Zavod za telekomunikacije

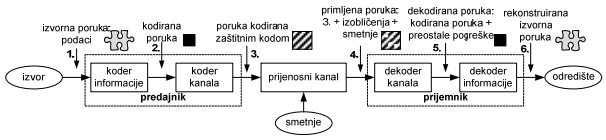
Zaštitno kodiranje I

Teorija informacije

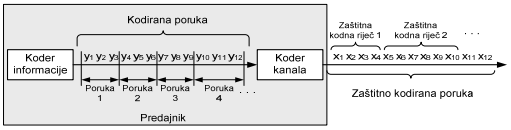
Sadržaj predavanja

- 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

Prijenos informacije komunikacijskim sustavom



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 izabranih 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

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

Kôd K_1 formiran dodavanjem jednog redundantnog simbola

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

Kôd K_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:

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

Blok kod n = 3

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

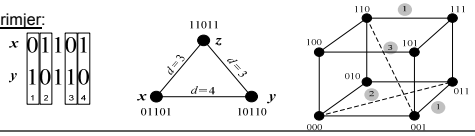
Blok kod n = 5

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 **x** *i* **y** *je d*(**x**, **y**).

- Za kodne riječi i **x**,**y** i **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 $\mathbf{x},\mathbf{y}\in K$;
  - $d(\mathbf{x},\mathbf{y}) \le d(\mathbf{x},\mathbf{z}) + d(\mathbf{z},\mathbf{y})$ za sve $\mathbf{x},\mathbf{y},\mathbf{z}\in K$ (nejednakost trokuta).

- Primjer:



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.*

$$d(K)=\min_{\mathbf{x},\mathbf{y}\in K}\left(d(\mathbf{x},\mathbf{y})\,\middle|\,\mathbf{x}\neq\mathbf{y}\right)$$

OZNAKA BLOK-KODA:

DULJINA KODA → (n, M, d) ← DISTANCA KODA

↑ BROJ KODNIH RIJEČI U KODU

Otkrivanje i ispravljanje pogrešaka (1/2)

- 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)

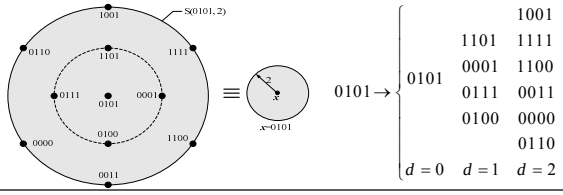
- Ako zaštitni kôd K ima distancu $d(K)$ i ako se dekodiranje provodi principom najbližeg susjeda, onda vrijedi sljedeće:
  - ...
  - Kôd K može ispraviti najviše $\lfloor (d(K)-1)/2 \rfloor$ pogrešaka u jednoj kodnoj riječi, gdje je $\lfloor x \rfloor$ oznaka za najveći cijeli broj manji od x. Drugim 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.

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

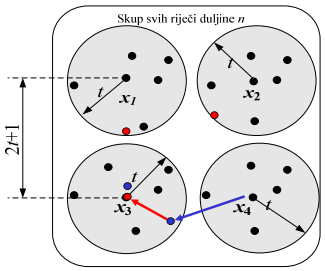
- Primjer: ($\mathbf{x}$ = [0101], Kugla S($\mathbf{x}$, 2))



$$0101 \rightarrow \begin{cases} & & 1001 \\ & 1101 & 1111 \\ 0101 & 0001 & 1100 \\ & 0111 & 0011 \\ & 0100 & 0000 \\ & & 0110 \\ d=0 & d=1 & d=2 \end{cases}$$

Primjer: kugla kodne riječi

- Primjer: Dan je kôd s četiri kodne riječi $\boldsymbol{x}_1$, $\boldsymbol{x}_2$, $\boldsymbol{x}_3$ i $\boldsymbol{x}_4$ 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

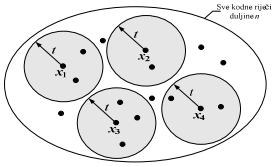
Hammingova međa za $A(n, d)$ i perfektan kôd

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

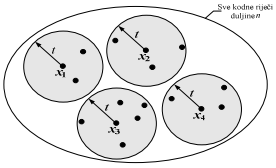
HAMMINGOVA MEĐA (SPHERE-PACKING BOUND)

PERFEKTAN KÔD

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



Neperfektan kôd i ograničenje sfernog pakiranja



Perfektan kôd – sve sfere pokrivaju sve vektore!

Ekvivalencija blok kodova

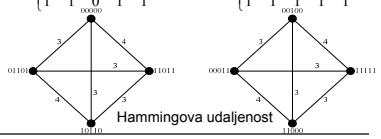
Zavod za telekomunikacije

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 → 1 i 1 → 0) na trećoj poziciji u kodu K_1;
(2) – zamjena pozicija 2 i 4 svih kodnih riječi.

$$K_1 = \begin{Bmatrix} 0&0&0&0&0 \\ 0&1&1&0&1 \\ 1&0&1&1&0 \\ 1&1&0&1&1 \end{Bmatrix} \qquad K_2 = \begin{Bmatrix} 0&0&1&0&0 \\ 0&0&0&1&1 \\ 1&1&0&0&0 \\ 1&1&1&1&1 \end{Bmatrix}$$

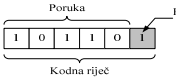


Hammingova udaljenost

Paritetno kodiranje (1/2)

Zavod za telekomunikacije

- 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*).



$$R = x_1 + x_2 + \cdots + x_k \qquad (parni\ paritet),$$
$$R = x_1 + x_2 + \cdots + x_k + 1 \qquad (neparni\ paritet).$$

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

- Primjer: Proračun vjerojatnost neotkrivenih pogrešaka (p_{np}) za parni paritet.

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

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

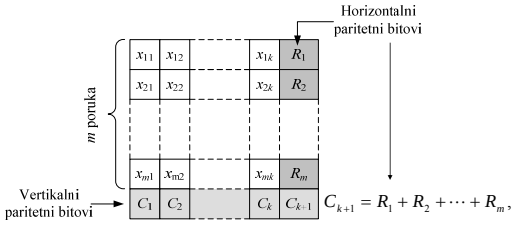
n - duljina kodne riječi; *p* - vjerojatnost pojave pogreške na jednom bitu.

Paritetno kodiranje (2/2)

Zavod za telekomunikacije

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

$$C_i = x_{1i} + x_{2i} + \cdots + x_{mi},\ i = 1, \ldots, k$$



Zavod za telekomunikacije

Linearno binarni blok kodovi

Vektorski prostor: definicija

Zavod za telekomunikacije

- Linearno binarni blok kodovi definiraju se preko skupa vektora (vektorski prostor) nad kojim su definirane određene operacije.
- Kodnu riječ opisujemo binarnim vektorom **x** = [x_1 x_2 … 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:

$$\mathbf{x} + \mathbf{y} = [x_1, x_2, x_3, \ldots, x_n] + [y_1, y_2, y_3, \ldots, y_n] = [x_1 + y_1, x_2 + y_2, x_3 + y_3, \ldots, x_n + y_n],$$

$$a \cdot \mathbf{x} = a \cdot [x_1, x_2, x_3, \ldots, x_n] = [a \cdot x_1, a \cdot x_2, a \cdot x_3, \ldots, a \cdot x_n],$$

a, x_i, y_i su skalari iz F_2; **x**, **y** su vektori iz $V(n)$

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

Definicija: linearni binarni blok kôd

Zavod za telekomunikacije

Linerani binarni blok kôd: *Neka je blok-kôd K potprostor vektorskog prostora V(n): K ⊂ V(n). Neka su* **x** *i* **y** *kodne riječi koda K i neka je a ∈ {0,1}. Ako je za sve* **x** *,* **y** *i a ispunjeno:*
*• **x**+**y** ∈ K,*
*• a·**x** ∈ 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 **0** pripada kodu *K*.
- *Linerani blok kodovi: proračun udaljenosti koda preko težine kodnih riječi.*

Definicija: težina kodne riječi

Zavod za telekomunikacije

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

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

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

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

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

$K: 2^2 \begin{Bmatrix} 000 \\ 011 \\ 101 \\ 110 \end{Bmatrix} \Rightarrow d(K)=2$

Vektorski prostor: baza prostora

Zavod za telekomunikacije

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

$K: 2^2 \begin{Bmatrix} 000 \\ 011 \\ 101 \\ 110 \end{Bmatrix}$ BAZA $\begin{Bmatrix} 011 \\ 101 \end{Bmatrix}$

dimenzija potprostora:

$k = 2$ (broj vektora u bazi)

$M = 2^k$ (broj kodnih riječi)

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

$$[0\ 0\ 0] = 0\,[0\ 1\ 1] + 0\,[1\ 0\ 1] \qquad [1\ 0\ 1] = 0\,[0\ 1\ 1] + 1\,[1\ 0\ 1]$$

$$[0\ 1\ 1] = 1\,[0\ 1\ 1] + 0\,[1\ 0\ 1] \qquad [1\ 1\ 0] = 1\,[0\ 1\ 1] + 1\,[1\ 0\ 1]$$

Definicija: generirajuća matrica G

Zavod za telekomunikacije

- Ako znamo bazu linearnog blok-koda (tj. vektorskog potprostora), onda svaku kodnu riječ možemo izraziti kao linearnu kombinaciju vektora baze:

$$\mathbf{x} = a_1 \cdot \mathbf{b}_1 + a_2 \cdot \mathbf{b}_2 + \ldots + a_k \cdot \mathbf{b}_k$$

- Iz razlga jednostavnosti generiranja kodnih riječi vektore baze stavljamo u matricu.

Generirajuća matrica koda: *Matrica dimenzija k×n čiji se reci sastoje od vektora baze koda* (*n*,*M*,*d*) *se zove generirajuća matrica.* Oznaka **G**.

$K = \begin{Bmatrix} 00000 \\ 11100 \\ 00111 \\ 11011 \end{Bmatrix} \Rightarrow \begin{matrix} M = 4 \\ k = 2 \end{matrix} \Rightarrow \mathbf{G} = \begin{bmatrix} & & & & \end{bmatrix}$

Primjer: generiranje kodnih riječi

Zavod za telekomunikacije

- Binarni kôd K=(5, 4, 3)

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

$$0 \cdot [0\,0\,1\,1\,1] + 0 \cdot [1\,1\,0\,1\,1] = [0\,0\,0\,0\,0]$$
$$0 \cdot [0\,0\,1\,1\,1] + 1 \cdot [1\,1\,0\,1\,1] = [1\,1\,1\,0\,0]$$
$$1 \cdot [0\,0\,1\,1\,1] + 0 \cdot [1\,1\,0\,1\,1] = [0\,0\,1\,1\,1]$$
$$1 \cdot [0\,0\,1\,1\,1] + 1 \cdot [1\,1\,0\,1\,1] = [1\,1\,1\,0\,0]$$

Definicija: oznaka linearnog blok koda

Zavod za telekomunikacije

Oznaka linearnog 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*].

$K = \begin{Bmatrix} 0&0&0&0&0 \\ 1&1&1&0&0 \\ 0&0&1&1&1 \\ 1&1&0&1&1 \end{Bmatrix}$ $M = 4 \Rightarrow k = \log_2(4) = 2 \Rightarrow [5, 2] = (5,4).$

$n = 5$

$d(K) = \min w(\mathbf{x}) = 3 \Rightarrow [5, 2, 3] = (5, 4, 3).$

Generirajuće matrice ekvivalentnih linearnih blok kodova

Zavod za telekomunikacije

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

$K = \begin{Bmatrix} 0&0&0&0 \\ 0&1&0&1 \\ 1&0&1&1 \\ 1&1&1&0 \end{Bmatrix}$ EKVIVALENTAN KÔD $K_e = \begin{Bmatrix} 0&0&1&0 \\ 0&1&1&1 \\ 1&0&0&1 \\ 1&1&0&0 \end{Bmatrix}$

- Ekvivalentan kôd linearnog 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 **G**1 i **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 **G**

***Standardni oblik generirajuće matrice*:** *Generirajuća matrica* **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 **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.

$$[\,0\;1\;0\;1\,] \qquad \mathbf{G} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \qquad [\,1\;0\;1\;1\,]$$

$$+ \quad 0\;1\;0\;0\;1\;0\;1 \qquad\qquad + \quad 0\;1\;1\;0\;0\;1\;1$$

Kodiranje linearnim blok kodovima (2/2)

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

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

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

- 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.

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

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

$$[\,0\,1\,] \cdot \overbrace{\begin{bmatrix} \cdot & \cdot \\ \cdot & \cdot \end{bmatrix}}^{\mathbf{I}_2} = \underbrace{[\,0\,1\,]}_{\text{poruka}} \qquad [\,0\,1\,] \cdot \overbrace{\begin{bmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix}}^{\mathbf{A}} = \underbrace{[\,1\,1\,1\,]}_{\text{zaštitni bitovi}}$$

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

Dekodiranje linearnog blok koda

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

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

- 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 pojmova: vektor pogreške, standardni niz, razred, matrica provjere pariteta i sindrom.

Definicija: vektor pogreške

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

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

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

Zavod za telekomunikacije

- 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 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

$K = \{ 0\,0\,0\,0\,0,\ 0\,1\,1\,0\,0,\ 0\,0\,1\,1\,1,\ 1\,1\,0\,1\,1 \}$

Standardni niz

Primjer: dekodiranje korištenjem standardnog niza (1/2)

Zavod za telekomunikacije

- 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 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: $\mathbf{y} = [\,1\,1\,1\,1\,0\,]$ VEKTOR POGREŠKE: $\mathbf{e} = [\,0\,0\,0\,1\,0\,]$ DEKODIRANO: $\mathbf{x} = [\,1\,1\,1\,0\,0\,]$

Primjer: dekodiranje korištenjem standardnog niza (2/2)

Zavod za telekomunikacije

- 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 **H**.
  - Potrebno je definirati sljedeće pojmove: ortogonalnost, dualni kôd i linearnost 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] × [0 0 1 1 1] = **0**.

Definicija: dualni kôd i njegova linearnost

Zavod za telekomunikacije

Dualni kôd: *Neka su* **x** *vektori koda K* (**x** ∈ *K*). *Skup svih vektora* **y** *vektorskog prostora V*(*n*) *koji su ortogonalni na sve* **x** ∈ *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 **x**·**y** *skalarni produkt vektora u aritmetici modulo 2.*

Linearnost dualnog koda: *Neka je K linearni blok-kôd* [*n*, *k*]. *Dualni kôd koda K je* ***linearan*** *blok-kôd* [*n*, *n* - *k*].

$$K = \begin{Bmatrix} 00000 \\ 11100 \\ 10111 \\ 01011 \end{Bmatrix}, \quad \mathbf{G} = \begin{bmatrix} 10111 \\ 01011 \end{bmatrix} \Rightarrow K^{\perp} = \begin{Bmatrix} 00000 & 01110 \\ 10100 & 01101 \\ 11010 & 00011 \\ 11001 & 10111 \end{Bmatrix}$$

Generirajuće matrice kodova *K* i $K^{\perp}$

Zavod za telekomunikacije

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

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

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

$$\mathbf{x} \cdot \mathbf{H}^{\mathrm{T}} = [\,0\,0 \ldots 0\,]$$

Matrica provjere pariteta koda *K*

Zavod za telekomunikacije

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

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

- Ukoliko je primljena kodna riječ **y** primljena ispravno, onda njenim množenjem s $\mathbf{H}^{\mathrm{T}}$ 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 **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 **H** zbog toga nazivamo MATRICA PROVJERE PARITETA!

Matrica provjere pariteta **H** i njen standardni oblik

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

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

gdje je **B** *kvadratna matrica, onda je paritetna matrica* **H** u **standardnom obliku**.

Proračun matrice provjere pariteta: *Neka je* **G** *generirajuća matrica linearnog binarnog koda K u standardnom obliku*:

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

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

$$\mathbf{H} = \left[\mathbf{A}^{\mathrm{T}} \mid \mathbf{I}_{n-k}\right].$$

Primjer: proračun matrice provjere pariteta **H**

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

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

$$\mathbf{H} = \left[\mathbf{A}^{\mathrm{T}} \,|\, \mathbf{I}_3\right] \quad \Rightarrow \quad \mathbf{H} = \left[\begin{array}{ccc|ccc} 1&1&&1&0&0 \\ 1&0&&0&1&0 \\ 0&1&&0&0&1 \end{array}\right].$$

Primjer: Dekodiranje pomoću matrice provjere pariteta **H**

Primljena kodna riječ $\mathbf{y}=[1\,1\,0\,1\,1]$ ✓

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

Primljena kodna riječ $\mathbf{y}=[1\,0\,0\,1\,1]$?

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

Dekodiraj pomoću standardnog niza!
Rješ: **e** = [0 1 0 0 0] i **x** = [1 1 0 1 1]

Definicija: sindrom

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

$$S(\mathbf{y}) = \mathbf{y}\cdot\mathbf{H}^{\mathrm{T}}.$$

e				S(**y**)
00000	11100	00111	11011	000
00001	11101	00110	11010	001
00010	11110	00101	11001	010
00100	11000	00011	11111	100
01000	10100	01111	10011	101
10000	01100	10111	01011	110

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 $S(\mathbf{y})$ primljene kodne riječi **y**;
- iz tablice preslikavanja odredi vektor pogreške **e**;
- poslana kodna riječ je $\mathbf{x} = \mathbf{y} - \mathbf{e}$.

PRIMLJENO: $\mathbf{y}=[1\,1\,0\,0\,0]$ ⇒ SINDROM: $\mathbf{y}\cdot\mathbf{H}^{\mathrm{T}}=[1\,0\,0]$ ⇒ VEKTOR **e**: $\mathbf{e}=[0\,0\,1\,0\,0]$ ⇒ DEKODIRANO: $\mathbf{x}=\mathbf{y}-\mathbf{e}=[1\,1\,1\,0\,0]$

- 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)

Zavod za telekomunikacije

- 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} → $N_0 = 1$; {00001, 00010, 00100, 01000, 10000} → $N_1 = 5$; $N_2 = N_3 = N_4 = N_5 = 0$.

Vjerojatnost ispravnog dekodiranja (3/3)

Zavod za telekomunikacije

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

Zavod za telekomunikacije

- 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.

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