

## Ponovitev analize

## Odvodi

1.  $\frac{1}{x} = -\frac{1}{x^2}$
2.  $x^n = nx^{n-1}$
3.  $\sqrt{x} = \frac{1}{2\sqrt{x}}$
4.  $\sqrt[n]{x} = \frac{1}{n\sqrt[n]{x^{n-1}}}$
5.  $\sin(ax) = a \cos ax$
6.  $\cos(ax) = -a \sin(ax)$
7.  $\tan x = \frac{1}{\cos^2 x}$
8.  $e^a x = ae^{ax}$
9.  $a^x = a^x \ln a$
10.  $x^x = x^x(1 + \ln x)$
11.  $\ln x = \frac{1}{x}$
12.  $\log_a x = \frac{1}{x \ln a}$
13.  $\arcsin x = \frac{1}{\sqrt{1-x^2}}$
14.  $\arccos x = -\frac{1}{\sqrt{1-x^2}}$
15.  $\arctan x = \frac{1}{1+x^2}$
16.  $\operatorname{arccot} x = -\frac{1}{1+x^2}$

## Integrali

1.  $\int x^a dx = \begin{cases} \frac{x^{a+1}}{a+1} + C & a \neq -1 \\ \ln|x| + C & a = -1 \end{cases}$
2.  $\int \ln x dx = x \ln x - x + C$
3.  $\int \frac{1}{\sqrt{x}} dx = 2\sqrt{x} + C$
4.  $\int e^x dx = e^x + C$
5.  $\int a^x dx = \frac{a^x}{\ln a} + C$
6.  $\int \cos(ax) dx = \frac{\sin(ax)}{a} + C$
7.  $\int \sin(ax) dx = \frac{-\cos(ax)}{a} + C$
8.  $\int \tan x dx = -\ln|\cos x| + C$
9.  $\int \frac{dx}{\cos^2 x} = \int \sec^2 x dx = \tan x + C$
10.  $\int \frac{dx}{\sin^2 x} = \int \csc^2 x dx = -\cot x + C$
11.  $\int \frac{1}{\sqrt{1-x^2}} dx = \arcsin x + C$
12.  $\int \frac{dx}{ax+b} = \frac{1}{a} \ln|ax+b| + C$
13.  $\int \frac{1}{x^2+1} dx = \arctan x + C$
14.  $\int \frac{dx}{x^2+a^2} = \frac{1}{a} \arctan \frac{x}{a} + C$
15.  $\int \frac{f'(x)}{f(x)} dx = \ln|f(x)| + C$

**Integriranje absolutnih vrednosti** (primer): Imamo funkcijo  $f(x) = |x|$ , ki je zvezna na intervalu  $[-1, 1]$ . Če hocemo to funkcijo integrirati in zelimo izračunati njeno *porazdelitveno* funkcijo integrirati locimo 2 primera:

1.  $-1 \leq x < 0$   

$$F(x) = \int_{-1}^x |t| dt = \int_{-1}^x -t dt = -\frac{t^2}{2} \Big|_{-1}^x = -\frac{1}{2}(x^2 - 1)$$
2.  $0 \leq x < 1$   

$$F(x) = \int_{-1}^x |t| dt = \int_{-1}^0 -t dt + \int_0^x t dt = -\frac{t^2}{2} \Big|_{-1}^0 + \frac{t^2}{2} \Big|_0^x = \frac{1}{2}(1 + x^2)$$

$$\sqrt[n]{x^m} = (x)^{\frac{m}{n}}, x^2 + y^2 \leq 1 \sim \text{krog s ploscino } \pi$$

## 1 Osnove

## 1.1 Ponovitev logaritmov

- $\log_a x = \frac{\log_b x}{\log_b a}$
- $\log_b\left(\frac{x}{y}\right) = \log_b x - \log_b y$
- $x = b^y \implies \log_b x = y$
- $\log_2 x = \log x$
- $0 \log 0 = 0$

## 1.2 Bayesova formula

$$\begin{aligned} P(H_i|A) &= \frac{P(H_i)P(A|H_i)}{P(A)} = \\ &= \frac{P(H_i)P(A|H_i)}{\sum_{k=1}^n P(H_k)P(A|H_k)} \end{aligned}$$

## 1.3 Lastna informacija

Opisuje dogodek, ki se je zgodil:

$$I_i = \log_2\left(\frac{1}{p_i}\right) = -\log_2(p_i)$$

## 1.4 Entropija

je povprečje vseh lastnih informacij:

$$H(X) = \sum_{i=1}^n p_i I_i = -\sum_{i=1}^n p_i \log_2 p_i$$

Lastnosti:

1. je zvezna, simetrična funkcija (vrtni red  $p_i$  ni pomemben, seštevanje je komutativno).
2.  $p_i \geq 0 \rightarrow -p_i \log_2 p_i \geq 0 \Rightarrow H(X) \geq 0$
3. je navzgor omejena z  $\log_r n$ .

Če sta dogodka **neodvisna** velja aditivnost:  $H(X, Y) = H(X) + H(Y)$ .

Vec zaporednih dogodkov neodvisnega vira:  $X^l = X \times \dots \times X \rightarrow H(X^l) = lH(X)$ .

## 2 Kodi

## 2.1 Uvod

**Kod** sestavljajo *kodne zamenjave*, ki so sestavljene iz znakov **kodne abecede**. Število znakov v kodni abecedi označujemo z **r**.

Ce so  $\{p_1, \dots, p_n\}$  verjetnosti znakov  $\{s_1, \dots, s_n\}$  osnovnega sporočila in  $\{l_1, \dots, l_n\}$  dolžine prejetih kodnih zmanjav, je povprečna dolžina kodne zamenjave

$$L = \sum_{i=1}^n p_i l_i$$

## 2.2 Tipi kodov

- **optimalen** - ce ima najmanjšo možno dolžino kodnih zamenjav
- **idealni** - ce je povprečna dolžina kodnih zamenjav enaka entropiji
- **enakomeren** - ce je dolžina vseh kodnih zamenjav enaka
- **enoznačen/enolichen** - ce lahko poljuben niz znakov dekodiramo na en sam način
- **trenuten** - ce lahko osnovni znak dekodiramo takoj, ko sprejmemo celotno kodno zamenjavo

2.3 Kraftova neenakost

Za dolzine kodnih zamenjav  $\{l_1, \dots, l_n\}$  in  $r$  znaki kodne abecede obstaja trenutni kod, iff

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

Kraftova neenakost je **potrebni** pogoj za trenutnost koda. **Za-**  
**dosten** pogoj za trenutnost koda: Nobena kodna zamenjava **ni** pred-  
pona drugi.

2.4 Povp. dolzina, ucinkovitost

Najkrajse kodne zamenjave imamo, ce velja:

$$H_r(X) = L \rightarrow l_i = \lceil -\log_r p_i \rceil$$

Ucinkovitost koda:

$$\eta = \frac{H(X)}{L \log_2 r}, \eta \in [0, 1]$$

Kod je **gospodaren**, ce je  $L$  znotraj:

$$H_r(X) \leq L < H_r(X) + 1$$

Ce pa imamo vec neodvisnih znakov:  
kjer je  $H_r(X)$ :

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

2.5 Shannonov prvi teorem

Za nize neodvisnih znakov dozline  $n$  obstajajo kodi, za katere velja:

$$\lim_{n \rightarrow \infty} \frac{L_n}{n} = H(X)$$

pri cemer je  $H(X)$  entropija vira  $X$ . Neformalno: *Vec znakov kot bomo združevali, bolj se bomo priblizali entropiji.*

$\Rightarrow$  Posledica prvega Shannonovega teorema, ce združujemo znake v vecje, sestavljene znake potem velja:

$$\begin{aligned} H_r(X^n) &\leq L_n < H_r(X^n) + 1 \\ nH_r(X) &\leq L_n < nH_r(X) + 1 \\ H_r(X) &\leq \frac{L_n}{n} < H_r(X) + \frac{1}{n} \end{aligned}$$

2.6 Shannonov kod

Postopek kodiranja po Shannonu:

1. znake razvrstimo po padajocih verjetnostih
2. dolocimo stevilo znakov v vsaki kodni zamenjavi ( $l_k$ )
3. za vse simbole izracunamo komulativne verjetnosti ( $P_k = \sum_{i=1}^{k-1} p_i$ )
4.  $P_k$  pretvorimo v bazo  $r$ . Kodno zamenjavo predstavlja prvih  $l_k$  znakov necelega dela stevila

2.7 Fanojev kod

Postopek kodiranja:

1. znake razvrstimo po padajocih verjetnostih
2. znake razdelimo v  $r$  cim bolj enako verjetnih skupin
3. Vsaki skupini priredimo enega od  $r$  znakov kodne abecede
4. Deljenje ponovimo na vsaki od skupin. Postopek ponavljamo, dokler je mogoce

$l_i$  dolocimo s pomocjo tabele.

2.8 Huffmanov kod

Huffmanov postopek kodiranja poteka od spodaj navzgor (Pri Fanoju je ravno obratno). Pri huffmanovem kodu imamo dve fazi:

1. Združevanje
  - (a) Posici  $r$  najmanj verjetnih znakov in jih zdruzi v sestavljeni znak, katerega verjetnost je vsota verjetnosti vseh znakov
  - (b) Preostale znake skupaj z novo sestavljenim znakom spet razvrsti
  - (c) Postopek ponavlja dokler ne ostane samo  $r$  znakov
2. Razdruževanje
  - (a) Vsakemu od preostalih znakov priredi po en znak kodirne abecede
  - (b) Vsak sestavljeni znak razstavi in mu priredi po en znak kodirne abecede
  - (c) Ko zmanjka sestavljenih znakov, je postopek zaključen

Pred kodiranjem, je vedno pametno preveriti, ce imamo zadostno stevilo znakov. Veljati mora:

$$n = r + k(r - 1), k \geq 0$$

Ce imamo premalo znakov, jih po potrebi dodamo s verjetnostjo  $p = 0$ .

Huffmanov kod lahko razsirimo tako, da vec osnovnih znakov združujemo v sestavljene znake  $\rightarrow$  bolj ucinkoviti kodi. Vendar naletimo na nevarnost kombinacijske eksplozije.  $l_i$  dolocimo s pomocjo tabele.

2.9 Aritmetichni kod

Je **hiter** in **blizu optimalnemu** kodu, ter manj ucinkovit kot Huffmanov, vendar se izogne kombinacijski eksploziji. Aritmetichni kod ni **gospodaren** saj zanj velja:

$$\mathcal{H}(X) \leq L_n \leq \mathcal{H}(X) + 2$$

Sepravi se nam lahko zgodi, da pri kodiranju niza uporabimo dva znaka prevec.

Vsak niz je predstavljen kot realno stevilo  $0 \leq R < 1$ , kar nam pove, da daljsi kot bo niz, bolj natančno mora biti podano naravno stevilo  $R$ .

Postopek kodiranja(znakov ni potrebno razvrstiti):

1. Zaczemo z intervalom  $[0, 1)$
2. Izbrani interval razdelimo na  $n$  podintervalov, ki se ne prekrivajo. Sirine podintervalov ustrezajo verjetnostim znakov. Vsak podinterval predstavlja en znak
3. Izberemo podinterval, ki ustreza iskanemu znaku
4. Ce niz se ni koncan, izbrani podinterval ponovno razdelimo (bne 2.tocka)
5. Niz lahko predstavimo s poljubnim realnim stevilom v zadnjem podintervalu

Ko dobimo realni interval, ga samo se pretvorimo v binarnega s pomocjo klasicnega pretvarjanja iz dec v bin stevilski sistem.

2.9.1 Dekodiranje

Recimo, da dobimo k.z. 0101. Potem sta spodnji in zgornji meji izracunani na naslednji nacin  
sp. meja:  $0.0101 \rightarrow 2^{-2} + 2^{-4}$   
zg. meja:  $0.0110 \rightarrow 2^{-2} + 2^{-3}$ (sp. meja + 1) Nato binarno razdeljujemo mejo. Ustavimo se ko zapolnimo eno izmed mej.

2.10 Kod Lempel-Ziv (LZ77)

Stiskanje temelji na osnovi slovarja, tako, da ne potrebujemo racunati verjetnosti za posamezne znake. **Kodirnik** med branjem niza gradi slovar, in **dekodirnik** med branjem kodnih zamenjav rekonstruira slovar in znake.

**Kodiranje:** uporablja drseca okna, znaki se premikajo iz desne na levo. Referenca je podana kot trojcek:

- odmik - razdalja do zacetka enakega podniza v medpomnilniku
- dolzina enakega podniza
- naslednji znak

npr. (0, 0, A) - ni ujemanja, (4, 3, B) - 4 znake nazaj se ponovi 3 znakovni podniz, ki se nato zakljuci s B.

**dekodiranje:** sledimo kodnim zamenjavam

2.11 Deflate

Gre za predelan LZ77. Uporablja pare (odmik, dolzina). Ce uje-manja v kodni tabeli ni, zapise kar znak. Uporablja dve kodni tabeli:

- tabela za znake in dolzine** - 285 simbolov (0-255 za osnovne znake, 256 konec bloka, 257-285 kodira dolzine) Kodne zamen-jave brez dodatnih bitov, se zakodira s Huffmanom.
- tabela odmikov**

Niz znakov se razdeli na bloke(64k) vsak blok se kodira na enega od treh nacinov:

- brez stiskanja** osnovni znaki se prepisejo
- stiskanje s staticnim Huffmanom** (verjetnosti podane vnaprej), Huffmanovo drevo ni zakodirano v bloku
- stiskanje s Huffmanom** izracunamo verjetnosti za vsak blok

Glava posameznega bloka: 1bit - zadnji/ni zadnji blok + 2bita tip stiskanja + pri (3) se Huffmanovo drevo Ker Huffmanovo drevo ni enolicno, uvedemo kanonicni Huffmanov kod.

2.11.1 Kanonicni Huffmanov kod

Postopek kodiranja:

- znake razvrstimo najprej po dolzinah kodnih zamenjav in nato po abecedi(narascujoce)
- prvi simbol ima same nicle
- vsakemu naslednjemu znaku dodelimo naslednjo binarno kodo (prejsnji + 1)
- ce je kodna zamenjava daljsa od binarne kode stevila, na koncu pripnemo niclo
- ponavljaj (3) do konca

Na taksen nacin dosežemo, da je potrebno kodirati samo dolzine kod-nih zamenjav.

2.12 Kod Lempel-Ziv (LZW)

Osnovni slovar je podan in ga sporti doponjujemo. Alogritem za **kodiranje:**

```
N = ""
ponavljaj:
  preberi naslednji znak z
  ce je [N,z] v slovarju:
    N = [N, z]
  drugace:
    izpisi indeks k niza N
    dodaj [N, z] v slovar
    N = z
izpisi indeks k niza N
```

Algoritem za **dekodiranje:**

```
preberi indeks k
poiisci niz N, ki ustreza indeksu k
izpisi N
L = N
ponavljaj:
  preberi indeks k
  ce je k v slovarju:
    poiisci niz N
  drugace:
    N = [L, L(1)]
  izpisi N
  v slovar dodaj [L, N(1)]
  L = N
```

LZW doseže optimalno stiskanje, približa se entropiji.

2.13 Verizno kodiranje ali RLE (run lenght en-coding)

Namesto originalnih podatkov, sharnjujemo dolzino verige (fffeef → 3f2e1f). Problemu, ko se podatki ne ponavljajo, se izognemo tako, da izvedemo kombinacijo direktnega kodiranja in kodiranja RLE.

2.14 Stiskanje z izgubami

S taksnim nacinom stiskanja lahko dosežemo veliko boljša kompresi-jška razmerja, vendar izgubimo podatke. Zato ga uporabljamo samo s formati, kjer se ne ukvarjamo z integriteto podatkov(MP3, MPEG, JPEG, ...). Postopki kodiranj znanih formatov:

- JPEG**
  - priprava slike → ker je svetlost bol pomembna, je barvna resolucija obicajno zmanjsana ( $YC_R C_B$ )
  - aproksimacija vsake od treh komponent s 2D DCT
  - kvantizacija → podatki ki bolj izstopajo so shranjeni manj natančno kot tisti ki so staticni
  - kodiranje blokov s pomocjo entropije
  - RLE cik-cak po sliki
  - RLE kodiramo z Huffmanom ali Aritmenticnim kodom
- MP3**
  - Modified DCT
  - odstranitev za cloveka neslisnih frekvenc
  - stereo, ce sta si L in R pretvorimo v mono
  - Huffman na koncu
- MPEG**
  - uvodno kodiranje → celotna slika JPEG
  - nato pa kodiramo samo spremembe, ki so se zgodile v sliki JPEG s pomocjo vektorja premika. V primeru, da je pre-vec razlik, se ponovno kodira JPEG slika.

2.15    Kompresijsko razmerje

Izracunamo ga po formuli  $\rightarrow$  stisnjeni binarni zapis  $C(M)$  / binarni zapis dokumenta  $(M)$ :

$$R = C(M)/M$$

3    Kanali

3.1    Uvod

Kanali so strukture, ki opisujejo medsebojno povezanost. Kanal prenaša informacijo o spemenljivki  $X$  do spremenljivke  $Y$ . Matematically ga opisemo s **pogojnimi verjetnostmi**, ki povezujejo izhodne verjetnosti z vhodom.

3.2    Diskretni kanal brez spomina

Povezuje diskretni naključni spremenljivki, s končno množico stanj  $X = \{x_1, \dots, x_r\}$  in  $Y = \{y_1, \dots, y_s\}$ . Obema naključnima spremenljivkama pripadajo tudi posamezne verjetnosti  $P_X = \{p(x_1), \dots, p(x_r)\}$  in  $P_Y = \{p(y_1), \dots, p(y_s)\}$ . Kjer velja, da je vsota posamezne množice verjetnosti enaka 1. Kanal je definiran kot množica **pogojnih verjetnosti**

$$p(y_j|x_i).$$

Pogojna verjetnost nam pove verjetnost za dogodek  $y_j$  na izhodu iz kanala, če je na vhodu v kanal dogodek  $x_i$ . Brez spomina je zato, ker so pogojne vrjetnosti konstantne in torej neodvisne od prehodnih simbolov, velja

$$\sum_j p(y_j|x_i) = 1.$$

Kanal popolnoma podamo z  $r \times s$  pogojnimi verjetnostmi.

3.2.1    Binarni simetrični kanal (BSK)

Gre za poseben primer diskretnega kanala brez spomina. Napaka kanala je  $p$ , saj se z verjetnostjo  $p$  znak prenese v napacnega.

$$P_k = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$$

3.3    Pogojna entropija

Pogojna entropija spremenljivke  $Y$  pri znanem  $X$  se zapise kot  $H(Y|X)$ . Vzemimo, da se je zgodil dogodek  $x_i \in X$ . Entropija dogodka  $Y$  je potem

$$H(Y|x_i) = -\sum_{j=1}^s p(y_j|x_i) \log(p(y_j|x_i)).$$

Velja:  $0 \leq H(Y|x_i)$ .  
Ce pa o dogodku  $X$  vemo le da se je zgodil, se lahko spomnemo na vis in uporabimo **vezano verjetnost** dogodkov  $X$  in  $Y$ , ki pravi:

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

Za entropijo:

$$H(Y|X) = \sum_i p(x_i)H(Y|x_i) = -\sum_{i=1}^r \sum_{j=1}^s p(x_i, y_i) \log p(y_j|x_i)$$

Splosno velja:  $0 \leq H(Y|X) \leq H(Y)$ , če poznamo spremenljivko  $X$ , se nedolocenost  $Y$  ne more povecati (lahko se pomanjša).

3.3.1    Pogojna verjetnost

Verjetnost da se zgodi dogodek  $A$ , če vemo, da se zgodi dogodek  $B$ , je

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{P(A)P(B|A)}{P(B)}$$

Dogodka  $A$  in  $B$  sta **neodvisna**, če velja  $P(A|B) = P(A)$  ali  $P(AB) = P(A)P(B)$ . Pazi! Za par **nezdružljivih** dogodkov  $A$  in  $B$  pa velja  $P(AB) = 0$ ,  $P(A + B) = P(A) + P(B)$ ,  $P(A|B) = 0$  in  $P(B|A) = 0$ .

3.3.2    Popolna verjetnost

Dogodki  $H_1, H_2, \dots, H_n$  tvorijo **popoln sistem dogodkov**, če se nobena dva dogodka ne moreta zgoditi hkrati in se vedno zgodi vsaj en od njih. Če dogodki izpolnjujejo ta pogoj, potem po nacelu vključitev/izključitev velja:

$$P(A) = \sum_{i=1}^{\infty} P(A \cap H_i) = \sum_{i=1}^{\infty} P(H_i)P(A|H_i)$$

3.4    Vezana entropija spremenljivk

Vezana entropija naključnih spremenljivk  $X$  in  $Y$  je entropija para  $(X, Y)$ . Pomembne zveze:

- $p(x_i, y_j) = p(y_j|x_i)p(x_i)$ ,
- $\sum_j p(x_i, y_j) = p(x_i)$ ,
- $\sum_i p(x_i, y_j) = p(y_j)$ ,
- $\sum_{i,j} p(x_i, y_j) = 1$  (pazi pri računskih!)

Velja:

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

kar nam pove, da če najprej izvemo, kaj se je zgodilo v dogodku  $X$  in potem dobimo se dodatne informacije od dogodku  $Y$ , vemo vse.

3.4.1    Obrat kanala

Ker velja tudi  $H(X, Y) = H(X|Y) + H(Y)$ , kanal lahko **obrnemo** (sepravi vhod  $Y$  in izhod  $X$ ). Pri tem ne obracamo fizicnega procesa, ampak samo verjetnostno strukturo, ki definira kanal. **Pogoj:** poznati moramo vhodne verjetnosti. Iz njih lahko določimo izhodne verjetnosti, ki jih lahko uporabimo kot vhodne verjetnosti v obrnjeni kanal. Lastnosti:

- izračun izhodnih verjetnosti  $p(y_j) = \sum_i p(y_j, x_i)p(x_i)$
- obratne pogojne vrjetnosti  $p(x_i, y_j) = p(y_j|x_i)p(x_i) = p(x_i|y_j)p(y_j)$

Za sprejemnika sporočila so obratne pogojne verjetnosti zelo pomembne, saj z njimi lahko iz prejetih znakov določi verjetnost za vhodne znake.

3.5    Medesebojna informacija

Pove nam, koliko o eni spremenljivki izvemo iz druge spremenljivke, definicija:

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

Lastnosti:

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

- $I(X; Y) = H(Y) - H(Y|X)$
- $I(X; Y) = H(X) + H(Y) - H(X, Y)$
- $I(X; Y)$  = simetrična glede na  $X$  in  $Y$
- $I(X; Y) = -\sum_i \sum_j p(x_i, y_j) \log \frac{p(x_i)p(y_j)}{p(x_i, y_j)}$
- $I(X; Y) \geq 0$
- $I(X; X) = H(X)$

Iz definicije medsebojne informacije lahko sklepamo:

$$0 \leq H(X|Y) \leq H(X).$$

### 3.6 Kapaciteta kanala

Kapaciteta kanala je največja možna medsebojna informacija, ki jo lahko prenesemo od vhoda na izhod.

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

#### 3.6.1 Kapaciteta kanala BSK

Lastnosti:

- $C = \max_{P(X)} (H(Y) - H(Y|X))$
- $p(x_0) = \alpha, p(x_1) = 1 - \alpha$
- $I(X; Y) = H(Y) - H(Y|X) = \dots = H(Y) - H(p, 1 - p)$
- $\frac{dI(X; Y)}{d\alpha} = 0$
- $H(Y) = 1 \Rightarrow C$  je max
- $C = I(X; Y)|_{\alpha=1/2} = 1 - H(p, 1 - p)$

#### 3.6.2 Kapaciteta kanala BSK z brisanjem

Definicija:

$$P_k = \begin{pmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{pmatrix}$$

Lastnosti:

- $C = 1 - p$
- $p(x_0) = \alpha, p(x_1) = 1 - \alpha$
- $p(y_0) = (1 - p)\alpha, p(y_1) = p, p(y_2) = (1 - p)(1 - \alpha)$
- $I(X; Y) = (1 - p)H(\alpha, 1 - \alpha)$
- $\frac{dI(X; Y)}{d\alpha} = 0 \Rightarrow \alpha = 1/2$

### 3.7 Shannonov drugi teorem

Shannon je ugotovil, da nam združevanje znakov v nize daje več možnosti za doseganje zanesljivega prenosa.

Naj bo  $M$  število različnih kodnih zamenjav, ki jih lahko oblikujemo z nizi dolžine  $n$ . Potem je **hitrost koda** (prenosa) definirana kot:

$$R = \frac{\max H(X^n)}{n} = \frac{\log M}{n} = \frac{k}{n}$$

Hitrost je največja takrat, ko so dovoljene kodne zamenjave na vhodu enako verjetne. Shannonov teorem pravi, da je možna skoraj popolna komunikacija s hitrostjo, enako kapaciteti kanala. **Teorem:**

Za  $\mathbf{R} \leq \mathbf{C}$  obstaja kod, ki zagotavlja tako preverjanje informacije, da je verjetnost napake pri dekodiran poljubno majhna. Za  $\mathbf{R} > \mathbf{C}$  kod, ki bi omogočal preverjanje informacije s poljubno majhno verjetnostjo napake, **ne** obstaja.

Ce so znaki neodvisni, velja:

$$\log(H(X^n)) = n \log H(X) \Rightarrow R = H$$

Za  $R \leq \frac{\log 2^{nC}}{n} = C$  je možno najti kodne zamenjave, ki omogočajo zanesljivo komunikacijo.

## 4 Varno kodiranje

### 4.1 Uvod

Omejili se bomo na enostavne linearne bločne kode za BSK. Dolžina bloka je  $k$  znakov, abeceda je enaka abecedi kanala, torej imamo  $M = 2^k$  blokov  $x_1, \dots, x_k, x_i \in \{0, 1\}$ . Za potrebe varovanja dodamo se nekaj varnostnih znakov, celotna dolžina vsake od  $M$  kodnih zamenjav je potem  $n$ . Namesto enega posljemo  $n$  enakih znakov. Boljši pristop pa je, da naredimo kode, kjer se povečujeta  $n$  in  $k$  hitreje od razlike  $n - k$ .

### 4.2 Kontrolne vsote

Varnost komunikacije povečamo tako, da dodamo nekaj bitov za preverjanje parnosti (paritetni biti). Nastavljeni so tako, da je vsota bitov v aritmetiki po modulu 2 fiksna vrednost (0 ali 1).

+/-/XOR	0	1
0	0	1
1	1	0

npr. 00|0, 01|1, 10|1, 11|1 (detektiramo samo eno napako).

#### 4.2.1 Pravokotni kodi

Zapišemo ga v obliki pravokotnika, gledamo sodost po vrsticah in po stolpcih.

1	0	1
0	1	1
0	1	0

#### 4.2.2 Trikotni kodi

Vsota elementov v stolpcu in vrstici s paritetnim bitom vred mora biti soda. (ravno tako vsota paritetnih bitov)

1	0	1
0	0	
1		

### 4.3 Hammingova razdalja

Hammingova razdalja med kodnima zamenjava nam pove število znakov, na katerih se razlikujeta. Kodni zamenjavi sta enaki, če je razdalja 0, razdalja med različnimi kodi mora biti vsaj 1, drugače je kod **singularen**. Razdalja je podana kot **minimalna** Hammingova razdalja med dvema kodnima zamenjavama. Število napak, ki jih kod zazna:

$$d_H \geq e + 1 \rightarrow e_{max} = d_H - 1$$

$$d_H \geq 2f + 1 \rightarrow f_{max} = \lfloor \frac{e_{max}}{2} \rfloor = \lfloor \frac{d_H - 1}{2} \rfloor$$

4.3.1 Hammingov pogoj

Za bloke dolzine  $n$  lahko zgradimo  $2^n$  razlicnih kodnih zamenjav. Ce zelimo zagotoviti odpornost na napake, mora biti razdalja  $d > 1$ . Uporabni kodi imajo st. kodnih zamenjav  $M = 2^k < 2^n$ . Hammingov pogoj: da bi lahko dekodirali vse kodne zamenjave, pri katerih je prislo do  $e$  ali manj napak mora veljati:

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

Spomnimo se:  $\binom{n}{i} = \frac{n!}{i!(n-i)!}$ ,  $n! = n(n-1)$

4.4 Linearni blocni kodi

Kode oznacimo kot dvojcek  $(n, k)$ .  $n$  predstavlja stevilo vseh bitov,  $k$  podatkovnih,  $n - k$  pa st. paritetnih. O linearnih blocnih kodic govorimo, kadar:

- je vsota vsakega para kodnih zamenjav spet kodna zamenjava.
- da produkt kodne zamenjave z 1 in 0 spet kodno zamenjavo.
- vedno obstaja kodna zamenjava s samimi niclami

Oznacimo jih z  $L(n, k)$ . **Hammingova razdalja** linearnega koda je enaka stevilu enic v kodni zamenjavi z najmanj enicami.

$$d_H = \min d(\vec{a}, \vec{b}) = \min d(0, \vec{b} - \vec{a}) = \min d(0, \vec{b} + \vec{a})$$

Naj bodo podatkovni biti oznaceni kot  $z_1, z_2$  in  $z_3$ , varnostni pa kot  $s_1, s_2$  in  $s_3$ :

$$\begin{matrix} z_1 & z_2 & s_3 \\ z_3 & s_2 & \\ s_1 & & \end{matrix}$$

Potem vrednosti zlozimo v vektor, in opravimo kodno zamenjavo.

$$\vec{x} = (x_1, x_2, x_3, x_4, x_5, x_6) = (z_1, z_2, z_3, s_1, s_2, s_3)$$

Velja:

$$\begin{aligned} z_1 + z_2 + s_1 &= 0 = x_1 + x_2 + x_4 \\ z_3 + s_2 + z_2 &= 0 = x_2 + x_3 + x_5 \\ s_3 + s_3 + z_1 &= 0 = x_1 + x_3 + x_6 \end{aligned}$$

4.4.1 Generatorska matrika

Generiranje kodne zamenjave lahko opisemo z generatorsko matriko.

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

V splosnem podatkovni vektor  $1 \times k$  mnozimo z generatorsko matriko  $k \times n$ , da dobimo kodno zamenjavo  $1 \times n$ . Matrika mora imeti linearno neodvisne vrstice. Kod, cigar generatorska matrika ima to obliko, je **sistematicni kod** - prvih  $k$  znakov koda je enakih sporocilu (podatkovnim bitom), ostalih  $n - k$  znakov pa so paritetni biti.

Za diskretne kanale brez spomina (sistematicne kode) jo vedno lahko zapisemo v obliki  $G = (I_k|A)$ .

4.4.2 Matrika za preverjanje sodosti

Linearne enacbe lahko zapisemo z matriko za preverjanje sodosti:

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

Lastnosti sist. kodov:

- $\vec{x}H^T = 0$
- $G = (I_k|A) \Rightarrow H = (A^T|I_{n-k})$
- $GH^T = 0$ 
$$GH^T = (I_k|A)(A_{I_m}^{TT}) = (I_k|A)(A_{I_m}) = I_kA + AI_m = AA = \vec{0}$$
- vsota dveh kodnih zamenjav je nova kodna zamenjava.

4.5 Sindrom v kanalu

Predpostavimo da se med posiljanjem v kanalu zgodi napaka:

$$z \rightarrow x = zG \rightarrow err \rightarrow y = x + e \rightarrow s = yH^T$$

Napako pri prenosu preprosto ugotavljamo tako, da pogledamo, ce je  $s = 0$ . Vendar to nam ne garantira da pri prenosu ni prislo do napake. Sindrom izracunamo na naslednji nacin(vektor velikosti  $1 \times n - k$ ):

$$yH^T = (x + e)H^T = 0 + eH^T = s$$

Ker je verjetnost za napako obicajno  $p \ll 1$ , je niz s  $t$  napakami veliko verjetnejši od niza s  $t + 1$  napakami.

4.5.1 Standardna tabela

Imejmo ponavljalni kod  $(0|00)$  in  $(1|11)$ . Sestavimo matrkii G in H.

$$G = [1|11] \text{ in } H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

Imamo 4 mozne sindrome:  $(00), (01), (10), (11)$ . Na izhodu lahko dobimo  $2^n = 8$  razlicnih nizov.

Mozne nize na izhodu in njihove sindrome obicajno razvrstimo v std. tabelo:

sindrom	popravljalnik	
00	000	111
01	001	110
10	010	101
11	100	011

V isti vrstici so nizi, ki dajo enak sindrom. V prvi vrstici so vedno kodne zamenjave, ki imajo sindrom 0. Skrajno levo je vedno niz, ki ima najmanj enic, saj je najbolj verjeten. Imenujemo ga popravljalnik. Ostale nize dobimo tako, da popravljalnik pristevamo k kodnim zamenjavam v prvi vrsti. Popravljanje je sedaj enostavno: izracunamo sindrom, popravljalnik odstejemo(pristevamo) od prejetega niza.

4.6 Hammingov kod

Hammingovi kodi so družina linearnih blocnih kodov, ki lahko popravijo eno napako. Najlazje jih predstavimo z matriko za preverjanje sodosti, v kateri so vsi stolpci nenicelni vektorji. Spadajo med **popolne kode** - sfere z radijem 1 okrog kodnih zamenjav ravno napolnijo prostor z  $2^n$  tockami.

Kod z  $m$  varnostnimi biti ima kodne zamenjave dolzine  $2^m - 1$ . Oznaka koda je potem  $H(2^m - 1, 2^m - 1 - m)$ . Ce stolpce v matriki H interpretiramo kot stevila v binarni obliki, nam oznaka stolpca doloca položaj napake. Stolpci v Hammingovem kodu so lahko poljubno razmetani. Pomembno je le to, da nastopajo **vs**a stevila od 1 do  $2^m - 1$ .

Hammingov kod je lahko:

- **leksikografski** - oznake stolpcev si sledijo po vrsti
- **sistematicni** - oznake stolpcev so pomesane

*Iz pozicije varnostnih bitov lahko pridobimo enacbe, s pomocjo katerih lahko potem sestavimo generatorsko matriko. Sepravi vsota vseh  $z_i$ , kjer se nahaja  $s_i$*

V Hammingovem kodu se za varnostne bite obicajno vzamejo tisti stolpci, ki imajo samo **eno** enico.

4.6.1 Dekodiranje

Dekodiranje leksikografskega Hammingovega koda je preprosto:

- 1. izracunamo sindrom  $s = yH^T$
- 2. ce je  $s = 0$ , je  $x' = y$
- 3. ce  $s \neq 0$ , decimalno stevilo  $S$  predstavlja mesto napake.

Za kod, ki pa ni leksikografski potrebujemo tabelo povezav med indeksi sindromov in stolpci(sepravi pogledamo, na kateri indeks se slika izracunani sindrom).

4.7 Ciklicni kodi

Ciklicni kod  $C(n, k)$  je linearni blocni kod, v katerem vsak krozni premik kodne zamenjave da drugo kodno zamenjavo. Zapišemo jih s polinomi po padajocih potencah (ravno tako jih sestevamo po mod 2).

4.7.1 Zapis s polinomi

Imejmo osnovni vektor:

$$x = (x_{n-1}, x_{n-2}, \dots, x_0) \Leftrightarrow x(p) = x_{n-1}p^{n-1} + x_{n-2}p^{n-2} + \dots + x_0$$

Izvedemo premik za eno mesto:

$$x' = (x_{n-2}, \dots, x_0, x_{n-1}) \Leftrightarrow x'(p) = x_{n-2}p^{n-2} + \dots + x_0p + x_{n-1}$$

Velja zveza:  $x'(p) = px(p) - x_{n-1}(p^n - 1)$ .

V mod 2 aritmetiki:

$$\Rightarrow x'(p) = px(p) + x_{n-1}(p^n - 1).$$

V mod( $p^n + 1$ ) aritmetiki:

$$\Rightarrow x'(p) = px(p) \bmod (p^n + 1).$$

**Pozor:** aritmetiko po mod 2 izvajamo na **istih** stopnjah polinoma (na bitih), aritmetiko po mod ( $p^n + 1$ ) pa na **polinomu**.

Izvajanje kroznega prekmika za  $i$  mest:

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

4.7.2 Generatorski polinomi

Vrstice generatorske matrike lahko razumemo kot kodne zamenjave. Za ciklicne kode v splosnem velja: **Generatorski polinom** je stopnje  $m$ , kjer je  $m$  stevilo varnostnih bitov, in ga oznacimo kot:

$$g(p) = p^m + g_{m-1}p^{m-1} + \dots + g_1p + 1$$

Za sistematicni kod velja:  $G = [I_k | A_{k, n-k}]$ . Generatorska matrika:

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

Sistematicni lahko dobimo z linearnimi operacijami nad vrsticami. Velja:

$$p^n + 1 = g(p)h(p)$$

Sepravi vsak polinom, ki polinom  $p^n + 1$  deli brez ostanka, je generatorski polinom.

4.7.3 Polinom za preverjanje sodosti

Velja:  $x(p)h(p) \bmod (p^n + 1) = 0 \Rightarrow \sum_{i=0}^{n-i} x_i h_{j-i} = 0$   
V matricni obliki:  $\vec{x}H^T = H\vec{x}^T = 0$

$$\begin{bmatrix} h_0 & \dots & h_k & 0 & \dots & 0 & 0 \\ 0 & h_0 & \dots & h_k & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & 0 & \dots & 0 & h_0 & \dots & h_k \end{bmatrix} \begin{bmatrix} x_{n-1} \\ \vdots \\ x_0 \end{bmatrix} = 0$$

4.7.4 Kodiranje z mnozenjem

Kodne zamenjave so veckratniki generatorskega polinoma. Velja:

$$x(p) = z(p)g(p) \bmod (p^n + 1)$$

, kjer je  $z(p)$  polinom, ki ustreza podatkovnemu vektorju  $\vec{z}$ . Kod, ki smo ga dobili z mnozenjem, ustreza generatorski matriki, ki ima v vrsticah koeficiente  $p^{k-1}g(p), \dots, pg(p), g(p)$ , zato ni sistematicen.

4.7.5 kodiranje z deljenjem

Kodiranje na osnovi deljenja ustvari sistematicen ciklicen kod. Kodna zamenjava je zato sestavljena iz sporocila (podatkovnega bloka) in varnostnega bloka znakov,  $x = (z|r)$ . Polinom podatkovnega bloka je:

$$z(p) = z_{k-1}p^{n-1} + \dots + z_1p^1 + z_0p^0$$

Ce pa polinom pomnozimo s  $p^m$ , dobimo na desni  $m$  nicel.

$$p^m z(p) = z_{k-1}p^{k-1} + \dots + z_1p^{m+1} + z_0p^m$$

To ustreza bloku  $z$ , premaknjenem za  $m$  znakov v levo,  $(z_{k-1}, \dots, z_0, 0, \dots, 0)$ .

V splosnem nastavek seveda ne bo deljiv, velja pa:

$$p^m z(p) = g(p)t(p) + r(p)$$

kjer je  $t(p)$  kolicnik  $r(p)$  pa ostanek, s stopnjo manj od  $m$ .

Ostanek lahko zapisemo v obliki niza, kot  $(0, \dots, 0, r_{m-1}, \dots, r_0)$ .

Polinom  $p^m z(p) + r(p) = g(p)t(p)$  je deljiv z  $g(p)$  in je zato ustrezna kodna zamenjava. Kodno zamenjavo tako dobimo, ce ostanek deljenja z generatorskim polinomom pristevamo k osnovnemu nastavku,  $(z_{k-1}, \dots, z_0 | r_{m-1}, \dots, r_0)$ .

4.7.6 Strojna izvedba kodirnika

Uporabljeni so trije tipi elementov: pomnilna celica tipa  $D$ , sestevalnik (XOR), mnozenje s konstanto ( $1 \mid 0$ ). Poznamo kodiranje na osnovi deljenja in na osnovi mnozenja. (insert pics here). Pri kodiranju se sepravi najprej na izhod posiljajo kar vhodni znaki, potem v naslednjih korakih se vsebina pomnilnih celic od zadaj naprej.

4.7.7 Dekodiranje

Dekodiranje ciklicnih kodov sloni na linearnih blocnih kodih. Vzemimo, da je pri prenosu prislo do napake  $y = x + e$ , ali pa zapisano v polinomski obliki  $y(p) = x(p) + e(p) = z(p)g(p) + e(p)$ .

- Najprej izracunamo sindrom. Ekvivalent enacbe  $s = yH^T$  v polinomskem zapisu je  $y(p) = q(p) * g(p) + s(p)$ , oz.  $s(p) = y(p) \bmod g(p)$ .
- Ce je ostanek deljenja  $y(p)$  z  $g(p)$  razlicen od nic, je prislo do napake.

Iz  $s(p) = y(p) \bmod g(p)$  sledi, da je v primeru, ko je napaka na zadnjih  $m$  mestih, stopnja  $e(p)$  manj kot  $m$  in velja kar  $e(p) = s(p)$ . Za ostale napake pa lahko izkoristimo ciklicnost kodov:

- Naredimo trik, osnovno enacbo premaknemo za  $i$  mest:

$$p^i y(p) = p^i x(p) + p^i e(p)$$

- Če najdemo pravi  $i$ , bo veljalo  $p^i e(p) = s(p)$
- Pravi  $i$  je tisti, pri katerem bo  $e(p)$  imel najmanj enic

#### 4.7.8 Klasifikacija napak

Napaki, ki se pojavi na izhodu odposlane kodne zamenjave neodvisno od morebitnih napak na sosednjih znakih, pravimo **posamicna** ali **neodvisna** napaka. Do posamicnih napak pride zaradi motenj, ki so krajše od casa posiljanja enega znaka.

Povezanim napakam na vec zaporednih znakih pravimo **izbruh**. Dolzina izbruha je stevilo znakov med prvim in zadnjim napacno sprejetim znakom. Do izbruha pride, ce je trajanje motenj daljse od casa posiljanja enega znaka.

Ciklicni kodi so posebej primerni za **ugotavljanje izbruhov napak**.

#### 4.7.9 Zmoznosti ciklicnih kodov

Odkrivanje napak s ciklicnimi kodi, kjer velja  $1 < \text{st}(g(p)) < n$ :

- Kod odkrije vsako posamicno napako:  $e(p) = p^i$

$$e(p) = p^i \text{ ni deljiv z } g(p)$$

- Za dolocene generatorske polinome odkrije tudi dve posamicni napaki do dolzine bloka  $n = 2^m - 1$

$$e(p) = p^i + p^j = p^j(p^{i-j} + 1)$$

*Pri pogoju, da  $p^j$  ni deljiv z  $g(p)$  in  $p^{i-j}$  ni deljiv z  $g(p)$  za vsak  $i - j$*

- Odkrije poljubno stevilo lihih napak, ce  $p + 1$  deli  $g(p)$

$$\begin{aligned} g(p) &= (p + 1)g_g(p) \\ (p + 1)p^i &= p^{i+1} + p^i \\ (p + 1)(p^i + p^{i-1}) &= p^{i+1} + p^i + p^i + p^{i-1} = p^{i+1} + p^{i-1} \end{aligned}$$

- Odkrije vsak izbruh napak do dolzine  $m$
- Odkrije vse razen  $2^{-(m-1)}$  izbruhov dozline  $m + 1$
- Odkrije tudi vse razen delez  $2^{-m}$  izbruhov daljsih od  $m + 1$

Popravljanje napak s ciklicnimi kodi, kjer velja  $1 < \text{st}(g(p)) < n$ :

- Izracun sindroma
- Ciklicno prilaganje sindroma prenesenemu blok  $y$ .
- Popravijo lahko do  $e = \lfloor \frac{d-1}{2} \rfloor$  posamicnih napak, kjer je  $d$  Hammingova razdalja koda.
- Popravijo lahko tudi izbruhe napak do dolzine  $e = \lfloor \frac{m}{2} \rfloor$

#### 4.7.10 CRC

Ali Cyclic Redundancy Check, temelji na ciklicnih kodih. Po standardu velja:

- Registri v **LSFR** so na zacetku nastavljeni na **1**; osnovni CRC ne loci sporocil, ki imajo razlicno stevilo vodilnih nicel. Ta sprememba, ki je ekvivalentna negiranju prvih  $m$  bitov, to tezavo odpravi.
- Na koncu sporocila dodamo  $m$  - bitov, odvisno od implementacije LSFR. Pri nasi se to ne dela!

- **Operacija XOR** na fiksнем ostanku deljenja, obicajno je to kar negacija vseh bitov.

- **Vrstni red bitov v bajtu** - nekateri serijski protokoli najprej oddajo najmanj pomembne bite (najmanj pomembni bit ima najvisjo stopnjo polinoma).

- **Vrsni red bajtov** - pomnilniska organizacija, odvisna od arhitekture (LE, BE).

- Notacija CRC polinomov - biti oznacujejo prisotnost faktorja. Veckrat se izpusca en izmed faktorjev  $p^m$  ali 1.

Ciklicni kodi so odlicni za detekcijo napak. Za popravljanje napak pa danes obstajajo boljsi kodi.

#### 4.7.11 Prepletanje

Motnje so mnogokrat v obliki izbruhov. V takih primerih pride na dolocenih kodnih zamenjavah do velikega stevila napak, na drugih pa napak ni. S prepletanjem bitov se da napake porazdeliti med vec kodnih zamenjav. Resitev:

- Kodne zamenjave v kodirnik vpisujemo vrstico po vrstico, oddaja pa jih stolpec po stolpec. Obratno je na strani dekodirnika.
- Naceloma je vzorec skoraj naključen. Matriko prepletanja poznata kodirnik in dekodirnik.
- Dodamo zakasnitev, izmenicno signali potujejo gor/dol, ena veja je zakasnjena.

Dejanske resitve so bolj kompleksne: vec vej, zakasnitve tudi do 20 vej.

#### 4.7.12 Konvolucijski kodi

Primerni za popravljanje napak. Konvolucijske kode genriramo z linearnimi premikalnimi registri, ki so sestavljeni iz pomnilnih celic D in vrat XOR. Spadajo pod nelinearne kode.

## 5 Analiza signalov

Pri analizi signalov in sistemov je izjemno pomembna kolicina frekvenca.

### 5.1 Invariantnost sinusoid

Vzemimo zvezni signal, ki prehaja skozi linearni medij (sistem) kot je na primer elektricno vezje.

V splosnem bo signal na izhodu drugacen od signala na vhody(zvok, ki ga poslusamo pod vodo je bistveno bolj popacen od tistega, ki ga poslusamo na zraku)

Pomembno pri signalih pa je, da se vhodni signal v obliki sinusoide

$$x(t) = A \sin(2\pi\nu t + \theta)$$

popaci v izhodni signal z drugacno amplitudo in fazo  $\theta$ , vendar ohrani frekvenco  $\nu$ .

$$x(t) = A' \sin(2\pi\nu t + \theta')$$

Razlog, da se frekvenca ohrani je v tem, da linearne sisteme lahko zapisemo v obliki elementarnih operacij, kot so (mnozenje s konstanto, odvajanje, integracija, zakasnitev, vsota).



5.2 Fourierova transformacija

Vsako periodicno funkcijo ( ce je dovolj lepa ), lahko zapisemo kot kombinacijo sinusoid. V kombinaciji z invariantnostjo sinusoid to pomeni, da lahko:

- vsako funkcijo razstavimo na sinusoide
- obravnavamo obnasanje vsake sinusoide v sistemu posebej
- na koncu zdruzimo locene rezultate

Ta koncept se danes uporablja pri vsaki analizi signalov.

5.2.1 Fourierova vrsta

Funkcija je periodicna s periodo  $T$ , ce velja:

$$x(t + T) = x(t), \forall t: -\infty < t < \infty$$

kjer je  $T$  najmanjsa pozitivna vrednost s to lastnostjo.

Funkciji  $\sin(t)$  in  $\cos(t)$  sta periodicni s periodo  $2\pi \Rightarrow$  Funkciji  $\sin(\frac{2\pi t}{T})$  in  $\cos(\frac{2\pi t}{T})$  sta potem periodicni funkciji s periodo  $T$  in frekvenco  $\nu_0 = \frac{1}{T}$ .

Cas merimo v sekundah, frekvenco pa v stevilu ciklov na sekundo. Pri analizi signalov zapis veckrat poenostavimo tako, da namesto frekvence uporabimo kotno hitrost

$$\omega_0 = 2\pi\nu_0 = \frac{2\pi}{T}$$

Visji harmoniki sinusoid s frekvenco  $\nu_0$  so  $\sin$  in  $\cos$  funkcije s frekvencami, ki so veckratniki osnovne frekvence,  $n\nu_0$ .

Fourier je pokazal, da lahko **vsako** periodicno funkcijo  $x(t)$  s periodo  $T$  zapisemo kot:

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

za  $n \geq 1$ .

Lastnosti preden se lotimo dokaza:

- $\int_0^T \cos(\omega_0 t) dt = \int_0^T \sin(\omega_0 t) dt = 0$
- $\int_0^T \sin(n\omega_0 t) dt = \int_0^T \sin(n\omega_0 t) dt = 0$  (visji harmoniki)
- $\sin(2\pi\nu_1 t) \sin(2\pi\nu_2 t) = \frac{1}{2}(\cos(2\pi(\nu_1 - \nu_2)t) - \cos(2\pi(\nu_1 + \nu_2)t))$

Se nekaj lastnosti z dokazi:

- $\cos(n\omega_0 t) \cos(m\omega_0 t) = \frac{1}{2}(\cos((n+m)\omega_0 t) + \cos((n-m)\omega_0 t))$   
ce  $n \neq m$   
 $= \frac{1}{2} \int_0^T (\cos((n+m)\omega_0 t) dt + \frac{1}{2} \int_0^T \cos((n-m)\omega_0 t) dt) = 0$   
ker velja  $n+m > 0$  in  $|n-m| \geq 1$   
ce pa  $n = m$   
 $= \frac{1}{2} \int_0^T (\cos((2n)\omega_0 t) dt + \frac{1}{2} \int_0^T \cos(0) dt) = \frac{T}{2}$
- Enako velja za produkt dveh sinusoid.
- $\int_0^T \sin(n\omega_0 t) \cos(n\omega_0 t) dt = 0$

Dokaz:

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

$$\int_0^T x(t) dt = \frac{a_0}{2} \int_0^T dt + \int \sum + \int \sum = \frac{a_0}{T} \rightarrow a_0 \frac{2}{T} \int_0^T x(t) dt$$

$$\int_0^T x(t) \cos(n\omega_0 t) dt = a_n \frac{T}{2} \rightarrow a_n = \frac{2}{T} \int_0^T x(t) \cos(n\omega_0 t) dt$$

Enako bi lahko pokazali za  $b_n$ .

To velja za vsako funkcijo, ki zadosca Dirichletovim pogojem:

- je enoznacna (za vsak  $t$  ena sama vrednost)
- je koncna povsod, oz. njen integral je koncen

- je absolutno integrabilna (ima koncno energijo)

$$\int_0^T |x(t)| dt < \infty$$

- mora imeti koncno stevilo ekstremov v vsakem obmocju
- imeti mora knco stevilo koncnih nezveznosti v vsakem obmocju

Bolj kompaktna predstavitev je z uporabo **Eulerjeve formule**  $e^{i\phi} = \cos(\phi) + i \sin(\phi)$ ,  $i = \sqrt{-1}$ :

$$x(t) = \sum_{n=-\infty}^{\infty} c_n e^{in\omega_0 t}$$

Koeficienti so kompleksni:

$$c_n = \frac{1}{T} \int_0^T x(t) e^{-in\omega_0 t} dt = \int_{-T/2}^{T/2} x(t) e^{-in\omega_0 t} dt$$

Zveza med obema zapisoma:

- $n = 0 : c_0 = \frac{a_0}{2}$
- $n > 0 : c_n = \frac{a_n - ib_n}{2}$
- $n < 0 : c_n = \frac{a_{-n} - ib_{-n}}{2}$

Negativne frekvence so matematichni konstrukt, ki nam pride prav pri opisovanju singalov. Vsako sinusoido opisemo z dvema parametroma, prej  $a_n, b_n$ , sedaj pa elegantno s  $c_n$  in  $c_{-n}$ .

5.2.2 Fourierova transformacija

Fourierovo vrsto lahko posplosimo tako, da spustimo  $T \rightarrow \infty$  in dobimo Fourierovo transformacijo. Predstavlja jedro vseh frekvencnih analiz. Enacba:

$$x(t) = \int_{-\infty}^{\infty} X(\nu) e^{-i2\pi\nu t} dt = \int_{-\infty}^{\infty} x(t) e^{-i\omega t} dt$$

Manjsi kot je  $T$  v casovnem prostoru, sirsi je signal v frekvencnem prostoru.

Lastnosti Fourierove transformacije:

- linearnost:  $f(t) = ax(t) + by(t) \rightarrow F(\nu) = aX(\nu) + bY(\nu)$
- skaliranje:  $f(t) = x(at) \rightarrow F(\nu) = \frac{1}{|a|} X(\frac{1}{a}\nu)$
- premik:  $f(t) = x(t - t_0) \rightarrow F(\nu) = e^{-i2\pi\nu t_0} X(\nu)$
- modulacija:  $f(t) = e^{i2\pi\nu_0 t} x(t) \rightarrow F(\nu) = X(\nu - \nu_0)$
- konvolucija:  $f(t) = \int_{-\infty}^{\infty} x(t - \tau) y(\tau) d\tau \rightarrow F(\nu) = X(\nu) Y(\nu)$

5.2.3 Diskretna Fourierova transformacija - DFT

Frekvenca vzorcenja  $\nu_s$  (sampling) je obratno sorazmerna periodi vzorcenja  $\nu_s = \frac{1}{\Delta}$ . Postopek:

- Ocenimo Fourierovo transformacijo iz  $N$  zaporednih vzorcev.

$$x_k = x(k\Delta), k = 0, 1, \dots, N - 1$$

- Iz  $N$  vzorcev na vhodu v DFT bomo lahko izracunali natanko  $N$  neodvisnih tock na izhodu.
- Namesto, da bi dolocili DFT za vse tocke od  $-\nu_C$  do  $+\nu_C$ , se lahko omejimo samo na dolocene vrednosti

$$\nu_n = \frac{n}{N\Delta}, n = -\frac{N}{2}, \dots, \frac{N}{2}$$

spodnja in zgornja meja ustrezata ravno Nyquistovi frekvenci.

- Trenuten zapis vkljucuje  $N + 1$  vrednost. Izkazalo se bo, da sta obe robni vrednosti enaki. Imamo jih zaradi lepsega zapisa.
- Naprej so stvari trivialne

$$X(\nu_n) = \int_{-\infty}^{\infty} x(t) e^{-i2\pi\nu_n t} dt = \sum_{k=0}^{N-1} x_k e^{-i2\pi\nu_n k\Delta} \Delta$$

- Če v zgornji enačbi izpustimo  $\Delta$ , dobimo enačbo za DFT:

$$X_n = \sum_{k=0}^{N-1} x_k e^{\frac{-i2\pi nk}{N}}$$

Povezava s Fourierovo transformacijo je  $X(\nu_n) \approx \Delta X_n$ . Iz enačbe za DFT sledi, da je DFT periodična s periodo  $N$ . To pomeni, da je  $X_{-n} = X_{N-n}$ . Koeficiente  $X_n$  lahko zato namesto na intervalu  $[-\frac{N}{2}, \frac{N}{2}]$  računamo na intervalu  $[0, N-1]$ .

Zveza med koeficienti  $X_0, \dots, X_{N-1}$  in frekvencami  $-\nu_C, \dots, \nu_C$ :

indeks	frekvenca
$n = 0$	$\nu = 0$
$1 \leq n \leq \frac{N}{2}-1$	$0 < \nu < \nu_C$
$\frac{N}{2}$	$-\nu_C, +\nu_C$
$\frac{N}{2} + 1 \leq n \leq N-1$	$\nu_C < \nu < 0$

#### 5.2.4 Inverzna DFT

$$x_k = \frac{1}{N} \sum_{n=0}^{N-1} X_n e^{\frac{i2\pi nk}{N}}$$

### 5.3 Resonanca

Do resonance pride, ko je frekvenca vsiljenega nihanja enaka frekvenci lastnega nihanja. Takrat pride do ojačitve amplitud. Resonanca je pomembna lastnost električnih vezij, s katero zagotovimo nihanja, nastavljanje radijskih sprejemnikov na pravo postajo, odstranimo sum.

### 5.4 Modulacija in frekvenčni premik

Iz analize vemo, da nelinearne operacije nad signali (kvadriranje, množenje) privedejo do pomembnih transformacij v frekvenčnem prostoru.

Iz osnovne trigonometrije vemo:

$$\begin{aligned} \sin(2\pi\nu_1 t) \sin(2\pi\nu_2 t) &= \frac{1}{2} [\cos(2\pi(\nu_1 - \nu_2)t) - \cos(2\pi(\nu_1 + \nu_2)t)] \\ \cos(2\pi\nu t) &= \sin(2\pi\nu t + \pi/2) \end{aligned}$$

Produkt sinusoid s frekvencama  $\nu_1$  in  $\nu_2$  lahko torej zapišemo kot vsoto sinusoid s frekvenco  $\nu_1 + \nu_2$  in sinusoid s frekvenco  $\nu_1 - \nu_2$ .

To lastnost izkorisča amplitudna modulacija (radijske postaje AM) in frekvenčni premik, s katerim lahko zagotovimo hkraten prenos več signalov po istem mediju.

## 5.5 Teorem vzorčenja

Signal moramo vzorčiti vsaj s frekvenco  $2\nu_c$ , ce je najvisja opazena frekvenca v signalu  $\nu_c$ . Na tem zaključku sloni vsa danasnja tehnologija.

$$\nu_s \geq 2\nu_c$$

#### 5.5.1 Zajem signalov

Zvezni signal  $x(t)$  je funkcija zvezne spremenljivke  $t$ . Diskreten signal je definiran samo za določene case, ki si najpogosteje sledijo v enakih časovnih intervalih  $x_k = x(k\Delta)$ ,  $\Delta$  je perioda vzorčenja.

Signale danes običajno zajemamo z računalniki. Za to se uporabljajo vezja  $A/D$  pretvorniki. Imajo končno natančnost, na primer 12bit. Signal torej opisemo s končno mnogo različnimi amplitudami  $2^{12}$ .

Diskretnemu in kvantiziranemu signalu recemo tudi digitalni signal. Kvantizacija je običajno tako fina, da jo lahko zanemarimo.

### 5.6 Energija signala

Definicija:

$$E = \int_{-\infty}^{\infty} x(t)^2 dt$$

#### Parsevalov teorem

$$\int_{-\infty}^{\infty} x(t)^2 dt = \int_{-\infty}^{\infty} |X(\nu)|^2 d\nu$$

Porazdelitev energije po frekvencah podaja funkcija  $|X(\nu)|^2$ , ki jo imenujemo **energijska spektralna gostota**.

#### 5.6.1 Mocnostni spekter diskretnega kanala

Diskretna različica Parsevalovega teorema:

$$\sum_{k=1}^{N-1} |x_k|^2 = \frac{1}{N} \sum_{n=0}^{N-1} |X_n|^2$$

Pri diskretni različici je PSD vedno v intervalu  $[-\nu_C, \nu_C]$ . Mocnostni spekter je potem:

- $P(0) = \frac{1}{N^2} |X_0|^2$
- $P(\nu_n) = \frac{1}{N^2} [|X_n|^2 + |X_{N-n}|^2]$ ,  $n = 1, 2, \dots, \frac{n}{2}-1$
- $P(\nu_C) = \frac{1}{N^2} |X_{\frac{N}{2}}|^2$