov opisuje osnovne lastnosti informacij in njenih prenosov od izvora k ponoru. Podaja osnovne pojme kodiranja v funkciji podatkovne kompresije in varovanja pred šumom ter računanja prenosnih funkcij na poti signalov s pomočjo matematičnih transformacij. Informacije postajajo vedno pomembnejše tudi v luči sodobnih inteligentnih sistemov, kjer jih lahko uporabljamo kot kriterijske funkcije brez omejitve (n.pr. Gaussova porazdelitev napake, ki je pogoj pri kriterijski funkcije srednjega kvadrata napake) v postopku učenja neznanih preslikav.

1.1 Tri osnovna vprašanja informacijske teorije

- Kaj določa končno kompresijo podatkov ?
  (Odgovor: entropija) - I. Shannonov teorem
- Kaj določa končno hitrost komunikacije ?
  (Odgovor: kapaciteta kanala) - II. Shannonov teorem
- Kaj določa frekvenco vzorčenja ?
  (Odgovor: največja frekvenca v signalu) - III. Shannonov teorem

1.2 Komunikacijski sistem (KS):



Poglavje 2

Entropija

Shannon je v 50-tih letih definiral komunikacijski sistem (KS) kot naključni dinamični sistem. Zanj je definiral veličino (**entropijo**), ki določa (podaja) **mero nedoločenosti**.

Vzemimo dinamični, diskretni, naključni sistem z n stanji: $\mathbf{x_1}, \mathbf{x_2}, \mathbf{x_3}, \ldots, \mathbf{x_n}$ in verjetnosti stanj: $\mathbf{p_1}, \mathbf{p_2}, \mathbf{p_3}, \ldots, \mathbf{p_n}$ Velja: $\mathbf{p_i} \geq \mathbf{0}$, $\sum_{\mathbf{i}} \mathbf{p_i} = \mathbf{1}$.

Za mero nedoločenosti sistema vzamemo $\mathbf{H}(\mathbf{p_1}, \mathbf{p_2}, \ldots, \mathbf{p_n})$, ter predpostavimo da velja:

1. $H(p_1, p_2, \ldots, p_n) \geq 0$; enakost le, če je nek $p_i = 1$
   (nedoločenost je nenegativna količina, ki je enaka 0 v statičnih nenaključnih sistemih),

2. $H(p_1, p_2, \ldots, p_n)$ je največje pri $p_1 = p_2 = \ldots = p_n = \frac{1}{n}$
   (nedoločenost je največja, če so vsa stanja enako verjetna),

3. $H(\frac{1}{n}, \ldots \frac{1}{n}) \;\geq\; H(\frac{1}{m}, \ldots \frac{1}{m})$, če $n > m$
   (sistem z več stanji je bolj nedoločen),

4. $H(p_1, p_2, \ldots, p_n)$ ni odvisna od permutacije števil $p_1, p_2, \ldots, p_n$,

5. $H(p_1, p_2, \ldots, p_n, 0) = H(p_1, p_2, \ldots, p_n)$,

6. $H(p_1, p_2, \ldots, p_n)$ je zvezna funkcija
   (majhna sprememba verjetnosti stanj ne more znatno spremeniti nedoločenosti sistema),

7. Pri $m, n \in \mathbb{N}$ velja: $H(\frac{1}{m \cdot n}, \ldots, \frac{1}{m \cdot n}) = H(\frac{1}{m}, \ldots, \frac{1}{m}) + H(\frac{1}{n}, \ldots, \frac{1}{n})$
   (pri dveh neodvisnih sistemih z m in n enako verjetnimi stanji, je skupna nedoločenost enaka vsoti nedoločenosti obeh posameznih sistemov),

8. Za $m, n \in \mathbb{N}$ in $p = p_1 + p_2 + \ldots + p_m,\ r = r_1 + r_2 + \ldots + r_n$,
   $p_i \geq 0,\ r_j \geq 0,\ i = 1 \ldots m,\ j = 1 \ldots n$, ter $p + r = 1$, velja:
   $H(p_1, \ldots, p_m,\ r_1, \ldots, r_n) = H(p, r) + p \cdot H(\frac{p_1}{p}, \ldots, \frac{p_m}{p}) + r \cdot H(\frac{r_1}{r}, \ldots, \frac{r_n}{r})$
   (če sistem lahko razvrstimo v dva razreda stanj, je nedoločenost sistema enaka vsoti nedoločenosti, da je stanje iz enega izmed obeh razredov in obteženih vsot nedoločenosti stanj v razredih)

Če $H(p_1, \ldots, p_n)$ zadošča postavkam $1, \ldots, 8$, potem je lahko enaka:

$$H(p) = H(p_1, \ldots, p_n) = -K \sum_{i=1}^{n} p_i \cdot \log_d p_i$$

$K > 0$ - poljubna konstanta

$d > 1$ - osnova logaritma

$H(p)$ **je ENTROPIJA oziroma mera nedoločenosti dinamičnega, naključnega in diskretnega sistema.**

Pišemo tudi: $H(D_n),\ D_n = (p_1, \ldots, p_n) \in \Delta_n$

Navadno je $K = 1$ in $d = 2$, tedaj je enota bit

$= e$, tedaj je enota nit

Ker je: $\log_b p = \log_b a \cdot \log_a p$

je tudi: $H_b = \log_b a \cdot H_a$

(npr.: $H_2 = \log_2 e \cdot H_e$)

2.1 Lastnosti entropije

1. $0 \leq H(p_1, \ldots, p_n) \leq H(\frac{1}{n}, \ldots, \frac{1}{n}) = K \cdot \log_d n = \log_2 n$
   Zgornjo mejo entropije določa logaritem števila stanj sistema.

2. Ker velja enačba za matematično upanje (srednja vrednost):

   $$E(g(X)) = \sum_i p_i \cdot g(x_i),$$

   je entropija pričakovana vrednost funkcije $g(X) = \log \frac{1}{p(X)}$:

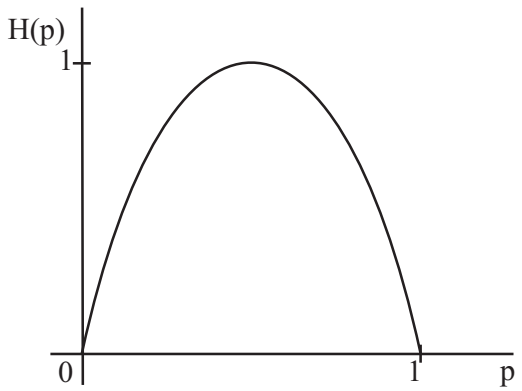
   $$H(D_n) = \sum_i p_i \cdot \log \frac{1}{p_i} = E\left(\log \frac{1}{p(X)}\right)$$

PRIMER 1:

Vzemimo sistem z dvemi stanji ($n = 2$) in zalogo vrednosti $Z(X) = (a, b)$ z $p(a) = p,\ p(b) = 1 - p$. Tedaj je:

$H(p, 1-p) = (-p \cdot \log\ p) - ((1-p) \cdot \log(1-p)) \stackrel{\triangle}{=} H(p)$

$H(p)$ je konkavna funkcija spremenljivke p. Pri $p = 0$ in $p = 1$ ni negotovosti.



◇

PRIMER 2:

$Z(X) = (a,\ b,\ c,\ d)$
$P = \left(\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8}\right)$

$H(X) = ?$

$$\begin{aligned} H(X) &= H\left(\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8}\right) \\ &= -\frac{1}{2}\log\frac{1}{2} - \frac{1}{4}\log\frac{1}{4} - \frac{1}{8}\log\frac{1}{8} - \frac{1}{8}\log\frac{1}{8} \\ &= 1,75 \text{ bitov} \end{aligned}$$

1,75 je tudi pričakovano (povprečno) število binarnih vprašanj, da uganemo, v katerem stanju je sistem.

1. vprašanje: Ali je $X = a$?
2. vprašanje: Če ni, ali je $X = b$?
3. vprašanje: Če ni, ali je $X = c$?

V našem primeru je 1,75 hkrati tudi minimalno pričakovano število binarnih vprašanj.
V splošnem je minimalno pričakovano število binarnih vprašanj med H(X) in H(X)+ 1.
(glej tudi I. Shannonov teorem)
◇

2.2 Entropija diskretnih naključnih spremenljivk

$X,\ Z(X) = (x_1, \ldots, x_n)$ - 1 spremenljivka
$P(X) = (p_1, \ldots, p_n)$

$$H(X) = -K \sum_{i=1}^{n} p_i \cdot \log_d p_i = -\sum_i p_i \cdot \log p_i$$
$$H(X) = H(p_1, \ldots, p_n) = H(D_n),\ D_n \in \Delta_n$$

2.2.1 Entropija para diskretnih naključnih spremenljivk

Par $X,\ Y$; $Z(X,Y) = \{(x_i, y_j)\}_{\substack{i=1\ldots m;\\ j=1\ldots n}}$,
$P(X,Y) = \{(p_{ij})\}$

$$p_{ij} = P(X = x_i,\ Y = y_j) \geq 0$$
$$\sum_i \sum_j p_{ij} = 1$$

- Entropija para diskretnih naključnih spremenljivk:

$$H(X,Y) = -K \sum_{i=1}^{m} \sum_{j=1}^{n} p_{ij} \cdot \log_d p_{ij} = -\sum_i \sum_j p_{ij} \cdot \log p_{ij}$$
$$H(X,Y) = H(D_{mn}),\ D_{mn} \in \Delta_{mn}$$

$$H(X) = -\sum_i p_i \cdot \log p_i\ ;\ p_i = \sum_j p_{ij}$$
$$H(Y) = -\sum_j p'_j \cdot \log p'_j\ ;\ p'_j = \sum_i p_{ij}$$

- Entropija spremenljivke X, ko je spremenljivka Y enaka y_j:

$$H(X|Y = y_j) = -\sum_i p_{i|j} \cdot \log p_{i|j}\ ;\ p_{i|j} = \frac{p_{ij}}{p'_j}$$

- Entropija spremenljivke Y, ko je spremenljivka X enaka x_i:

$$H(Y|X = x_i) = -\sum_j p'_{j|i} \cdot \log p'_{j|i}\ ;\ p'_{j|i} = \frac{p_{ij}}{p_i}$$

- Entropija spremenljivke X, ko poznamo spremenljivko Y:

$$H(X|Y) = \sum_j p'_j \cdot H(X|Y = y_j) = -\sum_j \sum_i p'_j \cdot p_{i|j} \cdot \log p_{i|j} = -\sum_i \sum_j p_{ij} \cdot \log p_{i|j}$$

- Podobno :

$$H(Y|X) = -\sum_i p_i \cdot H(Y|X = x_i) = -\sum_i \sum_j p_i \cdot p'_{j|i} \cdot \log p'_{j|i} = -\sum_i \sum_j p_{ij} \cdot \log p'_{j|i}$$

$H(X|Y)$ je pogojna entropija spremenljivke X glede na spremenljivko Y,

$H(Y|X)$ pa je pogojna entropija spremenljivke Y glede na spremenljivko X.

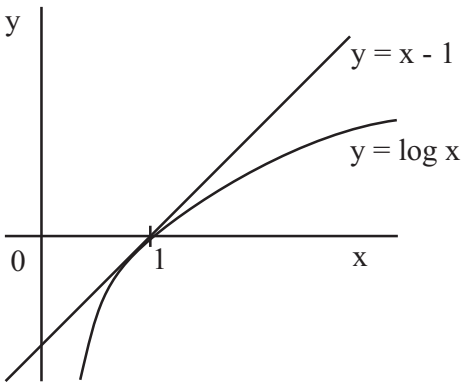
Lastnosti entropije para spremenljivk

1. $H(X|Y) \leq H(X)$
2. $H(Y|X) \leq H(Y)$
3. $H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$
4. $H(X) + H(Y) \geq H(X,Y)$

Dokazi:
Ad 4.)

$$\begin{aligned}
H(X) &= -\sum_i p_i \cdot \log p_i = -\sum_i \sum_j p_{ij} \cdot \log p_i \\
H(Y) &= -\sum_j p'_j \cdot \log p'_j = -\sum_i \sum_j p_{ij} \cdot \log p'_j \\
H(X) + H(Y) &= -\sum_i \sum_j p_{ij} \cdot (\log p_i + \log p'_j) \\
&= -\sum_i \sum_j p_{ij} \cdot \log(p_i \cdot p'_j) \\
&= -\sum_i \sum_j p_{ij} \cdot \log p'_{ij} \ ; \ p'_{ij} = p_i \cdot p'_j
\end{aligned}$$

Ker je $\sum_i p_i \cdot \log p'_i \leq \sum_i p_i \cdot \log p_i$, pri pogoju $\sum_i p_i = \sum_i p'_i = 1$, zaradi:



$$\log x \leq x - 1 \ ; \ x = \frac{p'_i}{p_i}$$

$$\log p'_i - \log p_i \leq \frac{p'_i}{p_i} - 1$$

$$p_i \cdot \log p'_i - p_i \cdot \log p_i \leq p'_i - p_i$$

$$\sum_i p_i \cdot \log p'_i - \sum_i p_i \cdot \log p_i \leq \sum_i p'_i - \sum_i p_i = 0$$

$$\sum_i p_i \cdot \log p'_i \leq \sum_i p_i \cdot \log p_i$$

in ker je

$$H(X,Y) = -\sum_i \sum_j p_{ij} \cdot \log p_{ij}$$

sledi:

$$\sum_i \sum_j p_{ij} \cdot \log p'_{ij} \leq \sum_i \sum_j p_{ij} \cdot \log p_{ij}$$

oz.

$$-\sum_i \sum_j p_{ij} \cdot \log p'_{ij} \geq -\sum_i \sum_j p_{ij} \cdot \log p_{ij}$$

kar je ravno

$$H(X) + H(Y) \geq H(X,Y) \ .$$

Ad 3.)

$$\begin{aligned}
H(X,Y) &= -\sum_i \sum_j p_{ij} \cdot \log p_{ij} = \\
&= -\sum_i \sum_j p_{ij} \cdot \log p_i \cdot p'_{j/i} = \\
&= -\sum_i \sum_j p_{ij} \cdot \log p_i - \sum_i \sum_j p_{ij} \cdot \log p'_{j/i} = \\
&= -\sum_i p_i \cdot \log p_i + H(Y|X) = \\
&= H(X) + H(Y|X) = \\
&= -\sum_i \sum_j p_{ij} \cdot \log p'_j \cdot p_{i/j} = \\
&= -\sum_i \sum_j p_{ij} \cdot \log p'_j - \sum_i \sum_j p_{ij} \cdot \log p_{i/j} \\
&= -\sum_j p'_j \cdot \log p'_j + H(X|Y) = \\
&= H(Y) + H(X|Y)
\end{aligned}$$

Ad 2, 1.) Z uporabo dokazov 3, 4 sledi:

$$H(X) \geq H(X|Y)$$
in
$$H(Y) \geq H(Y|X)$$

2.2.2 Entropija n diskretnih naključnih spremenljivk

$$X_1, \ldots, X_n; \quad Z(X_1, \ldots, X_n) = \{(x_{1_i}, \ldots, x_{n_i})\},$$
$$P(X_1, \ldots, X_n) = \{(p_{1_i} \ldots p_{n_i})\}$$

- Skupna entropija n diskretnih naključnih spremenljivk

$$\begin{aligned} H(X_1, \ldots, X_n) &= H(X_1) + H(X_2|X_1) + H(X_3|X_1, X_2) + \ldots + H(X_n|X_1, \ldots, X_{n-1}) \\ &= \sum_i H(X_i|X_1, \ldots, X_{i-1}) \ - \ \text{verižno pravilo} \end{aligned}$$

Dokaz:

$$\begin{aligned} H(X_1, X_2) &= H(X_1) + H(X_2|X_1) \\ H(X_1, X_2, X_3) &= H(X_1) + H(X_2, X_3|X_1) = \\ &= H(X_1) + H(X_2|X_1) + H(X_3|X_1, X_2) \\ &\vdots \\ H(X_1, \ldots, X_n) &= \sum_i H(X_i|X_1, \ldots, X_{i-1}) \end{aligned}$$

- Zveza med skupno entropijo in entropijami posameznih spremenljivk:

$$H(X_1, \ldots, X_n) \underset{\uparrow}{\leq} H(X_1) + \ldots + H(X_n) = \sum_i H(X_i)$$

Enakost velja, če so spremenljivke neodvisne

2.3 Entropija zveznih naključnih spremenljivk

X - naključna spremenljivka s **porazdelitveno funkcijo**

$$F(x) = P(X \leq x)$$

X je **zvezna** če je $F(x)$ zvezna nad množico vseh realnih števil $\mathbb{R}$.

Odvod porazdelitvene funkcije označimo z:

$$F'(x) = f_X(x)$$

Če je $\int_{-\infty}^{+\infty} f_X(x)dx = 1$, pravimo funkciji $f_X(x)$ **funkcija verjetnostne gostote** spremenljivke X. Množica x $\in \mathbb{R}$, za katero je $f_X(x) > 0$, imenujemo **podporna množica** naključne spremenljivke X $(\wp)$.

Entropija zvezne naključne spremenljivke X, ki je dana z gostoto verjetnosti $f_X(x), x \in \mathbb{R}$:

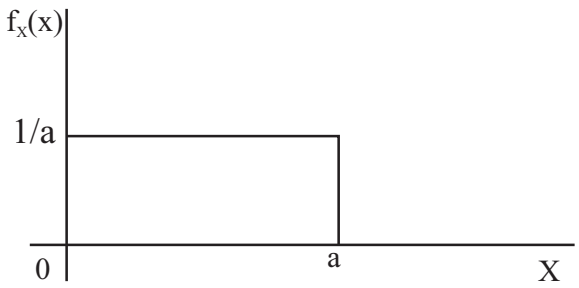
$$\underset{\substack{\uparrow \\ \text{POZOR: } H(X) \text{ lahko} \\ \text{tukaj tudi negativna (zato} \\ \text{pri zveznih sistemih} \\ \text{izgubi fizikalni pomen)}}}{H(X)} = -K \int_{\wp} f_X(x) \cdot \log_d f_X(x) dx$$

$K > 0$ – poljubna konstanta
$d > 1$ – osnova logaritma
(običajno $K = 1,\ d = 2$)

PRIMER 3:

Zvezna spremenljivka X je podana z gostoto verjetnosti

$$f_X(x) = \begin{cases} \frac{1}{a}, & 0 \le x \le a; \\ 0, & x > a,\ x < 0 \end{cases}$$



$$H(X) = -\int_0^a \frac{1}{a} \cdot ln\frac{1}{a}\ dx =$$
$$= \ln\ a \text{ (nit-ov)}$$

◇

PRIMER 4:

Zvezna spremenljivka X je porazdeljena normalno (z Gaussovo porazdelitvijo), s srednjo vrednostjo μ in varianco σ^2. Določite $H(X)$.

$$f_X(x) = \frac{1}{\sigma\sqrt{2\pi}}\ e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

$$
\begin{aligned}
H(X) &= -\int_{-\infty}^{+\infty} f_X(x) \left[-ln\ \sigma\sqrt{2\pi} - \frac{(x-\mu)^2}{2\sigma^2} \right]\ dx = \\
&= ln\ \sigma\sqrt{2\pi} \int_{-\infty}^{+\infty} f_X(x)\ dx + \frac{1}{2\sigma^2} \int_{-\infty}^{+\infty} (x-\mu)^2 f_X(x)\ dx \\
&= ln\ \sigma\sqrt{2\pi} \cdot 1 + \frac{1}{2\sigma^2} \cdot \sigma^2 = \\
&= ln\ \sqrt{2\pi\sigma^2} + \frac{1}{2} \cdot ln\ e \\
&= ln\ \sqrt{2\pi e\sigma^2} \quad \text{(nit-ov)}
\end{aligned}
$$

◇

- Med vsemi zveznimi naključnimi spremenljivkami z omejeno varianco ima največjo entropijo tista spremenljivka, ki je porazdeljena normalno.

Velja torej:

$$
\begin{aligned}
H(X) &\leq \log \sqrt{2\pi e\sigma^2} \\
&\uparrow \\
&\text{enakost velja v primeru normalne porazdelitve}
\end{aligned}
$$

2.3.1 Entropija para zveznih naključnih spremenljivk

Par (X, Y) naključnih spremenljivk X in Y ima **zvezno porazdelitveno funkcijo $\mathbf{F(x, y)}$**, definirano nad $\mathbb{R}^2$.
Odvod po obeh spremenljivkah označimo z:

$$f(x, y) = \frac{\delta^2 F(x, y)}{\delta x\ \delta y}$$

Če je: $\displaystyle\int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} f(x, y)\ dx\ dy = 1$, je

$f(x, y)$ je gostota verjetnosti para spremenljivk (X, Y)

Točke, v katerih je $f(x, y) > 0$ tvorijo podporno množico para (X,Y).

Vpeljemo oznaki:

$$
\begin{aligned}
f_X(x) = F_1'(x) &= \int_{-\infty}^{+\infty} f(x, y)\ dy \\
f_Y(y) = F_2'(y) &= \int_{-\infty}^{+\infty} f(x, y)\ dx
\end{aligned}
$$

$$
\left.\begin{array}{ll}
\text{kjer je:} & F_1(x) = F(x, \infty) \\
\text{in:} & F_2(y) = F(\infty, y)
\end{array}\right\} \quad \text{enorazsežni robni porazdelitvi}
$$

- Entropija para zveznih, naključnih spremenljivk je:

$$H(X,Y) = -K \int\int_{\wp_2} f(x,y) \cdot \log_d f(x,y)\ dx\ dy$$

$\wp_2$ - podporna množica

$K > 0, \quad d > 1$

- Entropija zvezne spremenljivke X, ko poznamo Y:

$$H(X|Y) = -K \int\int_{\wp_2} f(x,y) \cdot \log_d \frac{f(x,y)}{f_Y(y)}\ dx\ dy$$

Podobno velja tudi za $H(Y|X)$

2.3.2 Entropija n zveznih naključnih spremenljivk

$$H(X_1,\ldots,X_n) = -K \int\int_{\wp_n} f(x_1,\ldots,x_n) \cdot \log_d f(x_1,\ldots,x_n)\ dx_1\ dx_2 \ldots dx_n$$

PRIMER 5:

Dan je sistem X z n stanji in verjetnostmi $(p_1,\ldots,p_n)$, $\sum_i p_i = 1$. Kakšno entropijo ima sistem Y, ki je sestavljen iz $N \geq 2$ neodvisnih sistemov X?

$N = 2$:

$$\begin{aligned}
H(Y) &= -\sum_i \sum_j p_{ij} \log_2 p_{ij} \quad , \quad p_{ij} = p_i p_j \\
&= -\sum_i \sum_j p_i p_j \log_2(p_i p_j) = -\sum_i \sum_j p_i p_j (\log_2 p_i + \log_2 p_j) \\
&= -\sum_i p_i \log_2 p_i \sum_j p_j - \sum_i p_i \sum_j p_j \log_2 p_j \\
&= -\sum_i p_i \log_2 p_i - \sum_j p_j \log_2 p_j = -2 \sum_i p_i \log_2 p_i \\
&= 2H(X)
\end{aligned}$$

$N = N$:

$$\begin{aligned}
H(Y) &= -\sum_{i_1} \cdots \sum_{i_N} p_{i_1 \ldots i_N} \log_2 p_{i_1 \ldots i_N} \quad , \quad p_{i_1 \ldots i_N} = p_{i_1} \cdots p_{i_N} \\
&= -\sum_{i_1} \cdots \sum_{i_N} p_{i_1} \ldots p_{i_N} \log_2 p_{i_1} \ldots p_{i_N} \\
&= -N \sum_i p_i \log_2 p_i \\
&= NH(X)
\end{aligned}$$

$\diamond$

Poglavje 3

Informacija

- Informacija nastaja med komuniciranjem, zato komunikacijskim sistemom pravimo bolj splošno tudi informacijski sistem(IS).
- Vsako stanje x_i sistema X, ki se pojavi z verjetnostjo p_i, nosi informacjo $I(x_i)$.
- Od funkcije $I(x_i)$ zahtevamo naslednje:
  1. $I(x_i) = f(p_i)$;
     (informacija stanja x_i je funkcija njegove verjetnosti)
  2. $f(p)$ je zvezna funkcija na intervalu $(0, 1]$;
     ($(0, 1]$ pomeni $0 < p \leq 1$)
  3. $f(p)$ je strogo padajoča funkcija na intervalu $(0, 1]$;
     (bolj verjetni znaki nosijo manj informacije)
  4. $f(p' \cdot p'') = f(p') + f(p'')$, za vsak p' in $p'' \in (0, 1]$.
     (informacija dveh statistično neodvisnih znakov (stanj) je enaka seštevku informacij posameznih znakov)

Zgornjim zahtevam zadošča naslednja funkcija

$$f(p) = -K \cdot \log_d p,$$
$$K > 0$$
$$d > 1$$

- Stanje x_i vsebuje informacijo:

$$I(x_i) = -K \cdot \log_d p_i \underset{\substack{K=1 \\ d=2}}{\overset{\uparrow}{=}} -\log_2 p_i$$

- Povprečno informacijo sistema X z zalogo Z(X) pa dobimo kot srednjo vrednost oz. matematično upanje čez vse informacije posameznih stanj:

$$\begin{aligned} I(X) &= E\{I(x_i)\} = \sum_i p_i I(x_i) = \\ &= -K \sum_i p_i \cdot \log_d p_i \underset{\substack{K=1 \\ d=2}}{\overset{\uparrow}{=}} -\sum p_i \cdot \log_2 p_i \\ &= H(X) \end{aligned}$$

- **Povprečna vrednost lastne informacije E[I(X)] naključne spremenljivke X je enaka entropiji H(X) .**

PRIMER 6:

Imamo naključno spremenljivko X z $Z(X) = (x_1, x_2)$ in $P(X) = (\frac{1}{2}, \frac{1}{2})$. Kolikšno informacijo nosi stanje x_1 in kolikšna je povprečna informacija spremenljivke X?

$$
\begin{aligned}
I(x_1) &= -\log_2 \frac{1}{2} = \log_2 2 = 1 \text{ bit} \\
I(X) &= -\frac{1}{2} \cdot \log_2 \frac{1}{2} - \frac{1}{2} \cdot \log_2 \frac{1}{2} \\
&= \frac{1}{2} \cdot \log_2 2 + \frac{1}{2} \cdot \log_2 2 \\
&= \frac{1}{2} + \frac{1}{2} = 1 \text{ bit}
\end{aligned}
$$

◇

3.1 Povprečna medsebojna informacija $I(X;Y)$

Vzemimo KS z X na vhodu in Y na izhodu. Zaradi šuma v kanalu Y ni vedno enak X. Kljub temu moremo iz Y izluščiti X. Pri tem nam pomaga $I(X;Y)$:

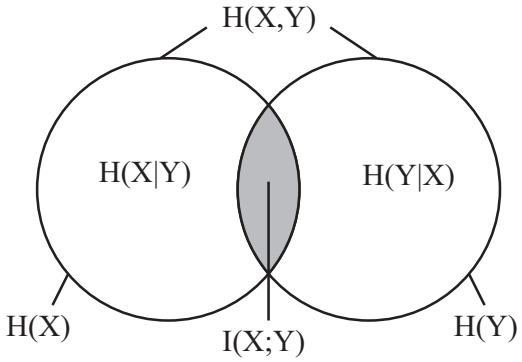
$$I(X;Y) = H(X) - H(X|Y)$$

$I(X;Y)$ nam pove koliko zvemo o X iz Y. Z enim znakom prenesemo po kanalu v povprečju $I(X;Y)$ enot (bitov).

Lastnosti $I(X;Y)$:

1. Če sta X in Y statistično neodvisna, se po kanalu ne prenaša nobena informacija. Tedaj je $H(X|Y) = H(X)$ in $I(X;Y) = H(X) - H(X) = 0$.
2. Če pa nam Y pove vse o X, tedaj je:
   $H(X|Y) = 0$ oz. $I(X;Y) = H(X) - 0 = H(X)$,
   kar pomeni, da se je prenesla vsa informacija o X.
3. Velja simetrija: $I(X;Y) = I(Y;X)$
   Dokaz:
   $$
   \begin{aligned}
   H(X,Y) &= H(X) + H(Y|X) \\
   &= H(Y) + H(X|Y) \\
   H(X|Y) &= H(X,Y) - H(Y) \\
   H(Y|X) &= H(Y,X) - H(X) \\
   I(X;Y) &= H(X) - H(X|Y) = \\
   &= H(X) + H(Y) - H(X,Y)
   \end{aligned}
   $$
   Ker je $H(X,Y) = H(Y,X)$, je tudi $I(X;Y) = I(Y;X)$

4. $I(X;X) = H(X) - H(X|X) = H(X)$



5. Pogojna povprečna medsebojna informacija je dana z:

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

6. Verižno pravilo:

$$I(X_1, X_2, \ldots, X_n; Y) = \sum_{i=1}^{n} I(X_i; Y|X_1, X_2, \ldots, X_{i-1})$$

Dokaz:

$$\begin{aligned} I(X_1, \ldots, X_n; Y) &= H(X_1, \ldots, X_n) - H(X_1, \ldots, X_n|Y) \\ &= \sum_{i=1}^{n} H(X_i|X_1, \ldots, X_{i-1}) - \sum_{i=1}^{n} H(X_i|X_1, \ldots, X_{i-1}, Y) \\ &= \sum_{i=1}^{n} I(X_i; Y|X_1, \ldots, X_{i-1}) \end{aligned}$$

Relativna entropija je definirana kot:

$$\underset{\substack{\uparrow \\ D(p||q) \geq 0 \\ \textit{Enakost v primeru} \\ p = q}}{D(p||q)} = \sum_i p_i \cdot \log \frac{p_i}{q_i} = E\left(\log \frac{p(X)}{q(X)}\right)$$

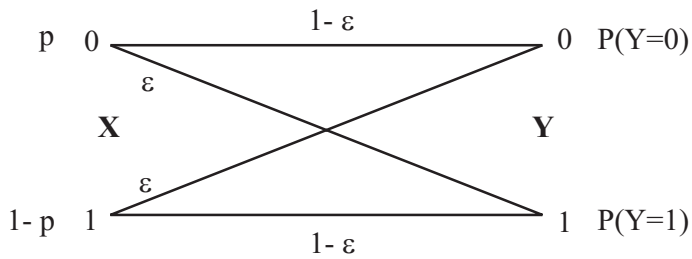
To je mera za razdaljo med dvema porazdelitvama p in q, oz. mera za neuspešnost predpostavke, da je porazdelitev q, če je resnična porazdelitev p. (Tudi Kullback - Leibler-jeva razdalja).

PRIMER 7:

V kanal vstopa X z $Z(X) = \{0, 1\}$ in $P(X) = \{p(0) = p,\ p(1) = 1 - p\}$.
Na izhodu kanala dobimo Y z $Z(Y) = \{0, 1\}$.
Poznane so še pogojne verjetnosti:

$$P(Y = 1|X = 0) = P(Y = 0|X = 1) = \varepsilon,$$
$$P(Y = 0|X = 0) = P(Y = 1|X = 1) = 1 - \varepsilon.$$

$$\begin{aligned} I(X;Y) &= H(X) + H(Y) - H(X,Y) \\ &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X) \end{aligned}$$



- Izračun $H(X)$:

$$\begin{aligned} H(X) &= -p \cdot \log\ p - (1-p) \cdot \log\ (1-p);\ q = 1 - p \\ &= -p \cdot \log\ p - q \cdot \log\ q \end{aligned}$$

- Izračun $H(Y)$:

$$\begin{aligned} p_{ij} = p_i \cdot p'_{j|i} :& P(X = 0, Y = 0) = p \cdot (1 - \varepsilon) \\ & P(0, 1) = p \cdot \varepsilon \\ & P(1, 0) = (1 - p) \cdot \varepsilon = q \cdot \varepsilon \\ & P(1, 1) = (1 - p)(1 - \varepsilon) \\ & \quad = q(1 - \varepsilon) \end{aligned}$$

$$\begin{aligned} p'_j = \sum\nolimits_i p_{ij} :\ P(Y = 0) &= p(1 - \varepsilon) + q \cdot \varepsilon \\ &= p + \varepsilon(q - p) \\ P(1) &= p \cdot \varepsilon + q(1 - \varepsilon) \\ &= q + \varepsilon(p - q) \end{aligned}$$

$$\begin{aligned} H(Y) = &- (p + \varepsilon(q - p)) \cdot \log(p + \varepsilon(q - p)) \\ &- (q + \varepsilon(p - q)) \cdot \log(q + \varepsilon(p - q)) \end{aligned}$$

- Izračun $H(X,Y)$:

$$\begin{aligned} H(X,Y) &= -p(1-\varepsilon)\cdot\log p(1-\varepsilon) - (p\cdot\varepsilon)\cdot\log(p\cdot\varepsilon) \\ &\quad - (q\cdot\varepsilon)\cdot\log(q\cdot\varepsilon) - q(1-\varepsilon)\cdot\log q(1-\varepsilon) \\ &= \ldots = \\ &= -p\cdot\log p - \varepsilon\cdot\log\varepsilon - (1-p)\cdot\log(1-p) - (1-\varepsilon)\cdot\log(1-\varepsilon) \end{aligned}$$

- Izračun $I(X;Y)$:

$$\begin{aligned} I(X;Y) &= H(X) + H(Y) - H(X,Y) \\ &= \varepsilon\cdot\log\varepsilon + (1-\varepsilon)\cdot\log(1-\varepsilon) - \\ &- (p+\varepsilon(q-p))\cdot\log(p+\varepsilon(q-p)) - \\ &- (q+\varepsilon(p-q))\cdot\log(q+\varepsilon(p-q)) \end{aligned}$$

- Pri $\varepsilon = 0 \to I(X;Y) = H(X)$ se prenese celotna informacija, ki jo oddaja vir. Pri $\varepsilon = \frac{1}{2} \to I(X;Y) = 0$ se informacija ne prenaša.
- Poznavanje Y lahko le zmanjša negotovost glede X, kar pa drži v povprečju.

◇

PRIMER 8:

		$p_1 = \frac{1}{8}$	$p_2 = \frac{7}{8}$
	$Y \setminus X$	1	2
$p'_1 = \frac{3}{4}$	1	0	$\frac{3}{4}$
$p'_2 = \frac{1}{4}$	2	$\frac{1}{8}$	$\frac{1}{8}$

$$p_{i|j} = \frac{p_{ij}}{p'_j} \quad , \quad p_{ij} = \text{verjetnost na preseku } X \text{ in } Y$$

$$\begin{aligned} H(X) &= H\left(\frac{1}{8}, \frac{7}{8}\right) = 0{,}54 \text{ bita} \\ H(X|Y=1) &= -\sum_i p_{i|j}\cdot\log p_{i|j} = H\left(\frac{0}{3/4}, \frac{3/4}{3/4}\right) = H(0,1) = 0 \\ H(X|Y=2) &= H\left(\frac{1/8}{1/4}, \frac{1/8}{1/4}\right) = H(\frac{1}{2}, \frac{1}{2}) = 1 \ > \ H(X) \\ H(X|Y) &= \frac{3}{4}\cdot H(X|1) + \frac{1}{4}\cdot H(X|2) = 0{,}25 \text{ bita} \end{aligned}$$

◇

- I(X;Y) lahko podamo tudi drugače:

$$
\begin{aligned}
I(X;Y) = H(X) - H(X|Y) &= -\sum_i \sum_j p_{ij} \cdot \log \frac{p_i}{p_{i|j}} = \\
&= -\sum_i \sum_j p_{ij} \cdot \log \frac{p_i \cdot p'_j}{p_{ij}} = \sum_i \sum_j p_{ij} \cdot \log \frac{p_{ij}}{p_i \cdot p'_j} = \\
&= D(p_{ij} || p_i \cdot p'_j) = \\
&= E\left[\log \frac{p(X,Y)}{p(X) \cdot p(Y)}\right] = \\
&= E[I(x_i; y_j)]
\end{aligned}
$$

Izraz $I(x_i; y_j) = \log \frac{p_{ij}}{p_i \cdot p'_j}$ imenujemo medsebojna informacija znaka x_i in y_j.

$I(X;Y)$ je torej povprečna vrednost medsebojnih informacij $I(x_i; y_j)$ vseh urejenih parov na vhodu in izhodu iz kanala.

$I(x_i; y_j)$ lahko pišemo še drugače:

$$
\begin{aligned}
I(x_i; y_j) &= \log \frac{p_{ij}}{p_i \cdot p'_j} = \log p_{ij} - \log p_i - \log p'_j \\
&= I(x_i) + I(y_j) - I((x_i, y_j))
\end{aligned}
$$

$I(x_i; y_j)$ je enaka seštevku lastnih informacij vhodnega in izhodnega znaka, zmanjšanemu za lastno informacijo vezanega para (x_i, y_j). Če zgornjo enačbo povprečimo, dobimo:

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

POZOR: $I(x_i; y_j)$ je glede na definicijo lahko pozitivna, negativna ali 0, $I(X,Y)$ kot povprečna medsebojna informacija pa je lahko le nenegativna količina.

3.2 Povprečna medsebojna informacija zveznih spremenljivk

- Definirana je z izrazom :

$$I(X;Y) = K \cdot \int\int_{\wp_2} f(x,y) \cdot \log_d \frac{f(x,y)}{f_X(x) f_Y(y)} \, dxdy$$

kjer je: $f_X(x) = \int_{-\infty}^{+\infty} f(x,y) dy$

$f_Y(y) = \int_{-\infty}^{+\infty} f(x,y) dx$

- Medsebojna informacija vezanega para (x,y) pa je enaka:

$$I(x;y) = K \cdot \log_d \frac{f(x,y)}{f_X(x) f_Y(y)}$$

- Pri statistično neodvisnih X in Y je: $f(x,y) = f_X(x) \cdot f_Y(y)$, kar implicira $I(x;y) = 0$. To pomeni, da vrednosti spremenljivk x in y ne dajeta nobene informacije ena o drugi.

Poglavje 4

Diskretni vir informacije

Diskretni vir informacije je dinamičen, naključni ali stohastini sistem, ki oddaja znake v diskretnem času na osnovi neke verjetnostne porazdelitve.

Opišemo ga lahko na dva načina:

1. Z **množico nizov:** S končno množico ali abecedo vira $A = \{x_1, x_2, \ldots, x_a\}$ in verjetnostno porazdelitvijo nad množico A^n za vsak n, $n \in \mathbb{N}$, kar pomeni, da vsakemu nizu $x_1, x_2, \ldots, x_n \in A^n$ pripada verjetnost $P(x_1, x_2, \ldots, x_n) \geq 0$, tako da je $\sum\limits_{x_1 \ldots x_n \in A^n} P(x_1, x_2, \ldots, x_n) = 1$

2. Kot **časovni proces:** Z nizom naključnih spremenljivk $\{X_t\}, t = 1, \ldots, n$, kjer spremenljivke črpajo vrednosti iz zaloge $Z(X_t) = A = \{x_1, \ldots, x_a\}$ in s porazdelitvijo verjetnosti, da vir odda zaporedje (sekvenco):
$P(X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n) = P(x_1, \ldots, x_n) \geq 0,\ x_1 \cdots x_n \in A_n$

4.1 Entropija stacionarnega vira

- Vir je stacionaren, če za $n, k \in \mathbb{N}$ velja:
$$P(X_{k+1} = x_1, X_{k+2} = x_2, \ldots, X_{k+n} = x_n) = P(X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n)$$
To pomeni, da je verjetnost sekvence v vsakem trenutku k enaka.

- Povprečna lastna informacija (entropija) znaka v n-členem nizu je dana z:
$$H_n = \frac{1}{n}\, H(X_1, \ldots, X_n) = -\frac{1}{n}\, K \sum_{\substack{\textit{preko vseh} \\ x_1, \ldots x_n \in A^n, \\ \textit{pri katerih je} \\ P(x_1, \ldots, x_n) > 0}} P(x_1 \cdots x_n) \cdot \log_d P(x_1, \ldots, x_n)$$

- Pogojna entropija n-tega (zadnjega) znaka v sekvenci, ko predhodne $n-1$ znake poznamo in je $n \geq 2$:
$$H'_n = H(X_n | X_1, \ldots, X_{n-1}) = -K \sum_{\substack{\textit{preko vseh} \\ x_1, \ldots x_n \in A^n, \\ \textit{kjer so vezane in} \\ \textit{pogojne verj.} > 0}} P(x_1, \ldots, x_n) \cdot \log_d P(x_n | x_1, \ldots, x_{n-1})$$

- Za stacionarni diskretni vir velja: H_n in H'_n konvergirata k H, ko gre $n \to \infty$;

$$\lim_{n\to\infty} H_n = \lim_{n\to\infty} H'_n = \underset{\substack{\uparrow \\ \text{entropija vira}}}{H} < \infty$$

4.2 Ergodični stacionarni viri

Vir je ergodičen, če je njegovo statistično povprečje enako časovnemu povprečju. Tedaj velja za vsako naravno število $m < n$ in za vsak niz m znakov $Y = (b_1 \dots b_m) \in A^m$, da je relativna pogostost niza Y v nizu X dolžine n, $X = (x_1, \dots, x_n) \in A^n$ v limiti, ko gre $n \to \infty$, enaka $P(Y)$. Ergodični vir ima en sam režim delovanja.

PRIMER 9:

Stacionarni vir z abecedo $A = \{0, 1\}$ deluje v 2 načinih in torej ni ergodičen. V 1. načinu se nahaja z verjetnostjo $\frac{1}{2}$ in tedaj oddaja samo niz n ničel: $\mathbf{x}_0 = \underbrace{00\dots0}_{n}$.

V 2. načinu se tudi nahaja z verjetnostjo $\frac{1}{2}$ in tedaj oddaja poljuben niz z enako verjetnostjo oddajanja znakov 0 in 1.

Zanima nas entropija vira in koliko informacije na znak oddaja vir.

- Verjetnosti:

$$\mathbf{x}_0,\ P(x_0) = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2^n} = \frac{2^n + 1}{2^{n+1}}$$

$$\mathbf{x} \neq \mathbf{x}_0,\ P(x) = \frac{1}{2} \cdot \frac{1}{2^n} = \frac{1}{2^{n+1}}$$

- Entropija:

$$\begin{aligned}
H(X_1, \dots, X_n) &= -\sum P(x_1, \dots, x_n) \cdot \log P(x_1, \dots, x_n) \\
&= -\left(\frac{1}{2} + \frac{1}{2^{n+1}}\right) \cdot \log\left(\frac{1}{2} + \frac{1}{2^{n+1}}\right) - (2^n - 1) \cdot \left(\frac{1}{2^{n+1}}\right) \cdot \log\left(\frac{1}{2^{n+1}}\right) \\
\text{(za velike n)} \quad &= -\frac{1}{2} \cdot \log\frac{1}{2} - \left(\frac{1}{2} - \frac{1}{2^{n+1}}\right) \cdot \log\left(\frac{1}{2^{n+1}}\right) \\
&= \frac{1}{2} \cdot \log 2 + \left(\frac{1}{2} - \frac{1}{2^{n+1}}\right)(\log 2 + \log 2^n) \\
&= \frac{1}{2} \cdot \log 2 + \frac{1}{2} \cdot \log 2 - \frac{1}{2^{n+1}} \cdot \log 2 + \frac{1}{2} \cdot \log 2^n - \frac{1}{2 \cdot 2^n} \cdot \log 2^n \\
&\doteq \frac{1}{2} + \frac{1}{2} - 0 + \frac{n}{2} + 0 \\
&\doteq 1 + \frac{n}{2} = \frac{n+2}{2} \text{ bitov}
\end{aligned}$$

$$H_n = \lim_{n\to\infty} \frac{1}{n} \cdot \frac{n+2}{2} = \frac{1}{2} \text{ bita/znak - povp. entropija vira/znak}$$

- Informacija:

$$I(\mathbf{x}_0) = -\log\left(\frac{1}{2} + \frac{1}{2^{n+1}}\right)$$

$$I(\mathbf{x} \neq \mathbf{x}_0) = -\log\left(\frac{1}{2^{n+1}}\right) = n + 1 \text{ bitov}$$

Povprečna informacija na znak v primeru niza $\mathbf{x}_0$:

$$\lim_{n\to\infty} \frac{I(\mathbf{x}_0)}{n} = 0 \text{ bitov/znak}$$

$$\lim_{n\to\infty} \frac{I(\mathbf{x} \neq \mathbf{x}_0)}{n} = \frac{n+1}{n} = 1 \text{ bit/znak}$$

Vir oddaja polovico časa 0 bitov informacije na znak (v načinu 1), drugo polovico časa pa 1 bit/znak (v načinu 2). Povprečna informacija na znak torej ne konvergira k entropiji $H(X_1, \ldots, X_n)$.

◇

- Za vse ergodične vire velja **AEL** (Asimptotična Enakodelitvena Lastnost), ki pravi, da lahko nize, ki jih vir oddaja, razdelimo v dve nepresečni množici: tipično in netipično. To velja za vire brez in s spominom.

$$\left(\text{AEL: } \lim_{n\to\infty} \frac{1}{n}\, I_n(\mathbf{x}) \xrightarrow{P} H; \text{ Informacija po znaku konvergira k entropiji vira}\right)$$

PRIMER 10:

Ilustracija AEL Vir ima abecedo A = {0,1} z verjetnostmi $p_1 = P(0) = \frac{1}{3}$ in $P(1) = \frac{2}{3}$.

Kakšne nize generira vir in kakšna je entropija vira.?

$$H\left(\frac{1}{3}, \frac{2}{3}\right) = 0{,}918$$

Predpostavimo dolžino nizov n in v njih m znakov 0, $m \leq n$.
Verjetnost takšnega niza je: $p_1^m \cdot (1 - p_1)^{n-m}$

Takšnih nizov je: $\binom{n}{m} = \frac{n!}{(n-m)! \cdot m!}$

Verjetnost nizov dolžine n z m ničlami je zato $\binom{n}{m} p_1^m (1 - p_1)^{n-m}$

Iz tabele (n = 15):

m	$\binom{n}{m}$	$p_1^m(1-p_1)^{n-m}$	$\binom{n}{m}p_1^m(1-p_1)^{n-m}$
0	št. načinov	verjetnost niza	celotna verjetnost niza
$\vdots$	$\}2^{nH} = \sum$	$\}2^{-nH}$	$\}\sum \doteq 0{,}95$
15	vsota	posamezni	vsota

sledi, da so najbolj verjetni nizi z $m \approx n \cdot p_1 = 15 \cdot \frac{1}{3} = 5$.
Verjetnost nizov z $2 \leq m \leq 8$ je 0,95.
Verjetnosti nizov ($2 \leq m \leq 8$) so blizu 2^{-nH}.
Število nizov ($2 \leq m \leq 8$) je blizu 2^{nH}.
$\diamond$

- Nize ergodičnega vira delimo na:
  - tipično množico zelo verjetnih nizov, ki imajo približno enako verjetnost ($P \approx 2^{-nH}$)
  - in na netipično množico malo verjetnih nizov s približno verjetnostjo ($P \approx 0$)

- AEL je analogna zakonu velikih števil v statistiki, ki pravi, da je $\sum p_i x_i$ za naključno in enakomerno porazdeljeno spremenljivko X ($Z(X) = \{x_1, x_2, \ldots, x_n\}$, $P(X) = \{p_1, p_2, \ldots, p_n\}$), blizu srednje vrednosti $E(X)$ in z $n \to \infty$ limitira k njej.

- AEL pravi, da povprečna informacija na znak verjetnostno konvergira k entropiji vira brez spomina, ko gre $n \to \infty$:

$$\lim_{n\to\infty} \frac{1}{n} I_n(\mathbf{X}) \xrightarrow{P} H$$
$$\frac{1}{n} \cdot \log \frac{1}{P(\mathbf{X})} \approx H$$
$$2^{-nH} \approx P(\mathbf{X}) = P(x_1, x_2, \ldots, x_n)$$

- Verjetnostna konvergenca ($\xrightarrow{P}$):
  Mogoče je najti poljubno majhni števili δ in γ, tako da pri $n \geq n_0$ velja:

$$P\left(\left|\frac{k}{n} - p\right| < \delta\right) > 1 - \gamma,$$

  kjer je p verjetnost dogodka in $\frac{k}{n}$ relativna pogostost dogodka v n ponovitvah. Izrazu pravimo tudi **Bernoullijev zakon velikih števil**.

- Zelo verjetni ali značilni nizi ergodičnega vira tvorijo množico, katere velikost določa izraz:

$$\begin{aligned} |P_1| \leq 2^{nH},\ & P_1 - \text{množica značilnih nizov} \\ & P_2 - \text{množica neznačilnih nizov} \\ \text{za } \mathbf{x} \in A^n \text{ je: } & P(\mathbf{x} \in P_1) \approx 2^{-nH} \\ & P(\mathbf{x} \in P_2) \approx 0 \\ |P_2| \doteq 2^n - |P_1| = 2^n - 2^{nH} & \end{aligned}$$

- Pogostosti znakov v nizih $n_1, .., n_a$ težijo k $p_1, \ldots, p_a$, če gredo dolžine nizov n $\to \infty$.
  Pri tem je:
  $n_1 = n \cdot p_1$, število pojavov znaka x_1,
  $\vdots$
  $n_a = n \cdot p_a$, število pojavov znaka x_a.

4.2.1 Viri brez spomina

- Zanje velja:

$$P(x_n|x_1,\ldots,x_{n-1}) = P(x_n); \quad n = 2,3,\ldots; \quad x_n \in A$$

Verjetnost sekvence dolžine n je tedaj:

$$P(x_1,\ldots,x_n) = P(x_1)\cdot P(x_2)\ldots P(x_n)$$

- Entropija vira brez spomina:

$$H_n = \frac{1}{n}[H(X_1) + H(X_2) + \ldots + H(X_n)]$$

Ker so pri viru brez spomina naključne spremenljivke $X_1, X_2, \ldots,$ neodvisne: ($X_1 = X$ v času $t = 1$), velja:

$$H_n = \frac{1}{n}[nH(X_1)] = H(X_1) = -K\sum_{i=1}^{a} p_i \cdot \log_d p_i \underset{\substack{(ker\ H_n\ ni \\ odvisen\ od\ n)}}{=} H$$

4.2.2 Viri s spominom (Markovov vir)

- Če je oddaja vira v sedanjem trenutku odvisna od določenega števila predhodno oddanih znakov, govorimo o viru s spominom.

Markovov vir oddaja znake odvisno le od predhodnega znaka:

$$P(X_n = x_j|X_1 = x_k,\ldots,X_{n-1} = x_i) = P(X_n = x_j|X_{n-1} = x_i)$$

- Prehodna verjetnost q_{ij} je verjetnost oddaje x_j v času n in x_i v času $(n-1)$:

$$q_{ij} = P(X_n = x_j|X_{n-1} = x_i) \geq 0$$

vsota vrstice v Q=1 $\rightarrow \sum_{\mathbf{j}} \mathbf{q_{ij}} = \mathbf{1}$

- Verjetnost oddaje znaka x_j v času n:

$$\begin{aligned} P(X_n = x_j) &= \sum_{i=1}^{a} P(X_n = x_j, X_{n-1} = x_i) = \\ &= \sum_{i=1}^{a} P(X_{n-1} = x_i)\cdot P(X_n = x_j|X_{n-1} = x_i) \\ &= \sum_{i=1}^{a} P(X_{n-1} = x_i)\cdot q_{ij} \end{aligned}$$

V matrični obliki izgleda zapis:

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

$$P_n = \begin{bmatrix} P(X_n = x_1) \\ P(X_n = x_2) \\ \vdots \\ P(X_n = x_a) \end{bmatrix}; \; Q = \begin{bmatrix} q_{11} & q_{12} & \cdots & q_{1a} \\ q_{21} & \ddots & & q_{21} \\ \vdots & & \ddots & \vdots \\ q_{a1} & \cdots & \cdots & q_{aa} \end{bmatrix}; \; P_{n-1} = \begin{bmatrix} P(X_{n-1} = x_1) \\ P(X_{n-1} = x_2) \\ \vdots \\ P(X_{n-1} = x_a) \end{bmatrix}$$

- Pri stacionarnih virih velja:

  $$P_n = P_{n-1} = P \equiv \text{(stacionarna porazdelitev oddaje vira)},$$

  kar implicira:

  $$P = Q^T \cdot P$$

PRIMER 11:

Za stacionarni Markovov vir z abecedo $A = \{0, 1\}$ in matriko prehodnih verjetnosti $Q = \begin{bmatrix} 1/4 & 3/4 \\ 3/4 & 1/4 \end{bmatrix}$, določite stacionarno porazdelitev vira.

$$P = Q^T \cdot P$$

$$p_1 = \frac{1}{4}p_1 + \frac{3}{4}p_2$$
$$p_2 = \frac{3}{4}p_1 + \frac{1}{4}p_2$$
$$p_1 + p_2 = 1$$

$$p_1 = \frac{1}{4}p_1 + \frac{3}{4}(1 - p_1) = -\frac{1}{2}p_1 + \frac{3}{4} \Longrightarrow p_1 = p_2 = \frac{1}{2}$$

◇

- Entropija Markovovega vira:

$$\underset{\substack{\uparrow \\ \textit{pogojna} \\ \textit{entropija} \\ \textit{n-tega} \\ \textit{znaka}}}{H'_n} = H(X_n|X_1, \ldots, X_{n-1}) = -K \sum_{(x_1 \cdots x_n) \in A^n} P(x_1, \ldots, x_n) \cdot \log_d P(x_n|x_1, \ldots, x_{n-1})$$

$$= -\sum_{(x_1 \cdots x_{n-1}) \in A^{n-1}} P(x_1)P(x_2|x_1) \cdots P(x_{n-1}|x_{n-2}) \cdot K \sum_{x_n \in A} P(x_n|x_{n-1}) \cdot \log_d P(x_n|x_{n-1})$$

$$= -\sum_{x_{n-1} \in A} P(x_{n-1}) K \sum_{x_n \in A} P(x_n|x_{n-1}) \cdot \log_d P(x_n|x_{n-1})$$

Zaradi upoštevanja stacionarnosti vira, dobimo končno:

$$H'_n = -\sum_{x_1 \in A} P(x_1) K \sum_{x_2 \in A} P(x_2|x_1) \cdot \log_d P(x_2|x_1)$$

Ker H'_n ni odvisna od n, je entropija stacionarnega Markovovega vira oz. povprečna informacija na znak iz vira enaka:

$$\begin{aligned} H &= \lim_{n\to\infty} H'_n = -\sum_{i=1}^{a} p_i \cdot K \sum_{j=1}^{a} q_{ij} \cdot \log_d \ q_{ij} \\ &= \sum_{i=1}^{a} p_i \cdot H_i; \ H_i = -K \sum_{j=1}^{a} q_{ij} \cdot \log_d \ q_{ij} \end{aligned}$$

PRIMER 12:

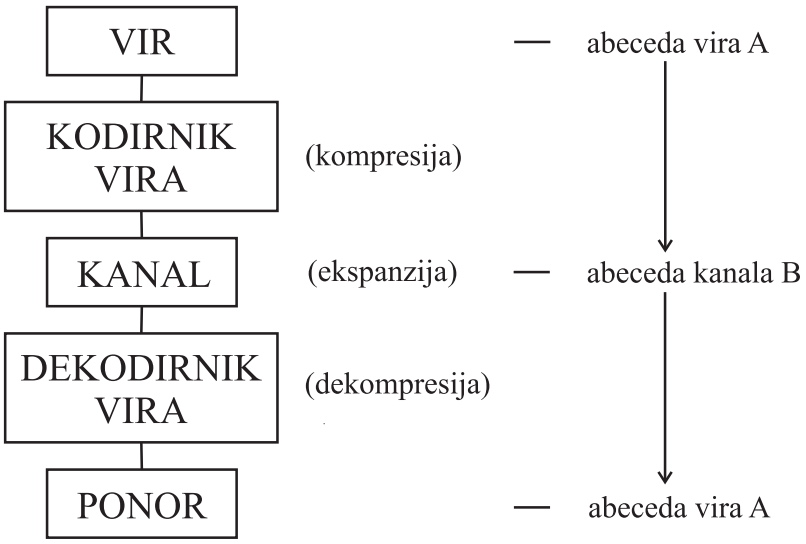
Za Markovov vir iz PRIMERA 10 določite entropijo.

$$\begin{aligned} H_i &= -\sum_{j=1}^{2} q_{ij} \cdot \log_d \ q_{ij} \\ H_1 &= -\frac{1}{4} \cdot \log \frac{1}{4} - \frac{3}{4} \cdot \log \frac{3}{4} = 0{,}811\text{bita} \\ H_2 &= -\frac{3}{4} \cdot \log \frac{3}{4} - \frac{1}{4} \cdot \log \frac{1}{4} = 0{,}811 \text{ bita} \\ H &= \sum_{i=1}^{2} p_i H_i = \frac{1}{2} \cdot H_1 + \frac{1}{2} \cdot H_2 = \\ &= 0{,}811 \text{ bita} \end{aligned}$$

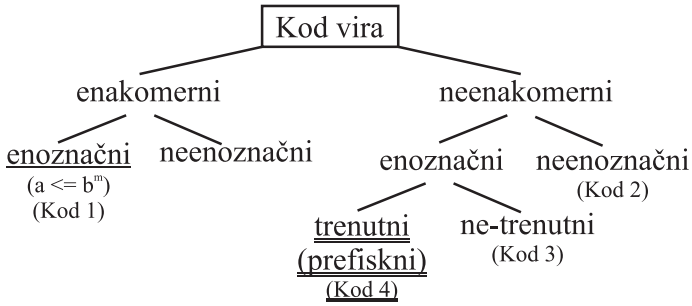
◇

Poglavje 5

Kodiranje vira informacij



- Vir uporablja drugačne znake (npr. ASCII) kot kanal (npr. dvojiške znake) Prirejanje znakov ene abecede znakov drugi abecedi je KODIRANJE.
- **Cilj kodiranja vira** je povečati hitrost in s tem skrajšati prenos. Gre za preslikavo abecede vira A v abecedo kanala B.
- Kodiranje vira (tudi KOD VIRA) določa trojica $< a, b, f >$, kjer je:
  - a : število znakov abecede A
  - b : število znakov abecede B
  - f : injektivna preslikava $f : A \to C,\ C = B^m$ ali $C = B^1 \cup B^2 \cup \ldots \cup B^m$
- Kod je **enakomeren**, če je dolžina vseh kodnih zamenjav enaka, sicer je neenakomeren.
- Kod je **enoznačen**, če vsakemu znaku iz abecede A ustreza drugačna kodna zamenjava.
- Kod je **trenutni** ali **prefiskni**, če ne vsebuje kodne zamenjave, ki bi bila predpona (prefix) kakšni drugi kodni zamenjavi.



PRIMER 13:

$A = \{x_1, x_2, x_3\};\ B = \{0, 1\}$

A	$P(x_i)$	Kod 1	Kod 2	Kod 3	Kod 4
x_1	0,5	00	0	1	0
x_2	0,3	01	1	10	10
x_3	0,2	10	01	100	11

Kod 1 je enakomeren, ostali so neenakomerni.

Kod 2 je neenoznačen, (ni ga mogoče enoznačno dekodirati)

Kod 3 omogoča dekodiranje (enoznačno) šele po sprejemu prvega znaka naslednje kodne zamenjave

Kod 4 je trenutni ali prefiksni kod

◇

- Kodiranje je **gospodarno**, če so kodne zamenjave čim krajše. Zato je **mera gospodarnosti** koda vira **povprečna dolžina** njegovih kodnih zamenjav:

$$\bar{n} = \sum_{i=1}^{a} p_i \cdot n_i, \quad p_i \text{ je verjetnost } i\text{-tega znaka, } n_i \text{ pa dolžina njegove kode}$$

PRIMER 14:

Povprečne dolžine kodov iz PRIMERA 12:

Kod 1 : $\bar{n} = 0{,}5 \cdot 2 + 0{,}3 \cdot 2 + 0{,}2 \cdot 2 = 2$

Kod 2 : $\bar{n} = 1{,}2$

Kod 3 : $\bar{n} = 1{,}7$

Kod 4 : $\bar{n} = 1{,}5$

Ker mora biti kod tudi enoznačen, je najboljši Kod 4.

◇

- Gospodarne kode iščemo med **neenakomernimi** kodi, ki jih lahko **enoznačno** dekodiramo.
  Za stacionarne vire brez spomina (najbolj pogosti) so najugodnejši **trenutni kodi**.

- **KRAFTOV IZREK:**
  Potreben in zadosten pogoj za obstoj trenutnega neenakomernega koda je:

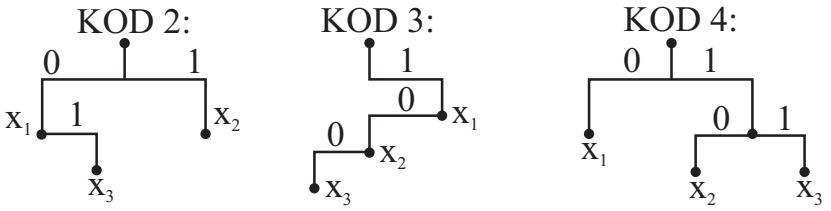
  $$\sum_{i=1}^{a} b^{-n_i} \leq 1$$

  Velja tudi obratno: če dolžine $n_1, ..., n_a$ zadoščajo neenačbi, je možno najti trenutni kod.

- Kodne zamenjave pogosto ponazarjamo s **kodnimi drevesi**. Vsaka veja je označena z znakom abecede B, koda pa je niz znakov od korena do lista.

PRIMER 15:

Kodna drevesa iz PRIMERA 12



◇

5.1 Prvi Shannon-ov teorem (pod. kompresija)

Za diskretni, stacionarni vir brez spomina velja:

IZREK (1. Shannon-ov teorem):
Obstajajo kodi (to so gospodarni kodi) z enoznačno možnostjo dekodiranja, katerih povprečna dolžina $\bar{n}$ je določena z:

$$\frac{H_1}{K \cdot \log_d b} \leq \bar{n} < \frac{H_1}{K \cdot \log_d b} + 1$$

oziroma, če je $K = 1,\ d = b = 2$:

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

kjer je entropija vira brez spomina za niz dolžine 1 enaka

$$H_1 = -\sum_{i=1}^{a} p_i \cdot \log p_i \quad .$$

- Kadar s krajšimi kodami opišemo bolj verjetne vrednosti naključnih spremenljivk govorimo o **PODATKOVNI KOMPRESIJI**.
- ENTROPIJA je limita podatkovne kompresije - kar izhaja iz 1. Shannon-ovega teorema.
- Izmed vseh gospodarnih kodov je tisti z najmanjšo povprečno dolžino $\bar{n}$ **optimalen**. Najmanjša $\bar{n}$ je določena z:

  $$\bar{n} = \frac{H_1}{K \cdot \log_d b}$$

  Pri K = 1, d = 2 imamo:

  $$\begin{aligned} H_1 &= \bar{n} \cdot \log_d b \\ -\sum_{i=1}^{a} p_i \cdot \log p_i &= \sum_{i=1}^{a} p_i n_i \cdot \log b \\ p_i &= b^{-n_i} \quad - \text{ to je pogoj za minimalni } \bar{n} \end{aligned}$$

- Od tod sledi: $n_i = -\log_b p_i$, kar imenujemo tudi **Shannon-ov kod**, saj določa optimalne dolžine kodnih zamenjav.

- Spodnji meji za $\bar{n}$ se približamo tudi, če namesto posameznih znakov abecede vira kodiramo bloke (r-terice) znakov, oz. elemente abecede A^r. Entropija znakov iz A^r je enaka:

  $$H(X_1, ..., X_r) = r \cdot H_1, \text{ (velja za vir brez spomina)}$$

- Če z $\bar{n}_r$ označimo povprečno dolžino kode pri kodiranju blokov z r znaki, potem za trenutni kod $< a^r, b, f >$ po analogiji velja:

  $$\begin{aligned} \frac{rH_1}{K \cdot \log_d b} \leq \bar{n}_r < \frac{rH_1}{K \cdot \log_d b} + 1 \quad / : r \\ \frac{H_1}{K \cdot \log_d b} \leq \frac{\bar{n}_r}{r} < \frac{H_1}{K \cdot \log_d b} + \frac{1}{r} \end{aligned}$$

  Ker je $\bar{n} = \frac{\bar{n}_r}{r}$ lahko zgornjo zvezo ob predpostavki $K = 1,\ d = b = 2$ zapišemo kot:

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

- Od tod sledi **Shannon–Fano-jev** izrek:

  $$\begin{aligned} \lim_{r \to \infty} \frac{\bar{n}_r}{r} &= \frac{H_1}{K \cdot \log_d b}, \\ \lim_{r \to \infty} \bar{n} &= H_1 \qquad \text{pri } K = 1 \text{ in } d = b = 2 \end{aligned}$$

  Gospodarnost koda se povečuje s podaljševanjem blokov znakov, ki jim prirejamo kodne zamenjave.

5.2 Huffman-ov kod

- Je gospodaren ('kvazi' optimalen) empiričen kod. Predstavlja postopek za učinkovito gradnjo trenutnih kodov.
- Bazira na dejstvu, da pri optimalnem kodu velja:

$$p_j > p_k \rightarrow n_j \leq n_k, j \neq k;\ j, k \in \{1, 2, ..., n\}$$

Huffmanov algoritem:

1. korak Abecedo vira A uredimo po padajočih verjetnostih znakov:
$p_1 \geq p_2 \geq ... \geq p_a$

2. korak Oblikujemo novo abecedo A_1 tako, da združimo zadnja dva znaka abecede A v en znak z vsoto obeh verjetnosti. Vsakemu izmed obeh združevanih znakov pripišemo en znak abecede B.

3. korak Prejšnja dva koraka ponavljamo dokler ne pridemo samo do b znakov nove abecede.

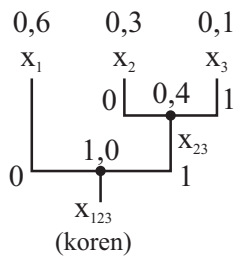
4. korak Kodo vsakega znaka x_i dobimo tako, da zapišemo vse znake abecede B na poti od konca (koren) do začetka (listi) postopka.

PRIMER 16:

$A = \{x_1, x_2, x_3\} \rightarrow a = 3$
$P = \{0{,}6,\ 0{,}3,\ 0{,}1\}$
$B = \{0, 1\} \rightarrow b = 2$

Huffmanov kod = ?

X	P	Huffmanov kod
x_1	0,6	0
x_2	0,3	10
x_3	0,1	11



$$\bar{n} = \sum_{i=1}^{3} p_i \cdot n_i = 1{,}4 \text{ znaka}$$

$$H_1 = -\sum_{i=1}^{3} p_i \cdot \log p_i = 1{,}295 \text{ bitov}$$

$$\tau = \frac{H_1}{\bar{n}} = 0{,}925 \text{ bita/znak} \quad \textbf{(učinkovitost koda)}$$

◇

PRIMER 17:

Za naključno spremenljivko X poznamo kod vira $< 4, 2, f >$:

X	P	f
x_1	0,5	0
x_2	0,25	10
x_3	0,125	110
x_4	0,125	111

Določite $\bar{n}$. Ali je optimalen?

$$\bar{n} = \sum_{i=1} p_i \cdot n_i = 1{,}75 \text{ bitov}$$

$$H_1(X) = -\sum_{i=1} p_i \cdot \log p_i = 1{,}75 \text{ bitov}$$

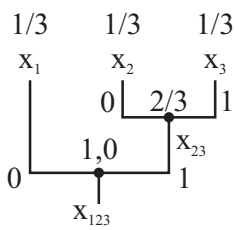
Odgovor: Kod je optimalen.

◇

PRIMER 18:

Ali je kod f optimalen?

X	P	f
x_1	0,333	0
x_2	0,333	10
x_3	0,333	11



Kod f je Huffmanov

$$\bar{n} = \sum_{i=1} p_i \cdot n_i = 1{,}66 \text{ bitov}$$

$$H_1 = -\sum_{i=1} p_i \cdot \log p_i = 1{,}58 \text{ bitov}$$

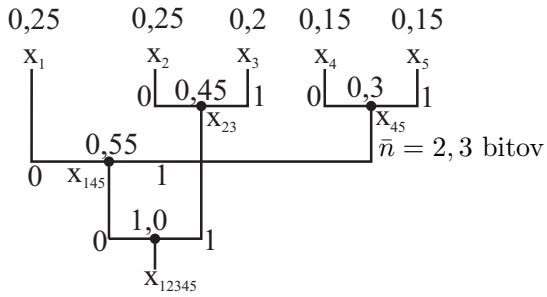
Ker $\bar{n} \neq H_1$, kod ni optimalen, je pa gospodaren, ker je: $H_1 \leq \bar{n} < H_1 + 1$.

◇

PRIMER 19:

Za vir X določite Huffmanov kod:

X	P	f
x_1	0,25	00
x_2	0,25	10
x_3	0,2	11
x_4	0,15	010
x_5	0,15	011



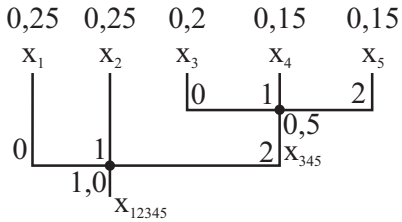
◇

PRIMER 20:

Določite Huffmanov kod za primer $b = 3$.

Pri $b \neq 2$ mora biti število vrednosti spremenljivke X enako: $a = 1 + k(b-1)$, kjer je k število nivojev drevesa. Če jih nimamo dovolj, dodamo 'prazne' spremenljivke z vrednostjo 0.

X	P	f
x_1	0,25	0
x_2	0,25	1
x_3	0,2	20
x_4	0,15	21
x_5	0,15	22



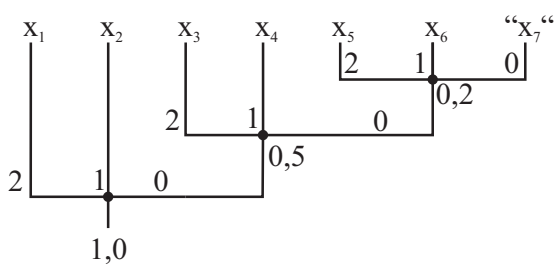
◇

PRIMER 21:

Določite Huffmanov kod ($b = 3$).

$a = 1 + 3 \cdot 2 = 7 \quad (1 + 2 \cdot 2 = 5)$

X	P	f
x_1	0,25	2
x_2	0,25	1
x_3	0,2	02
x_4	0,1	01
x_5	0,1	002
x_6	0,1	001
prazen = "x_7"	0	000

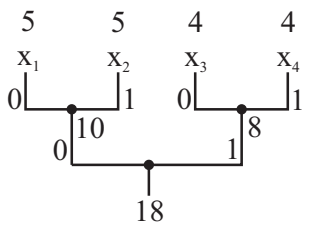


◇

Če so kodne besede utežene ($\omega_i \geq 0, \sum_i \omega_i \neq 1$) potem Huffmanov algoritem minimizira $\sum_i \omega_i \cdot n_i$, kar je **vsota ustreznih kodnih dolžin** (in ne povprečna kodna dolžina). Tedaj v algoritmu uporabimo ω_i namesto p_i

PRIMER 22:

X	ω_i	f
x_1	5	00
x_2	5	01
x_3	4	10
x_4	4	11



◇

PRIMER 23:

Čeprav je Shannonova dolžina optimalna, je lahko precej daljša od Huffmanove, kljub temu, da obe ležita v intervalu $H_1 \leq \bar{n} < H_1 + 1$.

- Shannon:

$$p_1 = 0{,}9999 \Longrightarrow n_1 = \lceil -\log p_1 \rceil = 1 \text{ bit}$$
$$p_2 = 0{,}0001 \Longrightarrow n_2 = \lceil -\log p_2 \rceil = 14 \text{ bitov}$$

- Huffman:

$$n_1 = 1$$
$$n_2 = 1$$

Shannonov teorem je le izhodišče za praktične konstruktivne algoritme kot je na primer Huffmanov algoritem.

◇

Poglavje 6

Komunikacijski kanal (KK):

- Komunikacijski kanal sestavljajo:

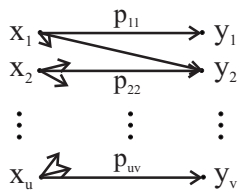
$$\text{KK}\left\{\begin{array}{l}\underline{\text{Kodirnik kanala}}\\ \text{Oddajnik}\\ \text{Linija - zvezni kanal}\\ \underline{\text{Sprejemnik}}\\ \text{Dekodirnik kanala}\end{array}\right\}\begin{array}{c}\text{Diskretni kanal}\\ \text{(DK)}\end{array}$$

- KK opisujemo z naslednjimi matematičnimi modeli:
  - z modelom zveznega kanala
  - z modelom diskretnega kanala
  - z modelom komunikacijskega kanala

6.1 Diskretni komunikacijski kanal

- DK je sistem, ki ga opisuje trojček $< U, P_k, V >$, kjer je:

$$\begin{aligned} U &= \{x_1, \ldots, x_u\}, \text{ množica, vhodnih znakov}\\ V &= \{y_1, \ldots, y_v\}, \text{ množica, izhodnih znakov}\\ P_k &= [a_{ij} \geq 0], \text{ verjetnostna matrika kanala}\\ a_{ij} &= P[y_j|x_i], \quad i = 1, \ldots, u; \; j = 1, \ldots, v \end{aligned}$$



Diskretni kanal brez spomina

- Za DK brez spomina velja:

$$P(\mathbf{y}|\mathbf{x}) = P((y_1, \ldots, y_n)|(x_1, \ldots, x_n)) =$$
$$= \prod_{i=1}^{n} P(y_i|x_i), \quad \text{za vsak } n \in \mathbb{N}$$

- Verjetnosti DK brez spomina:

$$P(x_i) = p_i \geq 0,\ i = 1, \ldots, u,\ \sum_{i=1}^{u} p_i = 1$$
$$P(y_j) = p'_j = \sum_{i=1}^{u} p_{ij} = \sum_{i=1}^{u} P(x_i) \cdot P(y_j|x_i),\ j = 1, \ldots, v,\ \sum_{j=1}^{v} p'_j = 1$$
$$a_{ij} = P(y_j|x_i)\ ;\ c_{ij} = P(x_i|y_j)$$
$$a_{ij} = \frac{p_{ij}}{p_i}\ ;\ c_{ij} = \frac{p_{ij}}{p'_j} = \frac{p_i \cdot a_{ij}}{p'_j}$$
$$\sum_j a_{ij} = \frac{\sum_j p_{ij}}{p_i} = \frac{\sum_j c_{ij} \cdot p_j}{p_i} = \frac{p_i}{p_i} = 1$$
$$\sum_i c_{ij} = \frac{\sum_i p_{ij}}{p'_j} = \frac{\sum_i a_{ij} \cdot p_i}{p'_j} = \frac{p'_j}{p'_j} = 1$$
$$P(x_i, y_j) = p_{ij} = a_{ij} \cdot p_i = c_{ij} \cdot p'_j$$
$$\sum_{i=1}^{u} \sum_{j=1}^{v} p_{ij} = 1$$

- Entropija DK brez spomina:

$$H(X) = -K \sum_{i=1}^{u} p_i \cdot \log_d p_i = -K \sum_i \sum_j p_{ij} \cdot \log_d p_i$$
$$H(Y) = -K \sum_{j=1}^{v} p'_j \cdot \log_d p'_j$$
$$H(X, Y) = -K \sum_i \sum_j (a_{ij} \cdot p_i) \cdot \log_d (a_{ij} \cdot p_i),\ p_{ij} = a_{ij} \cdot p_i$$
$$H(Y|X) = -K \sum_i \sum_j (a_{ij} \cdot p_i) \cdot \log_d\ a_{ij} = \sum_i p_i \cdot (-K \sum_j a_{ij} \cdot \log_d\ a_{ij})$$
$$H(X|Y) = -K \sum_i \sum_j (a_{ij} \cdot p_i) \cdot \log_d\ c_{ij}$$

- Povprečna medsebojna informacija za DK:

$$
\begin{aligned}
I(X;Y) &= H(X) - H(X|Y) = \\
&= -K \sum_i \sum_j p_{ij} \cdot \log_d p_i + K \sum_i \sum_j p_{ij} \cdot \log_d c_{ij} \\
&= -K \sum_i \sum_j (a_{ij} \cdot p_i) \cdot \log_d \frac{p_i}{c_{ij}} \\
&= -K \sum_i \sum_j (a_{ij} \cdot p_i) \cdot \log_d \frac{p_i \cdot p'_j}{p_i \cdot a_{ij}} \\
&= +K \sum_i \sum_j (a_{ij} \cdot p_i) \cdot \log_d \frac{a_{ij}}{\underbrace{\sum_{k=1}^{u} a_{kj} \cdot p_k}_{p'_j}}
\end{aligned}
$$

6.1.1 Kapaciteta DK brez spomina

- Definirana je kot:

$$C = \max_{P_X \in \Delta_u} \{I(X;Y)\}$$

  kjer maksimum iščemo preko vseh možnih porazdelitev vhodne množice znakov.

- Kapaciteta kanala določa prenosne lastnosti kanala glede na vpliv motenj, vpliv motenj pa je zajet v P_K (matriki pogojnih verjetnosti)

$$
\begin{aligned}
I(X;Y) &= H(X) - H(X|Y) = \\
&= K \sum_i \sum_j (a_{ij} \cdot p_i) \cdot \log_d \frac{a_{ij}}{\sum_{k=1}^{u} a_{kj} \cdot p_k}
\end{aligned}
$$

- Znak, ki vstopa v kanal, vsebuje v povprečju $H(X)$ lastne informacije. Zaradi motenj se v povprečju izgubi $H(X|Y)$ informacije po znaku.
  $I(X;Y)$ je povprečno prenešena informacija po znaku skozi kanal brez spomina. Ker v zgornji enačbi sledi odvisnost $I(X;Y)$ od $P_k(a_{ij})$ in $P_k(p_i)$, lahko z iskanjem najboljše porazdelitve P_X, prenos izboljšamo.
  C pove za dani kanal največjo informacijo po znaku, ki se lahko prenese skozi kanal brez spomina.
  Verjetnostno porazdelitev znakov lahko izboljšamo s **kodiranjem vira**.
  (Izenačitev verjetnosti dosežemo tudi tako, da bolj verjetne znake krajše kodiramo, manj verjetne pa z daljšo kodo)

Lastnosti kapacitete DK brez spomina

- **Zgornjo mejo** kapacitete določa izraz:

$$
\begin{aligned}
C &= \max_{P_X \in \Delta_u} \{H(X)\} = H(\frac{1}{u}, \ldots, \frac{1}{u}) = \\
&= K \cdot \log_d u
\end{aligned}
$$

  Tedaj ni motenj, oz. $H(X|Y) = 0$

- **Spodnjo mejo** kapacitete pa določa:

$$C = \max_{P_X \in \Delta_u} \{H(X) - H(X)\} = 0$$

Tedaj so motnje enake informaciji na vhodu, zato se ne prenese nobena informacija - kanal je neuporaben.

- **Simetričen kanal**: je takrat, kadar so vrstice matrike P_K različne razporedbe v števil, stolpci pa različne razporedbe u števil:

$$\text{npr.: } P_K = \begin{bmatrix} 0{,}2 & 0{,}1 & 0{,}7 \\ 0{,}7 & 0{,}2 & 0{,}1 \\ 0{,}1 & 0{,}7 & 0{,}2 \end{bmatrix}_{u \times v}$$
$$\downarrow$$
$$a_{ij}$$

- Kapaciteto simetričnega kanala določimo takole:

$$\begin{aligned} I(X;Y) &= K \sum_i \sum_j (a_{ij} \cdot p_i) \cdot \log_d \frac{a_{ij}}{\sum_{k=1}^{u} a_{kj} \cdot p_k} = \\ &= K \sum_i p_i \sum_j a_{ij} \cdot \log_d a_{ij} - K \sum_j p'_j \cdot \log_d p'_j \end{aligned}$$

Če v matriki P_k elemente izbrane vrstice označimo z $r_1, r_2, \ldots, r_v$ ($r_j \geq 0$, $\sum\limits_{j=1}^{v} r_j = 1$), elemente posameznega stolpca pa z $s_1, s_2, \ldots, s_u$ ($s_i \geq 0$, $\sum\limits_{i=1}^{u} s_i = \frac{u}{v}$) lahko $I(X;Y)$ pišemo nadalje kot:

$$\begin{aligned} I(X;Y) &= K \sum_i p_i \sum_j r_j \cdot \log_d r_j - K \sum_j p'_j \cdot \log_d p'_j \\ &= H(p'_1, \ldots, p'_v) - H(r_1, \ldots, r_v) \end{aligned}$$

Ker je $C = \max\limits_{P_X \in \Delta_u} \{I(X;Y)\}$, in ker z P_X ne moremo vplivati na $H(r_1, \ldots, r_v)$, ker je le-ta odvisna od lastnosti kanala (P_K), velja:

$$C = \max_{P_X \in \Delta_u} \{H(p'_1, \ldots, p'_v)\} - H(r_1, \ldots, r_v)$$

Največjo entropijo $H(p'_1, \ldots, p'_v)$, ki je enaka:

$$\max\{H(p'_1, \ldots, p'_v)\} = K \cdot \log_d v$$

pa implicira $p_i = \frac{1}{u}$ in $P_X = (\frac{1}{u}, \ldots, \frac{1}{u})$, ker je tedaj :

$$p'_j = \sum_{i=1}^{u} (a_{ij} \cdot p_i) = \frac{1}{u} \cdot \sum_{i=1}^{u} s_i = \frac{1}{v}$$

Rezultat je enak:

$$\begin{aligned} C &= K \cdot \log_d v - H(r_1, \ldots, r_v) \\ &= K \cdot \log_d v + K \sum_{i=1}^{v} r_i \cdot \log\ r_i \end{aligned}$$

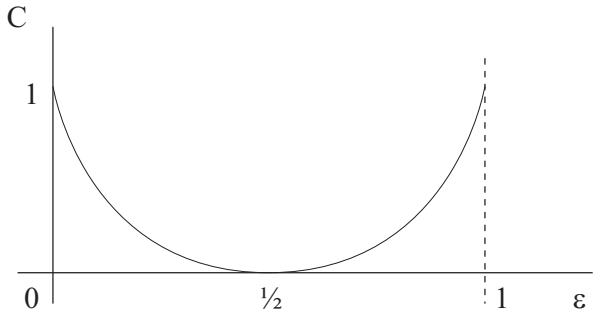
PRIMER 24:

Določite kapaciteto dvojiškega simetričnega kanala, ki ga podaja P_K:

$$P_K = \begin{bmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{bmatrix};\ P_X = (\tfrac{1}{2}, \tfrac{1}{2}) \rightarrow P_Y = (\tfrac{1}{2}, \tfrac{1}{2})$$

$$\begin{aligned} C &= H\left(\frac{1}{2}, \frac{1}{2}\right) - H(1-\varepsilon, \varepsilon) = \\ &= 1 + (1-\varepsilon) \cdot \log(1-\varepsilon) + \varepsilon \cdot \log \varepsilon \end{aligned}$$

Funkcija $C(\varepsilon)$ izgleda takole:



Pri $\varepsilon = 0$ in $\varepsilon = 1$ je simetrični kanal brez izgub, pri $\varepsilon = 1/2$ pa je neuporaben.
◇

6.2 Zvezni komunikacijski kanal

Zvezni komunikacijski kanal prenaša **zvezne signale**, ki so ali:

1. signali z diskretnim časom in zvezno amplitudo, ali
2. signali z zveznim časom in zvezno amplitudo

6.2.1 Zvezni signali z diskretnim časom in zvezno amplitudo

Kapaciteto zveznega kanala v tem primeru določa

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

Zaradi časovno diskretnih signalov je:

$$
\begin{aligned}
I(X;Y) &= H(Y) - H(Y|X) \\
&= H(Y) - H\left((X+Z)|X\right) \\
&= H(Y) - H(Z|X) \\
&= H(Y) - H(Z) \quad , \quad Z \text{ je šum, ki ni koreliran z } X.
\end{aligned}
$$

- Gaussov kanal ima šum modeliran z Gaussovo porazdelitveno funkcijo (funkcijo verjetnosti gostote). Moči signala in šuma sta omejeni:

$$
\begin{aligned}
E\{x_i^2\} &= \frac{1}{n}\sum_{i=1}^{n} x_i^2 \leq S && \text{– povprečna moč niza je omejena s konstanto } S \\
\sigma_Z^2 &= N && \text{– varianca šuma je konstanta } N
\end{aligned}
$$

Tedaj je:

$$
\begin{aligned}
C &= \max_{f_X(x)} \{H(Y) - H(Z)\} \\
&= \max_{f_X(x):E\{X^2\}\leq S} \{H(Y) - \ln\sqrt{2\pi e N}\} \\
&= \max_{f_X(x):E\{X^2\}\leq S} \{H(Y)\} - \ln\sqrt{2\pi e N}
\end{aligned}
$$

Če upoštevamo zvezo $\sigma_Y^2 = E\{Y^2\} = S + N$ dobimo končno:

$$
\begin{aligned}
C &= \frac{1}{2}\ln 2\pi e(S+N) - \frac{1}{2}\ln 2\pi e N \\
&= \frac{1}{2}\ln(1 + \frac{S}{N})
\end{aligned}
$$

oziroma splošno

$$
C = \frac{1}{2} K \log_d(1 + \frac{S}{N}) \quad \text{[bitov/vrednost signala v diskr. času, } d = 2]
$$

6.2.2 Zvezni signali z zveznim časom in zvezno amplitudo

Tukaj upoštevamo frekvenčno omejitev $(-F, +F)$, ki pove, da v signalu ni frekvence, višje od F. Tedaj lahko signal zapišemo diskretno z $2F$ vzorci/sek (3 Shannonov teorem), kar pomeni, da uporabimo Gaussov časovno diskretni kanal natanko $2F$-krat/sek.

Tedaj je:

$$
\begin{aligned}
C &= 2F\frac{1}{2}K\log_d(1 + \frac{S}{N}) \\
&= FK\log_d(1 + \frac{S}{N}) \quad \text{[bitov/sek, če } d = 2]
\end{aligned}
$$

PRIMER 25:

Telefonska linija je zvezni kanal s frekvenčnim pasom $(300 \div 3400Hz)$. Če je $\frac{S}{N} = 100 = 20dB$ $(\frac{S}{N}[dB] = 10\log_{10}\frac{S}{N})$, je kapaciteta kanala 20.640 bitov/sek. Dejansko pa lahko po takšnem kanalu dosežemo le hitrost 19.200 bitov/sek. Razlika je posledica realnih pomanjkljivosti telefonskih kanalov (presluha, odboja, ...).

$$20.640 = (3.400 - 300)\log_2 101 = 3.100\frac{\log_{10} 101}{\log_{10} 2}$$

$\diamond$

Poglavje 7

Kodiranje/dekodiranje kanala

- Naloga kodirnika in dekodirnika kanala je, da napravita prevajanje informacije po kanalu odporno na motnje.

- Kodirnik kanala obdeluje **niz** k znakov abecede B (po gospodarnem kodiranju vira), ki tvorijo **blok**.

  Z M označujemo število različnih blokov

  $$M \leq b^k \quad (\text{oz. } M \leq 2^k, \text{ če } B = \{0, 1\})$$

  in z D množico blokov

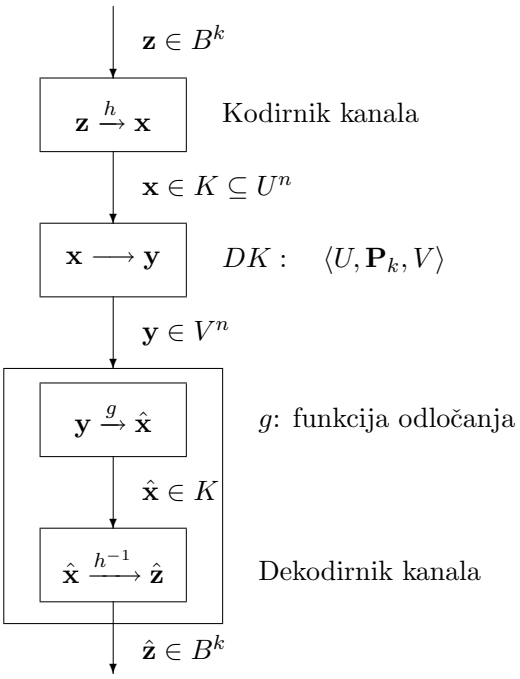
  $$D = \{\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_M\} \quad , \mathbf{z}_i \text{ je blok dolžine } k$$

- Kodirnik kanala preslika vsak blok $\mathbf{z}_i$ dolžine k v njegovo kodno zamenjavo $\mathbf{x}_i$ dolžine n, $n > k$. $\mathbf{x}_i$ je vhodni vektor v kanal in je sestavljen iz znakov abecede U:

  $$D = \{\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_M\} \longrightarrow K = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_M\}$$

- Pri prenosu skozi kanal z motnjami se $\mathbf{x}$ preslika v isti vektor $\mathbf{y}$, na osnovi katerega dekodirnik kanala oceni $\hat{\mathbf{x}}$.

Velja:



- Kodirnik in dekodirnik kanala skupaj določata kod $\mathcal{K}(n,k)$, oz. funkcijo $h(\mathbf{z} \to \mathbf{x})$ in funkcijo $g(\mathbf{y} \to \hat{\mathbf{x}})$ ter funkcijo $h^{-1}(\hat{\mathbf{x}} \to \hat{\mathbf{z}})$.

- Hitrost koda $\mathcal{K}(n,k)$ je določena z izrazom:

$$R = \frac{K \log_d M}{n} \underset{\substack{K=1 \\ d=2 \\ M=2^k}}{\overset{\uparrow}{=}} \frac{k}{n} \quad \text{(bitov/znak)}$$

7.1 Dekodiranje koda kanala

- Vektor napake zaradi motnje v kanalu je definiran kot:

$$\mathbf{e} = \mathbf{y} - \mathbf{x} \quad ; \quad \mathbf{e}, \mathbf{y}, \mathbf{x} \in \{0,1\}^n$$

N.pr.:

$$\left.\begin{array}{l} \mathbf{x} = (11011) \\ \mathbf{y} = (10001) \end{array}\right\} \longrightarrow \quad \mathbf{e} = (01010)$$

$$d_H(\mathbf{x}, \mathbf{y}) = 2$$

$d_H(\mathbf{x}, \mathbf{y})$ je Hammingova razdalja med vektorjema $\mathbf{x}$ in $\mathbf{y}$.

7.1.1 Dekodiranje z odkrivanjem napak

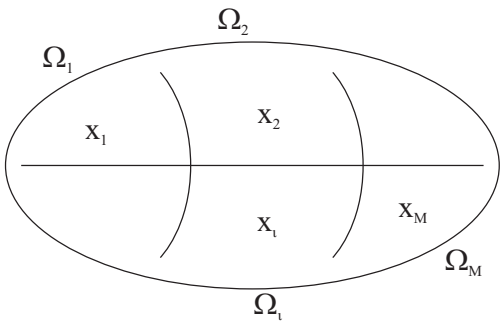
Dekodirnik ugotavlja, ali $\mathbf{y} \in K$. Če pripada, potem dekodirnik sklepa, da je $\mathbf{y} = \mathbf{x}$ in nato $\mathbf{x}$ prevede v $\mathbf{z}$.
Če pa ne pripada, ugotovi napako in zahteva ponovitev prenosa.
Verjetnost neodkrite napake ustreza primerom, ko je $\mathbf{y} \in K$ in $\mathbf{y} \neq \mathbf{x}$:

$$\underset{\substack{\text{verjetnost}\\ \text{neodkrite}\\ \text{napake pri}\\ \text{poslanem } x_i}}{P_{NN}(x_i)} = \sum_{\substack{\mathbf{y}\in K\\ \mathbf{y}\neq\mathbf{x}_i}} P\left(\mathbf{y}|\mathbf{x}_i\right)$$

7.1.2 Dekodirnik s popravljanjem napak

Prostor $\{0,1\}^n$ razdelimo na odločitvena področja $\Omega_1, \Omega_2, \ldots, \Omega_M$ (področja vektorja $\mathbf{y}$):

$$\begin{aligned} & \Omega_i = \big(\mathbf{y} : g(\mathbf{y}) = \mathbf{x}_i\big), && i = 1, 2, \ldots, M \\ \text{in} \quad & \Omega_i \cap \Omega_j = \emptyset, && i \neq j \end{aligned}$$



Če je $\mathbf{y}$ iz področja Ω_i, se dekodirnik odloči, da je bil poslan $\mathbf{x}_i$. Odločitev je napačna, če je $\mathbf{x} \neq \mathbf{x}_i$, oz. če ni bil poslan $\mathbf{x}_i$.

Verjetnost pravilnega dekodiranja je:

$$\underset{\text{pri poslanem } \mathbf{x}_i}{P_{PD}(\mathbf{x}_i)} = \sum_{\mathbf{y}\in\Omega_i} P(\mathbf{y}|\mathbf{x}_i)$$

Verjetnost napačnega dekodiranja pa je:

$$\begin{aligned} P_{ND}(\mathbf{x}_i) &= 1 - P_{PD}(\mathbf{x}_i) \\ &= \sum_{\substack{j=1\\ j\neq i}}^{M} \sum_{\mathbf{y}\in\Omega_j} P(\mathbf{y}|\mathbf{x}_i) \end{aligned}$$

Velja:

$$P_{ND}^{max} = \max_{1\leq i\leq M} \{P_{ND}(\mathbf{x}_i)\}$$

Iščemo g, ki ima minimalen P_{ND}^{max}.

7.1.3 Optimalno dekodiranje

Funkcija odločanja $g(\mathbf{y})$ lahko izbere $\hat{\mathbf{x}}$ na dva načina:

A. Na osnovi **največje verjetnosti pravilne odločitve**

$$P(\hat{\mathbf{x}}|\mathbf{y}) = \max_{1\leq i\leq M} \underbrace{\{P(\mathbf{x}_i|\mathbf{y})\}}_{\text{verjetnost pravilne odločitve}}$$

Ker velja Bayesov teorem:

$$P(\mathbf{x}_i|\mathbf{y}) = \frac{P(\mathbf{x}_i)P(\mathbf{y}|\mathbf{x}_i)}{\underbrace{\sum_{j=1}^{M} P(\mathbf{x}_j)P(\mathbf{y}|\mathbf{x}_j)}_{\substack{\| \\ P(\mathbf{y})}}}$$

je iskanje največje $P(\mathbf{x}_i|\mathbf{y})$ enakovredno iskanju največjega $P(\mathbf{y}|\mathbf{x}_i)$. Zato je mogoče g definirati tudi z:

B. Na osnovi **največje aposteriorne verjetnosti**:

$$P(\mathbf{y}|\hat{\mathbf{x}}) = \max_{1\leq i\leq M} (P(\mathbf{y}|\mathbf{x}_i))$$

Če so vhodni vektorji enako verjetni oz. $P(\mathbf{x}_i) = \frac{1}{M}$, $i = 1, \ldots, M$, sta obe funkciji odločanja enaki:

$$P(\mathbf{x}_i|\mathbf{y}) = \frac{\frac{1}{M}P(\mathbf{y}|\mathbf{x}_i)}{\underbrace{\frac{1}{M}\sum_{j=1}^{M} P(\mathbf{y}|\mathbf{x}_j)}_{1}} = P(\mathbf{y}|\mathbf{x}_i)$$

Tedaj govorimo o **idealni funkciji odločanja dekodirnika**.

PRIMER 26:

Za diskretni simetrični kanal z verjetnostno matriko $\mathbf{P}_K$ določite funkcijo odločanja g:

$$\mathbf{P}_K = \begin{bmatrix} 0{,}3 & 0{,}2 & \mathbf{0{,}5} \\ \mathbf{0{,}5} & 0{,}3 & 0{,}2 \\ 0{,}2 & \mathbf{0{,}5} & 0{,}3 \end{bmatrix}$$

Idealna funkcija odločanja g je:

$$g: \quad \begin{array}{l} y_1 \mapsto x_2 \\ y_2 \mapsto x_3 \\ y_3 \mapsto x_1 \end{array} \qquad \text{oziroma} \qquad g: \quad \begin{array}{l} x_1 \mapsto y_3 \\ x_2 \mapsto y_1 \\ x_3 \mapsto y_2 \end{array}$$

◇

Za dvojiški DSK, podan s $\mathbf{P}_K = \begin{bmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{bmatrix}$ z abecedo $B = \{0, 1\}$ velja:

$$P(\mathbf{y}|\mathbf{x}_1) > P(\mathbf{y}|\mathbf{x}_2) \Longleftrightarrow d_H(\mathbf{x}_1, \mathbf{y}) < d_H(\mathbf{x}_2, \mathbf{y}),$$

oz. pri sprejetem $\mathbf{y}$ določimo poslani vektor $\hat{\mathbf{x}}$ na osnovi najmanjše $d_H(\hat{\mathbf{x}}, \mathbf{y})$. Idealna funkcija odločanja je $g(\mathbf{y}) = \hat{\mathbf{x}}$.

Dokaz:

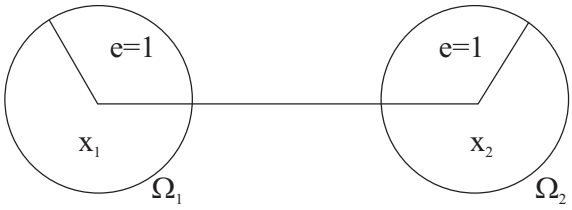
$$\frac{P(\mathbf{y}|\mathbf{x}_1)}{P(\mathbf{y}|\mathbf{x}_2)} = \frac{\varepsilon^{m_1}(1-\varepsilon)^{n-m_1}}{\varepsilon^{m_2}(1-\varepsilon)^{n-m_2}} = \underbrace{\left(\frac{1-\varepsilon}{\varepsilon}\right)^{m_2-m_1}}_{\substack{m\text{- število bitov,} \\ \text{kjer se } \mathbf{x} \text{ in } \mathbf{y} \text{ razlikujeta}}}$$

Za DSK brez spomina je $P(\mathbf{y}|\mathbf{x}) = P(y_1|x_1)P(y_2|x_2)\cdots P(y_n|x_n)$.
Če je $\varepsilon < 1/2$ sledi $(1-\varepsilon)/\varepsilon > 1$:, zato velja $\frac{P(y|x_1)}{P(y|x_2)} > 1$, če $m_1 < m_2$.

Zaradi varnega prenosa moramo iskati M kodnih zamenjav tako, da so Hammingove razdalje med njimi v prostoru $\{0, 1\}^n$ čim večje. Minimalno razdaljo med kodnimi zamenjavami določa pogoj:

$$d_{min} \geq 2e + 1 \ ,$$

kjer je e povprečno število napak v kanalu.



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

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

To je le **potreben pogoj**, saj vedno tega pogoja ni mogoče realizirati. Npr. $n = 4, e = 1 \rightarrow M = 3$, $d_{min} = 2e + 1 = 3$. Med vektorji dolžine $n = 4$ je mogoče najti le dva z $d_H = 3$, ne pa treh: $0xxx, 1xxx$.

7.2 Kanalski kodni teorem (2 Shannonov teorem)

- Govori o DK (diskretnem kanalu) brez spomina in s kapaciteto $C > 0$ ter o pogojih, pod katerimi je možno brez napak določiti poslano informacijo po kanalu s šumom.
- **2 Shannonov ali kanalski kodni teorem (Eksistenčni teorem):**

  Dana sta DK brez spomina s kapaciteto $C > 0$ in realno število R $(0 < R < C)$. Obstaja takšen kod $\mathcal{K}(n,k)$ in takšna funkcija odločanja g, da velja:

  $$\overline{P_{ND}^{max}} \leq \delta + d^{-\rho n}, \quad \lim_{n\to\infty} \overline{P_{ND}^{max}} \to 0$$
  $$M \leq d^{nR}$$

  kjer sta δ in ρ poljubno majhni pozitivni števili, M število kodnih zamenjav v množici K, R hitrost kode, d osnova logaritma ter $\overline{P_{ND}^{max}}$ povprečje največjih verjetnosti napak kodov preko vseh $\mathcal{K}(n,k)$ (oz. povprečje zgornjih mej nepravilnega dekodiranja preko vseh $\mathcal{K}(n,k)$).

  Dokaz: Brez izgube na splošnosti, vzemimo slučaj DSK, $u = v = 2$, verjetnost napake ε in $C = 1 - H(\varepsilon, 1-\varepsilon)$. Predpostavimo $R < C$. Kod $\mathcal{K}(n,k)$ določa M kodnih zamenjav, $M = 2^k = 2^{nR}$.

  Bernoullijev zakon velikih števil zagotavlja, da je pri dovolj velikem n verjetnost sprejema $\mathbf{y}_j$, oddaljenega od oddanega $\mathbf{x}_i$ za več kot $n(\varepsilon+\varphi)$, manjša od δ:

  $$P(\mathbf{y}_j|\mathbf{x}_i) < \delta, \quad d_H(\mathbf{x}_i, \mathbf{y}_j) > n(\varepsilon+\varphi)$$

  Označimo pri oddanem $\mathbf{x}_i$ in prejetem $\mathbf{y}_j$ z Ψ_i množico vektorjev, ki se od $\mathbf{y}_j$ razlikujejo za manj kot $n(\varepsilon+\varphi)$. Tedaj do napake dekodiranja pride, če odposlan $\mathbf{x}_i$ ni v Ψ_i ali če Ψ_i vsebuje več kot en vektor iz K. Zgornja meja za P_{ND}^{max} je zato podana z:

  $$\overline{P_{ND}^{max}} \leq \delta + \sum_{\substack{j=1\\ j\neq i}}^{M} P(\underbrace{\mathbf{x}_j \in \Psi_i}_{\mathbf{x}_j \neq \mathbf{x}_i \text{ v } \Psi_i})$$

  Za $P(\mathbf{x}_j \in \Psi_i)$ velja ocena:

  $$\hat{P}(\mathbf{x}_j \in \Psi_i) = \frac{\sum_{k=0}^{n(\varepsilon+\varphi)} \binom{n}{k}}{2^n}$$

  To je razmerje med številom vektorjev dolžine n, ki se od y razlikujejo za največ $n(\varepsilon+\varphi)$ in vsem vektorjem dolžine n.

  Če zgornjo oceno vstavimo v zgornjo mejo za P_{ND}^{max}, ter upoštevamo, da je povprečna zgornja meja preko vseh različnih kod kvečjemu manjša, dobimo:

  $$P_{ND}^{max} \leq \delta + (M-1) \cdot \frac{\sum_{k=0}^{n(\varepsilon+\varphi)} \binom{n}{k}}{2^n}$$

  Ob upoštevanju:

  $$\sum_{k=0}^{n\alpha} \binom{n}{k} \leq 2^{nH(1-\alpha,\alpha)}, \quad \alpha < \frac{1}{2}$$

dobimo:

$$\overline{P_{ND}^{max}} \leq \delta + 2^{-n[1-H(1-(\varepsilon+\varphi),(\varepsilon+\varphi))]}$$

in končno ob upoštevanju $M = 2^k = 2^{nR}$:

$$\overline{P_{ND}^{max}} \leq \delta + 2^{-n[1-H(1-(\varepsilon+\varphi),(\varepsilon+\varphi))-R]}$$

Ker sta δ in φ poljubno majhna, lahko, če je R manjši od $C = [1 - H(1-\varepsilon, \varepsilon)]$, naredimo $\overline{P_{ND}^{max}}$ poljubno majhen, ko gre $n \to \infty$. Če pa je $R > C$, potem $\overline{P_{ND}^{max}}$ ne gre proti 0 z $n \to \infty$.

7.3 Varno kodiranje

Obstajata 2 skupini postopkov za varno kodiranje: **bločno** in **konvolucijsko** kodiranje. Pri bločnem se vsak blok preslika v ustrezno kodno zamenjavo neodvisno od predhodnih blokov, pri konvolucijskem pa je kodna zamenjava odvisna tudi od določenega števila predhodnih blokov. V nadaljevanju bomo spoznali nekaj najbolj znanih postopkov **bločnega kodiranja**.

7.3.1 Linearni bločni kodi

Bločni kod je **linearni** z oznako $\mathcal{L}(n, k)$, če za vsak $x_i \in \mathcal{L}$ (i-ta kodna zamenjava) velja:

1. $\mathbf{x}_i + \mathbf{x}_j \in \mathcal{L}$, za vsak $i = 1, \ldots, M \quad i \neq j$
2. $a \cdot \mathbf{x}_i \in \mathcal{L}$, za vsak a iz posebne množice (Galoisov obseg)

Kodne zamenjave $\mathcal{L}(n, k)$ lahko ustvarimo iz ene same z operacijama 1 in 2.

a) Kodi s preverjanjem sodosti Tukaj je $n = k + 1$, kar pomeni, da k informacijskim bitom dodamo 1 bit, ki ga določimo tako, da je vsota vseh n bitov soda (soda pariteta), $x_n = \sum_{i=1}^{k} z_i \cdot \text{mod } 2$:

$$\mathbf{z} = (z_1, \ldots, z_k) \in \{0, 1\}^k \longrightarrow \mathbf{x} = (z_1, \ldots, z_k, x_n) \in \{0, 1\}^n$$

Torej velja naslednje:

$$\sum_{i=1}^{n} x_i \text{ mod } 2 = 0$$

PRIMER 27:

Za dano množico $D = \{(00), (01), (10), (11)\}$ določite množico K s preverjanjem sodosti.

$$K = \{(000), (011), (101), (110)\}$$

◇

b) Vodoravno in navpično preverjanje sodosti Če vzamemo $m = n - k \gg 1$, lahko iz sprejetega vektorja $\mathbf{y}$ sklepamo ne le o napaki, ampak tudi o lokaciji napake.
Npr.

$$\begin{aligned} \mathbf{z} &= (z_1, \ldots, z_k) && , k = 4 \\ \mathbf{x} &= (z_1, \ldots, z_4, x_5, \ldots, x_8) && , n = 8 \\ m &= n - k = 4 \end{aligned}$$

Preverjanje sodosti lahko določimo iz enačb:

$$\begin{aligned} x_5 &= z_1 + z_2 \\ x_6 &= z_3 + z_4 \\ x_7 &= z_1 + z_3 \qquad \text{ali} \\ x_8 &= z_2 + z_4 \end{aligned}$$

z_1	z_2	x_5
z_3	z_4	x_6
x_7	x_8	

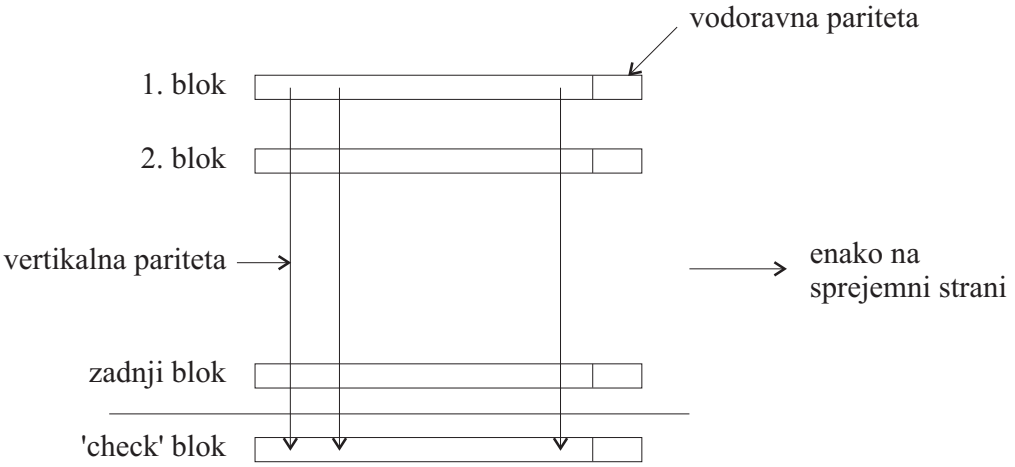
Pri $\mathbf{z} = (1101) \longrightarrow \mathbf{x} = (1101|0110)$.

Če dobimo $\mathbf{y} = (0101|0110)$ sledi iz enačb na sprejemni strani:

$$x_5 = 1 \quad x_6 = 1 \quad x_7 = 0 \quad x_8 = 0$$

Ker se x_5 in x_7 ne ujemata z dobljenimi, je napaka na preseku obeh, to je z_1. Ta sistem predpostavlja $k \gg m$ oz. da je napaka le na prvih k bitih, sicer odpove. Pri napaki informacijskega bita sta narobe dva varnostna bita, pri napaki varnostnega bita pa en sam.

- Splošna shema vodoravno-navpične kontrole sodosti pa je:



Enačbe za preverjanje sodosti lahko podamo kot sistem m linearno neodvisnih enačb:

$$\begin{array}{lllllllll} x_1 & +x_2 & & & +x_5 & & & = & 0 \\ & & x_3 & +x_4 & & +x_6 & & = & 0 \\ x_1 & & +x_3 & & & & +x_7 & = & 0 \\ & x_2 & & +x_4 & & & +x_8 & = & 0 \end{array}$$

oz. v matrični obliki:

$$\mathbf{H}_{4\times 8} \cdot \mathbf{x}^T_{8\times 1} = \mathbf{0}_{4\times 1}$$

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}; \quad \mathbf{x}^T = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_8 \end{bmatrix}$$

Če ima $\mathbf{H}$ rang matrike m (največji red poddeterminante, ki ni 0), potem ima poleg m neodvisnih (linearno neodvisnih) vrstic tudi m linearno neodvisnih stolpcev.
Tedaj imamo sistem enačb:

$$\begin{array}{ccccccccc} h_{11}x_1 & + & h_{12}x_2 & + & \cdots & + & h_{1n}x_n & = & 0 \\ \vdots & & \vdots & & \vdots & & \vdots & = & \vdots \\ h_{m1}x_1 & + & h_{m2}x_2 & + & \cdots & + & h_{mn}x_n & = & 0 \end{array}$$

kjer lahko za k x-ov izberemo poljubne vrednosti iz $\{0, 1\}$. Preostalih m vrednosti pa rešimo s pomočjo sistema: $\mathbf{H} \cdot \mathbf{x}^T = 0$.

Pozor: Pri reševanju enačb oziroma množenju matrik računamo po mod 2 – namesto seštevanja tako uporabimo ∇ (XOR), namesto množenja pa konjunkcijo (AND).

PRIMER 28:

Po kanalu želimo prenašati množico 8 blokov $D = \{(000), (001), \ldots, (111)\}$. Pričakujemo 1 napako na blok ($e = 1$). Določite K!

Iz $M = 8$ in $e = 1$ določimo n iz Hammingovega pogoja $2^n/(1+n) \geq 8 \longrightarrow n = 6$. Matrika $\mathbf{H}$ za določitev koda je dimenzije $m \times n = 3 \times 6$. Trije stolpci so lahko neodvisni, ostali se morajo razlikovati in ne smejo biti iz samih ničel. Na osnovi tega pogoja izberemo:

$$H_{3\times 6} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [I_m | B_{mk}]$$

V zgradbi $\mathbf{H}$ smo predpostavili tudi zgradbo $\mathbf{x} = (x_1, x_2, x_3, z_1, z_2, z_3)$.
Za vsak $\mathbf{z} \in D$ lahko izračunamo (x_1, x_2, x_3) iz sistema $\mathbf{H} \cdot \mathbf{x}^T = \mathbf{0}$. Dobimo rezultat:

	x_1	x_2	x_3	z_1	z_2	z_3
$\mathbf{x}_1$	0	0	0	0	0	0
$\mathbf{x}_2$	1	0	1	0	0	1
$\mathbf{x}_3$	1	1	0	0	1	0
$\mathbf{x}_4$	0	1	1	0	1	1
$\mathbf{x}_5$	1	1	1	1	0	0
$\mathbf{x}_6$	0	1	0	1	0	1
$\mathbf{x}_7$	0	0	1	1	1	0
$\mathbf{x}_8$	1	0	0	1	1	1
	iz $H \cdot \mathbf{x}^T = 0$			iz D		

Med kodnimi zamenjavami velja d_{min}.

◇

7.3.1.1 Dekodiranje linearnih bločnih kodov

Če s $\mathbf{H}_{m\times n}$ definiramo linearni bločni kod za množico M kodnih zamenjav (K), potem dobimo **sindrom** prejetega vektorja $\mathbf{y}$ iz izraza:

$$\mathbf{s}^T = \mathbf{H} \cdot \mathbf{y}^T$$

Dekodiranje z detekcijo napak Če **samo odkrivamo** napake na sprejemni strani kanala, potem nas zanima, ali je $\mathbf{s}^T = \mathbf{0}$ ali ne.

Če $\mathbf{s}^T = \mathbf{0} \longrightarrow \hat{\mathbf{x}} = \mathbf{y}$, sicer je potreben ponoven prenos po kanalu.

PRIMER 29:

Za kod $\mathcal{L}(3,2)$ z matriko $\mathbf{H} = [111]$ in $K = \{(000),(101),(011),(110)\}$, ugotovite pri prejetem $\mathbf{y} = (001)$ sindrom.

$$\mathbf{s}^T = \mathbf{H} \cdot \mathbf{y}^T = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = 1$$

Ker je $s \neq 0$, dekodirnik zahteva ponoven prenos. $\diamond$

Dekodiranje s popravljanjem napak Če želimo dekodirati skupaj s popravljanjem napake, potem velja:

$$\begin{aligned} \mathbf{s}^T &= \mathbf{H} \cdot \mathbf{y}^T \\ &= \mathbf{H} \cdot (\mathbf{x} + \mathbf{e})^T = \mathbf{H} \cdot \mathbf{x}^T + \mathbf{H} \cdot \mathbf{e}^T \\ &= \mathbf{H} \cdot \mathbf{e}^T \end{aligned}$$

Postopek dekodiranja:

1. Če $\mathbf{s}^T = \mathbf{H} \cdot \mathbf{y}^T = \mathbf{0} \longrightarrow \mathbf{x} = \mathbf{y}$
2. Če $\mathbf{s}_i^T = \mathbf{H} \cdot \mathbf{y}^T \neq \mathbf{0}$ in $\mathbf{s}_i^T = \mathbf{H} \cdot \mathbf{e}_i^T$, potem je $\mathbf{x} = \mathbf{y} + \mathbf{e}_i$
3. Če $\mathbf{s}_j^T = \mathbf{H} \cdot \mathbf{y}^T \neq \mathbf{0}$ in $\mathbf{s}_j^T \neq \mathbf{s}_i^T = \mathbf{H} \cdot \mathbf{e}_i^T$, potem zahtevamo ponoven prenos.

PRIMER 30:

Imamo kod $\mathcal{L}(3,1)$, ki lahko popravi vse enojne napake iz množice $E = \{(100),(010),(001)\}$.

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

Določite razmere pri $\mathbf{x} = (111)$ in $\mathbf{y} = (011)$!

Iz $D = \{0,1\}$ in s pomočjo $\mathbf{H} \cdot \mathbf{x}^T = \mathbf{0}$ dobimo $K = \{(000),(111)\}$:

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ 0 \end{bmatrix} = 0; \quad x_1 = 0, \quad x_2 = 0$$

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ 1 \end{bmatrix} = 0; \quad x_1 + 1 = 0 \longrightarrow x_1 = 1, \quad x_2 + 1 = 0 \longrightarrow x_2 = 1$$

Za vsak $\mathbf{e} \in E$ dobimo:

$$\mathbf{s}_1^T = \mathbf{H} \cdot \mathbf{e}_1^T = \mathbf{H} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\mathbf{s}_2^T = \mathbf{H} \cdot \mathbf{e}_2^T = \mathbf{H} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\mathbf{s}_3^T = \mathbf{H} \cdot \mathbf{e}_3^T = \mathbf{H} \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$\mathbf{s}^T = \mathbf{H} \cdot \mathbf{y}^T = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \mathbf{s}_1^T$$

Sledi: $\mathbf{x} = \mathbf{y} + \mathbf{e}_1 = (011) + (100) = \underline{(111)}$
$\diamond$

7.3.1.2 Dekodiranje z idealno funkcijo odločanja

- Za vsak $\mathbf{s}^T \in \{0,1\}^m$ imamo množico $\Omega_\mathbf{s} = \left\{\mathbf{y} \in \{0,1\}^n; \quad \mathbf{H} \cdot \mathbf{y}^T = \mathbf{s}^T\right\}$.
- Množice $\Omega_\mathbf{s}$ zapišemo v obliki standardne razpredelnice (v prvi vrstici vse kodne zamenjave, v drugi nove kodne zamenjave (z najmanjšo težo - številom 1), ki jih prištevamo k vektorjem 1 vrstice) (glej primer spodaj), itd.

  Postopek dekodiranja:

  1. določimo $\Omega_\mathbf{s} = \left\{\mathbf{y} | \mathbf{H} \cdot \mathbf{y}^T = \mathbf{s}^T\right\}$ iz standardne razpredelnice za prejeti $\mathbf{y}$
  2. poiščemo $\mathbf{y} \in \Omega_\mathbf{s}$ z najmanjšo težo (št. enic) - element v 1 koloni ($\mathbf{y}_0$)
  3. odločimo: $\hat{\mathbf{x}} = \mathbf{y} + \mathbf{y}_0$

PRIMER 31:

Za kod $\mathcal{L}(5,2)$ in $D = \{(00),(01),(10),(11)\}$ je podana matrika $\mathbf{H}$:

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \neq \left[\mathbf{I}|\mathbf{B}\right]_{n=5,k=2,m=3}$$

Izračunajte K in na osnovi standardne razpredelnice podajte odločitev dekodirnika, če je $\mathbf{x} = (11100)$ in $\mathbf{y} = (11000)$.

$$K = \{(00000), (11100), (00111), (11011)\}\text{, kar sledi iz } D \text{ in } \mathbf{H} \cdot \mathbf{x}^T = \mathbf{0}.$$

Tvorimo standardno razpredelnico:

	popravljalnik				sindrom
	00000	11100	00111	11011	000
poln razred enojnih napak	10000	01100	10111	01011	110
	01000	10100	01111	10011	100
	00100	11000	00011	11111	010
	00010	11110	00101	11001	011
	00001	11101	00110	11010	001
dvojne napake	10001	01101	10110	01010	111
	10010	01110	10101	01001	101

$$\mathbf{H} \cdot \mathbf{y}^T = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

Sindrom določa $\Omega_{\mathbf{s}} \longrightarrow \mathbf{y}_0(\Omega_{\mathbf{s}}) = (00100)$.

Končno: $\hat{\mathbf{x}} = \mathbf{y} + \mathbf{y}_0 = (11000) + (00100) = (11100)$

- V 1. vrstici so vse kodne zamenjave.
- 2. vrstico standardne razpredelnice tvorimo tako, da poiščemo vektor, ki ni v prvi vrstici. Ker jih je več, izberemo tistega z najmanjšo težo (število enic), saj je verjetnost take napake največja. Damo ga v 1. kolono 2. vrstice in nato ostale kolone določimo tako, da ta vektor prištejemo k vektorjem 1. vrstice (iščemo napačne vektorje, ki jih pokvarimo z vodilnim vektorjem).
- 3. vrstico sestavimo tako, da najprej poiščemo najmanjši vektor (z najmanjšo težo), ki ga ni v zgornjih vrsticah. Z njim pokvarimo vektorje 1. vrstice in dobimo preostale vektorje 3. vrstice, itd.
- **Ničelni vektor** zapišemo vedno na začetek 1. vrstice (tudi če ni kodna zamenjava).

◇

7.3.1.3 Dekodiranje Hammingovega koda $\mathcal{H}(n,k)$

- Hammingov kod $\mathcal{H}(n,k)$ je linearni bločni kod z dolžino kodnih zamenjav $n = 2^m - 1$, $m \geq 2$ in $e = 1$ ter matriko za preverjanje sodosti H, ki ima v stolpcih zapisana števila $1, 2, \ldots, 2^m - 1$ (vse razen 0). To je **popolni kod**, ker zanj velja:

$$M \cdot \sum_{i=0}^{e} \binom{n}{i} = 2^n \quad \text{(enakost v Hammingovemu pogoju)}$$

- Dekodiranje Hammingovega koda je posebej preprosto. $\mathbf{s}^T = \mathbf{H} \cdot \mathbf{y}^T$ pove mesto v prejetem $\mathbf{y}$, kjer je napaka. Če je $\mathbf{s}^T = \mathbf{0}$, ni napake.

  Kodiranje pa je enako kot prej, s pomočjo enačbe $\mathbf{H} \cdot \mathbf{x}^T = \mathbf{0}$ in D.

PRIMER 32:

Pokažite dekodiranje Hammingovega koda za primer:

$$m = 3 \qquad\qquad x = (100\underline{1}100)$$
$$D = \{(0000), \ldots, (1111)\} \qquad\qquad y = (100\underline{0}100)$$

Za $m = 3$ je matrika $\mathbf{H}$, ki določa Hammingov kod ($\mathcal{H}(7,4)$) enaka:

$$H = \begin{array}{c} \begin{array}{ccccccc} x_1 & x_2 & z_1 & x_3 & z_2 & z_3 & z_4 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

S kodiranjem kot prej (s pomočjo D in $\mathbf{H} \cdot \mathbf{x}^T = \mathbf{0}$) dobimo:

$$\begin{aligned} K = \{&(0000000), (1101001), (0101010), (1000011), \\ &(1001100), (0100101), (1100110), (0001111), \\ &(1110000), (0011001), (0011010), (0110011), \\ &(0111100), (1010101), (0010110), (1111111)\} \end{aligned}$$

$$\mathbf{H} \cdot \mathbf{y}^T \longrightarrow \mathbf{s}^T = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad \text{kar določa lego napake v } H$$

S popravljanjem $\mathbf{y}$ dobimo $\mathbf{x}$.

$\diamond$

7.3.2 Ciklični kodi

- **Ciklični kod** $\mathcal{C}(n,k)$ je linearni kod, v katerem da vsak cikličen premik znakov ene kodne zamenjave kakšno drugo kodno zamenjavo iz K:

  $$(x_{n-1}, x_{n-2}, \ldots, x_0) \in K \longrightarrow (x_{n-2}, \ldots, x_0, x_{n-1}) \in K$$

  N.pr.:

  $$K_1 = \{(0000), (1111)\}$$
  $$K_2 = \{(0000), (0001), (1000), (0100), (0010)\}$$

- Pri cikličnih kodih zapisujemo informacijske bloke in njihove kodne zamenjave s polinomi

  $$\mathbf{x} = (x_{n-1}, x_{n-2}, \ldots, x_1, x_0)$$
  $$x(p) = x_{n-1} \cdot p^{n-1} + \cdots + x_1 \cdot p + x_0$$

  Operacija + je vsota po modulu 2

  Operacija $\cdot$ pa je konjunkcija

  N.pr.:

  $$\mathbf{x} = (110101)$$
  $$x(p) = p^5 + p^4 + p^2 + 1$$

- Ciklični premik kodne zamenjave za 1 mesto v levo ustreza zmnožku polinoma $x(p)$ s p, po modulu $(p^n + 1)$:

  N.pr.:

  $$\begin{aligned}\left(x_{n-1} \cdot p^{n-1} + \cdots + x_1 \cdot p + x_0\right) \cdot p &= x_{n-1} \cdot p^n + \cdots + x_1 \cdot p^2 + x_0 \cdot p \\ &= x_{n-2} \cdot p^{n-1} + \cdots + x_0 \cdot p + x_{n-1} \\ &\uparrow \\ &\text{če } p^n = 1 \text{ ali } p^n - 1 = 0 = p^n + 1 \\ &(+ \equiv \bigtriangledown)\end{aligned}$$

- Premik za i-mest v levo tedaj ustreza

  $$p^i \cdot x(p) \bmod (p^n + 1)$$

PRIMER 33:

Prepričajte se o pravilnosti zapisa o cikličnem zamiku na primeru kode $\mathbf{x} = (10101)$ in njegovem zamiku za 3 mesta v levo:

$$\mathbf{x} = (10101) \longrightarrow x(p) = p^4 + p^2 + 1$$
$$\mathbf{x}''' = (01101) \longrightarrow x'''(p) = p^3 + p^2 + 1$$

$$p^3 \cdot \left(p^4 + p^2 + 1\right) \bmod \left(p^5 + 1\right) = \left(p^7 + p^5 + p^3\right) \bmod \left(p^5 + 1\right) = p^3 + p^2 + 1$$

$$\begin{array}{ccccccccccccc}
p^7 & + & p^5 & + & p^3 & : & p^5 & + & 1 & = & p^2 & + & 1 \\
p^7 & & & & & p^2 & & & & & & & \\
\hline
 & & p^5 & + & p^3 & + & p^2 & & & & & & \\
 & & p^5 & & & & & + & 1 & & & & \\
\hline
 & & & & p^3 & + & p^2 & + & 1 & \equiv & \text{ostanek oz. rezultat modulskega produkta} & &
\end{array}$$

◇

- Linearne bločne kode lahko definiramo tudi s pomočjo **generatorske matrike G** dimenzije $(k \times n)$ z rangom k $(rang(\mathbf{G}) = k)$ ter elementi $g_{ij} \in \{0, 1\}$, $i = 1, \ldots, k$, $j = 1, \ldots, n$. Njene vrstice predstavljajo k linearno neodvisnih n-komponentnih vektorjev, ki so **temeljne kodne zamenjave** (bazni vektorji v prostoru $\{0, 1\}^n$).

- Kodne zamenjave $\mathbf{x}$ linearnega bločnega koda $\mathcal{L}(n, k)$ določimo s pomočjo matrike $\mathbf{G}$ tako, da M vektorjev $\mathbf{z} \in D$ množimo na desni z $\mathbf{G}$:

$$\mathbf{x}_i = \mathbf{z}_i \cdot \mathbf{G} = \sum_{j=1}^{k} z_j \cdot v_j, \quad i = 1, \ldots, M$$

- Med $\mathbf{G}$ in $\mathbf{H}$ velja relacija:

$$\mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}$$

oz. če $\mathbf{H} = [\mathbf{I}_m | \mathbf{B}_{mk}] \longrightarrow \mathbf{G} = \left[\mathbf{B}_{mk}^T | \mathbf{I}_k\right]$
in če: $\mathbf{G} = [\mathbf{I}_k | \mathbf{A}_{km}] \longrightarrow \mathbf{H} = \left[\mathbf{A}_{km}^T | \mathbf{I}_m\right]$.

PRIMER 34:

Določite množico kodnih zamenjav K za kod $\mathcal{L}(5, 2)$, ki ga definira

$$G = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}, \quad D = \{(00), (01), (10), (11)\}$$

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

$$\vdots$$

Rezultat:

$$K = \{(00000), (11100), (00111), (11011)\}$$

◇

PRIMER 35:

Dana je matrika $\mathbf{H}$, ki določa kod $\mathcal{L}(5,2)$. Določite generatorsko matriko $\mathbf{G}$ istega koda.

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

S prerazporeditvijo najprej zapišemo $\mathbf{H}$ v standardno obliko:

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} = [\mathbf{I}_m | \mathbf{B}_{mk}]$$

Od tod sledi ob upoštevanju $\mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}$:

$$\mathbf{G} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix} = \left[\mathbf{B}_{mk}^T | \mathbf{I}_k\right]$$

$\diamond$

- Linearni bločni kod je **sistematičen**, če ima kodne zamenjave s strnjenimi informacijskimi znaki. Ostali varnostni znaki so ali predpona ali pripona.

- V matriki $\mathbf{G} = [\mathbf{I}_k | \mathbf{A}_{km}]$ ima zadnja vrstica oz. polinom posebno ime: **generatorski polinom koda**.

  Ta polinom ima najnižjo stopnjo, t.j. $m = n - k$. Označujemo ga z $g(p)$:

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

  Matriko $\mathbf{G}$ lahko sestavimo s pomočjo produktov: $g(p), p \cdot g(p), p^2 \cdot g(p), \ldots, p^{k-1} \cdot g(p)$, saj ustrezajo linearnim neodvisnim zamenjavam cikličnega koda:

  $$\mathbf{G} = \begin{bmatrix} 1 & g_{m-1} & g_{m-2} & \cdots & g_1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & g_{m-1} & \cdots & \cdots & g_1 & 1 & \cdots & \cdots & 0 \\ \vdots & & & & & & \vdots & & & \vdots \\ 0 & 0 & \cdots & \cdots & \cdots & 1 & g_{m-1} & \cdots & g_1 & 1 \end{bmatrix}$$

  Ker je $\mathbf{x}_i = \mathbf{z}_i \cdot \mathbf{G}$, so vse kodne zamenjave linearne kombinacije polinomov $g(p), p \cdot g(p), p^2 \cdot g(p), \ldots, p^{k-1} \cdot g(p)$. Kod dobljen s pomočjo $\mathbf{G}$ pa **ni sistematičen**. S prerazporeditvijo in z linearnimi operacijami nad vrsticami matrike $\mathbf{G}$ pa lahko določimo tudi **sistematični ciklični kod**.

- Za polinom $g(p)$ velja:

  $$p^n + 1 = g(p) \cdot h(p),$$

  kar pomeni, da je $p^n + 1$ deljiv z $g(p)$ brez ostanka (ker je $g(p)$ po definiciji polinom najnižje stopnje).

PRIMER 36:

Določite ciklični kod s pomočjo generatorskega polinoma:

$$g(p) = p^3 + p^2 + 1 \longrightarrow m = 3$$

Ustvarimo lahko ciklični kod $\mathcal{C}(7,4)$. Ustrezna matrika $\mathbf{G}$ je enaka:

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

Za vsak $\mathbf{z} \in \{0,1\}^k$ dobimo $\mathbf{x} \in \{0,1\}^n$ s pomočjo:

$$\mathbf{x}_{i_{(1\times n)}} \quad = \quad \mathbf{z}_{i_{(1\times k)}} \quad \cdot \quad \mathbf{G}_{(k\times n)}$$

◇

- Velja povezava med $h(p)$ in matriko za preverjanje sodosti $\mathbf{H}$ cikličnemu kodu $\mathcal{C}(n,k)$ enakovrednega koda. Iz $p^n + 1 = h(p) \cdot g(p)$ najprej izračunamo $h(p) = \frac{p^n+1}{g(p)}$, nato pa obrnemo smer zaporedja (od najmanjšega eksponenta do največjega) in z njim sestavimo matriko $\mathbf{H}$ (začenši s 1. vrstico, ki jo zamikamo v desno).

PRIMER 37:

Za ciklični kod, ki ga določa generatorski polinom $g(p)$, določite matriko za preverjanje sodosti $\mathbf{H}$ ekvivalentnemu kodu.

$$g(p) = p^3 + p^2 + 1; \qquad m = 3 \longrightarrow \mathcal{C}(7,4)$$
$$h(p) = (p^7 + 1) : p^3 + p^2 + 1 = p^4 + p^3 + p^2 + 1, \text{ost. } 0$$
$$h(p) = 1 + p^2 + p^3 + p^4$$

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

Zopet velja $\mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}$.

◇

7.3.2.1 Kodiranje cikličnih kodov

a) Kodiranje na osnovi množenja

$$x(p) = z(p) \cdot g(p) \mod (p^n + 1) \quad , \tag{7.1}$$

ki ne vodi k sistematinemu kodu.

b) Kodiranje na osnovi deljenja ustvari **sistematičen** kod.

Postopek:

- $z(p)$ množimo s p^m, m je stopnja generatorskega polinoma $g(p)$
- $p^m \cdot z(p)$ delimo z $g(p)$, in določimo ostanek:
  $p^m \cdot z(p) : g(p) = T(p) + \text{ost.}R(p)$
- Kod dobimo tako, da k $p^m \cdot z(p)$ prištejemo $R(p)$:
  $p^m \cdot z(p) + R(p) \equiv \text{kod}$

PRIMER 38:

$$z(p) = p^3 + p^2 + p$$
$$g(p) = p^3 + p + 1 \longrightarrow m = 3$$

Določite kod za $z(p)$?

$$p^3 \cdot z(p) = p^6 + p^5 + p^4 : p^3 + p + 1 = p^3 + p^2$$
$$\text{ost. } p^2$$

$$\begin{aligned} p^3 \cdot z(p) &\equiv 1110000 \\ R(p) &\equiv \quad\quad 100 \\ \hline \text{Kod } z(p) &\equiv 1110100 \end{aligned}$$

◇

7.3.2.2 Dekodiranje cikličnih kodov z detekcijo napak

Sprejeti vektor $\mathbf{y}$ delimo z $g(p)$; če je ostanek 0, ni napake $\longrightarrow \hat{\mathbf{x}} = \mathbf{y}$, sicer zahtevamo ponoven prenos.

PRIMER 39:

$$g(p) = p^3 + p + 1 \longrightarrow m = 3$$
$$y = 1010100 \longrightarrow y(p) = p^6 + p^4 + p^2$$

Ocenite poslani $\hat{\mathbf{x}}$!

$$
\begin{array}{ccccccccccccccc}
p^6 & + & p^4 & + & p^2 & : & p^3 & + & p & + & 1 & = & p^3 & + & 1 \\
p^6 & + & p^4 & + & p^3 & & & & & & & & & & \\
\hline
 & & & & p^3 & + & p^2 & & & & & & & & \\
 & & & & p^3 & & & + & p & + & 1 & & & & \\
\hline
 & & & & & & p^2 & + & p & + & 1 & \equiv & \text{ost} & \neq & 0
\end{array}
$$

Napaka, prenos je potrebno ponoviti!
◇

7.3.2.3 Dekodiranje cikličnih kodov z odkrivanjem in popravljanjem napak

Imamo ciklični kod $\mathcal{C}(n,k)$, ki smo ga dobili s pomočjo generatorskega polinoma $g(p)$.

Postopek:

1. Za sprejeti $\mathbf{y}$ določimo:

$$
\begin{aligned}
i &= 0 \\
s_i(p) &= \text{ost}\left\{\frac{y(p)}{g(p)}\right\}, \quad \text{ost} \equiv \text{ostanek pri deljenju.}
\end{aligned}
$$

2. Preverimo, ali je $\omega(\mathbf{s}_i) \leq e$ (ω je število enic v $\mathbf{s}_i$, e pa število napak, ki jih kod lahko popravi: $d_{min} = 2e+1 \longrightarrow \mathbf{H}$: matrika za preverjanje sodosti sistematičnega cikličnega koda)
   Če ni, gremo na 4, sicer gremo na 3.

3. Določimo: $e(p) = p^{n-i} \cdot s_i(p) mod(p^n+1)$ in $\hat{\mathbf{x}} = \mathbf{y} + \mathbf{e}$ (dekodiranje končano)

4. Postavimo: $i = i+1$ in preverimo, če je $i = n$. Če je, postopek ustavimo, ker ne moremo odpraviti napake. Če pa ni, gremo na 5.

5. Če je st $\{s_{i-1}(p)\} < n-k-1$, potem: $s_i(p) = ps_{i-1}$ in gremo na 2.
   Če pa je st $\{s_{i-1}(p)\} = n-k-1$, potem: $s_i(p) = ps_{i-1} - g(p)$ in gremo na 2.
   (st = stopnja polinoma)

6. konec postopka

PRIMER 40:

Dan je sistematičen ciklični kod $\mathcal{C}(7,4)$, ki smo ga zgradili z generatorskim polinomom $g(p) = p^3+p+1$, $d_{min} = 3$.
Na vhod v kanal smo poslali $\mathbf{x} = (1010011)$, na izhod pa smo dobili $\mathbf{y} = (1010001)$.

Odkrijte napako s postopkom dekodiranja!

Ad 1.) $s_0(p) = \text{ost}\left\{\frac{y(p)}{g(p)}\right\} = \text{ost}\left\{\frac{p^6+p^4+1}{p^3+p+1}\right\} = p$
$\mathbf{s}_0 = \underbrace{(010)}_{3}$, $m = 7 - 4 = 3$

Ad 2.) Ker je $\omega(\mathbf{s}_0) = 1 = e$ (izhaja iz $d_{min} = 3$), sledi:

Ad 3.) $e(p) = p^{7-0} \cdot s_0(p) = p^7 \cdot p = p^8 \bmod (p^7 + 1) = p$
$\mathbf{e} = (0000010)$
$\mathbf{x} = \mathbf{y} + \mathbf{e} = (1010001) + (0000010) = (1010011)$

$\diamond$

PRIMER 41:

Vzemimo, da smo prejeli $\mathbf{y} = (1011011)$. Kje je napaka sedaj?

Ad 1)

$$s_0(p) = \text{ost}\left\{\frac{y(p)}{g(p)}\right\} = \text{ost}\left\{\frac{p^6+p^4+p^3+p+1}{p^3+p+1}\right\} = p+1$$
$$\mathbf{s}_0 = (011) \equiv p+1$$

Ad 2) Ker je $\omega(\mathbf{s}_0) = 2 > e = 1$ in ker je $\text{st}(s_0(p)) = 1 < n-k-1 = 7-4-1 = 2$, dobimo:

Ad 4) $i = 1$

Ad 5) $s_1(p) = p \cdot s_0(p) \mod (p^n+1) = p\,(p+1) = p^2+p$

Ad 2) $\omega(\mathbf{s}_1) = 2 > e = 1$, $\text{st}(s_1(p)) = 2 = n-k-1$

Ad 4) $i = 2$

Ad 5) $s_2(p) = p \cdot s_1(p) - g(p) = p^2+p+1 \equiv (111)$

Ad 2) $\omega(\mathbf{s}_2) = 3 > e = 1$, $\text{st}(s_2(p)) = 2 = n-k-1$

Ad 4) $i = 3$

Ad 5) $s_3(p) = p \cdot s_2(p) - g(p) = p^2+1 \equiv (101)$

Ad 2) $\omega(\mathbf{s}_3) = 2 > e = 1$, $\text{st}(s_3(p)) = 2 = n-k-1$

Ad 4) $i = 4$

Ad 5) $s_4(p) = p \cdot s_3(p) - g(p) = 1$

Ad 2) $\omega(\mathbf{s}_4) = 1 = e$

Ad 3) $e(p) = p^{7-4} \cdot s_4(p) = p^3 \cdot 1 = p^3$
$\mathbf{e} = (0001000)$
$\mathbf{x} = \mathbf{y} + \mathbf{e} = (1011011) + (0001000) = (1010011)$

◇

- Za ciklični kod $\mathcal{C}(n,k)$ lahko z zgornjim postopkom dekodiranja z odkrivanjem napak odkrijemo:
  - da napake ni, če je ost $\left\{\frac{y(p)}{g(p)}\right\} = 0$
  - vsako enojno napako (ker je $p+1$ generatorski polinom, ki deli p^n+1 brez ostanka)
  - vsako razmestitev na dveh mestih, če je g(p) najmanj 2. stopnje
  - poljubno število lihih napak, če $g(p)$ vsebuje faktor $(p+1)$
  - vsak izbruh napak, če je dolžina izbruha krajša od stopnje $g(p)$, torej m
  - večji del daljših izbruhov, ker je $K \subset \{0,1\}^n$.

- Izbruh napake opišemo z: $e(p) = p^{i+1} \cdot b(p) \bmod (p^n + 1)$

  Na primer:

$$\mathbf{e} = (00000\overbrace{1011001}^{\text{izbruh}}000)$$
$$e(p) = p^3 \cdot \left(p^6 + p^4 + p^3 + 1\right) \bmod \left(p^{15} + 1\right)$$

7.3.2.4 Dekodiranje cikličnih kodov s popravljanjem izbruhov napak

- Pomembna je dolžina izbruha, ki je določena s prvim in zadnjim napačno sprejetim znakom v sprejetem vektorju (vmesni so lahko tudi pravilno sprejeti).

- S postopkom B lahko pri cikličnem kodu $\mathcal{C}(n, k)$ popravimo **izbruhe napak** do dolžine e, kjer je:

  $$e \leq \frac{n-k}{2} = \frac{m}{2}$$

  To pomeni, da v 2. koraku ne preverjamo več teže sindroma $\omega(\mathbf{s})$, temveč preverjamo, ali sindrom vsebuje izbruh napak dolžine, ki je $\leq e$.

PRIMER 42:

Dan je ciklični kod $\mathcal{C}(15, 9)$, zgrajen s pomočjo $g(p) = p^6 + p^3 + p^2 + p + 1$. Ker je $\frac{n-k}{2} = \frac{15-9}{2} = 3$, lahko kod popravi vse izbruhe napak do dolžine 3

Določite napako, če je $\mathbf{y} = (000001101110111)$.

$$s_0(p) = \text{ost}\left\{\frac{y(p)}{g(p)}\right\} = \text{ost}\left\{\frac{p^9 + p^8 + p^6 + p^5 + p^4 + p^2 + p + 1}{p^6 + p^3 + p^2 + p + 1}\right\} = p^5 + p^4 + p + 1$$
$$\mathbf{s}_0 = (110011) \text{ - s cikliranjem dobimo 4 enice skupaj, kar pomeni izbruh dolžine 4}$$

Ker je 4 (dolžina izbruha) $> e = 3$, računamo sindrom z dolžino izbruha 3 ali manj.
Pri indeksu $i = 9$, dobimo $\mathbf{s}_9 = (000101)$, ki ima dolžino izbruha 3. Tedaj je:

$$\begin{aligned} e(p) &= p^{n-i} \cdot s_i(p) = p^{15-9} \cdot s_9(p) \\ &= p^6 \cdot \left(p^2 + 1\right) = p^8 + p^6 \\ \mathbf{e} &= (000000101000000) \\ \mathbf{x} &= \mathbf{y} + \mathbf{e} = (000001000110111) \end{aligned}$$

◇

7.4 LFSR kodirnik/dekodirnik cikličnih kodov

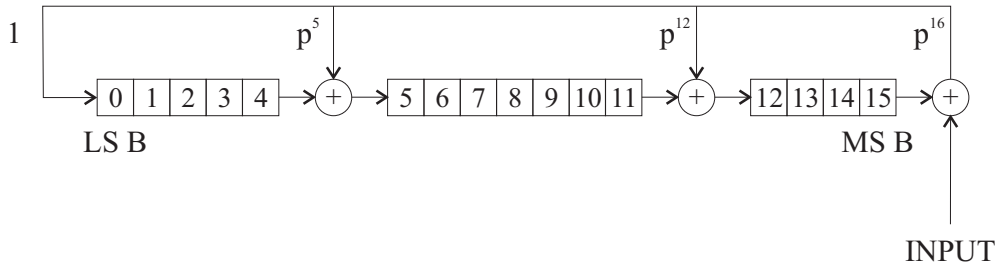
- LFSR (*ang.* Linear Feedback Shift Register) je implementacija konvolucijskega koda.
- Generiranje kodne zamenjave bazira na že znanem postopku (str. 60):

  $$p^m \cdot z(p) + R(p) \equiv \text{kodna zamenjava}$$

- LFSR je linearno sekvenčno vezje, ki na oddajni strani izračuna $R(p)$ na osnovi $z(p)$, na sprejemni strani pa se preverjanje $(p^m \cdot z(p) + R(p))$ ponovi. Struktura LFSR izhaja iz generatorskega polinoma $g(p)$. Če je na sprejemni strani ob koncu v registru 0, ni napake. Sicer sledi zahteva za ponovitev prenosa.

  Zaradi povratnih vezav je stanje registra odvisno od dolge zgodovine podatkov, zato dobro detektira tudi izbruhe napak do dolžine, ki jo določa stopnja $g(p)$.

  LFSR za $g(p) = p^{16} + p^{12} + p^5 + 1$ (CRC-CCITT standard):

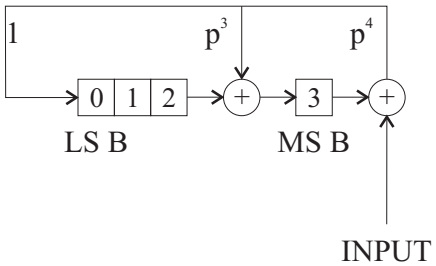


  CRC $\equiv$ Cyclic Redundancy Check

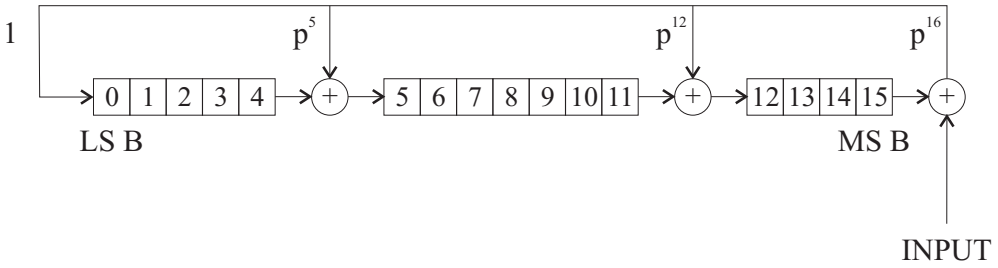
PRIMER 43:

Narišite LFSR za a) $g(p) = p^4 + p^3 + 1$ in b) $g(p) = p^{16} + p^{12} + p^5 + 1$:

a)



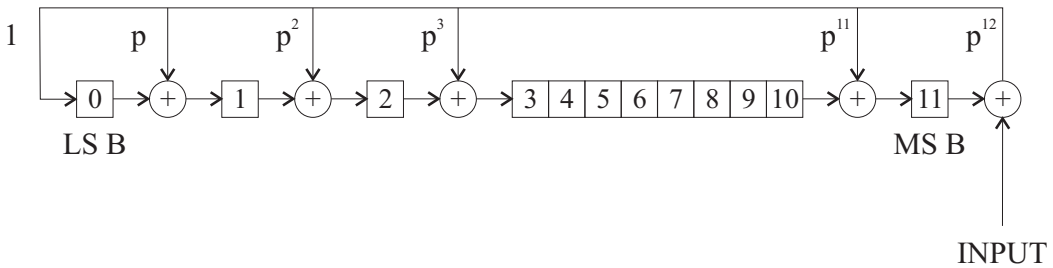
b)



◇

PRIMER 44:

S CRC metodo in LFSR pokažite kodiranje podatka $\mathbf{z} = (100000000000)$, če je $g(p) = p^{12} + p^{11} + p^3 + p^2 + p + 1$ (CRC-12).



št. premika				začetno stanje registra	MSB	
start	0	0	0	0 0 0 0 0 0 0 0	0	1
					1	
1	1	1	1	1 0 0 0 0 0 0 0	1	1
					0	
2	1	0	0	0 1 0 0 0 0 0 0	1	1
					0	
3	1	0	1	1 0 1 0 0 0 0 0	1	1
					0	
4	1	0	1	0 1 0 1 0 0 0 0	1	1
					0	
5	1	0	1	0 0 1 0 1 0 0 0	1	1
					0	
6	1	0	1	0 0 0 1 0 1 0 0	1	1
					0	
7	1	0	1	0 0 0 0 1 0 1 0	1	1
					0	
8	1	0	1	0 0 0 0 0 1 0 1	1	1
					0	
9	1	0	1	0 0 0 0 0 0 1 0	0	0
					0	
10	0	1	0	1 0 0 0 0 0 0 1	0	0
					0	
11	0	0	1	0 1 0 0 0 0 0 0	1	1
					0	
12	1	1	1	0 0 1 0 0 0 0 0	1	LSB
	LSB			R(p)	MSB	

Do istega rezultata pridemo lahko tudi po analitični poti z:

$$\begin{aligned} p^m \cdot z(p) : g(p) &= p^{12} \cdot p^{11} = p^{23} : g(p) \\ &= p^{23} : p^{12} + p^{11} + p^3 + p^2 + p + 1 \\ &= p^{11} + p^{10} + p^9 + p^8 + p^7 + p^6 + p^5 + p^4 + p^3 + 1 \\ \text{ostanek} &= p^{11} + p^5 + p^2 + p + 1 = R(p) \end{aligned}$$

◇

Poglavje 8

Kriptologija

8.1 Kriptografija in kriptoanaliza

Beseda kriptologija izhaja iz grških besed 'kruptos' in 'logos', kar pomeni študij skrivanja. Zato se ukvarja med drugim z razvojem metod za šifriranje in dešifriranje sporočil.
V preteklosti je bila zaščita sporočil v domeni vojske in diplomacije, danes pa se širi v vsakodnevno življenje. N.pr. uporabnik kabelske televizije naj sprejema le tiste programe, za katere plačuje najemnino. To je mogoče izvesti le, če je slika šifrirana in če vsak sprejemnik vsebuje napravo za dešifriranje slike. Naslednji primer je elektronsko bančništvo, ki tudi ni mogoče brez kriptologije. Magnetne kartice, bančni prenosi za denarne transakcije, itd. uporabljajo kriptografska orodja.
Vedno več je podatkov, za katere se pričakuje, da so privatne narave, n.pr. medicinski podatki, osebni podatki o kazenskih prekrških, itd. Za mnoge od njih je zaželeno, da so zaščiteni pred neželenimi uporabniki.
V okviru kriptologije obstaja razlika med dvema disciplinama, t.j. med kriptografijo in kriptoanalizo. Prva se ukvarja s študijo in razvojem metod in metodologij za šifriranje, kjer se običajno uporabljajo skrivni ključi, s katerimi je mogoče dešifrirati šifrirano sporočilo ali informacijo. Druga pa išče ozr. razvija tehnike za dešifriranje šifriranih sporočil, brez apriornega poznavanja ključa.
V tem poglavju se bomo omejili le na osnovne pojme iz kriptologije in predvsem osvetlili tiste aspekte kriptografije in kriptoanalize, kjer je poudarek na uporabi konceptov iz informacijske teorije.

8.2 Splošna shema šifrirnih sistemov

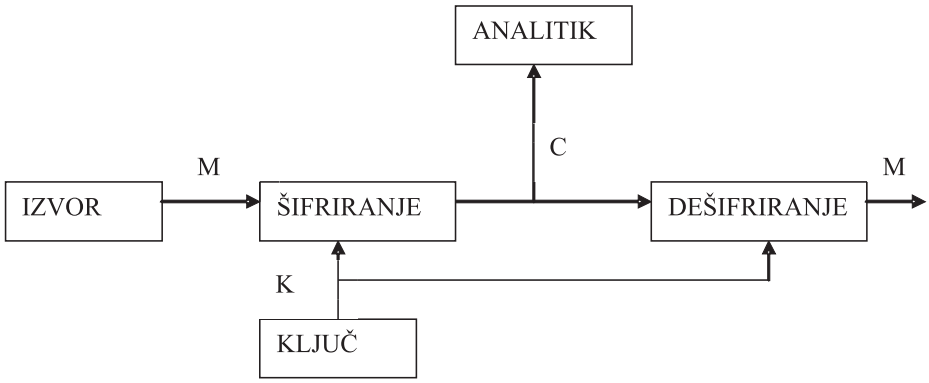
Slika 8.1 prikazuje osnovno idejo šifrirnega sistema. Izvor, ki generira sporočilo M (Message) kot običajni tekst, se nahaja na strani oddajnika. Čisti tekst M se transformira v šifrirani tekst C s pomočjo določene metode šifriranja. Šifrirna operacija je v bistvu transformacija T, ki pretvori M v C na osnovi ključa K:

$$C = T_K(M)$$

Dešifriranje poteka na sprejemni strani s procesiranjem sprejetega teksta C in z uporabo inverzne transformacije T^{-1} in ključa K:

$$M = T_K^{-1}(C)$$

Pri tem se običajno predpostavlja, da je transformacija T poznana, ključ K pa ne.



Slika 8.1: Shema šifirnega sistema

Kriptoanalitik ima nalogo, da ali odkrije ključ iz šifriranega teksta C ali pa odkrije čisti tekst M direktno. V nadaljevanju bomo predpostavljali, da je ključ različen za vsako novo sporočilo. To pomeni, da lahko čisti tekst, šifrirani tekst in ključ obravnavamo kot stohastične veličine. Na ta način lahko napravimo povezavo z informacijsko teorijo.
Ločujemo tri tipe kriptoanalitičnih napadov na kriptirne sisteme, glede na naravo informacije, do katere ima kriptoanalitik dostop:

A Napad s šifriranim tekstom

B Napad s čistim tekstom

C Napad z izbranim čistim tekstom

V slučaju A mora kriptoanalitik poizkusiti dešifrirati čisti tekst z analizo strukture in možnih statističnih lastnosti, ki so v šifriranem tekstu ali, kar je še pomembneje, najti ključ.
Če je na razpolago poleg šifriranega teksta še informacija o čistem tekstu (slučaj B), je situacija bolj ugodna. S kombinacijami med šifriranim in čistim tekstom se poizkuša dešifrirati tisti del šifriranega teksta, za katerega ustrezni čisti tekst ni poznan. Tak slučaj nastopi, ko je kriptoanalitik uspel vdreti v kriptirni sistem ali k uporabniku sistema. Primer: avtomatski monetarni promet, kjer mora vsako transakcijo spremljati podatek o pošiljatelju in o banki, kamor se denar prenaša. Če analitik odkrije, kje se znotraj šifriranega teksta nahaja informacija o banki, transakcijskem računu itd, lahko poizkusi dešifrirati ostanek šifriranega teksta na osnovi tega znanja.
Najugodnejša situacija za kriptoanalitika je C, ko lahko sam izbere čisti tekst in ga primerja s šifriranim tekstom.
Sistem, ki je odporen proti napadu A, ni nujno odporen proti napadu C. V praksi je sistem, ki je odporen proti napadu C, bolj cenjen kot sistem, ki je odporen proti napadu A, saj se tako obranimo večjega števila napadov zaradi lažjega dešifriranja.
Aplikacije, kjer se uporablja kriptografija, delimo v dve grupi, na aplikacije v zvezi s pomnilnikom in aplikacije v zvezi s prenosom. V prvem primeru gre za zaščito podatkov v pomnilniku (n.pr. na disku, magnetnem traku), za katere se predpostavlja, da so shranjeni za daljši čas. V drugem primeru (telefon, TV) je šifrirano sporočilo dosegljivo le kratek čas v času prenosa. Tudi informacija o čistem sporočilu ima zato pomen le kratek čas (n.pr. novice, vreme).

8.3 Šifrirni sistemi

Razlikujemo dve osnovni šifrirni metodi:

- tokovno šifriranje
- bločno šifriranje

Pri tokovnem šifriranju se predpostavlja, da sporočilo nastaja z zaporednimi sekvencami prostih elementov, ki so ali črke ali binarni (ASCII) znaki. Tekst se tukaj šifrira element za elementom. Pri bločnem šifriranju se vzame določeno število elementov (blok) skupaj in šifrira kot ena celota. Primer bločnega šifriranja je DES (Data Encryption Standard) algoritem (IBM, 1968-1975). DES je še vedno eden najbolj uporabljenih algoritmov za bločno šifriranje. DES predpostavlja binarne podatke in ima blok dolžine 64 bitov. Tudi ključ je dolžine 64 bitov, pri čemer je uporabljenih le 56 bitov. Število ključev je tako reda $7{,}2 \times 10^{16} \approx 2^{64}$.
Pri blokovnem šifriranju se uporabljata dva glavna sistema: transpozicija in substitucija. Uporabljala sta se do II. svetovne vojne, danes se uporabljata le še kot gradnika kompleksnejših metod. Moderni kriptografski algoritmi kot je n.pr. DES so v bistvu serija transpozicij in substitucij. Pri transpozicijskem šifriranju so simboli ohranjeni, njihova sekvenca pa se spremeni (določa jo ključ). Pri substitucijskem šifriranju pa se sekvenca ne spremeni, spremenijo pa se simboli.

8.3.1 Transpozicijske šifre

PRIMER 45:

V šifriranem tekstu je vrstni red simbolov v bloku tak, kot ga določa ključ, v tem primeru (3 2 5 1 4)

Čisti tekst:	the invasion will begin
Delitev v bloke:	thein vasio nwill begin
Šifrirani tekst:	ehnti saovi iwlnl genbi

Takšno šifriranje si lahko predstavljamo kot transpozicija v okviru posameznih blokov ozr. transpozicija stolpcev, če si bloke zapišemo enega pod drugim:

Zapis blokov v stolpce:	Uporaba ključa (3 2 5 1 4):
thein	ehnti
vasio	saovi
nwill	iwlnl
begin	genbi

◇

Sedaj je mogoče opisati transpozicijsko šifriranje bolj splošno. Pri dolžini bloka T je celotno število ključev enako $T!$, oziroma $T! - 1$, ker en ključ (1 2 3 ...) ponovi čisti tekst. V praksi je problem hitro rešen, če poznamo dolžino bloka, še posebej z uporabo računalnika. Težava nastopi pri obsežnih sporočilih in ekstremno dolgih blokih.
Problemi s transpozicijskimi šiframi so dvojne narave: prva je, kako ugotoviti dolžino bloka. Tukaj se uporablja izraz: $L = n \cdot T$, kjer je L dolžina sporočila, vendar je treba paziti še na eventuelne 'dummy' ozr. prazne simbole. Drugi problem pa je nato poiskati ključ

ne da bi preizkusili vseh kombinacij ('brute-force'). Če je čisti tekst v naravnem jeziku, potem je mogoče uporabiti znanje o jeziku, n.pr. frekvenco posameznih črk ali parov črk. Z izenačenjem simbolov določene frekvence iz šifriranega teksta s črkami abecede je mogoče poiskati povezavo med črkami osnovnega in šifriranega teksta.

8.3.2 Substitucijske šifre

Tukaj so simboli v čistem tekstu zamenjani z drugimi simboli. V splošnem opisujemo simbole čistega teksta z abecedo $A = (a_1, \ldots, a_{25})$ in simbole šifriranega teksta z abecedo $B = (b_1, \ldots, b_{25})$. Šifriranje sedaj omogoča povezava med simboli obeh abeced, n.pr.:

Čisti tekst:	$a_3, a_{23}, a_9, a_{17}, a_4$
Šifrirani tekst:	$b_3, b_{23}, b_9, b_{17}, b_4$

PRIMER 46:

Ena od najbolj znanih in enostavnih substitucij je Cezarjeva substitucija (po Juliju Cezarju), ki ima za abecedo B zamaknjeno abecedo A. N.pr. pri zamiku 3 dobimo:

abeceda A	a b c d e f ...
abeceda B	d e f g h i ...

Če zgornjo substitucijo uporabimo na prejšnjem zgledu, dobimo naslednji šifrirani tekst:

Čisti tekst:	the invasion will begin
Šifrirani tekst:	wkh lqydvlrq zloo ehjlq

◇

Pri tem je bila za abecedo A uporabljena angleška abeceda s 26 znaki. Za Cezarjevo substitucijo je karakteristično, da ostane abeceda ista. Število ključev je pri tem omejeno s številom črk, zato je dešifriranje enostavno. Dovolj je, da poznamo substitucijo za eno črko in že poznamo ključ. Takšno črko je mogoče hitro najti, če je le šifrirani tekst dovolj dolg. Potrebno je le poiskati črko z največjo frekvenco in jo izenačiti z najpogostejšo črko v čistem tekstu (za angleški tekst je to črka e).
Če so črke v abecedi B v poljubnem redu, potem postane število ključev precej večje, namreč 26!.

PRIMER 47:

abeceda A:	a b c d e f g h i j k l m n o p q r s t u v w x y z
abeceda B:	e s t v f u z g y x b h k w c i r j a l m p d q o n
Čisti tekst:	the invasion will begin
Šifrirani tekst:	lgf ywpeaycw dyhh sfzyw

◇

Kljub 26! možnih ključev je mogoče relativni enostavno rešiti takšen problem. Razlog je v znanih frekvencah črk naravnega jezika in v redundancah jezika. Zato se pri šifriranju uporablja več kot ena substitucija. Tedaj govorimo o polialfabetni substituciji. Primer takšne substitucije je Vigener-jev sistem, kjer je uporabljenih več Cezarjevih substitucij. Prva črka v čistem tekstu je zamaknjena n.pr. za 20 mest, druga za 17, itd. Pri takšnem šifriranju je ugodno uporabljati t.im. Vigener-jevo tabelo, ki podaja osnovno abecedo A kot prvo vrstico v tabeli, sledijo pa ji vrstice z zamiki 1, 2, 3, ... Število vrstic v tabeli je tako enako 26. Šifriranje se izvaja s pomočjo t.im. ključnega teksta, ki pove, kako izvesti substitucijo. Ključni tekst je enake dolžine kot čisti tekst. Zapišemo ga pod čisti tekst. Nato po vrsti preko celega teksta vzamemo črki iz čistega in ključnega teksta, ter v Vigener-jevi tabeli poiščemo presek stolpca (določa ga črka iz čistega teksta) in vrstice (določa jo črka ključnega teksta), ki določa črko v šifriranem tekstu.

PRIMER 48:

Čisti tekst:	the invasion will begin
Ključ:	rad ioradior adio radio
Šifrirani tekst:	khh qbmavqce wltz sejqb

◇

V tem primeru so karakteristike jezika veliko bolje skrite kot prej. V zgornjem primeru je ključni tekst sestavljen iz ponavljajoče ključne besede dolžine 5 (radio), kar pomeni, da smo iz Vigenerj-eve tabele uporabili 5 substitucij. Zato poznavanje dolžine ključne besede zelo pomaga pri dešifriranju. Oziroma povedano drugače, pri dobrem šifriranju je zaželena uporaba čim daljše ključne besede ozr. teksta. N.pr. ključni tekst je lahko sestavljen iz ključne besede, ki ji sledijo besede iz čistega teksta.
Pomembno pri šifriranju je prikriti karakteristike čistega teksta ozr. jezika v katerem je napisan, kar lahko dosežemo z izenačitvijo pogostosti znakov v šifriranem tekstu. Tedaj moramo najprej šifrirati črke čistega teksta n.pr. z Huffmanovo metodo, zatem pa uporabimo transpozicijsko ali substitucijsko metodo. Tedaj bodo imeli vsi kodni simboli enako verjetnost pojavljanja v šifriranem tekstu.

8.4 Informacija sporočil in varnost

Ker je varnost sporočil pomembna, nas bo v nadaljevanju zanimalo, kako varen je kriptirni sistem. Na to vprašanje bomo poizkušali odgovoriti s pomočjo informacijske teorije.
Če si predstavljamo sporočila v čistem tekstu kot elemente množice vseh možnih sporočil, ki imajo vsako svojo verjetnost, da jih vir generira, potem lahko govorimo o obsegu informacije v čistem tekstu, ki je definiran z enačbo:

$$H(M) = -\sum_{i=1}^{n} p(M_i) \log p(M_i)$$

kjer je $p(M_i)$ verjetnost, da se v čistem tekstu pojavi sporočilo M_i. Podobno govorimo lahko o obsegu informacije v šifriranem tekstu $H(C)$ in o obsegu informacije v ključu $H(K)$.
Analogno kot v prejšnjih poglavjih lahko govorimo tudi o pogojnem obsegu informacije. N.pr. $H(K|C)$ je obseg informacije ali nedoločenosti o ključu, če poznamo šifrirani tekst C, kar imenujemo tudi dvoumnost ključa. Podaja jo izraz:

$$H(K|C) = -\sum_{h=1}^{l}\sum_{j=1}^{m} p(K_h, C_j)\log p(K_h|C_j)$$

kjer so K_h ključi, C_j pa možni kriptogrami. Podobno bi z $H(M|C)$ opisali obseg informacije ozr. nedoločenost čistega teksta M pri danem šifriranem tekstu C in slednje poimenovali tudi z dvoumnostjo sporočila. $H(M|C,K)$ pa je nedoločenost čistega teksta pri znanem ključu in šifriranem tekstu.
Ker je M nedvoumno določljiv iz K in C, velja:

$$H(M|C,K) = 0$$

Nadalje je $H(K|M,C)$ nedoločenost ključa pri znanih M in C. V zvezi z njo velja naslednji teorem.

Teorem 8.1

$$H(K|M,C) = H(K|C) - H(M|C)$$

Dokaz:
Zaradi vezane entropije:

$$\begin{aligned} H(M,C,K) &= H(M|C,K) + H(C,K) = H(M|C,K) + H(K|C) + H(C) \\ &= H(K|M,C) + H(M,C) = H(K|M,C) + H(M|C) + H(C) \end{aligned}$$

sledi:

$$H(M|C,K) + H(K|C) = H(K|M,C) + H(M|C)$$

Ker je prvi izraz na levi enak 0, dobimo po preureditvi zgornji teorem.
Uporabnik si seveda želi čim večjo nedoločenost ključa glede na M in C. To lahko doseže z majhno nedoločenostjo čistega teksta na osnovi šifriranega, kar pa pomeni tudi, da nam šifrirani tekst pove veliko o čistem tekstu. Slednje pomeni, da večja nedoločenost ključa pomeni manjšo nedoločenost čistega teksta in obratno.
Od tod sledijo še naslednje ugotovitve. Ker je po definiciji:

$$I(M;C) = H(M) - H(M|C) = H(C) - H(C|M)$$

in ker želimo čim manjšo $I(M;C)$, mora biti $H(M|C)$ čim bližja $H(M)$.
Kriptirni sistem je absolutno varen, če velja $I(M;C) = 0$.

Teorem 8.2

$$I(M;C) \quad \geq \quad H(M) - H(K)$$

Dokaz: Iz Teorema 8.1. zaradi $H(K|M,C) \geq 0$ sledi

$$H(K|C) \geq H(M|C)$$

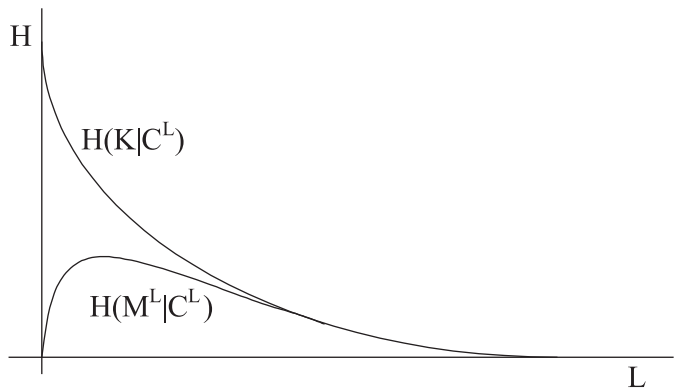
Ker je po definiciji $H(K) \geq H(K|C)$, sledi iz zgornje neenačbe še bolj:

$$H(K) \geq H(M|C)$$

Če ta izraz uporabimo v definiciji za $I(M;C)$, dobimo ravno Teorem 8.2. Ta pravi, da ključi z malo informacije v povprečju ozr. z majhno entropijo, omogočajo veliko povprečno medsebojno informacijo $I(M;C)$. Absolutno varnost ($I(M;C) = 0$) je mogoče doseči le z:

$$H(K) \geq H(M),$$

ozr. informacija v ključu mora biti vsaj tako velika kot informacija v čistem tekstu.
Do sedaj nismo upoštevali dolžine šifriranega teksta, čeprav je bistvena pri dešifriranju. N.pr. pri naravnem jeziku imajo znaki svoje značilnosti (frekvence), ki pa jih odkrijemo le, če imamo dovolj teksta na razpolago.
Če označimo šifrirani tekst dolžine L s C^L, potem se nedoločenost ključa $H(K|C^L)$ zmanjšuje z večanjem L (slika8.2). Podobno velja za $H(M^L|C^L)$, vendar z razliko, da je tukaj pri majhnih L tudi število sporočil majhno in pri povečanju L narašča število sporočil in zato tudi nedoločenost sporočil pri znanem C^L. Vendar pride pri določenem L do obrata, saj tedaj šifrirani tekst vsebuje dovolj informacije, da ustavi naraščanje števila najbolj verjetnih sporočil. Od tedaj dalje se z večanjem L zmanjšujeta obe nedoločenosti (ključa in čistega teksta) enako, saj C^L vsebuje vso informacijo za določitev ključa in posledično za določitev čistega teksta.



Slika 8.2: $H(K|C^L)$ in $H(M^L|C^L)$ kot funkciji L.

Teorem 8.3: Vzemimo, da pomeni ε število različnih simbolov v sporočilu ali šifriranem tekstu dolžine L. Tedaj velja:

$$H(K|C^L) \geq H(K) - D_L,$$

kjer je D_L absolutna redundanca, ki je definirana z:

$$D_L = L\log(\varepsilon) - H(M^L)$$

Dokaz:
Zaradi nedvoumne zveze med čistim tekstom M in šifriranim tekstom C velja vedno:

$$H(K, C^L) = H(K, M^L)$$

Ob predpostavki, da je ključ neodvisen od izvora sporočila, pa je:

$$\begin{aligned} H(K|C^L) &= H(K, C^L) - H(C^L) \\ &= H(K, M^L) - H(C^L) \\ &= H(K) + H(M^L) - H(C^L) \end{aligned}$$

Ker je ε število različnih simbolov v sporočilu ali šifriarnem tekstu, obstaja ε^L možnih sporočil ali kriptogramov dolžine L. Zaradi lastnosti entropije (zgornja vrednost) velja:

$$H(C^L) \leq L \log(\varepsilon)$$

Če to lastnost vstavimo v enačbo zgoraj, dobimo:

$$H(K|C^L) \geq H(K) + H(M^L) - L \log(\varepsilon)$$

Zadnja člena pa lahko izenačimo z $(-D_L)$ in tako dobimo izraz, ki ga podaja Teorem 8.3. Absolutno redundanco D_L lahko gledamo kot mero za obseg, do katerega se aktualno sporočilo razlikuje od izvora, kjer ima vsako sporočilo enako verjetnost, da se pojavi.
Teorem 8.3. v bistvu pove, da če redundanca narašča, potem nedoločenost ključa v povprečju pada. To pomeni, da zmanjševanje redundanc poveča varnost kriptirnega sistema. Dokler velja $H(K) > D_L$, je nedoločenost ključa pri znanem šifriranem tekstu $H(K|C^L)$ večja od nič in zato v povprečju ni mogoče nedvoumno določiti ključa.

Podobno ključa ne moremo določiti tudi v primeru, ko je šifrirano sporočilo kratko. Če predpostavimo, da so sosednji znaki med seboj neodvisni (vir brez spomina), potem velja

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

in zgornja neenakost postane

$$H(K|C^L) \geq H(K) + L[H(M) - \log \varepsilon] \ .$$

Kadar je nedoločenost ključa pri znanem šifriranem tekstu $H(K|C^L)$ enaka 0, pomeni, da na podlagi šifriranega sporočila lahko izluščimo ključ. Pogoj

$$0 \geq H(K) + L[H(M) - \log \varepsilon]$$

lahko preoblikujemo v

$$L \geq \frac{H(K)}{\log \varepsilon - H(M)} \ .$$

Z drugimi besedami, manjša kot je nedoločenost vira $H(M) \in [0, \log \varepsilon]$, krajši šifrirani tekst (L) potrebujemo, da odkrijemo ključ. Zato je smiselno poskrbeti, da je nedoločenost vira kar največja, na primer s kodiranjem vira informacije pred šifriranjem.

Minimalno dolžino šifriranega teksta L, ki zadosti zgornji neenačbi, imenujemo odpornost šifrirnega sistema

$$L_O = \frac{H(K)}{\log \varepsilon - H(M)}$$

in jo razumemo kot dolžino šifriranega teksta, v povprečju potrebno za razvozlanje ključa.

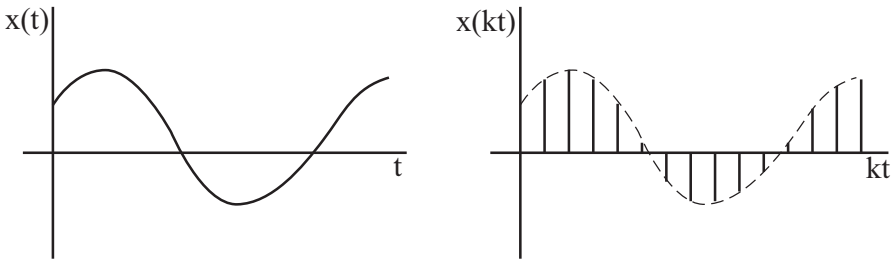
Poglavje 9

Signali in sistemi

9.1 Signali

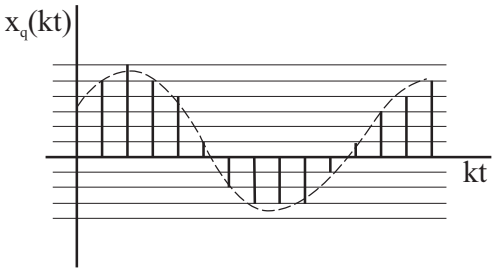
- Osnovne oznake:

  $x(t)$ – signal zvezne spremenljivke t (**analogni signali**)
  $x(kT)$ – diskretni signal, $t = kT, k =$ celo število, $T =$ perioda
  $\equiv x(k), x_k$



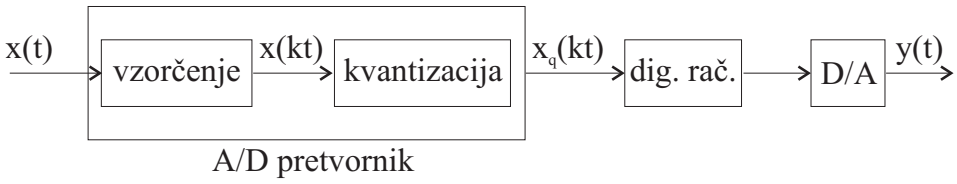
- Pri vnosu amplitud v digitalni računalnik imamo na voljo omejeno število bitov, zato je natančnost opisa signala omejena - govorimo o amplitudni kvantizaciji.

- Diskretni kvantiziran signal je **digitalni signal**: $x_q(kT)$.



- Način uporabe dig. računalnika:

  Običajno se ne dela razlika med diskretnim in digitalnim signalom (zaradi dovolj široke besede v računalniku).



- Signale nadalje delimo na **periodične** in **aperiodične**.

$x(t+T_p) = x(t)$	- zvezni periodični signal
$x\left[(k+N)T\right] = x(kT)$	- diskretni periodični signal
$x_q\left[(k+N)T\right] = x_q(kT)$	- digitalni periodični signal,

kjer je:

N celo število in
T_p poljubna konstanta.

- Ločimo tudi med **determinističnimi** in **naključnimi** signali.
  Amplituda naključnega signala je opisljiva z verjetnostno porazdelitvijo.

- Signali so lahko še:
  - časovno **pozitivni** (kavzalni), pri $t < 0$ oz $k < 0$ imajo vrednost 0;
  - časovno **negativni**, pri $t > 0$ oz $k > 0$ imajo vrednost 0;
  - **dvostranski** signali

9.2 Elementarni signali

9.2.1 Enotina impulzna funkcija

Enotina impulzna funkcija ali Diracova delta funkcija $\delta(t)$ (*ang.* Unit impulse function)je definirana z:

$$\int_{-\infty}^{+\infty} f(t)\delta(t)dt = f(0),$$

kjer je $f(t)$ poljubna funkcija, zvezna v izhodišču.

- Predstavljamo si jo, kot da ima povsod vrednost 0, razen v $t = 0$, kjer ima vrednost ∞ :

$$\delta(t) = \begin{cases} \infty & t = 0 \\ 0 & \text{sicer} \end{cases}$$

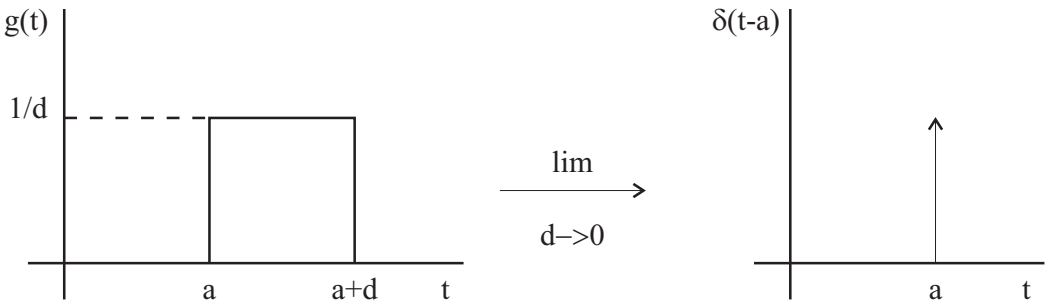
- Če spremenimo izhodišče, velja:

$$\int_{-\infty}^{+\infty} f(t)\ \delta(t-a)\ dt = f(a), \quad a \equiv \text{konstanta}$$

- Z enotino impulzno funkcijo lahko vzorčimo (sempliramo) poljubno funkcijo $f(t)$. Velja:

$$\int_{-\infty}^{+\infty} \delta(t-a)\ dt = \int_{a_-}^{a_+} \delta(t-a)\ dt = 1, \quad a_-, a_+ \text{ sta okolici } a$$

- $\delta(t-a)$ je limitna vrednost funkcije $g(t)$, ko se d približuje k 0:



$$g(t) = \begin{cases} \frac{1}{d} & , a \leq t \leq a+d \\ 0 & , \text{sicer} \end{cases}$$

Ploščina je 1 tudi po limitnem procesu - zato jo imenujemo **enotin impulz**.

9.2.2 Enotin pulz

Enotin pulz ali Kroneckerjeva delta funckcija (*ang.* unit pulse function) je diskretna varianta enotine impulzne funkcije:

$$\delta(k) = \begin{cases} 1 & , k = 0 \\ 0 & , k \neq 0 \end{cases}$$

oz.

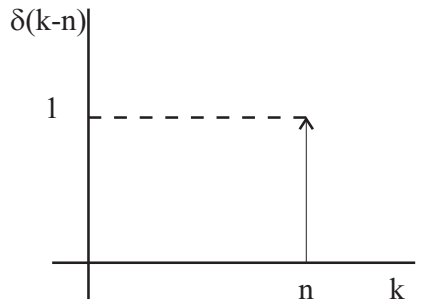
$$\delta(k-n) = \begin{cases} 1 & , k = n \\ 0 & , k \neq n \end{cases}$$

kjer sta k in n celi števili

- Za poljubno diskretno funkcijo $f(k)$ velja:

$$\sum_{k=-\infty}^{+\infty} f(k)\ \delta(k-n) = f(n)$$

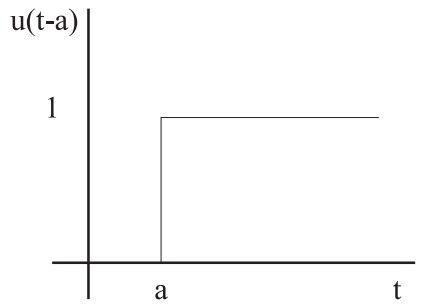
Tudi $\delta(k)$ ima semplirno značilnost.



9.2.3 Enotina stopničasta funkcija

- Enotina stopničasta funkcija (*ang.* unit step function) je definirana z:

$$u(t-a) = \begin{cases} 1 & , \ t \geq a \\ 0 & , \ t < a \end{cases} \quad (a \text{ je realna konstanta})$$



- Če zvezno funkcijo $f(t)$ množimo z $u(t-a)$, dobimo:

$$g(t) = f(t) \cdot u(t-a) = \begin{cases} f(t) & , \ t \geq a \\ 0 & , \ t < a \end{cases}$$

- Razlika med $u(t-a)$ in $u(t-b)$, $b > 0$, je impulz širine $(b-a)$:

$$p(t) = u(t-a) - u(t-b) = \begin{cases} 1 & , \ a \leq t < b \\ 0 & , \ \text{sicer} \end{cases}$$

- Če množimo $f(t)$ s $p(t)$, dobimo:

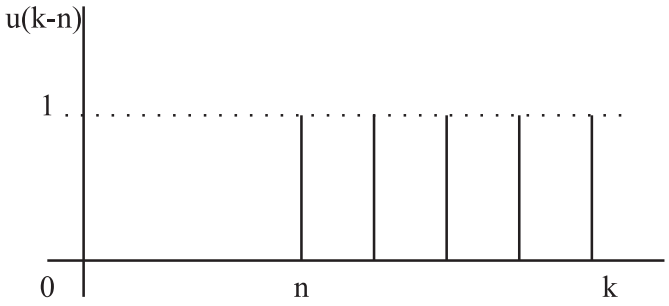
$$g(t) = f(t) \cdot p(t) = \begin{cases} f(t) & , \ a \leq t < b \\ 0 & , \ \text{sicer} \end{cases}$$

  Dobimo "okno", v katerem je funkcija enaka $f(t)$, širina okna pa je $(b-a)$.

9.2.4 Enotina stopničasta sekvenca

- Enotina stopničasta sekvenca (*ang.* unit step sequence) je definirana z:

$$u(k-n) = \begin{cases} 1 & , k \geq n \quad k, n \text{ sta celi števili} \\ 0 & , k < n \quad (n \text{ je lahko tudi neg.}) \end{cases}$$



- Enotin pulz in enolična stopničasta sekvenca sta povezani z izrazom:

$$\sum_{j=n}^{\infty} \delta(k-j) = u(k-n)$$

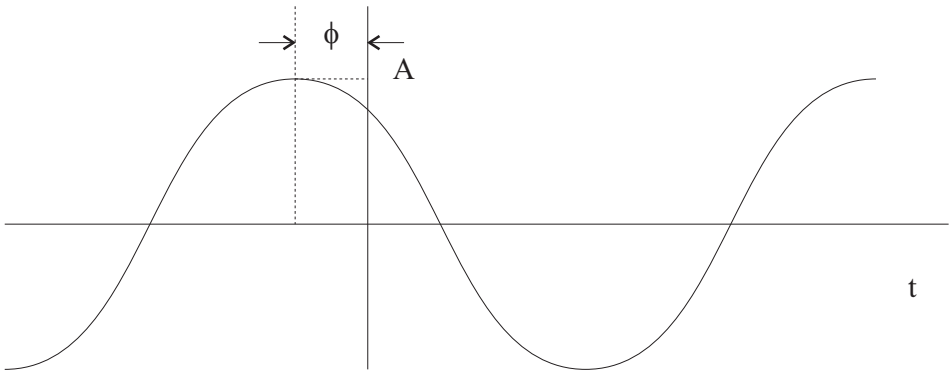
in

$$\delta(k-n) = u(k-n) - u(k-n-1)$$

9.2.5 Sinusoidni signal

- Sinusoidni signal (*ang.* sinusoidal signal) je definiran z izrazom:

$$x(t) = A \cdot \cos(\omega t + \phi)$$



- Kompleksni sinusoid $e^{j\omega t}$ omogoča zapis:

$$x(t) = Re\left\{A \cdot \exp\left[j(\omega t + \phi)\right]\right\}$$

Veljajo Eulerjeve enačbe:

$$\cos x = \frac{1}{2}(e^{jx} + e^{-jx})$$
$$\sin x = \frac{1}{2j}(e^{jx} - e^{-jx})$$

kjer je:

$$
\begin{aligned}
f &= \frac{\omega}{2\pi} \\
T_p &= \frac{1}{f} = \frac{2\pi}{\omega} \\
e^{j\varphi} &= \cos\varphi + j\sin\varphi
\end{aligned}
$$

- Diskretni sinusoid je:

$$x(k) = A \cdot \cos(\omega k + \phi)$$

oz.

$$x(kT) = A \cdot \cos(\omega kT + \phi)$$

oz.

$$x(k) = Re\left\{A \cdot \exp\left[j(\omega kT + \phi)\right]\right\}$$

9.3 Sistemi

- Sistemi spreminjajo vhodne signale v izhodne:

$$y(t) = \chi\{x(t)\} \quad \text{- za zvezne signale}$$

in

$$y(k) = \chi\{x(k)\} \quad \text{- za diskretne signale}$$

V nadaljevanju se bomo predvsem ukvarjali z **diskretnimi sistemi**.

- Primeri različnih diskretnih sistemov:
  - Linearni diskretni sistem: $y(k) = K \cdot x(k)$
  - Kvadratni diskretni sistem: $y(k) = K \cdot x^2(k)$
  - Diferenčna enačba: $y(k) = B_0 \cdot x(k) + B_1 \cdot x(k-1) + B_2 \cdot x(k-2)$
    B_i so lahko konstante ali časovno spremenljivi parametri.

- Sistem je **linearen**, če velja:

$$
\begin{aligned}
y(k) &= \chi\left\{\alpha_1 x_1(k) + \alpha_2 x_2(k)\right\} \\
&= \alpha_1 y_1(k) + \alpha_2 y_2(k),
\end{aligned}
$$

kjer je

$$
\begin{aligned}
y_1(k) &= \chi\left\{x_1(k)\right\} \\
y_2(k) &= \chi\left\{x_2(k)\right\}
\end{aligned}
$$

To pomeni, da linearen sistem izpolnjuje **princip superpozicije**. Če ga ne izpolnjuje, je sistem **nelinearen**.

PRIMER 49:

Test linearnosti za sistem, ki ga določa diferenčna enačba:

$$y(k) = B_0 x(k) + B_1 x(k-1)$$

Z uporabo x_1 in x_2 na vhodu dobimo:

$$y_1(k) = B_0 x_1(k) + B_1 x_1(k-1)$$
$$y_2(k) = B_0 x_2(k) + B_1 x_2(k-1)$$

Odziv sistema na $(\alpha_1 x_1(k) + \alpha_2 x_2(k))$ je:

$$\begin{aligned} y(k) &= B_0 \left[\alpha_1 x_1(k) + \alpha_2 x_2(k)\right] + B_1 \left[\alpha_1 x_1(k-1) + \alpha_2 x_2(k-1)\right] \\ &= \alpha_1 \left[B_0 x_1(k) + B_1 x_1(k-1)\right] + \alpha_2 \left[B_0 x_2(k) + B_1 x_2(k-1)\right] \\ &= \alpha_1 y_1(k) + \alpha_2 y_2(k) \end{aligned}$$

Sistem je torej linearen, ne glede na to, ali so koeficienti časovno spremenljivi ali ne.
◇

- Sistem je časovno **invarianten** (TI), če se parametri s časom ne spreminjajo, sicer je časovno **varianten** (TV). Za TI sisteme velja:

  $$\text{če } y(k) = \chi\left\{x(k)\right\}, \text{ potem } y(k-n) = \chi\left\{x(k-n)\right\}$$

  (pri $l = k - n$ vidimo, da se razmerje med vhodi in izhodi s časom ne spreminja)

- Če na izhod v času k vpliva le vhod v času k, potem je to **brezpomnilni** ali **trenutni** (*ang.* memoryless or instantaneous) sistem. V nasprotnem primeru govorimo o **dinamičnih** sistemih.

  Dinamični sistemi se nadalje delijo na:

  1. sisteme s **končnim pomnilnikom** (KP), tudi FIR (*ang.* Finit Impulse Response)
  2. sisteme z **neskončnim pomnilnikom** (NP), tudi IIR (*ang.* Infinite Impulse Response) ali **rekurzivne sisteme**

  KP:

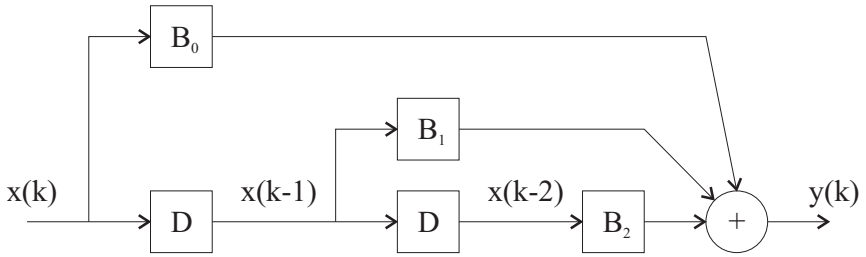
  $$y(k) = \sum_{i=0}^{m} B_i \cdot x(k-i)$$

  NP:

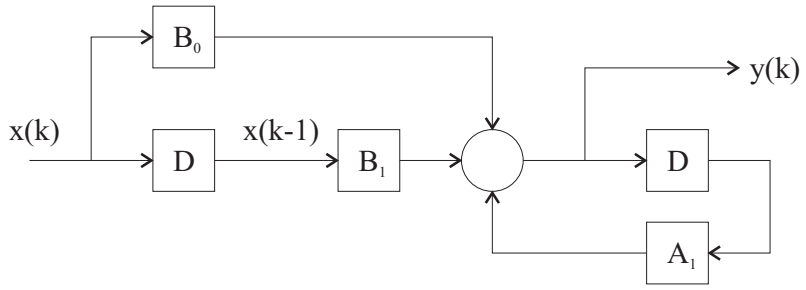
  $$y(k) = \sum_{i=1}^{n} A_i \cdot y(k-i) + \sum_{i=0}^{m} B_i \cdot x(k-i)$$

PRIMER 50:

Sistem s KP ($m = 2$):



Sistem z NP ($m = n = 1$):



◇

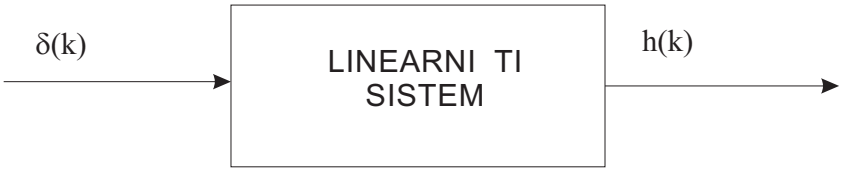
- Rekurzivni sistemi so zaradi povratne vezave lahko tudi nestabilni (izhod raste s časom preko mej).

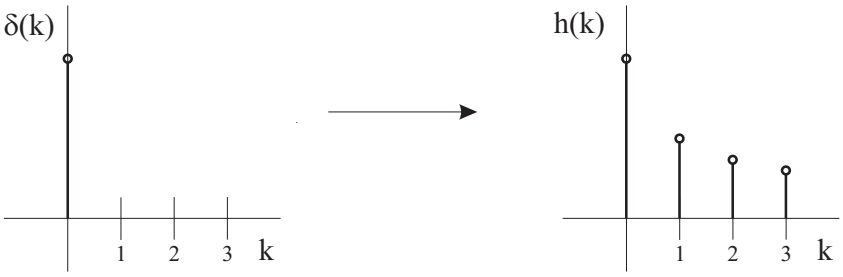
  Zvezni rekurzivni sistemi so predstavljeni z diferencialno enačbo:

$$\sum_{i=0}^{n} a_i y^{(i)}(t) = \sum_{i=0}^{m} b_i x^{(i)}(t) \qquad y^{(i)},\ x^{(i)} \text{ so i-ti odvodi } y(t),\ x(t) \text{ po času}$$

9.4 Interakcija signalov in sistemov

- Sistem lahko določimo z odzivom na elementarni testni signal (u. p. enotni pulz $\delta(t)$):





- Sistem je **kavzalen** (vzročen) ali **izvedljiv**, če njegov odziv ne prehiteva vhoda, ki ga povzroča. Pri kavzalnih sistemih je $h(k) = 0$, $k < 0$.

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

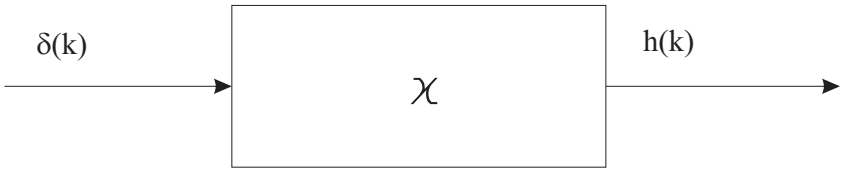
- Vzemimo poljubno sekvenco $x(k)$, ki vstopa v sistem. Ta povzroči izhodno sekvenco $y(k)$. Izpeljimo zvezo med vhodom x, odzivom na enotin pulz h in izhodom y:

  Iz semplirne lastnosti enotinega pulza sledi:

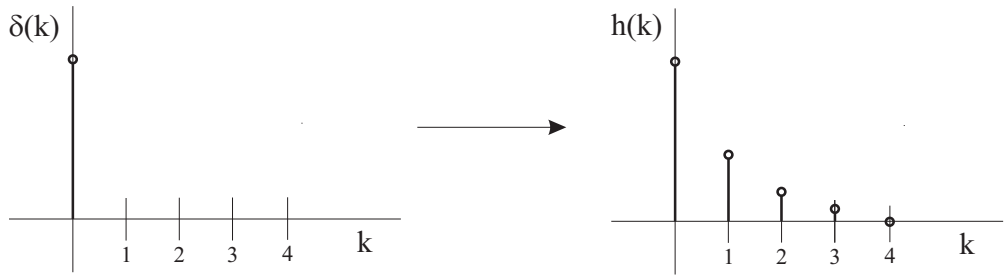
$$x(k) = \sum_{i=-\infty}^{+\infty} x(i)\delta(k - i)$$

- Odziv na $\delta(k-i)$ je $h(k-i)$, odziv na pulz $x(i)$ pa $x(i)h(k-i)$. Zaradi **superpozicije** je izhod $y(k)$ enak vsoti odzivov $x(i)h(k - i)$ na vse zamaknjene vhodne vzorce:

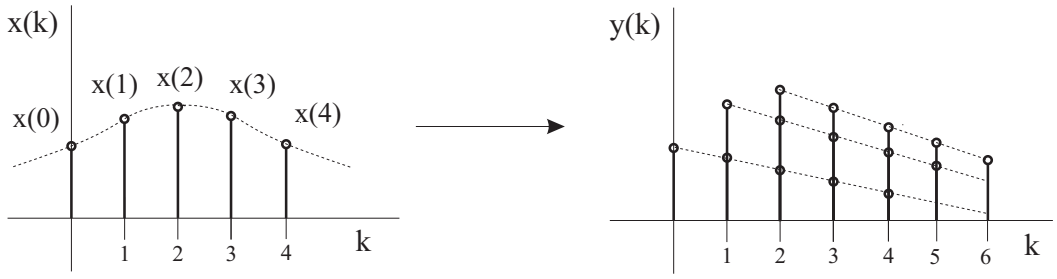
$$y(k) = \sum_{i=-\infty}^{+\infty} x(i)h(k - i)$$



1. odziv na $\delta(k)$:



2. odziv na $x(k)$:



$$y(0) = x(0)h(0)$$
$$y(1) = x(0)h(1) + x(1)h(0)$$
$$y(2) = x(0)h(2) + x(1)h(1) + x(2)h(0) \quad \ldots$$
$$y(k) = \sum_{i=0}^{k} x(i)h(k-i)$$

- Če v zgornji enačbi za $y(k)$ vpeljemo najprej $m = k - i$, nato pa namesto m zopet pišemo i, dobimo:

$$y(k) = \sum_{i=-\infty}^{+\infty} x(i)h(k-i) = \sum_{i=-\infty}^{+\infty} x(k-i)h(i) = x(k) * h(k) \quad \text{- konvolucija}$$

  Pravimo, da je y **linearna konvolucija** x-a in h-ja.

- Konvolucija velja tako za kavzalne kot za nekavzalne sisteme.

  Pri kavzalnih sistemih je:

$$y(k) = \sum_{i=0}^{\infty} x(k-i)h(i)$$

- V primerih sistemov LTV pa je:

$$y(k) = \sum_{i=-\infty}^{\infty} x(i)h(k,i)$$

- Velja analogija med enačbo KP sistema in konvolucijsko vsoto:

$$y(k) = \sum_{i=0}^{m} B_i x(k-i) \quad ; \quad y(k) = \sum_{i=0}^{m} h(i)x(k-i) \quad , h_i = B_i$$

PRIMER 51:

Reševanje diferenčne enačbe z uporabo **indukcije** in **konvolucije**:

- Z indukcijo:

$$
\begin{aligned}
y(k) &= Ay(k-1) + x(k) \\
k = 0: &\quad y(0) = Ay_{-1} + x(0) \\
k = 1: &\quad y(1) = Ay(0) + x(1) = A^2 y_{-1} + Ax(0) + x(1) \\
k = 2: &\quad y(2) = Ay(1) + x(2) = A^3 y_{-1} + A^2 x(0) + Ax(1) + x(2) \quad \ldots \\
k = k: &\quad y(k) = A^{k+1} y_{-1} + \sum_{i=0}^{k} A^i x(k-i)
\end{aligned}
$$

Če je $x(k)$ enotina stopničasta sekvenca $u(k)$, je:

$$y(k) = A^{k+1} y_{-1} + \sum_{i=0}^{k} A^i$$

$\sum_{i=0}^{k} A^i$ lahko poiščemo drugače zaradi:

$$
\begin{aligned}
S_n &= \sum_{i=0}^{n-1} C \cdot r^i = \frac{C(1-r^n)}{1-r} \\
S_n &= C + C \cdot r + \ldots + C \cdot r^{n-1} \qquad \backslash \cdot r \\
r \cdot S_n &= C \cdot r + C \cdot r^2 + \ldots + C \cdot r^n \\
r \cdot S_n &= S_n - C + C \cdot r^n \\
S_n(1-r) &= C(1-r^n) \\
S_n &= \frac{C(1-r^n)}{1-r}
\end{aligned}
$$

Če $|r| < 1$, je $S_\infty = \sum_{i=0}^{\infty} C \cdot r^i = \frac{C}{1-r}$.

$$
\begin{aligned}
\sum_{i=0}^{k} A^i &= \frac{1-A^{k+1}}{1-A} \\
y(k) &= A^{k+1} \cdot y_{-1} + \frac{1-A^{k+1}}{1-A}
\end{aligned}
$$

Če $|A| \geq 1$, $y(k)$ divergira z naraščajočim k. Če $|A| < 1$, $y(k)$ konvergira z naraščajočim k.

V limiti je: $y_{ss} = \lim_{k\to\infty} y(k) = \frac{1}{1-A}$. y_{ss} je y v mirovnem stanju (*ang.* steady state). Če je $y_{-1} = 0$ in $x(k) = \delta(k)$, imamo:

$$y(k) = h(k) = \sum_{i=0}^{k} A^i \delta(k-i) = A^k$$

Za sisteme višjih redov zgornja metoda ni praktična. Tedaj je smiselno uporabiti **Z transformacijo**, kar bomo storili v nadaljevanju. Možno pa je rešiti diferenčno enačbo tudi z uporabo **konvolucije** in predpostavke, da je h(k) poznan.

- S konvolucijo:

  Predpostavke:

$$h(k) = \begin{cases} A^k, & k \geq 0, 0 < A < 1 \\ 0, & k < 0 \end{cases}$$

$$y_{-1} = 0,\ x(k) = u(k)$$

$$y(k) = ?$$

$$y(k) = \sum_{i=-\infty}^{+\infty} x(i)h(k-i)$$

$$y(k) = \sum_{i=0}^{k} A^{k-i} = A^k \sum_{i=0}^{k} A^{-i} = \frac{1 - A^{k+1}}{1 - A}$$

  V limiti dobimo:

$$y_{ss} = \lim_{k \to \infty} y(k) = \frac{1}{1 - A}$$

  N.pr.: za $A = 0.8 \rightarrow y_{ss} = 5$.

◇

9.5 Stabilnost linearnih sistemov

- Linearni sistem je **stabilen**, če omejen vhod povzroči omejen izhod. Pogoj za stabilnost diskretnega LTI sistema je:

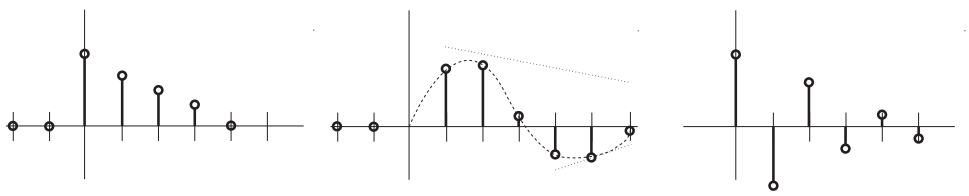
$$\sum_{i=-\infty}^{+\infty} |h(i)| < \infty,$$

  kar sledi iz:

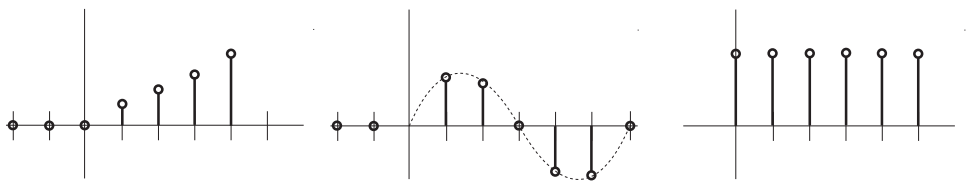
$$|y(k)| \leq \sum_{i=-\infty}^{+\infty} |h(i)||x(k-i)| \leq M \sum_{i=-\infty}^{+\infty} |h(i)|$$

  in je vhod omejen z: $|x(k)| \leq M$. Pogoj v bistvu pomeni omejen izhod.

- Primeri stabilnih sekvenc:



  in nestabilnih sekvenc:



Poglavje 10

Fourierova in Laplaceova transformacija

10.1 Fourierova vrsta

- Fourierova vrsta za **periodične** funkcije:

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

$$\omega_f = \frac{2\pi}{T_p} \equiv \text{osnovna frekvenca}$$

- Fourierova vrsta za **neperiodične** funkcije na intervalu $-L$ do $+L$, $L = \frac{T_p}{2}$, $\omega_f = \frac{\pi}{L}$:

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

- Za razvoj $f(x), x = \omega_f t$ s periodo 2π na intervalu $[-\pi, +\pi]$:

$$f(x) = a_0 + \sum_{n=1}^{\infty} a_n \cos nx + \sum_{n=1}^{\infty} b_n \sin nx$$

Glede na zapis funkcije ločujemo tudi izraze za izračun parametrov:

- Za periodične funkcije računamo parametre z enačbami:

$$\begin{aligned} a_0 =& \frac{1}{T_p} \int_0^{T_p} f(t)dt \\ a_n =& \frac{2}{T_p} \int_0^{T_p} f(t) \cos n\omega_f t dt, n = 1, 2, \ldots \\ b_n =& \frac{2}{T_p} \int_0^{T_p} f(t) \sin n\omega_f t dt, n = 1, 2, \ldots \end{aligned}$$

- Za neperiodične funkcije računamo parametre z enačbami:

$$
\begin{aligned}
a_0 =& \frac{1}{2L}\int_{-L}^{+L} f(t)dt \\
a_n =& \frac{1}{L}\int_{-L}^{+L} f(t)\cos\frac{n\pi t}{L}dt, n = 1, 2, \ldots \\
b_n =& \frac{1}{L}\int_{-L}^{+L} f(t)\sin\frac{n\pi t}{L}dt, n = 1, 2, \ldots
\end{aligned}
$$

- Za $f(x)$ na intervalu $[-\pi, +\pi]$:

$$
\begin{aligned}
a_0 =& \frac{1}{2\pi}\int_{-\pi}^{+\pi} f(x)dx \\
a_n =& \frac{1}{\pi}\int_{-\pi}^{+\pi} f(x)\cos nx dx, n = 1, 2, \ldots \\
b_n =& \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin nx dx, n = 1, 2, \ldots
\end{aligned}
$$

- Periodično funkcijo f(t) lahko razvijemo v Fourierovo vrsto na intervalu [a, b], če zadošča Dirichletovim pogojem:

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

- Predhodno podane enačbe predstavljajo **trigonometrijsko obliko** Fourierjeve vrste.

- **Polarno obliko** Fourierjeve vrste predstavlja izraz:

$$
f(t) = \sum_{n=0}^{\infty} A_n \cos(n\omega_f t + \phi_n)
$$

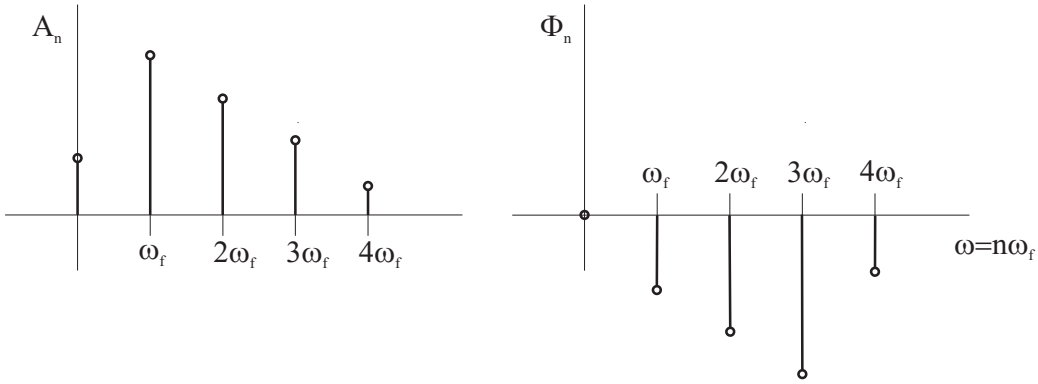
$$
A_n = \sqrt{a_n^2 + b_n^2} \quad , \phi_n = \arctan\frac{b_n}{a_n}
$$

  Polarna oblika ima v frekvenčnem prostoru dva spektra: **amplitudni** ($A_n(n\omega_f)$) in **fazni** ($\phi_n(n\omega_f)$).

- **Eksponentno obliko** Fourierjeve vrste dobimo z uporabo Eulerjevih enačb:

$$
f(t) = \sum_{n=-\infty}^{+\infty} C_n e^{jn\omega_f t} \quad , C_n = \frac{1}{T_p}\int_0^{T_p} f(t)e^{-jn\omega_f t}dt
$$

Primer spektrov:



10.2 Fourierova transformacija

- Frekvenčno informacijo za aperiodično časovno funkcijo, definirano na celotni časovni osi, podaja Fourierov integral:

$$F(j\omega) = \int_{-\infty}^{+\infty} f(t)e^{-j\omega t)dt} = \mathcal{F}\{f(t)\}$$

- Inverzni Fourierov transform je:

$$f(t) = \frac{1}{2\pi}\int_{-\infty}^{+\infty} F(j\omega)e^{j\omega t}d\omega = \mathcal{F}^{-1}\{F(j\omega)\}$$

- Pogoji, da ima $f(t)$ Fourierov transform, so enaki kot pri razvitju v Fourierjevo vrsto, le perioda je tukaj ∞ in zato:

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

- Lastnosti Fourierova transforma:

1. LINEARNOST

$$\mathcal{F}\{\alpha_1 f_1(t) + \alpha_2 f_2(t)\} = \alpha_1 F_1(j\omega) + \alpha_2 F_2(j\omega)$$

2. ČASOVNI ZAMIK:

$$\mathcal{F}\{f(t \pm t_0)\} = e^{\pm j\omega t_0} \cdot F(j\omega)$$

3. FREKVENČNI ZAMIK:

$$\mathcal{F}\{f(t)e^{\pm j\omega_0 t}\} = F[j(\omega \mp \omega_0)]$$

4. SKALIRNI FAKTOR:

$$\mathcal{F}\{f(at)\} = \frac{1}{a}F(\frac{j\omega}{a})$$

5. KONVOLUCIJSKI TEOREM:

$$\mathcal{F}\{\int_{-\infty}^{+\infty} f_1(\tau)f_2(t-\tau)d\tau\} = F_1(j\omega)\cdot F_2(j\omega)$$

6. KOMPLEKSNI KONVOLUCIJSKI TEOREM:

$$\mathcal{F}\{f_1(t)\cdot f_2(t)\} = \frac{1}{2\pi}\int_{-\infty}^{+\infty} F_1(p)\cdot F_2(\omega-p)dp$$

7. TEOREM ZA ODVAJANJE:

$$\mathcal{F}\{\frac{d^n f}{dt^n}\} = (j\omega)^n\cdot F(j\omega)$$

8. TEOREM ZA INTEGRACIJO:

$$\mathcal{F}\{\int_{-\infty}^{t} f(t)dt\} = \frac{1}{j\omega}F(j\omega)$$

10.3 Laplaceova transformacija:

- Mnoge zanimive aperiodične funkcije ne zadoščajo Dirichletovim pogojem (n.pr. stopničasta funkcija $u(t)$, rampa $f(t) = t\cdot u(t)$, vlak impulzov $\sum_{-\infty}^{+\infty}\delta(t-kT)$).
- Če pozitivno funkcijo (ki štarta ob $t=0$) množimo z $e^{-\sigma t}$, dobimo:

  $$\int_0^{\infty} |f(t)e^{-\sigma t}|dt < \infty$$

  To pomeni, da $f(t)e^{-\sigma t}$ izpolnjuje pogoje za Fourierov transform.
- Fourierov transform funkcije $f(t)e^{-\sigma t}$ je enak:

  $$\mathcal{F}\{f(t)e^{-\sigma t}\} = \int_0^{\infty} f(t)e^{-\sigma t}e^{-j\omega t}dt = \int f(t)e^{-st}dt = F(s) = \mathcal{L}\{f(t)\}$$

  kjer je $s = \sigma + j\omega$

  To je **Laplaceov transform**, ki ga označujemo z $F(s)$ ali $\mathcal{L}\{f(t)\}$.
- Inverzni Laplaceov transform je enak:

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

  c mora ležati v področju konvergence (ROC), kjer je izpolnjen pogoj:

  $$\int_0^{\infty} |f(t)e^{-\sigma t}|dt < \infty$$

  Transforme ali njihove inverze lahko izračunamo s pomočjo znanih parov:

$f(t), t \geq 0$	$F(s)$
$\delta(t-t_0), t_o > 0$	e^{-st_o}
A	$\frac{A}{s}$
e^{-at}	$\frac{1}{s+a}$
$\sin \omega_0 t$	$\frac{\omega_o}{s^2+{\omega_0}^2}$
$\cos \omega_0 t$	$\frac{s}{s^2+{\omega_0}^2}$
$e^{-at} \cdot \sin \omega_0 t$	$\frac{\omega_0}{(s+a)^2+{\omega_0}^2}$
$A \cdot t$	$\frac{A}{s^2}$
$A \cdot t^{n-1}$	$\frac{A(n-1)!}{s^n}$
$e^{-at} \cdot t^{n-1}$	$\frac{(n-1)!}{(s+a)^n}$

- Lastnosti Laplaceove transformacije:

1. LINEARNOST:

$$\mathcal{L}\{\alpha_1 f_1(t) + \alpha_2 f_2(t)\} = \alpha_1 F_1(s) + \alpha_2 F_2(s)$$

2. ČASOVNI ZAMIK:

$$\mathcal{L}\{f(t \pm t_o)\} = e^{\pm st_0} F(s)$$

3. FREKVENČNI ZAMIK:

$$\mathcal{L}\{f(t)e^{\pm bt} = F(s \mp b)$$

4. SKALIRNI FAKTOR:

$$\mathcal{L}\{f(at)\} = \frac{1}{a} F(\frac{s}{a})$$

5. KONVOLUCIJSKI TEOREM:

$$\mathcal{L}\{\int_0^\infty f_1(\tau) f_2(t-\tau) d\tau\} = F_1(s) \cdot F_2(s)$$

6. KOMPLEKSNI KONVOLUCIJSKI TEOREM:

$$\mathcal{L}\{f_1(t) f_2(t)\} = \frac{1}{2\pi j} \int_{c-j\infty}^{c+j\infty} F_1(p) F_2(s-p) dp$$

7. TEOREM ZA ODVAJANJE:

$$\begin{aligned}
\mathcal{L}\{\frac{df(t)}{dt}\} =& sF(s) - f(0_+) \\
\mathcal{L}\{\frac{d^2 f(t)}{dt^2}\} =& s^2 F(s) - sf(0_+) - \frac{df(0_+)}{dt} \\
\mathcal{L}\{\frac{d^n f(t)}{dt^n}\} =& s^n F(s) - s^{n-1} f(0_+) - s^{n-2} \frac{df(0_+}{dt} - \ldots - s \frac{d^{n-2} f(0_+)}{dt^{n-2}} - \frac{d^{n-1} f(0_+)}{dt^{n-1}}
\end{aligned}$$

8. TEOREM ZA INTEGRACIJO:

$$\mathcal{L}\{\int f(t)dt\} = \frac{F(s)}{s} + \frac{f^{(-1)}(0_+)}{s}$$

$$f^{(-1)}(t) = \int f(t)dt = \int_0^t f(t)dt + f^{(-1)}(0_+)$$

9. TEOREM KONČNE VREDNOSTI:

$$\lim_{t\to\infty} f(t) = \lim_{s\to 0} sF(s)$$

Pogoji:

- $f(t)$ in $\frac{df(t)}{dt}$ imata Laplaceov transform
- $sF(s)$ nima singularnosti na $j\omega$ osi oz. na desni strani s ravnine ($\sigma > 0$)

10. TEOREM ZAČETNE VREDNOSTI:

$$\lim_{t\to 0_+} f(t) = \lim_{s\to\infty} sF(s)$$

Pogoji:

- $f(t)$ in $\frac{df(t)}{dt}$ imata Laplaceov transform
- eksistira $\lim_{s\to\infty} sF(s)$

Poglavje 11

Sistemska prenosna funkcija

- Diskretni linearni časovno invariantni (LTI) sistem opisuje enačba:

$$y(k) = \sum_{i=1}^{n} A_i y(k-i) + \sum_{i=0}^{m} B_i x(k-i)$$

- Zvezni linearni časovno invariantni (LTI) sistem pa podaja enačba:

$$\sum_{i=0}^{n} a_i y^{(i)} = \sum_{i=0}^{m} b_i x^{(i)}$$

  Zgornjo diferencialno enačbo lahko prevedemo v algebraično s pomočjo Laplaceove transformacije:

$$(\sum_{i=0}^{n} a_i s^i) \cdot Y(s) = (\sum_{i=0}^{m} b_i s^i) \cdot X(s)$$

- **Prenosna funkcija** je definirana kot:

$$H(s) = \frac{Y(s)}{X(s)} = \frac{\sum_{i=0}^{m} b_i s^i}{\sum_{i=0}^{n} a_i s^i}$$

  V splošnem je $H(s)$ razmerje dveh polinomov reda m in n, kjer je $m \leq n$.

- Prenosno funkcijo zapisujemo v **kaskadni** ali pa v **paralelni** obliki: Kaskadna oblika:

$$H(s) = \frac{\prod_{i=1}^{m} (s - \beta_i)}{\prod_{i=1}^{n} (s - \alpha_i)}$$

  Paralelna oblika:

$$H(s) = \sum_{i=1}^{n} \frac{R_i}{(s - \alpha_i)}$$

  α_i določa pole, β_i pa ničle. R_i je **residuum** (ostanek) H(s) pri polu α_i.

- Do prenosne funkcije $H(s)$ lahko pridemo tudi z Laplaceovo transformacijo konvolucije

$$y(t) = \int_0^\infty x(\tau)h(t-\tau)d\tau$$

Konvolucijski teorem (5. lastnost Laplaceove transformacije) nam da:

$$Y(s) = H(s) \cdot X(s) \text{ oz. } H(s) = \frac{Y(s)}{X(s)}$$

- Izhodno funkcijo y(t) dobimo z inverzno Laplaceovo transformacijo:

$$y(t) = \mathcal{L}^{-1}\{H(s) \cdot X(s)\},$$

čeprav je največkrat enostavneje določiti $y(t)$ s pomočjo konvolucijskega integrala.

- Pri računanju **inverznega Laplaceovega transforma** za dano $F(s)$ so v rabi tri metode:

  1. Uporaba tabele Laplaceovih parov (samo pri enostavnih $F(s)$)
  2. Razširjava $F(s)$ v delne ulomke in izvedba inverzne Laplaceove transformacije nad enostavnejšimi členi.
  3. Uporaba residualne metode.

- Metoda 2:

  1. Razvij $F(s)$ v delne ulomke:

$$F(s) = \frac{B(s)}{A(s)} = \frac{B(s)}{(s-\alpha_1)(s-\alpha_2)\cdots(s-\alpha_n)} =$$

$$= \frac{R_1}{(s-\alpha_1)} + \cdots + \frac{R_{K_1}}{(s-\alpha_K)^3} + \frac{R_{K_2}}{(s-\alpha_K)^2} + \frac{R_{K_3}}{(s-\alpha_K)} \cdots \frac{R_n}{(s-\alpha_n)}$$

  2. Določi residuum za **enojne pole**:

$$R_i = (s-\alpha_i)F(s) \mid_{s=\alpha_i}$$

in za večkratne pole:

$$R_{K_l} = \frac{1}{(l-1)!} \cdot \frac{d^{l-1}}{ds^{l-1}}[(s-\alpha_k)^{\max} \cdot F(s)] \mid_{s=\alpha_K}$$

max - maksimalna stopnja pola l - tekoča stopnja pola (od 1 do max)
Za zgornji primer: max = 3

$$R_{K_1} = (s-\alpha_K)^3 F(s) \mid_{s=\alpha_K}$$
$$R_{K_2} = \frac{d}{ds}[(s-\alpha_K)^3 \cdot F(s) \mid_{s=\alpha_K}$$
$$R_{K_3} = \frac{1}{2} \cdot \frac{d^2}{ds^2}[(s-\alpha_K)^3 F(s)] \mid_{s=\alpha_K}$$

3. Inverz delnih ulomkov tipa $\frac{R_{K_1}}{(s-\alpha_K)^m}$ dobimo iz tabele parov:

$$\mathcal{L}^{(-1)}\{\frac{R_{K_1}}{(s-\alpha_K)^m}\} = \frac{R_{K_1}}{(m-1)!} \cdot t^{m-1} \cdot e^{\alpha_K t}$$

- Metoda 3 (residualna metoda): Bazira na **Cauchyjevem integralskem teoremu**: 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:

$$\int_c f(z)dz = 2\pi j \sum_i (\text{residuumi } f(z) \text{ pri } \alpha_i),$$

poli α_i so znotraj c

Ta teorem uporabimo nad inverzno Laplaceovo transformacijo:

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

če identificiramo z z s in $f(z)$ z $F(s)e^{st}$.

1. Residuum pri polu α_K izračunamo z:

$$R_K = \frac{1}{(m-1)!} \cdot \frac{d^{m-1}}{ds^{m-1}}[(s-\alpha_K)^m \cdot F(s) \cdot e^{st}]|_{s=\alpha_K}$$

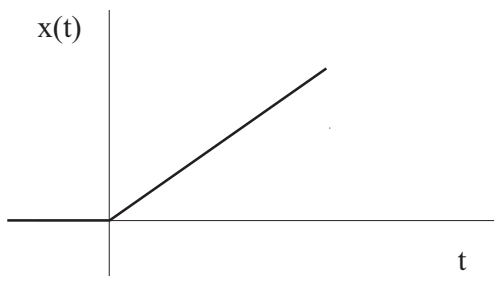
   Tukaj je samo en residuum za pol reda m!

2. Inverzni transform dobimo z vsoto vseh residuumov (Cauchyjev teorem).

PRIMER 52:

Poiščite odziv na enotino rampo (*ang.* unit ramp), če je sistem podan z:

$$H(s) = \frac{8(s+1)}{s(s+2)}, \quad x(t) = t \cdot u(t)$$



Po Metodi 2:

$$X(s) = \frac{1}{s^2} \quad \text{(tabela Laplaceovih parov)}$$

$$Y(s) = H(s) \cdot X(s) = \frac{8(s+1)}{s^3(s+2)}$$

$$Y(s) = \frac{R_1}{s+2} + \frac{R_{21}}{s^3} + \frac{R_{22}}{s^2} + \frac{R_{23}}{s}$$

$$R_1 = (s+2)Y(s)|_{s=-2} = 1$$
$$R_{21} = s^3Y(s)|_{s=0} = 4$$
$$R_{22} = \frac{d}{ds}[s^3Y(s)]|_{s=0} = 2$$
$$R_{23} = \frac{1}{2}\frac{d^2}{ds^2}[s^3Y(s)]|_{s=0} = -1$$

$$Y(s) = \frac{1}{s+2} + \frac{4}{s^3} + \frac{2}{s^2} - \frac{1}{s}$$

Iz tabele Laplaceovih parov dobimo:

$$y(t) = e^{-2t} + 2t^2 + 2t - 1$$

Po Metodi 3 (residualna metoda):

$$y(t) = \sum (\text{residuumi } Y(s)e^{st} \text{ pri } s = 0 \text{ in } s = -2)$$

$$= \sum_i \frac{1}{(m-1)!}\frac{d^{m-1}}{ds^{m-1}}[(s-\alpha_i)^m Y(s)e^{st}]|_{s=\alpha_i}$$

$\alpha_1 = -2:$

$$R_1 = \frac{8(s+1)}{s^3}e^{st}|_{s=-2} = e^{-2t}$$

$\alpha_2 = 0, m = 3:$

$$R_2 = \frac{1}{2}\frac{d^2}{ds^2}[\frac{8(s+1)}{(s+2)}e^{st}]|_{s=0} = [4t^2e^{st}\frac{(s+1)}{(s+2)} + \frac{8te^{st}}{(s+2)^2} - \frac{8e^{st}}{(s+2)^3}]|_{s=0}$$

$$= 2t^2 + 2t - 1$$

$$y(t) = R_1 + R_2 = e^{-2t} + 2t^2 + 2t - 1$$

- Za isti primer bi bil odziv na stopnico ($X(s) = \frac{1}{s}$) enak:

  $$y(t) = -2e^{-2t} + 4t + 2$$

  Izhod tudi tukaj narašča s časom, saj tudi integracija konstante s časom raste.

◇

- Potrebni in zadostni pogoj za **stabilnost zveznih LTI** sistemov s prenosno funkcijo $H(s) = \frac{B(s)}{A(s)}$ je: **vsi poli $H(s)$ morajo biti na levi strani s ravnine ($\sigma < 0$).**

11.1 Frekvenčni odziv sistema

- Sistemski frekvenčni odziv dobimo, če v $H(s)$ vzamemo $s = j\omega$:

$$H(j\omega) = A(\omega) + jB(\omega) = M(\omega)e^{j\phi(\omega)}$$

$M(\omega) \equiv$ amplitudni odziv, $\phi(\omega) \equiv$ fazni odziv

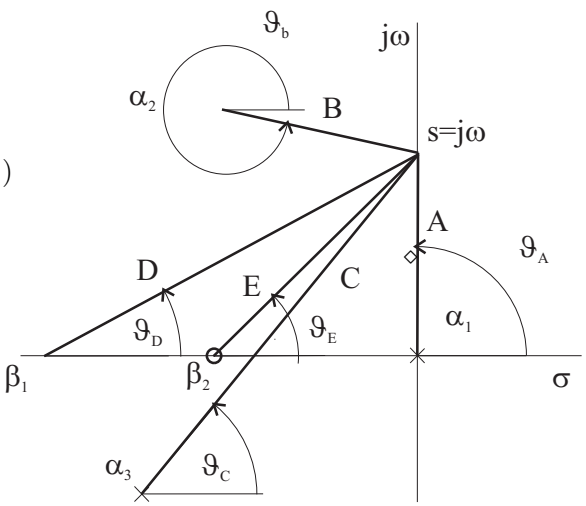
- Pri vsaki frekvenci ω je $H(j\omega)$ kompleksno število. N.pr:

$$\begin{aligned}
H(s) &= \frac{1}{T \cdot s + 1} \\
H(j\omega) &= \frac{1}{j\omega T + 1} = \frac{1 - j\omega T}{1 + \omega^2 T^2} \\
M(\omega) &= \left| \frac{1 - j\omega T}{1 + \omega^2 T^2} \right| = (A^2 + B^2)^{\frac{1}{2}} = \\
&= ((\frac{1}{1 + \omega^2 T^2})^2 + (\frac{\omega T}{1 + \omega^2 T^2})^2)^{\frac{1}{2}} = \\
&= (\frac{(1 + \omega^2 T^2)}{(1 + \omega^2 T^2)^2})^{\frac{1}{2}} = \sqrt{\frac{1}{1 + \omega^2 T^2}} = \\
&= \frac{1}{(1 + \omega^2 T^2)^{\frac{1}{2}}} \\
\phi(\omega) &= \arctan(-\omega T)
\end{aligned}$$

- Za sisteme višjih redov je iz $H(j\omega)$ težko določiti $M(\omega)$ in $\phi(\omega)$. Zato se uporabljajo računalniški programi ali grafična metoda.
- **Grafična metoda** zahteva zapis $H(s)$ v kaskadno obliko in označitev ničel in polov v kompleksni s ravnini.
- $M(\omega)$ je enak produktu konstante K (ojačanje) z dolžinami vektorjev od ničel, deljeno z dolžinami vektorjev od polov. $\phi(\omega)$ pa je algebraična vsota kotov vektorjev s pozitivno smerjo σ. S spreminjanjem s vzdolž $j\omega$ osi dobimo $M(\omega)$, $\phi(\omega)$.

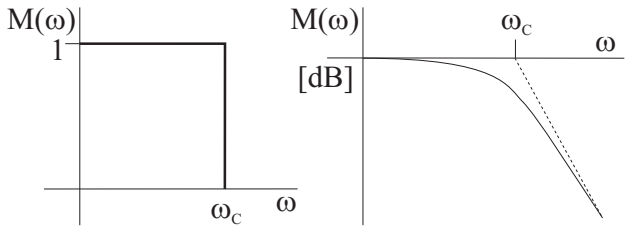
PRIMER 53:

$$\begin{aligned}
H(s) &= \frac{K \cdot (s - \beta_1)(s - \beta_2)}{s(s - \alpha_2)(s - \alpha_3)} \\
M(\omega) &= K \frac{DE}{ABC} \quad ; \\
\phi(\omega) &= \vartheta_D + \vartheta_E - (\vartheta_A + \vartheta_B + \vartheta_C)
\end{aligned}$$

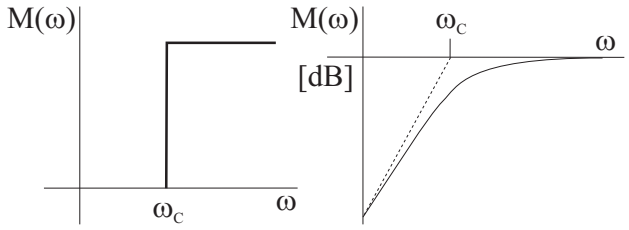


- Glede na amplitudni frekvenčni odziv, ločimo 4 kategorije sistemov (filtrov):

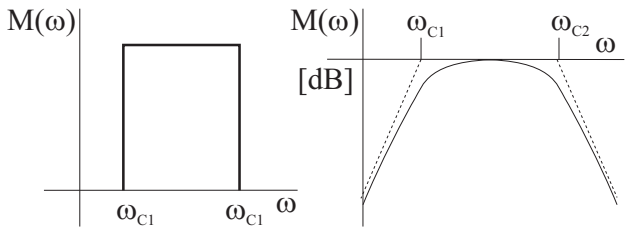
1. Nizko-prepustni (low-pass):



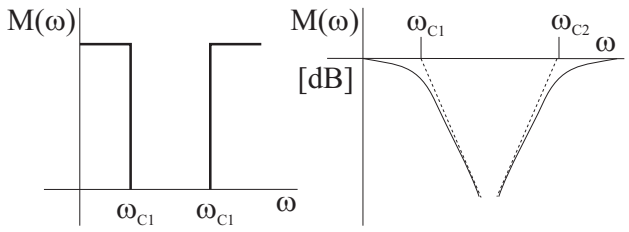
2. Visoko-prepustni (high-pass):



3. Pasovno-prepustni (band-pass):



4. Pasovno-zaporni (band-stop):



Poglavje 12

Vzorčenje in Z-transformacija

12.1 Vzorčenje zveznega signala

- Frekvenca vzorčenja je $f_s = \frac{1}{T}$, kjer je T perioda vzorčenja.

- Spodnjo mejo f_s podaja **teorem vzorčenja** ali **semplirni teorem** (3. Shannonov teorem):
  Če je **pasovno omejen signal** $f(t)$ (to je signal, ki ne vsebuje frekvenčnih komponent nad neko f_h) sempliran s frekvenco $f_s \geq f_h$, potem semplirne vrednosti vsebujejo vso informacijo iz zveznega signala. To pomeni, da je mogoča rekonstrukcija $f(t)$ iz $f(kT)$ s formulo:

$$f(t) = \sum_{k=-\infty}^{+\infty} f(kT) \frac{\sin\left[\omega_s(t-kT)/2\right]}{\omega_s(t-kT)/2} \quad , \quad \omega_s = 2\pi f_s$$

- Minimalno semplirno frekvenco $f_s = 2f_h$ imenujemo tudi **Nyquistovo frekvenco** za opazovani zvezni signal.

PRIMER 54:

$f(t) = \sin \omega_0 t$ želimo semplirati z ω_s, kar daje:

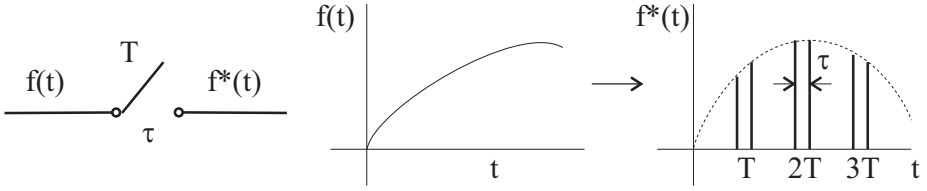
$$f(k) = \sin \omega_0 kT, T = \frac{2\pi}{\omega_s}$$

Če vzamemo sinus, katerega frekvenca se razlikuje od ω_0 za mnogokratnik ω_s, pa dobimo:

$$g(t) = \sin\left[(\omega_0 + n\omega_s)t\right] \rightarrow$$
$$g(k) = \sin\left[(\omega_0 + n\omega_s)kT\right] = \sin \omega_0 kT \quad , \quad \text{saj je } \omega_s T = 2\pi$$

Tedaj funkcij $f(k)$ in $g(k)$ ne moremo ločiti po sempliranju – višja frekvenca je zajeta v nižji (*ang.* aliasing). Pravilno je, da tudi $g(t)$ sempliramo z Nyquistovo frekvenco.
◇

- Semplirno operacijo lahko predstavimo s **filternim stikalom**:



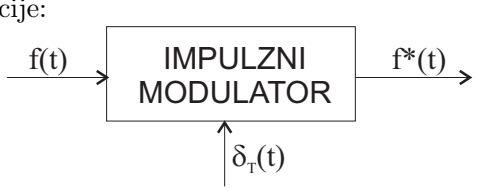
Če je $\tau \ll T$, lahko predpostavimo konstantno vrednost znotraj τ pri $f^*(t)$.

- Idealna semplirna funkcija:

$$\delta_T(t) = \sum_{k=-\infty}^{+\infty} \delta(t - kT) - \text{ veriga } \delta \text{ impulzov}$$

omogoča zapis semplirne funkcije:

$$f^*(t) = f(t) \cdot \delta_T(t) \quad ,$$



12.2 Laplace semplirne funkcije

Zanima nas izračun Laplaceove transformacije semplirne funkcije $f^*(t)$. Ogledali si bomo 3 metode in vselej upoštevali $f(t) = 0$ za $t < 0$.

1. Metoda:

$$\begin{aligned} f^*(t) &= f(t) \cdot \delta_T(t) = \\ &= f(t) \cdot \sum_{k=-\infty}^{+\infty} \delta(t - kT) == \sum_{k=-\infty}^{+\infty} f(t) \cdot \delta(t - kT) = \\ &= \sum_{k=0}^{+\infty} f(kT) \cdot \delta(t - kT) \quad , \quad \text{saj so vrednosti f(t) med vzorci izgubljene} \end{aligned}$$

Z uporabo Laplaceovega transforma $\mathcal{L}\{\delta(t - t_0)\} = e^{-st_0}$ (tabela stran 91) dobimo

$$F^*(s) = \sum_{k=0}^{\infty} f(kT) e^{-kTs}$$

2. Metoda: (z dokazom semplirnega teorema) Ker je $\delta_T(t)$ periodična funkcija, jo lahko razširimo v kompleksno Fourierovo vrsto:

$$\delta_T(t) = \sum_{n=-\infty}^{+\infty} C_n e^{jn\omega_s t} \quad , \quad \omega_s \text{ – semplirna frekvenca}$$

kjer je:

$$C_n = \frac{1}{T} \int_{-\frac{T}{2}}^{+\frac{T}{2}} \delta_T(t) e^{-jn\omega_s t} dt = \frac{1}{T}$$

samo $\delta(0)$ je v intervalu $[-\frac{T}{2}, +\frac{T}{2}]$ različen od 0, zato: $\int_{-\frac{T}{2}}^{+\frac{T}{2}} 1 \cdot e^0 dt = 1$
Sledi:

$$\delta_T(t) = \frac{1}{T} \sum_{n=-\infty}^{+\infty} e^{jn\omega_s t}$$

Če izraz za $\delta_T(t)$ vstavimo v izraz za $f^*(t) = f(t) \cdot \delta_T(t)$, dobimo:

$$f^*(t) = \frac{1}{T} \sum_{n=-\infty}^{+\infty} f(t) e^{jn\omega_s t}$$

Nad tem izračunom izvedemo člen po člen Laplaceovo transformacijo:

$$F^*(s) = \frac{1}{T} \sum_{n=-\infty}^{+\infty} F(s - jn\omega_s) = \frac{1}{T} \sum_{n=-\infty}^{+\infty} F(s + jn\omega_s)$$

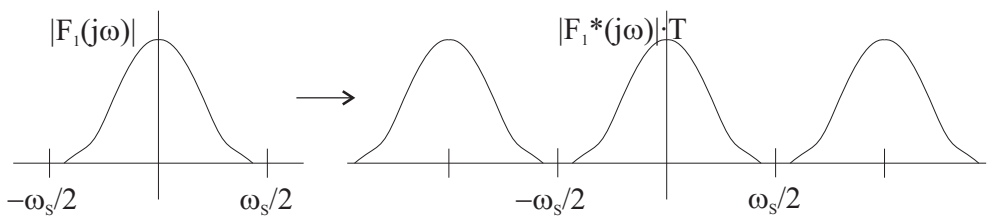
oz. če $s = j\omega$:

$$F^*(j\omega) = \frac{1}{T} \sum_{n=-\infty}^{+\infty} F(j(\omega + n\omega_s))$$

Ugotovitev: časovno periodične funkcije imajo diskretni frekvenčni spekter, diskretne časovne funkcije pa imajo zaradi periodičnega sempliranja periodičen frekvenčni spekter.

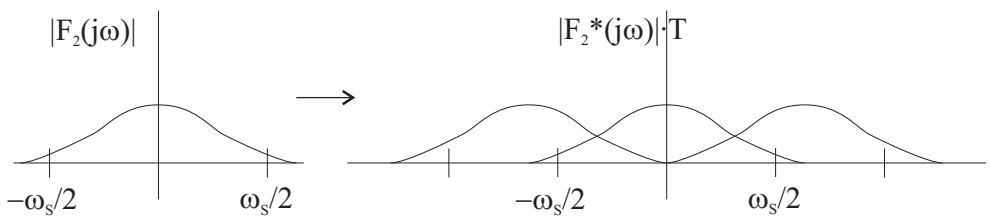
- Od tod sledita 2 primera:

  1. $\omega_s > 2\omega_h$:



     Opazimo, da je periodičen spekter sempliranega signala nepresečen. Originalni signal $F_1(j\omega)$ lahko dobimo s filtriranjem sempliranega signala (s filtrom širine ω_s).

  2. $\omega_s < 2\omega_h$:



     Tukaj je periodičen signal presečen, zato originalnega signala $F_2(j\omega)$ ne moremo rekonstruirati s filtriranjem.

- Oglejmo si rekonstrukcijo iz 1. primera ($\omega_s > 2\omega_h$). Tedaj je

$$T \cdot F^*(j\omega) = \sum_{n=-\infty}^{+\infty} F(j\omega + jn\omega_s)$$

periodična razširjava glede na $F(j\omega)$.

Rekonstrukcijo $F(j\omega)$ iz $F^*(j\omega)$ dobimo s pomočjo filtra $H(j\omega)$):

$$F(j\omega) = H(j\omega) \cdot T \cdot F^*(j\omega) \quad ,$$

kjer je

$$H(j\omega) = \begin{cases} 1, & |\omega| \leq \frac{\omega_s}{2} \\ 0, & |\omega| > \frac{\omega_s}{2} \end{cases} \quad .$$

$F^*(j\omega)$ zamenjamo z izrazom iz 1. Metode. Vzamemo še $s = j\omega$ in spremenimo spodnjo mejo $0 \to -\infty$:

$$F(j\omega) = H(j\omega) \cdot T \cdot \sum_{k=-\infty}^{+\infty} f(kT)e^{-jk\omega T}$$

Ker je:

$$f(t) = \mathcal{F}^{-1}\{F(j\omega)\} = T \sum_{k=-\infty}^{+\infty} f(kT)\mathcal{F}^{-1}\{H(j\omega)e^{-jk\omega T}\}$$

in:

$$\begin{aligned} \mathcal{F}^{-1}\{H(j\omega)\} &= \frac{1}{2\pi}\int_{-\infty}^{+\infty} H(j\omega)e^{j\omega t}d\omega \\ &= \frac{1}{2\pi}\int_{-\frac{\omega_s}{2}}^{+\frac{\omega_s}{2}} e^{j\omega t}d\omega = \\ &= \frac{1}{\pi t} \cdot \sin\frac{\omega_s}{2}t \end{aligned}$$

Sledi:

$$\begin{aligned} \mathcal{F}^{-1}\{H(j\omega)e^{-jk\omega T}\} &= \frac{\sin\left[\omega_s(t-kT)/2\right]}{\pi(t-kT)}, \quad \text{(časovni zamik)} \\ &= \frac{\sin\left[\omega_s(t-kT)/2\right]}{T\omega_s(t-kT)/2}, \quad (\omega_s = \frac{2\pi}{T} \Rightarrow \pi = \frac{\omega_s \cdot T}{2}) \end{aligned}$$

Končno je:

$$f(t) = \sum_{k=-\infty}^{+\infty} f(kT)\frac{\sin\left[\omega_s(t-kT)/2\right]}{\omega_s(t-kT)/2} \quad ,$$

kar predstavlja rekonstrukcijo $f(t)$ iz vzorcev $f(kT)$ sempliranega signala $f^*(t)$.

3. Metoda: Tukaj upoštevamo $\mathcal{L}\{f(t)\} = F(s)$, $\mathcal{L}\{\delta_T(t)\} = \Delta_T(s)$ in kompleksni konvolucijski teorem:

$$F^*(s) = \mathcal{L}\{f(t)\delta_T(t)\} = \frac{1}{2\pi j}\int_{c-j\infty}^{c+j\infty} F(p)\Delta_T(s-p)dp$$

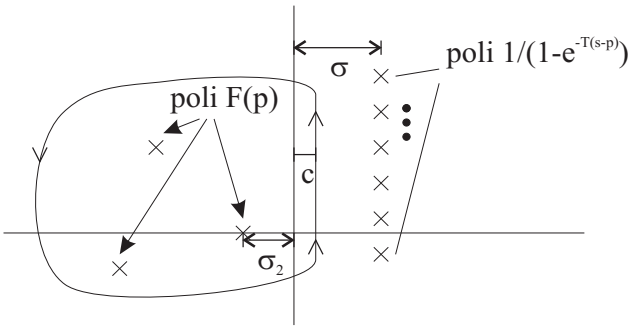
Ker velja:

$$\begin{aligned}\Delta_T(s) &= \mathcal{L}\{\sum_{n=0}^{\infty}\delta(t-nT)\} = \\ &= \sum_{n=0}^{\infty} e^{-nTs} = 1 + e^{-Ts} + e^{-2Ts} + \cdots = \\ &= \frac{1}{1-e^{-Ts}} \text{ , pri pogoju } |e^{-Ts}| < 1\end{aligned}$$

dobimo:

$$F^*(s) = \frac{1}{2\pi j}\int_{c-j\infty}^{c+j\infty} F(p)\frac{1}{1-e^{-T(s-p)}}dp$$

Integral lahko izračunamo z vsoto residuumov pri polih $F(p)$, če kontura c zapira le pole $F(p)$ in izključuje pole $\frac{1}{1-e^{-T(s-p)}}$. To velja v primeru, ko je $\sigma_2 < c < \sigma$.



$$\begin{aligned}e^{-T(s-p)} &= 1 = e^{j2l\pi} \\ l &= 0, \pm 1, \pm 2, \ldots \\ -Ts + Tp &= j2l\pi / : T \\ p - s &= jl\omega_s \\ p &= s + jl\omega_s = \\ &= \sigma + j\omega + jl\omega_s = \sigma + j(\omega + l\omega_s)\end{aligned}$$

$$F^*(s) = \sum \text{residuumov } F(p) \cdot \frac{1}{1-e^{-T(s-p)}} \text{ pri polih } F(p)$$

12.3 Z transformacija

- Spoznali smo 3 metode za izračun Laplaceove transformacije semplirnega signala $\mathcal{L}\{f^*(t)\} = F^*(s)$:
  1. $F^*(s) = \sum_{k=0}^{\infty} f(kT)e^{-kTs}$
  2. $F^*(s) = \frac{1}{T}\sum_{n=-\infty}^{+\infty} F(s + jn\omega_s)$
  3. $F^*(s) = \sum \text{residuumov} F(p)\frac{1}{1-e^{-T(s-p)}}$ pri polih $F(p)$

- Pri zveznih sistemih (LTI) je prednost Laplaceove transformacije, da diferencialno enačbo prevede v algebraično. Pri diskretnih sistemih to ni mogoče zaradi transcendentalnega izraza e^{Ts}.

- Zato bomo vpeljali **Z transformacijo** $F(z)$ funkcije $f(kT)$, s katero poenostavimo residuume:

  $$z = e^{Ts} \quad \text{oz.} \quad s = \frac{1}{T}\ln z$$

  Postopek:

  $$f(t) \underset{sempliranje}{\longrightarrow} f^*(t) \underset{\substack{Laplaceova \\ transformacija}}{\longrightarrow} F^*(s) \underset{z=e^{Ts}}{\longrightarrow} F(z)$$

  - Iz metode 1 dobimo:

    $$F(z) = \sum_{k=0}^{+\infty} f(kT)z^{-k}$$

  - Iz metode 2 prehod ni mogoč!
  - Iz metode 3 dobimo:

    $$F(z) = \sum \text{residuumov } F(p)\frac{1}{1 - e^{Tp} \cdot z^{-1}} \text{ pri polih } F(p)$$

- Splošna oblika Z transformacije je "dvostranska"

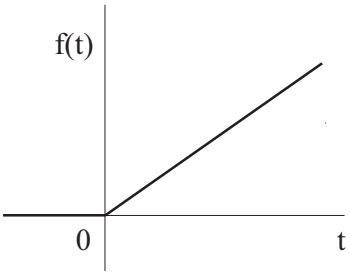
  $$F(z) = \mathcal{Z}\{f(k)\} = \sum_{k=-\infty}^{+\infty} f(kT)z^{-k} \quad ,$$

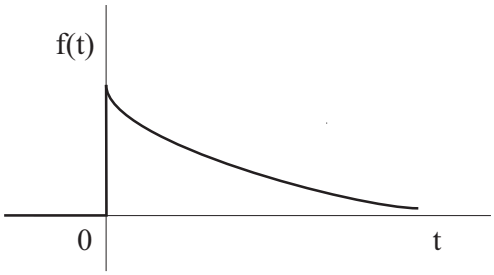
  saj je izbira začetka (običajno $k = 0$) poljubna.

PRIMER 55:

Po metodah 1 in 3 določite Z transformacijo dveh sekvenc, dobljenih s sempliranjem (s periodo T) naslednjih funkcij:

1. Enotina rampa $f(t) = t \cdot u(t)$
2. Eksponentna funkcija $f(t) = e^{-at}u(t)$





1. Enotina rampa

- Metoda 1:

$$f(kT) = kT, k = 0, 1, \ldots$$

$$F(z) = \sum_{k=0}^{\infty} kT \cdot z^{-k} = 0 + T \cdot z^{-1} + 2T \cdot z^{-2} + 3T \cdot z^{-3} + \cdots =$$

$$= T \cdot z^{-1}(1 + 2z^{-1} + 3z^{-2} + \cdots) =$$

$$= \frac{T \cdot z^{-1}}{(1 - z^{-1})^2} \quad , \quad \text{pogoj:} \quad |z^{-1}| < 1 \text{ oz. } z = r \cdot e^{i\phi}, |z| = r > 1,$$

- Metoda 3:

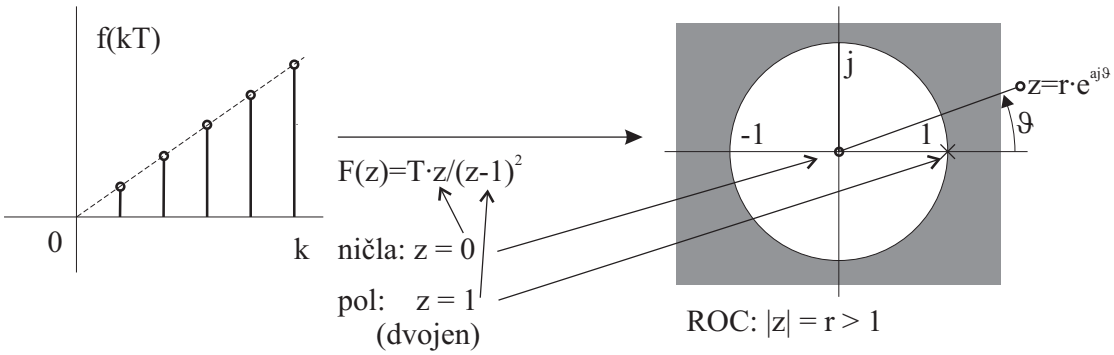
$$f(t) = t \cdot u(t) \rightarrow F(s) = \frac{1}{s^2}$$

$$F(z) = \sum \text{residuumov } \frac{1}{p^2} \cdot \frac{1}{1 - e^{Tp}z^{-1}} \text{ pri polu } p = 0 \text{ (dvojen)} =$$

$$= \frac{d}{dp}\left\{p^2[\frac{1}{p^2} \cdot \frac{1}{1 - e^{Tp}z^{-1}}]\right\}\Bigg|_{p=0} =$$

$$= \frac{T \cdot e^{Tp} \cdot z^{-1}}{(1 - e^{Tp} \cdot z^{-1})^2}\Bigg|_{p=0} =$$

$$= \frac{Tz^{-1}}{(1 - z^{-1})^2} = \frac{Tz}{(z - 1)^2}$$



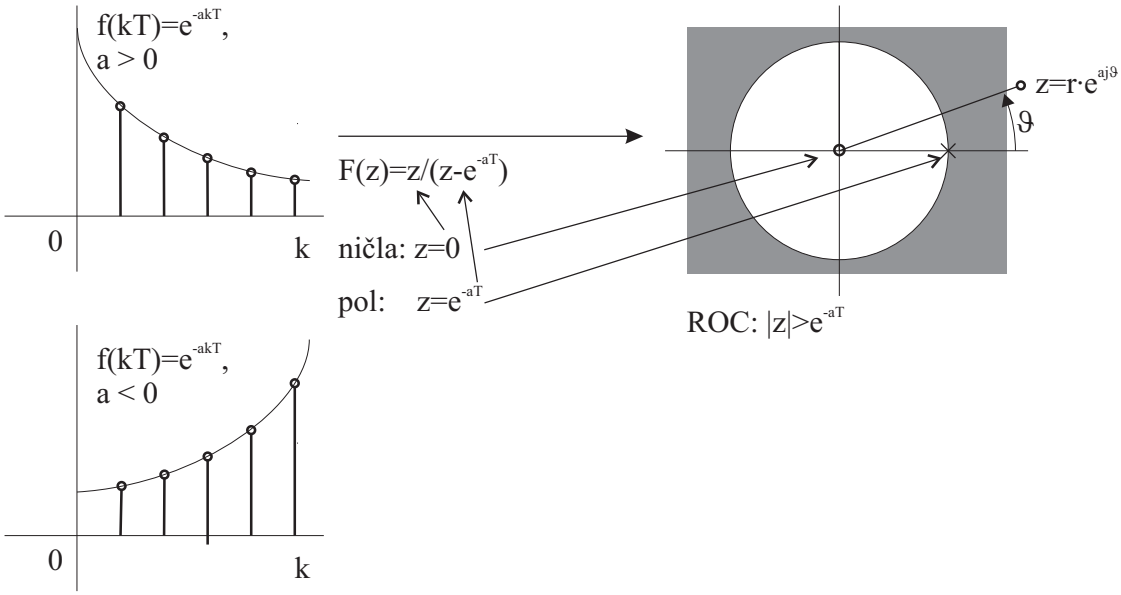
2. Eksponentna funkcija

   - Metoda 1:

$$
\begin{aligned}
f(kT) &= e^{-akT}, k = 0, 1, 2, \ldots \\
F(z) &= \sum_{k=0}^{+\infty} e^{-akT} \cdot z^{-k} = \\
&= 1 + e^{-aT} \cdot z^{-1} + (e^{-aT} \cdot z^{-1})^2 + (e^{-aT} \cdot z^{-1})^3 + \cdots = \\
&= \frac{1}{1 - e^{-aT} \cdot z^{-1}} \quad , \quad \text{pogoj: } |e^{-aT} \cdot z^{-1}| < 1 \text{ oz. } r > e^{-aT}
\end{aligned}
$$

   - Metoda 3:

$$
\begin{aligned}
f(kT) &= e^{-akT} \rightarrow F(s) = \frac{1}{s+a} \\
F(z) &= \sum \text{residuumov } \frac{1}{p+a} \cdot \frac{1}{1 - e^{Tp} \cdot z^{-1}} = \\
&= \left. \frac{1}{1 - e^{Tp} \cdot z^{-1}} \right|_{p=-a} \\
&= \frac{1}{1 - e^{-aT} z^{-1}} = \frac{z}{z - e^{-aT}}
\end{aligned}
$$



◇

- Pri **časovno pozitivnih** (kavzalnih) sekvencah je ROC (Region of Convergence) zunaj kroga z radijem, ki je enak razdalji od **najbolj oddaljenega pola** $F(z)$ do izhodišča. Tedaj se uporablja enostranska Z transformacija.

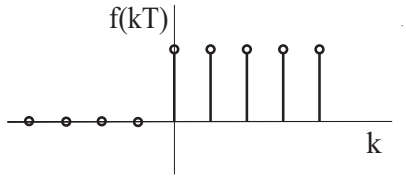
- Pri **časovno negativnih** sekvencah pa ima Z transformacija $F(z)$ ROC znotraj kroga, katerega radij je razdalja od **najbližjega pola** $F(z)$ do izhodišča.

- Pri **dvostranskih sekvencah** je ROC Z transforma $F(z)$ v kolobarju, katerega notranji radij je enak razdalji od izhodišča do najbolj oddaljenega pola pozitivnega dela funkcije, zunanji radij pa je enak razdalji od izhodišča do najbližjega pola negativnega dela funkcije.

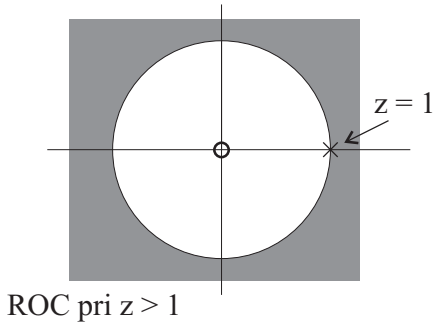
PRIMER 56:

Določimo Z transform za pozitivno sekvenco:

$$f(k) = u(k)$$



$$\begin{aligned} F(z) &= \sum_{k=-\infty}^{+\infty} f(kT) z^{-k} = \\ &= \sum_{k=0}^{+\infty} z^{-k} = \\ &= \frac{1}{1 - z^{-1}} \\ &= \underset{\substack{\uparrow \\ \text{ničla pri } z=0 \\ \text{pol pri } z=1}}{\frac{z}{z-1}} \end{aligned}$$

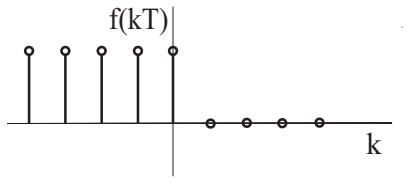


◇

PRIMER 57:

Določimo Z transform za negativno sekvenco:

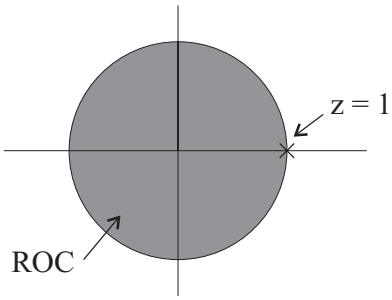
$$f(kT) = u(-k) = \begin{cases} 1, & k \leq 0 \\ 0, & k > 0 \end{cases}$$



$$F(z) = \sum_{k=-\infty}^{+\infty} f(kT) z^{-k}$$

Vzemimo: $l = -k$:

$$F(z) = \sum_{l=0}^{\infty} z^{l} = \underset{\substack{\uparrow \\ \text{pol pri } z=1}}{\frac{1}{1-z}}$$

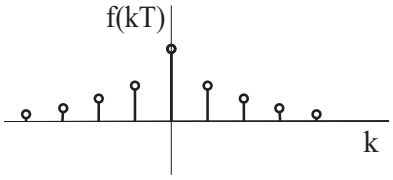


◇

PRIMER 58:

Za dvostransko sekvenco določimo Z transform in ROC.

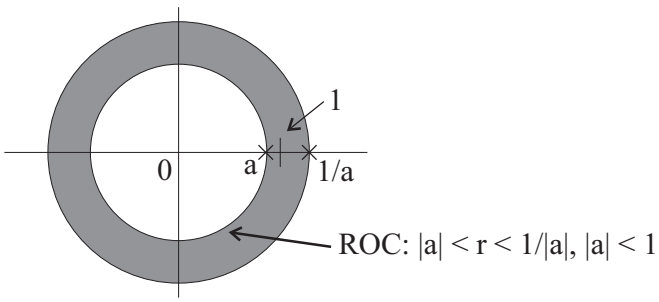
$$f(k) = a^{|k|} \quad , \quad |a| < 1 \ , \ a \in \mathbb{R}$$



$$\begin{aligned} F(z) &= \sum_{k=-\infty}^{\infty} a^{|k|} \cdot z^{-k} = \\ &= \sum_{k=-\infty}^{-1} a^{-k} \cdot z^{-k} + \sum_{k=0}^{\infty} a^{k} \cdot z^{-k} = \\ &\underset{\substack{\uparrow \\ -k=l}}{=} \underbrace{\sum_{l=0}^{\infty} a^l z^l}_{\substack{\downarrow \\ \textbf{Negativna funkcija:} \\ \text{konvergira k } \frac{1}{1-az}, \\ \text{pogoj: } |z|<\frac{1}{|a|}}} -1 + \underbrace{\sum_{k=0}^{\infty} a^k z^{-k}}_{\substack{\downarrow \\ \textbf{Pozitivna funkcija:} \\ \text{konvergira k } \frac{1}{1-az^{-1}}, \\ \text{pogoj: } |z|>|a|}} \end{aligned}$$

Sledi:

$$\begin{aligned} F(z) &= (\frac{1}{1-az} - 1) + \frac{z}{z-a} = \\ &= \underset{\substack{\downarrow \\ \text{pol: } |z|=r=\frac{1}{|a|}}}{\frac{az}{1-az}} + \underset{\substack{\downarrow \\ \text{pol: } |z|=r=|a|}}{\frac{z}{z-a}} = \frac{z(1-a^2)}{(1-az)(z-a)} \end{aligned}$$



Če bi bil $|a| > 1$, $F(z)$ ne bi nikjer v z polravnini konvergirala.

◇

12.4 Lastnosti Z transformacije

- Z transform:

$$F(z) = \sum_{k=-\infty}^{\infty} f(kT)z^{-k} = \mathcal{Z}\{f(k)\}$$

Inverzni transform:

$$f(k) = \mathcal{Z}^{-1}\{F(z)\}$$

- Lastnosti Z transformacije:

1. LINEARNOST

$$\mathcal{Z}\{\alpha_1 f_1(k) + \alpha_2 f_2(k)\} = \alpha_1 F_1(z) + \alpha_2 F_2(z)$$

2. ČASOVNI ZAMIK ALI TRANSLACIJA:
   (a) Če $F(z) = \mathcal{L}\{f(k)\}$ in je začetni pogoj za $f(k)$ enak 0, potem je:

$$\mathcal{Z}\{f(k-m)\} = z^{-m} \cdot F(z), m \text{ je pozitivno ali negativno celo število}$$

   (b) Če $F(z) = \mathcal{Z}_1\{f(k)\}$ (enostranska funkcija), potem:

$$\mathcal{Z}_1\{f(k-m)\} = z^{-m} \cdot \{F(z) + \sum_{p=1}^{m} f(-p)z^{p}\}$$

$$\mathcal{Z}_1\{f(k+m)\} = z^{m} \cdot \{F(z) - \sum_{p=0}^{m-1} f(p)z^{-p}\}$$

3. MNOŽENJE z a^k:
   Če $F(z) = \mathcal{Z}\{f(k)\}$ (dvostranska funkcija), potem:

$$\mathcal{Z}\{a^k f(k)\} = F(a^{-1} \cdot z), \quad a \text{ je realno ali kompleksno število.}$$

4. ČASOVNI OBRAT:
   Če $F(z) = \mathcal{Z}\{f(k)\}$, potem:

$$\mathcal{Z}\{f(-k)\} = F(z^{-1})$$

5. MNOŽENJE S ČASOVNIM INDEKSOM:
   Če $F(z) = \mathcal{Z}\{f(k)\}$, potem:

$$\mathcal{Z}\{kf(k)\} = -z\frac{dF(z)}{dz}$$

6. KONVOLUCIJSKI TEOREM:
   Če $F(z) = \mathcal{Z}\{f(k)\}$ in $G(z) = \mathcal{Z}\{g(k)\}$, potem:

$$\mathcal{Z}\{f(k) * g(k)\} = F(z) \cdot G(z)$$

7. KOMPLEKSNI KONVOLUCIJSKI TEOREM:
   Če $x_3(n) = x_1(n) \cdot x_2(n)$, potem:
   $$X_3(z) = \frac{1}{2\pi j} \oint_c X_2(\nu) X_1(\frac{z}{\nu}) \nu^{-1} d\nu$$
8. TEOREM ZAČETNE VREDNOSTI:
   Če $F(z) = \mathcal{Z}_1\{f(k)\}$, potem:
   $$f(0) = \lim_{z \to \infty} F(z)$$
9. TEOREM KONČNE VREDNOSTI:
   Če $F(z) = \mathcal{Z}_1\{f(k)\}$, potem:
   $$f(\infty) = \lim_{z \to 1} (z-1) F(z)$$
   Pogoj: ROC za $F(z)$: $|z| > 1$ in $(z-1) \cdot F(z)$ nima polov na enotinem krogu in izven njega.

- Transforme ali njihove inverze lahko izračunamo s pomočjo znanih transformov:

Sekvenca	$f(kT), k \geq 0$	$F(z)$
Enotin pulz	$\delta(k)$	1
Enotina stopnica	$u(kT)$	$\frac{z}{z-1}$
Enotina rampa	kT	$\frac{Tz}{(z-1)^2}$
Eksponentna fun.	e^{-akT}	$\frac{z}{z-e^{-aT}}$
Potenca	a^k	$\frac{z}{z-a}$
Sinus	$\sin \omega_0 kT$	$\frac{z \sin \omega_0 T}{z^2 - 2z \cos \omega_0 T + 1}$
Kosinus	$\cos \omega_0 kT$	$\frac{z(z - \cos \omega_0 T)}{z^2 - 2z \cos \omega_0 T + 1}$
Dušeni sinus	$e^{-akT} \cdot \sin \omega_0 kT$	$\frac{z \cdot e^{-aT} \cdot \sin \omega_0 T}{z^2 - 2ze^{-aT} \cdot \cos \omega_0 T + e^{-2aT}}$
Dušeni kosinus	$e^{-akT} \cdot \cos \omega_0 kT$	$\frac{z^2 - z \cdot e^{-aT} \cdot \cos \omega_0 T}{z^2 - 2ze^{-aT} \cdot \cos \omega_0 T + e^{-2aT}}$

- Za izračun inverzne Z transformacije $f(k) = \mathcal{Z}^{-1}\{F(z)\}$ si bomo ogledali dve metodi:
  1. Razširitev v delne ulomke
     Imenovalec najprej zapišemo v faktorsko obliko. Nato $F(z)$ razširimo v delne ulomke (glej inverzno Laplaceovo transformacijo). Iz tabele za posamezne člene dobimo ustrezne inverzne transformacije, ki jih moramo še sešteti, da dobimo $f(k)$.
  2. Residualna metoda
     Ob upoštevanju Cauchyjevega teorema ($\int_c f(z)dz = 2\pi j \sum \text{residuumov} f(z)$) in predpostavki, da c zapira izhodišče z ravnine, velja:
     $$\begin{aligned} f(k) &= \mathcal{Z}^{-1}\{F(z)\} \\ &= \frac{1}{2\pi j} \oint_c F(z) z^{k-1} dz = \\ &= \sum \text{residuumov } F(z) \cdot z^{k-1} \text{ pri polih } F(z) \cdot z^{k-1} \text{ znotraj } c \end{aligned}$$

PRIMER 59:

1. Za dano funkcijo $F(z)$ določi $f(k)$.

$$F(z) = \frac{z+0{,}2}{(z+0{,}5)(z-1)} \quad , \quad |z| > 1 \text{ (pozitivna funkcija)}$$

$$\begin{aligned}
F(z) &= \frac{R_1}{z+0{,}5} + \frac{R_2}{z-1} = \\
R_1 &= (z+0{,}5)\cdot F(z)|_{z=-0{,}5} = 0{,}2 \\
R_2 &= (z-1)\cdot F(z)|_{z=1} = 0{,}8 \\
F(z) &= \frac{0{,}2}{z+0{,}5} + \frac{0{,}8}{z-1} \quad \backslash \cdot z \\
z\cdot F(z) &= \frac{0{,}2z}{z+0{,}5} + \frac{0{,}8z}{z-1}
\end{aligned}$$

Z uporabo lastnosti časovnega zamika (lastnost 2) dobimo:

$$f(k+1) = \begin{cases} 0{,}2\cdot(-0{,}5)^k + 0{,}8, & k \geq 0 \\ 0, & k < 0 \end{cases}$$

Od tod sledi:

$$f(0) = 0, f(1) = 1, f(2) = 0{,}7, f(3) = 0{,}85, f(4) = 0{,}775, \ldots$$

2. Za dano negativno funkcijo $F(z)$ določi $f(k)$:

$$F(z) = \frac{z}{(z-3)(z-4)} \quad , \quad |z| < 3 \text{ (negativna funkcija)}$$

$$\begin{aligned}
F(z) &= \frac{R_1}{z-3} + \frac{R_2}{z-4} \\
R_1 &= (z-3)\cdot F(z)|_{z=3} = -3 \\
R_2 &= (z-4)\cdot F(z)|_{z=4} = 4 \\
F(z) &= \frac{-3}{z-3} + \frac{4}{z-4} = \\
&= \frac{1}{1-\frac{1}{3}z} - \frac{1}{1-\frac{1}{4}z} = \\
&= \frac{z^{-1}}{z^{-1}-\frac{1}{3}} - \frac{z^{-1}}{z^{-1}-\frac{1}{4}}
\end{aligned}$$

Z ulomki inverznega časovnega obrata (lastnost 4) dobimo:

$$\begin{aligned} f(k) &= \mathcal{Z}^{-1}\{\frac{z^{-1}}{z^{-1}-\frac{1}{3}}\} - \mathcal{Z}^{-1}\{\frac{z^{-1}}{z^{-1}-\frac{1}{4}}\} = \\ &= (\frac{1}{3})^{-k} - (\frac{1}{4})^{-k} = \\ &= 3^k - 4^k, k \leq 0 \end{aligned}$$

Od tod sledi $f(0) = 0, f(-1) = \frac{1}{12}, f(-2) = \frac{7}{144}, f(-3) = \frac{37}{1728}, \ldots$

3. Za dvostransko funkcijo $F(z)$ določi $f(k)$:

$$F(z) = \frac{z}{(z-0{,}5)(z-2)} \quad , \quad 0{,}5 < |z| < 2$$

$$\begin{aligned} F(z) &= \frac{R_1}{z-0{,}5} + \frac{R_2}{z-2} \\ R_1 &= (z-0{,}5)F(z)|_{z=0{,}5} = -\frac{1}{3} \\ R_2 &= (z-2)F(z)|_{z=2} = \frac{4}{3} \\ F(z) &= -\frac{1}{3(z-0{,}5)} + \frac{4}{3(z-2)} = \\ &= \underset{\text{čas. pozitivna fun.}}{\underset{\downarrow}{F_+(z)}} + \underset{\text{čas. negativna fun.}}{\underset{\downarrow}{F_-(z)}} \end{aligned}$$

Časovno pozitivna funkcija:

$$\begin{aligned} z \cdot \underset{\downarrow \text{lastnost 2}}{F_+(z)} &= -\frac{z}{3(z-0{,}5)} \\ f(k+1) &= -\frac{1}{3}(0{,}5)^k \longrightarrow f(k) = -\frac{2}{3}(0{,}5)^k \quad , \quad k \geq 0 \end{aligned}$$

Torej $f(1) = -\frac{1}{3}, f(2) = -\frac{1}{6}, f(3) = -\frac{1}{12}, \ldots$
Časovno negativna funkcija:

$$\begin{aligned} F_-(z) &= \frac{4}{3(z-2)} = -\underset{\downarrow \text{lastnost 4}}{\frac{2z^{-1}}{3(z^{-1}-0{,}5)}} \\ f(k) &= -\frac{2}{3}(0{,}5)^{-k} = -\frac{2}{3}2^k, k \leq 0 \end{aligned}$$

Po združitvi dobimo:

$$f(k) = \begin{cases} -\frac{2}{3}(0{,}5)^k, & k > 0 \\ -\frac{2}{3}2^k, & k \leq 0 \end{cases}$$

◇

PRIMER 60:

Za dano funkcijo $F(z) = \frac{z+0{,}2}{(z+0{,}5)(z-1)}, |z| > 1$ (pozitivna funkcija) določite $f(z)$ z residualno metodo.

$$\sum \text{residuumov } \frac{(z+0{,}2)z^{k-1}}{(z+0{,}5)(z-1)} \text{ pri njenih polih znotraj } c$$

Krivulja c zapira v področju ROC ($|z| > 1$) pole pri $z = -0{,}5$ in $z = 1$ in pri $k = 0$ pol $z = 0$.

Za $k = 0$ velja:

$$\begin{aligned} f(0) &= \left.\frac{z+0{,}2}{(z+0{,}5)(z-1)}\right|_{z=0} + \left.\frac{z+0{,}2}{z(z-1)}\right|_{z=-0{,}5} + \left.\frac{z+0{,}2}{z(z+0{,}5)}\right|_{z=1} = \\ &= -0{,}4 - 0{,}4 + 0{,}8 = 0 \end{aligned}$$

Za $k \geq 1$:

$$\begin{aligned} f(k) &= \left.\frac{z^{k-1}(z+0{,}2)}{z-1}\right|_{z=-0{,}5} + \left.\frac{z^{k-1}(z+0{,}2)}{z+0{,}5}\right|_{z=1} = \\ &= 0{,}2(-0{,}5)^{k-1} + 0{,}8 \end{aligned}$$

Sledi:

$$f(0) = 0, f(1) = 1, f(2) = 0{,}7, f(3) = 0{,}805, f(4) = 0{,}7975, \ldots$$

◇

12.5 Reševanje diferenčnih enačb z Z transformacijo

Metoda reševanja diferenčnih enačb z Z transformacijo je primerna za sisteme višjih redov, kjer induktivna metoda odpove.

PRIMER 61:

Določite y_k za rekurzivni digitalni filter prvega reda, ki ga podaja enačba:

$$\begin{aligned} y_k &= Ay_{k-1} + x_k \\ x_k &= u_k \end{aligned}$$

Uporabite Z transformacijo.

1. Enačbo množimo z z^{-k} in jo seštejemo od 0 do ∞:

$$\sum_{k=0}^{\infty} y_k z^{-k} = A \sum_{k=0}^{\infty} y_{k-1} z^{-k} + \sum_{k=0}^{\infty} x_k z^{-k}$$

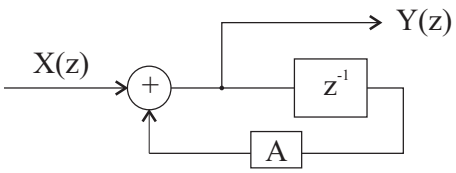
$$
\begin{aligned}
A\sum_{k=0}^{\infty} y_{k-1}\cdot z^{-k} &= Ay_{-1} + Az^{-1}\sum_{k=1}^{\infty} y_{k-1}\cdot z^{-(k-1)} \\
&= Ay_{-1} + Az^{-1}\sum_{l=0}^{\infty} y_l z^{-l} \quad , \quad l = k-1 \\
&= Ay_{-1} + Az^{-1}\cdot Y(z)
\end{aligned}
$$

Ker je $Y(z) = \sum_{k=0}^{\infty} y_k z^{-k}$ in $X(z) = \sum_{k=0}^{\infty} x_k z^{-k}$ lahko zapišemo

$$
\begin{aligned}
Y(z) &= Ay_{-1} + Az^{-1}Y(z) + X(z) \\
Y(z) &= \frac{X(z)}{1-Az^{-1}} + \frac{Ay_{-1}}{1-Az^{-1}}
\end{aligned}
$$

Če je $y_{-1} = 0$, velja:

$$
H(z) = \frac{Y(z)}{X(z)} = \frac{1}{1-Az^{-1}} = \frac{z}{z-A}
$$



2. Izvedemo inverzno Z transformacijo nad enačbo za $Y(z)$ po eni od obeh omenjenih metod.

$$
\begin{aligned}
X(z) &= \frac{z}{z-1} \qquad \text{(Z transform enotine stopničaste sekvence } x_k = u_k\text{)} \\
Y(z) &= \frac{X(z)}{1-Az^{-1}} + \frac{Ay_{-1}}{1-Az^{-1}} \\
Y(z) &= \frac{z^2}{(z-1)(z-A)} + \frac{Ay_{-1}z}{z-A} \quad , \quad |z| > 1 \text{ (časovno pozitivna funkcija)}
\end{aligned}
$$

Residualna metoda:

$$
y(k) = \sum \text{resid.}\underbrace{\frac{z^2\cdot z^{k-1}}{(z-1)(z-A)}}_{\text{prvi člen}} + \sum \text{resid.}\underbrace{\frac{A\cdot y_{-1}\cdot z\cdot z^{k-1}}{z-A}}_{\text{drugi člen}} \quad , \quad |z| > 1
$$

Prvi člen:

$$
\begin{aligned}
k = 0 : y_1(0) &= \left.\frac{z}{z-A}\right|_{z=1} + \left.\frac{z}{z-1}\right|_{z=A} = \frac{1}{1-A} + \frac{A}{A-1} = 1 \\
k \geq 1 : y_1(k) &= \left.\frac{z^2\cdot z^{k-1}}{z-A}\right|_{z=1} + \left.\frac{z^2\cdot z^{k-1}}{z-1}\right|_{z=A} = \frac{1}{1-A} + \frac{A^2\cdot A^{k-1}}{A-1} = \frac{1-A^{k+1}}{1-A} \\
k \geq 0 : y_1(k) &= \frac{1-A^{k+1}}{1-A}
\end{aligned}
$$

Drugi člen:

$$
\begin{aligned}
&k = 0 : y_2(0) = A \cdot y_{-1} \\
&k \geq 1 : y_2(k) = Ay_{-1}z \cdot z^{k-1}|_{z=A} = A^2 y_{-1} A^{k-1} = y_{-1} A^{k+1} \\
&k \geq 0 : y_2(k) = y_{-1} A^{k+1}
\end{aligned}
$$

Vsoti združimo:

$$y(k) = y_1(k) + y_2(k) = \frac{1 - A^{k+1}}{1 - A} + A^{k+1} \cdot y_{-1}, k \geq 0$$

Če $|A| < 1$ je v limiti: $\lim_{k \to \infty} y(k) = \frac{1}{1-A}$

Če $|A| > 1$, $y(k)$ divergira s naraščajočim k.

$\diamond$

Literatura

[1] N. Pavešič, Informacija in kodi, Založba FE in FRI, Ljubljana, 1997.

[2] E. P. Cunningham, Digital Filtering: An Introduction, Houghton Mifflin Company, Boston, 1992.

[3] M. J. Chapman, D. P. Goodalf, N. C. Steele, Signal Processing in Electronic Communications, Horwood Publishing, 1997.

[4] J. C. A. van der Lubbe, Information Theory, Cambridge University Press, Cambridge, 1997.