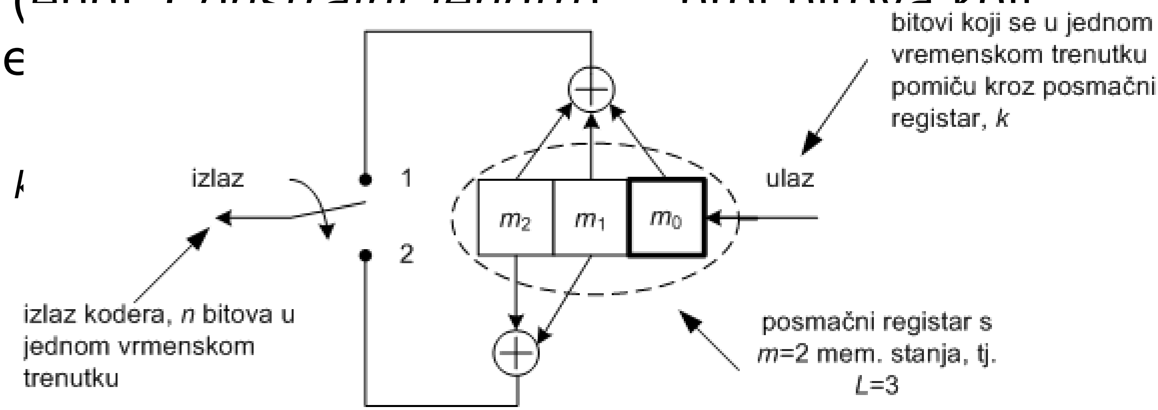
Sadržaj predavanja

- 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
    - Konvolucijski i turbo kodovi

Konvolucijski i turbo kodovi

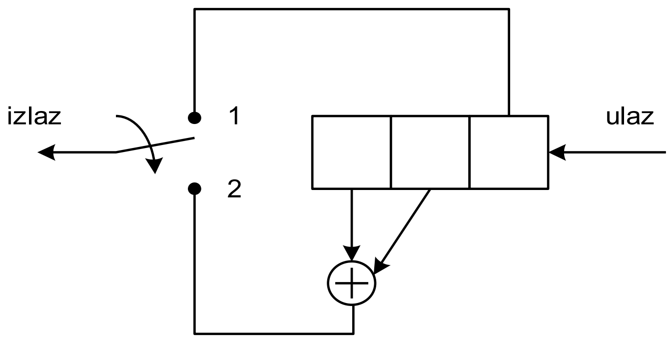
Konvolucijski kodovi

- Konvolucijski kodovi (engl. *Convolutional codes*) spadaju u grupu **memorijskih kodova**.
  - Generiranje *i*-tog bita u kodnoj riječi ovisi ne samo o trenutačnom ulaznom bitu kodera nego i o *k* prethodnih ulaznih bitova.
  - Blok kodovi su bezmemorijski kodovi.
- Konvolucijski koder se sastoji od:
  - binarnih posmačnih registara (svaki registar uključuje *m* memorijskih stanja);
  - digitalnog logičkog sklopovlja, tj. binarnih zbrajala preko kojih se definiraju izlazi kodera (Konv. koder može imati jedan i više izlaza.).
- Konvolucijski koder opisujemo s tri parametra, i to: (*n*, *k*, *L*)
  - *L* – granična duljina kodera (engl. *Constraint length*) – broj bitova koji utječu na pojedini izlaz kode
  - *k* – ulazni bitovi
    - **U okviru ovog predavanja: *k***
  - *n* – izlazni bitovi
- **Stanje *m*0 predstavlja ulaz kodera. Ulazni bit se iz njega na signal "clock" posmiče u stanje *m*1 i prema modulo-2 zbrajalu.**

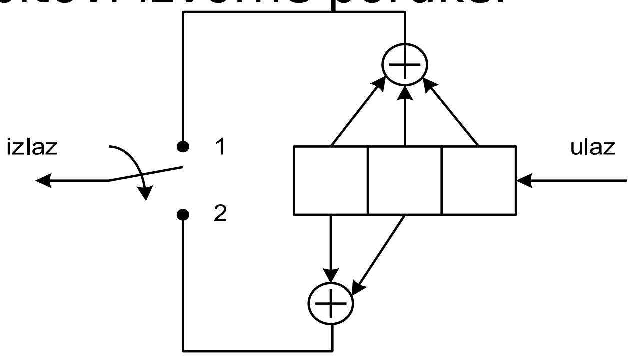


Tipovi konvolucijskih kodera

- Sistematski konvolucijski koder (k=1, n=2): u kodnoj riječi pored bitova zaštite pojavljuju se i bitovi izvorne poruke.



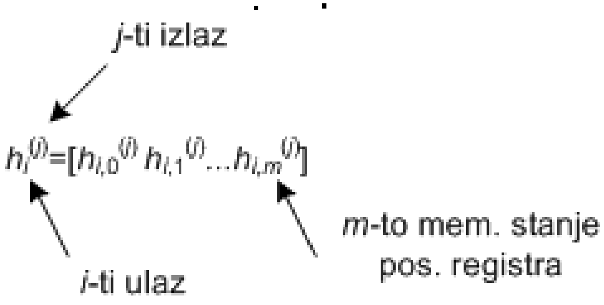
- Nesistematski konvolucijski koder (k=1, n=2): u kodnoj riječi ne nalaze se bitovi izvorne poruke.

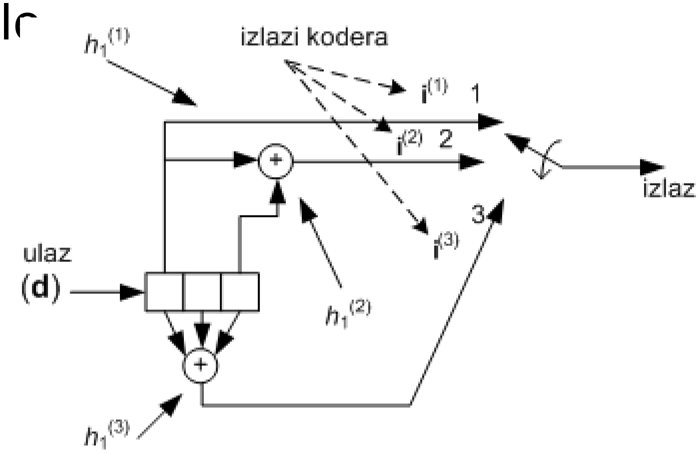


- **Sistematski koder daje manju Hammingovu udaljenost između kodnih riječi jer se odbacuje jedno ili više binarnih zbrajala.**

Generirajuća matrica konv. kodova (1/3)

- Općeniti gledano, gen. matrica **G** je beskonačna jer ulazni slijed informacijskih bitova može teoretski u svojoj duljini biti beskonačan.
- U praksi se uvijek kodira informacijski slijed konačne duljine iz konv. koda nastaje blok kôd.
- Matrica **G** se definira preko *n* vektora (<u>tzv. funkcijski generatori)</u>, i to jedan za svaki od *n* izlaza kodera.
  - *Svaki funkcijski generator (oznaka "h") označava veze između binarnih zbrajala i stanja posmačnih registara za pojedini izlaz kodera.*
  - Postojanje "1"/"0" na nekom mjestu unutar vektora (npr. *i*-to mjesto) pokazuje da je/nije *i*-to stanje u posmačnom registru spojeno na promatrano binarno zbrajalo
- <u>Primjer (3, 1, 3)/ funkc.</u>





$$h_1^{(1)}=[100]$$
$$h_1^{(2)}=[101]$$
$$h_1^{(3)}=[111]$$

Generirajuća matrica konv. kodova (2/3)

- <u>Primjer (3, 1, 3)/ izlazi kodera (tzv. kodirani vektori):</u>

$\mathbf{i}^{(1)}=\mathbf{d}*h_1^{(1)}=[i_0^{(1)}\ i_1^{(1)}\ldots]$

$\mathbf{i}^{(2)}=\mathbf{d}*h_1^{(2)}=[i_0^{(2)}\ i_1^{(2)}\ldots]$

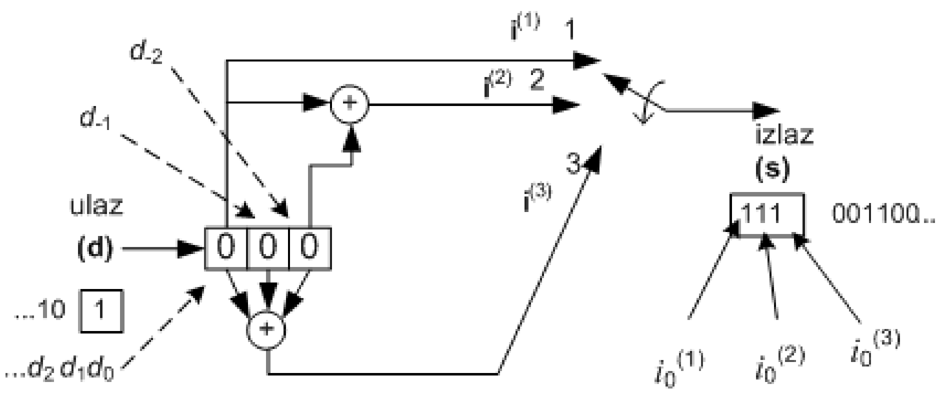
$\mathbf{i}^{(3)}=\mathbf{d}*h_1^{(3)}=[i_0^{(3)}\ i_1^{(3)}\ldots]$

- Znak "*" predstavlja binarnu (modulo-2) diskretnu konvoluciju

- Općenito, *r*-ti bit ($r \geq 0$) *j*-tog kodiranog vektora se određuje iz:

$$\mathbf{i}_r^{(j)} = \sum_{i=1}^{k}\sum_{t=0}^{m} d_{r-t}h_{i,t}^{(j)} = d_r h_{1,0}^{(j)} + d_{r-1}h_{1,1}^{(j)} + \ldots + d_{r-m}h_{1,m}^{(j)} + \ldots$$
$$+ d_r h_{k,0}^{(j)} + d_{r-1}h_{k,1}^{(j)} + \ldots + d_{r-m}h_{k,m}^{(j)},$$
$$j = 1,\ldots,n.$$

- <u>Polazno su sva stanja u posmačnom registru postavljena na "0".</u>



- $r = 0$

$$i_0^{(1)} = d_0 h_{1,0}^{(1)} \oplus d_{-1}h_{1,1}^{(1)} \oplus d_{-2}h_{1,2}^{(1)} = 1\cdot 1 \oplus 0\cdot 0 \oplus 0\cdot 0 = 1$$

$$i_0^{(2)} = d_0 h_{1,0}^{(2)} \oplus d_{-1}h_{1,1}^{(2)} \oplus d_{-2}h_{1,2}^{(2)} = 1\cdot 1 \oplus 0\cdot 0 \oplus 0\cdot 1 = 1$$

$$i_0^{(3)} = d_0 h_{1,0}^{(3)} \oplus d_{-1}h_{1,1}^{(3)} \oplus d_{-2}h_{1,2}^{(3)} = 1\cdot 1 \oplus 0\cdot 1 \oplus 0\cdot 1 = 1$$

- $r = 1$

$$i_1^{(1)} = d_1 h_{1,0}^{(1)} \oplus d_0 h_{1,1}^{(1)} \oplus d_{-1}h_{1,2}^{(1)} = 0\cdot 1 \oplus 1\cdot 0 \oplus 0\cdot 0 = 0 \ldots$$

- Izlaz: **s**=[*i* 0(1) *i* 0(2) *i* 0(3) *i* 1(1) *i* 1(2) *i* 1(3) ...]

Generirajuća matrica konv. kodova (3/3)

- Gen. matrica **G** je u potpunosti određena s funkcijskim generatorima, dok njena dimenzija ovisi o promatranoj informacijskoj poruci **d**.
- Općeniti oblik gen. Matrice, **G**, je:

$$\mathbf{G}_{\infty} = \begin{bmatrix} \mathbf{G}_0 & \mathbf{G}_1 & \mathbf{G}_2 & \cdots & \mathbf{G}_m & & & \\ & \mathbf{G}_0 & \mathbf{G}_1 & \cdots & \mathbf{G}_{m-1} & \mathbf{G}_m & & \\ & & \mathbf{G}_0 & \cdots & \mathbf{G}_{m-2} & \mathbf{G}_{m-1} & \mathbf{G}_m & \\ & & & \ddots & & & & \ddots \end{bmatrix} \text{ s podmatricama } \mathbf{G}_l = \begin{bmatrix} h_{1,l}^{(1)} & h_{1,l}^{(2)} & \cdots & h_{1,l}^{(n)} \\ h_{2,l}^{(1)} & h_{2,l}^{(2)} & \cdots & h_{2,l}^{(n)} \\ \vdots & \vdots & & \vdots \\ h_{k,l}^{(1)} & h_{k,l}^{(2)} & \cdots & h_{k,l}^{(n)} \end{bmatrix}$$

$l = 0, 1, \ldots, m$

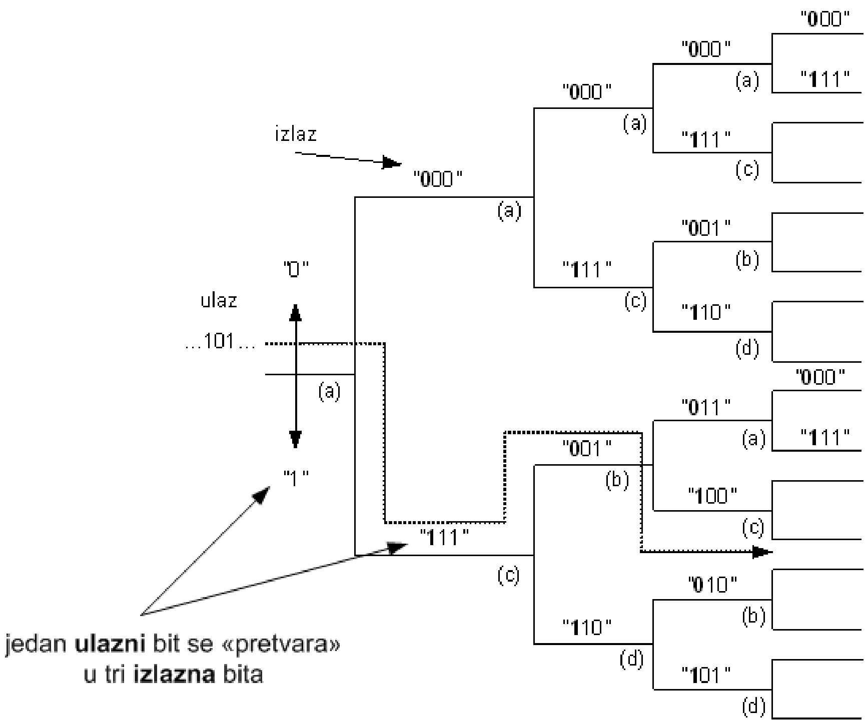
- <u>Primjer (3, 1, 3)/ gen matrica, **G**:</u>

Na ulaz kodera dolazi poruka **d**=[101]

$$\mathbf{G} = \begin{bmatrix} 111 & 001 & 011 & 0 & 0 \\ 0 & 111 & 001 & 011 & 0 \\ 0 & 0 & 111 & 001 & 011 \end{bmatrix} \quad \mathbf{s} = \mathbf{dG} = [101] \begin{bmatrix} 111 & 001 & 011 & 0 & 0 \\ 0 & 111 & 001 & 011 & 0 \\ 0 & 0 & 111 & 001 & 011 \end{bmatrix} = [111 \quad 001 \quad 100 \quad 001 \quad 011].$$

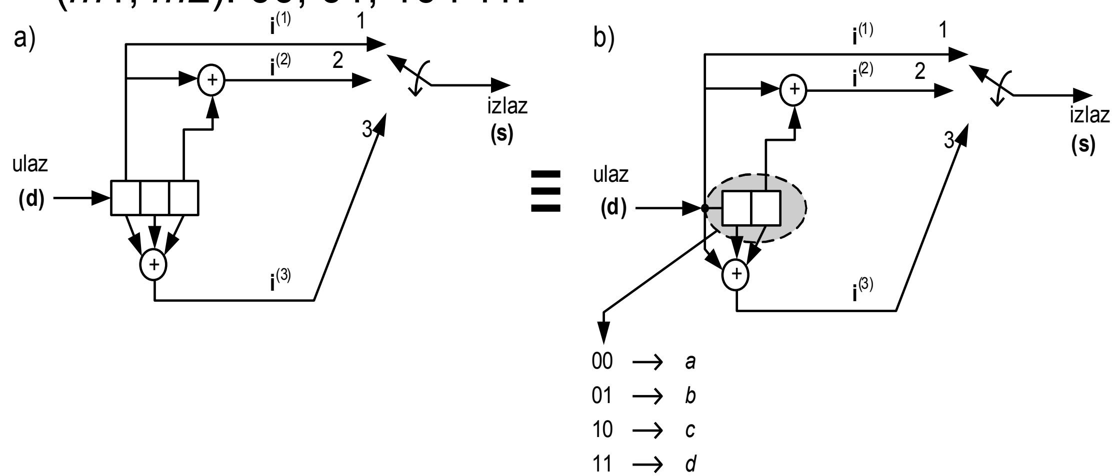
Grafički prikaz konv. kodova (1/2)

- Postoje tri metode za prikaz konvolucijkog kodiranja.
  - stablasti dijagram (engl. *tree diagram*)
  - rešetkasti dijagram (engl. *trellis diagram*)
  - dijagram stanja (engl. *state diagram*)



Stablasti dijagram za koder sa slajda 7

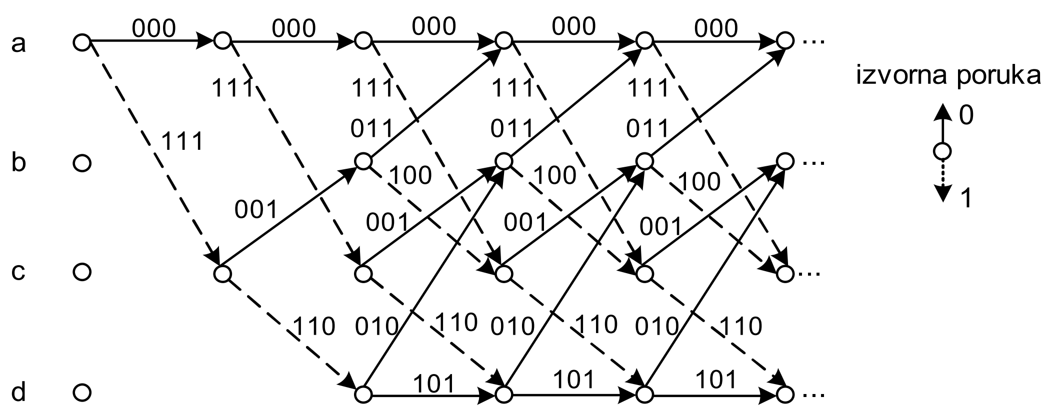
- Izlaz iz kodera određen je s ulaznim bitom (*m*0) i jednim od četiri moguća stanja posmačnog registra (*m*1, *m*2): 00, 01, 10 i 11.



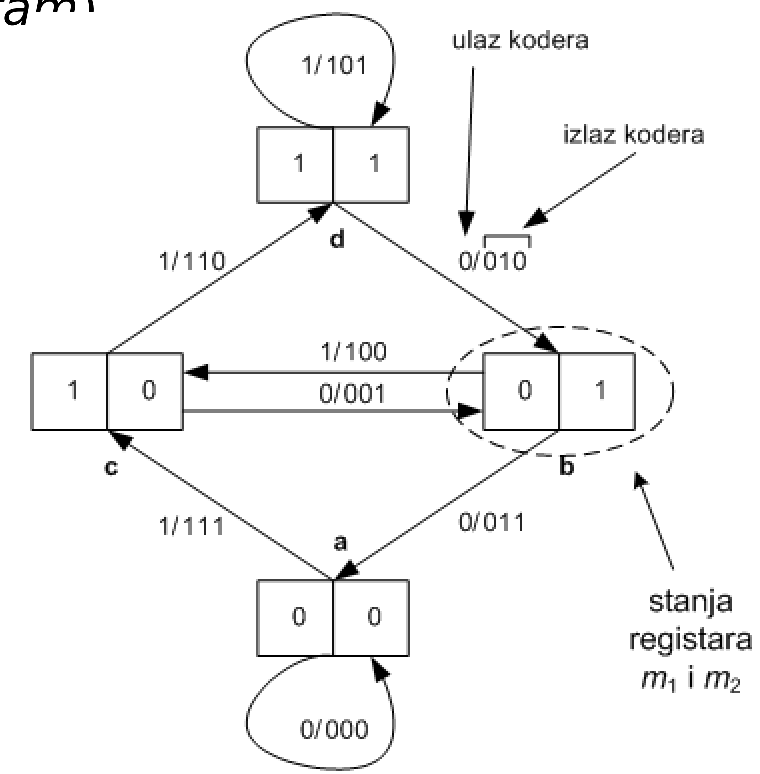
- Spajanjem čvorišta, u stablastom dijagramu, koja imaju isti izlazni slijed i istu oznaku nastaje rešetkasti dijagram.

Grafički prikaz konv. kodova (2/2)

- Postoje tri metode za prikaz konvolucijkog kodiranja.
  - stablasti dijagram (engl. *tree diagram*)
  - rešetkasti dijagram (engl. *trellis diagram*)
  - dijagram stanja (engl. *state diagram*)



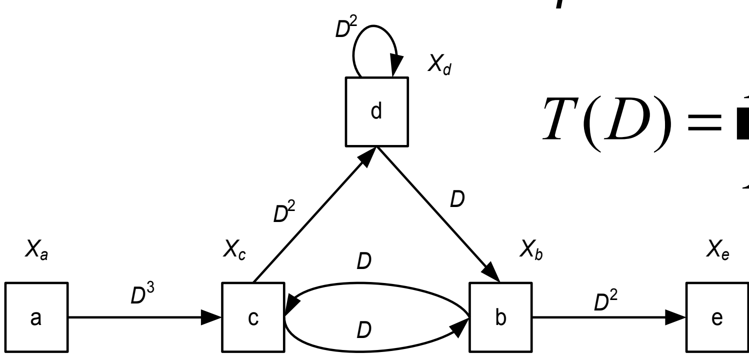
Rešetkasti dijagram za koder sa slajda 7.



Dijagram stanja za koder sa slajda 7

Prijenosna funkcija konv. koda i udaljenost koda (1/2)

- Prijenosna funkcija (oznaka -> *T*(*D*)) određuje udaljenost i performanse koda u pogledu pogrešaka.
- Prethodni dijagram stanja (slajd 10), uz izmjenu, iskoristit ćemo za objašnjenje i proračun udaljenosti konv. koda.
- Potrebno je napraviti sljedeće:
  - Podijeliti stanje “a” na dva nova stanja, tj. “a” (ulaz) i “e” (izlaz) potrebno je ukloniti vlastitu petlju u stanju “a”;
  - Označiti svaku granu u grafu s *Di*, gdje *i* označava <u>težinu kodne riječi</u> *n* (izlazni bitovi kodera);
  - Uvesti jednu varijablu (*X*a, ..., *X*e) za svako stanje (a, ...,e).
  - *Kao referentni put odabran je put sastavljen isključivo od nula*;

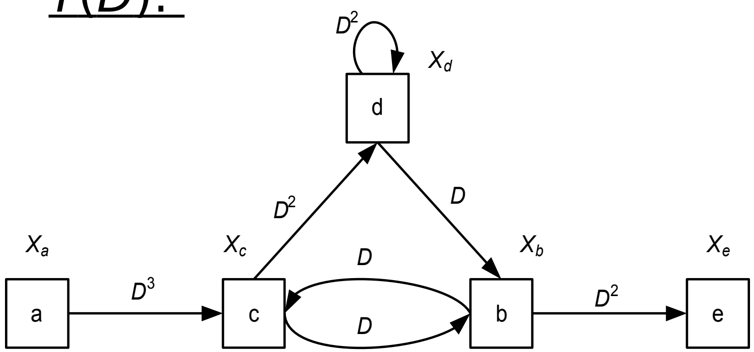


$$T(D) = \frac{X_e}{X_a}$$

- **Potrebno je pronaći sve putove od stanja “a” do stanja “e” i zbrojiti njihove težine. Put s najmanjom težinom je ujedno i put s najmanjom Hamm. udaljenosti.**

Prijenosna funkcija konv. koda i udaljenost koda (2/2)

- Primjer (3, 1, 3)/ *T*(*D*):



$$T(D)=\frac{X_e}{X_a}$$

$$X_c = D^3 X_a + DX_b$$

$$X_b = DX_c + DX_d$$

$$X_d = D^2 X_c + D^2 X_d$$

$$X_e = D^2 X_b$$

Rješavanjem sustava jednadžbi, dobivamo

$$T(D)=\frac{D^6}{1-2D^2}=D^6\left(1+2D^2+4D^4+8D^6+\ldots\right)=1D^6+2D^8+4D^{10}+8D^{12}+\ldots$$

jedan put udaljenosti 6, $d_{\min}$
a-c-b-e

dva puta udaljenosti 8

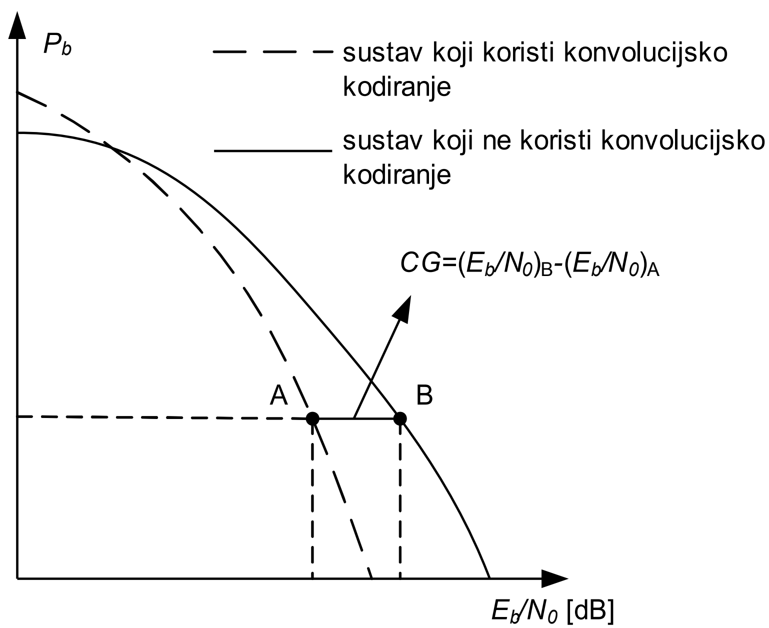
Napomena: Za dodatne mogućnosti prijenosne funkcije konv. koda vidjeti: PANDŽIĆ, I.S. BAŽANT, A. ILIĆ, Ž. VRDOLJAK, Z. KOS, M. SINKOVIĆ, V. *Uvod u teoriju informacije i kodiranje.* Element, 2 izdanje, 2010. (ISBN 978-953-197-605-3)

Dekodiranje konv. kodova: dekoder s tvrdim i mekim odlučivanjem

- **Udaljenost koda:** *mjera sličnosti* između dvaju kodnih riječi nekog koda *K*.
  - Dvije mjere sličnosti: Hammingova i euklidska udaljenost koda;
  - Primjena neke od navedenih mjera ovisi o odabranom kodnom sustavu, zahtijevanom BER-u, tipu prijenosnog kanala i vrsti demodulatora.
- Hammingova udaljenost koda
  - Kod prijenosa binarnim simetričnim kanalom u kojem se svaki simbol promatra zasebno (bezmemorijski kanal);
  - U prijemu se koristi tzv. **većinska odluka** o tome koji je simbol primljen;
  - Koristi se tzv. **dekoder s tvrdim odlučivanjem** (engl. *hard-decision decoder*).
- Euklidska udaljenost koda
  - Kod prijenosa kanalom s aditivnim bijelim Gaussovim šumom (skr. AWGN);
  - Odluka o primljenom simbolu provodi se **uzimajući u razmatranje cijelu kodnu riječ**;
  - Koristi se tzv. **dekoder s mekim odlučivanjem** (engl. *soft-decision decoder*).

Dekodiranje konv. kodova: performanse kodnih sustava

- **Za procjenu performansi kodnog sustava** najčešće se uzima ovisnost vjerojatnosti pogreške bita naprema odnosu srednje snage signala prema srednjoj snazi šuma, tj. *BER*=*f*(*S*/*N*) ili *Pb*=*f*(*S*/*N*).
- **Kodno pojačanje** (engl. *coding gain,* skr. CG): određuje potrebni omjer *S*/*N* (definiran kao srednja primljena energija po bitu *Eb* u odnosu na jednostanu spektralnu gustoću snege šuma *N*0) koji osigurava zahtijevanu vjerojatnost pogreške bita, *Pb*.



- Za dekoder s tvrdim odlučivanjem:

$$CG \approx 10\log_{10}\left[R(t+1)\right]$$

- Za dekoder s mekim odlučivanjem:

$$CG \approx 10\log_{10}\left[Rd\right]$$

  - *R* - kodna brzina (=*k*/*n*)
  - *t* – broj pogrešaka koje kôd može ispraviti
  - *d* - min. udaljenost koda

Dekodiranje konv. kodova: dekodiranje ML

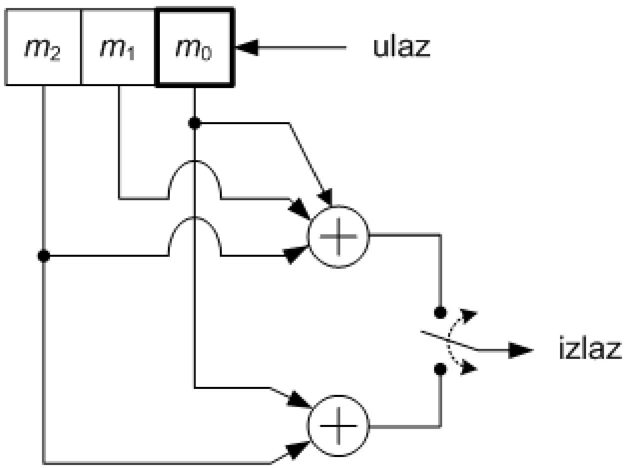
- Dekodiranje konv. kodova provodi se na <u>principu maksimalne vjerojatnosti </u>(engl. *maximum likelyhood decoding*), tzv. dekodiranje ML.
  - Neka je **c** (=[*c*0*c*1*c*2…*cj*…]) kodirani slijed bitova (kodna riječ) koji se prenosi preko kanala s pogreškama (**e**), tada je primljeni slijed (primljena kodna riječ) **c**’=**c**+**e** (=[*c’*0*c’*1*c’*2…*c’j*…]) ;
  - Vjerojatnost dekodiranja simbola je $p(\mathbf{c}',\mathbf{c}) = \prod_{j=0}^{\infty} p(c_j'|c_j)$
  - Dekoder traži takav slijed bitova koji osigurava maksimum navedene <u>metrike</u> *p*(**c**’,**c**). Također, dekoder analizira cijeli primljeni slijed bitova **c**’.
  - *Dekoder koristi rešetkasti dijagram u kojem izračunava težinu (tj. metriku) svake putanje i u svakom koraku grananja donosi odluku o primljenoj kodnoj riječi*.
    - Dosta često se prethodni izraz zapisuje kao (iz razloga što su vjerojatnosti “mali” brojevi):

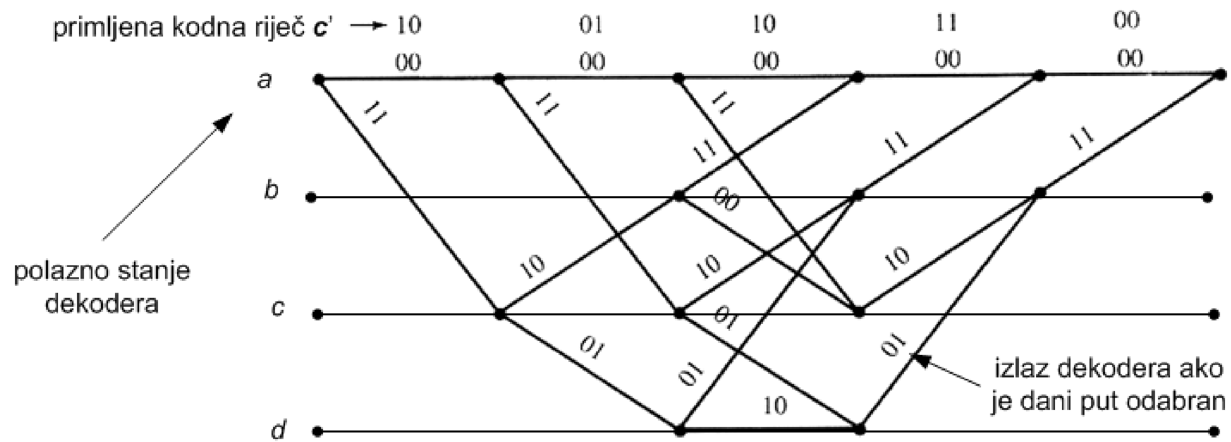
$$\ln\{p(\mathbf{c}',\mathbf{c})\} = \sum_{j=0}^{\infty} \ln\{p(c_j'|c_j)\}$$

    - **Napomenimo da ovo odgovara traženju najmanje Hammingove udaljenosti između c’ i svih mogućih putanja u rešetkastom dijagramu. Objašnjenje slijedi u sljedećem primjeru!**

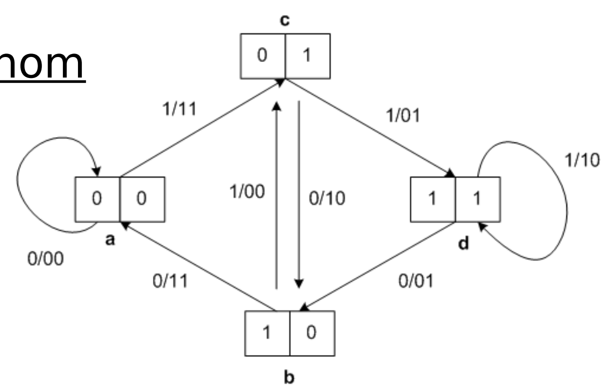
Dekodiranje konv. kodova: dekodiranje ML, Primjer (1/3)

- Primjer: Dan je konv. koder (2,1,3). Pet bitova je kodirano i dobivena je kodna riječ koja se prenosi preko kanala u kojem je vjerojatnost pogreške bita *Pb*=0.1. Na prijemnoj strani pojavljuje se slijed bitova (s pogreškama) **c**'=[10 01 10 11 00]. Odredite najvjerojatniju poslanu kodnu riječ, **c**.





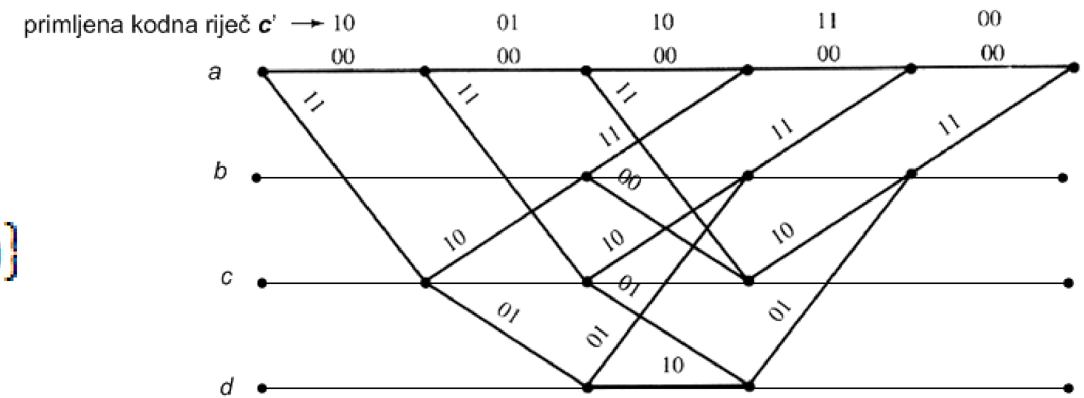
- Polazno su sva stanja u posmačnom registru postavljena na "0".



Dekodiranje konv. kodova: dekodiranje ML, Primjer (2/3)

$$p(\mathbf{c}',\mathbf{c}) = \prod_{j=0}^{\infty} p(c'_j|c_j)$$

$$\ln\{p(\mathbf{c}',\mathbf{c})\} = \sum_{j=0}^{\infty} \ln\{p(c'_j|c_j)\}$$



- Rješenje: Dekodiranje možemo provesti računajući metriku svih osam putova u rešetkastom dijagramu. Kao rješenje uzimamo put s najvećom metrikom. Također, dekodiranje se može provesti računajući Hamm. udaljenost između **c**' i svih osam putova u reš. dijagramu. Kao rješenje uzimamo put s najmanjom Hamm. udaljenosti. Metrike za dani kanal su (za jedan simbol):

$$\ln[p(0|0)] = \ln[p(1|1)] = \ln(0.9) = -0.11$$

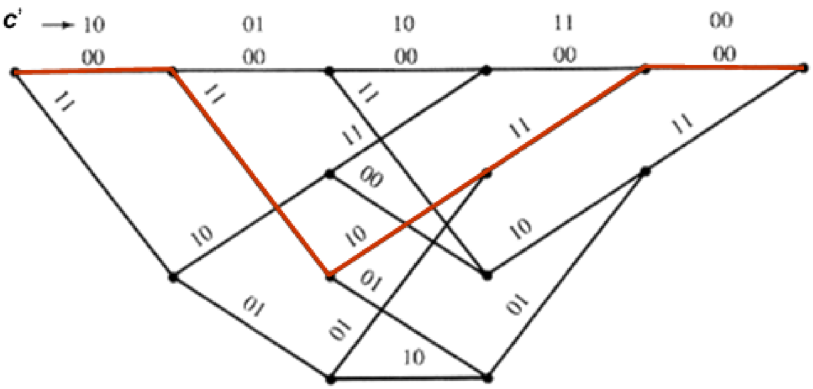
$$\ln[p(1|0)] = \ln[p(0|1)] = \ln(0.1) = -2.30 = \text{Pogrešan prijenos jednog simbola}$$

Primjer: Promatrajmo put u reš. dijagramu koji ima sve nule. Dani put se od **c**' razlikuje u pet pozicija. Njegova u

$5(-2.3) + 5(-0.11) = -12.5$

pogrešan prijenos — ispravan prijenos

Dekodiranje konv. kodova: dekodiranje ML, Primjer (3/3)



Odabrani put:

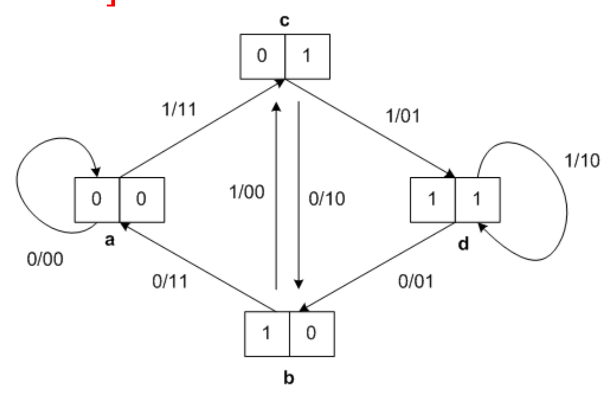
$ispravan\ prijenos: 8 \cdot (-0.11) = -0.88$

$pogrešan\ prijenos: 2 \cdot (-2.30) = -4.60$

Ukupna metrika puta: -5.48

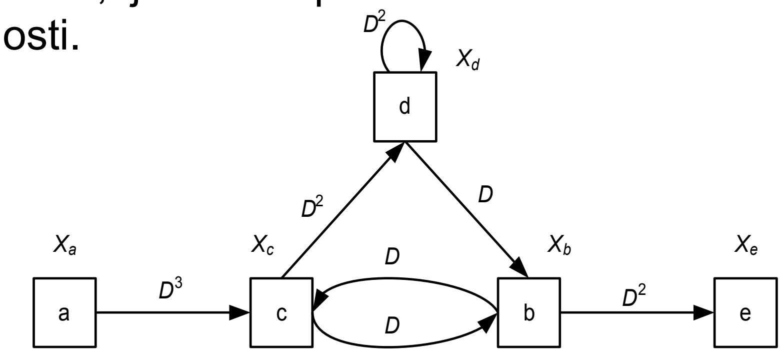
Put	Metrika puta	Hamm. udaljenost
00 00 00 00 00	-12.05	5
00 00 11 10 11	-14.24	6
00 11 10 11 00	-5.48	2
00 11 01 01 11	-16.43	7
11 10 11 00 00	-14.24	6
11 10 00 10 11	-16.43	7
11 01 01 11 00	-7.67	3
11 01 10 01 11	-9.86	4

- Put s najvećom metrikom, odnosno najmanjom Hamm. udaljenosti. Najvjerojatnija poslana kodna riječ **c**=[00 11 10 11 00], odnosno poruka **d**=[0 1 0 0 0]

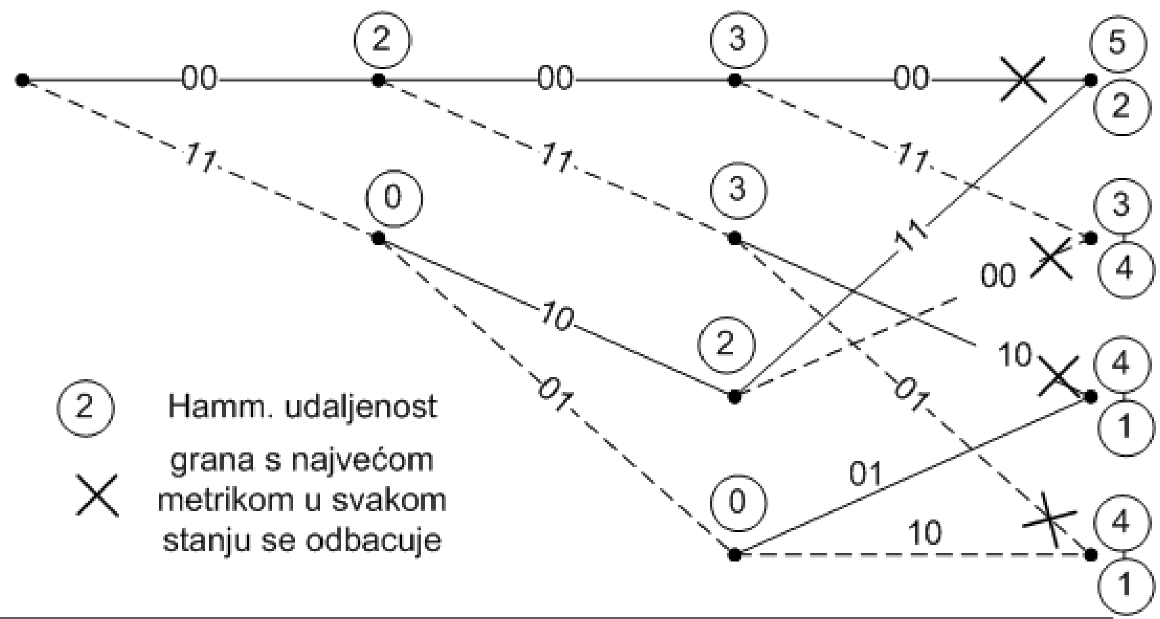


Dekodiranje konv. kodova: Viterbijev algoritam (1/2)

- Optimalno dekodiranje konv. kodova svodi se na nalaženje puta, u rešetkastom dijagramu, koji od primljene kodne riječi **c**’ ima minimalnu Hamm. udaljenost, tj. traži se put u rešetkastom dijagramu od stanja *a* do stanja *e* s min. Hamm. udaljenosti.



- Problem dekodiranja ML je što mora odrediti sve putove u rešetkastom dijagramu kako bi se dekodiranje provelo. To uključuje 2*L* putova.
- **Viterbijev algoritam poboljšava proračun tako što uspoređuje dvije metrike za putove koji se spajaju u nekom stanju i odbacuje onaj put s manjom metrikom.** Navedeni postupak se ponavlja za sva stanja. **Na ovaj način na svakoj razini rešetke imamo 2*m* “preživjelih” putova.**

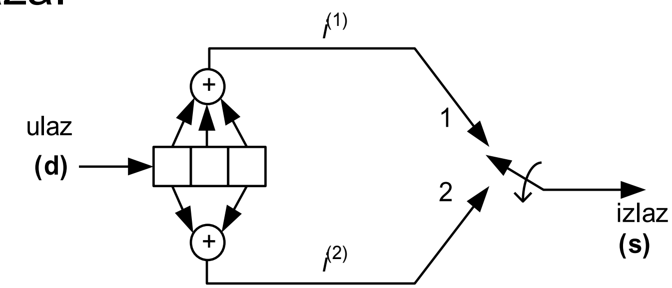


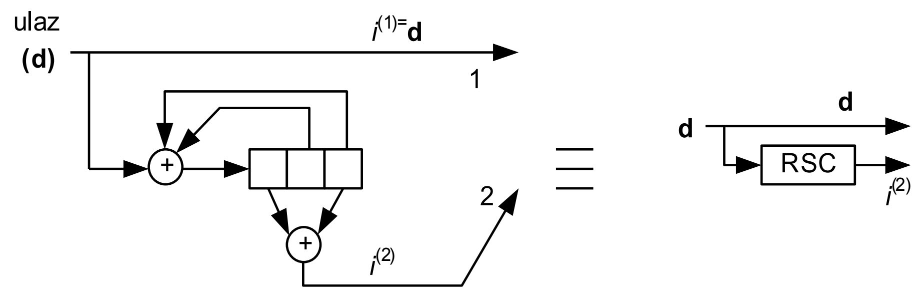
Dekodiranje konv. kodova: Viterbijev algoritam (2/2)

- Sa slike (slajd 19) je vidljivo da dekoder (koristi Viterbijev algoritam) u potpunosti može početi s radom (sva stanja su uključena) nakon trećeg koraka grananja.
- Pitanje: Koliko dugo (do kojeg koraka grananja) algoritam treba ponavljati, tj. kada treba donijeti odluku o primljenom slijedu bitova? Na ovaj način se određuje dio bitova koji pripadaju izvornoj poruci.
  - Odgovor na dano pitanje je jako bitan jer cijena dekodera ovisi o veličini memorije u koju se spremaju "preživjeli" putovi.
  - Pokazuje se da veličina memorije koja je 4 do 5 puta dulja od *L* daje performanse koda bliske optimumu.
    - Kao izlaz dekodera, tj. bitovima poruke proglašavaju se bitovi koji pripadaju najvjerojatnijem putu od svih "preživjelih".
    - Kad se donese odluka o izlazu dekodera svi "preživjeli" putovi u memoriji se brišu i u istu spremaju novi.
- Pitanje: Što dekoder radi ako u istom stanju ima dva puta koji imaju jednaku metriku?
  - U takvim prilikama dekoder odabire slučajno jedan od dva puta.
- Drugi algoritmi dekodiranja konvolucijskih kodova.
  - Sekvencijalni algoritam (dosta sličan Viterbijevom algoritmu);
  - Algoritam dekodiranja s povratnom vezom (engl. *feedback decoding*).

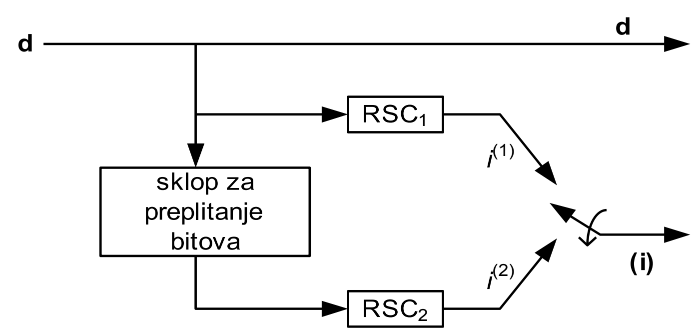
Turbo kodovi

- Podgrupa konvolucijskih kodova.
- Kodiranje se temelji na paralelnom ulančavanju nekih klasa sistematskih konvolucijskih kodova, tzv. *rekurzivni sistematski konv. kodovi* (RSCC, engl. *recursive systematic convolutional codes*).
- RSCC – nesistematski koder u kojem se na njegov ulaz spaja jedan ili više njegovih izlaza.





- Turbo kodovi – paralelna veza najčešće dva jednaka RSC kodera odvojena sklopom za preplitanje bitova (engl. *interleaver*).



Što smo naučili?

- Razliku između cikličnih i konvolucijskih kodova.
- Odrediti generirajuću matricu konvolucijskog koda na osnovu funkcijskih generatora.
- Skicirati dijagram stanja za neki konvolucijski koder.
- Skicirati konv. koder uz poznavanje funkcijskih generatora.
- Odrediti prijenosnu funkciju i udaljenost konv. koda.
- Princip dekodiranja Viterbijevim algoritmom.