

Teorija informacije

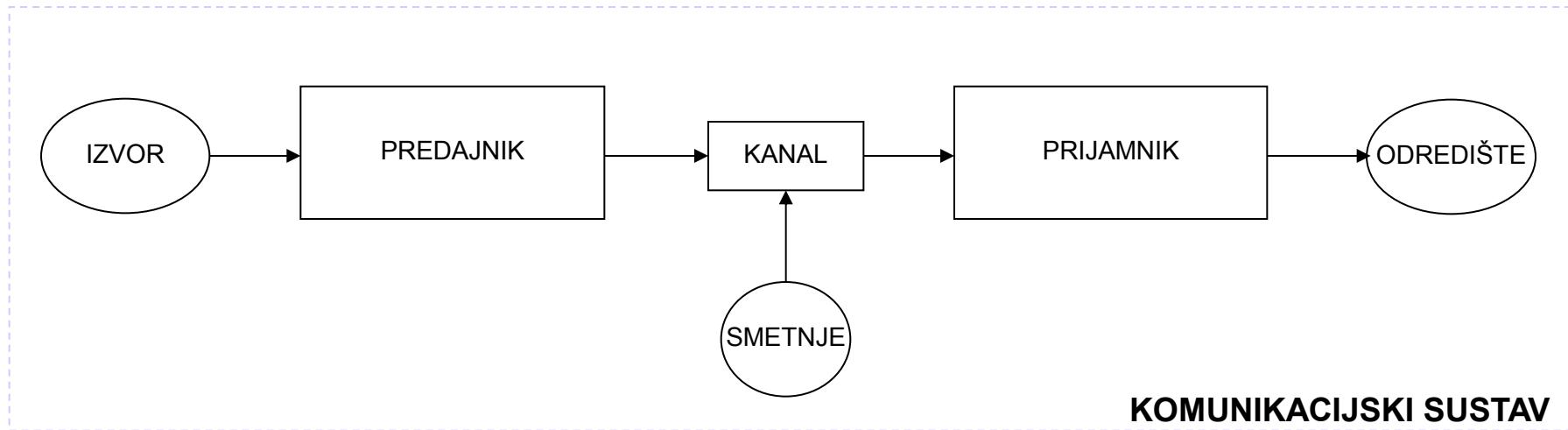
Osnovni pojmovi teorije informacije

Osnovni pojmovi teorije informacije

- ◆ Opći model komunikacijskog sustava
 - Diskretni komunikacijski sustav
 - Poruka i prijenos poruke
- ◆ Sadržaj informacije, entropija
- ◆ Kodiranje
- ◆ Informacijski opis komunikacijskog sustava, informacijske mjere
- ◆ Kapacitet kanala
- ◆ Prijenos informacije komunikacijskim sustavom

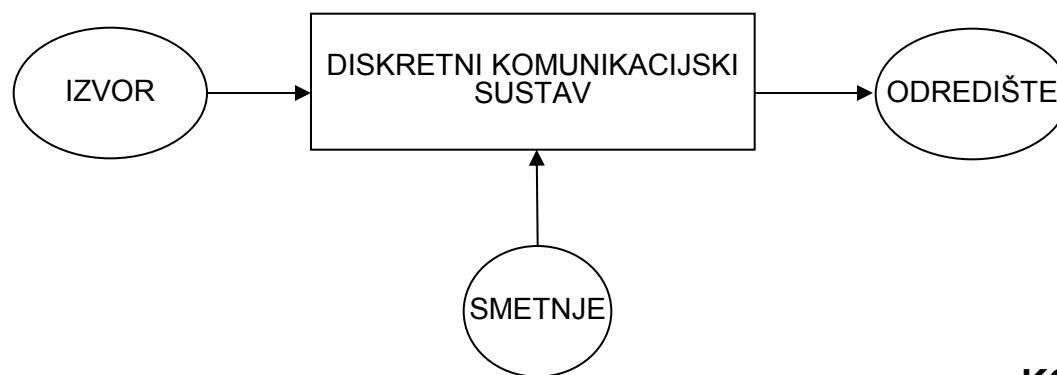
Opći model komunikacijskog sustava

Temeljni problem komunikacije je točno ili aproksimativno reproducirati u jednoj točki informacijskog prostora (odredište) poruku odabranu na nekoj drugoj točki (izvor) [Shannon 1948].



Diskretni komunikacijski sustav

- ◆ Jednostavniji slučaj – diskretni signali
- ◆ Ključna pitanja:
 - Što je poruka?
 - Što znači prenijeti poruku?
 - Koja je mjera za količinu informacije u nekoj poruci, te informacije prenesene sustavom?

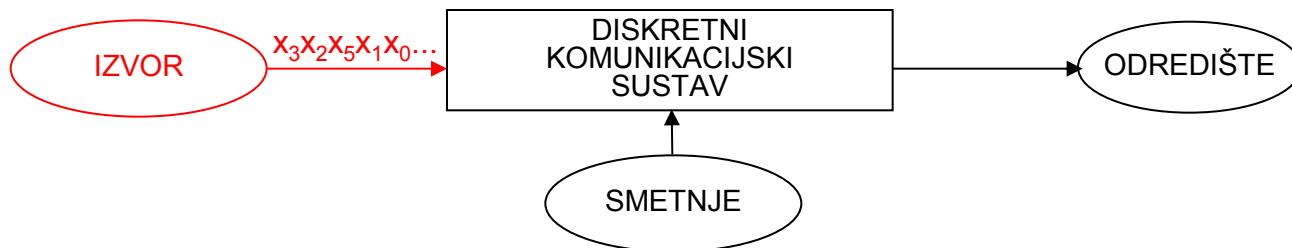


KOMUNIKACIJSKI SUSTAV

Poruka

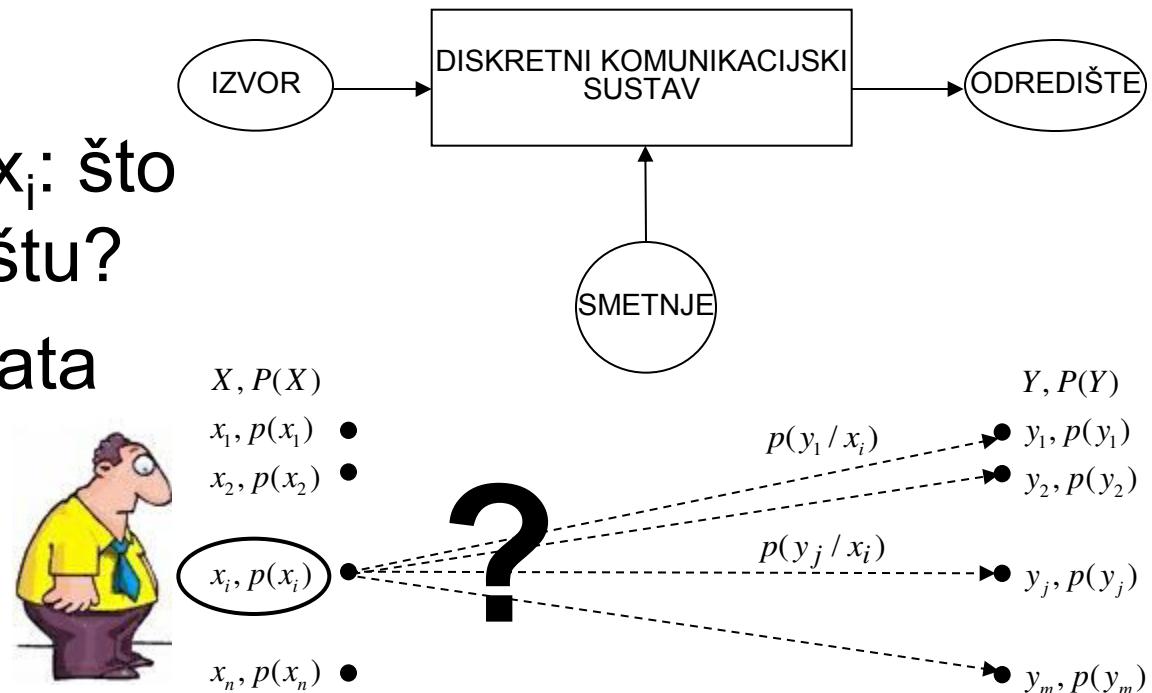
Zavod za telekomunikacije

- ◆ Niz simbola odabralih iz konačne abecede X
 - Abeceda je skup elementarnih simbola
$$X = \{x_1, x_2, \dots, x_i, \dots, x_n\}$$
- ◆ Svaki simbol pri N -tom biranju ima vjerojatnost pojavljivanja: $x_i \longrightarrow p_N(x_i)$
- ◆ Pretpostavka (za sada): odabir simbola neovisan o prethodno odabranim simbolima: $x_i \longrightarrow p(x_i)$

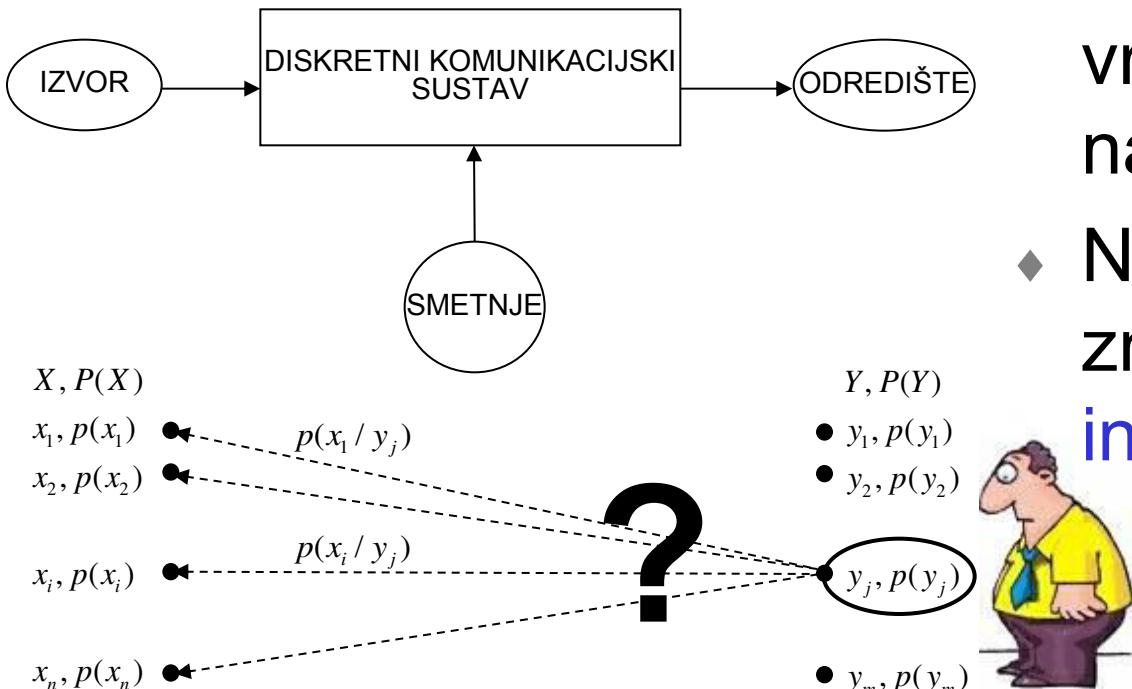


Prijenos poruke: pogled sa izvora

- ◆ Prijenos poruke = prijenos simbola
- ◆ Na izvoru odabran x_i : što se pojavi na odredištu?
- ◆ Pretpostavka: poznata statistička svojstva prijenosa



Prijenos poruke: pogled sa odredišta



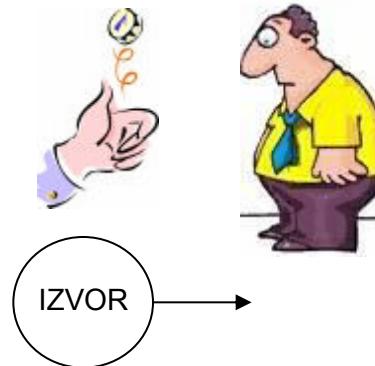
- ◆ Prije pojave y_j , znamo vrlo malo o događajima na izvoru
- ◆ Nakon opažanja y_j , znamo više: primili smo informaciju!



- $X, P(X)$
- $y_1, p(y_1)$
 - $y_2, p(y_2)$
 - $y_j, p(y_j)$
 - $y_m, p(y_m)$

Sadržaj informacije poruke - primjer

- ◆ Koliko informacije možemo maksimalno prenijeti nekom porukom?
- ◆ Primjer: pismo ili glava



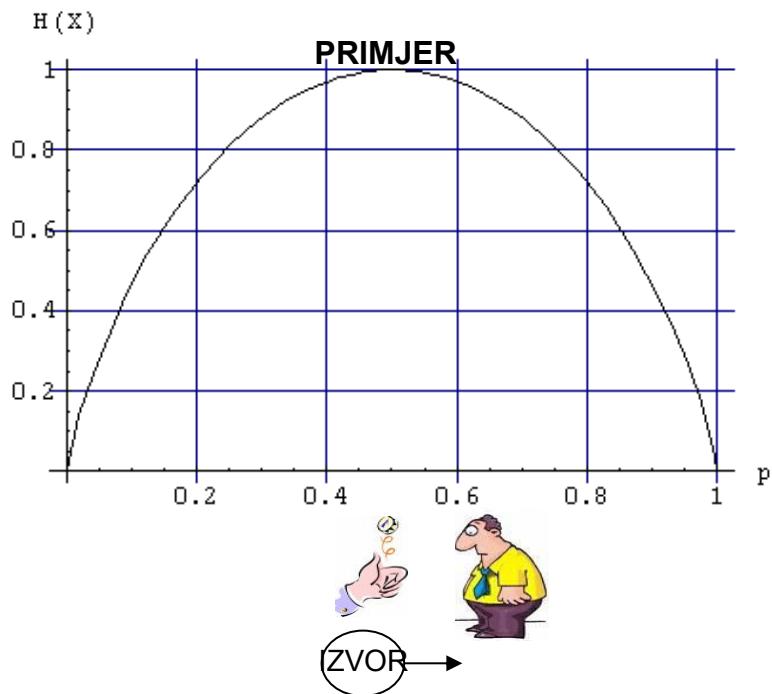
- ◆ Koliko informacije je primio promatrač?
- ◆ Što ako uvijek pada pismo?
- ◆ Što ako pismo pada 70% puta?

Entropija

- ◆ Entropija diskretne slučajne varijable

$$H(X) = - \sum_{i=1}^n p(x_i) \log p(x_i) [\text{bit / simbol}]$$

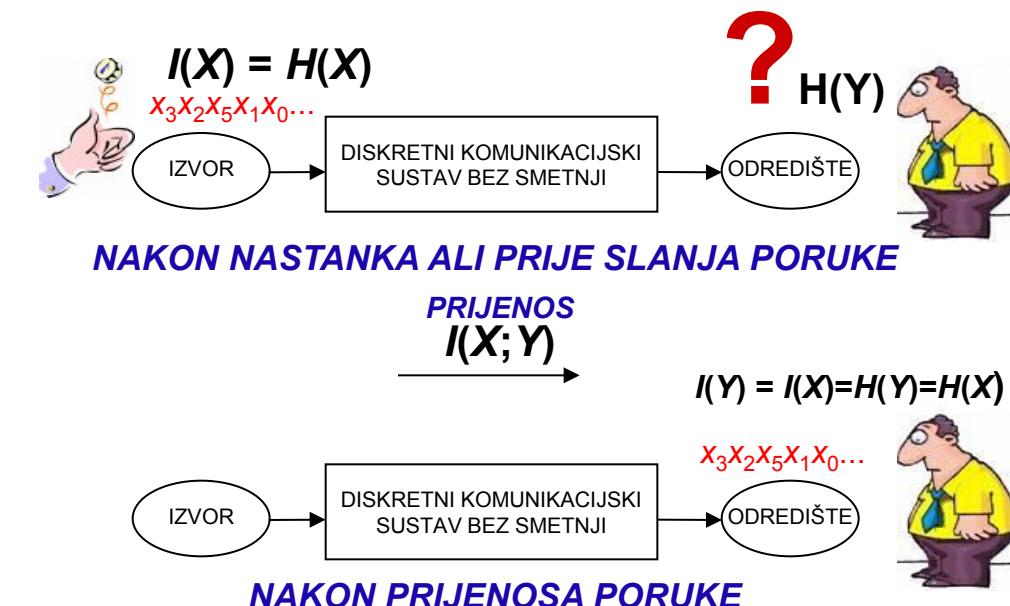
- ◆ Entropija daje mjeru za sadržaj informacije



Entropija, neodređenost, sadržaj informacije u sustavu bez smetnji



- ◆ Neodređenost = entropija



- ◆ Informacija na izvoru, neodređenost na odredištu
- ◆ Prijenosom poruke neodređenost je nestala

Svojstva entropije

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

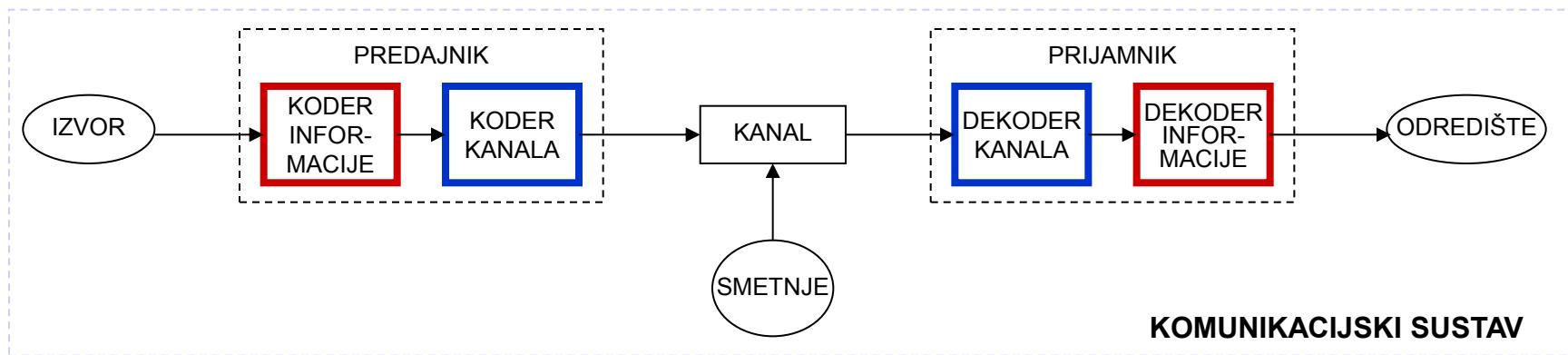
- ◆ Sadržaj informacije ne može biti negativan $H(X) \geq 0$
- ◆ Sadržaj informacije je 0 ako se uvijek pojavljuje samo jedan simbol $H(X) = 0 \Leftrightarrow \exists i \mid p(x_i) = 1$
- ◆ Neodređenost i sadržaj informacije su maksimalni ako su vjerojatnosti simbola jednakoraspoređene $H(X) \leq \log n$
- ◆ Zašto baš logaritam? $H(XY) = H(X) + H(Y)$ 

Bit i binarna znamenka

- ◆ Teorija informacije: bit je osnovna jedinica informacije
- ◆ Ostatak svijeta: bit je binarna znamenka
- ◆ Bacamo “nepošteni” novčić, pismo=1, glava=0; koliko je ovo bitova: **1111111111** ?
- ◆ Kada znamo razliku, iz konteksta je jasno što se misli

Kodiranje

- ◆ Dodjela kodnih riječi simbolima poruke
- ◆ Poruka se “samo” pretvara u novi oblik (niz simbola)
- ◆ Zašto onda kodirati?
- ◆ U praksi, kodovi su binarni



Kodiranje i entropija

PRIMER	SIMBOL (x_i)	VJEROJATNOST POJAVLJIVANJA $p(x_i) = p_i$	KODNA RIJEČ (C_i)	DULJINA KODNE RIJEĆI (l_i)
	1	1/2	0	1
	2	1/4	10	2
	3	1/8	110	3
	4	1/8	111	3

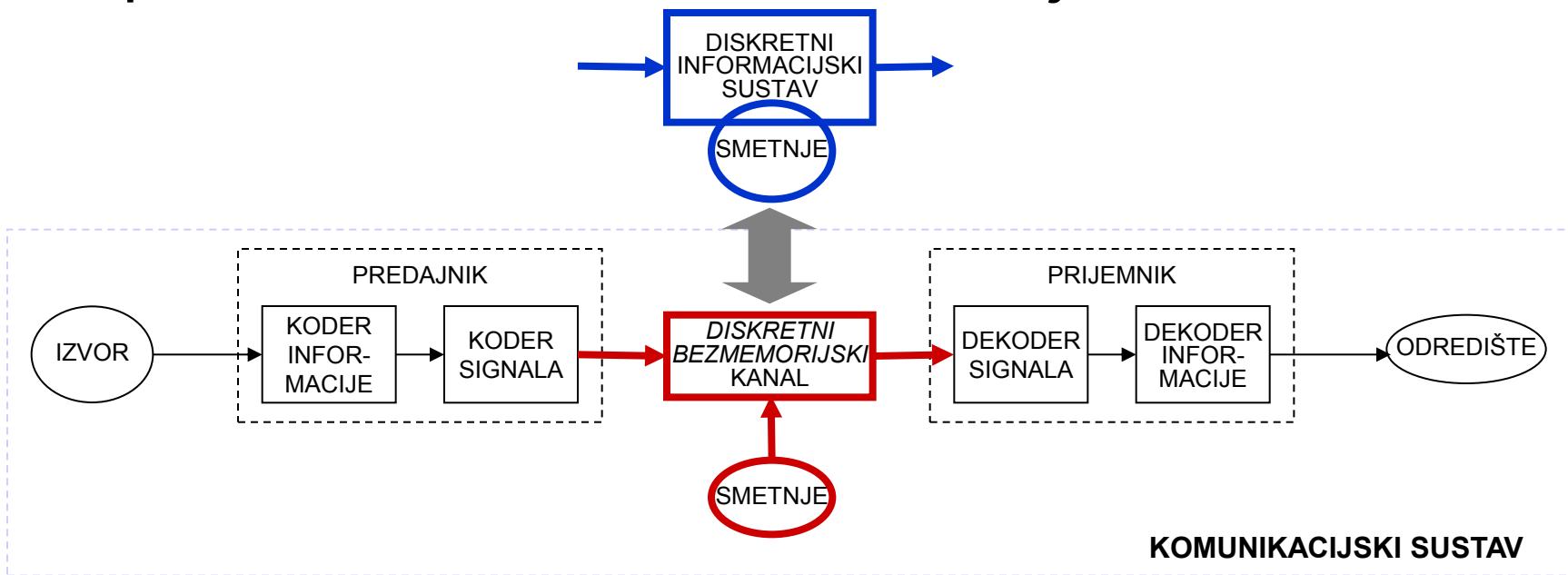
- ◆ Prosječna duljina kodne riječi:

$$L = \sum_{i=1}^n p_i l_i = 0.5 \cdot 1 + 0.25 \cdot 2 + 0.125 \cdot 3 + 0.125 \cdot 3 = 1.75 [\text{bit / simbol}] = H(X)$$

- ◆ Ne postoji kod sa manjom prosječnom duljinom
- ◆ **Entropija je granica kompresije bez gubitaka**

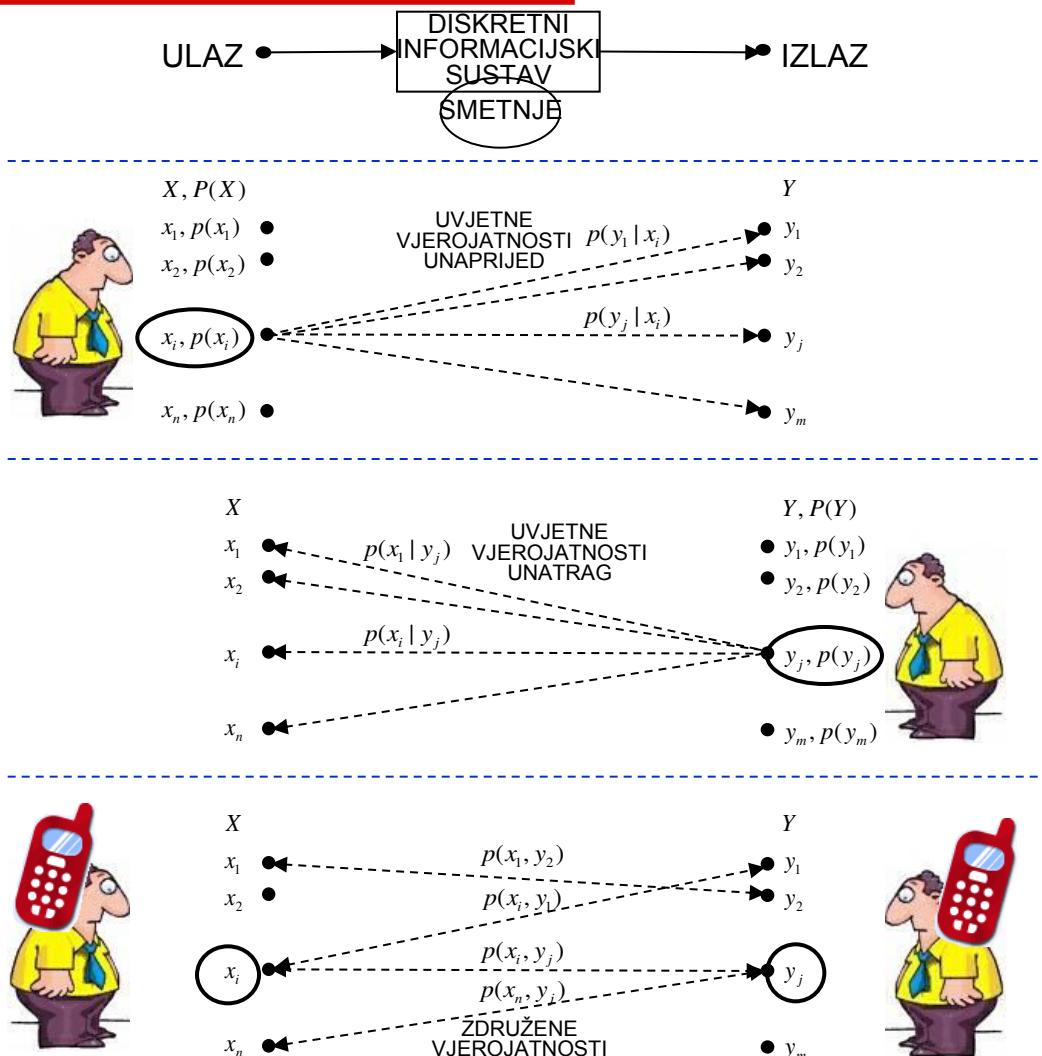
Informacijski opis komunikacijskog sustava

- ◆ Sustav bez smetnji ne postoji
 - Promatramo opći sustav uz (manja) ograničenja: diskretni bezmemorijski kanal
- ◆ Opis kanala – diskretni informacijski sustav



Vjerojatnosni opis inf. sustava (kanala)

- ◆ Opis sustava skupom vjerojatnosti
- ◆ Svaki od ova tri pogleda potpuno određuje sustav i pojavu na ulazu/izlazu
- ◆ Vjerojatnosti prijelaza $x \rightarrow y$ potpuno definiraju kanal



Primjer

- ◆ Komunikacijski kanal prenosi simbole {a, b, c}
 - $p(a) = p(b) = 2p(c)$
- ◆ Matrica uvjetnih vjerojatnosti prijelaza u kanalu:

$$\left[p(y_j | x_i) \right] = \begin{bmatrix} 0,7 & 0,1 & 0,2 \\ 0,2 & 0,7 & 0,1 \\ 0,1 & 0,2 & 0,7 \end{bmatrix}$$

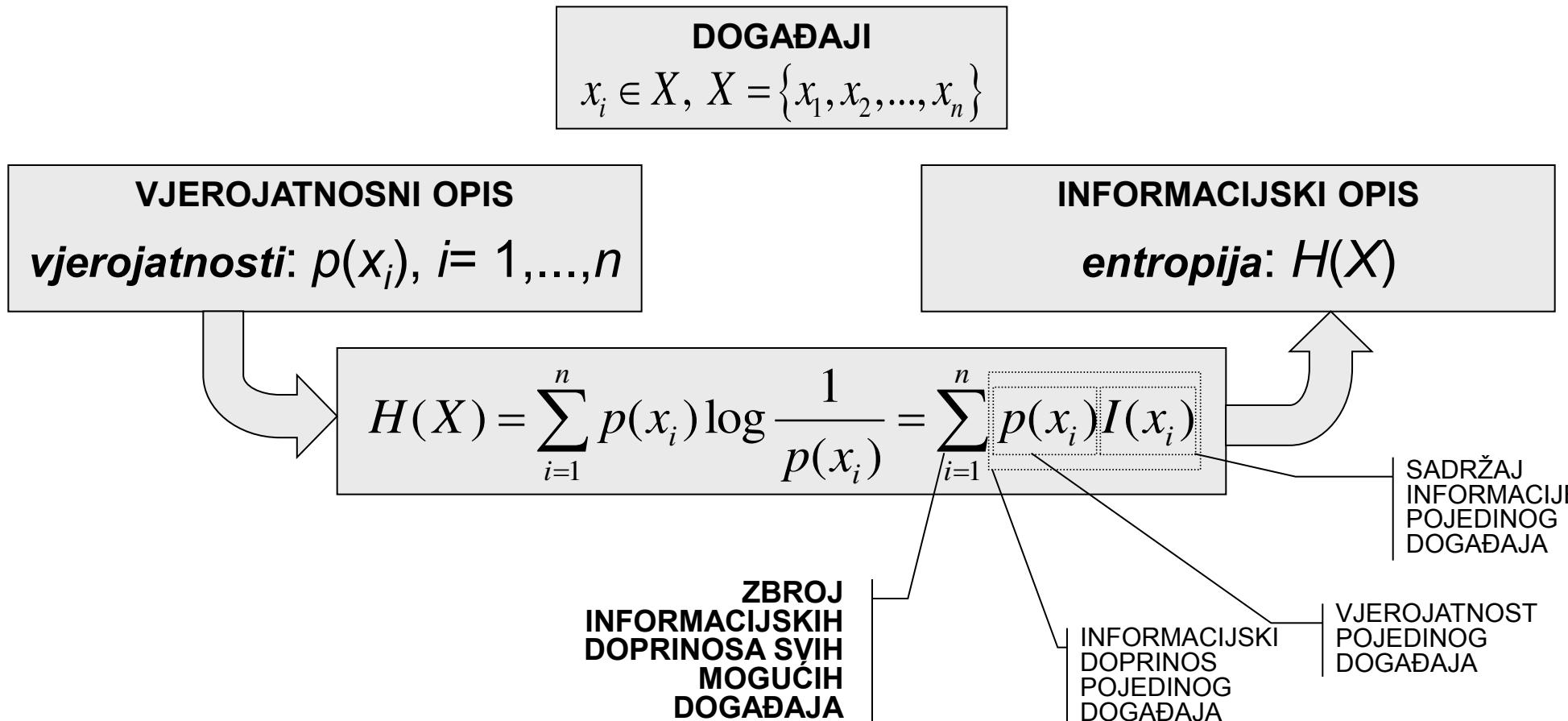
- a) nacrtati graf prijelaza u kanalu.
- b) odrediti vjerojatnost pojave pojedinog simbola na izlazu iz kanala

Odnosi vjerojatnosti u inf. sustavu (kanalu)

MATEMATIČKI OPIS	ZNAČENJE
$\sum_{i=1}^n p(x_i) = \sum_{j=1}^m p(y_j) = 1$	Skup simbola na ulazu je potpun; isto vrijedi i za izlaz.
$p(x_i) = \sum_{j=1}^m p(x_i, y_j), p(y_j) = \sum_{i=1}^n p(x_i, y_j)$	Vjerojatnost pojave simbola je zbroj vjerojatnosti pojave svih parova u kojima se taj simbol pojavljuje.
$p(x_i, y_j) = p(x_i)p(y_j x_i) = p(y_j)p(x_i y_j)$	Prijelazi između tri pogleda na sustav (pogled s ulaza, s izlaza ili oboje istovremeno). Veza između tri načina potpunog opisa sustava.
$p(x_i y_j) = \frac{p(x_i, y_j)}{p(y_j)} = \frac{p(x_i, y_j)}{\sum_{i=1}^n p(x_i, y_j)} = \frac{p(x_i)p(y_j x_i)}{\sum_{i=1}^n p(x_i)p(y_j x_i)}$	Prijelaz iz apriorne u aposteriornu vjerojatnost pojave x_i . Izračun unazadnih vjerojatnosti prijelaza. Bayesova formula.

Vjerojatnosni opis → informacijski opis

- Entropija: informacijski opis slučajnih događaja



- vlastite entropije {
 - $H(X)$ ◆ Entropija na ulazu sustava
 - $H(Y)$ ◆ Entropija na izlazu sustava
 - $H(X, Y)$ ◆ Združena entropija

- uvjetne entropije {
 - $H(Y|X)$ ◆ Entropija šuma, irelevantnost
 - $H(X|Y)$ ◆ Ekvivokacija, mnogoznačnost
 - $I(X; Y)$ ◆ Srednji uzajamni sadržaj informacije, transinformacija

Entropija na ulazu, izlazu, združena entropija

Zavod za telekomunikacije

- ◆ Promatramo događaje na ulazu i izlazu odvojeno:

$$H(X) = - \sum_{i=1}^n p(x_i) \log p(x_i) \quad H(Y) = - \sum_{j=1}^m p(y_j) \log p(y_j)$$

- ◆ Promatramo događaje zajednički:
 - Združena entropija para slučajnih varijabli (definicija):

$$H(X, Y) = - \sum_{i=1}^n \sum_{j=1}^m p(x_i, y_j) \log p(x_i, y_j)$$

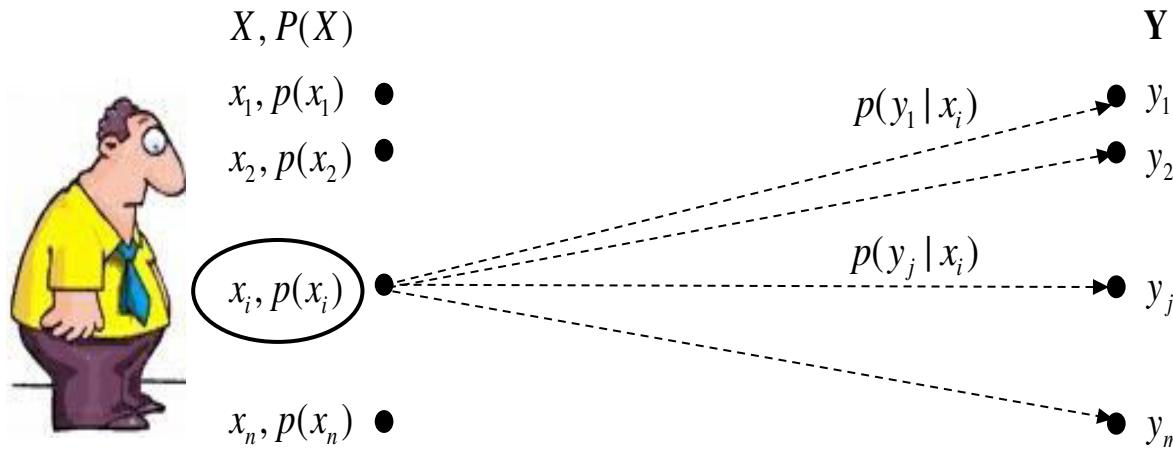
Uvjetna entropija (općenito)

- ◆ Prosječna preostala neodređenost varijable Y nakon što je poznata varijabla X

$$\begin{aligned} H(Y | X) &= \sum_{i=1}^n p(x_i) H(Y | x = x_i) \\ &= -\sum_{i=1}^n p(x_i) \sum_{j=1}^m p(y_j | x_i) \log p(y_j | x_i) \\ &= -\sum_{i=1}^n \sum_{j=1}^m p(x_i, y_j) \log p(y_j | x_i) \end{aligned}$$

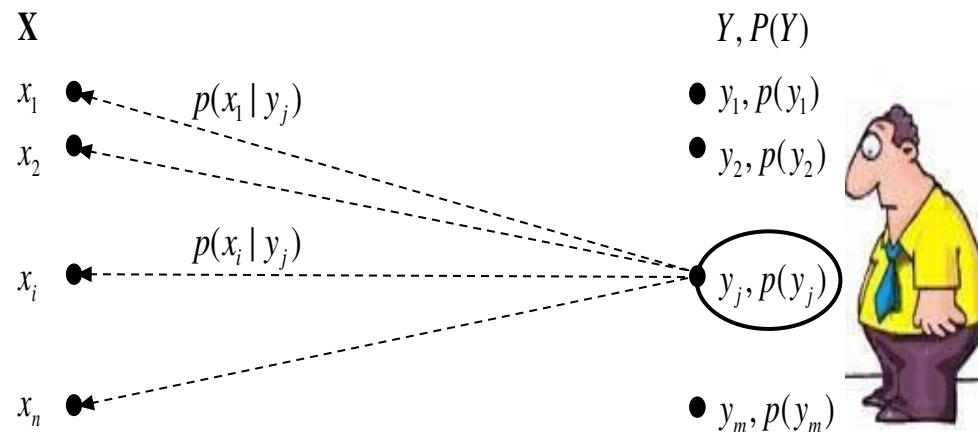
Entropija šuma ili irelevantnost

- ◆ Uvjetna entropija $H(Y|X)$
- ◆ Neodređenost simbola na izlazu nakon što je poslan simbol sa ulaza (promatrano s ulaza)
- ◆ Posljedica smetnji



Mnogoznačnost ili ekvivokacija

- ◆ Uvjetna entropija $H(X|Y)$
- ◆ Preostala neodređenost simbola na ulazu nakon što je primljen simbol na izlazu (promatrano s izlaza)



Relativna entropija

Zavod za telekomunikacije

- ◆ Mjera udaljenosti između dviju raspodjela vjerojatnosti varijable:

$$D(p \parallel q) = \sum_{i=1}^n p(x_i) \log \frac{p(x_i)}{q(x_i)}$$

- ◆ Interpretacija
 - Stvarne vjerojatnosti su p ; mi prepostavljamo q
 - Ta pogreška nosi neefikasnost; to je relativna entropija
 - Kodiranjem prema pogrešnim vjerojatnostima trošimo $D(p||q)$ više bitova po simbolu nego što je potrebno:

$$L = \sum_{i=1}^n p(x_i) \log \frac{1}{q(x_i)} = \sum_{i=1}^n p(x_i) \log \frac{1}{p(x_i)} + \sum_{i=1}^n p(x_i) \log \frac{p(x_i)}{q(x_i)} = H(X) + D(p \parallel q)$$

Srednji uzajamni sadržaj informacije (transinformacija)

- ◆ Definicija:

$$I(X;Y) = \sum_{i=1}^n \sum_{j=1}^m p(x_i, y_j) \log \frac{p(x_i, y_j)}{p(x_i)p(y_j)}$$

- ◆ Interpretacija:

- Koliko informacije jedna varijabla pruža o drugoj
- U kojoj mjeri su dvije varijable zavisne
 - Nezavisne: $I(X;Y) = 0$
 - Jednake: $I(X;Y) = H(X) = H(Y)$

Odnos entropije i uzajamnog sadržaja informacije

- ◆ Uzajamni sadržaj informacije $I(X;Y)$ predstavlja smanjenje neodređenosti varijable X uzrokovano poznavanjem varijable Y

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

- ◆ Uzajamni sadržaj informacije dviju varijabli je simetričan:

$$I(Y;X) = I(X;Y).$$

Odnos između entropije, združene entropije i uvjetne entropije

- ◆ Združena entropija (neodređenost) para varijabli jednaka je zbroju neodređenosti jedne varijable, te preostale neodređenosti druge varijable uz uvjet da je prva varijabla poznata.

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

- ◆ Uzajamni sadržaj informacije je razlika između zbroja pojedinačnih entropija varijabli i združene entropije tih istih varijabli.

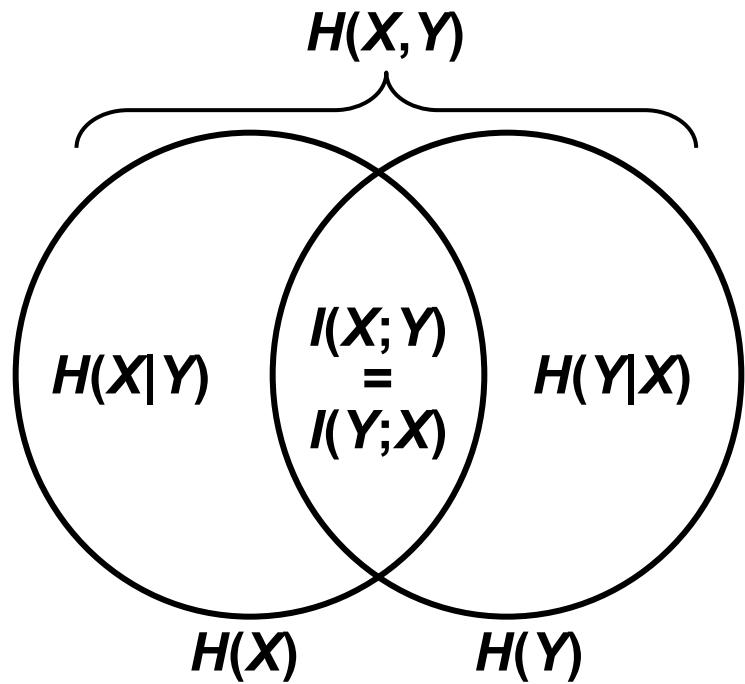
$$I(X; Y) = H(X) + H(Y) - H(X, Y)$$

Vlastiti sadržaj informacije

- ◆ Uzajamni sadržaj informacije jedne varijable same sa sobom naziva se vlastiti sadržaj informacije.
- ◆ Vlastiti sadržaj informacije slučajne varijable je upravo njena entropija:

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

Odnosi i svojstva informacijskih mjera



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

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

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

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

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

$$I(X;Y) = I(Y;X)$$

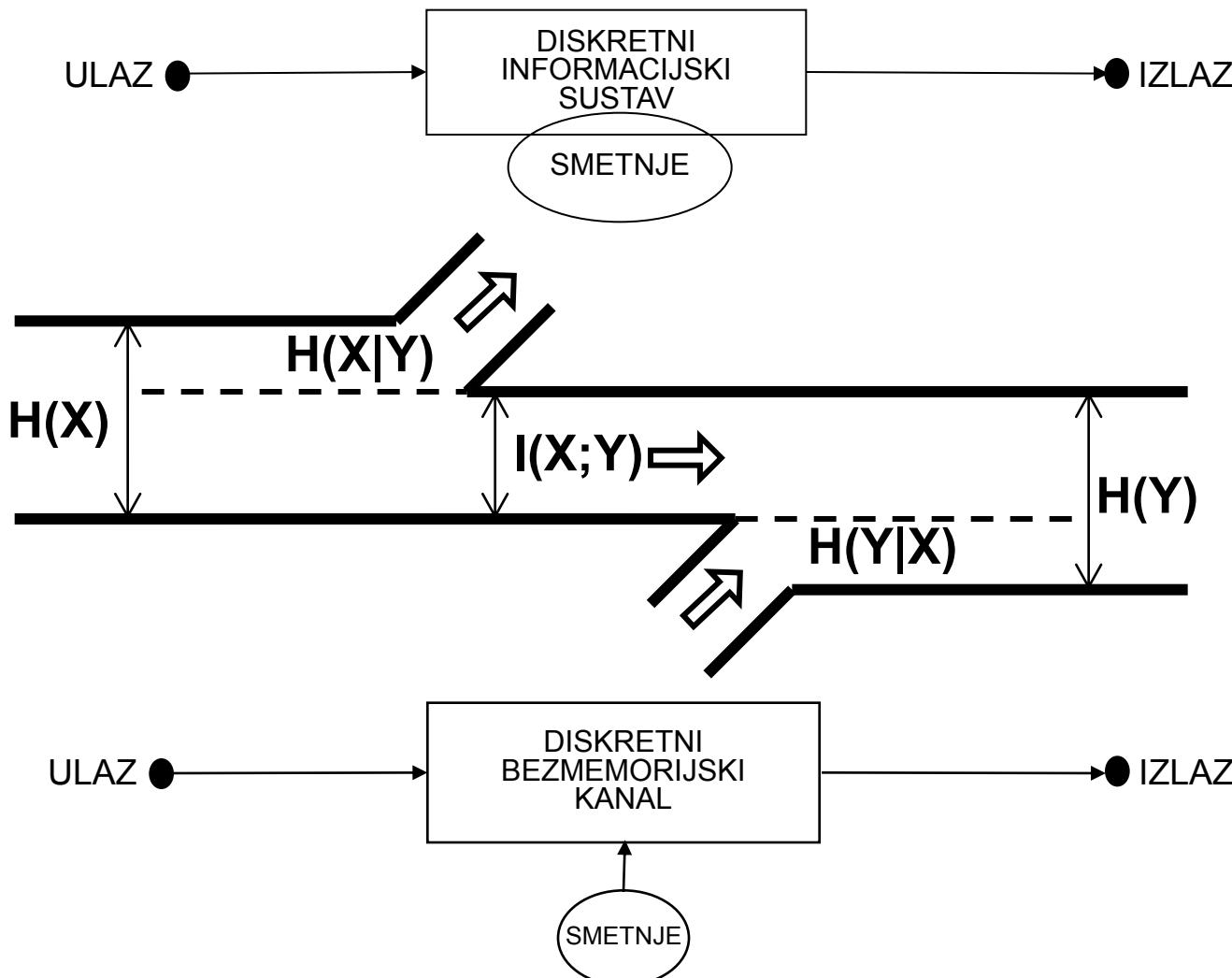
$$I(X;X) = H(X)$$

$$I(X;Y) \geq 0$$

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

Prijenos informacije i informacijske mjere

Zavod za telekomunikacije



Primjer

- ◆ Za komunikacijski sustav zadan u prethodnom primjeru matricom uvjetnih vjerojatnosti potrebno je odrediti:
 - a) entropiju ulaznog i izlaznog skupa simbola, tj. $H(X)$ i $H(Y)$;
 - b) uvjetne entropije $H(X|Y)$ i $H(Y|X)$;
 - c) uzajamni sadržaj informacije $I(X; Y)$;
 - d) združenu entropiju para varijabli $H(X, Y)$.

Kapacitet kanala

- ◆ Promatramo prijenos informacije kom. kanalom
- ◆ Simboli na ulazu s vjerojatnostima $p(x_i)$
- ◆ Kapacitet kanala je definiran kao:

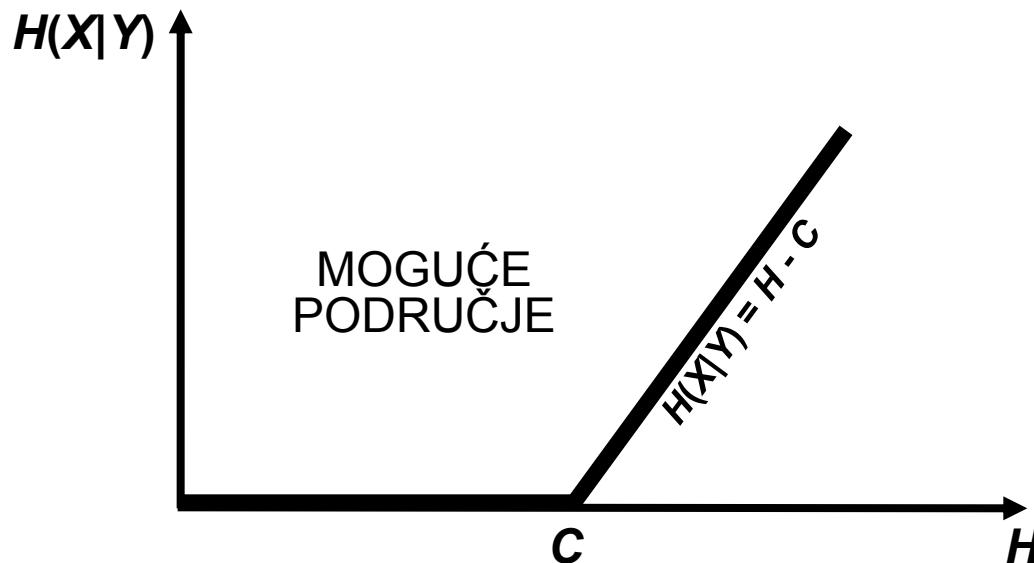
$$C = \max_{\{p(x_i)\}} I(X;Y) \text{ [bit/simbol]}$$

Kapacitet kanala je maksimalna količina informacije po simbolu koja se u prosjeku može prenijeti kanalom

Temeljni teorem kanala sa smetnjama

Zavod za telekomunikacije

- ◆ Kanal kapaciteta C [bit/simbol]
- ◆ Izvor entropije H [bit/simbol]
- ◆ Ako je $H \leq C$, mogući proizvoljno mali gubici
- ◆ Ako je $H > C$, nemoguć prijenos bez gubitaka

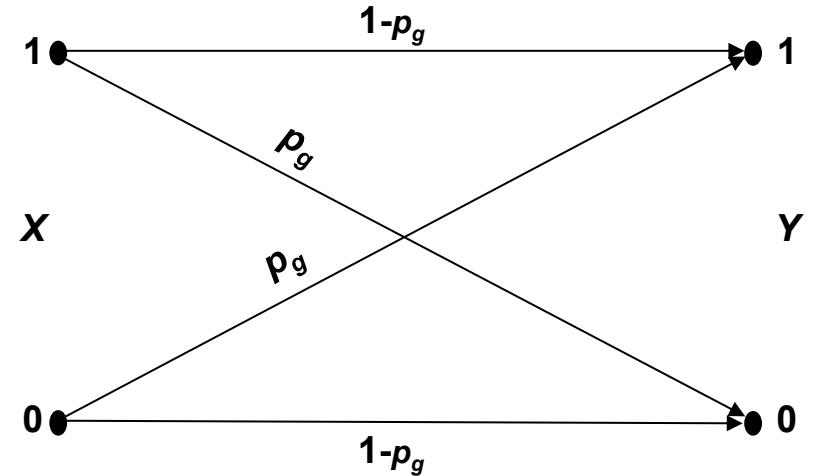


Primjer: kapacitet simetričnog binarnog kanala

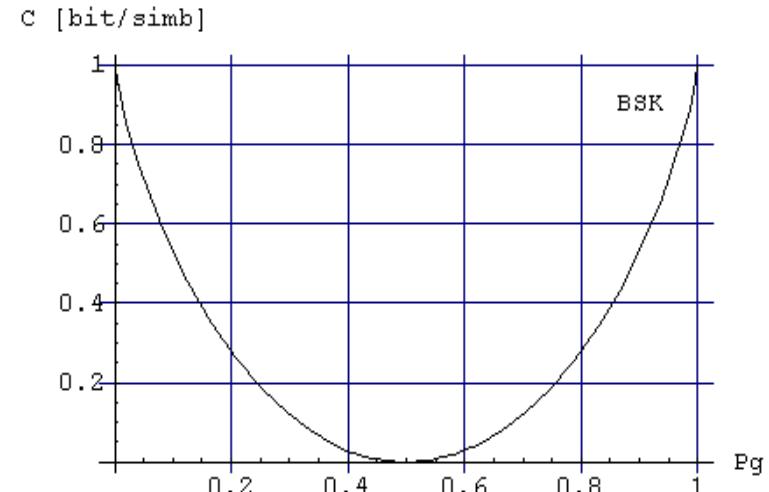
$$C = \max_{\{p(x_i)\}} I(X;Y)$$

$$= \max_{\{p(x_i)\}} [H(Y) - H(Y | X)]$$

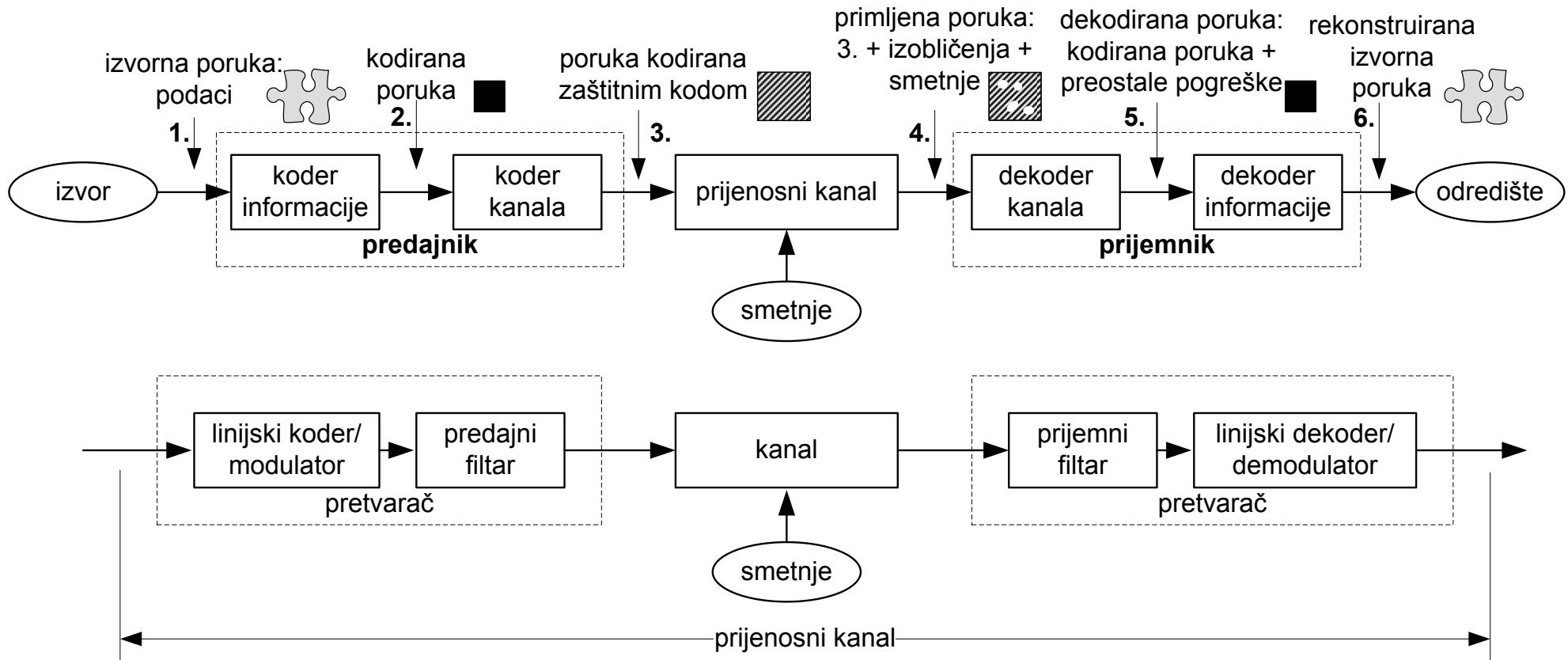
max. za
 $p(0)=p(1)=0.5$ neovisno
o $p(x_i)$



$$C = 1 + p_g \log p_g + (1 - p_g) \log(1 - p_g) [\text{bit} / \text{s}]$$



Prijenos informacije komunikacijskim sustavom

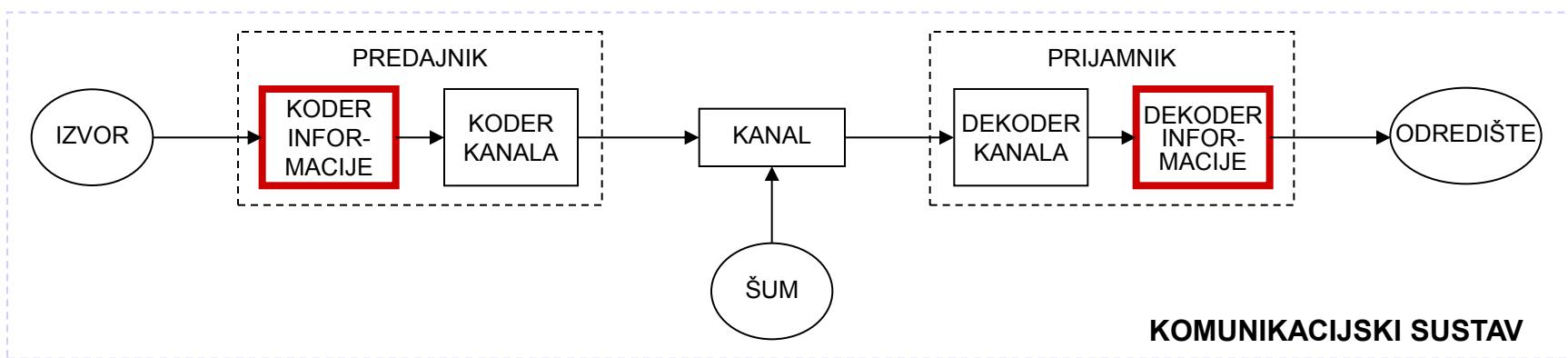


Teorija informacije

Entropijsko kodiranje

Kodiranje i kompresija

- ◆ Kodiranje: dodjela kodnih riječi simbolima poruke
- ◆ Kompresija: kodiranje koje smanjuje broj bitova potreban za izražavanje poruke
- ◆ U jasnom kontekstu, koristimo ove pojmove kao sinonime
- ◆ Kompresija se vrši u koderu informacije



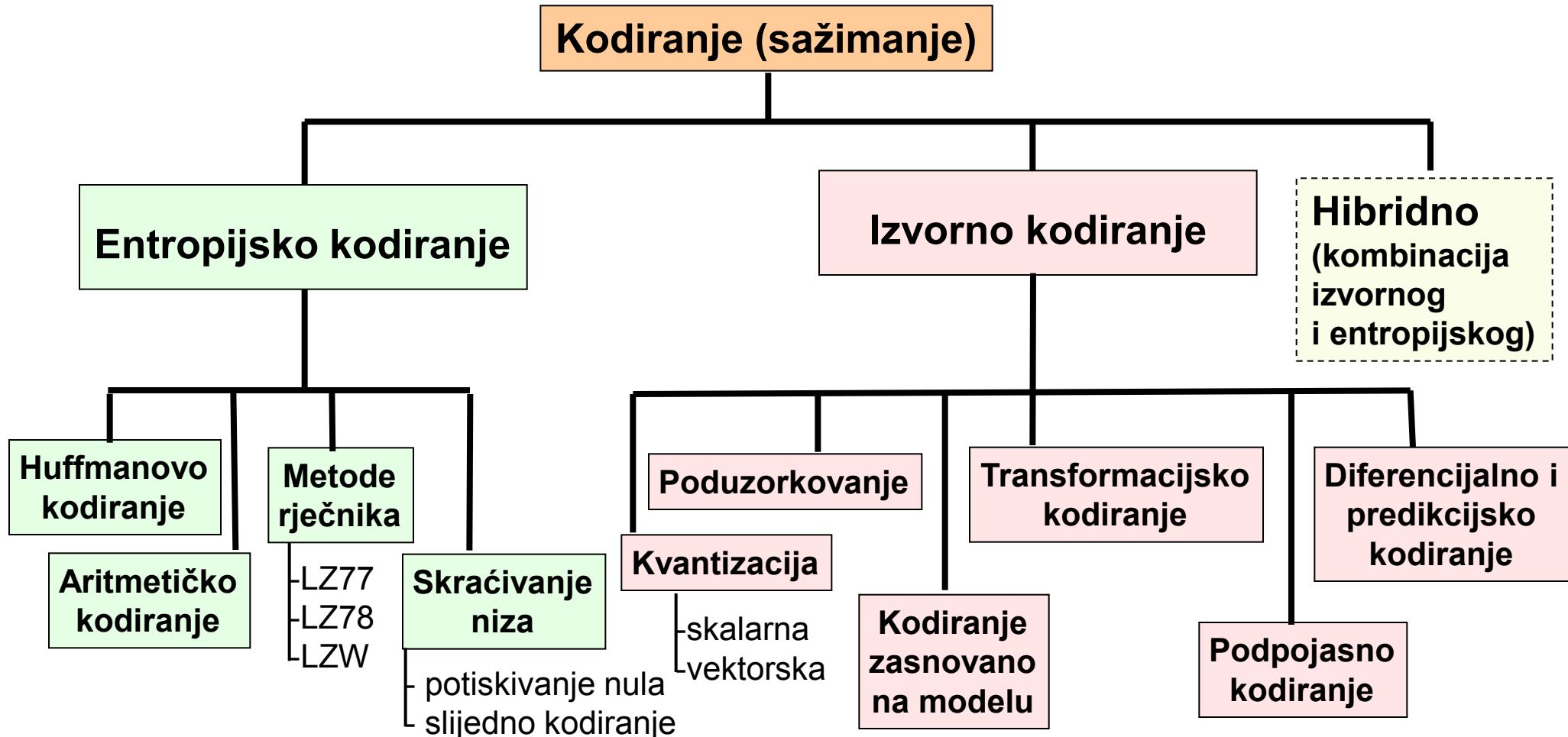
Entropijsko kodiranje

- ◆ Uvod u kodiranje i kompresiju
 - Definicije, podjela metoda kompresije
 - Uvod u entropijsko kodiranje
- ◆ Karakteristike izvora informacije
 - Stacionarni izvor, ergodički izvor, izvori s memorijom (Markovljevi)
- ◆ Vrste kodova i njihova svojstva
 - Singularni, nesingularni, jednoznačno dekodabilni, prefiksni kodovi
- ◆ Optimalno kodiranje
- ◆ Metode entropijskog kodiranja
 - Shannon-Fanoovo kodiranje
 - Huffmanovo kodiranje
 - Aritmetičko kodiranje
 - Metode rječnika (LZ77, LZ78, LZW)
 - Metode skraćivanja niza (potiskivanje nula, slijedno kodiranje)

Osnovna svojstva kompresije

- ◆ Kompresija **bez gubitaka**
 - Komprimirani podaci mogu se dekomprimiranjem rekonstruirati bez gubitka informacije (*reverzibilno*)
 - Primjene: npr. tekst, medicinske slike, satelitske snimke
- ◆ Kompresija **s gubicima**
 - Cilj je ili dobiti najbolju vjernost rekonstruiranih podataka za zadanu brzinu (bit/s) ili postići najmanju brzinu za zadanu granicu vjernosti
 - Primjene: npr. govor, slika, video
- ◆ Važan parametar je **omjer kompresije**
 - Omjer veličine komprimiranih i originalnih podataka, npr. 1:10

Klasifikacija postupaka kodiranja



Uvod u entropijsko kodiranje

- ◆ Osnovna ideja: skraćeno zapisati višestruko ili često ponavljane simbole ili nizove simbola
- ◆ Zajedničko svim metodama entropijskog kodiranja:
 - temelje se direktno na teoriji informacije
 - kodiranje bez gubitaka
 - omjer kompresije ovisi samo o statističkim svojstvima izvora informacije
 - poruka se promatra isključivo kao niz niz slučajnih vrijednosti, ne uzimaju se u obzir svojstva medija (za razliku od izvornog kodiranja)

Karakteristike izvora informacije

- ◆ Izvor informacije promatramo kao stohastički proces, tj. niz slučajnih varijabli:

$$X_1, X_2, \dots, X_n$$

- ◆ Izvor u potpunosti opisan raspodjelom zdrženih vjerojatnosti pojavljivanja varijabli:

$$P\{(X_1, X_2, \dots, X_n) = (x_1, x_2, \dots, x_n)\} = p(x_1, x_2, \dots, x_n)$$

- ◆ Općenito, moguća zavisnost među varijablama

Stacionarni izvor

- ◆ Statistička svojstva se ne mijenjaju s vremenom

$$P\{(X_1, X_2, \dots, X_n) = (x_1, x_2, \dots, x_n)\} = P\{(X_{1+l}, X_{2+l}, \dots, X_{n+l}) = (x_1, x_2, \dots, x_n)\},$$
$$\forall l, (x_1, x_2, \dots, x_n) \in X^n, n > 0$$

- ◆ Trivijalan primjer stacionarnog izvora:
AEAEAEAEAEAEAEAE.....
- ◆ Trivijalan primjer nestacionarnog izvora:
AEAAEEAAAEEEEAAAAEEEAAAAAEEEEEE...

Ergodički izvor

- ◆ Izvor kao skup svih mogućih proizvedenih nizova
 - Prosjek po skupu: prosjek pojavljivanja simbola na nekom mjestu u nizu, gledano među svim nizovima
 - Prosjek po vremenu: učestalost pojavljivanja simbola unutar pojedinog niza
- ◆ Ergodičnost: prosjek po skupu = prosjek po vremenu
- ◆ Svaki proizvedeni niz ima ista svojstva i ona se ne mijenjaju u vremenu
- ◆ Za entropijsko kodiranje promatramo ergodičke izvore (aproksimacija stvarnih izvora)

Ergodičnost izvora - primjer

- ◆ Izvor počinje $1/3$ sa A, $1/3$ B i $1/3$ E
 - Ako počne sa A ili B ponavlja ih izmjenično
 - Ako počne sa E, ponavlja samo E
 - Skup mogućih nizova:

Niz 1: ABABABABABABAB...

Niz 2: BABABABABABABA...

Niz 3: EEEEEEEEEE...

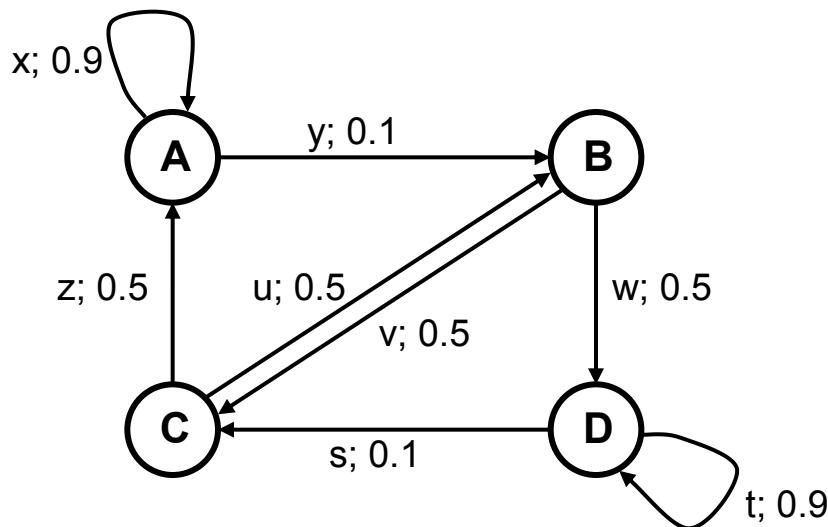
Simbol	Prosjek po vremenu za niz 1	Prosjek po vremenu za niz 2	Prosjek po vremenu za niz 3	Prosjek po skupu
A	$\frac{1}{2}$	$\frac{1}{2}$	0	$\frac{1}{3}$
B	$\frac{1}{2}$	$\frac{1}{2}$	0	$\frac{1}{3}$
E	0	0	1	$\frac{1}{3}$

Izvori s memorijom

- ◆ Vjerojatnost pojavljivanja simbola je ovisna o jednom ili više prethodnih simbola
- ◆ Neki nizovi simbola vjerojatniji od drugih
- ◆ Većina prirodnih izvora su izvori s memorijom
 - Npr. iz slova u tekstu, zvuk govora, slika

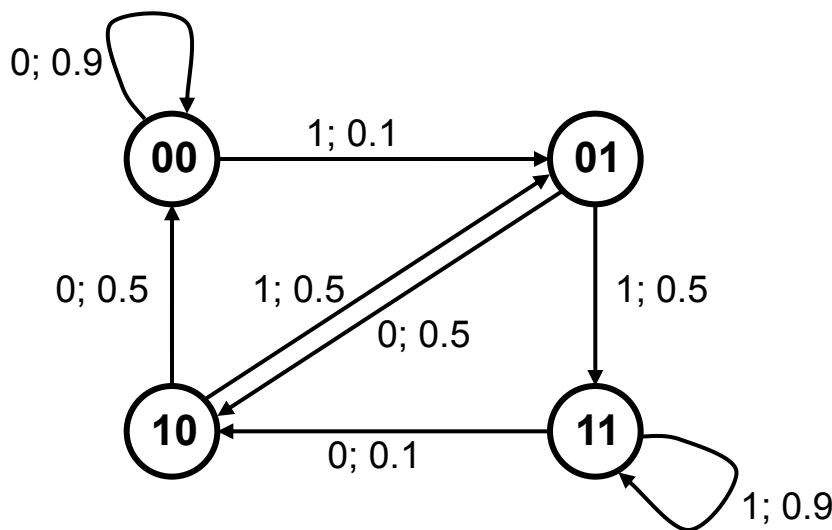
Markovljevi informacijski izvori

- ◆ Izvori s memorijom često se mogu opisati pomoću Markovljevih
- ◆ Stanja, vjerojatnosti prijelaza
- ◆ Pri prijelazu stanja generira se simbol



Primjer Markovljevog izvora

- ◆ Binarni Markovljev izvor s memorijom od dva simbola



- ◆ Tipičan izlaz:

0000000000000000111111111111111100001111111111000001111111111111...

Kodiranje

- ◆ Dodjela kodnih riječi simbolima poruke

$$X = \{x_1, x_2, \dots, x_i, \dots, x_n\}$$

$$x_i \in X \xrightarrow{\text{KODIRANJE}} C(x_i)$$

$$C(x_i) \in D^*, D = \{a_1, a_2, \dots, a_d\},$$

- ◆ Kodiranje sa svojstvom sažimanja: kompresija
- ◆ U praksi gotovo uvijek binarna abeceda
 - $d = 2, D = \{0, 1\}$
 - Izlaz kodera: struja bitova (engl. *bitstream*)

Prosječna duljina kodne riječi

- ◆ Duljina pojedine kodne riječi: $l(x_i)$, skraćeno l_i
 - broj simbola koji čine tu kodnu riječ
- ◆ Prosječna duljina kodne riječi (prosječna duljina koda):
$$L = \sum_{i=1}^n p(x_i)l(x_i) = \sum_{i=1}^n p_i l_i$$
- ◆ Za dugačku poruku od N simbola, očekivana duljina kodirane poruke je NL
- ◆ L [bit/simbol] je mjera efikasnosti koda

Primjer kodiranja 1

SIMBOL (x_i)	VJEROJATNOST POJAVLJIVANJA $p(x_i) = p_i$	KODNA RIJEČ (C_i)	DULJINA KODNE RIJEĆI (l_i)
1	1/2	0	1
2	1/4	10	2
3	1/8	110	3
4	1/8	111	3

- ◆ Prosječna duljina kodne riječi:

$$L = \sum_{i=1}^n p_i l_i = 0.5 \cdot 1 + 0.25 \cdot 2 + 0.125 \cdot 3 + 0.125 \cdot 3 = 1.75 [\text{bit / simbol}] = H(X)$$

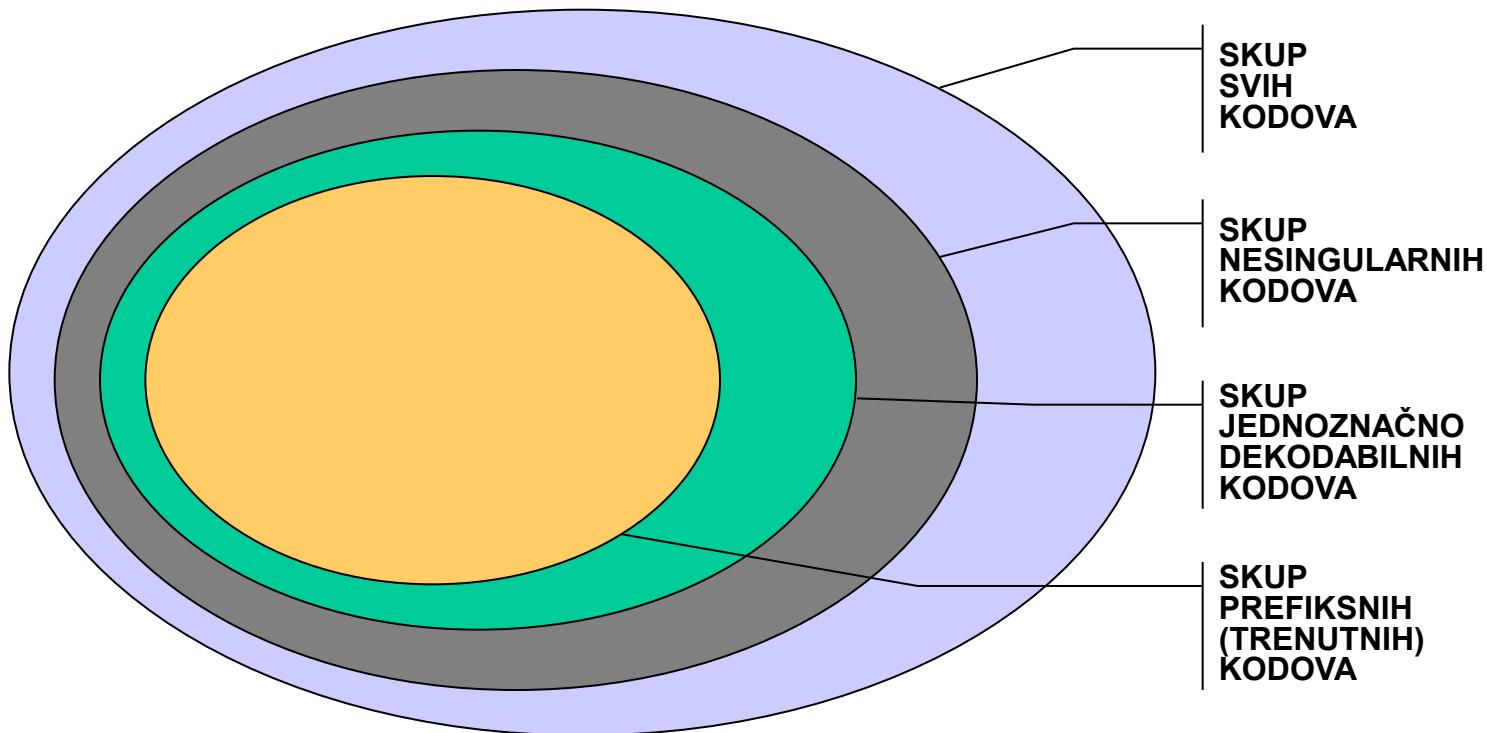
Primjer kodiranja 2

SIMBOL (x_i)	VJEROJATNOST POJAVLJIVANJA $p(x_i) = p_i$	KODNA RIJEČ (C_i)	DULJINA KODNE RIJEĆI (l_i)
1	1/3	0	1
2	1/3	10	2
3	1/3	11	2

$$H(X) = -\sum_{i=1}^n p_i \log p_i = -\log \frac{1}{3} = 1.58 \text{ [bit/simbol]},$$

$$L = \sum_{i=1}^n p_i l_i = \frac{1}{3} \cdot 1 + \frac{1}{3} \cdot 2 + \frac{1}{3} \cdot 2 = 1.66 \text{ [bit/simbol]}.$$

Vrste kodova



Nesingularni kodovi

- ◆ Kod je nesingularan ako svakom simbolu dodjeljuje drugačiju kodnu riječ

$$x_i \neq x_j \Rightarrow C(x_i) \neq C(x_j)$$

- ◆ To nije garancija jednoznačnosti
- ◆ Primjer:
 - Simboli A, B, C; kod: $C(A) = 0$, $C(B) = 01$ i $C(C) = 1$
 - “ABC” \rightarrow “0011”
 - “0011” \rightarrow ?

Jednoznačno dekodabilni kodovi

$$x \xrightarrow{KOD} C(x)$$

$$x_1 x_2 \dots x_n \xrightarrow{\text{PROŠIRENI KOD}} C(x_1 x_2 \dots x_n) = C(x_1)C(x_2) \dots C(x_n)$$

- ◆ Kod jednoznačno dekodabilan ako je proširenje nesingularno
 - Različite poruke → različite kodirane poruke
- ◆ Primjer:
 - Simboli A, B, C; kod: $C(A) = 0$, $C(B) = 01$ i $C(C) = 011$
 - “ABC” → ““001011” → “ABC”
 - “001...” → ?
- ◆ Ne može se trenutno dekodirati

Prefiksni (trenutni) kodovi

- ◆ Prefiksni kod je kod u kojem niti jedna kodna riječ nije prefiks neke druge kodne riječi
- ◆ Svaka kodna riječ se može trenutno dekodirati, bez znanja iduće kodne riječi
- ◆ U prethodnom primjeru, problem je upravo u tome što su kodne riječi jedna drugoj prefiks

Vrste kodova: primjer

SIMBOL (x_i)	VRSTA KODA			
	SINGULARNI	NESINGULARNI	JEDINSTVENO DEKODABILNI	PREFIKSNI
1	0	0	10	0
2	0	010	00	10
3	0	01	11	110
4	0	10	110	111
“1234” →	0000	00100110	100011110	010110111
Dekodirano	?	?	1234	1234
Prvih 6 simbola	?	?	? (123 ili 124)	123

Kraftova nejednakost

- ◆ Za svaki prefiksni kod sa abecedom od d simbola i duljinama kodnih riječi l_1, l_2, \dots, l_n vrijedi:

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

i obrnuto, za bilo koji skup duljina kodnih riječi li koje zadovoljavaju ovu nejednakost, postoji prefiksni kod s takvim duljinama kodnih riječi.

- ◆ Određuje minimalne duljine kodnih riječi potrebne za prefiksni kod

Kraftova nejednakost – primjeri

1. Prethodni primjer koda $\{0, 10, 110, 111\}$

- Binarna abeceda, $D=2$

$$\sum_{i=1}^n 2^{-l_i} \leq 1$$

$$2^{-1} + 2^{-2} + 2^{-3} + 2^{-3} = 1$$

- Nema kraćeg koda

2. Tražimo kod za tri simbola

$$2^{-1} + 2^{-2} + 2^{-2} = 1 \Rightarrow \text{mora postojati pref. kod duljina } 1, 2, 2$$

Optimalni kodovi (1/2)

- ◆ Općenito, više kodova zadovoljava K.N.; koji je optimalan?
 - npr: {0, 10, 110, 111}, {111, 0, 10, 110}...
- ◆ Optimalan kod: prefiksni kod sa najmanjom mogućom prosječnom duljinom kodne riječi

$$\min \left[L = \sum_{i=1}^n p_i l_i \right] \text{ uz uvjet } \sum_{i=1}^n d^{l_i} \leq 1$$

Optimalni kodovi (2/2)

- ◆ Minimum se dobiva za:

$$l_i^* = -\log_d p_i \Rightarrow L = -\sum_{i=1}^n p_i \log_d p_i = H(X)$$

- ◆ Ali l_i moraju biti cijeli brojevi, pa se ne može uvijek postići $L=H$:

$$L \geq H(X)$$

- ◆ Za optimalni kod, prosječna duljina kodne riječi je unutar jednog bita od entropije: $H(X) \leq L < H(X) + 1$

- ◆ Efikasnost koda:

$$\varepsilon = \frac{H(X)}{L}$$

Metode entropijskog kodiranja

- ◆ **Shannon-Fanoovo kodiranje**
- ◆ **Huffmanovo kodiranje**
 - optimalno kodiranje
 - binarno stablo
 - kraći zapis čestih znakova
- ◆ **Aritmetičko kodiranje**
 - poopćenje Huffmanovog kodiranja
 - cijela poruka se pretvara u jednu kodnu riječ
- ◆ **Metode rječnika**
 - isti rječnik kodnih riječi na strani pošiljatelja i primatelja
 - dinamička konstrukcija rječnika
 - Lempel-Ziv (LZ77, LZ78), Lempel-Ziv-Welch (LZW)
- ◆ **Metode skraćivanja niza**
 - potiskivanje nula, slijedno kodiranje

Shannon-Fanoovo kodiranje

- ◆ Jedna je od prvih metoda kodiranja utemeljenih na teoriji informacije
- ◆ Ne daje uvijek optimalan kod
 - Vrlo rijetko se koristi
- ◆ Zasniva se na željenim svojstvima kôda:
 - Niti jedna kodna riječ ne smije biti prefiks neke druge kodne riječi;
 - Želimo da se u kodiranim porukama simboli 0 i 1 pojavljuju s podjednakom vjerojatnošću.

Shannon-Fanoovo kodiranje: postupak

- ◆ Posložiti simbole po padajućim vjerojatnostima
- ◆ Podjela simbola u grupe
- ◆ Dodjela znamenke 0 jednoj, a 1 drugoj grupi
- ◆ Postupak se ponavlja dok se grupe ne svedu na 1 simbol

Shannon-Fanoovo kodiranje: primjer

x_i	$p(x_i)$	KORAK 1	KORAK 2	KORAK 3	KORAK 4	KODNA RIJEČ	DULJINA KODNE RIJEČI
x_1	0.25	0	0			00	2
x_2	0.25	0	1			01	2
x_3	0.125	1	0	0		100	3
x_4	0.125	1	0	1		101	3
x_5	0.0625	1	1	0	0	1100	4
x_6	0.0625	1	1	0	1	1101	4
x_7	0.0625	1	1	1	0	1110	4
x_8	0.0625	1	1	1	1	1111	4
Prosječna duljina kodne riječi:							2.75

Huffmanovo kodiranje

- ◆ D. A. Huffman, 1952. godine
- ◆ Kodira pojedinačne simbole kodnim riječima promjenjive duljine, ovisno o (poznatim!) vjerojatnostima njihova pojavljivanja
- ◆ Temelji se na dvije jednostavne činjenice:
 - (1) U optimalnom kodu, simboli s većom vjerojatnošću pojavljivanja imaju kraće kodne riječi od onih s manjom vjerojatnošću
 - (2) U optimalnom kodu, dva simbola s najmanjim vjerojatnostima imaju kodne riječi jednakog duljina (vrijedi za prefiksni kod)
- ◆ Ishod: sažetiji zapis (npr. tipičan tekst se sažima za 45%)

Huffmanovo kodiranje: postupak

- ◆ Algoritam stvaranja koda:

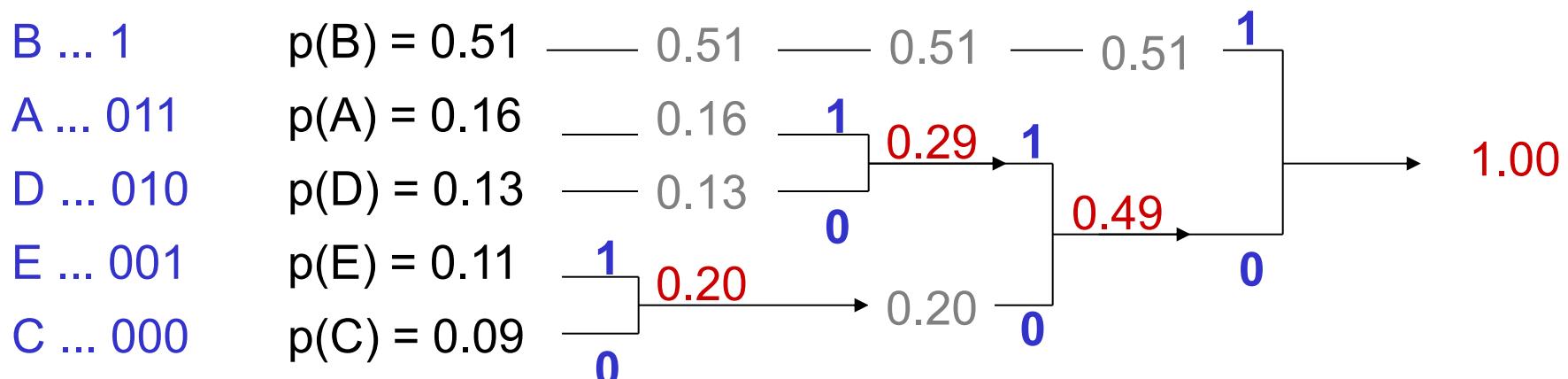
1. Sortiraj simbole po padajućim vjerojatnostima
2. Pronađi dva simbola s najmanjim vjerojatnostima
3. Jednom od njih dodijeli simbol "0", drugom "1"
4. Kombiniraj ta dva simbola u jedan nadsimbol (nadsimbol je novi simbol čija je vjerojatnost pojavljivanja jednaka zbroju vjerojatnosti pojavljivanja dvaju simbola od kojih je nastao) i zapiši ih kao dvije grane binarnog stabla, a nadsimbol kao račvanje iznad njih
5. Ponavljam 1-4 dok ne dobiješ samo jedan nadsimbol
6. Povratkom kroz stablo očitaj kodove

- ◆ Podatkovna struktura algoritma je binarno stablo

- ◆ Algoritam dekodiranja koristi isti postupak za gradnju stabla
 - Dekoder mora znati vjerojatnosti pojavljivanja simbola

Huffmanovo kodiranje: primjer

- ◆ Skup simbola $\{A, B, C, D, E\}$ s vjerojatnostima pojavljivanja $p(A) = 0.16$, $p(B) = 0.51$, $p(C) = 0.09$, $p(D) = 0.13$, $p(E) = 0.11$
- ◆ Za uniformni kod, prosječna duljina koda je **3 bit/simbol** (jer je $2^2 \leq 5 \leq 2^3$).
- ◆ Entropija: **1.96 bit/simbol**



- ◆ Prosječna duljina dobivenog koda u našem slučaju je:

$$L = \sum_{x \in X} p_x l_x = 3 \times (0.09 + 0.11 + 0.13 + 16) + 0.51 = \mathbf{1.98 \text{ bit/simbol}}$$

Huffmanovo kodiranje: svojstva

- ◆ kodiranje je idealno ako su vjerojatnosti $1/2, 1/4, \dots, 1/2^n$
- ◆ u stvarnim slučajevima to obično nije slučaj, te rezultat ovisi o vjerojatnostima pojavljivanja simbola
- ◆ prednosti:
 - jednostavan za izvedbu
 - vrlo dobro kodiranje za „dobre“ vjerojatnosti pojavljivanja simbola
- ◆ nedostaci:
 - vjerojatnosti pojavljivanja simbola moraju biti poznate; ovise o primjeni (tekst, slika)
 - za “loše raspoređene” vjerojatnosti pojavljivanja dobiju se izrazito loši kodovi

Primjer lošeg koda i prošireni Huffmanov kod

Simbol	Vjerojatnost	Kodna riječ
a_1	0.95	0
a_2	0.02	10
a_3	0.03	11

PROSIRENI KOD		
Simbol	Vjerojatnost	Kodna riječ
a_1a_1	0.9025	0
a_1a_2	0.0190	111
a_1a_3	0.0285	100
a_2a_1	0.0190	1101
a_2a_2	0.0004	110011
a_2a_3	0.0006	110001
a_3a_1	0.0285	101
a_3a_2	0.0006	110010
a_3a_3	0.0009	110000

- ◆ Entropija: 0.335 bit/simbol
- ◆ Prosječna duljina: 1.05 bit/simbol: **213% više od entropije!!**
- ◆ Prošireni kod: $1.222 / 2 = 0.611$ bit/simbol: 72% više od entropije.
- ◆ Bolje je kodirati duže sekvence, ali tada broj kodnih riječi raste eksponencijalno

Huffmanovo kodiranje: primjene

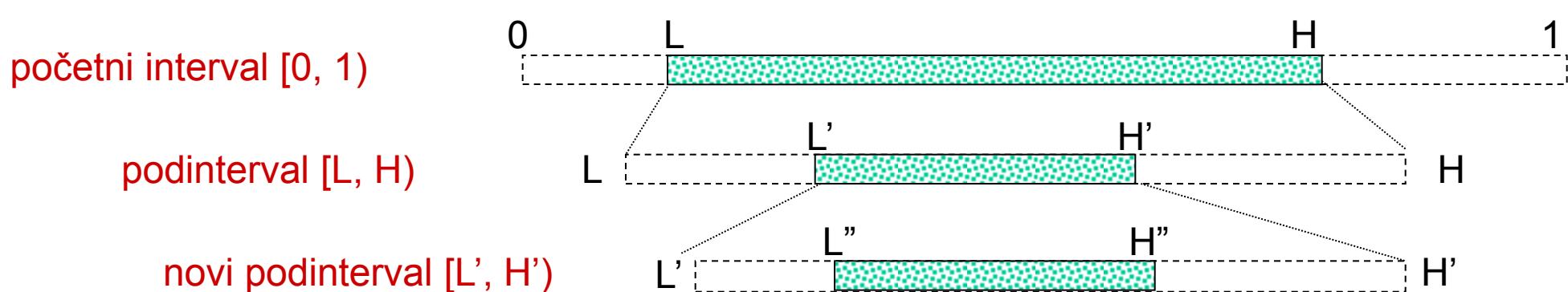
- ◆ Česta primjena unutar složenijih algoritama
- ◆ Primjeri:
 - standardi za telefaks (T.4, T.6)
 - standard za nepomičnu sliku JPEG

Aritmetičko kodiranje

- ◆ Autori Pasco & Rissanen (nezavisno), 1976. godine
- ◆ Algoritam uzima kao ulaz cijele nizove simbola (“poruke”) i preslikava ih na realne brojeve, ovisno o (poznatim!) statističkim svojstvima

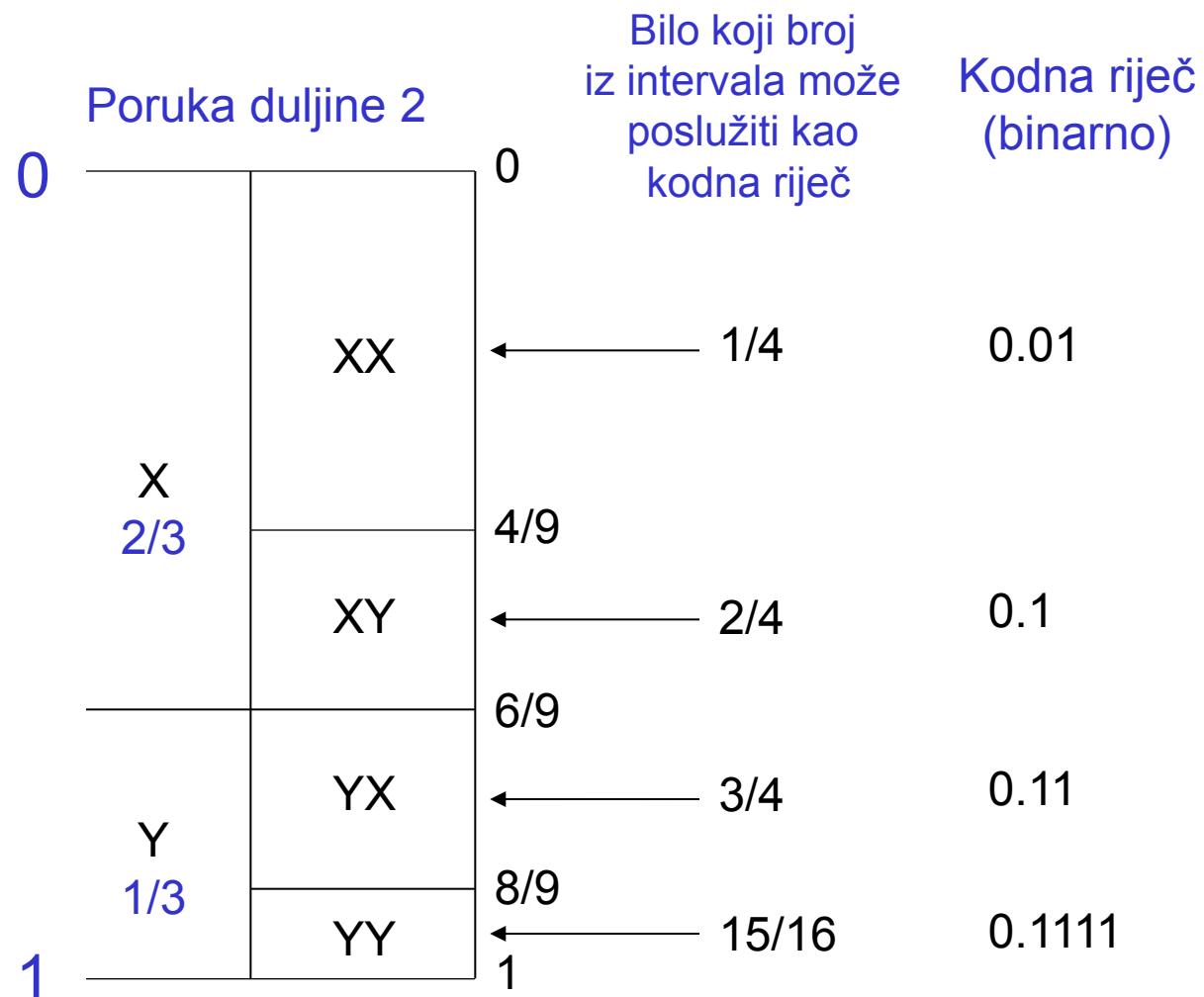
Aritmetičko kodiranje: postupak

1. Podijeli interval $[0, 1)$ u n podintervala koji odgovaraju simbolima iz abecede; duljina svakog podintervala proporcionalna vjerojatnosti odgovarajućeg simbola
2. Iz promatranih skupa podintervala, odaberi podinterval koji odgovara sljedećem simbolu u poruci
3. Podijeli taj podinterval u n novih podintervala, proporcionalno vjerojatnostima pojavljivanja simbola iz abecede; tako nastaje novi skup podintervala koji promatramo
4. Ponavljam korake 2 i 3 dok cijela poruka nije kodirana
5. Konačni kod za čitavu poruku je jedan broj iz intervala u binarnom obliku



Aritmetičko kodiranje: primjer (1)

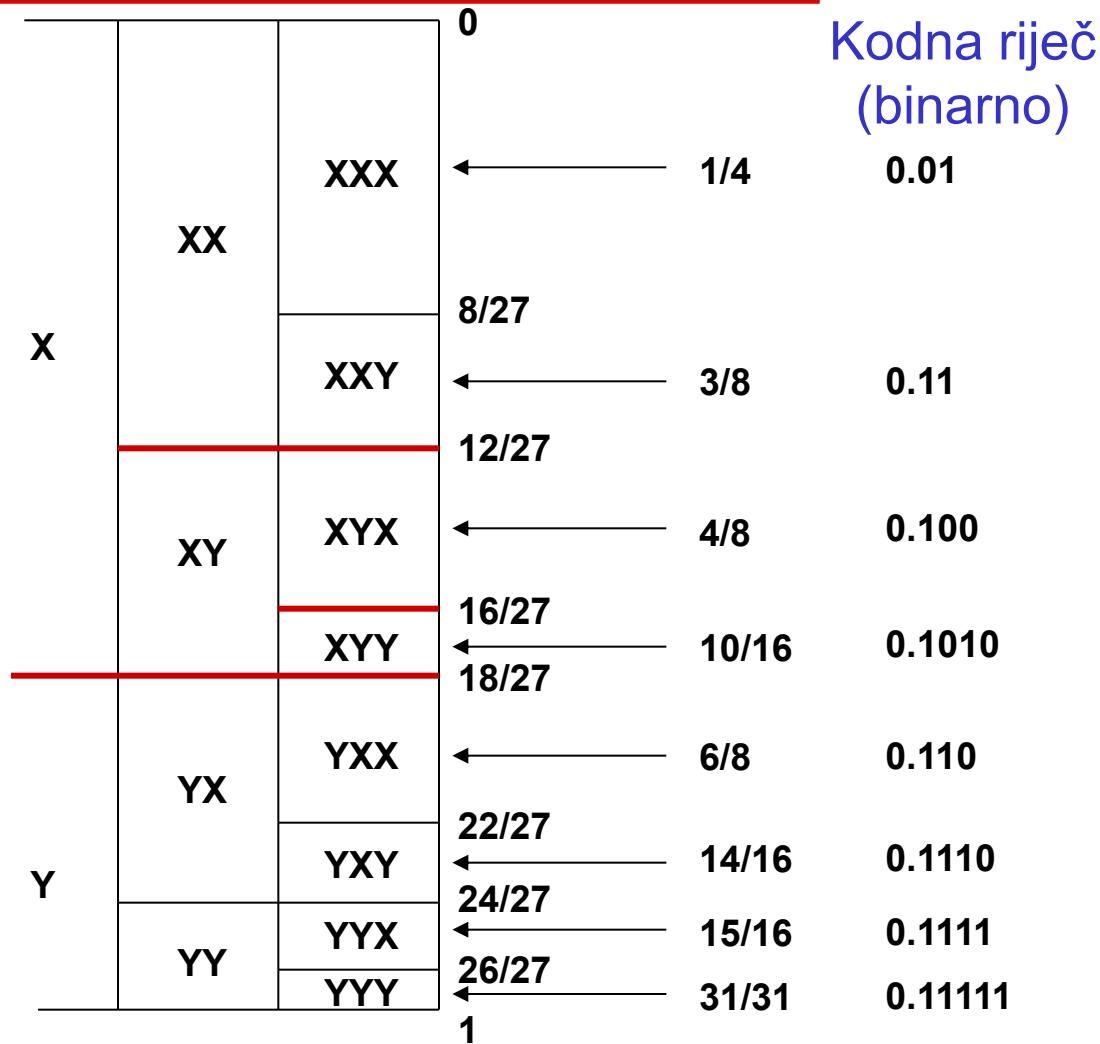
- $M=2$
- simboli: X, Y
- $p(X) = 2/3$
- $p(Y) = 1/3$
- poruka duljine 2 (moguće poruke XX, XY, YX, YY) kodira se onim brojem bita dovoljnim za jedinstveno određivanje intervala (binarni razlomak!)



Aritmetičko kodiranje: primjer (2)

- primjer za poruku duljine 3

- $M=2$
- simboli:
X, Y
 $p(X) = 2/3$
 $p(Y) = 1/3$



Postupak dekodiranja

1. Podijeli početni interval $[0, 1)$ u podintervale po vjerojatnostima pojavljivanja simbola
2. Uzmi primljeni kod kao realni broj
3. Pronađi podinterval u kojem se nalazi broj (kod)
4. Zapiši simbol koji odgovara tom podintervalu
5. Podijeli taj podinterval u n novih podintervala, proporcionalno vjerojatnostima pojavljivanja simbola iz abecede; tako nastaje novi skup podintervala koji promatramo
6. Ponavljam korake 3-5 dok ne dođe kraj poruke

Dekodiranje: primjer

- primjer za poruku duljine 3

- $M=2$

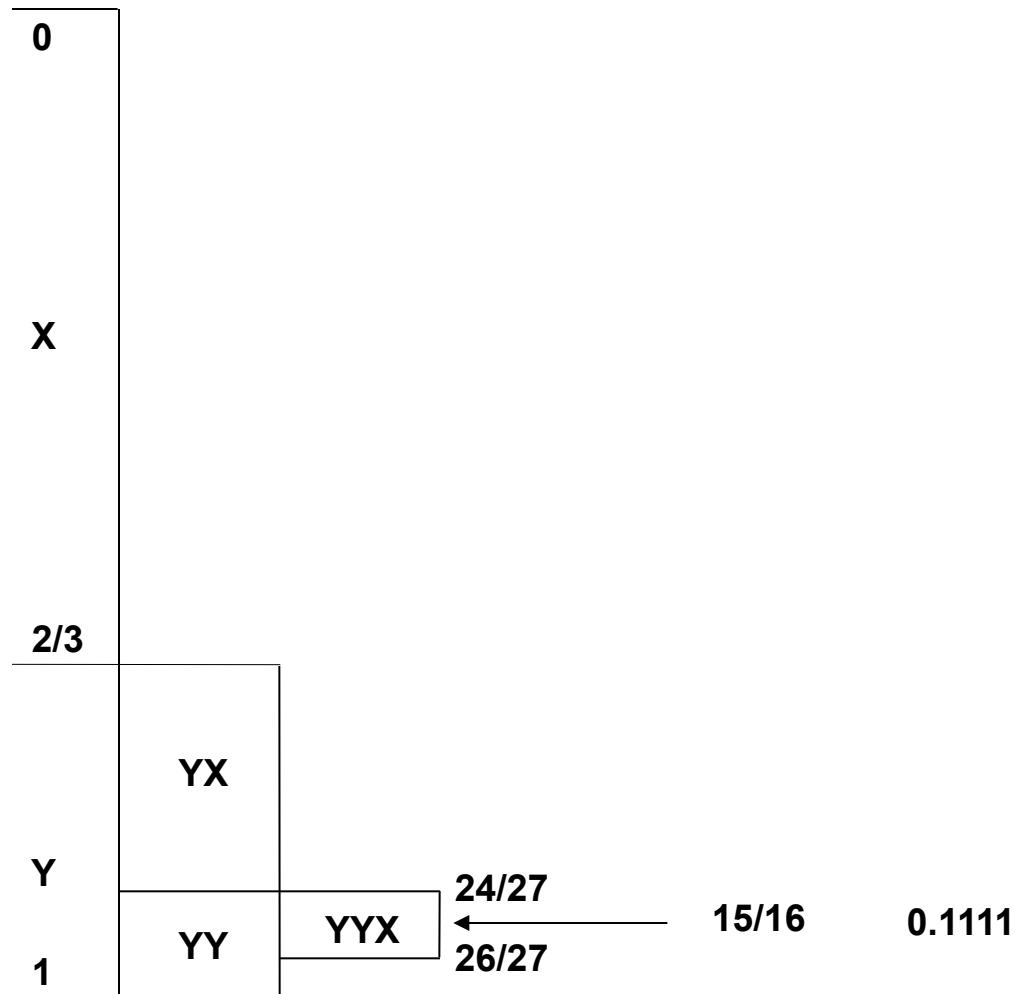
- simboli:

X, Y

$$p(X) = 2/3$$

$$p(Y) = 1/3$$

- Primljeni kod 1111
tj. 15/16



Odabir koda

- ◆ Kojim brojem iz podintervala kodirati poruku?
- ◆ Može se uzeti bilo koja vrijednost iz podintervala
- ◆ Dovoljan broj znamenki:

$$l(x) = \left\lceil \log \frac{1}{P(x)} \right\rceil + 1 \text{ [bit]}$$

- ◆ Na ovakav način dobiva se uvijek prefiksni kod

Implementacija

- ◆ Do sada opisani algoritam neupotrebljiv
 - Neprihvatljivo čekanje do kraja poruke
 - Algoritam podrazumijeva beskonačnu preciznost realnih brojeva – na računalu prikaz s pomičnim zarezom
 - Operacije s realnim brojevima su skupe
- ◆ Potreban je algoritam koji:
 - Koristi operacije sa cijelim brojevima
 - Koristi prikaz sa fiksnim brojem bitova
 - Proizvodi simbole koda tokom postupka kodiranja, a ne na kraju

Aritmetičko kodiranje: praktičan postupak

- ◆ Osnovni postupak podjele na podintervale je isti
- ◆ Koristi se fiksni broj znamenki za prikaz intervala
- ◆ Kada je prva znamenka u prikazu gornje i donje granice ista, interval se *renormalizira*:
 - Prvih n znamenki se šalje na izlaz kodera
 - Znamenke se pomiću ulijevo za jedno mjesto
 - Desno se dodaje znamenka: 0 na donju, 1 na gornju granicu intervala (ako su znamenke binarne)

Renormalizacija: primjer

x	p(x)
RAZMAK	1/10
A	1/10
B	1/10
E	1/10
G	1/10
I	1/10
L	2/10
S	1/10
T	1/10

		GORNJA GRANICA	DONJA GRANICA	DULJINA INTERVALA	KUMULATIVNI IZLAZ
Početno stanje		99999	00000	100000	
Kodiraj B (0.2-0.3)		29999	20000		
Renormalizacija, izlaz: 2		99999	00000	100000	.2
Kodiraj I (0.5-0.6)		59999	50000		.2
Renormalizacija, izlaz: 5		99999	00000	100000	.25
Kodiraj L (0.6-0.8)		79999	60000	20000	.25
Kodiraj L (0.6-0.8)		75999	72000		.25
Renormalizacija, izlaz: 7		59999	20000	40000	.257
Kodiraj RAZMAK (0.0-0.1)		23999	20000		.257
Renormalizacija, izlaz: 2		39999	00000	40000	.2572
Kodiraj G (0.4-0.5)		19999	16000		.2572
Renormalizacija, izlaz: 1		99999	60000	40000	.25721
Kodiraj A (0.1-0.2)		67999	64000		.25721
Renormalizacija, izlaz: 6		79999	40000	40000	.257216
Kodiraj T (0.9-1.0)		79999	76000		.257216
Renormalizacija, izlaz: 7		99999	60000	40000	.2572167
Kodiraj E (0.3-0.4)		75999	72000		.2572167
Renormalizacija, izlaz: 7		59999	20000	40000	.25721677
Kodiraj S (0.8-0.9)		55999	52000		.25721677
Renormalizacija, izlaz: 5		59999	20000		.257216775
Renormalizacija, izlaz: 2					.2572167752
Renormalizacija, izlaz: 0					.25721677520

Usporedba aritmetičko - Huffman

Huffman	Aritmetičko kodiranje
Kodira svaki simbol posebno	Kodira cijelu poruku jednim kodom: realni broj 0 - 1
Minimalno 1 bit/simbol	Moguće < 1 bit/simbol
Duljina poruke nije važna	Teoretski optimalno za dugačke poruke
Kodiranje niza simbola moguće samo proširenim Huffman kodom	Uvijek se kodira cijela poruka
Jednostavno za računanje	Zahtjevnije za računanje

Aritmetičko kodiranje: primjene

- ◆ Primjena kao komponente u raznim standardima i za razne vrste medija
- ◆ Dokumenti
 - JBIG (Joint Bi-level Image Processing Group)
- ◆ Slika
 - JPEG
- ◆ Sintetički sadržaji/animacija
 - MPEG-4 FBA (Face and Body Animation)

Metode rječnika

- ◆ Algoritmi kodiranja metodama rječnika uzimaju kao ulaz nizove simbola ("riječi") promjenjive duljine i kodiraju ih kodnim riječima stalne duljine iz rječnika
- ◆ Ne trebaju znati vjerojatnosti pojavljivanja simbola, nazivaju se i *univerzalni koderi*
- ◆ Koder i dekoder moraju imati isti rječnik
- ◆ Rječnik može biti statičan, no najčešće je prilagodljiv

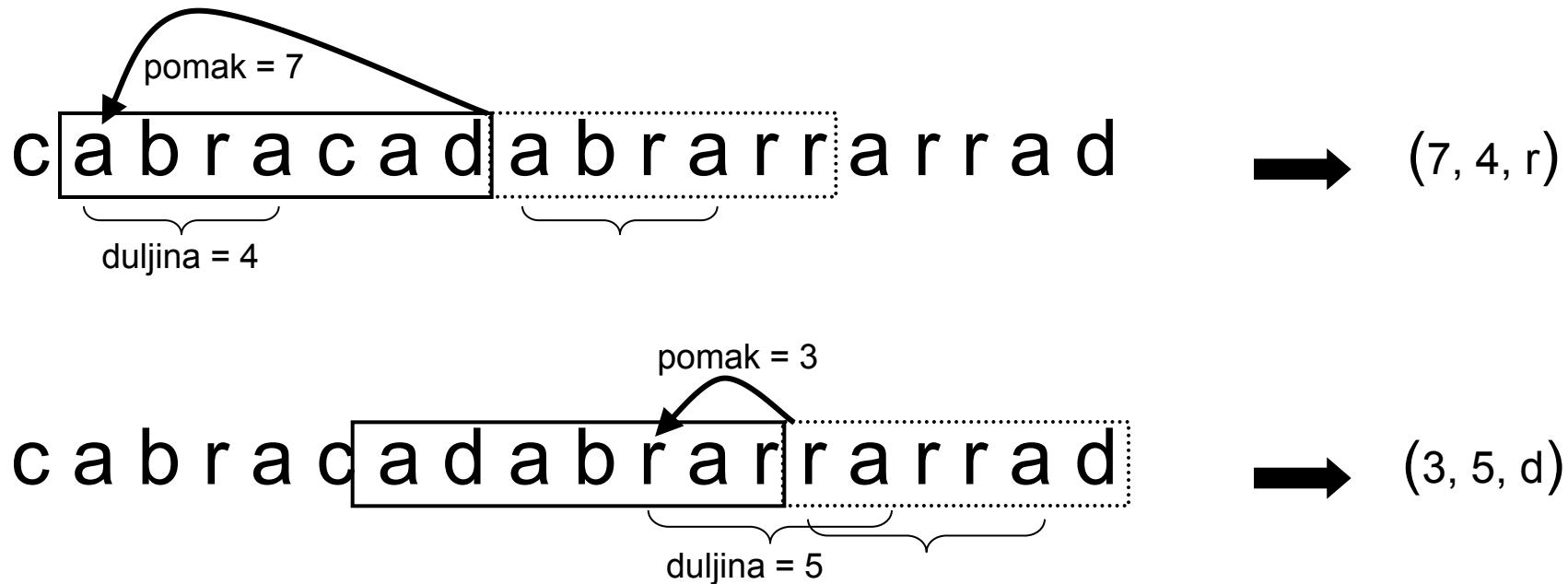
Metode s prilagodljivim rječnikom

- ◆ Koder i dekoder dinamički grade rječnik
 - LZ77: Rječnik je posmični prozor
 - LZ78: riječi se grade dodavanjem slova na postojeće riječi (u početku rječnik je prazan)
 - Lempel-Ziv-Welch (LZW) algoritam
 - izvorni algoritam smislili Ziv i Lempel (1977 - LZ77, 1978 - LZ78), a Welch ga je doradio i poboljšao 1984 (zato **LZW**)
 - algoritam relativno jednostavan, iako složeniji od Huffmanovog
 - izvorni LZW algoritam koristi rječnik s 4K riječi, s tim da su prvih 256 riječi standardni ASCII kodovi

Algoritam LZ77

- ◆ Rječnik je posmični prozor od N zadnjih simbola
- ◆ U svakom koraku traži se u rječniku najduži niz simbola jednak nadolazećim simbolima, te se kodira kao uređena trojka (*pomak, duljina, sljedeći_simbol*)
- ◆ Nedostatak: “kratka” memorija

LZ77: primjer kodiranja



Algoritmi LZ78 i LZW

- ◆ Umjesto posmičnog prozora, zasebna memorija za rječnik
 - Rječnik je poredana lista riječi (nizova simbola)
 - Riječ se dovaća pomoću indeksa (rednog broja)
- ◆ LZ78
 - Rječnik u početku prazan
 - U svakom koraku šalje se (*indeks, idući simbol*)
 - Indeks pokazuje na najdulju riječ u rječniku jednaku nadolazećem nizu simbola
 - Rječnik se nadopunjava novim rijećima tijekom kodiranja

LZW algoritam

- Algoritam kodiranja:

1. **RadnaRiječ** = slijedeći simbol sa ulaza
2. WHILE (ima još simbola na ulazu) DO
3. **NoviSimbol** = slijedeći simbol sa ulaza
4. IF **RadnaRiječ+NoviSimbol** postoji u rječniku THEN
5. **RadnaRiječ** = **RadnaRiječ+NoviSimbol**
6. ELSE
7. **IZLAZ**: kod za **RadnaRiječ**
8. dodaj **RadnaRiječ+NoviSimbol** u rječnik
9. **RadnaRiječ** = **NoviSimbol**
10. END IF
11. END WHILE
12. **IZLAZ**: kod za **RadnaRiječ**

Kodiranje algoritmom LZW: primjer

Sadržaj rječnika na početku:

kodna riječ	znak
(1)	A
(2)	B
(3)	C

Niz znakova koje treba kodirati:

Mjesto	1	2	3	4	5	6	7	8	9
Simbol	A	B	B	A	B	A	B	A	C

LZW:

korak	mjesto	sadržaj rječnika	izlaz iz kodera
1.	1	(4) A B	(1)
2.	2	(5) B B	(2)
3.	3	(6) B A	(2)
4.	4	(7) A B A	(4)
5.	6	(8) A B A C	(7)
6.	9		(3)

LZW kodiranje: primjer dekodiranja

KORAK	ULAZ DEKODERA	DEKODIRANI SIMBOLI	SADRŽAJ RJEČNIKA
1	(1)	A	
2	(2)	B	(4) AB
3	(2)	B	(5) BB
4	(4)	AB	(6) BA
5	(7)	ABA	(7) ABA
6	(3)	C	(8) ABAC

Metode rječnika: primjene

- ◆ LZW
 - UNIX compress
 - GIF
 - Modem V.24 bis
- ◆ LZ77
 - ZIP

Metode skraćivanja niza

- ◆ potiskivanje ponavljanja (engl. *repetition suppression*)
 - ◆ primjer - potiskivanje nula:

zastavica (flag)
koja označava nule

→ 894**f**32

↑
broj ponavljanja

- ◆ **slijedno kodiranje** (engl. *run-length encoding*) broj ponavljanja
 - ◆ algoritam kodiranja temelji se na kraćem zapisu ponavljanih simbola pomoću specijalnog znaka (!)
 - ◆ primjer: ABCCCCCCCCDEFFFABC...

ABCCCCCCCC
8 okteta

DEFFFABC...
3 okteta

ABC!8 DEFFFABC...
3 okteta 3 okteta

← “isplati” se za 4+ znakova

- ◆ Primjena: prva generacija telefaksa, unutar JPEG-a

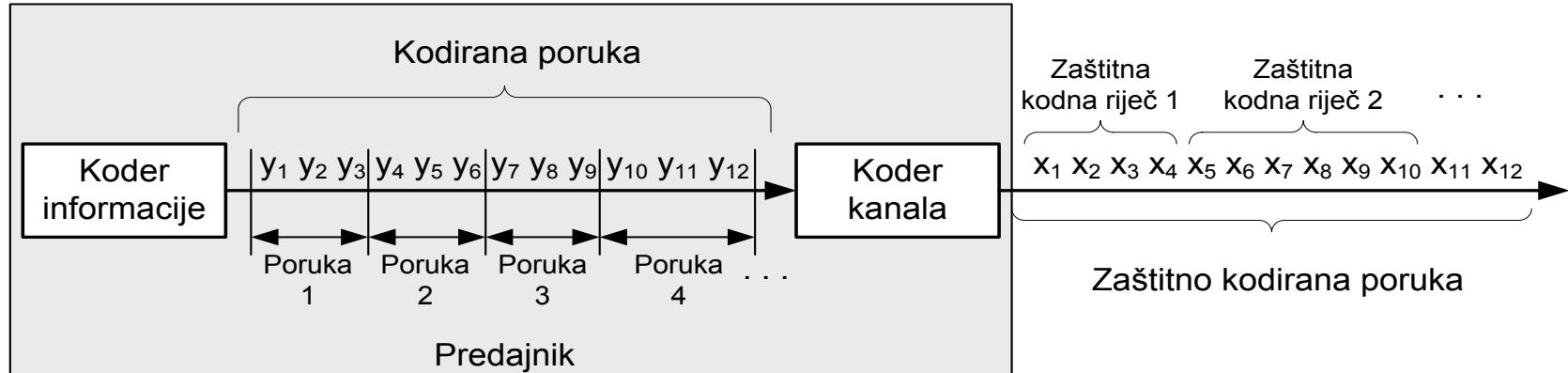
Zaštitno kodiranje I

Teorija informacije

Sadržaj predavanja

- ◆ Uvod
 - Komunikacijski sustav; Cilj zašt. kodiranja; Podjela zaštitnih kodova.
- ◆ Blok kodovi
 - Uvod
 - Paritetno kodiranje
 - Linearno binarni blok kodovi
 - Generirajuća matrica **G** i njen standardni oblik
 - » Kodiranje
 - » Dekodiranje (dekodiranje preko sindroma)
 - » Proračun vjerojatnosti ispravnog dekodiranja
 - Hammingovi kodovi
 - Ciklični kodovi

Komunikacijski sustav



- ◆ Koder informacije
 - Formira poruku (tzv. kodirana poruka) minimalne duljine koja opisuje sadržaj na izvoru;
- ◆ Koder kanala
 - Dijeli kodiranu poruku na fragmente koje u okviru ovog poglavlja nazivamo "porukama";
 - Definira zaštitni kôd kojim se provodi pridruživanje zaštitnih kodnih riječi porukama.
 - Nazivlje: zaštitne kodne riječi → kodne riječi (engl. *code words*).

Cilj zaštitnog kodiranja

- ◆ Cilj zaštitnog kodiranja je iskoristiti onaj zaštitni kôd koji:
 - Uvodi najmanje moguće povećanje prosječne duljine kodnih riječi u odnosu na prosječnu duljinu poruka;
 - Osigurava prihvatljivo malu vjerojatnost da pogreške simbola zaštitno kodirane poruke ostanu neotkrivene.

Što kada otkrijemo pogrešku?

- ◆ Pokreće se neki od postupaka otklanjanja pogreške (engl. *error correction*).
 - Ispravljanje pogreški u dekoderu kanala (FEC – engl. *forward error correction*);
 - Koriste se kodovi za otkrivanje i ispravljanje pogrešaka (engl. *error correcting codes*).
 - Ispravljanje pogreški ponovnim slanjem (BEC – engl. *backward error correction*).
 - Koriste se kodovi za otkrivanje pogrešaka (engl. *error detection codes*).

Podjela zaštitnih kodova

- ◆ Dvije glavne skupine zaštitnih kodova, i to:
 - Blok kodovi (engl. *block codes*);
 - Konvolucijski kodovi (engl. *convolutional codes*).
- ◆ Glavne razlike se odnose na način izvedbe kodera.
 - Blok kodovi: k -bitna poruka potpuno se preslikava u n -bitnu kodnu riječ, tj. generiranje nekog bita u kodnoj riječi funkcija je trenutačnog stanja ulaza kodera;
 - Konv. kodovi: generiranje nekog bita u kodnoj riječi funkcija je trenutačnog stanja ulaza kodera kao i nekolicine prethodnih stanja.
- ◆ Druga podjela zaštitnih kodova napravljena je na osnovu strukture i svojstava kodnih riječi, i to na:
 - Linearane (engl. *linear*).
 - Blok, konvolucijski i turbo kodovi.
 - Nelinearne (engl. *nonlinear*).

Blok kodovi

Definicija: abeceda koda

Abeceda koda: Kodne riječi koda K sastoje se od simbola izabralih iz konačnog skupa simbola F_q s “q” elemenata kojeg nazivamo abeceda koda.

- ◆ Primjer: U digitalnim komunikacijskim sustavima koristi se abeceda $F_2=\{0, 1\}$. Simbolu abecede F_2 su binarne znamenke 0 i 1, dok se kodovi koji koriste ovu abecedu zovu binarni kodovi.
- ◆ Napomena: U okviru kolegija Teorija informacije proučavat će se isključivo zaštitni binarni kodovi!

Primjer: zaštitno kodiranje

- ◆ Primjer: Izvor informacije generira četiri različita simbola: A , B , C i D , a koder informacije kodira ih kao:

$$P = \begin{cases} 0 & 0 & - & A; \\ 0 & 1 & - & B; \\ 1 & 0 & - & C; \\ 1 & 1 & - & D. \end{cases}$$

Koder kanala		
$K_1 = \begin{cases} 0 & 0 & 0 & - & A; \\ 0 & 1 & 1 & - & B; \\ 1 & 0 & 1 & - & C; \\ 1 & 1 & 0 & - & D. \end{cases}$	$K_2 = \begin{cases} 0 & 0 & 0 & 0 & 0 & - & A; \\ 0 & 1 & 1 & 0 & 1 & - & B; \\ 1 & 0 & 1 & 1 & 0 & - & C; \\ 1 & 1 & 0 & 1 & 1 & - & D. \end{cases}$	

Kôd K_1 formiran dodavanjem jednog redundantnog simbola

Kôd K_2 formiran dodavanjem tri redundantna simbola

Definicija: blok kôd

Blok kôd: Kôd K zove se **blok-kôd** ukoliko su duljine svih njegovih kodnih riječi jednake. Ako kodne riječi koda K imaju duljinu n , onda je K **blok-kôd duljine n** .

- ◆ Primjer:

$$K_1 = \begin{cases} 0 & 0 & 0 & - & A; \\ 0 & 1 & 1 & - & B; \\ 1 & 0 & 1 & - & C; \\ 1 & 1 & 0 & - & D. \end{cases} \quad K_2 = \begin{cases} 0 & 0 & 0 & 0 & 0 & - & A; \\ 0 & 1 & 1 & 0 & 1 & - & B; \\ 1 & 0 & 1 & 1 & 0 & - & C; \\ 1 & 1 & 0 & 1 & 1 & - & D. \end{cases}$$

Blok kod $n = 3$

Blok kod $n = 5$

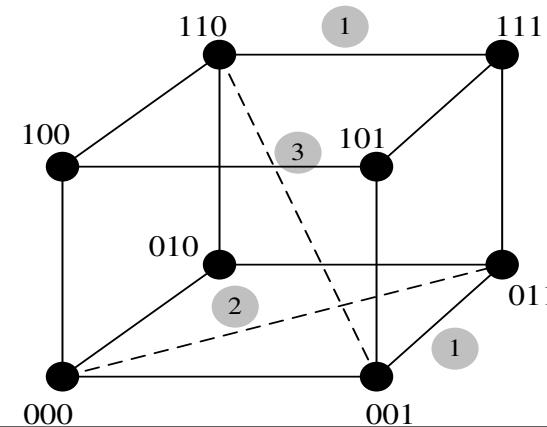
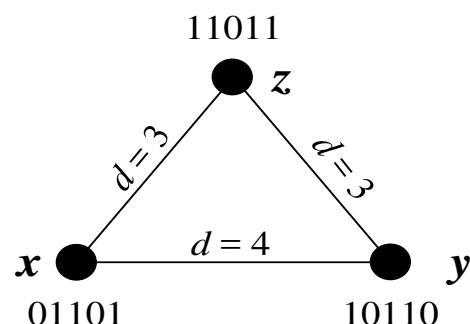
Definicija: Hammingova udaljenost

Hammingova udaljenost: Hammingova udaljenost između dvije kodne riječi je broj pozicija na kojima se kodne riječi razlikuju, tj. broj pozicija na kojima kodne riječi imaju različite simbole.

Oznaka Hammingove udaljenosti između dviju kodnih riječi \mathbf{x} i \mathbf{y} je $d(\mathbf{x}, \mathbf{y})$.

- ◆ Za kodne riječi i \mathbf{x}, \mathbf{y} i \mathbf{z} blok-koda K , Hammingova udaljenost ima sljedeća svojstva:
 - $d(\mathbf{x}, \mathbf{y}) = 0$ ako i samo ako je $\mathbf{x} = \mathbf{y}$;
 - $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$ za sve $\mathbf{x}, \mathbf{y} \in K$;
 - $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$ za sve $\mathbf{x}, \mathbf{y}, \mathbf{z} \in K$ (nejednakost trokuta).
- ◆ Primjer:

x	0	1	1	0	1
y	1	0	1	1	0
	1	2	3	4	



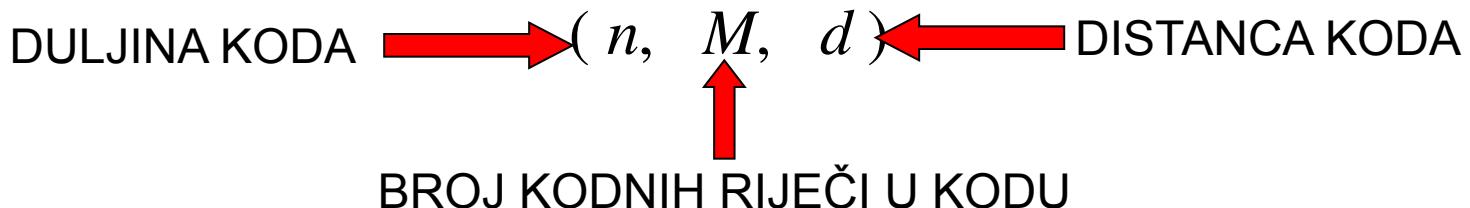
Definicija: Udaljenost blok-koda i njegova oznaka

- ◆ Dekodiranje kodne riječi se provodi na način da se kao primljena kodna riječ odabire ona koja od primljene riječi ima najmanju Hammingovu udaljenost – princip dekodiranja najbližim susjedom.
- ◆ Sposobnost koda da otkrije ili ispravi pogreške ovisi o najmanjoj Hammingovoj udaljenosti između svih parova kodnih riječi nekog koda K .

Udaljenost koda: *Udaljenost koda K , s oznakom $d(K)$, je najmanja Hammingova udaljenost svih parova kodnih riječi koda K , tj.*

$$d(K) = \min_{\mathbf{x}, \mathbf{y} \in K} (d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \neq \mathbf{y})$$

OZNAKA BLOK-KODA:



- ◆ Ako zaštitni kôd K ima distancu $d(K)$ i ako se dekodiranje provodi principom najbližeg susjeda, onda vrijedi sljedeće:
 - Kôd K može otkriti najviše $d(K)-1$ pogrešaka u jednoj kodnoj riječi, tj. ako je najveći broj pogrešaka koje kôd može otkriti s , onda mora biti zadovoljen izraz $d(K) \geq s+1$.
- ◆ Primjer (blok kôd $n = 3, M = 4, d(K) = 2 \rightarrow s = 1$):

$$K_1 = \begin{cases} 0 & 0 & 0 & - & A; \\ 0 & 1 & 1 & - & B; \\ 1 & 0 & 1 & - & C; \\ 1 & 1 & 0 & - & D. \end{cases}$$

Otkrivanje i ispravljanje pogrešaka (2/2)

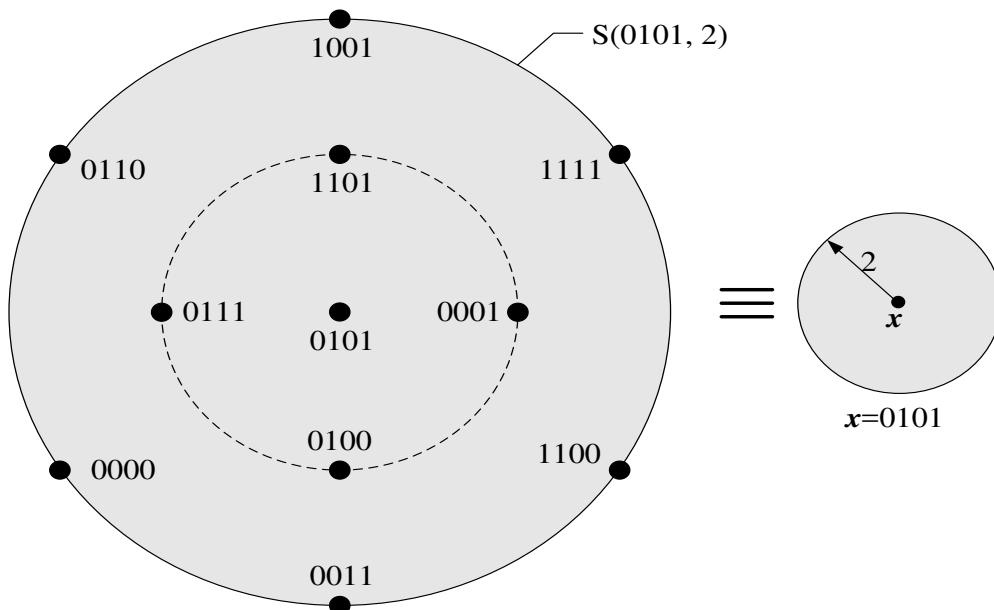
- ◆ Ako zaštitni kôd K ima distancu $d(K)$ i ako se dekodiranje provodi principom najbližeg susjeda, onda vrijedi sljedeće:
 - ...
 - Kôd K može ispraviti najviše $\lfloor (d(K)-1)/2 \rfloor$ pogrešaka u jednoj kodnoj riječi, gdje je $\lfloor x \rfloor$ oznaka za najveći cijeli broj manji od x . Drugim riječima, ukoliko se s t označi najveći broj pogrešaka koje kôd K može ispraviti u jednoj kodnoj riječi, onda mora biti zadovoljen izraz $d(K) \geq 2t+1$.
(Napomena: Objašnjenje slijedi u nastavku!)

Kugla kodne riječi

Kugla kodne riječi \mathbf{x} radijusa r su sve riječi (vektori) duljine n sa skalarima 0 i 1 čija je Hammingova distanca od \mathbf{x} manja ili jednaka r .

$$S(\mathbf{x}, r) = \left\{ \mathbf{y} \in F_2^n \mid d(\mathbf{x}, \mathbf{y}) \leq r \right\}$$

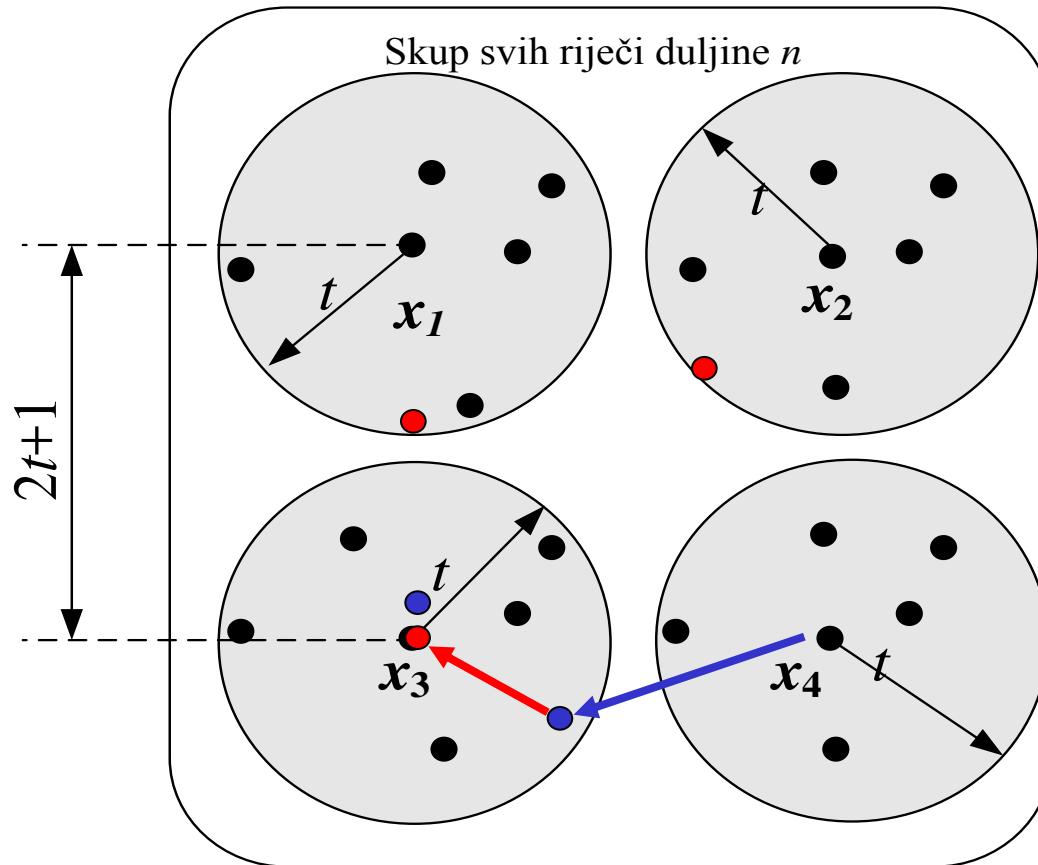
- ◆ Primjer: ($\mathbf{x} = [0101]$, Kugla $S(\mathbf{x}, 2)$)



$0101 \rightarrow$		1001
$d = 0$	$d = 1$	$d = 2$
0101	0001	1101
0111	0011	1111
0100	0000	1100
0110		0011
0011		1010

Primjer: kugla kodne riječi

- ◆ Primjer: Dan je kôd s četiri kodne riječi x_1, x_2, x_3 i x_4 i $d(K) \geq 2t+1$.



Osnovni zadatak teorije kodiranja

- ◆ Za definiranu duljinu kodne riječi n koda K i definiranu distancu d , odrediti najveći mogući broj kodnih riječi $M = A(n, d)$.

n	$d = 3$	$d = 5$	$d = 7$
5	4	2	-
6	8	2	-
7	16	2	2
8	20	4	2
9	40	6	2
10	72-79	12	2
11	144-158	24	4
12	256	32	4
13	512	64	8
14	1024	128	16
15	2048	256	32
16	2560-3276	256-340	36-37

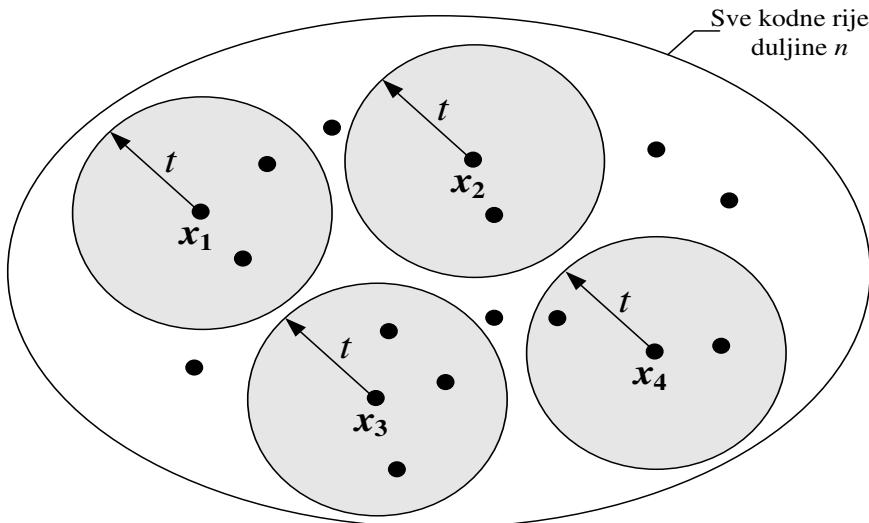
Hammingova međa za $A(n, d)$ i perfekstan kôd

$$M \leq \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{t}}$$

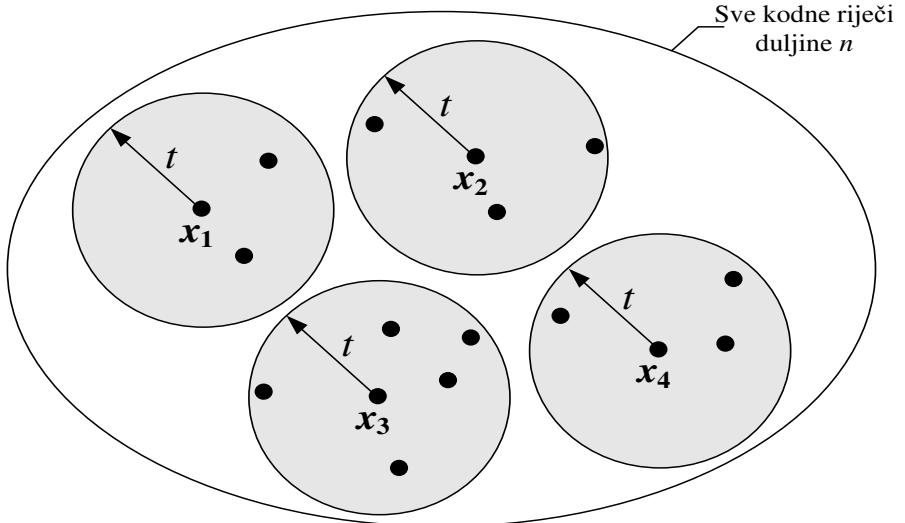
HAMMINGOVA MEĐA
(SPHERE-PACKING BOUND)

PERFEKTAN KÔD

$$M = \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{t}}$$



Neperfekstan kôd i ograničenje sfernog pakiranja



Perfekstan kôd – sve sfere pokrivaju sve vektore!

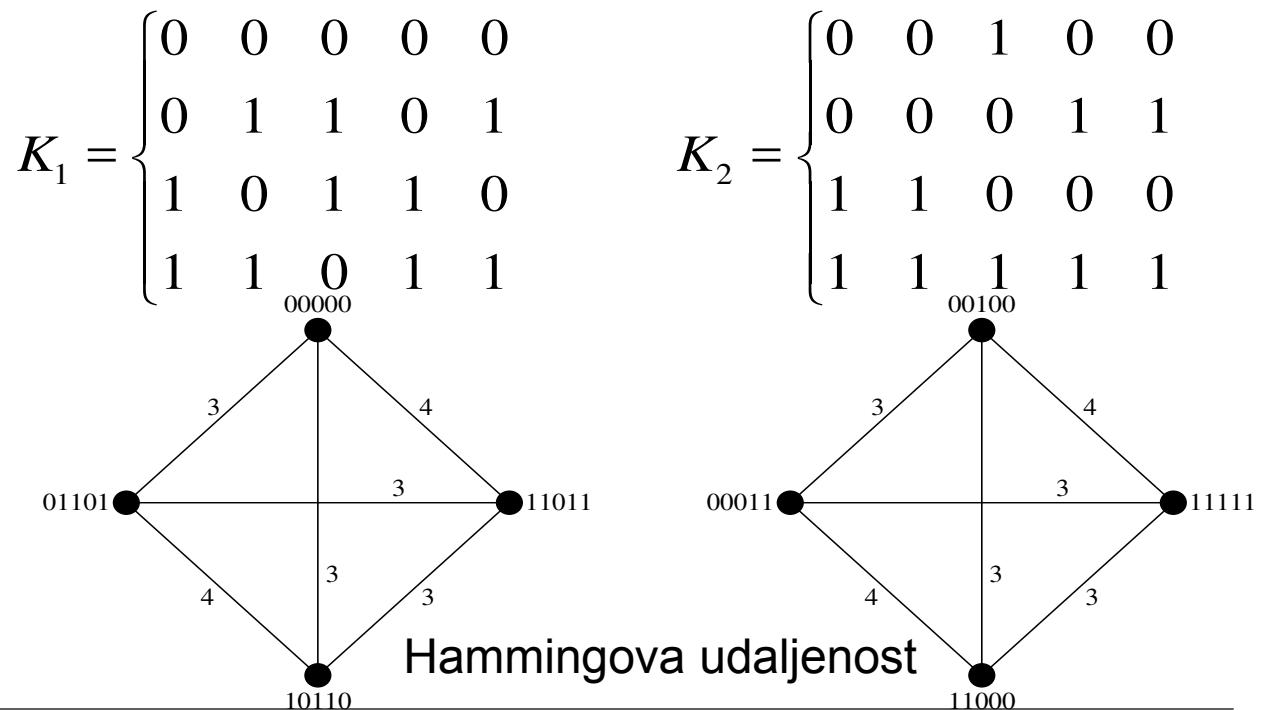
Ekvivalencija blok kodova

Ekvivalentni kodovi: Dva binarna blok-koda su ekvivalentna ukoliko se jedan iz drugog mogu dobiti:

- (1) postupkom invertiranja simbola nad jednom ili više pozicija koda,
- (2) zamjenom dviju ili više pozicija koda prije ili nakon (1).

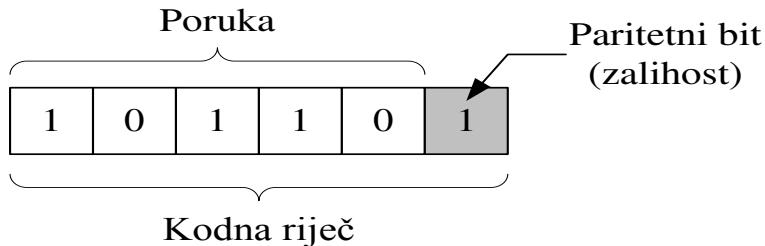
◆ Primjer: Kod K_2 nastao iz koda K_1 .

- (1) – zamjena simbola ($0 \rightarrow 1$ i $1 \rightarrow 0$) na trećoj poziciji u kodu K_1 ;
- (2) – zamjena pozicija 2 i 4 svih kodnih riječi.



Paritetno kodiranje (1/2)

- ♦ Koristi se isključivo za otkrivanje pogrešaka u kodnoj riječi.
- ♦ Na poruku se dodaje jedan zalihosni simbol (bit) koji se naziva paritetni bit (engl. *parity check*).
- ♦ U praksi se koristi parni paritet (engl. *even parity*) ili neparni paritet (engl. *odd parity*).



$$R = x_1 + x_2 + \dots + x_k \quad (\text{parni paritet}),$$

$$R = x_1 + x_2 + \dots + x_k + 1 \quad (\text{neparni paritet}).$$

Napomena: Paritetni bit R se izračunava zbrajanjem aritmetikom modulo 2.

- ♦ Primjer: Proračun vjerojatnosti neotkrivenih pogrešaka (p_{np}) za paritet.

$$p_{np} = \binom{n}{2} p^2 (1-p)^{n-2} + \binom{n}{4} p^4 (1-p)^{n-4} + \dots + \binom{n}{n} p^n \quad n - \text{parno}$$

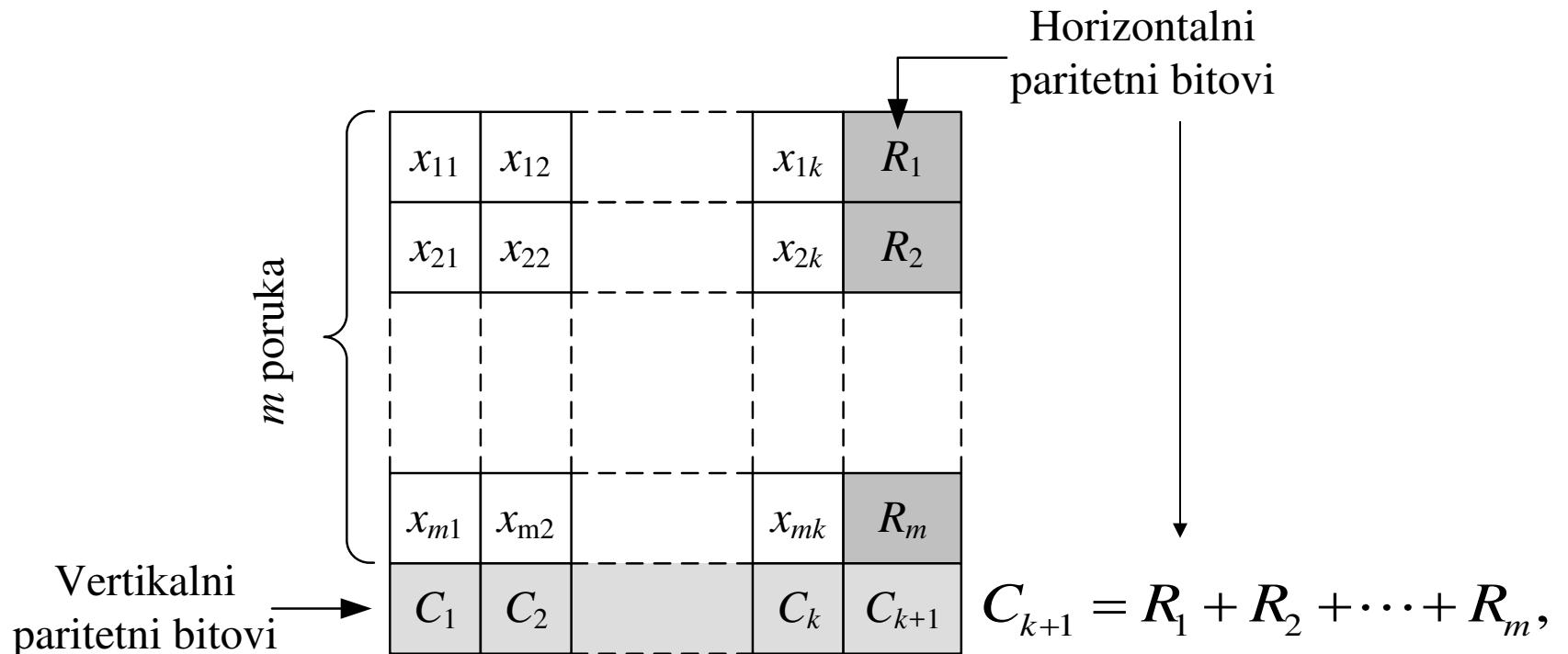
$$p_{np} = \binom{n}{2} p^2 (1-p)^{n-2} + \binom{n}{4} p^4 (1-p)^{n-4} + \dots + \binom{n}{n-1} p^{n-1} (1-p) \quad n - \text{neparno}$$

n - duljina kodne riječi; p - vjerojatnost pojave pogreške na jednom bitu.

Paritetno kodiranje (2/2)

- Vertikalna i horizontalna provjera zalihosti.
 - Uvođenje zajedničkih paritetnih bitova za više uzastopnih poruka.
 - Formiranje posebne kodne riječi s bitovima C_1, \dots, C_k .

$$C_i = x_{1i} + x_{2i} + \dots + x_{mi}, \quad i = 1, \dots, k$$



Linearno binarni blok kodovi

Vektorski prostor: definicija

- Linearno binarni blok kodovi definiraju se preko skupa vektora (vektorski prostor) nad kojim su definirane određene operacije.
- Kodnu riječ opisujemo binarnim vektorom $\mathbf{x} = [x_1 \ x_2 \ \dots \ x_n]$; x_i su iz abecede $F_2 = \{0, 1\}$.
- Na skupom $F_2 = \{0, 1\}$ definiraju se operacije zbrajanja i množenja u aritmetici modulo 2.

x_1	x_2	$x_1 + x_2$	$x_1 \cdot x_2$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

- Neutralni element s obzirom na zbrajanje je 0, a s obzirom na množenje je 1.
 - U aritmetici modulo 2 zadovoljene su jednakosti: $-1 = 1$ i $1 \cdot 1^{-1} = 1$.
 - Neka je $V(n)$ skup svih binarnih vektora duljine n nad kojim su definirane operacije zbrajanja vektora i množenja vektora skalarom na sljedeći način:
- $$\mathbf{x} + \mathbf{y} = [x_1, x_2, x_3, \dots, x_n] + [y_1, y_2, y_3, \dots, y_n] = [x_1 + y_1, x_2 + y_2, x_3 + y_3, \dots, x_n + y_n],$$
- $$a \cdot \mathbf{x} = a \cdot [x_1, x_2, x_3, \dots, x_n] = [a \cdot x_1, a \cdot x_2, a \cdot x_3, \dots, a \cdot x_n],$$
- a, x_i, y_i su skalari iz F_2 ; \mathbf{x}, \mathbf{y} su vektori iz $V(n)$

- S ovako definiranim operacijama skup $V(n)$ je **VEKTORSKI PROSTOR!**

Definicija: linearni binarni blok kôd

Linerani binarni blok kôd: Neka je blok-kôd K potprostor vektorskog prostora $V(n)$: $K \subset V(n)$. Neka su \mathbf{x} i \mathbf{y} kodne riječi koda K i neka je $a \in \{0, 1\}$. Ako je za sve \mathbf{x} , \mathbf{y} i a ispunjeno:

- $\mathbf{x} + \mathbf{y} \in K$,
- $a \cdot \mathbf{x} \in K$,

onda je K linearan binarni blok-kôd.

- ◆ Svi vektori duljine n čine vektorski prostor $V(n)$. Ako je K potprostor od $V(n)$, onda je K LINEARAN BLOK KÔD!
- ◆ Zbrajanjem dvije kodne riječi nastaje neka nova riječ koda K .
- ◆ Množenjem neke kodne riječi s konstantom nastaje neka nova riječ koda K .
- ◆ **Kodna riječ $\mathbf{0}$ pripada kodu K .**
- ◆ *Linerani blok kodovi: proračun udaljenosti koda preko težine kodnih riječi.*

Definicija: težina kodne riječi

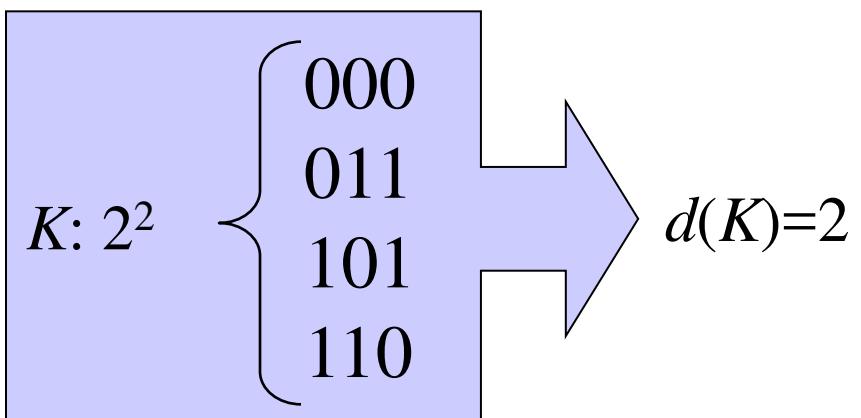
Težina kodne riječi: Težina kodne riječi \mathbf{x} koda K je broj pozicija kodne riječi na kojima se nalazi simbol 1. Oznaka težine kodne riječi \mathbf{x} je $w(\mathbf{x})$.

- ◆ Primjer: $w(101011) = 4$, $w(001000) = 1$.
- ◆ Kod linearnih blok kodova vrijedi:

$$d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$$

- ◆ Budući da je svaka razlika dvije kodne riječi neka kodna riječ linearog blok-koda, distancu koda određujemo kao:

$$d(K) = \text{mini } w(\mathbf{x}) \text{ uz } \mathbf{x} \neq \mathbf{0}$$



Vektorski prostor: baza prostora

- ◆ Baza vektorskog prostora/potprostora: Skup svih linearno nezavisnih vektora.
- ◆ Svi vektori nekog prostora/potprostora mogu se dobiti kao linearna kombinacija vektora baze.
- ◆ Primjer:

$$K: 2^2 \quad \left\{ \begin{array}{l} 000 \\ 011 \\ 101 \\ 110 \end{array} \right. \quad \text{BAZA} \quad \left\{ \begin{array}{l} 011 \\ 101 \end{array} \right. \quad \begin{array}{l} \text{dimenzija potprostora:} \\ k = 2 \text{ (broj vektora u bazi)} \\ M = 2^k \text{ (broj kodnih riječi)} \end{array}$$

$$x = a [0 \ 1 \ 1] + b [1 \ 0 \ 1], \quad a, b \in \{0, 1\}$$

$$[0 \ 0 \ 0] = 0 [0 \ 1 \ 1] + 0 [1 \ 0 \ 1] \quad [1 \ 0 \ 1] = 0 [0 \ 1 \ 1] + 1 [1 \ 0 \ 1]$$

$$[0 \ 1 \ 1] = 1 [0 \ 1 \ 1] + 0 [1 \ 0 \ 1] \quad [1 \ 1 \ 0] = 1 [0 \ 1 \ 1] + 1 [1 \ 0 \ 1]$$

Definicija: generirajuća matrica \mathbf{G}

- ◆ Ako znamo bazu linearog blok-koda (tj. vektorskog potprostora), onda svaku kodnu riječ možemo izraziti kao linearu kombinaciju vektora baze:
- $$\mathbf{x} = a_1 \cdot \mathbf{b}_1 + a_2 \cdot \mathbf{b}_2 + \dots + a_k \cdot \mathbf{b}_k$$
- ◆ Iz razloga jednostavnosti generiranja kodnih riječi vektore baze stavljamo u matricu.

Generirajuća matrica koda: Matrica dimenzija $k \times n$ čiji se reci sastoje od vektora baze koda (n, M, d) se zove generirajuća matrica. Oznaka \mathbf{G} .

$$K = \begin{Bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{Bmatrix} \quad \begin{array}{l} M = 4 \\ k = 2 \end{array} \quad \mathbf{G} = \left[\quad \right]$$

Primjer: generiranje kodnih riječi

- Binarni kôd $K=(5, 4, 3)$

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

$$0 \cdot [00111] + 0 \cdot [11011] = [00000]$$

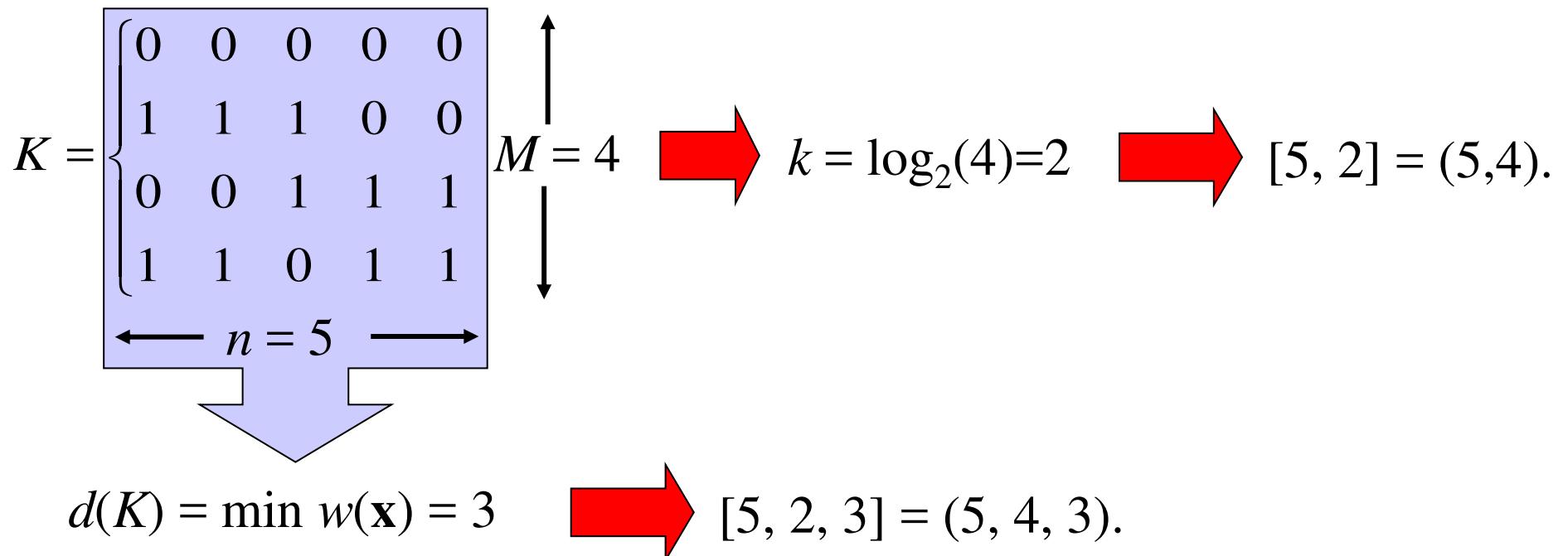
$$0 \cdot [00111] + 1 \cdot [11011] = [11100]$$

$$1 \cdot [00111] + 0 \cdot [11011] = [00111]$$

$$1 \cdot [00111] + 1 \cdot [11011] = [11100]$$

Definicija: oznaka linearog blok koda

Oznaka linearog blok koda: Ako je kôd K vektorski k -dimenzionalni potprostor vektorskog prostora $V(n)$, onda kôd K ima oznaku $[n, k]$. Ukoliko je poznata udaljenost koda d , onda je oznaka koda $[n, k, d]$.



Generirajuće matrice ekvivalentnih linearnih blok kodova

- Primjer: ekvivalentan kôd (zamjena $0 \rightarrow 1$, $1 \rightarrow 0$ na trećoj poziciji)

$$K = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \xrightarrow{\text{EKVIVALENTAN KÔD}} K_e = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

- Ekvivalentan kôd linearog blok koda nije nužno i linearan! Mora postojati kodna riječ **0**.
- Sljedeće pravilo definira način dobivanja ekvivalentnih linearnih blok kodova:

Generirajuće matrice ekvivalentnih linearnih blok kodova: Dva ekvivalentna linearna binarna blok-koda $[n, k]$, K_1 i K_2 , imaju generirajuće matrice \mathbf{G}_1 i \mathbf{G}_2 koje se jedna iz druge mogu dobiti sljedećim operacijama:

- (1) Zamjena redaka;
- (2) Dodavanje jednog retka drugom retku;
- (3) Zamjena stupaca.

Definicija: standardni oblik generirajuće matrice \mathbf{G}

Standardni oblik generirajuće matrice: Generirajuća matrica \mathbf{G} nekog koda K ima standardni oblik ako ima strukturu

$$\mathbf{G} = [\mathbf{I}_k \mid \mathbf{A}],$$

gdje je \mathbf{I}_k jedinična matrica reda k , a \mathbf{A} matrica dimenzija $k \times (n-k)$.

- Primjer: Binarni kôd $K=(5, 4, 3)$ – Generirajuće matrice

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

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

Kodiranje linearnim blok kodovima

(1/2)

- ♦ Ideja kodiranja – kodirana poruka određuje vektore baze (retke matrice \mathbf{G}) koji ulaze u linearnu kombinaciju s koeficijentom 1 kako bi dali kodnu riječ.
- ♦ Na primjer: Ako je poruka $[0\ 1\ 0\ 1]$, to znači da će se toj poruci pridružiti kôd dobiven zbrajanjem 2. i 4. vektora baze.

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

$$\begin{array}{r} + \\ \hline 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{array}$$

$$\begin{array}{r} + \\ \hline 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{array}$$

Kodiranje linearnim blok kodovima (2/2)

- ♦ Način formiranja kodne riječi \mathbf{x} odgovara množenju vektor-retka kodirane poruke \mathbf{m} duljine k i generirajuće matrice \mathbf{G} u aritmetici modulo 2.

$$\mathbf{G} = \begin{bmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \\ \vdots \\ \mathbf{r}_k \end{bmatrix} \quad \mathbf{x} = \sum_{i=1}^k m_i \cdot \mathbf{r}_i = \mathbf{m} \cdot \mathbf{G}.$$

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

- ♦ PROBLEM – gdje su bitovi kodirane poruke a gdje zaštitni bitovi?
- ♦ Nesistematičan kôd.

Kodiranje s matricom G u standardnom obliku

- ◆ Kada je generirajuća matrica u standardnom obliku, generiranje kodne riječi se pojednostavljuje, a kôd postaje sistematičan.

$$\mathbf{m} \cdot [\mathbf{I}_k | \mathbf{A}] = \{\mathbf{m}, \mathbf{m} \cdot \mathbf{A}\}.$$

$$[0 \ 1] \cdot \underbrace{\begin{bmatrix} & \\ & \end{bmatrix}}_{I_2} = \underbrace{[0 \ 1]}_{\text{poruka}}$$

$$[0 \ 1] \cdot \underbrace{\begin{bmatrix} & \\ & \end{bmatrix}}_A = \underbrace{[1 \ 1 \ 1]}_{\text{zaštitni bitovi}}$$

$$[0 \ 1] \cdot \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix} = \underbrace{[0 \ 1]}_{\text{poruka}} \underbrace{[1 \ 1 \ 1]}_{\text{zaštitni bitovi}}.$$

Dekodiranje linearog blok koda

- ◆ Primjer: Kôd $(5, 4, 3) = [5, 2, 3]$ → otkriva dvostruku i ispravlja jednostruku pogrešku korištenjem principa dekodiranja najbližim susjedom.

$$K = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

- ◆ Dekodiranje po principu pronalaženja kodne riječi koja od primljene kodne riječi ima najmanju Hammingovu distancu.
 - Složenost postupka raste s brojem kodnih riječi M ;
 - Za velike kodove ovaj postupak zahtijeva veliko opterećenje procesora prijemnika.
 - Razvijene su druge metode brzog dekodiranja linearnih blok kodova (Na primjer: Sindromsko dekodiranje).
- ◆ Sindromsko dekodiranje.
 - Za razumijevanje ovog načina dekodiranja potrebno je poznavanje sljedećih pojmoveva: **vektor pogreške, standardni niz, razred, matrica provjere pariteta i sindrom.**

Definicija: vektor pogreške

Vektor pogreške: Vektor pogreške \mathbf{e} za poslanu kodnu riječ $\mathbf{x} = [x_1, x_2, \dots, x_n]$ i primljenu kodnu riječi $\mathbf{y} = [y_1, y_2, \dots, y_n]$ se definira kao razlika vektora:

$$\mathbf{e} = \mathbf{y} - \mathbf{x} = [e_1 \ e_2 \ \dots \ e_n].$$

Predajnik šalje

$$\mathbf{x} = [1 \ 1 \ 0 \ 1 \ 1]$$

Prijemnik prima

$$\mathbf{y} = [1 \ 0 \ 1 \ 1 \ 1]$$

Vektor pogreške

$$\mathbf{e} = [0 \ 1 \ 1 \ 0 \ 0]$$

Definicija: standardni niz i razred

- ◆ Standardni niz je tablica koja se formira na sljedeći način:

- U prvom retku su kodne riječi koda K ;
- Prva kodna riječ je **0**;
- Prvi stupac je stupac vektora pogreški;
- U ostalim redcima nalaze se razredi koda K nastali dodavanjem vektora pogreške e kodnim riječima koda K .
- Članovi nekog retka predstavljaju jedan razred (engl. coset) skupa kodnih riječi koda K . Svaki razred koda K je blok kôd nastao dodavanjem nekog vektora pogreške svim kodnim riječima koda K .

0 0 0 0 1	1 1 1 0 1	0 0 1 1 0	1 1 0 1 0
0 0 0 1 0	1 1 1 1 0	0 0 1 0 1	1 1 0 0 1
0 0 1 0 0	1 1 0 0 0	0 0 0 1 1	1 1 1 1 1
0 1 0 0 0	1 0 b 0 0 0	0 1 1 1 1	1 0 0 1 1
1 0 0 0 0	0 1 1 0 0 0	1 0 1 1 1	0 1 0 1 1
$K = \left\{ \begin{array}{l} 0 0 1 1 1 \\ 1 1 0 1 1 \end{array} \right.$			
<i>Standardni niz</i>			

Primjer: dekodiranje korištenjem standardnog niza (1/2)

- Neka je primljena kodna riječ $y = [1\ 1\ 1\ 1\ 0]$
 - Pronađi primljenu kodnu riječ y u standardnom nizu;
 - Ako y postoji tada je prvi element retka vektor pogreške, a prvi element stupca je poslana kodna riječ;
 - Ako y ne postoji tada je pogreška otkrivena, ali se ne može ispraviti!

Ako je primljeno
[1 0 1 0 1] ?

0 0 0 0 0	1 1 1 0 0	0 0 1 1 1	1 1 0 1 1
0 0 0 0 1	1 1 1 0 1	0 0 1 1 0	1 1 0 1 0
0 0 0 1 0	1 1 1 1 0	0 0 1 0 1	1 1 0 0 1
0 0 1 0 0	1 1 0 0 0	0 0 0 1 1	1 1 1 1 1
0 1 0 0 0	1 0 1 0 0	0 1 1 1 1	1 0 0 1 1
1 0 0 0 0	0 1 1 0 0	1 0 1 1 1	0 1 0 1 1

PRIMLJENO:
 $y = [1\ 1\ 1\ 1\ 0]$

VEKTOR POGREŠKE:
 $e = [0\ 0\ 0\ 1\ 0]$

DEKODIRANO:
 $x = [1\ 1\ 1\ 0\ 0]$

Primjer: dekodiranje korištenjem standardnog niza (2/2)

- ◆ Dekodiranje pomoći standardnog niza je procesorski zahtijevan postupak u tablicama velikih dimenzija što rezultira skupom i složenom izvedbom dekodera kanala.
- ◆ Ubrzavanje postupka dekodiranja preko matrice provjere pariteta \mathbf{H} .
 - Potrebno je definirati sljedeće pojmove: **ortogonalnost, dualni kôd i linearost dualnog koda!**
- ◆ ORTOGONALNOST
 - Pretpostavimo da postoji linearni blok kôd s oznakom K^\perp čije su sve kodne riječi ortogonalne na sve kodne riječi koda K .
 - Što je ortogonalnost? → Skalarni umnožak svih vektora kodnih riječi iz K i K^\perp jednak je nula. Na primjer: $[1\ 1\ 0\ 0\ 0] \times [0\ 0\ 1\ 1\ 1] = 0$.

Definicija: dualni kôd i njegova linearost

Dualni kôd: Neka su \mathbf{x} vektori koda K ($\mathbf{x} \in K$). Skup svih vektora \mathbf{y} vektorskog prostora $V(n)$ koji su ortogonalni na sve $\mathbf{x} \in K$ čini **dualni kôd** koda K i ima oznaku K^\perp :

$$K^\perp = \{\mathbf{y} \in V(n) \mid \forall \mathbf{x} \in K, \mathbf{y} \cdot \mathbf{x} = 0\},$$

gdje je $\mathbf{x} \cdot \mathbf{y}$ skalarni produkt vektora u aritmetici modulo 2.

Linearost dualnog koda: Neka je K linearни blok-kôd $[n, k]$. Dualni kôd koda K je **linearan** blok-kôd $[n, n - k]$.

$$K = \begin{cases} 00000 \\ 11100 \\ 10111 \\ 01011 \end{cases}, \quad \mathbf{G} = \begin{bmatrix} 10111 \\ 01011 \end{bmatrix} \quad \xrightarrow{\hspace{1cm}} \quad K^\perp = \begin{cases} 00000 & 01110 \\ 10100 & 01101 \\ 11010 & 00011 \\ 11001 & 10111 \end{cases}$$

Generirajuće matrice kodova K i

K^\perp

- ♦ Dualni kôd je linearan → posjeduje bazu i generirajuću matricu koju ćemo označavati s \mathbf{H} .
- ♦ Skalarni produkti između svih parova redaka matrica \mathbf{G} (kôd K) i \mathbf{H} (kôd K^\perp) jednaki su $\mathbf{0}$ te vrijedi jednadžba:

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

- ♦ **Važno:** Za provjeru ispravnosti primljene kodne riječi \mathbf{x} dovoljno je skalarno pomnožiti primljenu kodnu riječ sa svim vektorima generirajuće matrice dualnog koda kojih ima $n-k$.

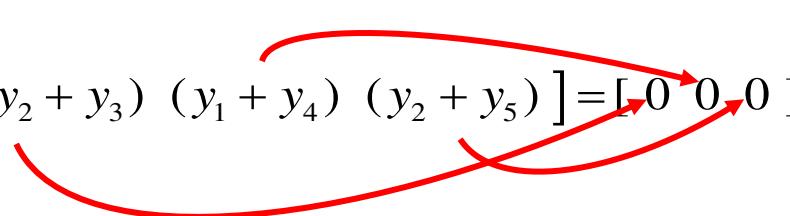
$$\mathbf{x} \cdot \mathbf{H}^T = [0\ 0\dots 0]$$

Matrica provjere pariteta koda K

- Primjer: Sljedeći par matrica \mathbf{G} i \mathbf{H} zadovoljava jednadžbu $\mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}$.

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

- Ukoliko je primljena kodna riječ \mathbf{y} primljena ispravno, onda njenim množenjem s \mathbf{H}^T moramo dobiti nul-vektor.

$$[y_1 \ y_2 \ y_3 \ y_4 \ y_5] \cdot \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [(y_1 + y_2 + y_3) \ (y_1 + y_4) \ (y_2 + y_5)] = [0 \ 0 \ 0]$$


Matrica \mathbf{H} praktički određuje pozicije u kodnoj riječi čiji zbroj u aritmetici modulo 2 mora biti 0, odnosno pozicije na kojima mora biti zadovoljen **PARNI PARITET**. Matricu \mathbf{H} zbog toga nazivamo **MATRICA PROVJERE PARITETA!**

Matrica provjere pariteta \mathbf{H} i njen standardni oblik

Matrica provjere pariteta: Neka je \mathbf{H} generirajuća matrica dualnog koda K^\perp . Matrica \mathbf{H} se naziva *matrica provjere pariteta* (engl. *parity-check matrix*) ili *paritetna matrica* koda K . U svakom retku matrice \mathbf{H} jedinice određuju pozicije unutar ispravne kodne riječi na kojima zbroj vrijednosti simbola mora biti paran broj. Ukoliko \mathbf{H} ima strukturu:

$$\mathbf{H} = [\mathbf{B} | \mathbf{I}_{n-k}],$$

gdje je \mathbf{B} kvadratna matrica, onda je paritetna matrica \mathbf{H} u **standardnom obliku**.

Proračun matrice provjere pariteta: Neka je \mathbf{G} generirajuća matrica linearног binarnog koda K u standardnom obliku:

$$\mathbf{G} = [\mathbf{I}_k | \mathbf{A}].$$

Generirajuća matrica dualnog koda K^\perp zadovoljava jednadžbu $\mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}$ i jednaka je

$$\mathbf{H} = [\mathbf{A}^T | \mathbf{I}_{n-k}].$$

Primjer: proračun matrice provjere pariteta \mathbf{H}

$$K = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix} \rightarrow \mathbf{G} = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{array} \right]$$

$$\mathbf{I}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{A} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

$$\mathbf{H} = [\mathbf{A}^T | \mathbf{I}_3] \quad \longrightarrow \quad \mathbf{H} = \left[\begin{array}{cc|ccccc} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{array} \right].$$

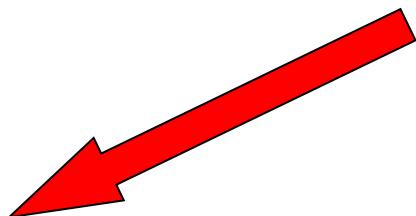
Primjer: Dekodiranje pomoću matrice provjere pariteta H

Primljena kodna riječ $y = [11011]$



$$[11011] \cdot \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [000].$$

Primljena kodna riječ $y = [10011]$



$$[10011] \cdot \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [101].$$

Dekodiraj pomoću standardnog niza!

Rješ: $e = [01000]$ i $x = [11011]$

Definicija: sindrom

Sindrom: Sindrom primljene kodne riječi y kada K s paritetnom matricom H je vektor dobiven umnoškom:

$$S(y) = y \cdot H^T.$$

e				S(y)
0 0 0 0 0	1 1 1 0 0	0 0 1 1 1	1 1 0 1 1	0 0 0
0 0 0 0 1	1 1 1 0 1	0 0 1 1 0	1 1 0 1 0	0 0 1
0 0 0 1 0	1 1 1 1 0	0 0 1 0 1	1 1 0 0 1	0 1 0
0 0 1 0 0	1 1 0 0 0	0 0 0 1 1	1 1 1 1 1	1 0 0
0 1 0 0 0	1 0 1 0 0	0 1 1 1 1	1 0 0 1 1	1 0 1
1 0 0 0 0	0 1 1 0 0	1 0 1 1 1	0 1 0 1 1	1 1 0

JEDAN VEKTOR POGEŠKE – JEDAN SINDROM

Sindromsko dekodiranje

- ♦ Sindrom jedinstveno određuje vektor pogreške. Stoga možemo formirati tablicu preslikavanja između sindroma $S(y)$ i vektora pogreške e !

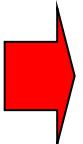
e	00000	00001	00010	00100	01000	10000
$S(y)$	000	001	010	100	101	110

POSTUPAK DEKODIRANJA:

- izračunaj sindrom $S(y)$ primljene kodne riječi y ;
- iz tablice preslikavanja odredi vektor pogreške e ;
- poslana kodna riječ je $x = y - e$.

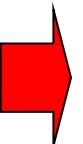
PRIMLJENO:

$$y = [1 \ 1 \ 0 \ 0 \ 0]$$



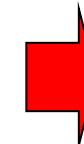
SINDROM:

$$y \cdot H^T = [1 \ 0 \ 0]$$



VEKTOR e :

$$e = [0 \ 0 \ 1 \ 0 \ 0]$$



DEKODIRANO:

$$x = y - e = [1 \ 1 \ 1 \ 0 \ 0]$$

- ♦ Ukoliko se pojavi sindrom [011] ili [111], došlo je do višestruke pogreške koju nije moguće ispraviti!

Vjerojatnost ispravnog dekodiranja (1/3)

- ◆ Promatramo prijenos poruke preko BSC-a.
 - Događaji pogrešnog prijenosa simbola iste kodne riječi su neovisni → omogućen jednostavan proračun vjerojatnosti pojave pogreške na k pozicija unutar kodne riječi duljine n simbola.
- ◆ Primjer: Neka je točno k unaprijed određenih pozicija simbola neke kodne riječi, duljine n , pogrešno preneseno. Vjerojatnost ovog događaja je:
$$p_g^k (1 - p_g)^{n-k}$$
- ◆ Dobiveni izraz predstavlja vjerojatnost pojave bilo kojeg vektora pogreške s k pogrešnih simbola.

Vjerojatnost ispravnog dekodiranja (2/3)

- ◆ Primjer: Za kôd $[n, k, d] = [5, 2, 3]$ vrijedi:
 $p(00001)=p(00010)=p(00100)=p(01000)=p(10000)=$
 $= p_g (1 - p_g)^4$
- ◆ Vjerojatnost $p(K)$ da će riječ dobivena dekodiranjem **pomoću standardnog niza** biti jednaka poslanoj računa se iz:

$$p(K) = \sum_{i=0}^n N_i p_g^i (1 - p_g)^{n-i}$$

- N_i je broj vektora pogreške s i jedinica koji pripadaju standardnom nizu blok koda K duljine n .

- Primjer (kôd $[5, 2, 3]$): $\{00000\} \rightarrow N_0 = 1$; $\{00001, 00010, 00100, 01000, 10000\} \rightarrow N_1 = 5$; $N_2 = N_3 = N_4 = N_5 = 0$.

Vjerojatnost ispravnog dekodiranja (3/3)

- ◆ Ukoliko je poznata udaljenost koda – $d(K)$ tada kôd K može ispraviti najviše t -struku pogrešku $\rightarrow d(K) \geq 2t + 1$.

- U standardnom nizu se zasigurno nalaze svi vektori pogreške s $0 \leq i \leq t$ jedinica.

$$N_i = \binom{n}{i}$$

- Općenito gledano, u standardnom nizu se mogu nalaziti i vektori pogreške s više od t jedinica.
 - Ne postoji jednostavan način proračuna N_i .
- ◆ Ako je kôd K perfektan tada su sve riječi unutar kugli radijusa t .
 - U standardnom nizu tada se nalaze isključivo vektori pogreške s t i manje jedinica.
- ◆ *Vjerojatnost ispravnog dekodiranja u tom slučaju je:*

$$p(K) = \sum_{i=0}^t \binom{n}{i} p_g^i (1 - p_g)^{n-i}$$

Definicija: Kodna brzina zaštitnog koda

- ◆ Oznaka: $R(K)$ = udio informacijskih bitova u kodnoj riječi.
 - $K = [n,k]$ - linearni binarni blok kôd;
 - n – duljina kodne riječi;
 - k – broj informacijskih bitova u kodnoj riječi.

$$R(K) = \frac{k}{n} \leq 1$$

Zaštitno kodiranje II

Teorija informacije

Sadržaj predavanja

- ◆ Uvod
 - Komunikacijski sustav; Cilj zašt. kodiranja; Podjela zaštitnih kodova.
- ◆ Blok kodovi
 - Uvod
 - Paritetno kodiranje
 - Linearno binarni blok kodovi
 - Generirajuća matrica **G** i njen standardni oblik
 - » Kodiranje
 - » Dekodiranje (dekodiranje preko sindroma)
 - » Proračun vjerojatnosti ispravnog dekodiranja
 - Hammingovi kodovi
 - Ciklični kodovi

Hammingovi i ciklični kodovi

(klasa linearnih blok kodova)

Hammingovi kodovi

Definicija: Hammingov kôd

Hammingov kôd: Neka je r pozitivan cijeli broj i neka je \mathbf{H} matrica dimenzija $r \times (2^r - 1)$ čije stupce sačinjavaju svi vektori dimenzije r različiti od $\mathbf{0}$ iz vektorskog prostora $V(r)$. Matrica \mathbf{H} je matrica provjere pariteta Hammingovog koda s oznakom $\text{Ham}(r)$.

- ◆ Primjer: Matrice provjere pariteta: $r = 3$, $n = 2^3 - 1 = 7$

$$\mathbf{H}_1^T = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{matrix} \quad \text{ili} \quad \mathbf{H}_2^T = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{matrix} 7 \\ 6 \\ 3 \\ 5 \\ 4 \\ 2 \\ 1 \end{matrix}$$

- ◆ Stupci matrica provjere pariteta su binarni ekvivalenti cijelih brojeva od 1 do $2^r - 1$!
Redoslijed je nevažan!

Svojstva Hammingovih kodova

Svojstva Hammingovih kodova: Neka je $\text{Ham}(r)$ binarni Hammingov kôd. Za $r \geq 2$ vrijedi da je $\text{Ham}(r)$:

- linearan blok-kôd $[2^r-1, 2^r-1-r]$;
- ima najmanju distancu 3 (otkriva dvostruku i ispravlja jednostruku pogrešku);
- perfektni kôd.

Neki mogući Hammingovi
kodovi i njihove distance!

$[n,k,3]$	$[n,k,5]$	$[n,k,7]$	$[n,k,9]$	$[n,k,11]$	$[n,k,13]$
[3,1,3]	[5,1,5]	[7,1,7]	[9,1,9]	[11,1,11]	[13,1,13]
[5,2,3]	[8,2,5]	[11,2,7]	[14,2,9]	[17,2,11]	[20,2,13]
[6,3,3]	[10,3,5]	[13,3,7]	[17,3,9]	[20,3,11]	[24,3,13]
[7,4,3]	[11,4,5]	[14,4,7]	[19,4,9]	[22,4,11]	[26,4,13]
[9,5,3]	[13,5,5]	[15,5,7]	[20,5,9]	[23,5,11]	[27,5,13]
[10,6,3]	[14,6,5]	[17,6,7]	[22,6,9]	[25,6,11]	[29,6,13]
[11,7,3]	[15,7,5]	[18,7,7]	[24,7,9]	[26,7,11]	[32,7,13]
[12,8,3]	[16,8,5]	[19,8,7]	[25,8,9]	[28,8,11]	[34,8,13]
[13,9,3]	[17,9,5]	[20,9,7]	[26,9,9]	[30,9,11]	[35,9,13]
[14,10,3]	[19,10,5]	[21,10,7]	[28,10,9]	[31,10,11]	[36,10,13]

Kodiranje pomoću Hammingovog koda

- ◆ Primjer: Hammingov kôd [7, 4, 3]

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

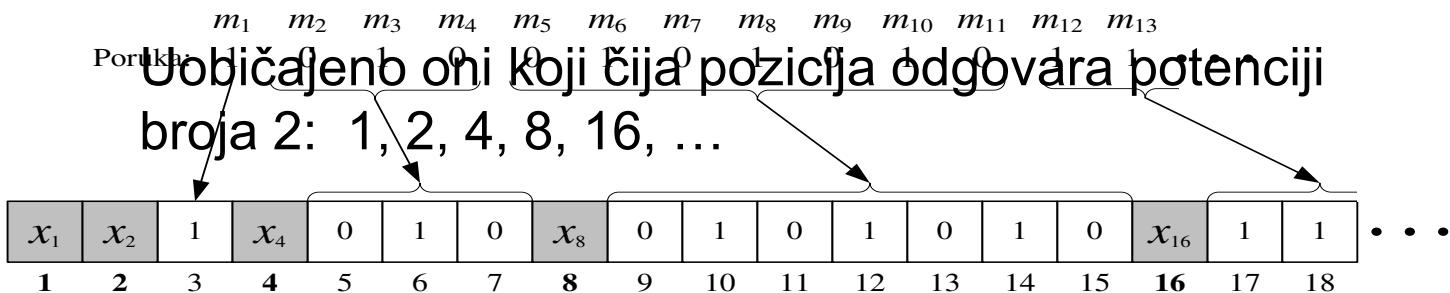
- ◆ Generirajuću matricu \mathbf{G} nije jednostavno izračunati iz \mathbf{H} jer ista nije u standardnom obliku, tj. jednadžba $\mathbf{GH}^T = \mathbf{0}$ daje velik broj mogućnosti.
- ◆ Potrebno je dobiti sistematičan kôd iz kojeg jednostavno dobivamo poslanu kodiranu poruku.
- ◆ **Važno svojstvo matrice \mathbf{H} :** Svaki redak matrice provjere pariteta određuje pozicije simbola kodne riječi čiji zbroj mora bit paran broj (ili jednak 0 u aritm. mod. 2).

Formiranje kodne riječi Hammingovog koda

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

prvi redak	Pozicije (1), (3), (5) i (7).
drugi redak	Pozicije (2, 3), (6 i 7),
treći redak	Pozicije (4, 5, 6 i 7),

Ključno pitanje - koji bitovi su zaštitni?



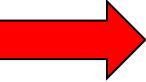
$$x_1 = m_1 + m_2 + m_4 + m_5 + m_7 + \dots = x_3 + x_5 + x_7 + x_9 + \dots$$

$$x_2 = m_1 + m_3 + m_4 + m_6 + m_7 + \dots = x_3 + x_6 + x_7 + x_{10} + x_{11} + \dots$$

$$x_4 = m_2 + m_3 + m_4 + m_8 + m_9 + m_{10} + m_{11} + \dots = x_5 + x_6 + x_7 + x_{12} + x_{13} + x_{14} + x_{15} \dots$$

•

Primjer: formiranje kodne riječi za Hammingov kôd [7, 4, 3]

Poruka  1 0 1 0

x_1	x_2		x_4			
-------	-------	--	-------	--	--	--

Okvir kodne riječi

$$H = \begin{array}{|c|c|c|c|c|c|c|} \hline & \times & & \times & & \times & \\ \hline & & \times & & & \times & \times \\ \hline & & & \times & & & \\ \hline \end{array}$$

Primjer: generirajuća matrica za Hammingov kôd [7, 4, 3]

- (1) Izbriši one stupce koji su na pozicijama paritetnih bitova
- (2) Dobivenu matricu transponiraj
- (3) Stupce transponirane matrice postavi na pozicije 1, 2, 4, 8, 16, ...
- (4) Ostatak stupaca popuni jediničnom matricom

1 2 4

↓ ↓ ↓

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

G = $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$

$$I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

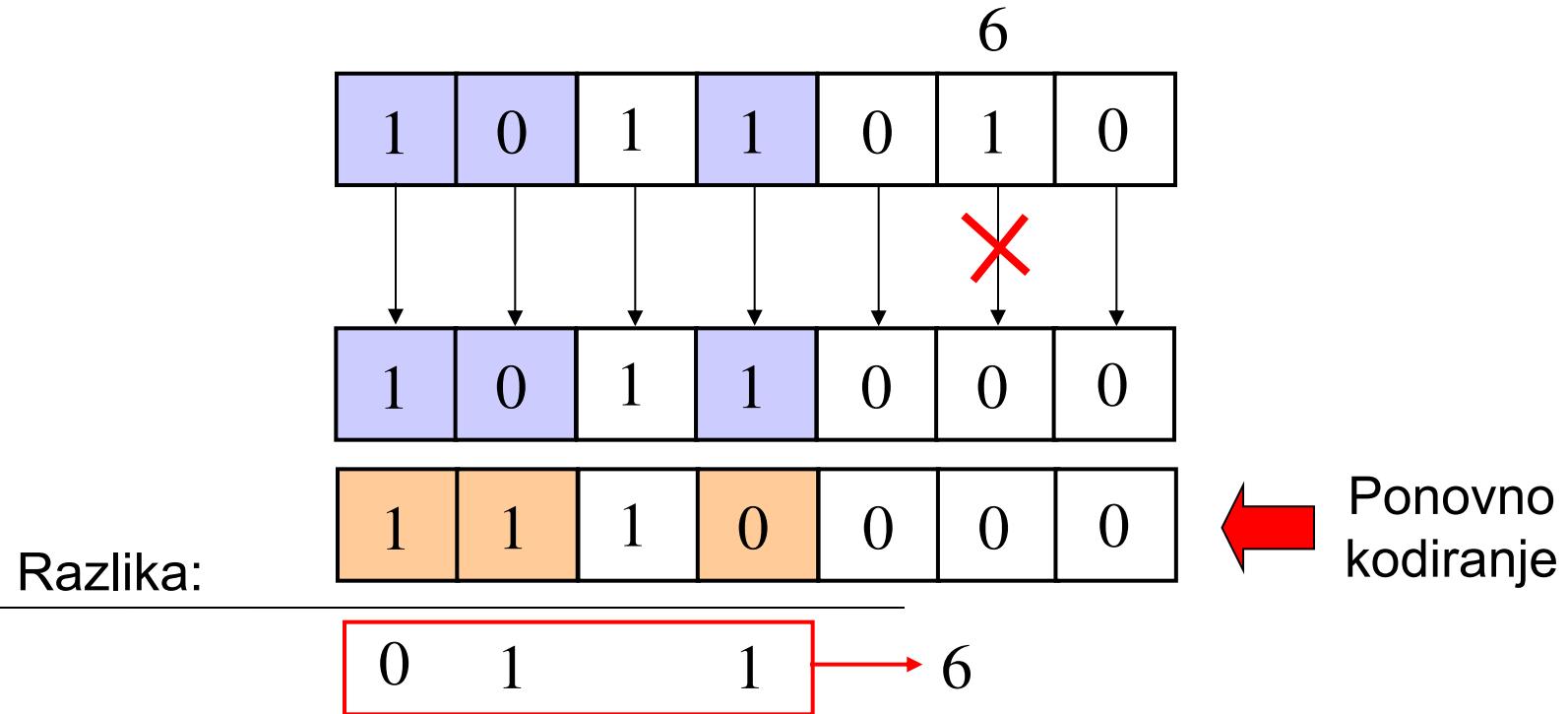
Primjer: sindrom za Hammingov kôd [7, 4, 3]

Napomena: Vrijedi samo za standardni način formiranja Hammingovih riječi!

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

e	S(y)	CJELOBROJNI EKVIVALENT
1 0 0 0 0 0 0	1 0 0	1
0 1 0 0 0 0 0	0 1 0	2
0 0 1 0 0 0 0	1 1 0	3
0 0 0 1 0 0 0	0 0 1	4
0 0 0 0 1 0 0	1 0 1	5
0 0 0 0 0 1 0	0 1 1	6
0 0 0 0 0 0 1	1 1 1	7

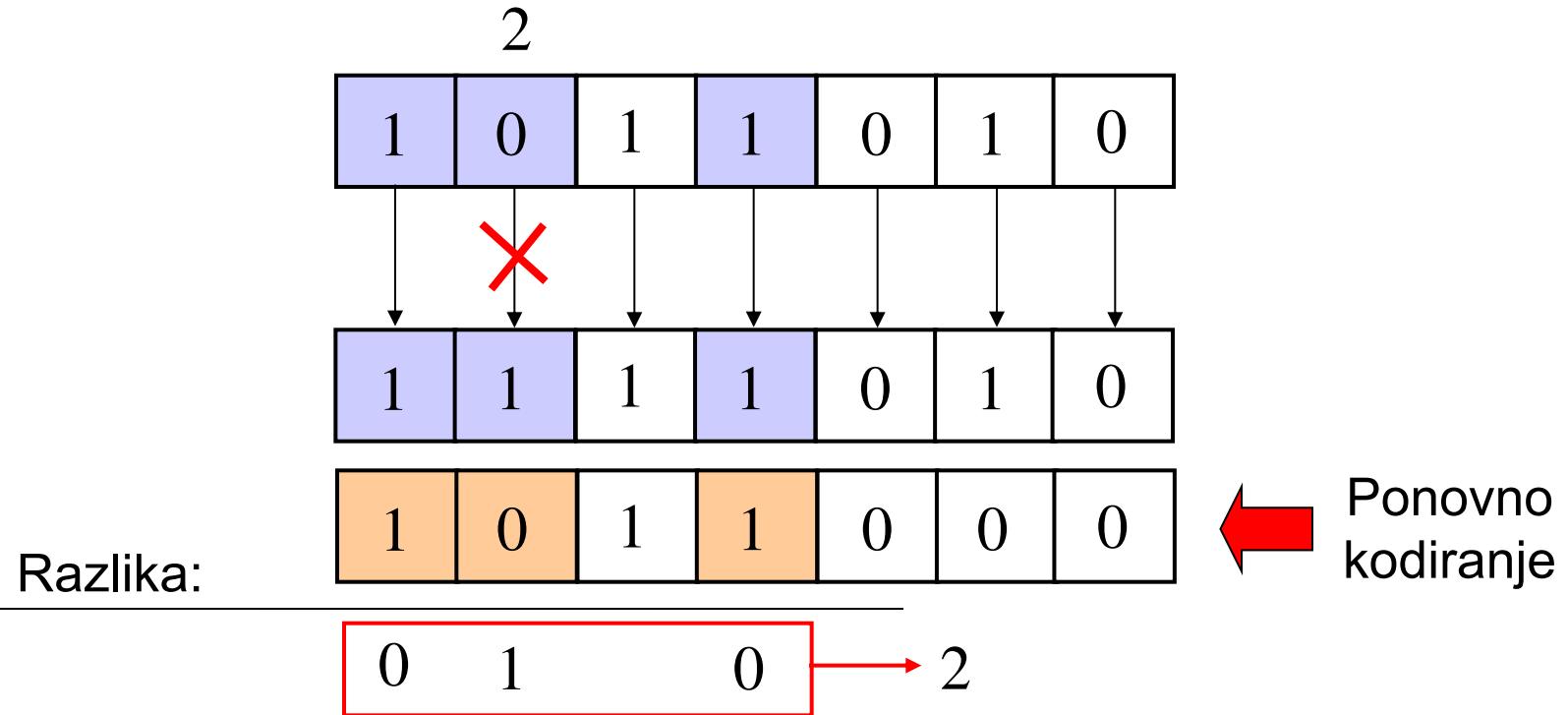
Primjer: određivanje sindroma bez matrice provjere pariteta (1/2)



Pogreška je na poziciji br. 6, a ispravna kodna riječ

1 0 1 1 0 1 0

Primjer: određivanje sindroma bez matrice provjere pariteta (2/2)



Pogreška je na poziciji br. 2, a ispravna kodna riječ

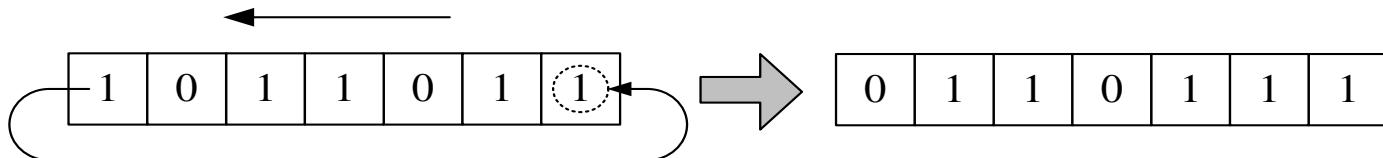
1 0 1 1 0 1 0

Ciklični kodovi

Definicija: ciklični kôd

Ciklični kôd: Blok kôd K je ciklični kôd ako je:

- linearan blok-kôd i
- ako bilo koji ciklični posmak kodne riječi iz K opet daje kodnu riječ iz K .



Ako je 11110000 kodna riječ, onda su kodne riječi i

11100001
 11000011
 10000111
 00001111
 00011110
 00111100
 01111000

Polinomski zapis kodne riječi

- ♦ Kodna riječ $[a_{n-1} \ a_{n-2} \dots \ a_2 \ a_1 \ a_0]$ cikličnog koda može se poistovjetiti s polinomom stupnja $n - 1$:

$$\mathbf{a} = [a_{n-1} \dots \ a_2 \ a_1 \ a_0] \leftrightarrow \ a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_2x^2 + a_1x^1 + a_0x^0$$

$a(x)$ ne promatramo kao funkciju, nego čisto kao način zapisa. Na primjer,

$$a_{n-1}(x^n - 1) + a_{n-2}x^{n-1} + \dots + a_1x^2 + a_0x^1 + a_{n-1}\overset{\wedge}{x^0} \quad : \quad x^n - 1 = a_{n-1}$$

Koeficijenti $-a_{n-1}(x^n - 1)$
aritmetički

$$\begin{aligned} & a_{n-2}x^{n-1} + \dots + a_1x^2 + a_0x^1 + a_{n-1}\overset{\wedge}{x^0} && \leftarrow \text{ostatak nakon dijeljenja.} \\ &= a_{n-1}(x^n - 1) + a_{n-2}x^{n-1} + \dots + a_1x^2 + a_0x^1 + a_{n-1}\overset{\wedge}{x^0}. \end{aligned}$$

Nad polinomima kodnih riječi vršimo operacije u aritmetici modulo $x^n - 1$!
Zbrajanje polinoma odgovara zbrajanju vektora, a množenje s x odgovara cikličnom posmaku ulijevo.

Primjer: ciklični posmak kodne riječi

- ◆ $a = [1 \ 0 \ 1]$ – polinom je $a(x) = x^2 + 1$, duljina riječi $n = 3$

$$b'(x) = a(x) \cdot x = x^3 + x,$$

$$\begin{array}{r} x^3 + x \\ - x^3 \quad +1 \\ \hline x + 1 \end{array} \quad \leftarrow \text{ostatak nakon dijeljenja.}$$

- ◆ $b = [0 \ 1 \ 1]$ kodna riječ nastala cikličnim posmakom kodne riječi a ulijevo za jedno mjesto!
- ◆ Svaka kodna riječ duljine n je polinom stupnja $n - 1$ i nad njim sve operacije provodimo u aritmetici mod $x^n - 1$;
- ◆ Skup svih riječi u mod $x^n - 1$ aritmetici označavamo s R_n ;
- ◆ Ciklični kôd je neki podskup od R_n :

$$K \subset R_n$$

Uvjeti za cikličan kôd

Uvjeti za cikličan kôd: Kôd $K \subset R_n$ je cikličan kôd ako i samo ako K zadovoljava sljedeća dva uvjeta:

- $\forall a(x), b(x) \in K$, vrijedi $a(x) + b(x) \in K$ (svojstvo linearnosti);
- $\forall a(x) \in K$ i $\forall r(x) \in R_n$, vrijedi $r(x) \cdot a(x) \text{mod}(x^n - 1) \in K$.

Kako dobiti sve kodne riječi nekog cikličkog koda?

- izaberi bilo koji polinom $f(x)$ najvećeg stupnja $n - 1$;
- sve kodne riječi cikličnog koda K dobit će se množenjem svih $r(x) \in R$ s $f(x)$;

Kaže se da je kôd K generiran polinomom $f(x)$:

$$K \equiv \langle f(x) \rangle = \{r(x)f(x) \mid r(x) \in R_n\}.$$

$f(x)$ je kodna riječ koda K !

Primjer: generiranje cikličnog koda

- ◆ Polinom kojim se generira kôd K : $f(x) = x^2 + 1$
- ◆ $n=3$, broj polinoma u R^n je $2^3 = 8$.

$(0x^2 + 0x + 0)$	\cdot	$(x^2 + 1)(\text{mod } (x^3 - 1))$	$=$	$0x^2 + 0x + 0$	[000]
$(0x^2 + 0x + 1)$	\cdot	$(x^2 + 1)(\text{mod } (x^3 - 1))$	$=$	$1x^2 + 0x + 1$	[101]
$(0x^2 + 1x + 0)$	\cdot	$(x^2 + 1)(\text{mod } (x^3 - 1))$	$=$	$0x^2 + 1x + 1$	[011]
$(0x^2 + 1x + 1)$	\cdot	$(x^2 + 1)(\text{mod } (x^3 - 1))$	$=$	$1x^2 + 1x + 0$	[110]
$(1x^2 + 0x + 0)$	\cdot	$(x^2 + 1)(\text{mod } (x^3 - 1))$	$=$	$1x^2 + 1x + 0$	[110]
$(1x^2 + 0x + 1)$	\cdot	$(x^2 + 1)(\text{mod } (x^3 - 1))$	$=$	$0x^2 + 1x + 1$	[011]
$(1x^2 + 1x + 0)$	\cdot	$(x^2 + 1)(\text{mod } (x^3 - 1))$	$=$	$1x^2 + 0x + 1$	[101]
$(1x^2 + 1x + 1)$	\cdot	$(x^2 + 1)(\text{mod } (x^3 - 1))$	$=$	$0x^2 + 0x + 0$	[000]

$$K = \begin{Bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{Bmatrix} \quad \xrightarrow{\hspace{1cm}} \quad \mathbf{G} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Generirajući polinom cikličnog koda

Generiranje cikličnog koda: Neka je K ciklični kôd dimenzije veće od 1, podskup od R_n .

- Postoji jedinstven polinom $g(x)$ najmanjeg stupnja u K .
- Kôd K je generiran upravo polinomom $g(x)$.
- $g(x)$ je faktor polinoma $x^n - 1$, tj. $x^n - 1 = g(x) \cdot q(x)$.

Polinom $g(x)$ koji zadovoljava ovo svojstvo nazivamo:

Generirajući polinom cikličkog koda

Primjer: $g(x)$ je jedan od faktora polinoma $x^{15} - 1$:

$$x^{15} - 1 = (x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$$

Svaki faktor generira jedan mogući ciklički kôd, pa faktORIZIRANjem polinoma $x^{15} - 1$ praktički dobivamo 5 različitih cikličkih kodova s generirajućim polinomima:

$$\begin{aligned}g_1(x) &= x + 1, & g_2(x) &= x^2 + x + 1, & g_3(x) &= x^4 + x + 1, \\g_4(x) &= x^4 + x^3 + 1, & g_5(x) &= x^4 + x^3 + x^2 + x + 1\end{aligned}$$

Generirajuća matrica cikličnog koda

Generirajuća matrica cikličnog koda: Neka je generirajući polinom cikličnog koda $K \subset R_n$:

$$g(x) = g_r x^r + \dots + g_2 x^2 + g_1 x + g_0.$$

Onda je dimenzija koda $k = n - r$, a generirajuća matrica koda je:

$$\mathbf{G} = \begin{bmatrix} g_r & g_{r-1} & g_{r-2} & \cdots & g_1 & g_0 & 0 & 0 & \cdots & 0 \\ 0 & g_r & g_{r-1} & g_{r-2} & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\ 0 & 0 & g_r & g_{r-1} & g_{r-2} & \cdots & g_1 & g_0 & \vdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & g_r & g_{r-1} & g_{r-2} & \cdots & g_1 & g_0 \end{bmatrix}.$$

- ◆ Broj redaka matrice \mathbf{G} odgovara dimenziji koda - $k = n - r$;
- ◆ Broj stupaca matrice \mathbf{G} odgovara duljini kodne riječi – n ;
- ◆ Što je stupanj generirajućeg polinoma $g(x)$ veći, dimenzija koda je manja!

Primjer: generirajuća matrica cikličnog koda ($n = 5$)

$$n = 5$$



$$x^5 - 1 = (x+1)(x^4 + x^3 + x^2 + x + 1)$$

Potencijalni generirajući polinomi:

$$\left\{ \begin{array}{l} g_1(x) = x + 1 \\ g_2(x) = x^4 + x^3 + x^2 + x + 1 \end{array} \right. \quad \begin{array}{l} r = 1, k = 5 - 1 = 4 \\ r = 4, k = 5 - 4 = 1 \end{array}$$

$$g_1(x) = x + 1 \quad \rightarrow \quad G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad \begin{array}{c} \uparrow \\ k = 4 \\ \downarrow \\ \longleftarrow n = 5 \longrightarrow \end{array}$$

$$g_2(x) = x^4 + x^3 + x^2 + x + 1$$



$$G = [\ 1 \ 1 \ 1 \ 1 \ 1 \]$$

Faktorizacije nekih polinoma oblika $x^n - 1$

n	aritmetika	faktorizacija u aritmetici modulo 2
1	$x^1 - 1$	$x + 1$
2	$x^2 - 1$	$(x + 1)^2$
3	$x^3 - 1$	$(x + 1)(x^2 + x + 1)$
5	$x^5 - 1$	$(x + 1)(x^4 + x^3 + x^2 + x + 1)$
7	$x^7 - 1$	$(x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$
9	$x^9 - 1$	$(x + 1)(x^2 + x + 1)(x^6 + x^3 + 1)$
11	$x^{11} - 1$	$(x + 1)(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$
13	$x^{13} - 1$	$(x + 1)(x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$
15	$x^{15} - 1$	$(x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$
17	$x^{17} - 1$	$(x + 1)(x^8 + x^5 + x^4 + x^3 + 1)(x^8 + x^7 + x^6 + x^4 + x^2 + x + 1)$
19	$x^{19} - 1$	$(x + 1)(x^{18} + x^{17} + x^{16} + \dots + x^4 + x^3 + x^2 + x + 1)$

Standardni oblik generirajuće matrice

- ◆ Traženi oblik matrice \mathbf{G} : $\mathbf{G} = [\mathbf{I}_k \mid \mathbf{A}]$.

ALGORITAM:

- ◆ I. Upiši $g(x)$ u binarnom obliku u k -ti redak.
- ◆ II. $(k - 1)$ -vi redak dobije se cikličnim posmakom k -tog retka za jedno mjesto u lijevo. Ovo odgovara operaciji $xg(x)$.
- ◆ k -ti stupac mora u $(k - 1)$ -om retku imati nulu kako bi imali standardni oblik matrice \mathbf{G} .
 - Ako je $1 \rightarrow$ na $(k - 1)$ -i redak treba dodati k -ti redak (aritm. mod. 2);
- ◆ III. Za $(k - 2)$ redak treba primijeniti postupak iz točke II.
 - Napraviti ciklični posmak $(k - 1)$ -og retka za jedno mjesto u lijevo.
 - Ako k -ti stupac u $(k - 2)$ -om retku ima $1 \rightarrow$ dodaj na $(k - 2)$ -i redak k -ti redak (aritm. mod. 2);
- ◆ Ponavljaj algoritam za svaki sljedeći redak sve dok se ne popuni matrica \mathbf{G} .

Primjer: standardni oblik generirajuće matrice G

- Neka je $g(x) = x^4 + x^3 + x^2 + 1$ i neka je dan ciklični kôd $[n, k] = [7, 3]$.

$$\begin{array}{c}
 \left[\begin{array}{|ccc|cccc|} \hline & & & & & & \\ \hline 0 & 0 & 1 & | & 1 & 1 & 0 & 1 \\ \hline \end{array} \right] \xleftarrow{\text{Upišimo } g(x) \text{ u 3. redak}}
 \\
 \\
 \left[\begin{array}{|ccc|cccc|} \hline & & & & & & \\ \hline 0 & 1 & 1 & | & 1 & 0 & 1 & 0 \\ \hline 0 & 0 & 1 & | & 1 & 1 & 0 & 1 \\ \hline \end{array} \right] \xleftarrow{\text{2. redak dobijemo cikličnim posmakom 3. retka za jedno mjesto u lijevo.}}
 \\
 \\
 \left[\begin{array}{|ccc|cccc|} \hline & & & & & & \\ \hline 0 & 1 & 0 & | & 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 1 & | & 1 & 1 & 0 & 1 \\ \hline \end{array} \right] \xrightarrow{\text{2. redak i 3. stupac } \rightarrow 1. \text{ Potrebno je dodati 3. redak na 2. redak (aritm. mod. 2).}}
 \\
 \\
 \left[\begin{array}{|ccc|cccc|} \hline & & & & & & \\ \hline 1 & 0 & 0 & | & 1 & 1 & 1 & 0 \\ \hline 0 & 1 & 0 & | & 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 1 & | & 1 & 1 & 0 & 1 \\ \hline \end{array} \right] \xleftarrow{\text{1. redak dobijemo cikličnim posmakom 2. retka za jedno mjesto u lijevo.}}
 \end{array}$$

t

Matrica provjere pariteta cikličnog koda

Polinom za provjeru pariteta: Neka je K ciklični kôd duljine n i dimenzije k $[n,k]$ s generirajućim polinomom $g(x)$. Neka je $h(x)$ polinom koji zadovoljava jednadžbu:

$$x^n - 1 = g(x) \cdot h(x).$$

$h(x)$ se zove **polinom za provjeru pariteta cikličnog koda K** .

Matrica provjere pariteta cikličnog koda: Neka je $K \subset R_n$ ciklični kôd duljine n i dimenzije k s generirajućim polinomom $g(x)$ i polinomom za provjeru pariteta

$$h(x) = h_k x^k + \dots + h_2 x^2 + h_1 x + h_0.$$

- *Bilo koji polinom $c(x)$ koda K zadovoljava jednakost $c(x) \cdot h(x) = 0$.*
- *Paritetna matrica koda K je:*

$$\mathbf{H} = \begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k & 0 & 0 & \cdots & 0 \\ 0 & h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k & 0 & \cdots & 0 \\ 0 & 0 & h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k & \vdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k \end{bmatrix}.$$

Primjer: matrica provjere pariteta cikličnog koda ($n = 7$)

Promatramo ciklički kod $n = 7$: $g(x) = x^3 + x^2 + 1$

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

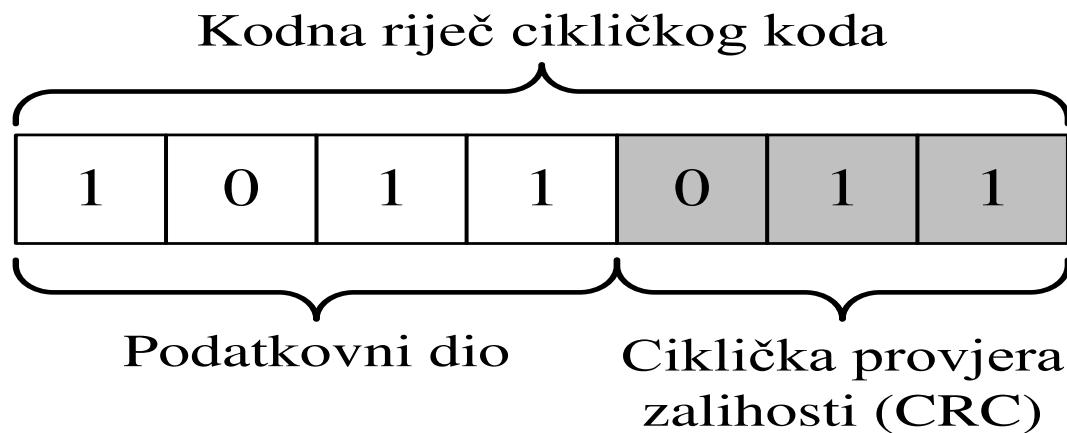
$$x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1) \quad \rightarrow \quad h(x) = \underbrace{1 + x^2 + x^3 + x^4}_{\begin{array}{ccccc} 1 & 0 & 1 & 1 & 1 \end{array}}$$

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & & & & & \end{bmatrix} \begin{array}{c} \uparrow \\ r = 3 \\ \downarrow \end{array}$$

$\longleftrightarrow n = 7 \longleftrightarrow$

Implementacija kodera cikličnog koda (1/2)

- ◆ Duljina kodne riječi može biti iznimno velika!
- ◆ Generirajuća i paritetna matrica imaju prevelike dimenzije za praktičnu implementaciju.
- ◆ Želimo kodnu riječ koja je sistematična tako da odmah možemo razlučiti zaštitne bitove od bitova kodirane poruke:



Rješenje:

- ◆ Cikličku provjeru zalihosti izračunati na osnovu podatkovnog dijela!

Implementacija kodera cikličnog koda (2/2)

- $d(x)$ – polinom kodirane poruke: $[1 \ 0 \ 1 \ 1 \ 1] \rightarrow d(x) = x^4 + x^2 + x + 1$
- $d(x)$ se može pomnožiti s x^r , gdje je r stupanj generirajućeg polinoma:

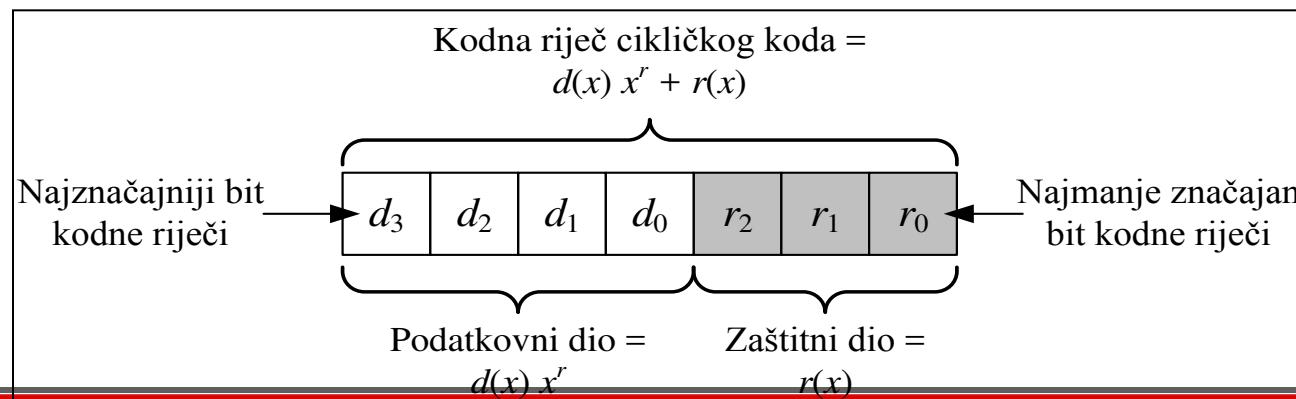
$$d(x) \cdot x^r = g(x)q(x) + r(x).$$

generirajući polinom   kvocijent

ostatak nakon dijeljenja s $g(x)$

Svaki polinom pomnožen s $g(x)$ u aritmetici mod $x^n - 1$ je neka kodna riječ $c(x)$ koda K , pa je i $g(x) \cdot q(x)$ neka kodna riječ. Stoga se bilo koja kodna riječ može dobiti kao zbroj:

$$c(x) = g(x)q(x) = d(x) \cdot x^r + r(x),$$
$$r(x) = d(x) \cdot x^r \bmod [g(x)].$$



Primjer: Generiranje CRC-a

- Poruka je: $\mathbf{d} = [1\ 0\ 1\ 0]$, tj. $d(x) = x^3 + x$,
- Generirajući polinom: $g(x) = x^3 + x + 1 = [1\ 0\ 1\ 1]$,
- Umnožak: $d(x) \cdot x^3 = x^6 + x^4 = [1\ 0\ 1\ 0\ 0\ 0\ 0]$.

$$\begin{array}{r}
 \overbrace{\quad\quad\quad\quad}^{d(x)} \quad\quad\quad\quad \overbrace{\quad\quad\quad\quad}^{g(x)} \\
 \begin{array}{r}
 1\ 0\ 1\ 0 \\
 - 1\ 0\ 1\ 1 \\
 \hline
 0\ 0\ 1 \\
 - 0\ 0\ 0\ 0 \\
 \hline
 0\ 1\ 0 \\
 - 0\ 0\ 0\ 0 \\
 \hline
 1\ 0\ 0 \\
 - 1\ 0\ 1\ 1 \\
 \hline
 \boxed{0\ 1\ 1}
 \end{array} : \quad \begin{array}{r}
 1\ 0\ 1\ 1 = \\
 1\ 0\ 0\ 1
 \end{array}
 \end{array}$$

ostatak nakon dijeljenja

Primjer: Dijeljenje polinoma - Generiranje CRC-a

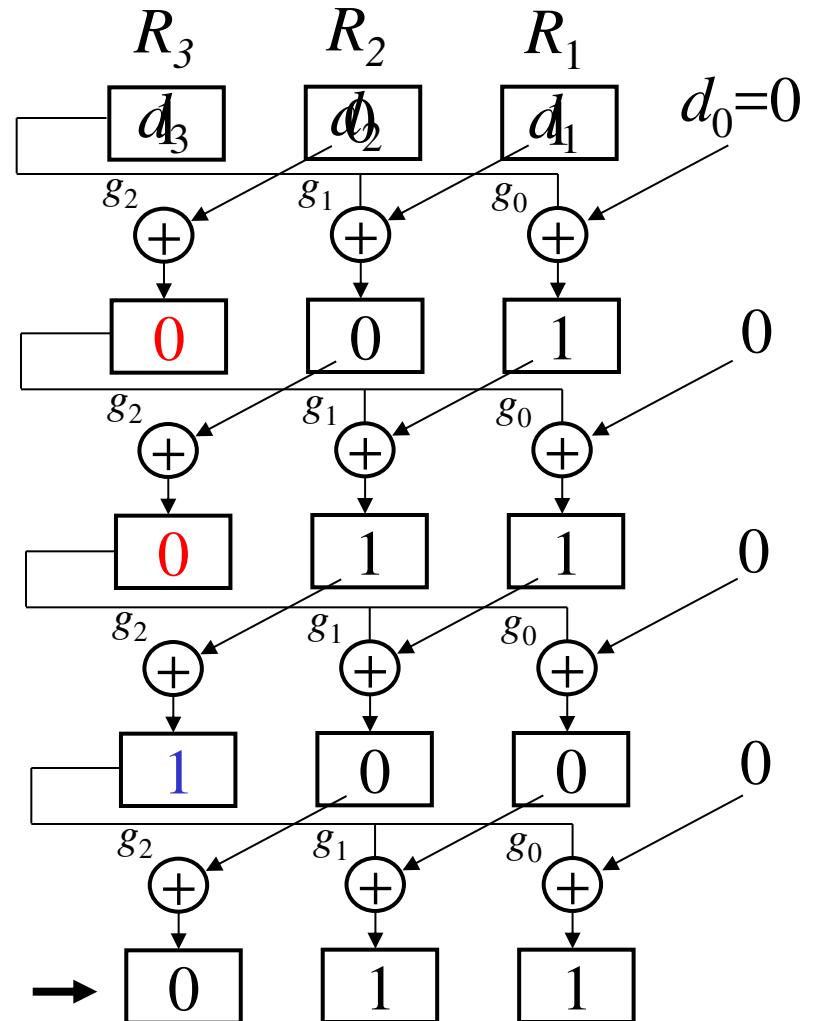
$$q(x) = 1 \ 0 \ 0 \ 1$$

$$\begin{array}{r} 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 : 1 \ 0 \ 1 \ 1 \\ \hline - \ 1 \ 0 \ 1 \ 1 \end{array}$$

- (1) $R_3 = R_2 \oplus (R_3 \cdot g_2)$
 (2) $R_2 = R_1 \oplus (R_3 \cdot g_1)$
 (3) $R_1 = \text{ulazni bit} \oplus (R_3 \cdot g_0),$

$$\begin{array}{r} 1 \ 0 \ 0 \\ - \ 1 \ 0 \ 1 \ 1 \\ \hline 0 \ 1 \ 1 \end{array}$$

ostatak nakon dijeljenja

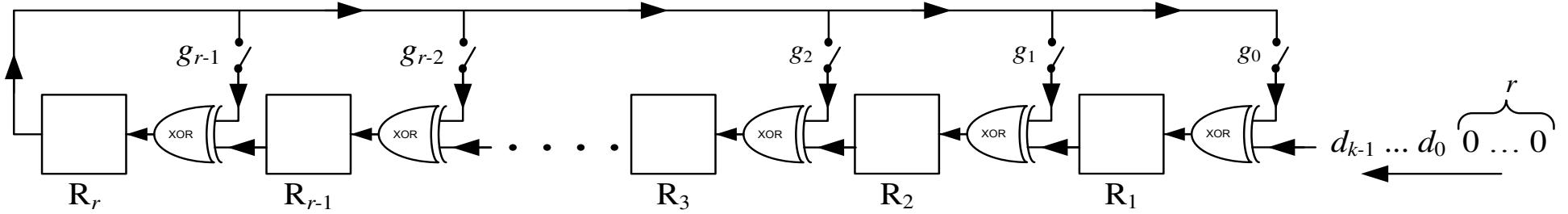
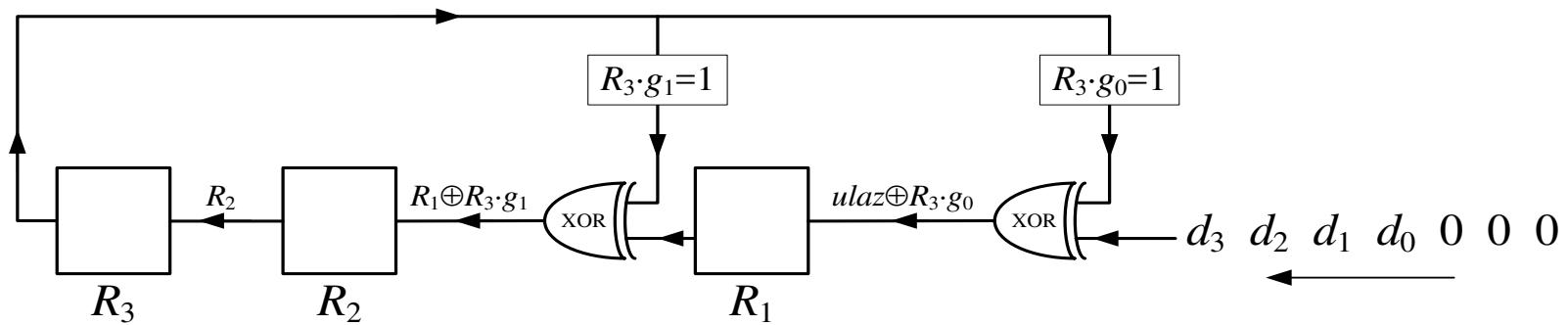


Primjer: Sklop za generiranje CRC-a

$$(1) \quad R_3 = R_2 \oplus (R_3 \cdot g_2)$$

$$(2) \quad R_2 = R_1 \oplus (R_3 \cdot g_1)$$

$$(3) \quad R_1 = \text{ulazni bit} \oplus (R_3 \cdot g_0),$$



Implementacija dekodera (1/4)

- ◆ Proračun sindroma ima preveliku složenost zbog velike duljine kodnih riječi.
- ◆ Temeljno pitanje: Možemo li sindrom izračunati principom sličnim izračunu zalihosnog dijela CRC?
- ◆ Smisao sindroma: Svaka kodna riječ na kojoj je nastupila pogreška na istoj poziciji mora imati isti sindrom!

e				S(y)
00000	1 1 1 0 0	0 0 1 1 1	1 1 0 1 1	0 0 0
00001	1 1 1 0 1	0 0 1 1 0	1 1 0 1 0	0 0 1
00010	1 1 1 1 0	0 0 1 0 1	1 1 0 0 1	0 1 0
00100	1 1 0 0 0	0 0 0 1 1	1 1 1 1 1	1 0 0
01000	1 0 1 0 0	0 1 1 1 1	1 0 0 1 1	1 0 1
10000	0 1 1 0 0	1 0 1 1 1	0 1 0 1 1	1 1 0

Implementacija dekodera (2/4)

$e(x)$ je polinom pogreške: $\mathbf{e} = [1 \ 0 \ 0 \ 1 \ 1]$, $e(x) = x^4 + x + 1$

Primljena kodna riječ: $y(x) = c(x) + e(x)$.

Što dobivamo funkcijom $S[y(x)] = x^r \cdot y(x) \bmod g(x)$?

$$\begin{aligned} S[y(x)] &= x^r y(x) \bmod g(x) \\ &= x^r [c(x) + e(x)] \bmod g(x) \\ &= x^r c(x) \bmod g(x) + x^r e(x) \bmod g(x) \\ &= S[c(x)] + S[e(x)]. \end{aligned}$$

$$\begin{aligned} c(x) &= g(x)q(x) \mid \cdot x^r \Rightarrow \\ c(x)x^r &= g(x)q(x)x^r. \end{aligned}$$

Ako $c(x) \cdot x^r$ podijelimo s $g(x)$ ostatak je 0!

$$S[c(x)] = x^r \cdot c(x) \bmod g(x) = 0.$$

Implementacija dekodera (3/4)

Primjenom funkcije $S[y(x)] = x^r \cdot y(x) \bmod g(x)$

na primljenu kodnu riječ $y(x)$ dobivamo:

$$S[y(x)] = S[c(x)] + S[e(x)] = S[e(x)],$$

$S[y(x)]$ za kodne riječi s istom pogreškom uvijek daje isti rezultat!

$S[y(x)]$ je funkcija za računanje sindroma primljene kodne riječi!!!

$$S[y(x)] = x^r \cdot y(x) \bmod [g(x)]$$

$$r(x) = d(x) \cdot x^r \bmod [g(x)].$$

JOŠ VAŽNIJE:

Sindrom se određuje na IDENTIČAN način kao i zaštitni dio kodne riječi.

Slijedi da je i sklop za računanje sindroma jednak onome za izračunavanje CRC-a!

Implementacija dekodera (4/4)

Primjer dekodera za slučaj koda $(7, 4, 3)$ s generirajućim polinomom: $g(x) = x^3 + x + 1$

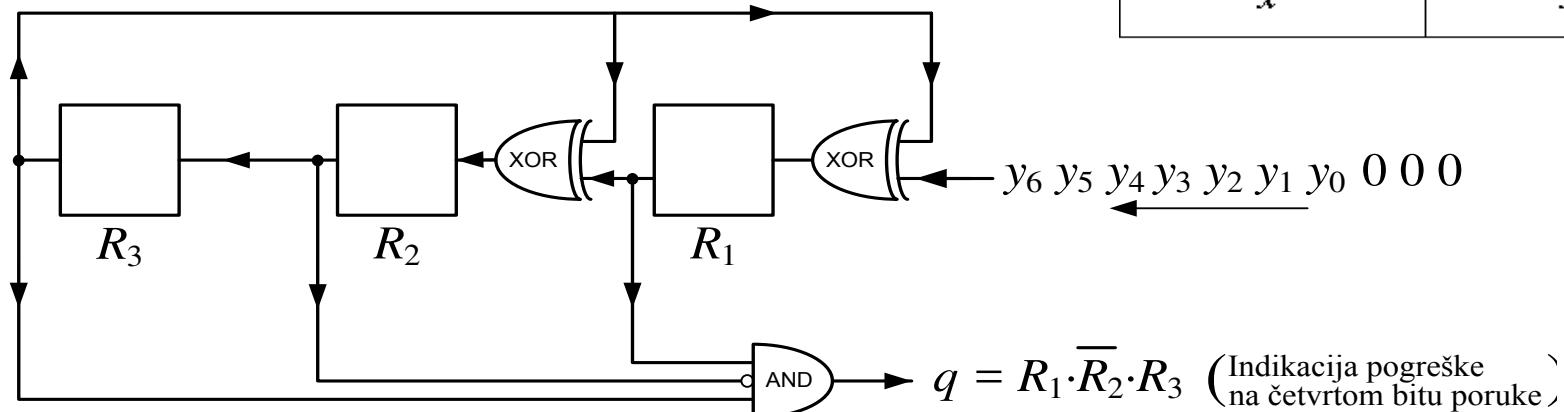
Želimo detektirati pogrešku na 4. bitu – $e(x)=x^3$

$$S[y(x)] = S[e(x)] = x^2 + 1$$

$$q = R_3 \cdot \overline{R_2} \cdot R_1$$

Tablica sindroma

$e(x)$	$S[e(x)]$
1	$x+1$
x	$x^2 + x$
x^2	$x^2 + x + 1$
x^3	$x^2 + 1$
x^4	1
x^5	x
x^6	x^2



Komunikacijski kanali i signali

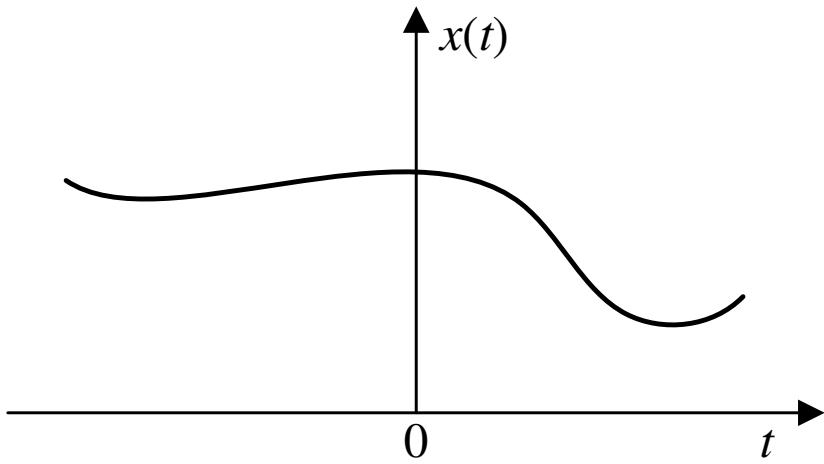
Teorija informacije

- ◆ signal – pojava koja opisuje neku fizikalnu veličinu
 - u električkim sustavima ta veličina je napon ili struja
- ◆ signal se matematički prikazuje (modelira) funkcijom neovisne varijable t , $t \in \mathbb{R}$
 - t najčešće predstavlja vrijeme
 - funkcija $x(t)$, $x: t \rightarrow x(t)$
 - promatramo isključivo realne signale: $x: \mathbb{R} \rightarrow \mathbb{R}$
- ◆ poseban naglasak bit će stavljen na
 - signale u kontinuiranom vremenu
 - na snagu i energiju signala
 - razlog: snaga potrebna za određivanje kapaciteta kanala

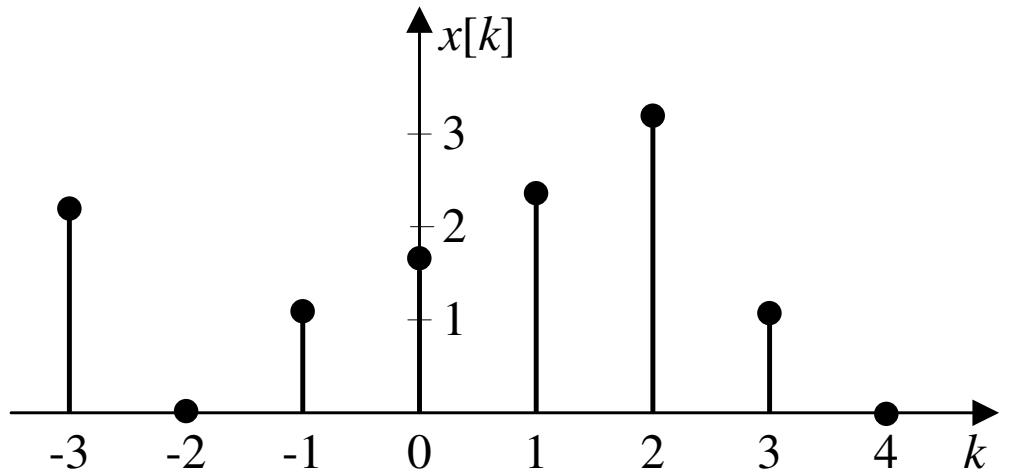
Kontinuirani i diskretni signali

- ◆ signal u kontinuiranom vremenu
 - ako je t kontinuirana varijabla
 - kraći naziv: kontinuirani signal
 - primjer: $x(t) = A \cdot \sin(2\pi ft)$
 - f – frekvencija signala $x(t)$, A – amplituda signala
- ◆ signal u diskretnom vremenu
 - ako varijabla t poprima vrijednosti isključivo u $t = kT$
 - $T \in \mathbb{Q}$, $T \geq 0$, $k \in \mathbb{Z}$
 - označava se kao $\{x_k\}$ ili $x[k] = x[kT]$
 - kraći naziv: diskretni signal

Primjeri kontinuiranih i diskretnih signala



a)



b)

- ◆ a – kontinuirani signal, b – diskretni signal

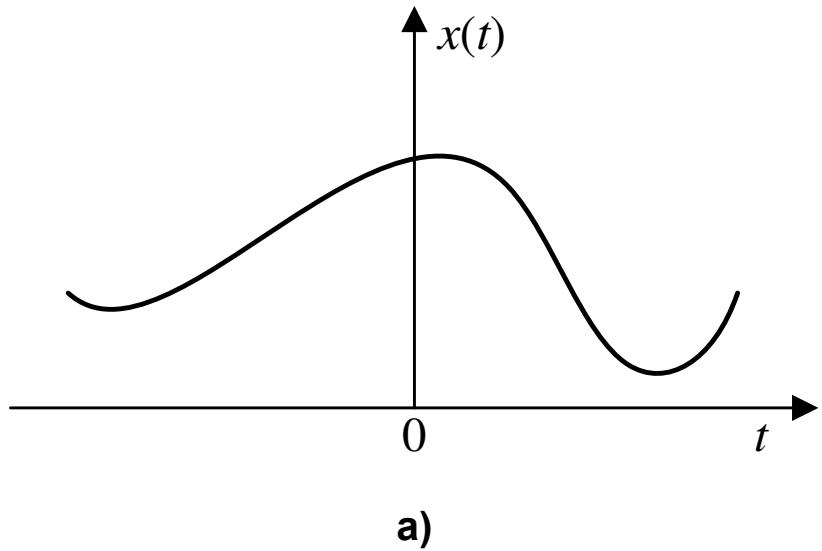
Analogni i digitalni signali

- ◆ promatramo vrijednosti koje signal poprima
- ◆ ako neki signal u kontinuiranom vremenu, $x(t)$, može poprimiti bilo koju vrijednost unutar kontinuiranog intervala (a, b) , $a, b \in \mathbb{R}$ tada se takav signal naziva **analogni signal**
 - primjer analognog signala: $x(t) = A \cdot \sin(2\pi ft)$
 - poprima bilo koju vrijednost na intervalu $[-A, A]$:
 - $x(t) \in [-A, A]$

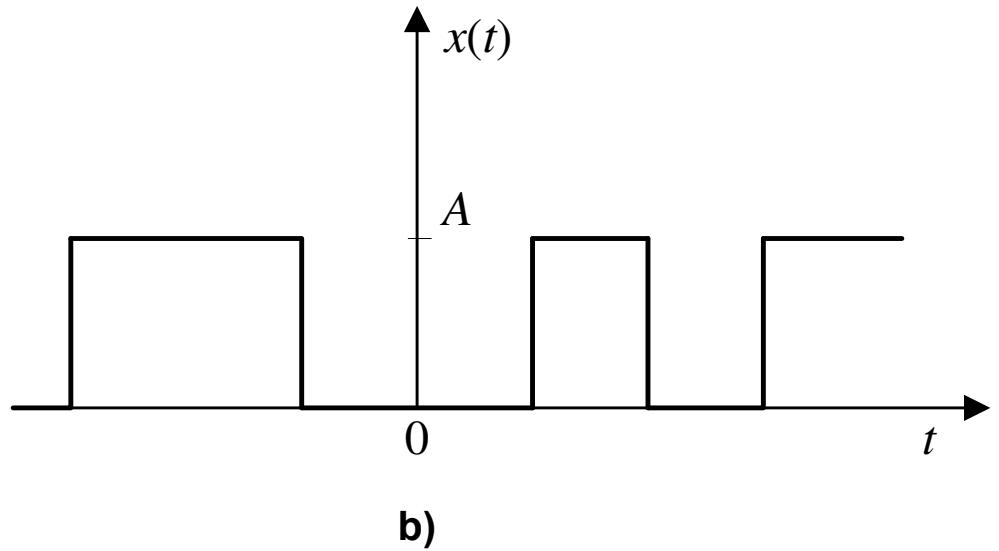
Analogni i digitalni signali (II)

- ◆ neka je $\{a_1, a_2, \dots, a_N\}$ konačan skup od N realnih brojeva
- ◆ **digitalni signal** može u bilo kojem trenutku poprimiti samo jednu od N mogućih vrijednosti iz tog skupa: $x(t) \in \{a_1, a_2, \dots, a_N\}$
- ◆ ako neki signal u diskretnom vremenu, $x[n]$, može poprimiti samo konačan broj različitih vrijednosti, tada se takav signal naziva **digitalni signal**
- ◆ primjer: binarni signal
 - u bilo kojem trenutku može poprimiti jednu od dvije vrijednosti iz skupa $\{0, A\}$, $A \in \square$

Primjeri analognog i digitalnog signala



a)



b)

- ◆ a – analogni signal, b – digitalni signal

Deterministički i slučajni signali

- ◆ deterministički signal
 - vrijednosti $x(t)$ su u potpunosti specificirane u svakom vremenskom trenutku
 - deterministički signal može biti modeliran poznatom funkcijom vremena t
- ◆ slučajni signal
 - u bilo kojem vremenskom trenutku signal poprima neku slučajnu vrijednost i stoga se karakteriziraju statistički
 - modelira se pomoću slučajnog procesa
- ◆ signale u kontinuiranom vremenu dijelimo na **periodične i neperiodične** signale

Srednja snaga determinističkih signala

- ◆ napon $u(t)$, odnosno struja $i(t)$ na otporniku od R ohma [Ω] proizvodi energiju E , odnosno srednju snagu P

$$E = \int_{-\infty}^{\infty} R i^2(t) dt = \int_{-\infty}^{\infty} \frac{u^2(t)}{R} dt \text{ [Ws]},$$

$$P = \lim_{T \rightarrow \infty} \frac{1}{T} \int_{-T/2}^{T/2} R i^2(t) dt \text{ [W]}.$$

- ◆ u nastavku napon, odnosno struja - $x(t)$
- ◆ $R = 1$ om

Periodični signali

- ◆ **periodični signal:** $x(t) = x(t + T), \forall t \in \mathbb{C}$
 - T je realna konstanta
 - neka je T_0 najmanji T za kojeg vrijedi gornja jednakost
 - T_0 se naziva osnovni (fundamentalni) period signala $x(t)$
- ◆ **neperiodični signal** – ne zadovoljava gornje svojstvo
- ◆ razvoj u Fourierov red
$$x(t) = \sum_{k=-\infty}^{\infty} c_k e^{jk\omega_0 t}, \omega_0 = 2\pi f_0$$

$$c_k = \frac{1}{T_0} \int_{-T_0/2}^{T_0/2} x(t) e^{-jk\omega_0 t} dt \quad x(t) \square \quad \sum_{k=-\infty}^{\infty} c_k \delta(f - kf_0) = X(f)$$

Diracova delta funkcija

- ◆ definicija

$$\delta(t) \neq 0 \quad \text{za } t=0 \\ i \quad , \quad t \in \mathbb{R} , \\ \delta(t) = 0 \quad \text{za } t \neq 0$$

- ◆ svojstva

$$\int_{-\infty}^{\infty} \delta(t) dt = 1$$

- neka $x: \mathbb{R} \rightarrow \mathbb{R}$

$$\int_{-\infty}^{\infty} \delta(t - t_0) x(t) dt = x(t_0)$$

Spektar periodičnog signala

- ◆ spektar periodičnog signala $x(t)$ je diskretan
 - poprima vrijednosti samo za diskrete vrijednosti frekvencije: $f_k = k/T_0, k \in \mathbb{Z}$
 - u općenitom slučaju c_k su kompleksne veličine i vrijedi

$$c_{-k} = \overline{c_k}$$

$$c_k = |c_k| e^{-j\theta_k}$$

- ◆ absolutne vrijednosti koeficijenata c_k čine tzv. amplitudni spektar signala $x(t)$
- ◆ θ_k su vrijednosti tzv. faznog spektra signala $x(t)$

Srednja snaga periodičnog signala

- ◆ srednja snaga periodičnog signala u kontinuiranom vremenu

$$P = \lim_{k \rightarrow \infty} \left[\frac{1}{kT_0} k \int_0^{T_0} |x(t)|^2 dt \right] = \frac{1}{T_0} \int_0^{T_0} |x(t)|^2 dt = \sum_{k=-\infty}^{\infty} |c_k|^2$$

$$c_{-k} = \overline{c_k} \quad P = |c_0|^2 + 2 \sum_{k=1}^{\infty} |c_k|^2$$

- ◆ srednja snaga periodičkog signala jednaka je zbroju srednjih snaga svih harmoničkih komponenti od kojih je signal sastavljen

Primjer 1: spektar i srednja snaga trigonometrijskih signala

- ◆ signal $x(t) = A \sin(\omega_0 t)$, $\omega_0 = 2\pi f_0 = 2\pi/T_0$

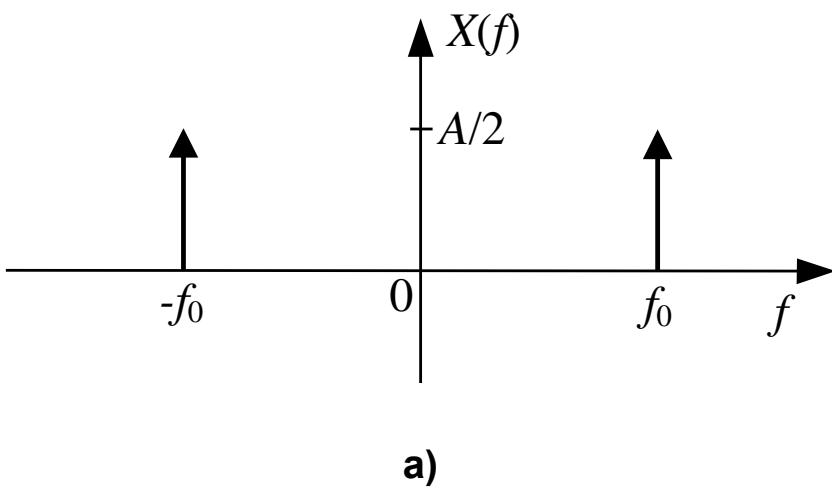
- spektar $X(f)$
$$X(f) = -j \frac{A}{2} [\delta(f - f_0) - \delta(f + f_0)]$$

- ◆ signal $x(t) = A \cos(\omega_0 t)$

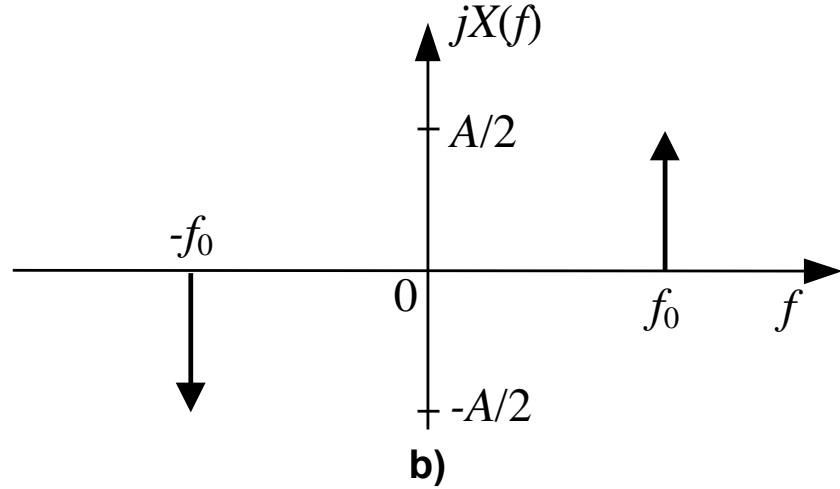
- spektar $X(f)$
$$X(f) = \frac{A}{2} [\delta(f - f_0) + \delta(f + f_0)]$$

- $-j$ u izrazu za spektar sinusnog signala potječe od faznog kašnjenja funkcije sinus u odnosu na funkciju kosinus: $\sin(x) = \cos(x - \pi/2)$, $\forall x \in \mathbb{R}$.

Spektar kosinusnog i sinusnog signala



a)

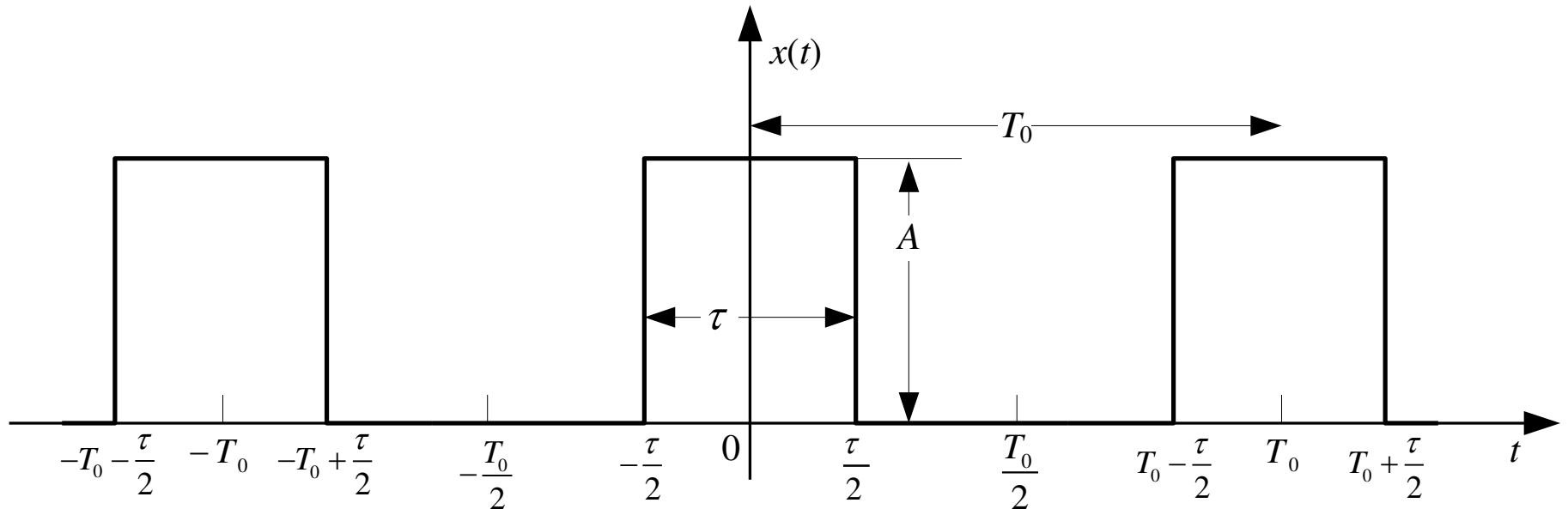


b)

- ◆ a – kosinusni signal, b – sinusni signal

Primjer 2: periodičan slijed pravokutnih impulsa

$$x(t) = \begin{cases} A & \text{za } 0 \leq |t| < \tau/2 \\ 0 & \text{za } \tau/2 < |t| \leq T_0/2 \end{cases}, t \in \mathbb{R}$$



$$c_k = A \frac{\tau}{T_0} \frac{\sin(k\omega_0 \tau/2)}{k\omega_0 \tau/2}$$

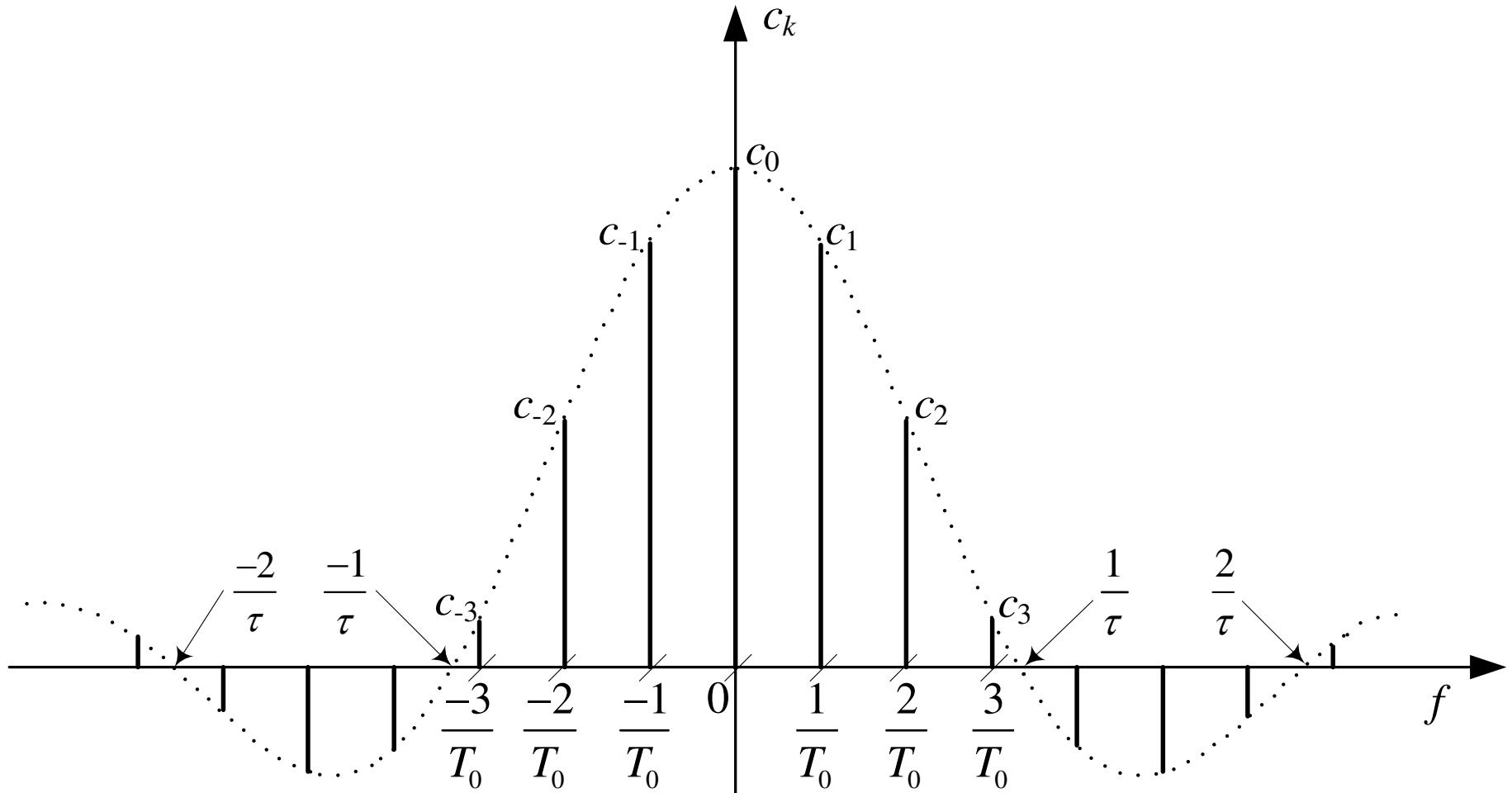
Primjer 2: periodičan slijed pravokutnih impulsa (II)

- ◆ spektar periodičkog slijeda pravokutnih impulsa) diskretan
 - komponente c_k pojavljuju samo na diskretnim frekvencijama k/T_0 [Hz], $k \in \mathbb{Z}$.

$$x(t) = A \frac{\tau}{T} \sum_{k=-\infty}^{\infty} \frac{\sin(k\omega_0\tau/2)}{k\omega_0\tau/2} e^{jk\omega_0 t} = A \frac{\tau}{T} \left[1 + 2 \sum_{k=1}^{\infty} \frac{\sin(k\omega_0\tau/2)}{k\omega_0\tau/2} \cos(k\omega_0 t) \right]$$

$$P = c_0^2 + 2 \sum_{k=1}^{\infty} |c_k|^2 = \left(\frac{A\tau}{T} \right)^2 \left\{ 1 + 2 \sum_{k=1}^{\infty} \left[\frac{\sin(k\omega_0\tau/2)}{k\omega_0\tau/2} \right]^2 \right\} = A^2 \frac{\tau}{T}$$

Spektar periodičnog slijeda pravokutnih impulsa



Neperiodični signali

- ◆ snaga i energija signala $x(t)$

$$E = \lim_{T \rightarrow \infty} \int_{-T}^T |x(t)|^2 dt = \int_{-\infty}^{\infty} |x(t)|^2 dt,$$

$$P = \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T |x(t)|^2 dt.$$

- ◆ spektar signala $x(t)$, $X(f)$ – Fourierova transformacija

$$X(f) = \int_{-\infty}^{\infty} x(t) e^{-j2\pi ft} dt \text{ ili } X(\omega) = \int_{-\infty}^{\infty} x(t) e^{-j\omega t} dt, \omega = 2\pi f$$

- ◆ Fourierov transformacijski par

$$x(t) \Leftrightarrow X(f) \text{ ili } x(t) \Leftrightarrow X(\omega)$$

Neperiodični signali (II)

- ◆ amplitudni i fazni spektar

$$X(f) = |X(f)| e^{j\theta(f)}$$

- ◆ prikaz signala pomoću poznatog spektra

$$x(t) = \int_{-\infty}^{\infty} X(f) e^{j2\pi ft} df \text{ ili } x(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} X(\omega) e^{j\omega t} d\omega$$

- ◆ energija neperiodičnog signala (Parsevalov teorem)

$$E = \int_{-\infty}^{\infty} |x(t)|^2 dt = \int_{-\infty}^{\infty} |X(f)|^2 df = \frac{1}{2\pi} \int_{-\infty}^{\infty} |X(\omega)|^2 d\omega$$

Razredi neperiodičnih signala

- ◆ signali koji imaju konačnu ukupnu energiju, tj. $E < \infty$
 - takvi signali moraju imati srednju snagu jednaku nuli;
 - primjer: signal $x(t)$ čija je vrijednost jednaka 1 u intervalu $0 \leq t \leq 1$, a 0 izvan tog intervala
 - za takav signal vrijedi $E = 1$, $P = 0$;
- ◆ signali koji imaju konačnu srednju snagu veću od nule
 - ako je $P > 0$, tada je $E = \infty$;
- ◆ signali kojima su i srednja snaga i ukupna energija beskonačne
 - primjer: signal $x(t) = t$, $\forall t \in \mathbb{R}$.

Primjer: Diracov impuls

- ◆ spektar Diracovog impulsa

$$\Delta(f) = \int_{-\infty}^{\infty} \delta(t) e^{-j2\pi ft} dt = e^0 = 1$$

- ◆ promotrimo funkciju $x(t) = K\delta(t)$, $k \in \mathbb{C}$

$$X(f) = \int_{-\infty}^{\infty} K\delta(t) e^{-j2\pi ft} dt = K e^0 = K$$

Primjer: pravokutni impuls

- ◆ definicija pravokutnog impulsa

$$x(t) = \begin{cases} A & \text{za } 0 \leq |t| < \tau/2 \\ 0 & \text{za } |t| > \tau/2 \end{cases}, t \in \mathbb{R}$$

- ◆ spektar pravokutnog impulsa

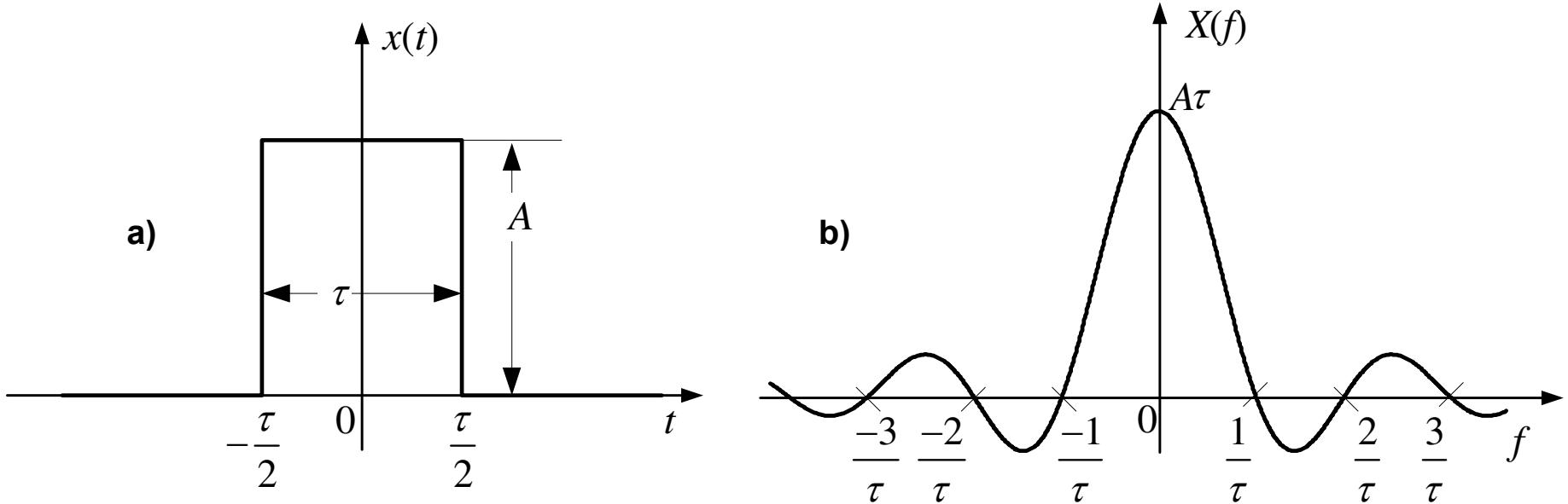
$$X(f) = \int_{-\infty}^{\infty} x(t) e^{-j2\pi ft} dt = A \int_{-\tau/2}^{\tau/2} e^{-j2\pi ft} dt = A\tau \frac{\sin(2\pi f\tau/2)}{2\pi f\tau/2}$$

- ◆ energija pravokutnog impulsa

$$E = \int_{-\infty}^{\infty} x^2(t) dt = \int_{-\infty}^{\infty} |X(f)|^2 df = A^2\tau$$

- ◆ srednja snaga pravokutnog impulsa jednaka nuli

Spektar pravokutnog impulsa



- ◆ spektar ima maksimalnu vrijednost za frekvenciju $f = 0 \text{ Hz}$ i iznosi $X(0) = A\tau$
- ◆ spektar prolazi kroz nulu u točkama $f_k = k/\tau$, $k \in \mathbb{Z}$.

Slučajni signali

- ◆ slučajni proces $X(t)$ je familija slučajnih varijabli $\{X(t), t \in \mathbb{D}\}$
- ◆ srednja vrijednost slučajnog procesa

$$\mu_x(t) = E[X(t)] = \int_{-\infty}^{\infty} x f_x(x, t) dx$$

- $f_x(x, t)$ je funkcija gustoće vjerojatnosti prvog reda slučajnog procesa $X(t)$
 - ◆ autokorelacijska funkcija i autokovarijanca slučajnog procesa $X(t)$
- $$R_x(t_1, t_2) = E[X(t_1) X(t_2)]$$

$$C_x(t_1, t_2) = E\{[X(t_1) - \mu_x(t_1)][X(t_2) - \mu_x(t_2)]\} = R_x(t_1, t_2) - E[X(t_1)]E[X(t_2)]$$

Stacionarni slučajni procesi

- ◆ ako je slučajni proces $X(t)$ stacionaran u širem smislu, tada zadovoljava sljedeće uvjete

$$E[X(t)] = \mu_X, \forall t \in \mathbb{D},$$

$$R_X(t_1, t_2) = K_X(|t_2 - t_1|) = K_X(\tau), \forall t_1, t_2 \in \mathbb{D},$$

- ◆ neka je autokorelacijska funkcija slučajnog procesa u kontinuiranom vremenu, $X(t)$, koji je stacionaran u širem smislu definirana kao

$$R_X(\tau) = E[X(t)X(t + \tau)]$$

- ◆ neka vrijedi: $R_X(-\tau) = R_X(\tau)$, $|R_X(\tau)| \leq R_X(0)$ i $R_X(0) = E[X^2(t)] \geq 0$

Spektralna gustoća snage slučajnog signala

$$S_X(f) = \int_{-\infty}^{\infty} R_X(\tau) e^{-j2\pi f\tau} d\tau \text{ [W/Hz]}$$

- ◆ ako je spektralna gustoća snage $S_X(f)$ poznata

$$R_X(\tau) = \int_{-\infty}^{\infty} S_X(f) e^{j2\pi f\tau} df$$

- ◆ srednja snaga P slučajnog signala modeliranog stacionarnim slučajnim procesom

$$P = E[X^2(t)] = R_X(0) = \int_{-\infty}^{\infty} S_X(f) df$$

Primjer: Gaussov bijeli šum

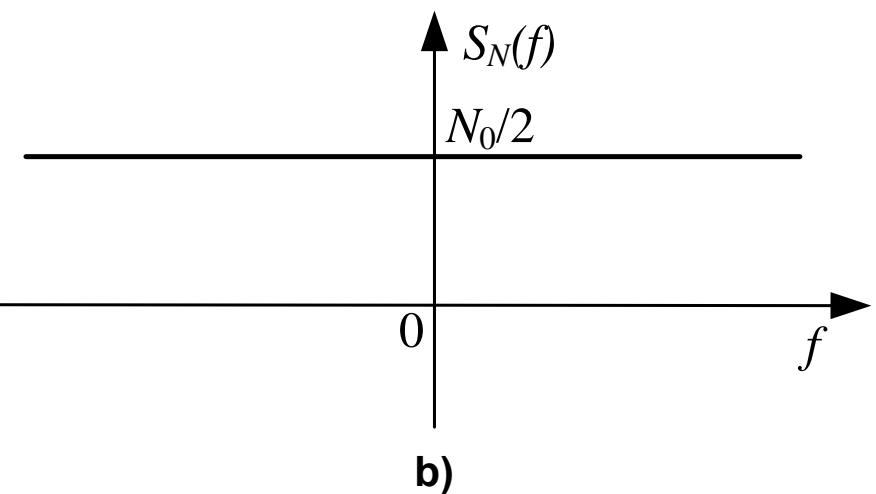
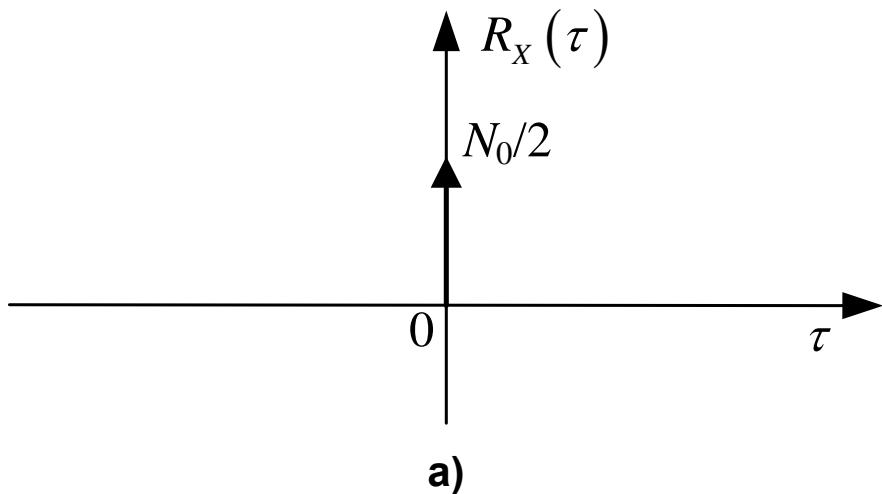
- ◆ slučajan proces $W(t)$ nazivamo **bijeli šum** ako su njegove vrijednosti, tj. slučajne varijable u trenucima t_i i t_j , $t_i \neq t_j$, međusobno potpuno nekorelirane
 - tada je autokovarijanca $C_X(t_i, t_j)$ jednaka nuli kad god vrijedi $t_i \neq t_j$
 - ako su slučajne varijable $W(t_i)$ i $W(t_j)$ istovremeno nekorelirane i neovisne, tada se radi o striktno bijelom šumu
 - bijeli šum u kontinuiranom vremenu je stacionarni slučajni proces u širem smislu, $W(t)$

Gaussov bijeli šum (II)

- ◆ srednja vrijednost bijelog šuma je jednaka nuli

$$R_W(\tau) = \sigma^2 \delta(\tau)$$

$$S_W(f) = \sigma^2 \int_{-\infty}^{\infty} \delta(t) e^{-j2\pi ft} dt = \sigma^2$$



Gaussov bijeli šum (III)

- ◆ slučajni proces nazivamo **bijeli Gaussov šum** ako su zadovoljena prethodno navedena svojstva bijelog šuma i ako su slučajne varijable slučajnog procesa Gaussove

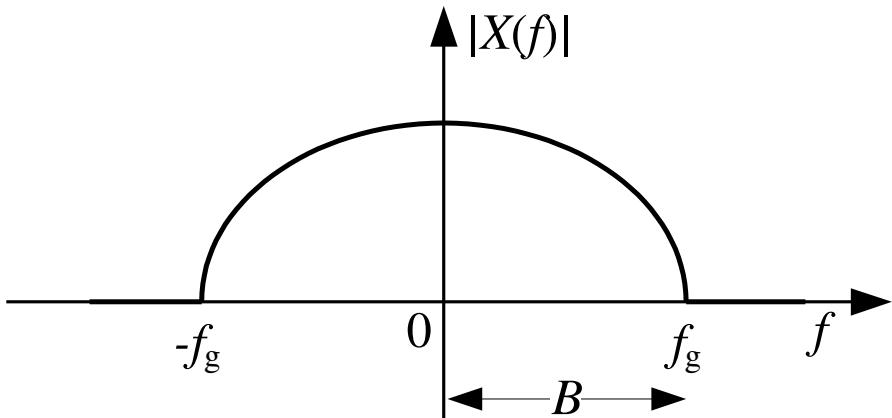
- za neku slučajnu varijablu X kažemo da ima Gaussovu razdiobu ako je njena funkcija gustoće vjerojatnosti definirana kao

$$f_X(x) = \frac{1}{\sigma_X \sqrt{2\pi}} e^{-(x-\mu_X)^2/(2\sigma_X^2)}$$

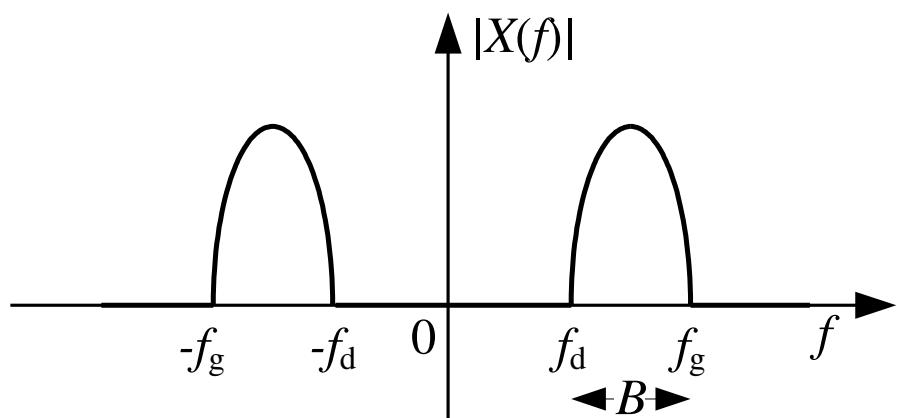
- varijanca ili disperzija $\text{var}(X) = E\{(X - E[X])^2\} = E[X^2] - \{E[X]\}^2 = \sigma_X^2$
- ako vrijedi $E[X] = 0$, tada je $\text{var}(X) = E[X^2] = \sigma_X^2$
 - tj. varijanca je jednaka srednjoj snazi signala na otporu 1 om

Širina spektra signala

- ◆ ovisno o pojasu frekvencija kojeg zauzima amplitudni spektar signala, signale dijelimo na
 - a) signale u osnovnom frekvencijskom pojasu
 - b) signale u pomaknutom frekvencijskom pojasu



a)



b)

- ◆ primjer: širina spektra pravokutnog signala
 - slajd 24

Komunikacijski kanal

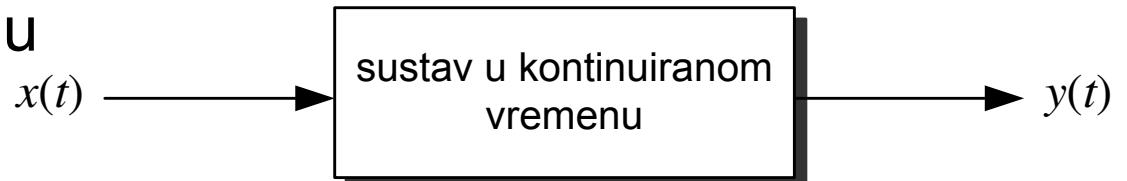
- ◆ komunikacijski kanal \approx prijenosni medij
- ◆ prijenosni mediji
 - žični
 - upredene parice
 - koaksijalni kabeli
 - vodovi energetske mreže
 - optičke niti
 - bežični
 - radijski, mikrovalni ili optički (ovisi o frekvenciji)
- ◆ primjer komunikacijskog kanala
 - telefonski kanal: od 300 do 3400 Hz
- ◆ po definiciji ITU-T-a kanal je sredstvo za **jednosmjerni** prijenos između predajnika i prijemnika

Klasifikacija komunikacijskih kanala

- ◆ linearni i nelinearni kanali
 - telefonski kanal je primjer linearog kanala
 - satelitski kanal je obično nelinearan (ali ne uvijek)
- ◆ neovisni o vremenu ili ovisni o vremenu
 - primjer vremenski nepromjenjivog kanala: optička nit
 - primjer vremenski promjenjivog kanala: radijski kanal u pokretnoj komunikacijskoj mreži
- ◆ ograničenja kanala
 - po širini prijenosnog pojasa (primjer: telefonski kanal) i
 - po raspoloživoj snazi predajnika (primjer: optički prijenos)

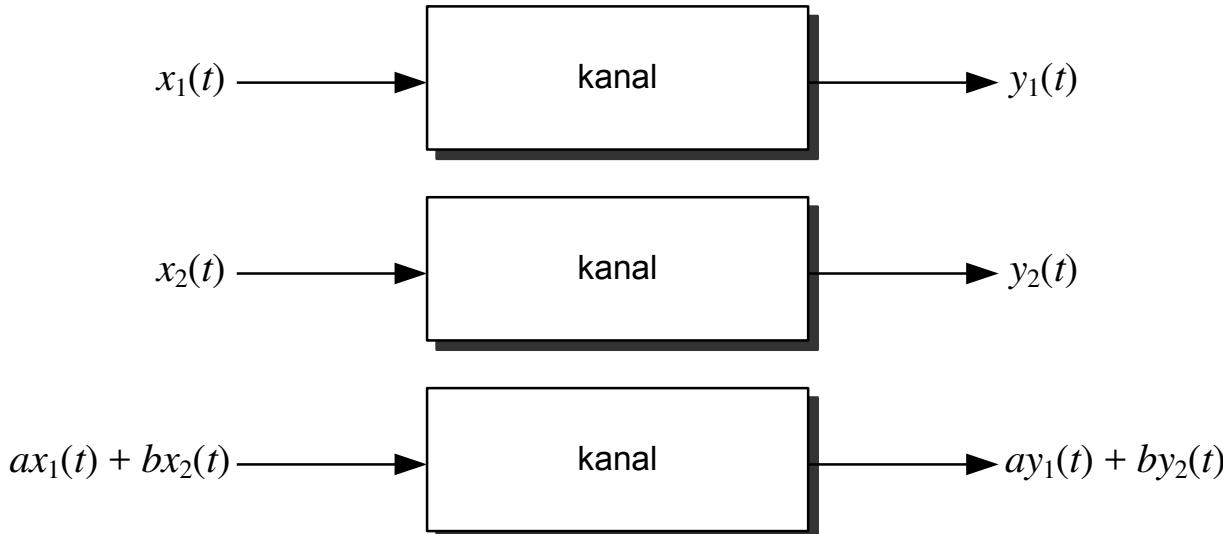
Matematički model kanala

- ◆ sustav definiramo kao preslikavanje skupa F (ulaz u sustav) u skup G (izlaz iz sustava)
 - u kontekstu komunikacija - sustav je proces uslijed kojeg su ulazni signali transformirani djelovanjem sustava u izlazne signale
 - **kontinuiran ili analogni** sustav - elementi skupova F i G funkcije kontinuirane varijable
 - **diskretan ili digitalni** sustav - elementi skupova F i G funkcije diskretnе varijable
 - kanal je moguće modelirati sustavom u **kontinuiranom** ili diskretnom vremenu

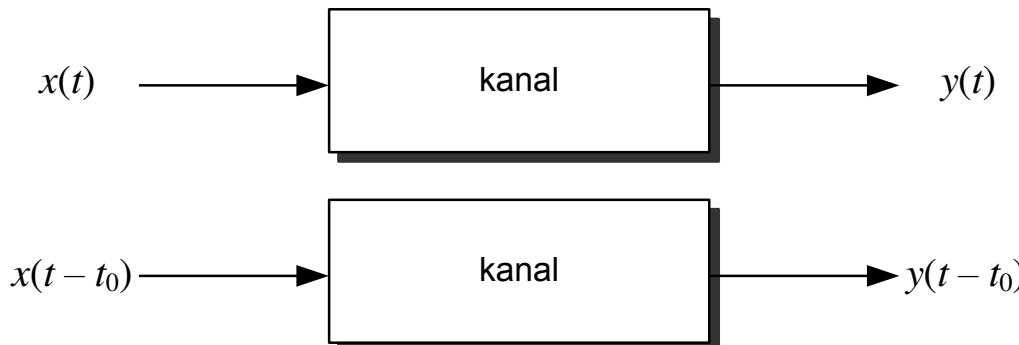


Linearni i vremenski nepromjenjivi kanali

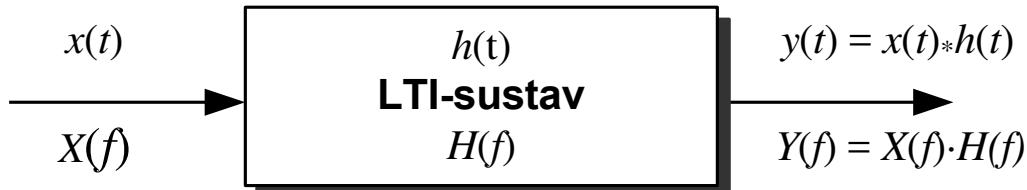
- ◆ kanal je linearan ako vrijedi:



- ◆ kanal je vremenski nepromjenjiv ako vrijedi:



Impulsni odziv i prijenosna funkcija kanala



- ◆ $h(t)$ – impulsni odziv sustava
 - odziv sustava na pobudu Diracovim impulsom

$$y(t) = \int_{-\infty}^{\infty} x(\tau)h(t-\tau)d\tau = \int_{-\infty}^{\infty} h(\tau)x(t-\tau)d\tau$$

$$y(t) = x(t) * h(t) = h(t) * x(t)$$

- ◆ $H(f)$ – impulsni odziv sustava

$$H(f) = \int_{-\infty}^{\infty} h(t)e^{-j2\pi ft}dt$$

Svojstva prijenosne funkcije

$$H(f) = |H(f)| e^{-j\theta(f)}$$

- ◆ amplitudni i fazni odziv $|H(-f)| = |H(f)|$,
 $\theta(-f) = -\theta(f)$.

$$h(t) = \int_{-\infty}^{\infty} H(f) e^{j2\pi ft} df$$

- ◆ impulsni odziv i prijenosna funkcija LTI-sustava čine Fourierov transformacijski par

$$h(t) \square H(f)$$

Slučajni signali i LTI-sustav

- ◆ pretpostavka: na ulazu LTI-sustava prijenosne funkcije $H(f)$ djeluje signal obilježja stacionarnog slučajnog procesa $X(t)$
 - srednja vrijednost μ_X
 - spektralna gustoća snage $S_X(f)$

$$\mu_Y = \mu_X H(0)$$

$$S_Y(f) = S_X(f) |H(f)|^2$$

- ◆ prolaskom kroz LTI-sustav, slučajni proces zadržava stacionarnost i na izlazu sustava

Širina prijenosnog pojasa kanala

- ◆ širina prijenosnog pojasa kanala je područje frekvencija u kojem komunikacijski kanal propušta signale sa svog ulaza na izlaz
- ◆ realni kanali prigušuju signale koje prenose
 - srednja snaga izlaznog signala uvijek je manja od srednje snage ulaznog signala
 - vrijedi i za energiju signala
- ◆ prigušenje kanala $A(f) = 1/|H(f)|$
- ◆ kanal djeluje i na fazu signala
 - faze frekvencijskih komponenti ulaznog signala se razlikuju od faza frekvencijskih komponenti izlaznog signala – **disperzija signala**

Širina prijenosnog pojasa kanala (II)

- ♦ na ulaz LTI-kanala dovedemo signal $x(t)$ čiji je spektar $X(f)$ definiran kao

$$X(f) = |X(f)| e^{j\varphi(f)}$$

- ♦ za spektar signala na izlazu LTI-kanala, $Y(f)$, vrijedi

$$Y(f) = |Y(f)| e^{j\vartheta(f)},$$

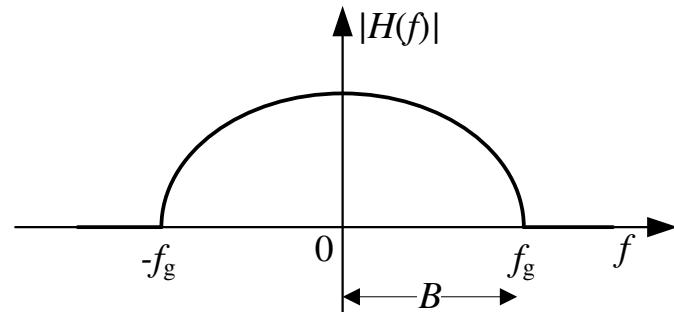
$$|Y(f)| = |X(f)| |H(f)|,$$

$$\vartheta(f) = \varphi(f) - \theta(f),$$

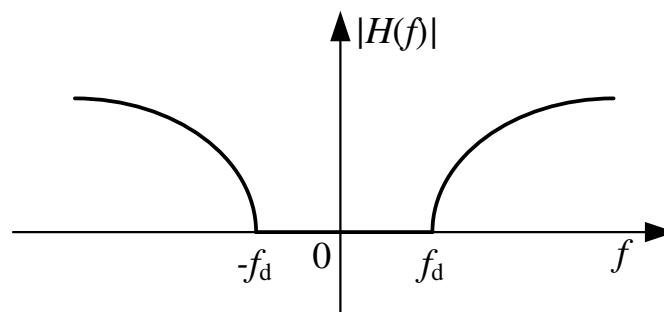
- ♦ kanal propušta one frekvencije na kojima je njegov amplitudni odziv veći od nule

Oblik amplitudnog odziva i vrste kanala

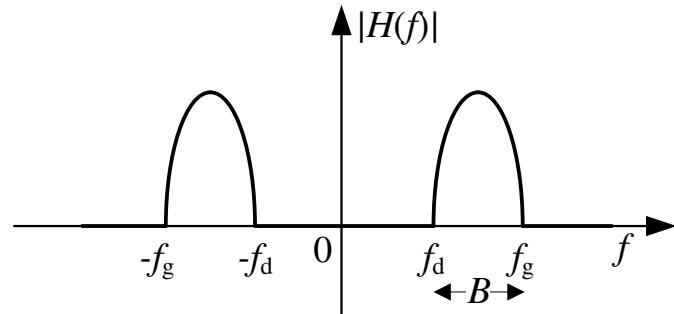
- ◆ a) niskopropusni kanal, b) visokopropusni kanal
- ◆ c) pojASNopropusni kanal, d) pojASna brana



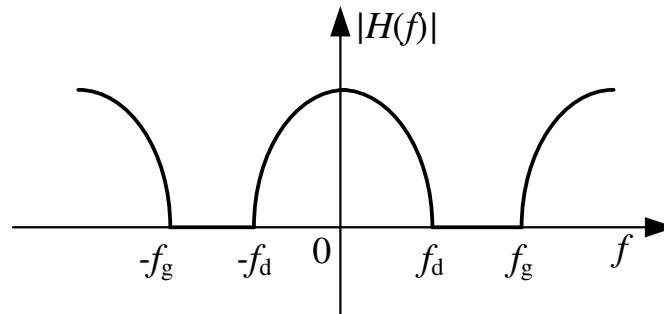
a)



b)

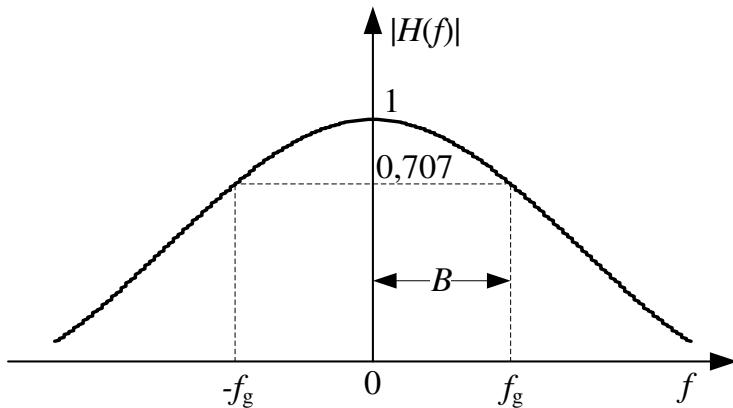
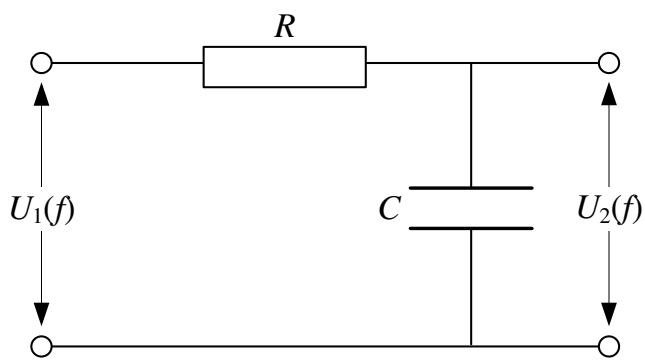


c)



d)

Primjer: RC-krug



- ◆ **a)** amplitudni odziv RC-kruga:
- ◆ u praksi se širina prijenosnog pojasa računa pomoću tzv. točaka prigušenja 3 decibela

$$\text{b)} |H(f)| = \left| \frac{U_2(f)}{U_1(f)} \right| = \frac{1}{\sqrt{1 + (2\pi f RC)^2}}$$

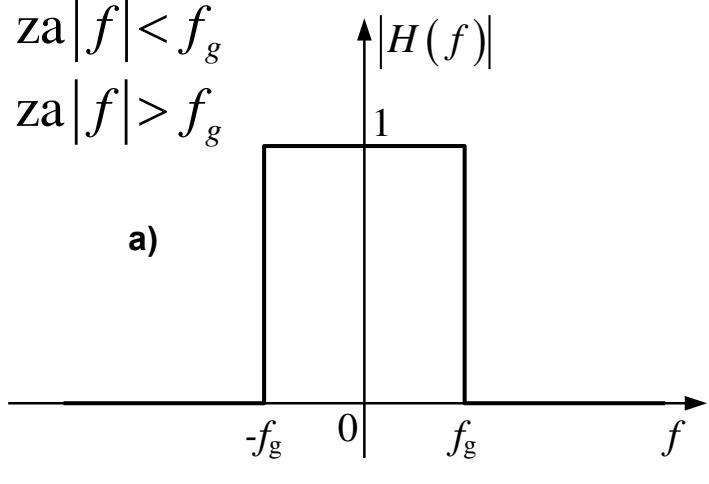
$$20 \log \left(\frac{|H(f)|}{|H(0)|} \right) = 20 \log(|H(f)|) - 20 \log(|H(0)|) = 20 \log(|H(f)|) [dB]$$

- ◆ $|H(0)| = 1$, pa vrijedi $20 \log(|H(0)|) = 0 \text{ dB}$
- ◆ na f na kojoj $|H(f)| \approx 0,707$ amplitudni je odziv za 3 dB slabiji od $|H(0)|$

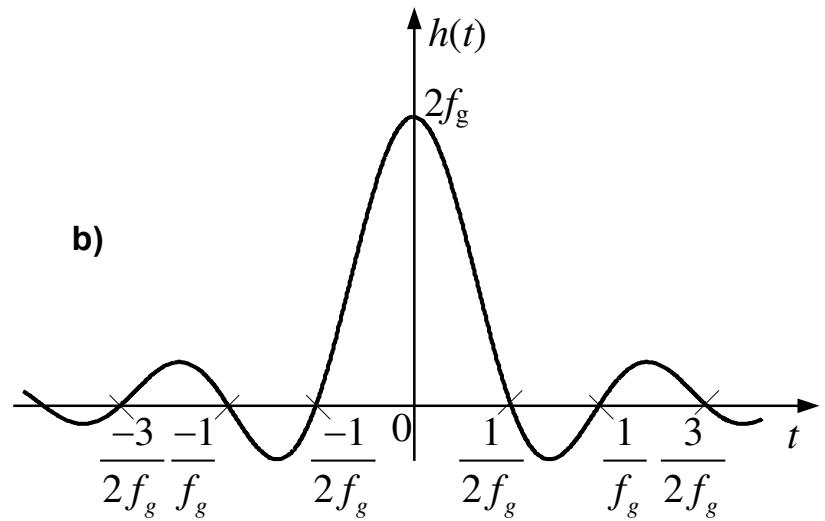
Idealan niskopropusni kanal

$$|H(f)| = \begin{cases} 1 & \text{za } |f| < f_g \\ 0 & \text{za } |f| > f_g \end{cases}$$

a)



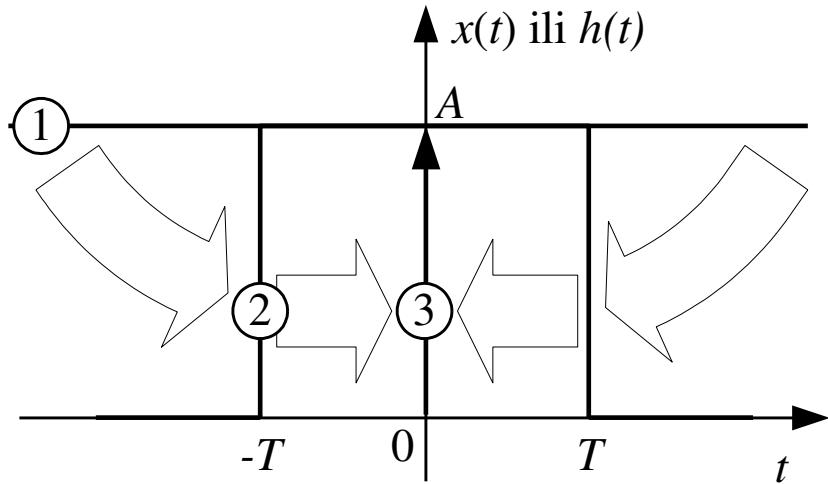
b)



$$h(t) = \int_{-\infty}^{\infty} H(f) e^{j2\pi ft} df = \int_{-f_g}^{f_g} e^{-j2\pi f\tau} e^{j2\pi ft} df = 2f_g \frac{\sin[2\pi f_g(t-\tau)]}{2\pi f_g(t-\tau)}$$

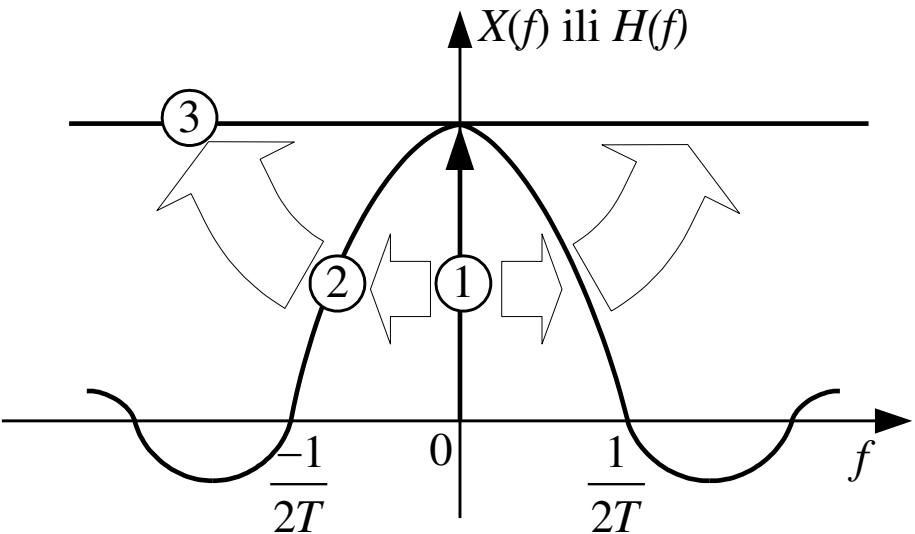
- ◆ svi su realni sustavi kauzalni, tj. odziv sustava ne može početi prije pobude
- ◆ u stvarnosti niskopropusni kanal ne može biti striktno ograničen na neki pojas frekvencija

Ograničavanje signala u vremenu



a)

$$x(t) = \begin{cases} A, & t \in [-T, T] \\ 0, & \text{inače} \end{cases}$$

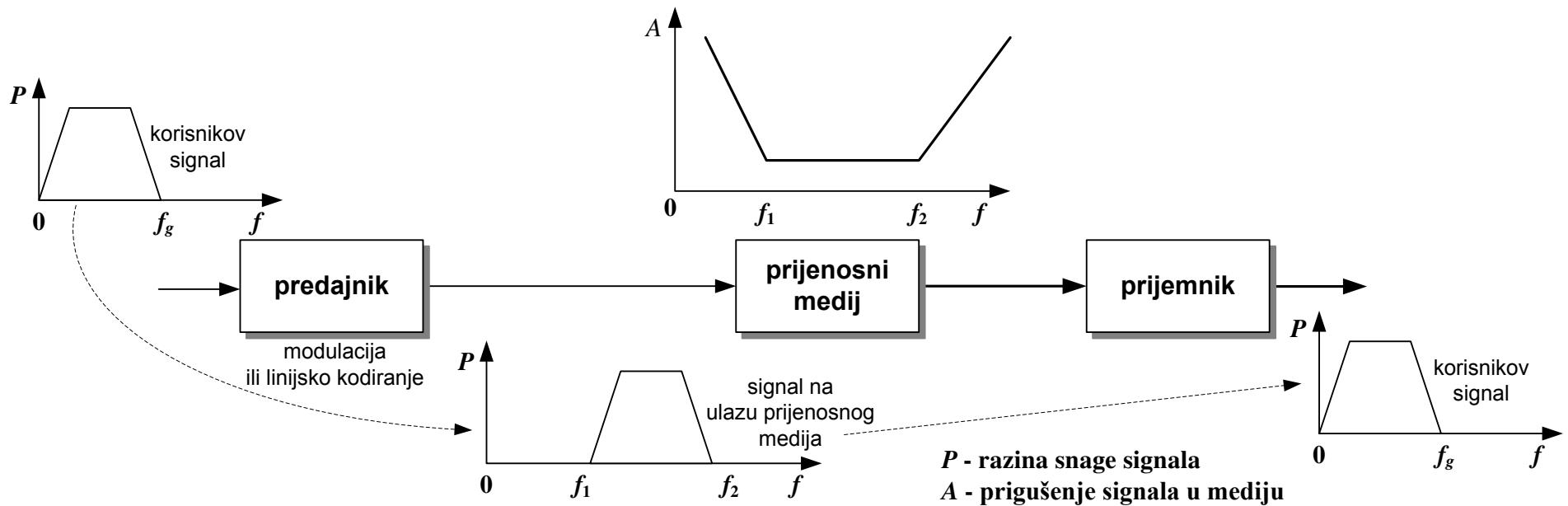


b)

- ◆ gornje razmatranje vrijedi i kad bi na apscisi na slici a) bila frekvencija, a na slici b) vrijeme

- ◆ kako bi u praksi mogli odrediti točnu širinu prijenosnog pojasa kanala, B , potrebno je definirati iznos prigušenja iznad kojeg smatramo da je prijenosna funkcija kanala praktično jednaka nuli
 - za niskopropusni kanal
 - potrebno je definirati frekvenciju f_g takvu da vrijedi
 - $|X(f)| \approx 0$ za $|f| > f_g$, $B = f_g$
 - za pojasnopropusni kanal
 - potrebno je definirati frekvencije f_d i f_g takve da vrijedi $|X(f)| > 0$ samo ako je $f_g > |f| > f_d$, $B = f_g - f_d$

Veza između širine prijenosnog pojasa kanala i širine spektra signala



- ◆ signal prije prijenosa kanalom oblikuje kako bi se svojim spektrom što bolje uklopio u prijenosni pojas kanala
 - modulacijski postupci
 - linijsko kodiranje

Uzorkovanje signala i kvantizacija uzoraka

Teorija informacije

Analogni prijenos signala

- ◆ ograničit ćemo se na skup striktno pojasno ograničenih signala, $\{x(t)\}$

$$X(f) = \int_{-\infty}^{\infty} x(t) e^{-j2\pi ft} dt = 0 \text{ za } |f| > f_g \neq 0$$

- ◆ pri prijenosu signala koji nije pojasno ograničen nužno je prenositi neprebrojiv skup kontinuiranih vrijednosti tog signala
 - sve vrijednosti signala $x(t)$, $\forall t \in [t_1, t_2]$, $t_1, t_2 \in \mathbb{R}$
 - $[t_1, t_2]$ je promatrani vremenski interval unutar kojeg se odvija prijenos signala $x(t)$
 - takav prijenos zovemo i **analogni prijenos**

- ◆ ako je signal pojasno ograničen, tada je unutar promatranog vremenskog intervala dovoljno prenositi prebrojiv skup njegovih vrijednosti
 - pojasno ograničen signal u kontinuiranom vremenu moguće je jednoznačno specifikirati pomoću njegovih vrijednosti uzetih u diskretnim trenucima
 - proces uzimanja uzoraka kontinuiranog signala u diskretnim trenucima naziva se **uzorkovanje**
 - uzorkovanje se provodi u predajniku, a rekonstrukcija izvornog signala u prijemniku
 - uzorkovanje je osnova digitalnog prijenosa signala
 - prvi korak u digitalizaciji analognog signala

- za striktno pojasno ograničene signale konačne energije
- ◆ Prvi dio teorema odnosi se na **predajnik**
- ◆ Pojasno ograničeni signal konačne energije, $x(t)$, $t \in \mathbb{R}$, čiji spektar ne sadrži frekvencijske komponente na frekvencijama iznad B Hz
 - $X(f) = 0$ za $|f| > B$
- ◆ u potpunosti je i na jednoznačan način opisan pomoću vrijednosti tog signala uzetih u diskretnim vremenskim trenucima $T_n = n/(2B)$
 - $n \in \mathbb{Z}$, B je gornja granična frekvencija signala

Teorem uzorkovanja u vremenskoj domeni (II)

- ◆ Drugi dio teorema odnosi se na **prijemnik**
- ◆ Pojasno ograničeni signal $x(t)$ konačne energije čiji spektar ne sadrži frekvencijske komponente na frekvencijama iznad B Hz
 - $X(f) = 0$ za $|f| > B$
- ◆ moguće je u potpunosti i na jednoznačan način rekonstruirati na temelju poznavanja njegovih uzoraka uzetih u diskretnim trenucima međusobno razmaknutim za $1/(2B)$ sekundi
 - frekvencija $2B$ uzorak/s – Nyquistova frekvencija
 - $(1/2B)$ [s] – Nyquistov interval uzorkovanja

Frekvencija uzorkovanja

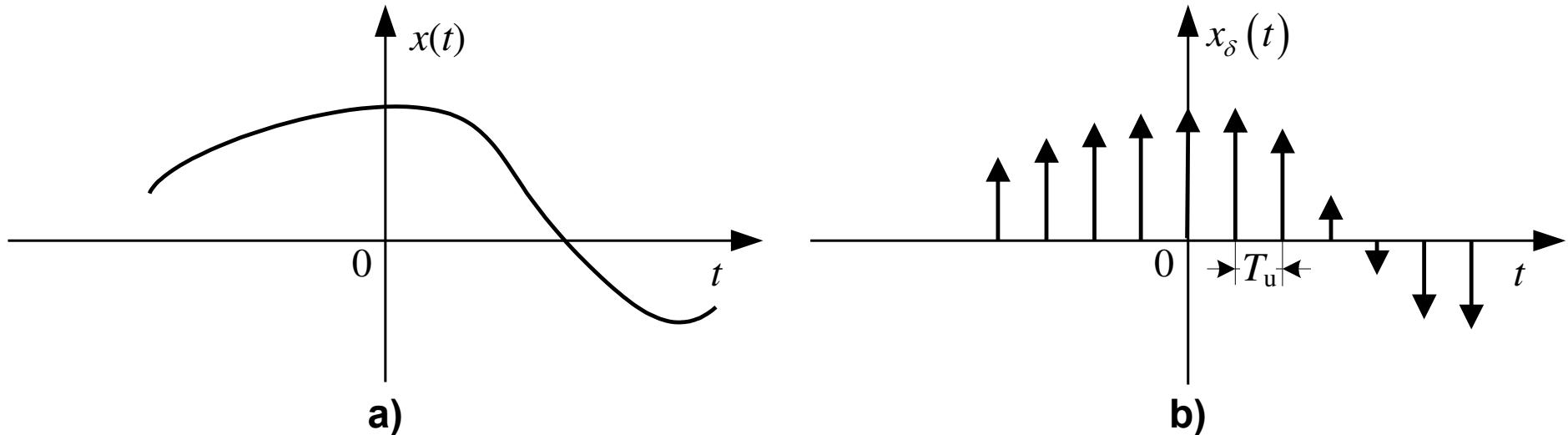
- ◆ osnovni problem uzorkovanja – odabir adekvatne frekvencije uzorkovanja f_u
 - slijed uzoraka mora jednoznačno definirati izvorni analogni signal
- ◆ poželjno je da f_u bude što manja
 - tada je i broj uzoraka manji
- ◆ što su uzorci gušći, to je slijed uzoraka sve bliži originalnom analognom signalu
 - međutim, potrebno prenositi više uzoraka
 - rezultat: neučinkovito korištenje mrežnih resursa

Dokaz teorema uzorkovanja

- ◆ promatrajmo proizvoljni signal $x(t)$ konačne energije, definiran za svaki $t \in \mathbb{R}$
- ◆ uzorci se uzimaju jednolikom frekvencijom
 - jedan uzorak svakih T_u sekundi
 - nastaje slijed uzoraka $\{x(nT_u)\}, n \in \mathbb{Z}$
 - T_u nazivamo period uzorkovanja
 - $f_u = 1/T_u$ je frekvencija uzorkovanja
 - idealno uzorkovanje: trajanje uzimanja uzorka $\Delta t \rightarrow 0$
- ◆ uzorkovani signal je slijed Diracovih impulsa

$$x_\delta(t) = \sum_{n=-\infty}^{\infty} x(nT_u) \delta(t - nT_u)$$

Proces uzorkovanja



- ◆ a) originalni kontinuirani signal
- ◆ b) njegova uzorkovana inačica
- ◆ Diracov impuls pomnožen koeficijentom $x(nT_u)$
 - aproksimiramo ga pravokutnim impulsom trajanja Δt i amplitude $x(nT_u)/\Delta t$

Svojstva Fourierove transformacije

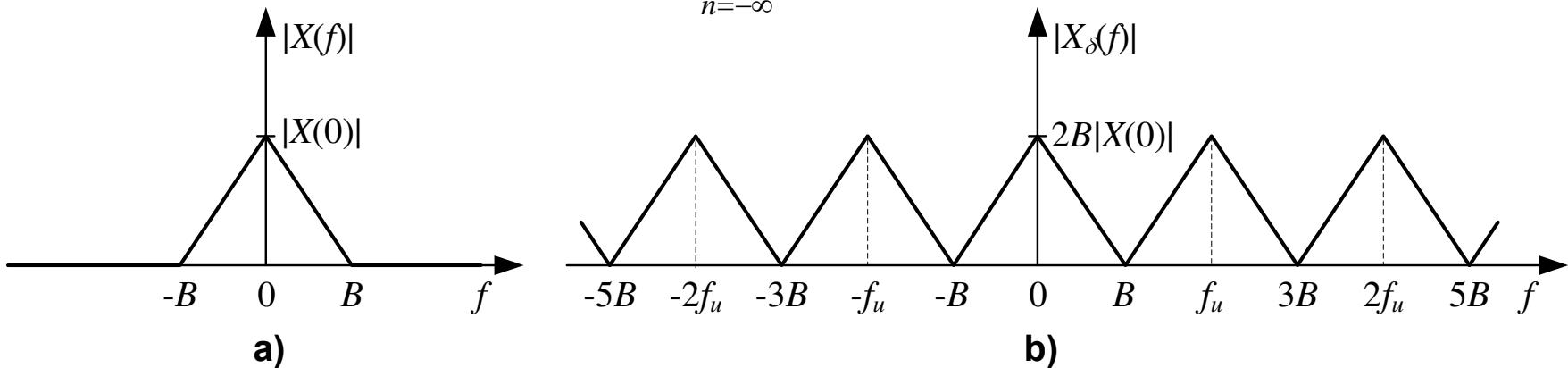
- ◆ prvo svojstvo: $\sum_{n=-\infty}^{\infty} \delta(t - nT_0) \Leftrightarrow \frac{1}{T_0} \sum_{n=-\infty}^{\infty} \delta\left(f - \frac{n}{T_0}\right)$
- ◆ drugo svojstvo: funkcija $x_\delta(t)$ je umnožak funkcije $x(t)$ i beskonačnog slijeda Diracovih delta impulsa $\delta(t - nT_u)$
 - ◆ spektar od $x(t)$ je $X(f)$
 - ◆ spektar od slijeda $\delta(t - nT_u)$ - prvo svojstvo
- ◆ $x_\delta(t)$ se preslikava u konvoluciju

$$\begin{aligned}
 X(f) * \left[f_u \sum_{n=-\infty}^{\infty} \delta(f - nf_u) \right] &= \int_{-\infty}^{\infty} X(\phi) f_u \sum_{n=-\infty}^{\infty} \delta(f - nf_u - \phi) d\phi = \\
 &= f_u \sum_{n=-\infty}^{\infty} \int_{-\infty}^{\infty} X(\phi) \delta(f - nf_u - \phi) d\phi = f_u \sum_{n=-\infty}^{\infty} X(f - nf_u),
 \end{aligned}$$

Dokaz teorema uzorkovanja (nastavak)

- ◆ proces jednolikog uzorkovanja kontinuiranog signala konačne energije rezultira periodičkim spektrom čiji je period jednak frekvenciji uzimanja uzoraka

$$x_\delta(t) \triangleq f_u \sum_{n=-\infty}^{\infty} X(f - nf_u)$$



- ◆ a) amplitudni spektar signala pojasno ograničenog na pojas frekvencija $(-B, B)$
- ◆ b) amplitudni spektar uzorkovane inačice tog signala uzorkovane frekvencijom $f_u = 1/(2B)$

Dokaz teorema uzorkovanja (nastavak)

- ◆ primijenimo Fourierovu transformaciju na obje strane izraza

$$x_\delta(t) = \sum_{n=-\infty}^{\infty} x(nT_u) \delta(t - nT_u)$$

- ◆ iskoristimo svojstvo: $\delta(t - nT_u) \square e^{-j2\pi nfT_u}$

- ◆ dobivamo: $X_\delta(f) = \sum_{n=-\infty}^{\infty} x(nT_u) e^{-j2\pi nfT_u}$

- ◆ gornji se izraz naziva diskretna Fourierova transformacija (DFT)
- ◆ $X_\delta(f)$ je spektar signala $x_\delta(t)$

Dokaz teorema uzorkovanja (nastavak)

- ◆ pretpostavimo
 - $X(f) = 0$ za $|f| > B$ i $T_u = 1/(2B)$
- ◆ spektar od $x_\delta(t)$ je dan izrazom
$$X_\delta(f) = \sum_{n=-\infty}^{\infty} x\left(\frac{n}{2B}\right) e^{-j\pi n f/B}$$
- ◆ koristeći izraz
$$x_\delta(t) = f_u \sum_{n=-\infty}^{\infty} X(f - nf_u)$$
- ◆ dobivamo
$$X_\delta(f) = f_u X(f) + f_u \sum_{\substack{m=-\infty \\ m \neq 0}}^{\infty} X(f - mf_u)$$
- ◆ ako vrijedi $X(f) = 0$ za $|f| > B$ i $f_u = 2B$
 - tada je
$$f_u \sum_{\substack{m=-\infty \\ m \neq 0}}^{\infty} X(f - mf_u) = 0$$

Dokaz teorema uzorkovanja (kraj)

- ◆ dakle, vrijedi:
$$X(f) = \begin{cases} \frac{1}{2B} X_\delta(f), & -B \leq f \leq B \\ 0, & \text{inače} \end{cases}$$
- ◆ uvrstimo u prethodni izraz
$$X_\delta(f) = \sum_{n=-\infty}^{\infty} x\left(\frac{n}{2B}\right) e^{-j\pi n f/B}$$
- ◆ pa dobivamo
$$X(f) = \begin{cases} \frac{1}{2B} \sum_{n=-\infty}^{\infty} x\left(\frac{n}{2B}\right) e^{-j\pi n f/B}, & -B \leq f \leq B \\ 0, & \text{inače} \end{cases}$$
- ◆ ako su $x[n/(2B)]$ poznate za svaki $n \in \mathbf{Z}$ tada je $X(f)$ jednoznačno određen DFT-om
- ◆ $x(t)$ je inverzna Fourierova transformacija od $X(f)$
- ◆ dakle, $x(t)$ jednoznačno određen uzorcima $x[n/(2B)]$

Rekonstrukcija signala

- ◆ Kako iz $\{x[n/(2B)]\}$ dobiti $x(t)$?

$$x(t) = \int_{-\infty}^{\infty} X(f) e^{j2\pi ft} df = \int_{-B}^{B} \frac{1}{2B} \sum_{n=-\infty}^{\infty} x\left(\frac{n}{2B}\right) e^{-j\pi nf/B} e^{j2\pi ft} df$$

$$x(t) = \sum_{n=-\infty}^{\infty} x\left(\frac{n}{2B}\right) \frac{1}{2B} \int_{-B}^{B} e^{j2\pi f[t-n/(2B)]} df$$

$$x(t) = \sum_{n=-\infty}^{\infty} x\left(\frac{n}{2B}\right) \frac{\sin(2\pi Bt - n\pi)}{2\pi Bt - n\pi}, \quad -\infty < t < \infty$$

$$x(t) = \sum_{n=-\infty}^{\infty} x\left(\frac{n}{2B}\right) \text{sinc}(2Bt - n), \quad -\infty < t < \infty$$

- ◆ $\text{sinc}(x) = \sin(\pi x)/(\pi x)$

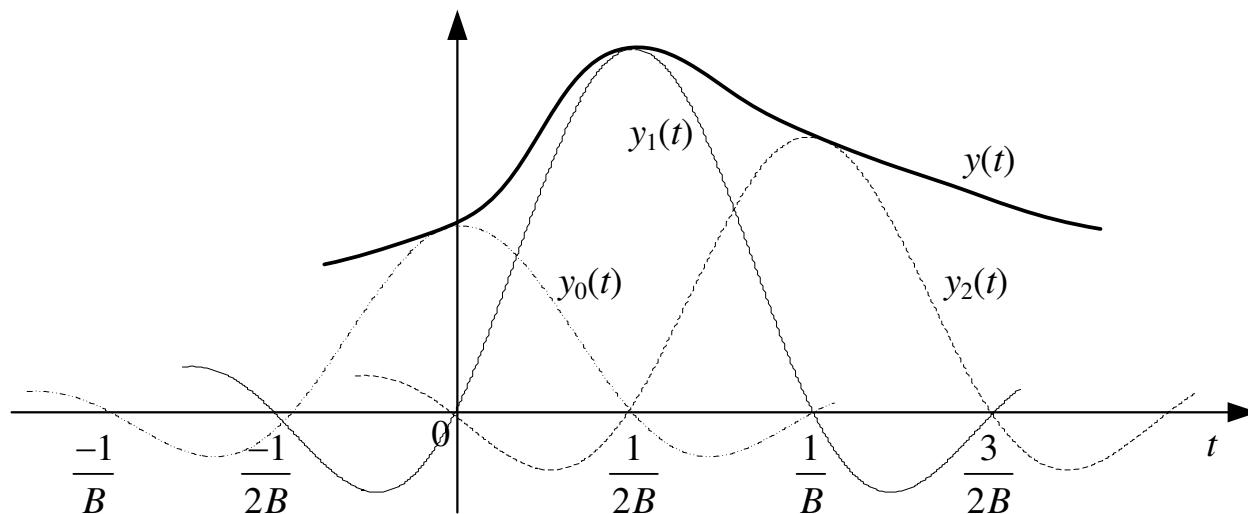
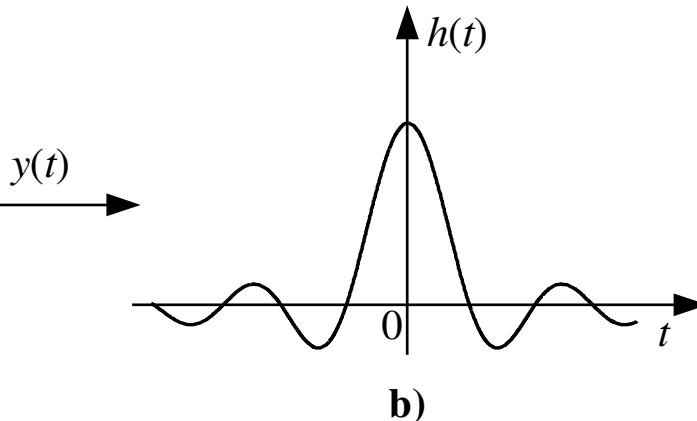
Rekonstrukcija signala (II)

$$\sum_{n=-\infty}^{\infty} x\left(\frac{n}{2B}\right) \delta\left(t - \frac{n}{2B}\right)$$

idealni niskopropusni
filtrar
 $H(f)$

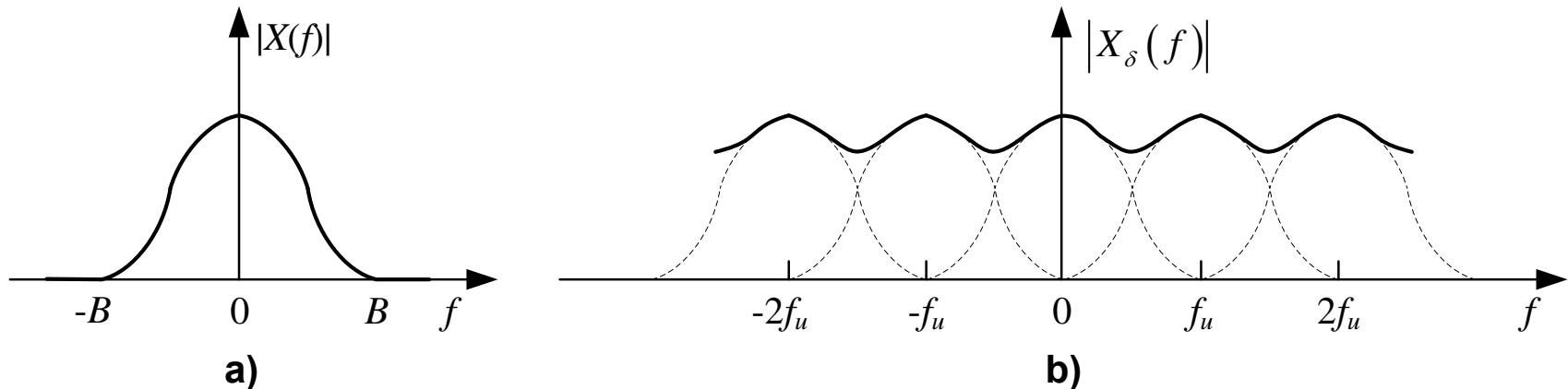
a)

$$H(f) = \begin{cases} 1, & 0 \leq |f| < B, \\ 0, & |f| > B. \end{cases}$$



Poduzorkovanje

- ◆ u praksi se uvijek odvija poduzorkovanje jer realni signali nisu striktno pojasno ograničeni
- ◆ ako je pak signal pojasno ograničen, a $f_u < 2B$



- ◆ rezultat poduzorkovanje je preklapanje spektara
 - ◆ iz izobličenog spektra nije moguće točno rekonstruirati izvorni signal

Kvantizacija uzorka

- ◆ nakon uzorkovanja kvantizacija je sljedeći korak u pretvorbi analognog u digitalni signal
 - analogni signal ima beskonačno mnogo mogućih vrijednosti amplitude
 - nije potrebno prenositi točne vrijednosti uzorka
 - ljudska osjetila mogu detektirati samo konačne razlike između razina signala
 - originalni analogni signal je moguće aproksimirati signalom sastavljenim od diskretnih amplitudnih razina
 - odabiru se iz konačnog skupa po kriteriju minimalne pogreške u razlici između stvarnih i aproksimiranih vrijednosti signala
 - osnova tzv. *impulsno-kodne modulacije* (PCM)

Matematički model kvantizacije

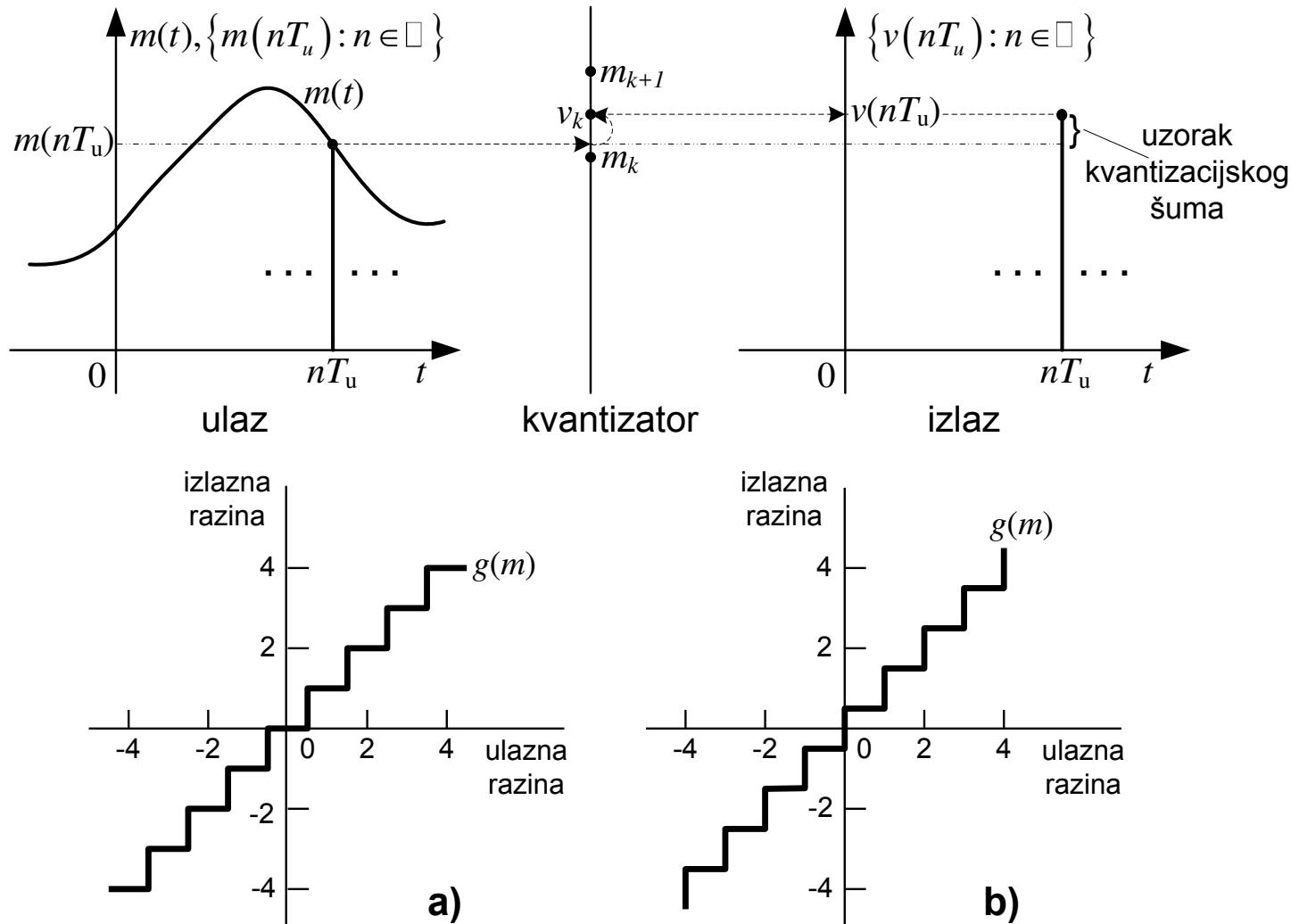
- ◆ amplitudni uzorci $m(nT_u)$ uzeti od $m(t)$ u nT_u , $n \in \mathbf{Z}$ se pretvaraju u diskretne amplitudne razine $v(nT_u)$
 - skupa mogućih razina je konačan
 - T_u je period uzorkovanja signala
 - pretpostavka: kvantizacijski proces je bezmemorijski i trenutan – ne koristi se u naprednijim postupcima
- ◆ neka je $m_k < m(nT_u) \leq m_k + 1$, $k = 1, 2, \dots, L$ i
- ◆ $m_k < v_k \leq m_k + 1$, $k = 1, 2, \dots, L$
 - L – broj stupnjeva amplitude kvantizatora (broj kvantizacijskih razina)
- ◆ tada kvantizator preslikava $m(nT_u) \rightarrow v_k$

Kvantizator



- ◆ m_k – razine odlučivanja ili pragovi odluke
- ◆ $v_k+1 - v_k$ je korak kvantizacije
- ◆ $v = g(m)$ – kvantizacijska karakteristika
- ◆ najčešći slučaj u praksi: $v_k = (m_k + m_{k+1})/2$
- ◆ ovisno o veličini koraka kvantizacija
 - jednolika kvantizacija – svi koraci jednaki
 - u suprotnom – nejednolika kvantizacija

Primjer kvantiziranja i jednolika kvantizacija



Kvantizacijski šum

- ◆ šum je razlika između $m(nT_u)$ i $v(nT_u)$
- ◆ ulaz u kvantizator kontinuirana slučajna varijabla M
- ◆ na izlazu kvantizatora diskretna slučajna varijabla V
 - vrijednosti od M i V su m , odnosno v , i vrijedi $v = g(m)$
- ◆ kvantizacijski šum – slučajna varijabla Q
 - vrijedi: $Q = M - V$, odnosno $q = m - v$
 - ako je $E[M] = 0$ i kvantizacijska karakteristika simetrična
 - vrijedi: $E[V] = E[Q] = 0$
- ◆ cilj: odrediti standardnu devijaciju kvantizacijskog šuma

Varijanca kvantizacijskog šuma

- ◆ prepostavka:
 - amplitude ulaznog signala mogu poprimati kontinuirane vrijednosti iz intervala $(-m_{\max}, m_{\max})$
 - ako su amplitude ulaznog signala izvan tog intervala, nastupa preopterećenje kvantizatora i izobličenje
- ◆ korak kvantizacije $\Delta = 2m_{\max}/L$
- ◆ dakle, kvantizacijski šum je ograničen: $-\Delta/2 \leq q \leq \Delta/2$
 - ako je korak kvantizacije dovoljno mali
 - opravdano je prepostaviti da slučajna varijabla Q ima jednoliku razdiobu

$$f_Q(q) = \begin{cases} \frac{1}{\Delta}, & -\frac{\Delta}{2} < q \leq \frac{\Delta}{2}, \\ 0, & \text{inače.} \end{cases}$$

Varijanca kvantizacijskog šuma (II)

- ◆ s obzirom da je $E[Q] = 0$, vrijedi:

$$\text{var}(Q) = \sigma_Q^2 = E[Q^2] = \int_{-\Delta/2}^{\Delta/2} q^2 f_Q(q) dq$$

$$\text{var}(Q) = \sigma_Q^2 = \frac{1}{\Delta} \int_{-\Delta/2}^{\Delta/2} q^2 dq = \frac{\Delta^2}{12}$$

- ◆ uzorci se prije prijenosa kodiraju binarnim kodom i prenose binarnim signalom (dvije razine)
- ◆ r označava broj bita za opis svakog uzorka v_k
 - mora vrijediti: $L = 2^r$
 - $L > 2^r$ – ne možemo jednoznačno opisati sve uzorke
 - $L < 2^r$ – nepotrebna zalihost u kodiranju

Varijanca kvantizacijskog šuma (III)

- ◆ nadalje, $\Delta = 2m_{\max}/2^r$

$$\sigma_Q^2 = \frac{1}{3} m_{\max}^2 2^{-2r}$$

- ◆ neka je S srednja signala $m(t)$
- ◆ tada vrijedi:

$$(S/N) = \frac{S}{\sigma_Q^2} = \left(\frac{3S}{m_{\max}^2} \right) 2^{2r}$$

Primjer: kvantizacija sinusnog signala

- ◆ sinusni signal amplitude A_m
 - koristi sve razine za rekonstrukciju signala
 - srednja snaga signala na otporniku otpora 1 om $P = \frac{A_m^2}{2}$
 - raspon amplituda na ulazu kvantizatora iznosi $2A_m$
 - dakle, $m_{\max} = A_m$

$$\sigma_Q^2 = \frac{1}{3} A_m^2 2^{-2r}$$

$$(S/N) = \frac{A_m^2 / 2}{A_m^2 2^{-2r} / 3} = \frac{3}{2} (2^{2r})$$

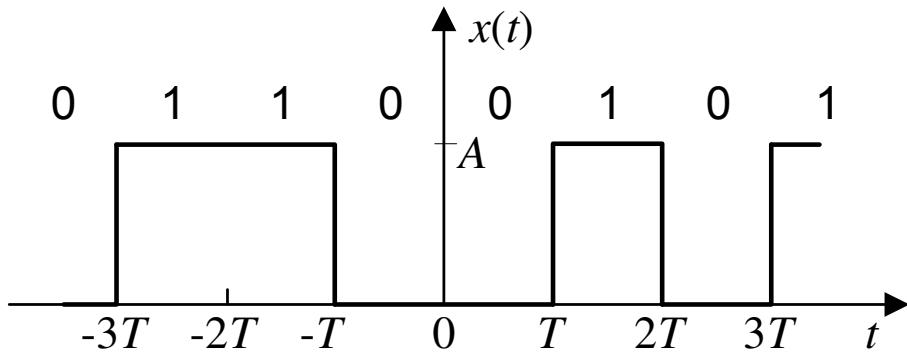
$$10 \log_{10} (S/N) = 1,76 + 6,02 \cdot r \text{ [dB]}$$

L	r	S/N [dB]
32	5	31,8
64	6	37,8
128	7	43,8
256	8	49,8

Kodiranje kvantiziranih uzoraka

- ◆ kôd – pravilo dodjele sljedova simbola diskretnim kvantizacijskim razinama
 - kodna riječ – slijed simbola koji se dodjeljuje nekoj kvantizacijskoj razini
 - ako se prilikom kodiranja uzorka koriste binarni simboli, tada se radi o binarnom kodu
 - pravilo kodiranja ovisi o vrsti komunikacijskog sustava
 - najčešće je određeno odgovarajućim preporukama, odnosno normama
 - primjer: na izlazu kvantizatora 4 kvantizacijske razine ($L = 4$): $-3U, -U, U$ i $3U$, U – napon u voltima
 - nužno koristiti 2 bita po svakoj razini
 - $-3U \rightarrow 11, -U \rightarrow 10, U \rightarrow 00$ i $3U \rightarrow 01$

Unipolarni binarni signal



- ◆ uobičajeno pravilo je da se
 - binarnoj nuli pridjeljuje razina 0 [V]
 - binarnoj jedinici razina A [V]
- ◆ T – trajanje binarnih signalnih elemenata
 - ili trajanje bita, izraženo u sekundama
 - prijenosna brzina $R = 1/T$ [bit/s]

Kapacitet kanala u kontinuiranom vremenu

Teorija informacije

Entropija u kontinuiranim kanalima

- ◆ definicija entropije jednodimenzionalne slučajne varijable X s kontinuiranom razdiobom:

$$H(X) = E[-\log f_X(X)] = - \int_{-\infty}^{\infty} f_X(x) \log f_X(x) dx$$

- ◆ diferencijalna entropija može biti i negativna
- ◆ primjer: X ima jednoliku razdiobu na intervalu $(0, a)$

$$f_X(x) = \begin{cases} \frac{1}{a}, & 0 < x < a, \\ 0, & \text{inače.} \end{cases} \quad H(X) = \int_0^a \frac{1}{a} \log(a) dx = \log(a)$$

- ◆ ako je $a < 1$, tada je $\log(a) < 0$, pa je $H(X)$ negativna

Informacijske mjere kontinuiranog sustava

- ◆ ulaz u kanala – slučajna varijabla X
 - kontinuirana funkcija gustoće vjerojatnosti $f_1(x)$
- ◆ izlaz iz kanala – slučajna varijabla Y
 - kontinuirana funkcije gustoće vjerojatnosti $f_2(y)$
- ◆ združena funkcija gustoće vjerojatnosti od X i Y
 - kontinuirana funkcija $f(x,y)$

$$f_1(x) = \int_{-\infty}^{\infty} f(x, y) dy,$$

$$f_2(y) = \int_{-\infty}^{\infty} f(x, y) dx.$$

Informacijske mjere kontinuiranog sustava (II)

entropija na ulazu kanala: $H(X) = E[-\log f_1(X)] = - \int_{-\infty}^{\infty} f_1(x) \log f_1(x) dx$

,

entropija na izlazu kanala: $H(Y) = E[-\log f_2(Y)] = - \int_{-\infty}^{\infty} f_2(y) \log f_2(y) dy$

ekvivokacija: $H(X|Y) = E[-\log f_y(X|Y)] = - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) \log \frac{f(x, y)}{f_2(y)} dx dy$

entropija šuma: $H(Y|X) = E[-\log f_x(Y|X)] = - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) \log \frac{f(x, y)}{f_1(x)} dx dy$

zdržena entropija: $H(X, Y) = E[-\log f(X, Y)] = - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) \log f(x, y) dx dy$

Transinformacija u kontinuiranom kanalu

- ♦ transinformacija je očekivanje slučajne varijable / definirane funkcijom

$$\log \left(\frac{f(X, Y)}{f_1(X) f_2(Y)} \right)$$

$$E[I] = I(X; Y) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) \log \frac{f(x, y)}{f_1(x) f_2(y)} dx dy$$

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

- ♦ $I(X; Y) = I(Y; X)$
- ♦ $I(X; Y) \geq 0$
- ♦ $I(X; Y) = 0$ ako su X i Y međusobno neovisne slučajne varijable

Entropija slučajnog vektora

- ◆ neka je \mathbf{X} slučajni vektor sastavljen od n kontinuiranih slučajnih varijabli $X_k, k = 1, \dots, n$
- ◆ diferencijalna entropija dana izrazom

$$H(X_1, \dots, X_n) = E\left[-\log\left\{f_{\mathbf{X}}(X_1, \dots, X_n)\right\}\right] = -\int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} f_{\mathbf{X}}(x_1, \dots, x_n) \log[f_{\mathbf{X}}(x_1, \dots, x_n)] dx_1 \cdots dx_n$$

$$H(\mathbf{X}) = E\left[-\log\left\{f(\mathbf{X})\right\}\right] = -\int_{-\infty}^{\infty} f_{\mathbf{X}}(\mathbf{x}) \log[f_{\mathbf{X}}(\mathbf{x})] d\mathbf{x}$$

- ◆ $f_{\mathbf{X}}(\mathbf{x})$ zdržena funkcija gustoće vjerojatnosti slučajnog vektora \mathbf{X}

Određivanje maksimuma entropije kontinuirane slučajne varijable

- ◆ Maksimum $H(X)$ za DSV nastupa kad su svi elementarni događaji jednako vjerojatni
 - ako je kontinuirana slučajna varijabla ograničena na neki konačan interval, tada ima smisla razmatrati koja gustoća vjerojatnosti daje maksimalnu vrijednost entropije
- ◆ od svih jednodimenzionalnih razdioba s unaprijed zadanim standardnom devijacijom najveću entropiju pruža Gaussova (normalna) razdioba

$$f_1(x) = \frac{1}{\sigma_X \sqrt{2\pi}} e^{-x^2/(2\sigma^2)}$$

$$H(X) = \ln(\sigma_X \sqrt{2\pi e})$$

- ◆ općenito gledano, proračun kapaciteta kontinuiranog kanala je vrlo složen problem
 - ne postoji općenita metoda za određivanje kapaciteta u svim okolnostima
 - jednostavno je proračunati kapacitet kanala s aditivnim šumom
- ◆ neka X opisuje izlaz predajnika, a Y ulaz u prijemnik
 - X i Y su kontinuirane slučajne varijable
 - uvjetna funkcija gustoće vjerojatnosti $f_x(y|x) = \frac{f(x,y)}{f_1(x)}$

Kapacitet kanala s aditivnim šumom

- ◆ pretpostavimo da je šum u kanalu aditivan i neovisan o X
- ◆ $Y = X + Z$ i $f_x(y|x) = f_x(z + x|x) = \phi(z)$
 - Z je slučajna varijabla koja opisuje šum
 - funkcija gustoće vjerojatnosti šuma je $\phi(z)$
 - $f_x(z + x|x)$ ovisi samo o z
 - iz toga proizlazi jednakost $H(Y|X) = H(X + Z|X) = H(Z)$
- ◆ dakle, za transinformaciju vrijedi:

$$I(X;Y) = H(Y) - H(Y|X) = H(Y) - H(Z) = H(Y) + \int_{-\infty}^{\infty} \phi(z) \log[\phi(z)] dz$$

- ◆ kapacitet određujemo pronalaženjem maksimuma transinformacije $I(X;Y)$ u ovisnosti o funkciji $f_1(x)$ i pod određenim ograničenjima

Kapacitet kanala s aditivnim šumom (II)

- ◆ problem:
 - određivanje **kapaciteta kanala**
 - u prisustvu **Gaussovog aditivnog šuma**
 - te uz zadanu **srednju snagu signala na izlazu predajnika i**
 - **srednju snagu šuma**
- ◆ ograničenja bitna za proračun kapaciteta
 - pretpostavka: šum ima Gaussovu razdiobu
 - srednja vrijednost jednaka nuli i
 - srednja snaga jednaka σ_z^2

$$\int_{-\infty}^{\infty} \frac{1}{\sigma_z \sqrt{2\pi}} e^{-z^2/(2\sigma_z^2)} dz = 1 \quad \int_{-\infty}^{\infty} f_1(x) dx = 1 \quad \int_{-\infty}^{\infty} x f_1(x) dx = 0 \quad \int_{-\infty}^{\infty} x^2 f_1(x) dx = \sigma_x^2$$

Kapacitet kanala s aditivnim šumom (III)

- ◆ transinformacija u kanalu

$$I(X;Y) = H(Y) - H(Z) = H(Y) - \frac{1}{2} \ln(2\pi e \sigma_z^2)$$

- ◆ vrijedi: $\max I(X;Y) = \max [H(Y) - H(Z)]$
 - ◆ kapacitet kanala je moguće izračunati maksimizacijom entropije $H(Y)$ i
 - ◆ uz ranije navedena ograničenja
- ◆ nadalje, $E[Y] = E[X + Z] = E[X] + E[Z] = 0$
- ◆ $E[Y^2] = E[(X + Z)^2] = E[X^2] + 2E[X]E[Z] + E[Z^2]$
- ◆ $E[X]E[Z] = 0$ pa vrijedi $E[Y^2] = \sigma_x^2 + \sigma_z^2 = \text{konst.}$

Kapacitet kanala s aditivnim šumom (IV)

- ◆ dakle, problem pronalaženja kapaciteta kanala svodi se na pronalaženje
 - funkcije gustoće vjerojatnosti koja daje
 - srednju vrijednost 0 i
 - standardnu devijaciju $\sigma_x^2 + \sigma_z^2$
 - rezultat od prije: za takvu slučajnu varijablu najveću entropiju daje **Gaussova funkcija gustoće vjerojatnosti**
- ◆ maksimalna entropija na ulazu u prijemnik

$$H(Y) = \ln \left[\sqrt{2\pi e (\sigma_x^2 + \sigma_z^2)} \right] \text{ [nat/simbol]}$$

$$C_1 = \max I(X;Y) = \max \left[H(Y) - \frac{1}{2} \ln (2\pi e \sigma_z^2) \right] = \frac{1}{2} \ln \left(\frac{\sigma_x^2 + \sigma_z^2}{\sigma_z^2} \right) \text{ [nat/simbol]}$$

Kapacitet kanala s aditivnim šumom (V)

- ◆ ako pretpostavimo da vrijedi $\sigma_x^2 = S$ i $\sigma_z^2 = N$
 - S je srednja snaga signala na izlazu predajnika
 - N je srednja snaga šuma u kanalu

$$C_1 = \frac{1}{2} \ln \left(1 + \frac{S}{N} \right) [\text{nat/simbol}]$$

$$C_1 = \frac{1}{2} \log_2 \left(1 + \frac{S}{N} \right) [\text{bit/simbol}]$$

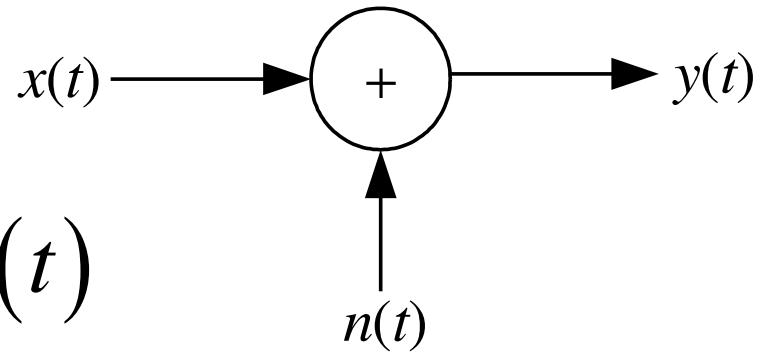
- ◆ **rezime:** u kanalu u kojem djeluje aditivni Gaussov šum, a srednja snaga signala na izlazu predajnika i srednja snaga šuma su ograničene, signal na ulazu kanala i signal na izlazu kanala moraju imati Gaussovu razdiobu kako bi brzina prijenosa informacije takvim kanalom bila maksimalna, tj. jednaka kapacitetu tog kanala

Informacijski kapacitet pojasno ograničenog kanala

- ◆ problem egzaktnog opisa kontinuiranih signala
 - vrijednost slučajnog kontinuiranog signala $x(t)$ u bilo kojem trenutku je nepredvidiva
 - u bilo kojem trenutku t_k , $x(t_k)$ je slučajna varijabla
 - potrebno je poznavanje statističkih svojstava praktički beskonačnog broja slučajnih varijabli
- ◆ rješenje: prikazati kontinuirani signal diskretnim signalom
 - u prelasku s kontinuiranog prikaza signala na diskretni uzorkovanje ima glavnu ulogu
 - promatrani skup signala svodi se na pojasno ograničene signale

AWGN-kanal

- ◆ model AWGN-kanala



- ◆ pravilo u praksi za korištenje bijelog šuma u analizi realnih sustava
 - ◆ sve dok je širina frekvencijskog pojasa šuma na ulazu sustava znatno veća nego širina prijenosnog pojasa sustava
 - ◆ šum možemo modelirati kao bijeli šum.

Teorem o informacijskom kapacitetu AWGN-kanala

- ◆ ako signale $x(t)$ i $y(t)$ uzorkujemo sukladno teoremu uzorkovanja,
 - dobivamo diskretne signale koje je moguće prikazati n -dimenzionalnim slučajnim vektorima \mathbf{X} , odnosno \mathbf{Y}

$$\mathbf{X} = [X_1, X_2, \dots, X_n] \text{ i } \mathbf{Y} = [Y_1, Y_2, \dots, Y_n]$$

$$E[X_k] = 0, \\ E[X_k^2] = \sigma_{xk}^2.$$

$$\mathbf{Z} = [Z_1, Z_2, \dots, Z_n] \quad E[Z_k] = 0, \\ E[Z_k^2] = \sigma_{zk}^2, \quad C_Z(Z_i, Z_j) = 0, \quad i \neq j$$

$$\mathbf{Y} = \mathbf{X} + \mathbf{Z}$$

Transinformacija u AWGN-kanalu

$$I(\mathbf{X}; \mathbf{Y}) = H(\mathbf{Y}) - H(\mathbf{Y} | \mathbf{X})$$

$$f_x(\mathbf{y} | \mathbf{x}) = f_x(\mathbf{x} + \mathbf{z} | \mathbf{x}) = \phi(\mathbf{z}) \quad \phi(\mathbf{z}) = \prod_{k=1}^n \left[\frac{1}{\sigma_{z_k} \sqrt{2\pi}} e^{-z_k^2 / (2\sigma_{z_k}^2)} \right]$$

- ◆ komponente šuma međusobno neovisne
- ◆ entropija šuma jednaka je zbroju entropija njegovih pojedinačnih komponenata

$$H(\mathbf{Y} | \mathbf{X}) = H(\mathbf{Z}) = - \int_{-\infty}^{\infty} \phi(\mathbf{z}) \log[\phi(\mathbf{z})] d\mathbf{z} = \sum_{k=1}^n \log(\sigma_{z_k} \sqrt{2\pi e})$$

$$I(\mathbf{X}; \mathbf{Y}) = H(\mathbf{Y}) - H(\mathbf{Y} | \mathbf{X}) = H(\mathbf{Y}) - H(\mathbf{Z}) = H(\mathbf{Y}) - \sum_{k=1}^n \log(\sigma_{z_k} \sqrt{2\pi e})$$

Određivanje maksimalne vrijednosti transinformacije

- ◆ svodi se na maksimizaciju entropije $H(\mathbf{Y})$
- ◆ $Y_k = X_k + Z_k$
 - na svaku komponentu slučajnog vektora \mathbf{X} djeluje neovisna Gaussova smetnja

$$\sigma_{y_k}^2 = \sigma_{x_k}^2 + \sigma_{z_k}^2, \quad k = 1, 2, \dots, n$$

- ◆ entropija $H(\mathbf{Y})$ će biti maksimalna kad su ispunjeni sljedeći uvjeti
 - ◆ sve komponente slučajnog vektora \mathbf{Y} su međusobno neovisne slučajne varijable
 - ◆ svaka komponenta ima najveću entropiju pod zadanim uvjetima

Određivanje maksimalne vrijednosti transinformacije (II)

$$I_{\max}(\mathbf{X}; \mathbf{Y}) = \sum_{k=1}^n \log\left(\sigma_{y_k} \sqrt{2\pi e}\right) - \sum_{k=1}^n \log\left(\sigma_{z_k} \sqrt{2\pi e}\right) = \sum_{k=1}^n \log\left(\frac{\sigma_{y_k}}{\sigma_{z_k}}\right) = \sum_{k=1}^n \frac{1}{2} \log\left(1 + \frac{\sigma_{x_k}^2}{\sigma_{z_k}^2}\right)$$

- ◆ pretpostavka: $\sigma_{x_k} = \sigma_x$, $k = 1, 2, \dots, n$
 $\sigma_{z_k} = \sigma_z$,

$$I_{\max}(\mathbf{X}; \mathbf{Y}) = \sum_{k=1}^n \frac{1}{2} \log\left(1 + \frac{\sigma_x^2}{\sigma_z^2}\right) = \frac{n}{2} \log\left(1 + \frac{\sigma_x^2}{\sigma_z^2}\right)$$

$$I_{\max}(\mathbf{X}; \mathbf{Y}) = \frac{n}{2} \log\left(1 + \frac{S}{N}\right) [\text{bit/simbol}]$$

- ◆ ako je slučajni signal \mathbf{X} pojasno ograničen na pojas $0 \leq |f| \leq B$ herca - $f_u \geq 2B$ i $n = 2B$

Određivanje maksimalne vrijednosti transinformacije (III)

$$C = \frac{2B}{2} I_{\max}(\mathbf{X}; \mathbf{Y}) = B \log \left(1 + \frac{S}{N} \right) [\text{bit/s}]$$

- ◆ $C = 2BD$, D je dinamika

$$D = \frac{1}{2} \log \left(1 + \frac{S}{N} \right) [\text{bit/uzorak}]$$

- ◆ spektralna gustoća snage šuma definiramo kao

$$S_N(f) = \frac{N_0}{2}, \forall f \in \square$$

- ◆ $N = N_0 B$ $C = B \log \left(1 + \frac{S}{N_0 B} \right) [\text{bit/s}]$

Teorem o informacijskom kapacitetu AWGN-kanala (II)

- ◆ uz uvjete zadane teoremom
- ◆ kanalom je moguće prenositi C bit/s uz proizvoljno malu vjerojatnost pogreške
 - ako se primijeni sustav za kodiranje zadovoljavajuće razine složenosti
- ◆ kanalom nije moguće prenositi informaciju brzinom većom od C bit/s,
- ◆ a da je pri tome vjerojatnost pogreške proizvoljno mala
 - bez obzira na složenost kodera
- ◆ C lakše povećati povećanjem B umjesto S

Primjer određivanja kapaciteta kanala

♦ telefonski kanal

- pojasni propust od 300 do 3400 herca
- pretpostavimo kvantizaciju s 256 razina ($L = 256$, $R = 8$)
- odnos srednje snage sinusnog signala prema srednjoj snazi kvantizacijskog šuma iznosi 49,8 dB
- $B = 3100 \text{ Hz}$ i $S/N = 95499$
- $C = 51283 \text{ bit/s}$
- šum kvantizacije nije jedina smetnja u telefonskom kanalu
- barem 50% krajnjih korisnika ima odnos srednje snage signala prema srednjoj snazi šuma manji ili jednak 35 dB
- $S/N = 3162$, $C = 36044 \text{ bit/s}$

Učinkovitost prijenosnog pojasa

- ◆ idealan sustav: prijenosna brzina $R_b = C$ [bit/s]
- ◆ promatramo neki signal $x(t)$ trajanja T
 - pomoću njega se bitovi informacije prenose kanalom

$$S = \frac{1}{T} \int_0^T x^2(t) dt = \frac{1}{T} \int_{-\infty}^{\infty} x^2(t) dt = \frac{E}{T}$$

- ◆ predajnik generira R_b bit/s
 - ◆ šalje jedan bit informacije svakih $1/R_b$ sekundi
- ◆ srednja energija po svakom bitu $E_b = S/R_b$
 - ◆ u idealnom sustavu $S = E_b C$

Učinkovitost prijenosnog pojasa (II)

$$\frac{C}{B} = \log_2 \left(1 + \frac{E_b}{N_0} \frac{C}{B} \right),$$

$$\frac{E_b}{N_0} = \frac{2^{C/B} - 1}{C/B},$$

- ◆ omjer prijenosne brzine R_b i širine prijenosnog pojasa sustava naziva se **učinkovitost prijenosnog pojasa**
 - kako se širina prijenosnog pojasa povećava prema beskonačnosti, omjer E_b/N_0 se približava svojoj donjoj graničnoj vrijednosti

$$\lim_{B \rightarrow \infty} \left(\frac{E_b}{N_0} \right) = \log(2) = 0,693 \quad \lim_{B \rightarrow \infty} C = \frac{S}{N_0} \log_2 e$$

Odnos prijenosne brzine i kapaciteta kanala

- ◆ $R_b = C$
 - granična vrijednost prijenosne brzine
- ◆ $R_b < C$
 - prijenos brzinom koja je manja od kapaciteta kanala moguće je realizirati s po volji malom vjerojatnošću pogrešaka simbola u prijemu
- ◆ $R_b > C$
 - prijenos brzinom koja je veća od kapaciteta kanala nije moguće realizirati s po volji malom vjerojatnošću pogrešaka simbola u prijemu
- ◆ realni prijenosni sustavi uvijek su projektirani tako da je $R_b < C$ – nužno zbog pouzdanosti sustava

Prijenosna brzina

- ◆ smanjenje odnosa srednje snage signala prema srednjoj snazi šuma, Γ
 - prilikom razmatranja praktičnih prijenosnih sustava u kojima je vjerojatnost pogreške dovoljno mala
 - funkcija dozvoljene vjerojatnosti pogreške i kodnog sustava korištenog u prijenosu
 - određuje učinkovitost realnog kodnog sustava u odnosu na idealni sustav

$$\Gamma = \frac{2^{2C} - 1}{2^{2R} - 1} = \frac{(S/N)}{2^{2R} - 1}$$

$$R = \frac{1}{2} \log \left(1 + \frac{S}{\Gamma N} \right) [\text{bit/simbol}]$$

$$R_b = B \log \left(1 + \frac{S}{\Gamma N} \right) [\text{bit/s}]$$