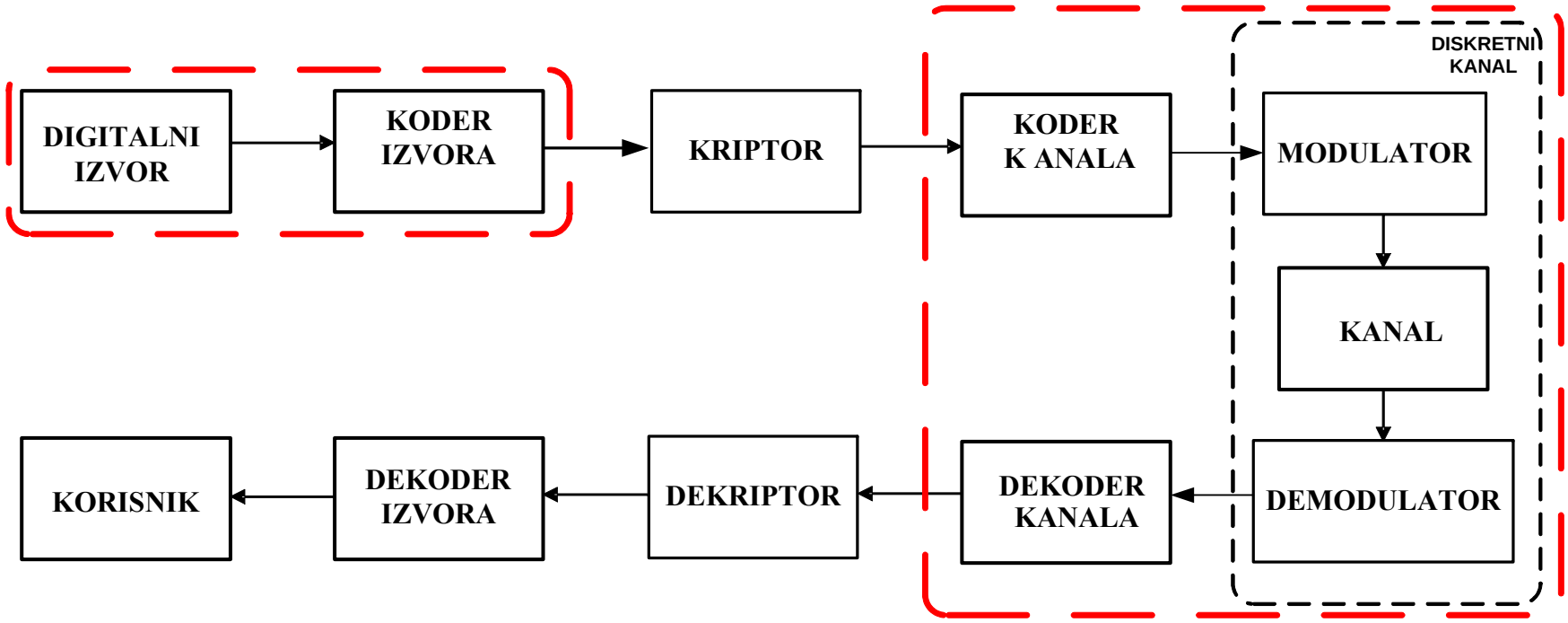
PRINCIPI MODERNIH TELEKOMUNIKACIJA

Elektrotehnički fakultet
Katedra za telekomunikacije
Beograd, 2019/2020.

-III-
Zaštitni kodovi

Blok šema sistema sa stanovišta teorije informacija

* Smatra se da izvor emituje nekakve simbole –> *q*-nivoski digitalni signal može se opisati sa *q* mogućih amplituda.
* Ciljevi sistema – *efikasan*, *siguran* i *pouzdan* prenos podataka.



Blok kodovi

* **Zadatak blok kodera je da prihvati izvestan broj (*k*) bita i da ih predstavi odgovarajućom kodnom reči dužine *n* bita.**
* **Pošto otkrivanje i eventualno ispravljanje grešaka zahtevaju unošenje redundanse, mora biti ispunjeno *n*>*k*.**

* **Kodna reč se sastoji od**
  - ***k informacionih*** **bita, tipično označenih sa** $i_1 i_2, \ldots, i_k$
  - ***n-k kontrolnih*** **(*zaštitnih* bita) , tipično označenih sa** $z_1, z_2, \ldots, z_{n-k}$
* **Blok kod se označava sa (*n*,*k*), dok je veličina *R*=*k*/*n* u stvari *kodni količnik* blok koda.**

Linearni blok kodovi (LBK)

* **Na ulazu u blok kod je jedan od 2^k mogućih blokova od k informacionih simbola, a na izlazu je odgovarajuća kodna reč dužine n, koja je po nekom kriterijumu odabrana od 2^n mogućih "kandidata".**

* **Neka je dato konačno polje *GF(q)*, tj. polje sa q simbola. Sekvence od po n elemenata polja čine vektorski prostor dimenzije n nad datim poljem. Linearni kod je podprostor vektorskog prostora nad *GF(q)*.**

* **Osobine LBK za q=2:**

  1) Ko mora da sadrži kombinacije "sve nule" i "sve jedinice" jer su to neutralni elementi u odnosu na sabiranje i množenje.

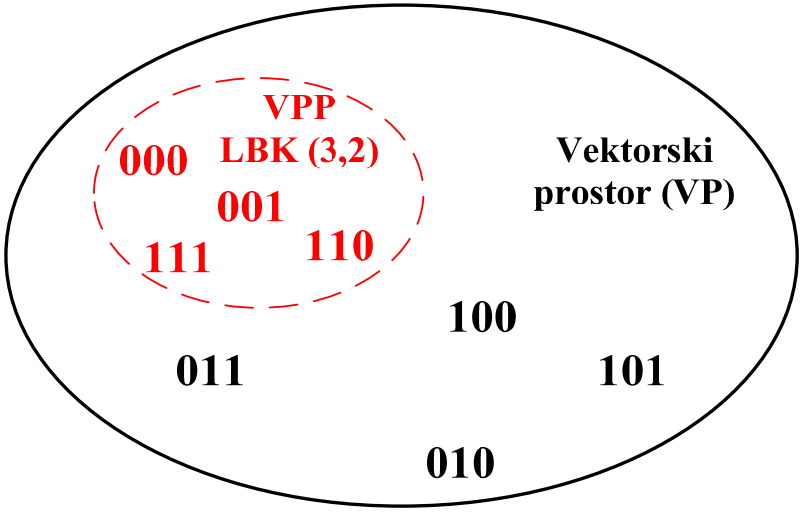
  2) Zatvorenost u odnosu na sabiranje.

* **Ako je minimalno Hemingovo rastojanje dve kodne reči označeno sa d, tada ni u kom slučaju broj grešaka koje ovaj kod koriguje ne može biti veći od e_c a broj grešaka koje detektuje ne može biti veći od e_d, pri čemu važi:**

$$d \geq 2e_c+1 \qquad d \geq e_c+e_d+1$$

Primer linearnog blok koda

* Primer (3,2) koda na polju GF(2)



* Vektorski prostor ima 2^3=8 elemenata dužine 3.
* Vektorski potprostor ima 2^2=4 elemenata dužine 3. Ovaj potprostor je jedan LBK (3,2).

* Kodne reči su

  000, 001, 110, 111

* Neutralni elementi

  000 i 111

* Zatvorenost za +

  001 + 000 = 001

  001 + 111 = 110 ...

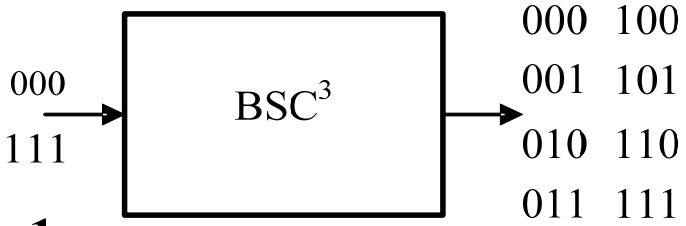
* Zatvorenost za * nije neophodna (ali je ovde ispunjena)

  001 * 111 = 001

  001 * 110 = 000 ...

Ponavljanje poruke, pravilo odlučivanja

* **Kod zasnovan na ponavljanju poruke tri puta**
  - broj poruka je M=2, poruke bi mogle da se predstave sa ld(M)=1 bita;
  - dužina kodne reči je n=3, kodni količnik R=1/3 a protok Φ=v(X,Y)/3;



* **Pravilo odlučivanja br. 1**
  - Neka se 000 i 111 dekoduje kao 0, odnosno 1, a u svim ostalim slučajevima smatra da su se pojavile greške;
  - Verovatnoća neotkrivene greške za E_b/N_0=4.3dB tj. p=10^{-2}.

$$P_e^{(1)} = p^3 = 10^{-6}.$$

  - Ovaj nivo greške bez primene koda postiže se za E_b/N_0=10.5dB -> p=10^{-6}.

* **Pravilo odlučivanja br. 2**
  - Majoritetna logika: greške se detektuju ali i koriguju.
  - Ispravlja samo jednostruke, verovatnoća neotkrivene greške je sada nešto veća

$$P_e^{(2)} = \binom{3}{0} p^3 + \binom{3}{1} p^2 (1-p) = 0,000298.$$

Hemingov kod – konstrukcija pomoću šablona

* **Šablon**

1	0 0 **1**	z_1
2	0 **1** 0	z_2
3	0 1 1	i_1
4	**1** 0 0	z_3
5	1 0 1	i_2
6	1 1 0	i_3
7	1 1 1	i_4

* **Vektori**

I = [1101]
X = [1010101]
E = [0000010]
Y = [1010111]

- decimalni zapis sindroma pokazuje poziciju greške.

- ovaj kod može da detektuje i ispravlja greške.

* **Neka treba kodovati bite** $i_1=1$, $i_2=1$, $i_3=0$, $i_4=1$.
* **Pozicije prve jedinice u kolonama (počev od krajnje desne) određuju pozicije zaštitnih bita**

$$z_1, z_2, i_1, z_3, i_2, i_3, i_4$$

* **Preostale jedinice u pojedinim kolonama određuju kontrolne sume**

$$z_1 = i_1 \oplus i_2 \oplus i_4 = 1 \oplus 1 \oplus 1 = 1,$$
$$z_2 = i_1 \oplus i_3 \oplus i_4 = 1 \oplus 0 \oplus 1 = 0,$$
$$z_3 = i_2 \oplus i_3 \oplus i_4 = 1 \oplus 0 \oplus 1 = 0.$$

* **Greška na šestoj poziciji,** $e_6=1$.
* **Dekodovanje se obavlja pomoću sindroma**

$$s_1 = y_1 \oplus y_3 \oplus y_5 \oplus y_7 = 1 \oplus 1 \oplus 1 \oplus 1 = 0$$
$$s_2 = y_2 \oplus y_3 \oplus y_6 \oplus y_7 = 0 \oplus 1 \oplus 1 \oplus 1 = 1$$
$$s_3 = y_4 \oplus y_5 \oplus y_6 \oplus y_7 = 0 \oplus 1 \oplus 1 \oplus 1 = 1$$

$S=[110]=6$ (pozicija greške).

Pojava dvostruke greške

* **Poslato je [1101] a pri prenosu je pogrešno prenet 5. i 6. bit**

Koder :	*Kanal* :	*Dekoder* :
$z_1 = 1 \oplus 1 \oplus 1 = 1$	$x = [1\ 0\ 1\ 0\ 1\ 0\ 1]$	$s_1 = 1 \oplus 1 \oplus 0 \oplus 1 = 1$
$z_2 = 1 \oplus 0 \oplus 1 = 0$	$e = [0\ 0\ 0\ 0\ 1\ 1\ 0]$	$s_2 = 0 \oplus 1 \oplus 1 \oplus 1 = 1$
$z_3 = 1 \oplus 0 \oplus 1 = 0$	$y = [1\ 0\ 1\ 0\ 0\ 1\ 1]$	$s_3 = 0 \oplus 0 \oplus 1 \oplus 1 = 0$

* **Sindrom S=[011] ukazuje na treću poziciju koja se komplementira pa se rekonstruisana informaciona reč [0011] razlikuje od poslate za tri bita!**

* **U ovom primeru dekodovanje je čak pogoršalo performanse sistema. Zato se često dodaje još jedan zaštitni bit - ukupna provera parnosti.**

* **Osobine Hemingovog (7,4) koda**
  - **d=3, e_c=1, e_d=1;**
  - **ovaj kod može da detektuje jednu grešku, koju istovremeno i koriguje (ne može da detektuje dodatne greške).**

Tumačenje sindroma kod Heminga (8,4)

* **Modifikovano kodovanje i dekodovanje**

$$z_4 = \sum_{i=1}^{7} x_i, \qquad s_4 = \sum_{i=1}^{8} y_i$$

* **Sindromi**

  1) S=0, s_4=0 - nije bilo greške pri prenosu

  2) S>0, s_4=1 - neparan broj grešaka, sindrom pokazuje poziciju

  3) S>0, s_4=0 - paran broj grešaka

  4) S=0, s_4=1 - greška baš na bitu parnosti

* **Heming (8,4)**

  - ***d*=4, e_c=1, e_d=3; ovaj kod može da detektuje jednu grešku (koju i koriguje) a može da detektuje i još jednu dodatnu grešku.**
  - **Ako je s_4=1, postojao je neparan broj grešaka (na prvih sedam pozicija!), tj. jedna, tri, pet ili sedam grešaka. Za $p=10^{-3}$ verovatnoće da se ovo desi su, respektivno**

$$P_{e1} = \binom{7}{1} p(1-p)^6 \approx 7\cdot 10^{-3}, \quad P_{e3} = \binom{7}{3} p^3(1-p)^4 \approx 3.5\cdot 10^{-8}$$

$$P_{e5} = \binom{7}{5} p^5(1-p)^2 \approx 2.1\cdot 10^{-14}, \quad P_{e7} = \binom{7}{7} p^7 \approx 1\cdot 10^{-21}$$

Skraćeni Hemingovi kodovi

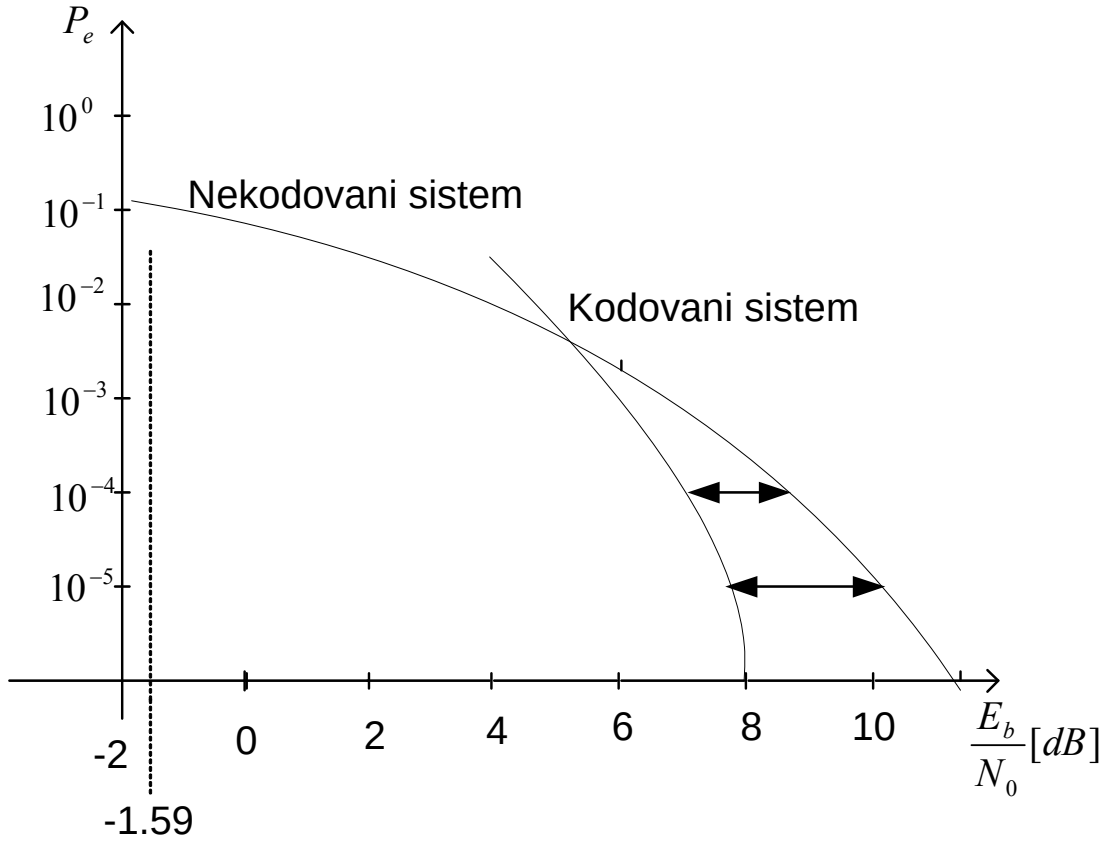
* **Kodovi dobijeni dodavanjem ukupne provere na parnost često se zovu *prošireni* (*expanded*) kodovi,**
* ***Skraćeni* (*shortened*) oni kodovi gde se izostavljaju pojedini informacioni simboli.**
* **Hemingov kod (12,7)**

1	0 0 0 **1**	k_1
2	0 0 **1** 0	k_2
3	0 0 1 1	i_1
4	0 **1** 0 0	k_3
5	0 1 0 1	i_2
6	0 1 1 0	i_3
7	0 1 1 1	i_4
8	**1** 0 0 0	k_4
9	1 0 0 1	i_5
10	1 0 1 0	i_6
11	1 0 1 1	i_7
12	1 1 0 0	i_8
~~13~~	~~1 1 0 1~~	
~~14~~	~~1 1 1 0~~	
~~15~~	~~1 1 1 1~~	

Neke od kombinacija u šablonu se ne koriste!

Kodni dobitak

* ***Efektivni kodni dobitak*** **(G_{eff}) pokazuje za koliko se decibela u posmatranom sistemu može smanjiti odnos E_b/N_0 a da pri tome verovatnoća greške ostane nepromenjena!**
* **Zavisi od:**
  - **primenjenog koda;**
  - **zahtevane verovatnoće greške;**



Druga Šenonova teorema

* ***Sve dokle god je:***
  - ***protok manji od kapaciteta kanala***
  - ***kodni količnik manji od parametra I_{max}***

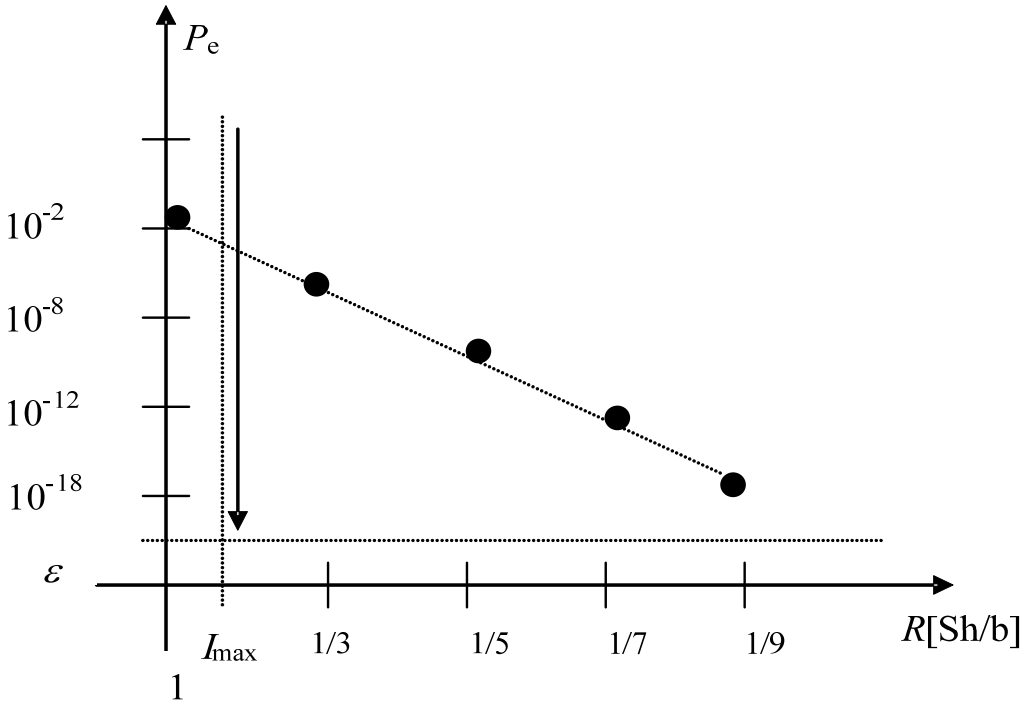
može se naći takav zaštitni kod da se verovatnoća greške proizvoljno smanji!

- **mogući je pouzdan prenos (s proizvoljno malom verovatnoćom greške, označenom sa ε) kroz nepouzdan kanal!**
- **kapacitet kanala je maksimalna moguća brzina kojom se informacije mogu (pouzdano) prenositi kroz dati kanal!**

$$I_{\max} = 1 - (1-p)\cdot \mathrm{ld}\left(\frac{1}{1-p}\right) - p\cdot \mathrm{ld}\frac{1}{p}.$$

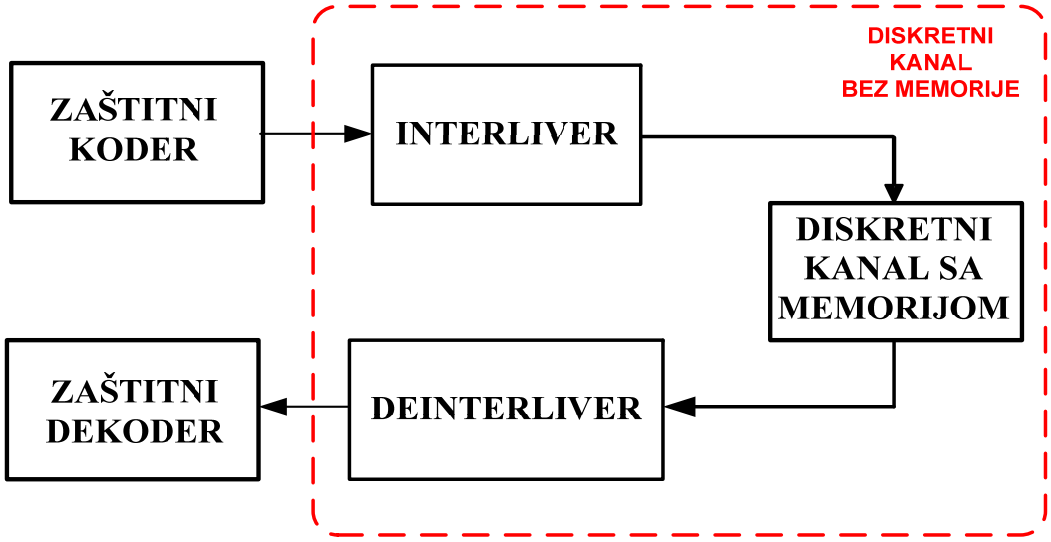
$$p = 10^{-2} \Rightarrow I_{\max} = 0.9192$$

Kod sa ponavljanjem *n* puta, - pravilo odlučivanja br. 1 -		
n=5	R=1/5	P_e=10^{-10}
n=7	R=1/7	P_e=10^{-14}
n=9	R=1/9	P_e=10^{-18}



Linearni blok kodovi sa interlivingom

* Postoje posebni kodovi za “borbu” s paketima grešaka otkrivanje i ispravljanje paketa grešaka (npr. Fajerov – opisan kasnije).
* Kodovi koji otkrivaju i ispravljaju pojedinačne greške mogu se također koristiti i za borbu s paketima grešaka.
* Posebnim postupkom – interlivingom (“*interleaving*” - *pletenje*, *upredanje*), ukoliko je idealno izveden, može se izbrisati memorija kanala.
* Položaji interlivera na predaji i deinterlivera na prijemu.



Interliver

* **Formirane kodne reči se ne šalju sukcesivno na kanal, već se čuvaju u memoriji u interliveru.**
* **Kada se u memoriju upiše određen broj kodnih reči (*l* – *stepen interlivinga*), tada se iz memorije šalju u kanal najpre samo prvi biti reči, za njima drugi biti itd.**
* **Analogno dvodimenzionalnim proverama na parnost, i ovde se formira dvodimenzionalni blok kodnih reči dužine *n*, prema šemi:**

$$\begin{matrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{l1} & x_{l2} & \cdots & x_{ln} \end{matrix}$$

* **Na ulaz u kanal biti idu po redosledu i na nekima od njih se jave greške**

$$x_{11}\, x_{21} \ldots \underline{x_{l1}}\, \underline{x_{12}}\, \underline{x_{22}} \ldots x_{l2} \ldots x_{1n}\, x_{2n} \ldots x_{ln}.$$

Deinterliver

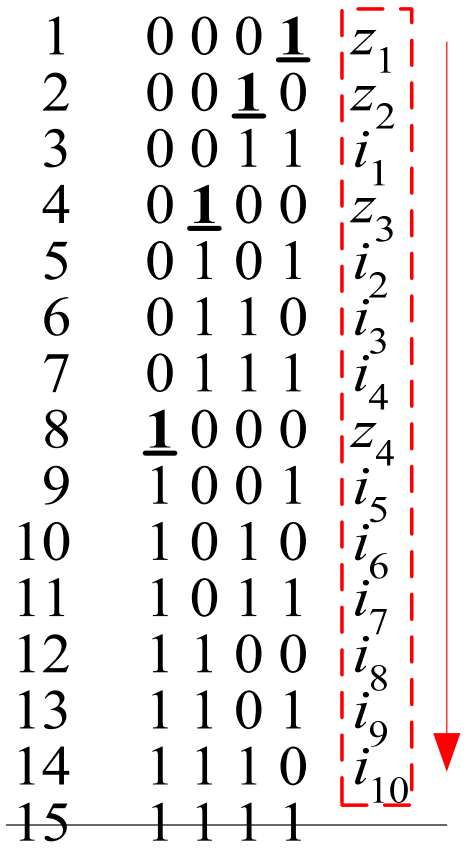
* **Na prijemu se opet formira ceo blok kodnih reči i vrši ispravljanje pojedinačnih grešaka.**
* **Kada se pojavi paket grešaka on će pogoditi sukcesivne bite u kanalu. Međutim, ti biti pripadaju različitim kodnim rečima i ako je paket grešaka kraći od stepena interlivinga u svakoj reči će se pojaviti najviše po jedna greška.**

$$\begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1n} \\ y_{21} & y_{22} & \cdots & y_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ y_{l1} & y_{l2} & \cdots & y_{ln} \end{bmatrix} \rightarrow \begin{matrix} [y_{11} & y_{12} & \cdots & y_{1n}] \\ [y_{21} & y_{22} & \cdots & y_{2n}] \\ & \cdots & & \\ [y_{l1} & y_{l2} & \cdots & y_{ln}] \end{matrix}$$

* **Znači, kod koji ispravlja jednu pojedinačnu grešku u kodnoj reči, uz interliving stepena *l* će moći da**
  - **ispravi paket grešaka čija dužina ne prelazi *l* bita.**
  - **ako je paket duži od *l* bita ili ako se pojavi još neka pojedinačna greška u kodnoj reči koja je već zahvaćena paketom, interliving neće biti uspešan.**

Hemingov kod (14,10) + interliving na pet kodnih reči

* **Šablon**



* **Kontrolne sume**

$$z_1 = i_1 \oplus i_2 \oplus i_4 \oplus i_5 \oplus i_7 \oplus i_9,$$
$$z_2 = i_1 \oplus i_3 \oplus i_4 \oplus i_6 \oplus i_7 \oplus i_{10}$$
$$z_3 = i_2 \oplus i_3 \oplus i_4 \oplus i_8 \oplus i_9 \oplus i_{10}$$
$$z_4 = i_5 \oplus i_6 \oplus i_7 \oplus i_8 \oplus i_9 \oplus i_{10}$$

* **Kodne reci**

[0 1 0 1 0 1 0 1 0 1] -> [0 1 0 0 1 0 1 1 0 1 0 1 0 1]
[0 1 1 1 0 0 0 1 1 1] -> [1 1 0 1 1 1 1 1 0 0 0 1 1 1]
[0 0 1 1 1 1 1 1 0 0] -> [1 0 0 0 0 1 1 0 1 1 1 1 0 0]
[0 0 0 0 0 0 0 0 0 0] -> [0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[1 1 1 1 1 1 1 1 1 1] -> [0 0 1 0 1 1 1 0 1 1 1 1 1 1]

* **Sekvenca na ulazu u kanal**

0 1 1 0 0 1 1 0 0 **0 0 0 0 0** 1 0 1 0 0 0 1 1 0 0 **1** 0 1 1 0 1 1 11 01....
.... 1 1 0 0 0 0 0 1 0 1 1 0 1 0 1 0 0 1 0 1 1 1 1 0 1 0 1 0 0 1 1 1 0 0 1

Deinterliving i dekoder

* **Sekvenca na izlazu iz kanala**

0 1 1 0 0 1 1 0 0 **1 1 1 1 1** 1 0 1 0 0 0 1 1 0 **1** 1 0 1 1 0 1 1 11 01....

.... 1 1 0 0 0 0 0 1 0 1 1 0 1 0 1 0 0 1 0 1 1 1 1 0 1 0 1 0 0 1 1 1 0 0 1

* **Deinterliving**

0 1 **1** 0 1 0 1 1 0 1 0 1 0 1 -> **1. kodna reč**

1 1 **1** 1 1 1 1 1 0 0 0 1 1 1 -> **2. kodna reč**

1 0 **1** 0 0 1 1 0 1 1 1 1 0 0 -> **3. kodna reč**

0 0 **1** 0 **1** 0 0 0 0 0 0 0 0 0 -> **4. kodna reč**

0 **1** 1 0 1 1 1 0 1 1 1 1 1 1 -> **5. kodna reč**

* **Sindromi**
  - $S^{(1)}$=[0011]=3, potiče od impulsne smetnje
  - $S^{(2)}$=[0011]=3, potiče od impulsne smetnje
  - $S^{(3)}$=[0011]=3, potiče od impulsne smetnje
  - $S^{(4)}$=[0011]=**6**, impulsna smetnja + AWGN, ne pokazuje grešku (!)
  - $S^{(5)}$=[0011]=2, potiče od impulsne smetnje

Literatura

[1] C. E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal,* vol. 27, pp. 379-423, July 1948; pp. 623-656, October 1948.

[2] S. Lin, D. J. Costello, *Error Control Coding*, Second Edition, Prentice Hall, New Jersey, 2004.

[3] D. Drajić, P. Ivaniš, “*Uvod u teoriju informacija sa kodovanjem*”, treće izdanje, Akademska misao, Beograd, 2009.

[4] D. J. Costello, Jr., J. Hagenauer, H. Imai, S. B. Wicker, “Applications of Error-Control Coding”, *IEEE Trans. Inform. Theory*. Vol 44 (1998), pp. 2531-2560

[5] R. H. Morelos-Zaragoza, *The Art of Error Correcting Coding*, John Wiley & Sons, Ltd, England, 2002.