

# Postupci zaštite od prijenosnih pogrešaka u sustavu GSM-R

---

Petrović, Darko

Professional thesis / Završni specijalistički

2020

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **University of Zagreb, Faculty of Electrical Engineering and Computing / Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva**

*Permanent link / Trajna poveznica:* <https://urn.nsk.hr/urn:nbn:hr:168:718408>

*Rights / Prava:* [In copyright](#)/[Zaštićeno autorskim pravom.](#)

*Download date / Datum preuzimanja:* **2024-07-13**



*Repository / Repozitorij:*

[FER Repository - University of Zagreb Faculty of Electrical Engineering and Computing repository](#)



**SVEUČILIŠTE U ZAGREBU  
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA**

**Darko Petrović**

**POSTUPCI ZAŠTITE OD PRIJENOSNIH  
POGREŠAKA U SUSTAVU GSM-R**

**SPECIJALISTIČKI RAD**

**Zagreb, 2020.**

# SADRŽAJ

1. UVOD.....	1
2. POSTUPCI ZAŠTITNOG KODIRANJA.....	2
2.1. Blok-kodovi.....	4
2.1.1. Linearno binarni blok-kod.....	5
2.1.2. Hammingov kod.....	6
2.1.3. Ciklički kod.....	7
2.1.4. <i>Fire</i> -kod.....	10
2.1.5. BCH kod.....	12
2.2. Konvolucijski kod.....	15
2.2.1. Kodiranje konvolucijskog koda.....	17
2.2.2. Dekodiranje konvolucijskog koda.....	19
2.2.3. Maksimalna vjerojatnost i Viterbijev algoritam.....	20
2.3. Usporedba različitih postupaka kodiranja.....	24
3. ISPREPLITANJE.....	26
4. GSM-R.....	29
4.1. Osobine GSM-R.....	29
4.2. Kodiranje kanala.....	31
5. PRIJENOS PUTEM KOMUNIKACIJSKOG KANALA.....	38
6. ZAKLJUČAK.....	45
7. LITERATURA.....	46
SAŽETAK.....	48
ABSTRACT.....	49
ŽIVOTOPIS.....	50
BIOGRAPHY.....	51

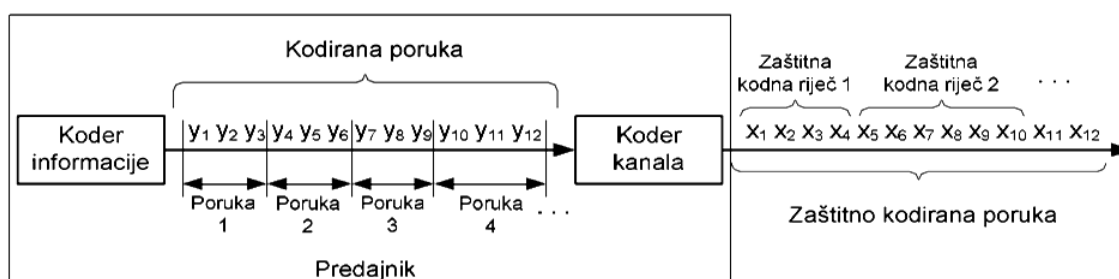
## 1. UVOD

Željeznice su veliki i složeni sustavi. Postupno tijekom godina one se grade, proširuju i nadograđuju novim tehnologijama. Tradicionalnim pristupom svaka država razvija vlastite sustave manje-više neovisno od susjeda. Posljedica, inkompatibilnost različitih sustava i standarda, najviše u komunikacijsko-signalnim tehnologijama. Razlika u tehnologijama glavna je prepreka u međunarodnom prometu vlakova. Kao odgovor započet je rad na Europskom sustavu upravljanja željezničkim prometom ERTMS (*engl. European rail traffic management system*) s ciljem interoperabilnog upravljačko-kontrolnog sustava. ERTMS se sastoji od dva komplementarna sustava, europskog sustava kontrole vlakova ETCS (*engl. European train control system*) i globalnog mobilnog sustava komunikacije za željeznice GSM-R (*engl. global system for mobile communication - railways*). ETCS na temelju komunikacije upravlja i kontrolira kretanje vlaka. Razlikujemo ETCS razinu 1, 2 i 3. ETCS razine 1 komunikaciju obavlja prolaskom vlaka preko eurobalize uz opciju dodatka europetlje slanjem telegrama ili radiokomunikacije. ETCS razine 2 signalizaciju obavlja monitorom u lokomotivskoj kabini. Vlak kontinuirano šalje podatke u radio blok centar GSM-R-om o svom točnom položaju i smjeru. Eurobalize se koriste kao pasivni elementi. ETCS razine 3 je u potpunosti temeljen na radiokomunikaciji, bez ikakve pružne opreme. Radio blok centar prima kontinuirano pozicioniranje svakog vlaka i izračunava najmanju moguću udaljenost vlaka u bilo kojem trenutku. Zbog toga se promet više ne odvaja u fiksnim blokovskim razmacima. Kako sustav GSM-R zahtjeva obavljanje komunikacije s visokim stupnjem pouzdanosti, od velikog je značaja implementacija tehnika za zaštitu od pogrešaka u tom sustavu. Zbog nesavršenosti komunikacijskog kanala (npr. šum, interferencija, fading) u ovom radu posebna pažnja će biti usmjerena na upoznavanje tehnika otkrivanja i ispravljanja prijenosnih pogrešaka u sustavu GSM-R uz opis i analizu modela komunikacijskog kanala.

## 2. POSTUPCI ZAŠTITNOG KODIRANJA

Prijenos informacije od izvora do odredišta s što manje pogrešaka osnovni je zadatak komunikacijskog sustava. Da bi sadržaj informacije bio pogodan za prijenos komunikacijskim kanalom potrebno ju je prikazati kodiranom porukom. Kodiranje poruke je postupak prikazivanja simbola informacije pomoću slijeda simbola kodne abecede  $F_q = \{\lambda_1, \lambda_2, \dots, \lambda_q\}$ . Kodna abeceda obično je binarna  $F_2 = \{0, 1\}$  u praktičnim sustavima. Kodiranje obavlja koder informacije koji sadrži pravilo za prikaz svakog pojedinog slijeda simbola izvora pomoću jedinstvenog slijeda binarnih kodnih riječi i obrnuto dekodiranje obavlja dekodek s pravilima kako da preslika slijed binarnih kodnih riječi u slijed simbola izvora. Kako bi nastale što manje pogreške pri prijenosu informacije, komunikacijski sustav mora osigurati zaštitu kodirane poruke upotrebom zaštitnog kodiranja. Zaštitno kodiranje je postupak dodjeljivanja zaštitnih kodnih riječi simbolima kodirane poruke. Pravilo dodjeljivanja kodnih riječi simbolima kodirane poruke zovemo zaštitni kod. Zaštitne kodove dijelimo u dvije skupine: blok-kodovi (*engl. block codes*) i konvolucijski kodovi (*engl. convolutional codes*) koji se još nazivaju stablasti (*engl. tree*) ili rešetkasti (*engl. trellis*) kodovi. Glavne razlike među navedenim skupinama kodova su načinu izvedbe koder. Koder za blok-kodove spada u grupu koder bez memorije jer je generiranje nekog bita isključivo funkcija trenutnog stanja na ulazu koder. Konvolucijski kodovi spadaju u grupu memorijskih kodova jer je generiranje nekog bita u kodnoj riječi funkcija trenutnog stanja ulaza koder kao i nekoliko njegovih prethodnih stanja. Zaštitne kodove još dijelimo na linearne (*engl. linear*) i nelinearne (*engl. nonlinear*) kodove. U narednim poglavljima ovog rada, fokus opisivanja metode zaštitnog kodiranja je na linearnim zaštitnim kodovima.

Zaštitno kodiranje predstavlja efikasan mehanizam pomoću kojeg možemo omogućiti pouzdan prijenos podataka u otežanim uvjetima prijenosa. Koder informacije formira slijed kodiranih poruka minimalne duljine koje opisuju izlaz izvora informacije. Slijed simbola kodiranih poruka, koder kanala dijeli u fragmente (blokove) koji predstavljaju zaštitnu kodiranu riječ dobivenu dodjeljivanjem redundantnih (kontrolnih) simbola, simbolima kodirane poruke. Slijed zaštitnih kodnih riječi formira zaštitnu kodiranu poruku koju prenosimo komunikacijskim kanalom (slika 2.1)



Slika 2.1 Fragmentiranje kodirane poruke na ulazu u koder kanala i zaštitno kodiranje [12]

Zaštićena kodirana poruka sadrži kontrolne riječi ili simbole veće prosječne duljine od prosječne duljine poruke što omogućava otkrivanje pogreške nastale prijenosom. Otkrivanjem pogreške aktivira se postupak otklanjanja pogreški s pristupom ispravljanja pogreški u dekoderu kanala (*FEC - engl. forward error correction*) ili pristupom ispravljanja pogreški ponovnim slanjem (*BEC - engl. backward error correction*). Kodove za ispravljanje pogrešaka (*engl. error correcting code*) koristimo pri postupku ispravljanja pogreški u dekoderu kanala dok pri postupku ispravljanja pogreški ponovnim slanjem koristimo kodove za otkrivanje pogrešaka (*engl. error detection code*) koji mogu imati i sposobnost otklanjanja pogrešaka. Kvaliteta otkrivanja i otklanjanja pogreški ovisi o broju kontrolnih simbola što gledano sa strane memorijskih medija dovodi do povećanja količine bitova koje snimamo uz nepromijenjenu količinu informacije tj. smanjivanje efektivnog kapaciteta memorije. Gledano sa strane prijenosnog kanala to dovodi do povećanja vremena prijenosa tj. povećanja kašnjenja, a samim tim i smanjivanja efektivnog kapaciteta kanala.

Hammingova udaljenost  $d(x,y)$  je broj pozicija na kojima kodne riječi  $x$  i  $y$  imaju različite simbole. Koristimo je za kodne riječi jednakih duljina i jedno je od važnih svojstva kad govorimo o sposobnosti koda da otkrije ili ispravi pogrešku. Sposobnost koda da otkrije ili ispravi pogrešku ovisi o najmanjoj Hammingovoj udaljenosti svih parova kodnih riječi nekog koda  $K$ . Najmanju Hammingovu udaljenost nazivamo udaljenost koda  $d(K)$  [12],

$$d(K) = \min_{x,y \in K} (d(x,y) | x \neq y) \quad (2-1)$$

Kod  $K$  može otkriti najveći broj pogrešaka ( $s$ ),  $d(K)-1$  u jednoj kodnoj riječi kad zadovolji uvjet  $d(K) \geq s+1$ , dok najviše pogreški može ispraviti ( $t$ ),  $\lfloor (d(K)-1)/2 \rfloor$  u jednoj kodnoj riječi kad zadovolji uvjet  $d(K) \geq 2t+1$ . U svakom binarnom blok-kodu vrijedi da je broj kodnih riječi  $M$  uvijek manji ili jednak  $2^n$ , gdje je  $n$  duljina koda. Zadatak kodiranja je pronaći onaj kod  $K$  duljine  $n$  i najmanje Hammingove udaljenosti  $d(K)$  koji ima najveći broj kodnih riječi  $M$ . Najveći ostvarivi  $M$  označit ćemo s  $A(n,d)$ . Neka je udaljenost koda  $d=2t+1$  pa oko svake od  $M$  kodnih riječi možemo opisati kuglu radijusa  $t$  te prikazati gornju granicu za  $M$ ,

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

koju zovemo Hammingova međa (*engl. Sphere-packing bound*). Kada se svi vektori duljine  $n$  nalaze unutar granice udaljenosti  $2t+1$  govorimo o savršenom kodu za koji vrijedi

$$M = \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{t}} \quad (2-3)$$

Kod  $K$  određuju relativni odnosi pozicija kodnih riječi. Postoje različiti kodovi jednakih Hammingovih udaljenosti, a samim time i jednakih sposobnosti da otkriju i isprave pogreške. Dobiju se jedan iz drugoga postupkom permutacije simbola nad jednim ili više pozicija koda te zamjenom dviju pozicija koda. Takve kodove zovemo ekvivalentni kodovi. Kodnu riječ (blok) koda  $K$  duljine  $n$  moguće je prikazati binarnim vektorom oblika  $x=[x_1 \dots x_n]$  gdje su  $x_i$  skalari

(simboli) iz abecede  $F_2 = \{0,1\}$ . Nad skupom  $F_2$  možemo definirati operacije zbrajanja, množenja u aritmetici modulo-2 i kao takav predstavlja algebarsku strukturu koju zovemo Galoisovo polje.

Binarni blok-kod nazivamo linearni binarni blok kod ako zbrajanjem dvije kodne riječi ili množenjem kodne riječi s skalarom iz abecede dobijemo drugu kodnu riječ unutar istog koda. Skup svih mogućih binarnih vektora  $V(\mathbf{n})$  duljine  $\mathbf{n}$  tj. vektorski prostor od  $2^n$  vektora sadrži linearni blok-kod koji je vektorski potprostor prostora  $V(\mathbf{n})$ . Sve vektore nekog potprostora možemo dobiti linearnom kombinacijom vektora baze definiranim kao  $k$ -vektori baze. Matricu vektora baze dimenzije  $k \times n$  zovemo generirajuća matrica  $\mathbf{G}(\mathbf{n},k)$ .

Cilj poznavanja generirajuće matrice je skraćivanje zapisa linearnog blok-koda i pojednostavljivanje operacija kodiranja i dekodiranja. Svaku generirajuću matricu  $\mathbf{G}$  možemo operacijama zamjene redaka, zamjene stupaca i dodavanja jednog retka drugom svesti po strukturi u jednostavniji ekvivalentni oblik tj. standardni oblik generirajuće matrice  $[\mathbf{I}_k | \mathbf{A}]$  gdje je  $\mathbf{I}_k$  jedinična matrica reda  $k$ , a  $\mathbf{A}$  matrica dimenzija  $k \times (n-k)$ . Pogledamo li kod  $\mathbf{K}^\perp$  čije su kodne riječi ortogonalne na kodne riječi koda  $\mathbf{K}$ , skalarni umnožak svih vektora kodnih riječi iz koda  $\mathbf{K}$  i jednak je nuli. Kod  $\mathbf{K}^\perp$  zovemo dualni kod koji ima svoju generirajuću matricu  $\mathbf{H}$ , a jednaka je

$$\mathbf{H} = [\mathbf{A}^T | \mathbf{I}_{n-k}] \quad (2-4)$$

Množenjem poruke s generirajućom matricom  $\mathbf{G}$  dobivamo kodnu riječ koja se sastoji od originalne poruke i zalihosnih bitova. Množenjem ove kodne riječi s transportiranom matricom matrice  $\mathbf{H}$  dobivamo vektor  $\mathbf{0}$  što potvrđuje ispravnu kodnu riječ. Matrica  $\mathbf{H}$  svojim jedinicama unutar svakog retka određuje pozicije unutar ispravne kodne riječi na kojima zbroj vrijednosti gledano aritmetikom modulo-2 mora biti jednak nuli tj. parnim paritetom štiti zalihosni bit. Zalihosni bitovi predstavljaju bitove za provjeru pariteta za odabrane pozicije unutar originalne poruke i zbog tog svojstva matricu  $\mathbf{H}$  zovemo matrica provjere pariteta. Sindrom  $\mathbf{S}(\mathbf{y})$  je vektor koji dobijemo množenjem primljene kodne riječi i transponirane matrice provjere pariteta

$$\mathbf{S}(\mathbf{y}) = \mathbf{y} \cdot \mathbf{H}^T \quad (2-5)$$

Sindrom omogućuje da složenost dekodiranja jedne kodne riječi svedemo na razinu  $\mathcal{O}(1)$ .

## 2.1 Blok-kodovi

Zadatak koda kanala je da skup  $m$ -komponentnih vektora  $\mathbf{v} = (a_1, a_2, \dots, a_m)$  čije su vrijednosti uzete iz polja (abecede)  $F_q$  s  $q$  elemenata pretvori u  $n$ -komponentne vektore u kojima je dodana redundancija za kontrolu pogrešaka. Za zadane vrijednosti  $n$  i  $q$  postoji veliki broj mogućih  $m$ -dimenzionalnih potprostora u skupu  $n$ -torki. Budući da je takav potprostor određen s  $m$ -linearno neovisnih vektora može se tvrditi slijedeće: za bazu potprostora konkurira svaki vektor izuzev nul-vektora, što je ukupno  $q^n - 1$  vektora. Za svaki odabrani vektor postoji  $q^n - q$  linearno neovisnih vektora (jer je točno  $q$  vektora koji su linearno ovisni o odabranom vektoru). Odabrana grupa od  $k$  linearno neovisnih vektora generira potprostor dimenzije  $k$ , koji ukupno sadrži  $q^k$  vektora. Broj linearno neovisnih vektora je  $q^n - q^k$ .

Proizlazi da je moguće odabrati

$$(q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{m-1}) \quad (2-6)$$

različitih  $m$  linearno neovisnih vektora. Svaki  $m$ -dimenzionalni prostor ima

$$(q^m - 1)(q^m - q)(q^m - q^2) \dots (q^m - q^{m-1}) \quad (2-7)$$

uređenih grupa od  $m$  linearno neovisnih vektora pa je ukupan broj  $m$ -dimenzionalnih potprostora u skupu  $n$ -torki:

$$K = \frac{(q^n - 1)(q^{n-1} - 1) \dots (q^{n-m+1} - 1)}{(q^m - 1)(q^{m-1} - 1) \dots (q - 1)} \quad (2-8)$$

Broj mogućih potprostora je proporcionalan razlici  $n$  i  $m$ . Kako bi uz određeni kapacitet kanala osigurali maksimalnu sigurnost prijenosa moramo odabrati takvu bazu  $m$ -dimenzionalnog potprostora unutar prostora  $X^n(\mathbf{F})$  koja ima maksimalnu Hammingovu udaljenost koju zbog jednostavnosti određujemo preko Hammingove težine  $w(\mathbf{K})$  pojedinih kodnih grupa  $x$  tj. broja jedinica unutar kodne riječi. Određivanje udaljenosti nekog koda  $\mathbf{K}$  svodi se na određivanje težine tog potprostora, koja odgovara najlakšoj kodnoj grupi izuzev vektora 00..0

$$d(K) = w(K) \quad (2-9)$$

Hammingova težina definirana je relacijom

$$w(K) = \min\{w(x) : x \in K, x \neq \mathbf{0}\} . \quad (2-10)$$

### 2.1.1 Linearni binarni blok-kod

Generirajuća matrica je matrica čiji redci odgovaraju bazi vektorskog potprostora prostora  $V(\mathbf{n})$ . Stoga se bilo koja kodna riječ može dobiti kao linearna kombinacija vektora baze.

Kodiranje poruke možemo provesti tako da bitovi poruke budu koeficijenti za linearnu kombinaciju vektora baze. Generiranje zaštite kodne riječi  $x$  za poruku  $m$  svodimo na umnožak vektora retka poruke i vektora  $r$  generirajuće matrice s složenošću kodiranja poruke  $O(\mathbf{n} \cdot \mathbf{k})$ :



$$\mathbf{x} = \sum_{i=1}^k (\mathbf{m}_i \cdot \mathbf{r}_i) = \sum_{i=1}^k [\mathbf{m}_i r_{i1}, \dots, \mathbf{m}_i r_{ik}] = \mathbf{m} \cdot \mathbf{G} \quad (2-11)$$

Možemo koristiti i standardni oblik generirajuće matrice kako bi smanjili složenost kodiranja. Standardni oblik generirajuće matrice generira tzv. sustavni linearni  $(n, m)$ -kod kod kojeg se kodna riječ sastoji iz dva dijela. Prvih  $k$  pozicija su informacijski, a ostalih  $(n-k)$  pozicija kontrolni simboli tj. umnožak  $\mathbf{m} \cdot \mathbf{A}$ . Složenost kodiranja postaje  $O(n \cdot k - k^2)$ .

Dekodiranje obavljamo preko sindroma ili korektora primljene kodne riječi. Sindrom je vektor dobiven umnoškom primljene kodne riječi i transponirane generirajuće matrice dualnog koda. Zbroj ili razlika primljenog  $\mathbf{y}$  i poslanog  $\mathbf{x}$  vektora definiramo kao vektor pogreške  $\mathbf{e}$

$$\mathbf{e} = \mathbf{y} + \mathbf{x} = [\mathbf{e}_1 \mathbf{e}_2 \dots \mathbf{e}_n] . \quad (2-12)$$

Prije dekodiranja formira se standardni niz tj. tablica svih vektora koje dekoder može primiti. U tablici definiramo razrede skupa kodnih riječi. Svaki razred koda  $\mathbf{K}$  je blok-kod nastao dodavanjem nekog vektora pogreške svim vektorima kodnih riječi i sadrži potpuno različite vektore. Standardni niz koda  $\mathbf{K}$  je tablica koja u prvom retku sadrži kodne riječi s tim da je prva kodna riječ  $\mathbf{0}$ . Osobina brzog dekodiranja linearnih blok-kodova preko sindroma je da vektori istog razreda imaju isti sindrom. Za određivanje sindroma jednog retka standardnog niza izračunamo sindrom vodećeg člana retka, vektora pogreške  $\mathbf{e}$  što znači da postoji preslikavanje jedan-na-jedan između vektora pogreške i sindroma. Postupak dekodiranja možemo opisati na slijedeći način: izračunati sindrom primljene kodne riječi  $\mathbf{y}$ , iz tablice preslikavanja odrediti vektor pogreške  $\mathbf{e}$ , kodna riječ je razlika između primljenog vektora i vektora pogreške.

## 2.1.2 Hammingov kod

Hammingov kod je linearni blok-kod  $[2^r-1, 2^r-1-r]$  čija matrica provjere pariteta  $\mathbf{H}$  dimenzije  $r \times (2^r-1)$  ima  $r$  (broj pogrešaka) redaka, a u stupcima ima sve moguće vektore dimenzije  $r$  različitih od nule koji predstavljaju binarne ekvivalente dekadskih brojeva od 1 do  $2^r-1$ . Ima najmanju udaljenost 3 (otkriva dvostruku i ispravlja jednostruku pogrešku) i savršen je kod jer se svaka  $n$ -torka (kodna riječ) nalazi u sferi radijusa 1. Kod koji može korigirati  $r$  pogrešaka i za svaku kodnu riječ dužine  $n$  ima samo jednu kodnu grupu dužine  $n$ , za koju je Hammingova udaljenost  $d \leq r$ , zovemo savršen kod. Kodiranje Hammingovim kodom definiramo množenjem poruke generirajućom matricom  $\mathbf{G}$  dobivenom iz matrice provjere pariteta  $\mathbf{H}$  slijedećim postupcima: u matrici  $\mathbf{H}$  izbrisati sve stupce koji se nalaze na pozicijama s indeksom jednakim potenciji broja 2, zatim dobivenu matricu transponirati, stupce dobivene matrice smjestiti na pozicije generirajuće matrice  $\mathbf{G}$  čiji indeksi odgovaraju potencijama broja 2, a ostale stupce popuniti redom stupcima jedinične matrice. Potvrda ispravnosti matrice  $\mathbf{G}$  je rezultat u obliku nul-matrice ako je pomnožimo s transponiranom matricom provjere pariteta. Dekodiranje, uz pretpostavku jednostruke pogreške na  $i$ -tom bitu primljene kodne riječi, svodimo na postupak izračunavanja sindroma  $\mathbf{S}(\mathbf{y})$  primljene kodne riječi  $\mathbf{y}$  preko  $\mathbf{H}$ . Ako je  $\mathbf{S}(\mathbf{y}) \neq \mathbf{0}$  potrebno je invertirati bit na poziciji koja odgovara decimalnom ekvivalentu sindroma. Zbog posljedice savršenosti koda kodna riječ ima sindrom jednostruke pogreške.

### 2.1.3 Ciklički kod

Ciklički kodovi su podklasa linearnih blok-kodova koje karakterizira ciklička struktura. Njihova važnost proizlazi uglavnom iz dva razloga:

- kodiranje i dekodiranje mogu biti elegantnije riješeni jer se generirajuća matrica i matrica pariteta ne trebaju prikazati tablicom, nego mogu biti generirane preko algoritma;
- uz isti broj korekcija, ciklički kodovi mogu biti generirani uz značajno manju zalihost.

Koriste se prilikom prijenosa velikih blokova podataka smanjujući prostor za zaglavlje, adresiranje i sinkronizaciju, a učinkovito rješavaju kontrolu pogrešaka. Osobina cikličkih kodova je da se cikličkim pomicanjem jedne kodne riječi uvijek dobiva neka kodna riječ iz istog cikličkog koda. Cikličko pomicanje kodne riječi  $[a_{n-1} a_{n-2} \dots a_2 a_1 a_0]$  je promjena pozicija simbola u kodnoj riječi kako bi dobili kodnu riječ  $[a_{n-2} \dots a_2 a_1 a_0 a_{n-1}]$  pomakom u lijevo, odnosno  $[a_0 a_{n-1} a_{n-2} \dots a_2 a_1]$  pomakom u desno. Ciklički kod je takav da kodnu riječ  $[a_{n-1} a_{n-2} \dots a_2 a_1 a_0]$  možemo prikazati polinomom stupnja  $n - 1$ :

$$\begin{aligned} a &= [a_{n-1} a_{n-2} \dots a_2 a_1 a_0] \leftrightarrow a(x) \\ &= a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_2x^2 + a_1x^1 + a_0x^0 \quad (2-13) \end{aligned}$$

gdje su  $a_i \in \{0,1\}$ , a operacije se provode u aritmetici modulo-2. Polinom  $a(x)$  služi samo kao povoljnije sredstvo zapisa kodne riječi od vektora simbola. Polinom  $a(x)$  ne promatramo kao funkciju čiji argumenti  $x$  mogu poprimiti neku konkretnu vrijednost, nego kao sredstvo zapisa kodne riječi. Zapis kodne riječi od vektora simbola prikazujemo polinomom stupnja  $n - 1$ . Postupak pomicanja polinoma  $a(x)$  reda  $n - 1$  duljine  $n$  za  $m$  pozicija u lijevo obavljamo množenjem polinoma  $a(x)$  s  $x^m$ , a potom izračunamo ostatak dijeljenja polinomom  $x^n - 1$  u aritmetici modulo-2. S obzirom da pomicanjem bilo koje kodne riječi cikličkog koda moramo opet dobiti kodnu riječ koda, polinomi svih kodnih riječi moraju biti u aritmetici modulo- $(x^n - 1)$ . Skup svih polinoma  $F[x] = a(x) : a(x) \pmod{(x^n - 1)}$  označimo s  $R_n$ . Prikazivanjem kodne riječi polinomom, ciklički kod  $K$  je neki podskup  $R_n$ ,  $K \subset R_n$ . Kod  $K \subset R_n$  je ciklički kod ako i samo ako  $K$  ispunjava slijedeće uvjete:

- $\forall a(x), b(x) \in K \Rightarrow a(x) + b(x) \in K$ ,
- $\forall a(x) \in K \text{ i } \forall r(x) \in R_n \Rightarrow r(x) \cdot a(x) \pmod{(x^n - 1)} \in K$ .

Prvo svojstvo odgovara svojstvu linearnosti. Drugo svojstvo govori da rezultat umnoška polinoma koda  $K$  s polinomom iz skupa  $R_n$  je polinom odnosno kodna riječ iz skupa  $K$ . Kažemo da je ciklički kod zatvoren s obzirom na množenje s bilo kojim polinomom iz  $R_n$ . S obzirom da su svi polinomi  $a(x)$  u skupu  $R_n$  proizlazi jednostavan algoritam za generiranje cikličkog koda duljine kodne riječi  $n$ :

- izaberi bilo koji polinom  $f(x)$  najvećeg stupnja  $n - 1$ ,
- sve kodne riječi cikličkog koda  $K$  dobit ćemo množenjem svih  $r(x) \in R_n$  s  $f(x)$ .

$f(x)$  je element koda  $K$  i kaže se da je kod  $K$  generiran polinomom  $f(x)$ , s oznakom

$$K \equiv \langle f(x) \rangle = \{r(x)f(x) | r(x) \in R_n\} \quad (2-14)$$

Generiranje kodnih riječi cikličnog koda duljine  $n$  obavljamo postupkom izbora bilo kojeg polinoma  $f(x)$  najvećeg stupnja  $n - 1$  i množenjem svih mogućih polinoma  $r(x)$  kojih ima  $2^n$  u skupu  $R_n$  s  $f(x)$  u aritmetici modulo- $(x^n - 1)$ . Zbog velikog broja riječi i složenosti generiranja uvodimo generirajući polinom  $g(x)$  koji određuje kod. Generirajući polinom  $g(x)$  je faktor polinoma  $x^n - 1$ , a stupanj  $r$  je jednak broju zaštitnih bitova koda. Polinom najmanjeg stupnja cikličkog koda  $K$  zove se generirajući polinom cikličkog koda  $K$ ,

$$g(x) = g_r x^r + \dots + g_2 x^2 + g_1 x + g_0 \quad (2-15)$$

Dimenzija koda je  $k = n - r$ , a generirajuću matricu koda opisujemo:

$$G = \begin{bmatrix} g_r & g_{r-1} & g_{r-2} & \dots & g_1 & g_0 & 0 & 0 & \dots & 0 \\ 0 & g_r & g_{r-1} & g_{r-2} & \dots & g_1 & g_0 & 0 & \dots & 0 \\ 0 & 0 & g_r & g_{r-1} & g_{r-2} & \dots & g_1 & g_0 & \vdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & g_r & g_{r-1} & g_{r-2} & \dots & g_1 & g_0 \end{bmatrix} \quad (2-16)$$

Kodiranje cikličnih kodova dijelimo na sistematsko i nesistematsko kodiranje. Razlika je u tome što kod nesistematskog kodiranja kodnu riječ prikazujemo ispremiješanim bitovima poruke i redundancije, a kod sistematskog kodnu riječ prikazujemo redom od najznačajnijih prema najmanje značajnim bitovima i to prvo poruka, a nakon nje redundancija koju nazivamo ciklička provjera zalihosti (*engl. cyclic redundancy check - CRC*). Kodnu riječ  $c(x)$  kod nesistematskog kodiranja dobijemo umnoškom polinoma koji opisuje poruku  $d(x)$  i generirajućeg polinoma

$$c(x) = d(x) \cdot g(x) \quad (2-17)$$

Kodnu riječ (slika 2.2) sistematskog kodiranja dobijemo množenjem poruke  $d(x)$  polinomom  $x^r$ . Umnožak  $d(x) \cdot x^r$  podijelimo s generirajućim polinomom  $g(x)$  da dobijemo polinom  $r(x)$  kojeg dodamo umnošku [12]:

$$c(x) = d(x) \cdot x^r + r(x) \quad (2-18)$$

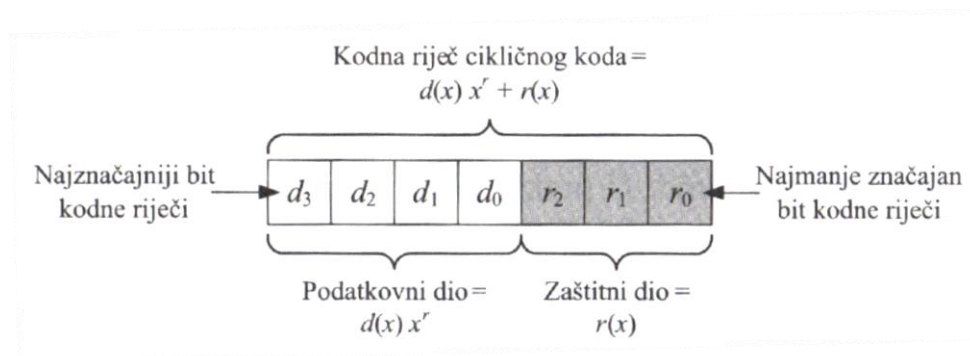
$$r(x) = d(x) \cdot x^r \text{ mod } [g(x)] \quad (2-19)$$

$$x^n - 1 = g(x)h(x) \quad (2-20)$$

$$h(x) = h_k x^k + \dots + h_2 x^2 + h_1 x + h_0 \quad (2-21)$$

$$H = \begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k & 0 & 0 & \cdots & 0 \\ 0 & h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k & 0 & \cdots & 0 \\ 0 & 0 & h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k & \vdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k \end{bmatrix} \quad (2-22)$$

Ciklički kod je linearni blok-kod koji cikličkim promjenama pozicija simbola (lijevo ili desno) jedne kodne riječi daje drugu kodnu riječ iz istog cikličkog koda. Polinomi u aritmetici modulo- $(x^n-1)$  su polinomi dobiveni dijeljenjem polinoma proizvoljnog stupnja s polinomom  $x^n-1$ , a za ostatak pri dijeljenju daju same sebe. Oznaka polinoma  $a(x)$  u aritmetici modulo- $(x^n-1)$  je  $a(x)(\text{mod}(x^n-1))$ , a skup svih polinoma s  $R_n$ .



Sl.2.2 Struktura sistematske kodne riječi [12]

Dekodiranje obavljamo preko sindroma primljene kodne riječi  $S[y(x)]$ . Primljenu kodnu riječ  $y(x)$  definiramo kao poslanu kodnu riječ  $c(x)$  kojoj je dodan polinom pogreške  $e(x)$ . Sindrom možemo dobiti množenjem paritetnim polinomom  $h(x)$  ili preko identičnog računanja zašitnog dijela ciklične kodne riječi

$$S[y(x)] = x^r \cdot y(x) \text{mod} g(x) \quad (2-23)$$

Polinom sindroma ovisi o polinomu pogreške a ne i o polinomu kodne riječi u kojoj se nalazi pogreška. Iz tablice pridruživanja polinoma sindroma polinomima pogreške dekođer odredi poziciju pogreške.

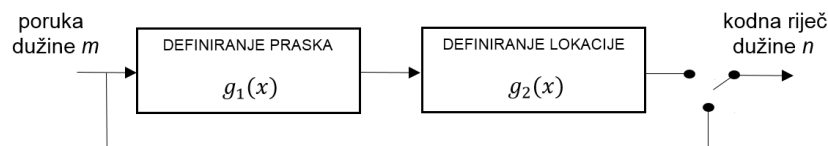
## 2.1.4 Fire-kod

Povećanje efikasnosti cikličkog koda u cilju korekcije skupnih pogrešaka možemo postići primjenom *Fire*-koda. *Fire*-kod nam služi za korekciju jednog praska s do  $r$  pogrešaka po svakoj kodnoj riječi. Konceptija *Fire*-koda temelji se na činjenici da se postupak detekcije i korekcije skupnih pogrešaka može razdvojiti u dva dijela:

- određivanje strukture praska preko sindroma,
- određivanje lokacije pogreške.

*Fire*-koder možemo opisati kaskadom dva registra (slika 2.3) od kojih svaki unosi određenu redundanciju potrebnu za definiranje praska i njegove lokacije, odnosno generirajući polinom opisujemo kao umnožak pojedinačnih polinoma koji osiguravaju detekciju i korekciju jedne praskave pogreške dužine  $r$  po kodnoj riječi [11]:

$$g(x) = g_1(x) \cdot g_2(x) . \quad (2-24)$$



Sl.2.3 Blok shema *Fire*-kodera [11]

Stupanj polinoma  $g_1(x)$  određuje dužinu skupne pogreške koji možemo ispraviti, a stupanj  $g_2(x)$  dopuštenu vjerojatnost da pogreška bude nedetektirana.

### Određivanje strukture skupne pogreške

U standardnom CRC kodu, strukturu praska (slika 2.4) određujemo zadnjim korakom kada simultano odredimo i lokaciju pogreške pri čemu je uvjet izvršavanja detekcije i korekcije praska dužine  $r$  bio  $n - m \geq 2r$  odnosno broj kontrolnih simbola je minimalno  $2r$ . Ako želimo kod koji samo određuje strukturu praska bez lokacije dovoljno je uzeti broj kontrolnih simbola  $c = 2r - 1$ .

Ciklički kod dobiven generirajućim polinomom oblika:

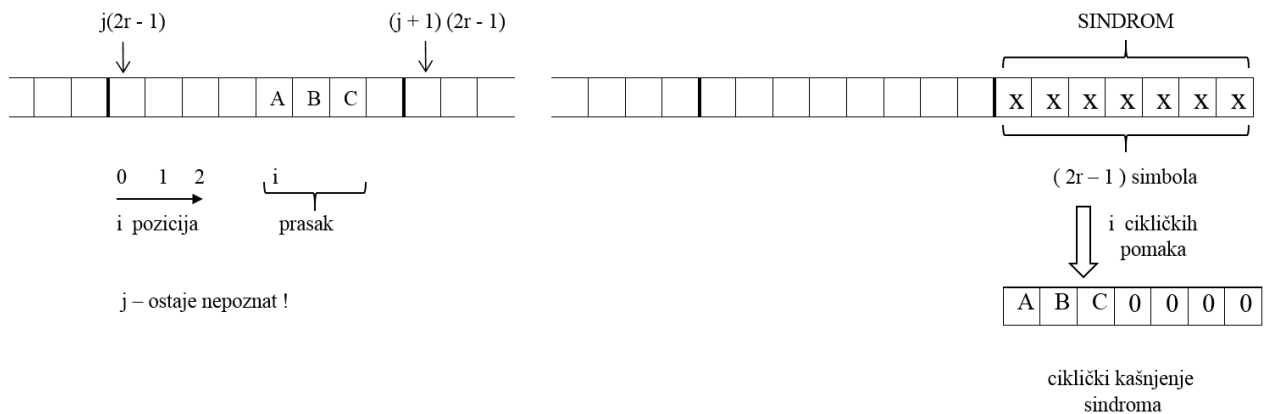
$$g_1(x) = 1 + x^{2r-1} \quad (2-25)$$

ima slijedeća svojstva:

- sindrom  $s(x) = \text{rem}[y(x)/g_1(x)]$  ima strukturu cikličkog praska pogrešaka ako je kontrolni broj simbola  $c_1 = 2r - 1$ ,
- cikličkim kašnjenjem sindroma (udesno) može se dobiti barem  $r - 1$  nula na kraju vektora  $s$  sa  $2r - 1$  elemenata (najmanje značajni simboli), tako da je dužina praska jednaka najviše  $r$  i on jednoznačno predstavlja strukturu praskave pogreške,
- broj cikličkih pomaka da u sindromu sa  $c_1 = 2r - 1$  simbola dobijemo barem  $r - 1$  nula na desnom kraju određuje poziciju početka praska  $s$  obzirom na neki od  $j \cdot (2r - 1)$  simbola u kodnoj riječi,
- veličina  $j$  ostaje nepoznata. To je problem lokacije praska kod *Fire*-koda koji rješava drugi registar, a posljedica je korištenja generirajućeg polinoma oblika:

$$g_1(x) = 1 + x^{c_1} \quad (2-26)$$

koji je reducibilan i ima dužinu perioda od  $c_1$  te kontrolira položaj praska samo do razine grupa od  $c_1$  simbola.



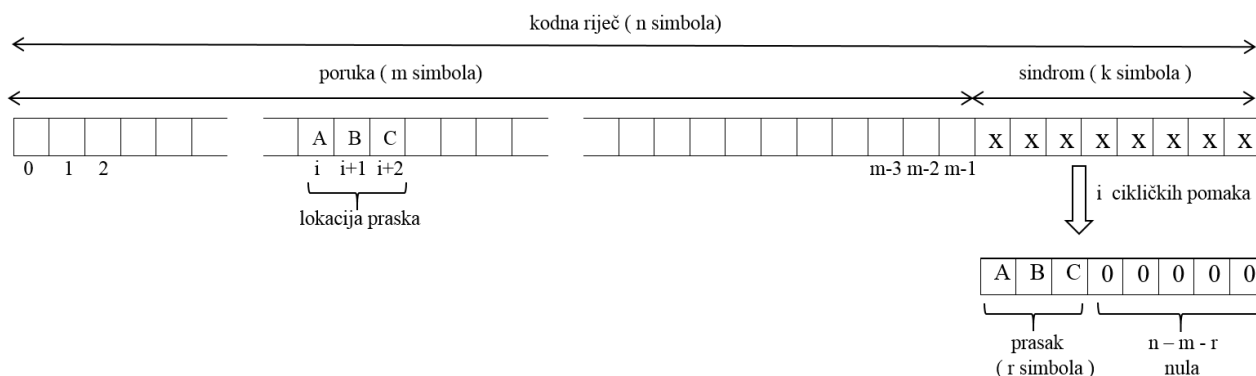
#### Sl.2.4 Prikaz određivanja strukture skupne pogreške [11]

Po prijemu bloka podataka od  $n$  podataka ( kodna riječ), proračunati sindrom sadrži ciklički prask čija točna struktura proizlazi iz ciklički kašnjenog sindroma za koji vrijedi da ima barem  $r - 1$  nulu na desnom kraju.

#### Određivanje lokacije skupne pogreške

Za određivanje lokacije praska (slika 2.5), *Fire*-kod koristi standardni ciklički kod generiran jednim od ireducibilnih polinoma stupnja  $c_2$ , a time i dodatnih  $c_2$  redundantnih simbola odnosno ukupan broj simbola u kontrolnom vektoru je:

$$c = c_1 + c_2 = (2r - 1) + c_2 \quad (2-27)$$



Sl.2.5 Struktura praska i moguća lokacija skupne pogreške [11]

## 2.1.5 BCH kod

BCH (*engl. Bose-Chaudhuri-Hocquenghem*) kodovi su klasa cikličkih kodova za otkrivanje i ispravljanje višestrukih pogrešaka. Standardni ciklički  $(n, m)$  kod generiran je polinomom  $g(x)$  stupnja  $(n-m)$  koji je jedan od mogućih ireducibilnih faktora od polinoma  $x^n - 1$ . Za određenu dužinu bloka poruke  $m$  i izborom ukupne dužine kodne riječi  $n$  bira se samo broj kontrolnih simbola  $r = n - m$  koji govore o unesenoj redundanciji ali ne i o stvarnoj sposobnosti generiranog  $(n, m)$  cikličkog koda da detektira i korigira pogreške. Kako bi povezali generirajući polinom i najveću, odnosno željenu Hammingovu udaljenost nad Galoisovim poljem  $GF(q)$  uz isti broj kontrolnih simbola kodove prikazujemo preko nula  $\alpha$  generirajućeg (ireducibilni) polinoma. Ireducibilni polinom definiran nad poljem  $GF(q)$  nema nula  $\alpha^j$  u polju  $GF(q)$ , ali zato ima u proširenom polju  $GF(2^m)$ . Red polja je  $2^m$  gdje je  $m$  stupanj ireducibilnog polinoma. Članove polja  $GF(2^m)$  prikazujemo kao ostatke pri dijeljenju potencije  $\alpha^j$  ( $j=1, 2, \dots, 2^m-1$ ), a za potencije veće od  $2^m-1$  koristimo jednakost  $\alpha^j = \alpha^{j \bmod (2^m-1)}$ . Cikličke kodove generiramo ireducibilnim polinomima stupnja  $n-m$  ili s najmanjim umnoškom minimalnih polinoma. Generirajući polinom BCH koda s udaljenošću  $t$  moguće je faktorizirati i polinom ima strukturu

$$g(x) = m_1(x) \cdot m_3(x) \cdots m_{2t-1} \quad (2-28)$$

gdje su  $m_i(x)$  minimalni polinomi. Indeks  $i$  minimalnog polinoma dolazi od potencije nule  $\alpha$  čiji je on minimalni polinom. Neka je  $b$  član  $GF(2^m) = F[x] / f(x)$  gdje je  $F[x]$  skup svih polinoma, a  $f(x)$  ireducibilni polinom. Minimalni polinom elementa  $b$  polja  $F[x] / f(x)$  je onaj ireducibilni polinom najmanjeg mogućeg stupnja za koji vrijedi  $m(b) = 0$ . Ako promatramo

polje  $F[x]/f(x)$  generirano polinomom  $f(x)$ , onda je  $f(x)$  minimalni polinom svojih nula  $\alpha, \alpha^2, \alpha^4, \dots, \alpha^z$  ( $z = 2^{m-1}$ ) i njihovih konjugacija. Važno svojstvo nule  $\alpha$  je da za  $GF(2^m)$  vrijedi:

$$x^{2^m-1} - 1 = \prod_{j=0}^{2^m-1} (x - \alpha^j) \quad (2-29)$$

S jedne strane polinome možemo faktorizirati u polinome stupnja jedan koji imaju nule  $\alpha, \dots, \alpha^j$  a s druge strane u niz ireducibilnih polinoma. Stoga je svaki od  $\alpha, \dots, \alpha^j$  nula jednog od ireducibilnih faktora. Faktor koji je nula elementa polja  $\alpha^j$  je ujedno i minimalni polinom elementa  $\alpha^j$ . Zbog potrebe za faktorizacijom polinoma velikog stupnja koristimo različite postupke određivanja koeficijenata minimalnih polinoma. Stupanj minimalnog polinoma nam govori koliko nula ima taj polinom, a indeks potenciju nule. Ovisno o stupnju ireducibilnog polinoma ispišemo polinom s koeficijentima pazeći da koeficijent uz komponentu najvećeg stupnja i komponenta najmanjeg stupnja budu jednaki jedinici. Na primjer, minimalni polinom  $m_5(x)$  je trećeg stupnja pišemo:

$$m_5(\alpha^5) = (\alpha^5)^3 + a_2(\alpha^5)^2 + a_1(\alpha^5) + (\alpha^5)^0 = 0. \quad (2-30)$$

Kkoristeći članove polja  $\alpha^5$  određujemo minimalni polinom za elemente  $\alpha^{15}, \alpha^{10}$  i  $\alpha^5$ .

Posebna klasa BCH kodova za koju je jednostavno ustanoviti udaljenost koda je klasa primitivnih BCH kodova. Neka je  $m_1(x)$  ireducibilni polinom stupnja  $m$  s koeficijentima  $\{0,1\}$ , a  $\alpha$  element polja  $F[x] / m_1(x) = GF(2^m)$  koji je ujedno i nula polinoma  $m_1(x)$ . Ukoliko se svi elementi polja  $GF(2^m)$  mogu dobiti kao ostatak pri dijeljenju  $\alpha^i \bmod m_1(x)$ , onda se kaže da je  $\alpha$  primitivan element polja  $GF(2^m)$ , a  $m_1(x)$  primitivan polinom. Neka je  $m_1(x)$  primitivan polinom stupnja  $m$ , a  $m_i(x)$  minimalni polinom elementa  $\alpha^i$  polja  $GF(2^m)$ , gdje je  $\alpha$  nula polinoma  $m_1(x)$  BCH kod s generirajućim polinomom

$$g(x) = m_1(x) \cdot m_3(x) \cdot m_5(x) \cdot m_7(x) \cdots m_{2^t-1}(x) \quad (2-31)$$

je primitivan BCH kod. Duljina kodne riječi je  $n=2^m - 1$ . Stupanj generirajućeg polinoma  $g(x)$  je manji li jednak  $m \cdot t$ , a dimenzija  $k \geq 2^m - 1 - m \cdot t$ . Udaljenost primitivnog BCH koda je  $d(K) \geq 2 \cdot t + 1$ .

Kodiranu poruku prikazujemo kao umnožak polinomskog zapisa poruke  $d(x)$  i  $x^r$  gdje je  $r$  stupanj generirajućeg polinoma  $g(x)$  i dodajući tom umnošku redundantne simbole koje dobijemo kao ostatak pri dijeljenju umnoška  $d(x) \cdot x^r$  s generirajućim polinomom  $g(x)$ . Generirajući polinom određujemo ovisno o stupnju kodirane poruke kako bi odredili stupanj primitivnog polinoma  $m$  iz izraza  $n=2^m - 1$ . S obzirom koliko kod mora biti sposoban ispraviti pogrešaka određujemo strukturu generirajućeg polinoma i pripadajuće nule  $\alpha^i$ , faktora generirajućeg polinoma ovisno o indeksu  $m_i(x)$ . Odredimo koeficijente faktora generirajućeg



polinoma uvrštavajući članove  $\alpha^i$  polja  $GF(2^m)$  i množenjem minimalnih polinoma odredimo stupanj  $g(x)$ . Možemo i jednostavnije ako znamo faktorizirati stupanj kodne riječi pa uvrštavanjem nula u svaki faktor polinoma odredimo koji su minimalni polinomi određenih nula  $\alpha^i$ .

Dok se u standardnim cikličkim kodovima kontrola pogrešaka zasniva na djeljivosti kodne riječi s generirajućim polinomom, kod BCH kodova kontrola pogrešaka je definirana na djeljivosti kodne riječi sa skupom faktora generirajućeg polinoma. Dekodiranje se svodi na izračunu sindroma tj. ostatka dijeljenja primljene kodne riječi s faktorima

$$s_i[y(x)] = \text{rem} \left[ \frac{y(x)}{m_i(x)} \right], \quad (2-32)$$

$$S_i = s(\alpha^{i+1}); 0 \leq i \leq d(K) - 2. \quad (2-33)$$

U izrazu za koeficijente polinoma, za  $s$  koristimo izraz ostatka faktora minimalnog polinoma nule  $\alpha^{i+1}$ . Iz osobine maksimalnog broja ispravljanja pogrešaka koda  $t = i$  definiramo matricu  $A (t \times t)$  s koeficijentima  $S_i$

$$A = \begin{bmatrix} S_1 & S_2 & \cdots & S_i \\ S_2 & S_3 & \cdots & S_{i+1} \\ \vdots & \vdots & \cdots & \vdots \\ S_i & S_{i+1} & \cdots & S_{2i-1} \end{bmatrix}. \quad (2-34)$$

Zatim izračunamo determinantu, a ako je matrica singularna ( $A=0$ ) smanjujemo  $i-1$  i ponovimo postupak sve dok matrica nije regularna kada računamo inverznu matricu  $A^{-1}$ . Rang regularne matrice nam govori o broju nastalih pogrešaka  $\mu$ . Definiramo matricu sindroma  $S_i$

$$S_i = \begin{bmatrix} S_{\mu+1} \\ S_{\mu+2} \\ \vdots \\ S_{2\mu} \end{bmatrix}, \quad (2-35)$$

računamo koeficijente polinoma lokacije pogreške

$$\begin{bmatrix} \sigma_\mu \\ \sigma_{\mu-1} \\ \vdots \\ \sigma_1 \end{bmatrix} = A^{-1} \begin{bmatrix} S_{\mu+1} \\ S_{\mu+2} \\ \vdots \\ S_{2\mu} \end{bmatrix} \quad (2-36)$$

pa dobijemo polinom lokacije pogreške:

$$\sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 + \sigma_3 x^3 + \dots + \sigma_\mu x^\mu \quad (2-37)$$

Chienovim algoritmom pretraživanja dobivamo broj različitih korijena  $\alpha^i$  koji ukazuju na broj pogrešnih bitova, a njihove inverzije na lokaciju pogrešaka definirajući vektor pogreške kojeg koristimo za ispravljanje pogrešno primljene kodne riječi.

## 2.2 Konvolucijski kod

U blok-kodovima, svaka  $m$ -torka simbola poruke definira, preko 1:1 korespondencije kontrolnu grupu od  $n-m$  simbola u kodnoj riječi sistematskog, odnosno kompletnu kodnu riječ  $n$ -torku nesistematskog koda. Ovakva operacija preslikavanja odgovara sistemu bez memorije tako da kodna riječ ovisi o ulaznim  $m$ -torkama simbola poruke. Konvolucijski kod predstavlja izlaz iz sustava s memorijom tj. kodna riječ  $n$ -torka ne ovisi samo o ulaznoj  $m$ -torci poruke nego i o prethodnim ulaznim  $m$ -torkama. Na taj način ne postoji jednostavna 1:1 korespondencija između ulazne i izlazne grupe simbola pa se struktura koda proteže na cijeli kodirani niz koji može biti beskonačan u svojoj duljini. Kodna riječ je definirana kontinuiranim slijedom bitova prolaskom poruke s ulaza kroz posmačne registre s  $m$ -memorijskih stanja i binarnih zbrajala (po modulo-2) koji predstavljaju izlaze konvolucijskog koda. Sve izlaze multipleksiranjem dovodimo na jedan izlaz na kojem se pojavljuje kodna riječ. Osobine konvolucijskih kodova su *omjer koda* (engl. *code rate*)

$$R = \frac{k}{n} \quad (2-38)$$

gdje za svaki  $k$ -bitni ulazni slijed simbola dobijemo  $n$  izlaznih bitova odnosno  $k \times n$  predstavlja dimenziju matrice  $\mathbf{G}$ , *graničnu duljinu* (engl. *constraint length*)

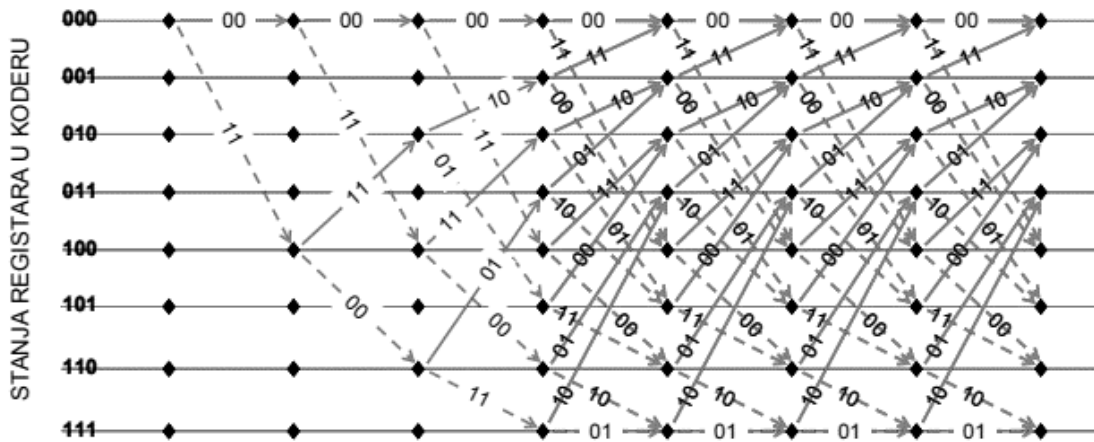
$$L = M + 1 = k(m - 1) \quad (2-39)$$

koja određuje broj bitova koji utječu na vrijednost pojedinog izlaza i *memoriju*

$$M = \max_{ij} [\deg(g_{ij})] \quad (2-40)$$

koja definira broj memorijskih stanja posmačnog registra. Konvolucijski se kodovi mogu proučavati preko polinomskih matrica, skalarnih matrica, posmačnih registara, dijagrama stanja (engl. *state diagram*), rešetkastog dijagrama (engl. *trellis diagram*) i stablastog dijagrama (engl. *tree diagram*).

Dijagrami rešetke (slika 2.6) predstavljaju linearni vremenski redoslijed događaja. Os  $x$  prikazuje diskretno vrijeme, a sva moguća stanja prikazana su na osi  $y$ .



Sl.2.6 Dijagram rešetke za (2,1,4) kod

Krećemo se vodoravno kroz rešetku u vremenu, a svaki prijelaz označava dolazak novih bitova. Dijagram rešetke ostvaruje se crtanjem svih mogućih stanja  $2^L$  na okomitoj osi. Onda spajamo svako stanje sa sljedećim stanjem dopuštene kodne riječi za to stanje. Postoje samo dva moguća izbora u svakome stanju. Ono je određeno dolaskom bita 0 ili bita 1. Streljice usmjerene prema gore, predstavljaju bit 0, a one usmjerene prema dolje, predstavljaju bit 1.

Da bi matricu polinoma  $G$  upotrijebili za zaštitno kodiranje bitove informacije moramo preslikati u koeficijente  $k$ -torki polinoma  $i = \{i_0(x), i_1(x), \dots, i_{k-1}(x)\}$ . Kodna riječ  $c = \{c_0(x), c_1(x), \dots, c_{n-1}(x)\}$  je opisana relacijom:

$$c = iG . \tag{2-41}$$

Kodnu riječ  $c$  opisujemo preko koeficijenata polinoma odnosno  $j$ -ti polinom pišemo  $c_j(x) = c_{j0} + c_{j1}x + \dots$ , a skalarnu kodnu riječ:

$$c = \{c_{00}c_{10} \dots c_{n-1;0}, c_{01}c_{11} \dots c_{n-1;1}, \dots\} . \tag{2-42}$$

Matrica polinoma  $G$  je

$$G = \begin{bmatrix} G_0 & G_1 & G_2 & \dots & G_M & 0 & 0 \\ 0 & G_0 & G_1 & \dots & G_{M-1} & G_M & 0 \\ 0 & 0 & G_0 & \dots & G_{M-2} & G_{M-1} & G_M \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \dots & \dots & \dots \end{bmatrix} \tag{2-43}$$

gdje koeficijente u ovoj matrici možemo odrediti na osnovu relacije:

$$G = \sum_{i=0}^M G_i x^i. \quad (2-44)$$

Stupanj polinoma informacije u principu bi trebao biti što je moguće veći u cilju približavanja uvjetima kodnih teorema (za velike dužine koda moguće je definirati kod bez pojavljivanja pogreške s kodnim odnosom blizak kapacitetu kanala), ali zbog praktičnih razloga mora se uvesti ograničenja. To nas vodi na definiciju  $L$ -tog ograničenja. Informacijski polinomi moraju zadovoljiti uvjet  $\deg[i_j(x)] \leq L - 1, j = 0, 1, \dots, k - 1$ . Na osnovi ovog uvjeta dobijemo kodnu riječ  $c = \{i_0(x), i_1(x), \dots, i_{k-1}(x)\}$  čija svaka komponenta ima stupanj manji od  $M + L - 1$ . Tako informaciju  $i = \{i_0(x), i_1(x), \dots, i_{k-1}(x)\}$  možemo prikazati pomoću  $kL$  bita, a kodnu riječ  $c$  pomoću  $n(M + L)$  bita. Kodno preslikavanje možemo prikazati relacijom:

$$c = iG_L. \quad (2-45)$$

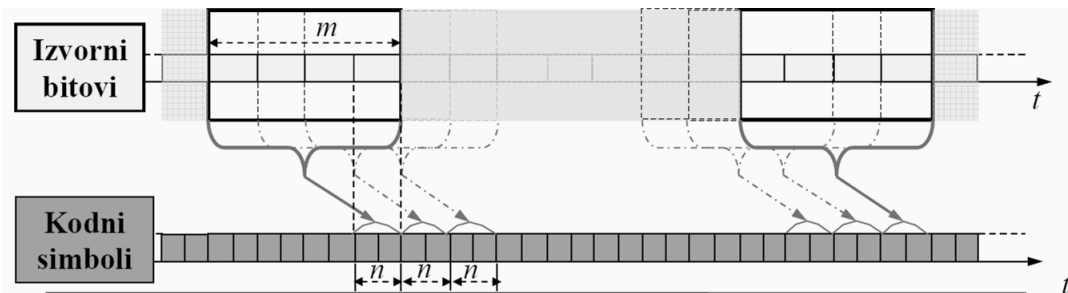
Ovdje se vidi zašto se pomoću konvolucijskih kodova s osnovnom kodnom riječi koja je bitno kraća nego kod blok-kodova postiže približavanje performansama II Shannonovog teorema. Kod konvolucijskog koda trenutni izlaz zavisi od određenog broja prethodnih informacijskih poruka, što nije slučaj kod blok-kodova.  $L$ -to ograničenje konvolucijskog koda  $(n, k)$  možemo opisati kao  $(n(M + L), kL)$  linearni blok-kod i u tom slučaju konvolucijski kodovi su posebna vrsta blok-koda. Relacija kodne brzine ograničenog koda je:

$$R_L = \frac{kL}{n(M+L)} = R \left( 1 - \frac{M}{M+L} \right). \quad (2-46)$$

Kako u mnogim aplikacijama uzimamo  $L$  mnogo veći od  $M$ , to će brzina ograničenog koda biti bliska brzini neograničenog koda.

## 2.2.1 Konvolucijski koder

Kod blok koda kodiramo  $k$ -bitni blok u  $n$ -bitnu kodnu riječ, tako da svaka kodna riječ štiti svoje vlastite  $k$ -bitne blokove podataka. Kod konvolucijskog kodiranja koristimo drugčiji način preslikavanja podatkovnih u kodne simbole odnosno koncept pomičnog prozora širine  $m$ -bita podataka koji se preslikavaju u grupu od  $n$ -kodnih simbola koji se prenose za trajanja samo jednog podatkovnog bita. Nakon pomaka prozora udesno za jedno mjesto, obnovljeni  $m$ -bitni blok se preslikava u slijedeću  $n$ -bitnu grupu simbola (slika 2.5).



Sl.2.5 Preslikavanje  $n$  bitnih simbola [15]

Ako imamo dva binarna niza  $a_n$  i  $b_n$  njihova konvolucija je niz  $c_n$  definiran s:

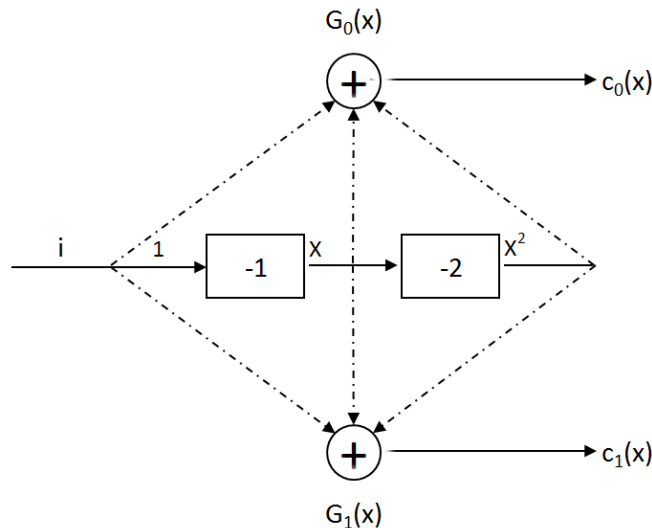
$$c_n = \sum_v a_n b_{n-v} \cdot \quad (2-47)$$

Ako definiramo generirajuće funkcije kao:

$$a(x) = \sum_n a_n x^n \quad (2-48)$$

$$b(x) = \sum_n b_n x^n \quad (2-49)$$

množenje generirajućih funkcija odgovara konvoluciji nizova binarnih simbola. Konvolucijski kod prikazat ćemo posmačnim registrima (slika 2.6) preko generirajuće funkcije koju definiramo preko  $n$  izlaznih vektora i to jedan vektor za svaki funkcijski generator. Strukturu konvolucijskog koda vidimo preko njegovih parametara. Broj  $m$  predstavlja  $m$  registara,  $n$  broj zbrajala modulo-2 koja rezultiraju u  $n$  izlaznih bitova, a način njihovog međusobnog spajanja definira generator polinomskih funkcija. Funkcijski generator označava veze između binarnih zbrajala i stanja posmačnih registara za pojedini izlaz koda. Postojanje jedinice na nekom mjestu unutar vektora znači da je mjesto unutar posmačnog registra spojeno na promatrano binarno zbrajalo dok nula označava da ne postoji veza.



Sl. 2.6 Opći prikaz povezivanja posmačnih registara i zbrajala

## 2.2.2 Konvolucijski dekodir

Dekodiranje konvolucijskih kodova se svodi na nekoliko različitih pristupa, koji su grupirani u dvije osnovne kategorije:

- serijsko dekodiranje (Fanov algoritam),
- dekodiranje najvećom vjerojatnosti (Viterbijev algoritam),

koje predstavljaju dva različita pristupa u osnovnoj ideji dekodiranja. Npr. postupkom kodiranja ulazni niz od tri bita i uz omjer koda  $1/2$  preslikavanjem dobijemo niz na izlazu od 6 bita. Permutacija triju ulaznih bitova rezultira u osam mogućih ulaznih nizova. Svaki od njih kodiranjem jedinstveno se preslikava u nizove od šest izlaznih bitova. Ovo čini skup dopuštenih nizova pa je zadatak dekodera odrediti koji niz se poslao. Možemo pristupiti na dva načina:

- usporediti primljen niz sa svim dopuštenim nizovima i odabrati onaj s najmanjom Hammingovom udaljenošću,
- napraviti korelaciju i odabrati nizove s najboljom korelacijom.

Prvi pristup nazivamo dekodiranje tvrdom odlukom (*engl. hard decision decoding*), a drugi pristup dekodiranje mekom odlukom (*engl. soft decision decoding*). Kako broj bitova raste, povećava se broj izračuna potrebnih za dekodiranje tvrdom odlukom, pa dekodiranje ovim načinom više nije praktično. Moramo pronaći učinkovitiji način da se ne ispituju sve varijacije, ali da možemo riješiti problem dva moguća odgovora. Osnovna ideja postupka je dekodiranje niza bez provjere svake od  $2^n$  kodnih riječi.

## 2.2.3 Maksimalna vjerojatnost i Viterbijev algoritam

Viterbijev algoritam je jedan od najpoznatijih za dekodiranje konvolucijskih kodova po pravilu najvećih izgleda (*maximum likely-hood decoding*). Viterbijev dekodirer ispituje cijelu primljenu sekvencu dane dužine. Dekoder izračunava metriku svake putanje i donosi odluku na osnovu ove metrike. Prate se sve putanje, dok se dvije putanje ne spoje u jedan čvor. Onda se putanja s većom metrikom zadržava, a ona sa manjom metrikom se odbacuje. Viterbijev algoritam primjenjuje pravila maksimalnih izgleda kako bi ograničio usporedbe na  $2^{kL}$  preživjelih putanja umjesto provjere svih putanja. Najčešća korištena metrika je metrika Hammingove udaljenosti. Ovo je samo broj pozicija bitova u kojima se primljena kodna riječ i dozvoljene kodna riječ poklapaju. Ove metrike su kumulativne, tako da je putanja s najvećom ukupnom metrikom najvjerojatnija. Kroz slijedeći primjer opisat ćemo Viterbijev algoritam. Poslana je sekvenca 1011000. Zadnja tri bita posljedica je *flush* bitova i njihov izlaz se naziva bitovima repa (*tail bits*).

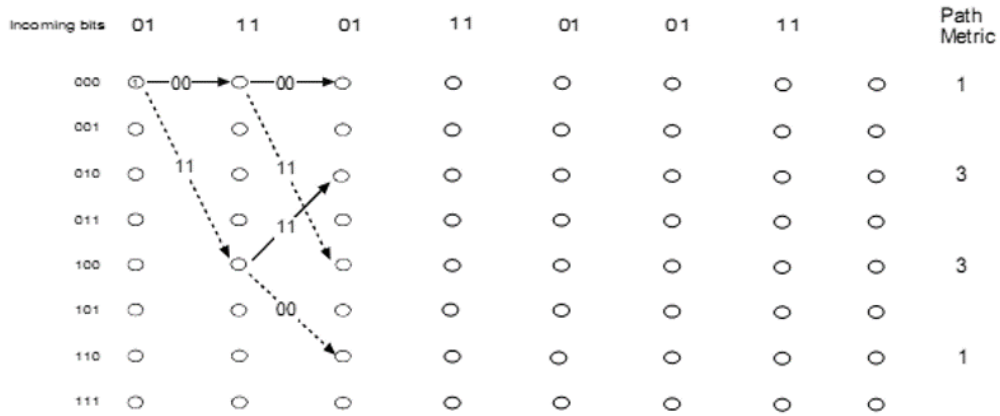
Neka je primljena sekvenca 01 11 01 11 01 01 11.

1. U  $t=0$ , primaju se bitovi 01. Dekoder uvijek započinje u stanju 000. Od ove točke dostupne su mu dvije putanje, ali ni jedna ne odgovara dolazećim bitovima. Dekoder izračunava metriku obje grane i nastavit će simultano duž obje grane za razliku od sekvencijalnog dekodiranja gdje se izbor pravi na svakoj točki odluke. Metrika za obje grane je jedna, što znači da jedan od dva bita odgovara dolaznim bitovima (slika 2.7).



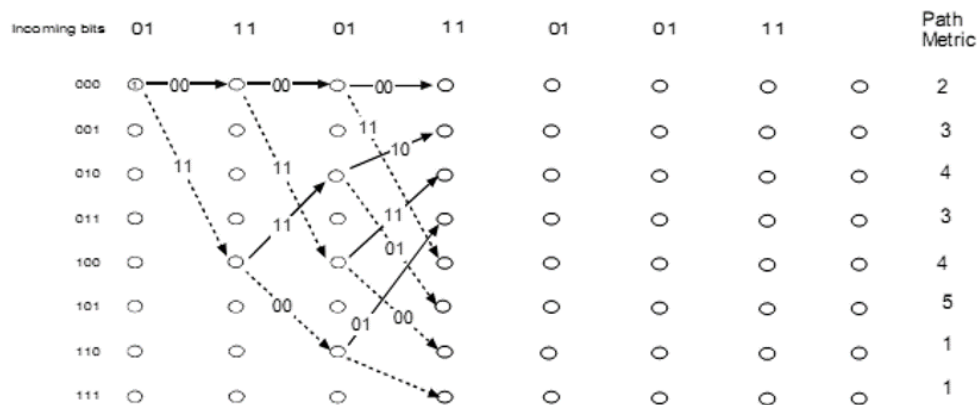
Sl.2.7 Grafički prikaz Viterbijevog algoritma [14]

2. U  $t=1$ , dekodirer se širi iz dva moguća stanja u četiri stanja. Metrike ovih grana se proračunavaju preko slaganja kodne riječi i dolazećih bitova, 11. Nova metrika je prikazana desno od *trellisa* (slika 2.8)



Sl.2.8 Grafički prikaz Viterbijevog algoritma [14]

3. U  $t=2$ , četiri stanja se šire u osam, kako bi pokazala sve moguće putanje. Metrike putanja izračunate za bitove 01 su dodane na prethodne metrike iz  $t=1$  (slika 2.9)

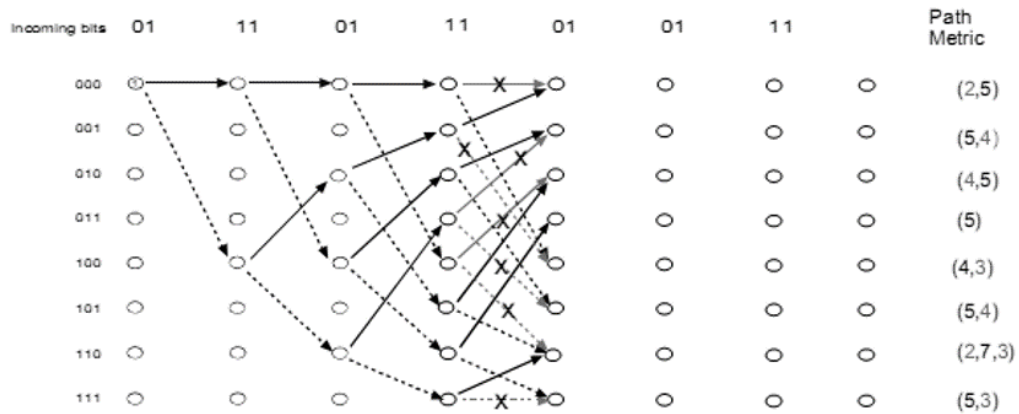


Sl.2.9 Grafički prikaz Viterbijevog algoritma [14]

4. U  $t=3$ , *trellis* je potpuno popunjen. Svaki čvor ima najmanje jednu putanju koja dolazi u njega. Metrike su prikazane na slici.

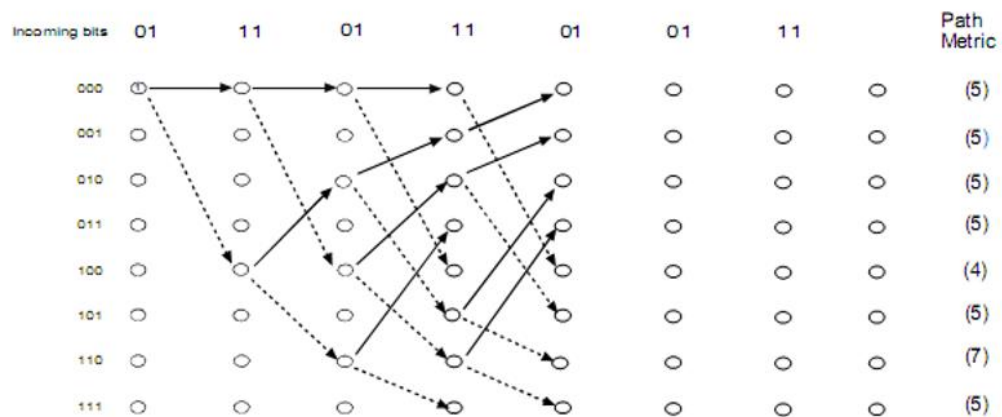
5. U  $t=4$ , putanje nastavljaju naprijed i sada počinju da konvergiraju u čvorovima. Dobiju se dvije metrike za svaku od putanja koja dolazi u čvor po principu maksimalnih izgleda, u svakom čvoru se odbacuje putanja sa manjom metrikom, jer za nju postoje manji izgledi, odnosno manje je vjerojatna. Ovo odbacivanje putanja na svakom čvoru pomaže u smanjivanju broja putanja koje trebaju biti ispitane (slika 2.10)





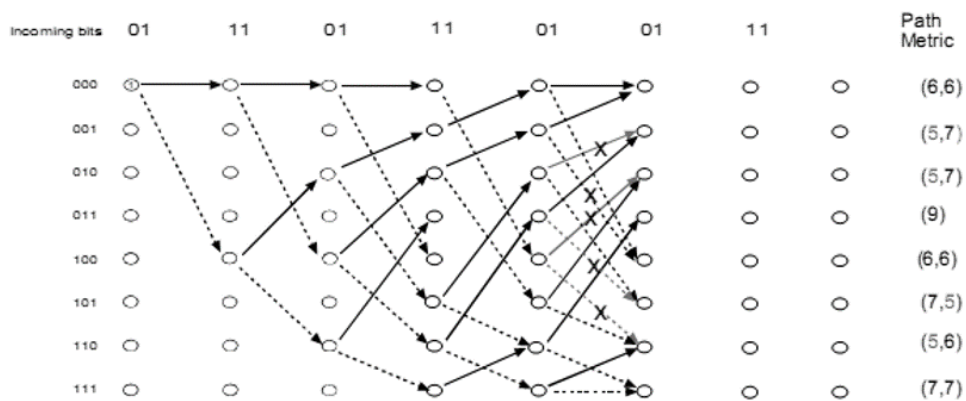
Sl. 2.10 Grafički prikaz Viterbijevog algoritma [14]

Sada u svakom čvoru postoji jedna ili više putanja koje konvergiraju. Metrike za sve putanje su dane na desnoj strani. U svakom čvoru zadržava se samo putanja sa najvećom metrikom, a odbacuju ostale prikazane crvenom bojom. Poslije odbacivanja putanje sa manjom metrikom ostaju putanje koje prikazuje (slika 2.11). Prikazana metrika je ona pobjedničke putanje.



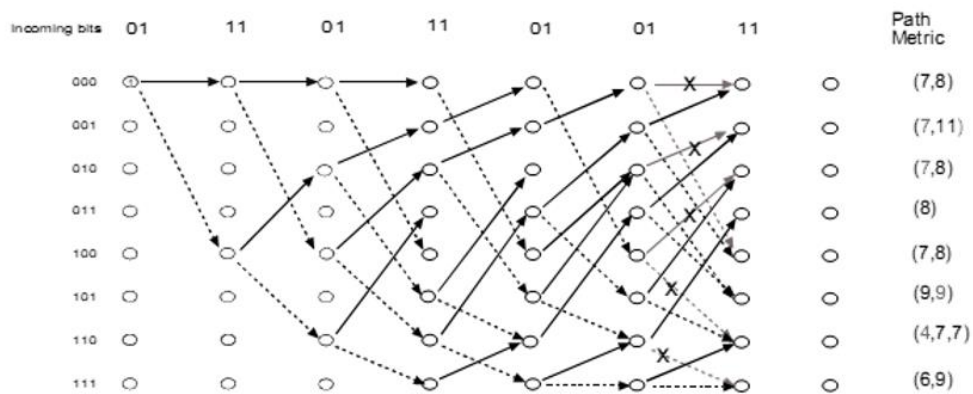
Sl. 2.11 Grafički prikaz Viterbijevog algoritma [14]

6. U  $t=5$ , poslije odbacivanja putanja kao što je prikazano, ponovo se ide naprijed i proračunavaju se nove metrike. Na slijedećem čvoru putanje ponovo konvergiraju i ponovo se odbacuju one sa manjom metrikom (slika 2.12)



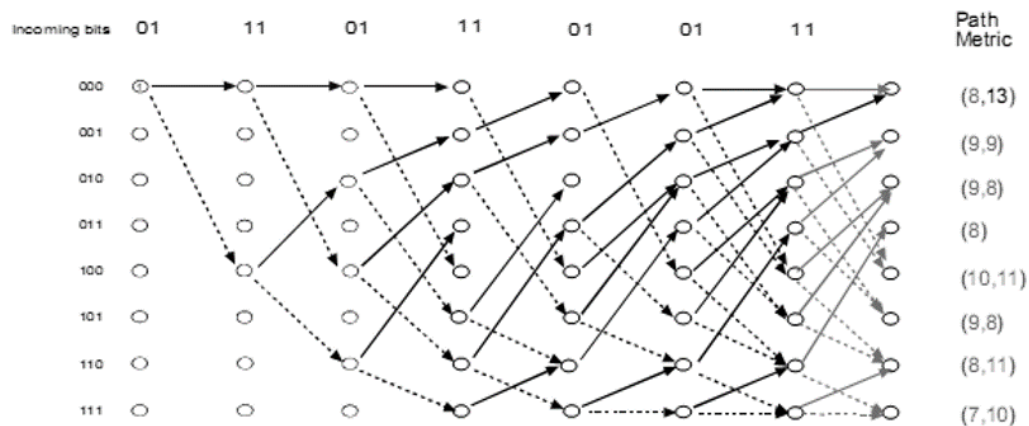
Sl. 2.12 Grafički prikaz Viterbijevog algoritma [14]

7. U  $t=6$ , primljeni bitovi su 11. Ponovo se metrike proračunavaju za svaku putanju. Odbacuju se sve putanje s manjom metrikom, ali se zadržavaju obje ako su im metrike jednake (slika 2.13)



Sl.2.13 Grafički prikaz Viterbijevog algoritma [14]

*Trellis* od sedam koraka je kompletiran. Sada se promatra putanja sa najvećom metrikom, koja je pobjednik. Putanja koja prolazi kroz stanja 000, 100, 010, 101, 110, 011, 001, 000 odgovara bitovima 1011000, koji predstavljaju dekodiranu sekvencu (slika 2.14)

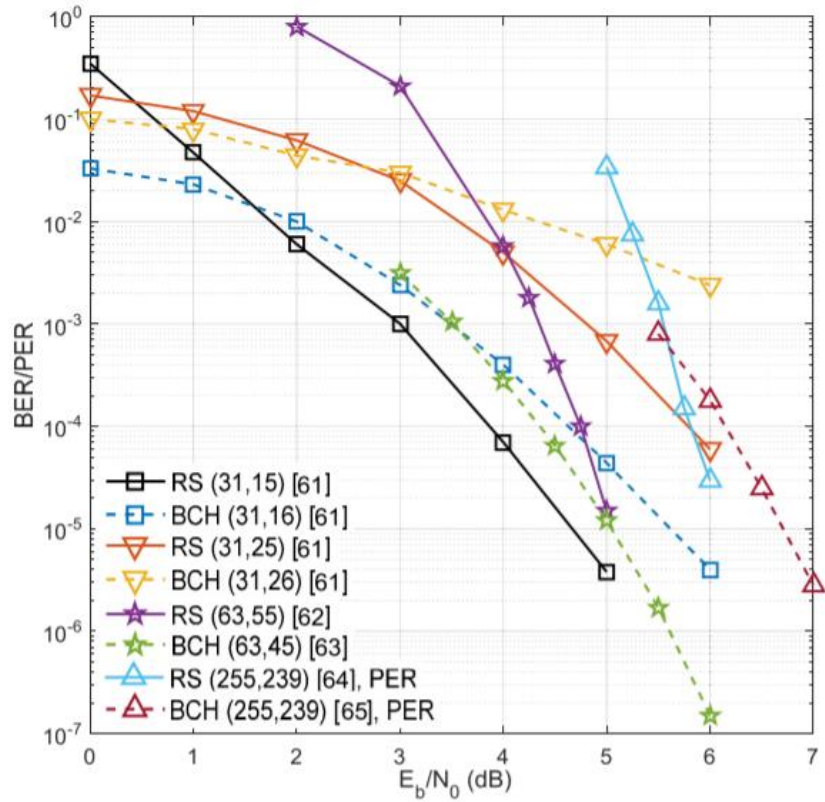


Sl.2.14 Grafički prikaz Viterbijevog algoritma [14]

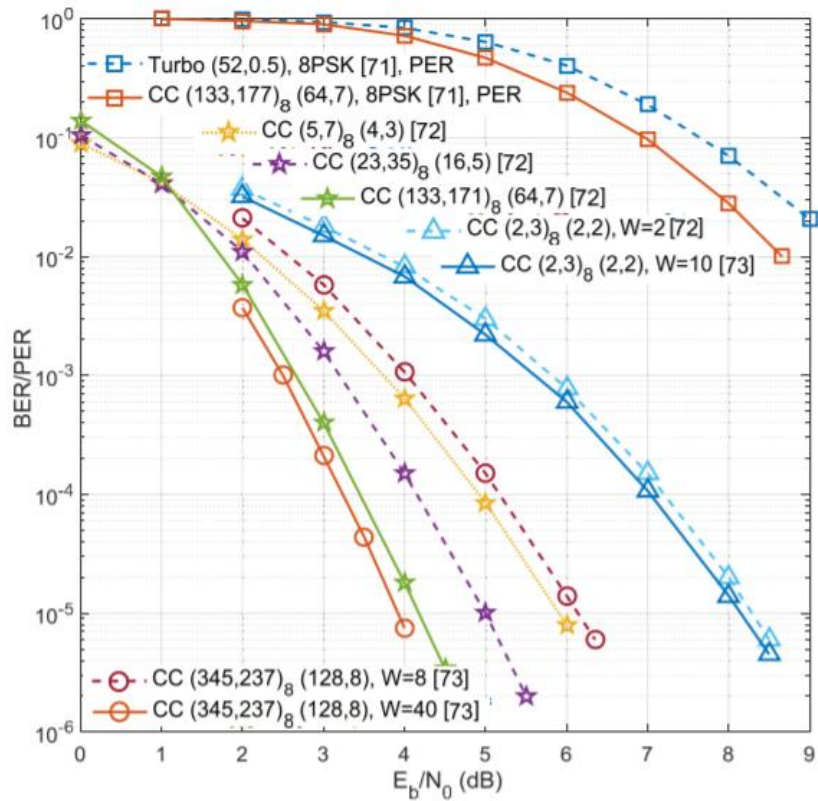
## 2.3 Usporedba različitih postupaka kodiranja

Klasični postupci kodiranja nisu u mogućnosti približiti se Shannonovoj granici, ali zbog jednostavne strukture kodiranja postižu nisku latenciju dekodiranja. Iskoristivši njihovu algebarsku strukturu koja olakšava hardversku implementaciju ciklički kodovi omogućuju rasprostranjenu primjenu. BCH kodovi s malim kašnjenjem u obradi i dostupnim omjerima koda i duljinama paketa našli su primjenu u memorijskim i optičkim komunikacijskim sustavima. Složenost dekodiranja je jednostavnija na manjoj veličini simbola što rezultira u manjoj sposobnosti ispravljanja praskave (skupne) pogreške. Reed-Solomonovo kodiranje, definirano preko Galoisovog polja ( $2^m$ ) sa simbolom od  $m$  bita ima bolju mogućnost ispravljanja praskave pogreške (slika 2.15). Pod pretpostavkom približno jednakih omjera kodova RS-kodovi imaju bolje BER/PER (*engl. packet error rate*) performanse nego BCH kodovi, a povećanjem odnosa signal/šum dolazi do značajnijeg poboljšanja performansi oba načina kodiranja. Međutim, u područjima srednjih i visokih odnosa signal/šum kod RS (63, 55), koji ima veći omjer koda od oko 0,87, još uvijek nadmašuje kod BCH (63, 45) s manjim omjerom koda od oko 0,71.

Za razliku od blok-kodova koder/dekoder konvolucijskog koda omogućava obradu tijekom primanja bitova, a samim tim i prednost u latenciji prema blok-kodovima. Za kratke pakete podataka konvolucijski kod ostvaruje bolje BER/PER performanse od binarnih blok-kodova (slika 2.16).



Sl.2.15 Usporedba BCH i RS koda za različite omjere kodova [21]



Sl.2.16 Usporedba konvolucijskih kodova za različite parametre [21]

### 3. ISPREPLITANJE

Ispreplitanje (*engl. interleaving*) je tehnika kojom se bez daljnjeg povećanja redundancije povećava efikasnost korigiranja praskavih pogrešaka. Tehnika ispreplitanja može se primijeniti na razini bita ili na razini simbola. Efekt ispreplitanja može se prikazati kao transformacija  $(n,m)$  koda u  $(n*k,m*k)$  gdje je  $k$  dubina ispreplitanja. Općenito se transformacija koda tehnikom ispreplitanja može opisati matricom:

$$\mathbf{T} = \begin{bmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1n} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \mathbf{a}_{k1} & \mathbf{a}_{k2} & \cdots & \mathbf{a}_{kn} \end{bmatrix}, \quad (3-1)$$

gdje je  $a_{ij}$   $j$ -ti element  $i$ -te kodne riječi uz  $i = 1, 2, \dots, k$ . Uzimajući stupce matrice  $\mathbf{T}$  formira se nova kodna riječ dužine  $n*k$ :

$$(a_{11}a_{21} \dots a_{k1}a_{12}a_{22} \dots a_{k2} \dots a_{1n}a_{2n} \dots a_{kn}). \quad (3-2)$$

Ako  $(n, m)$  kod omogućuje korekciju praska do dužine  $b$ , novi kod dobiven ispreplitanjem do dubine  $k$  omogućuje korekciju praska do dužine  $b*k$ . Ispreplitanjem nekog cikličkog koda dobiva se opet ciklički kod. Tehnika ispreplitanja, definirana matricom  $\mathbf{T}$  koja transformira  $(n,m)$  u  $(n*k, m*k)$ -kod, uzrokuje transformaciju raspodjele vjerojatnosti dužine praska pogrešaka i to ovisno o dubini ispreplitanja. Veća dubina ispreplitanja utječe na smanjenje vjerojatnosti većih duljina praska. Opisani način ispreplitanja s definiranom dubinom  $k$  može biti opisan tako da se proces ispreplitanja protegne teoretski na beskonačnu dubinu. Ovakav način omogućuje konvolucijsko ispreplitanje ili zakašnjelo ispreplitanje gdje je dubina ograničena zbog praktičnih razloga, ali je raspodijeljena na više vrijednosti. Princip možemo objasniti primjerom (slika 3.1) gdje se blokovi sastoje od 4 uzorka. U taktu uzimanja uzoraka, pune se 4 lokacije redom 1,2,3,4, zatim 5,6,7,8 itd. s kašnjenjem za 4, 8 intervala ovisno o poziciji u bloku. Na primjer, dogode se dva praska (15,12 i 19,16) duljine po 2 simbola. Ovo odgovara po jednom pogrešnom simbolu u bloku III i V odnosno dva u bloku IV koji neće biti ispravljani. Ispreplitanje omogućuje efikasno ispravljanje dužih prasaka osim u slučaju maksimalne dužine dopuštenog praska i slučajne pogreške u njegovoj blizini.

Da bi riješili problem, kodne riječi se oblikuju prije i nakon ispreplitanja. Ako se primjenjuje konvolucijsko ispreplitanje govorimo o unakrsnom ispreplitanju ili tzv. ulančanom kodu. Binarni ciklički  $(7,4)$  kod  $C_1$  generiran matricom [11]:

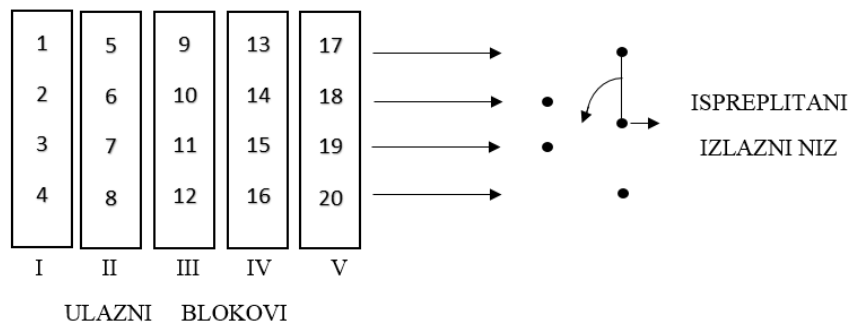
$$\mathbf{G}_1 = \begin{bmatrix} 1000 : 101 \\ 0100 : 111 \\ 0010 : 110 \\ 0001 : 011 \end{bmatrix}, \quad (3-3)$$

ima svojstvo ispravljanja jedne pogreške. Ako želimo ispraviti skup praskave pogreške do dužine 3, potrebno je ispreplitanje do dubine 3. Neka su tri kodne riječi;

$$x_1 = (1011000); \quad x_2 = (1100010); \quad x_3 = (0001011),$$

ispreplitanje obavljamo preko matrice;

$$\mathbf{T} = \begin{bmatrix} 1011 : 000 \\ 1100 : 010 \\ 0001 : 011 \end{bmatrix}. \quad (3-4)$$



Sl.3.1 Princip tehnike preplitanja [11]

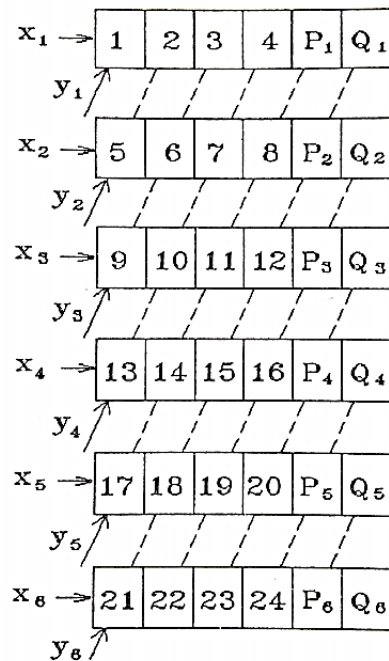
Za razliku od običnog ispreplitanja, u unakrsnom ispreplitanju (slika 3.2) stupci matrice  $\mathbf{T}$  nisu simboli nove kodne riječi, nego predstavljaju informacijske simbole za drugi kod  $C_2$ . Neka je  $C_2$  binarni ciklički (6,3) kod uz generirajuću matricu:

$$\mathbf{G}_2 = \begin{bmatrix} 100 : 110 \\ 010 : 111 \\ 001 : 011 \end{bmatrix} \quad (3-5)$$

i relacijom  $\mathbf{T}^T * \mathbf{G}_2$  generiraju se kodne riječi:

$$\begin{bmatrix} 110 \\ 010 \\ 100 \\ 101 \\ 000 \\ 011 \\ 001 \end{bmatrix} * \begin{bmatrix} 100 : 110 \\ 010 : 111 \\ 001 : 011 \end{bmatrix} = \begin{bmatrix} 110001 \\ 010111 \\ 100110 \\ 001101 \\ 000000 \\ 011100 \\ 001011 \end{bmatrix} . \quad (3-6)$$

Kod  $C_2$  može ispraviti dvije izbrisane pozicije. Ako sada analiziramo problem dva prska dužine 2 i to baš simbola 12,15 i 19,16 postupak dekodiranja će uspješno korigirati oba praska. Lokaciju pogrešnih simbola određujemo preko koda  $C_2$  i preko kontrolnih simbola  $Q$ . Budući da se prvi pogrešni simbol 12 nalazi u kodnoj riječi  $x_3$  od  $C_1$  on će biti ispravljen pripadajućim paritetnim simbolom  $P_3$ . Kodna riječ  $x_4$  u  $C_1$  ima dva pogrešna simbola 15 i 16 koji se ne mogu korigirati s  $P_4$ , ali unakrsna kodna riječ  $y_6$  (pošto je simbol 12 već korigiran) ima samo jedan pogrešan simbol i to 15 koji može biti ispravljen preko paritetnog simbola  $Q_1$ . Nakon korekcije 15, paritetni simbol  $P_4$  ispravlja simbol 16, a  $P_3$  korigira simbol 19.



Sl.3.2 Postupak unakrsnog ispreplitanja [11]

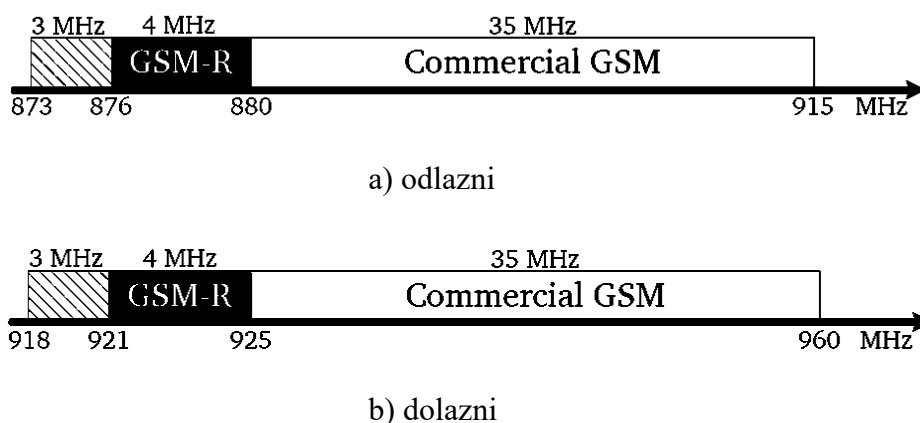
## 4. GSM-R

GSM-R je prvi standard mobilne komunikacije dizajniran za potrebe željeznice koji nudi dvije osnovne usluge, prijenos podataka između vlaka i željezničke infrastrukture u ETCS razine 2 i 3 i glasovne komunikacije. Baziranom na standardu globalnog sustava za mobilnu komunikaciju (GSM) komercijalnih mreža prilagođenom uputama EIRENE (*engl. european integrated radio enhanced network*) i MORANE (*engl. mobile oriented radio network*) implementirane su specifične dodatne usluge:

- Functional Addressing (FA) - određena sekvenca znakova dodijeljena za svaku funkciju posebno (npr. funkcija ispitivanja, prijave, odjave itd.),
- Location Dependent Addressing (LDA) - dinamički određivanje poziva prema lokaciji pozivatelja,
- Voice Group Call Service (VGCS) - grupno povezivanje željezničkih djelatnosti
- Voice Broadcast Service (VBS) - grupno informiranje željezničkih djelatnosti,
- Railway Emergency Call (REC) - željeznički hitni poziv kategorije visokog prioriteta,
- Enhanced Multi-Level Precedence and Pre-emption (eMLPP) - definira prioritet korisnika radi postizanja visokih performansi prilikom hitnih poziva,
- Shunting mode - regulacija i kontrola pristupa u komunikaciji uslijed obavljanja operacije ranžiranja.

### 4.1 Osobine GSM-R

Razliku GSM-R u odnosu na GSM vidimo u dodijeljenom frekvencijskom pojasu (slika 4.1). Širina frekvencijskog pojasa od 4 MHz smještena je u frekvencijskom području od 876 – 880 MHz za odlazni i 921 – 925 MHz za dolazni smjer.



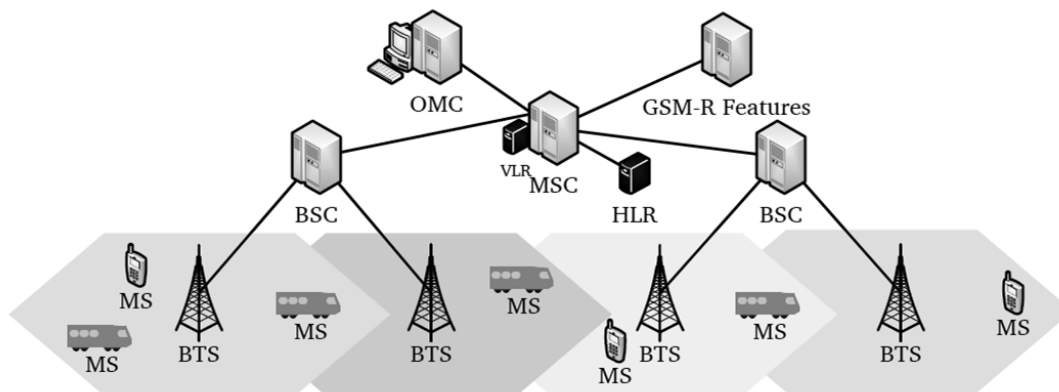
Sl. 4.1 Raspodjela frekvencijskog pojasa GSM-R mreže [16]



Na nacionalnoj razini dodavanjem pojasa od 3 MHz u frekvencijskom području 873 – 876 MHz za odlazni i 918 – 921 MHz za dolazni smjer dobiven je prošireni GSM-R (*engl. extended GSM-R*). GSM-R mreža sadrži tri glavna podsustava slika (4.2):

- mobilna stanica MS (*engl. mobile station*) – bežično priključena na mrežu,
- podsustav bazne stanice BSS (*engl. base station subsystem*) koju čine kontroler bazne stanice BSC (*engl. base station controller*) i broja primopredajnih baznih stanica BTSs (*engl. base transceiver stations*),
- mrežni komutacijski podsustav NSS (*engl. network and switching subsystem*) koji uključuje jezgru mreže s komutacijskim centrom mobilne mreže MSC (*engl. mobile switching center*), registar domaćih korisnika HLR (*engl. home location register*) i registar gostujućih korisnika VLR (*engl. visitor location register*).

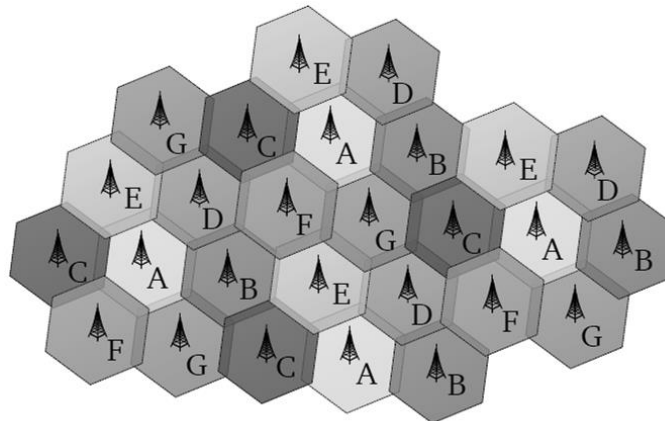
MSC je središnji element NSS-a odgovoran za upravljanje mobilnom mrežom. GSM-R uključuje servere odgovorne za pružanje željezničkih usluga kao čvorove odgovorne za funkcioniranje i održavanje OMC (*engl. operations and maintenance centre*).



Sl.4.2 Podsustavi GSM-R mreže [16]

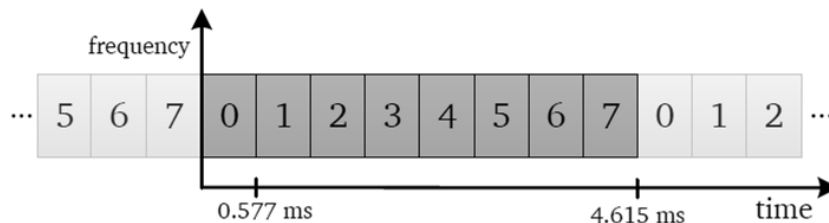
GSM-R mreža je ćelijske strukture raspona 8 km, a razmak 7 – 15 km između baznih stanica. Frekvencijski pojas širine 4 MHz podijeljen je na 19 kanala širine 200 kHz raspoređenih po ćelijama. Ćelije mogu koristiti iste kanale s uvjetom da udaljenost između njih bude dovoljna za siguran i pouzdan rad. Za pokrivanje šireg područja obično je potrebno 7 kanala (slika 4.3). Svaka ćelija može koristiti jedan ili više kanala ovisno o potrebnim kapacitetom korisnika pokrivenog područja. Na otvorenoj pruzi gdje postoji potreba samo linearnog pokrivanja dovoljan je manji broj kanala.

A = 1, 8, 15  
 B = 2, 9, 16  
 C = 3, 10, 17  
 D = 4, 11, 18  
 E = 5, 12, 19  
 F = 6, 13  
 G = 7, 14



Sl.4.3 Čelijska struktura s primjerom dodjele kanala [16]

Da bi se omogućio veći broj korisnika svaki kanal koristi višestruki pristup po vremenu TDMA (*engl. time division multiple access*). GSM-R radio prijenos podijeljen je na vremenske okvire trajanja 4.615 ms koji se sastoji od 8 vremenskih odsječaka trajanja 0.577ms (slika 4.4). Svaka ćelija barem jedan vremenski odsječak koristi za mrežnu signalizaciju dok sedam za simultane pozive.



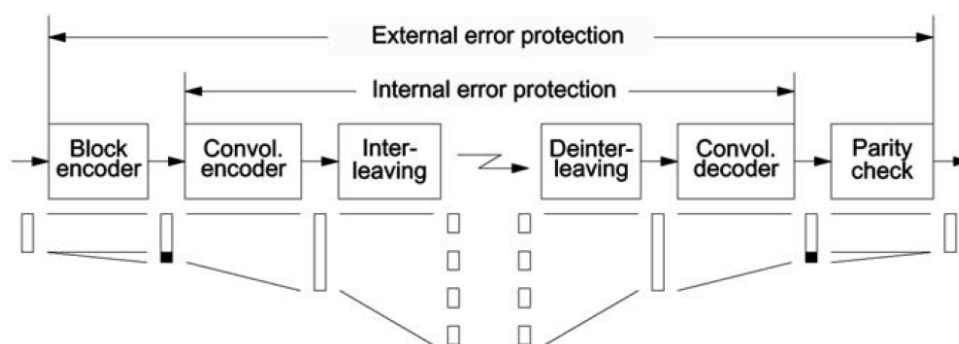
Sl.4.4 Vremenski okvir s odsječcima [16]

GSM-R prilikom prijenosa signala koristi modulaciju GMSK (*engl. Gaussian minimum shift keying*). Latencija prilikom prijenosa nalazi se u području između 200 ms i 400 ms, a maksimalna brzina prijenosa iznosi 9,6 kbit/s. Vrijeme uspostave poziva kreće se oko 5 sekundi.

## 4.2. Kodiranje kanala

Različita svojstva komunikacijskog kanala rezultiraju vrlo visokom vrijednošću vjerojatnosti pogreške bita BER (*engl. bit error rate*) reda od  $10^{-3}$  do  $10^{-1}$ . Visokomprimirano izvorno kodiranje sa smanjenim brojem dodatnih redundantnih bitova čini neprihvatljivom kvalitetom govorne komunikacije. Iz tog razloga kodiranjem kanala odnosno dodavanjem prihvatljivog broja redundantnih bitova i primjenom postupaka otkrivanja i

ispravljanja pogrešaka smanjujemo BER na prihvatljivih  $10^{-5} - 10^{-6}$ . GSM-R sustav koristi kombinaciju nekoliko postupaka prilikom kodiranja kanala prikazanim kroz faze (slika 4.5).



Sl.4.5 Faze kodiranja radi zaštite od pogrešaka bitova [4]

Uz blok-kodove koji generiraju dodatne bitove pariteta za otkrivanje pogrešaka, konvolucijski kodovi dodaju redundanciju potrebnu za ispravljanje pogrešaka i postupak ispreplitanja radi zaštite od skupnih ili praskavih (*engl. burst*) pogrešaka. Kodiranje govora obavlja RPE-LTP koder (*engl. regular pulse excitation – long term prediction – linear predictive coder*). Govor se dijeli na uzorke duljine 20 ms kodirane s 260 bita, a signalna informacija s 184 bita. Od bloka 260 (TCH, *full rate*) bita određeni broj bitova je važniji za razumijevanje nego ostali. Tako se blok od 260 bitova dijeli na dvije klase osjetljivosti, klasa I - 182 bita i klasa II - 78 bita. Klase imaju različitu osjetljivost na pojavljivanje pogrešnih bitova. Bitovi klase I imaju veći utjecaj na kvalitetu govora i iz tog razloga moraju biti bolje zaštićeni. Bitovi klase II manje su važni, nisu uključeni u postupak konvolucijskog kodiranja, ali jesu u postupak ispreplitanja. U slučaju TCH, *half rate* blok od 112 bita ulazi kanalni koder, a od toga 95 bita pripadaju klasi I, a 17 bita klasi II.

Kao što smo rekli da pojedina grupa bitova bitno utječe na kvalitetu govora pa ju moramo dodatno zaštititi, na 50 bita klase I (klasa Ia, TCH, F) dodamo tri paritetna bita CRC koda generatorom polinoma izraza [4],

$$G_{CRC}(x) = x^3 + x + 1 \quad (4-1)$$

a signalnom bloku 40 bitova *Fire*-koda u svrhu detekcije pogreške:

$$G_F(x) = (x^{23} + 1)(x^{17} + x^3 + 1) . \quad (4-2)$$

53 bita klase Ia zajedno s 132 bita klase Ib i 4 bita završne sekvence ukupno sadrže 189 bita govora koji ulaze u konvolucijski koder. Svaki ulazni bit se kodira na dva izlazna bita tako da na izlazu koderima imamo 378 bita govora kojima dodajemo okvir od 78 bita klase II tako da

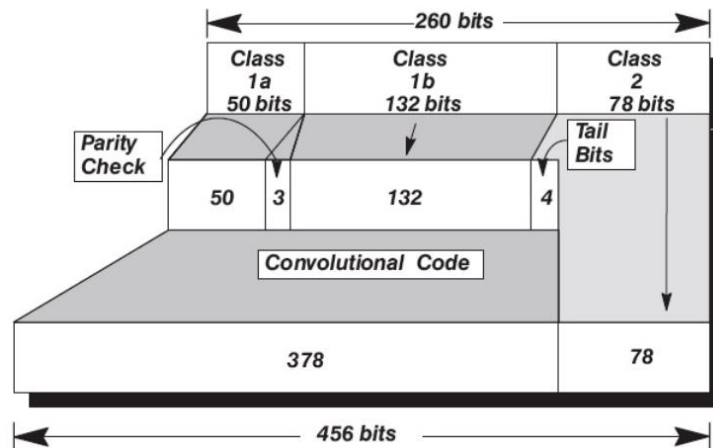
ukupno svakih 20 ms govora kodiramo s 456 bita (slika 4.6). Zbog zaštite od skupnih pogrešaka svaki uzorak se isprepliće. Na izlazu kodera 456 bitova se dijeli na 8 podblokova od 57 bita (tablica 4.1) za razne vrste kanala i s pripadajućim karakteristikama pojedinih postupaka kodiranja. Za kanale RACH i SCH koristi se drugi pristup. Sekvenca slučajnog pristupa i sinkronizacije dopušta duljinu od 6 bita (RACH) i 25 bita (SCH) s dodatnim zaštitnim bitovima korištenjem generatora polinoma,

$$G_{RACH}(x) = x^6 + x^5 + x^3 + x^2 + x + 1 \quad (4-3)$$

$$G_{SCH}(x) = x^{10} + x^8 + x^6 + x^5 + x^4 + x^2 + 1. \quad (4-4)$$

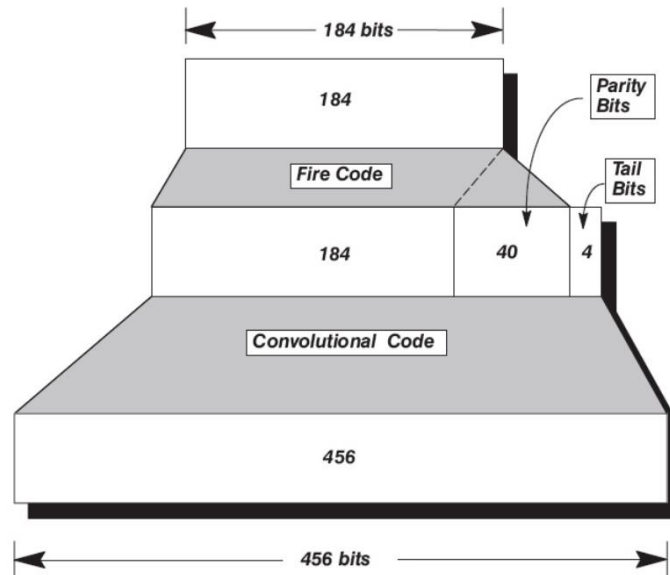
Tablica 4.1 Tipovi kanala s parametrima [4]

Channel type	Abbreviation	Block distance (ms)	Bits per block			Convolution code rate	Encoded bits per block	Interleaver depth
			Data	Parity	Tail			
TCH, full rate, speech Class I	TCH/FS	20	260				456	8
Class II			182	3	4	1/2	378	
TCH, half rate, speech Class I	TCH/HS	20	112				228	4
Class II			95	3	6	104/211	211	
TCH, full rate, 14.4 kbit/s	TCH/F14.4	20	290	0	4	294/456	456	19
TCH, full rate, 9.6 kbit/s	TCH/F9.6	5	4 × 60	0	4	244/456	456	19
TCH, full rate, 4.8 kbit/s	TCH/F4.8	10	60	0	16	1/3	228	19
TCH, half rate, 4.8 kbit/s	TCH/H4.8	10	4 × 60	0	4	244/456	456	19
TCH, full rate, 2.4 kbit/s	TCH/F2.4	10	2 × 36	0	4	1/6	456	8
TCH, half rate, 2.4 kbit/s	TCH/H2.4	10	2 × 36	0	4	1/3	228	19
FACCH, full rate	FACCH/F	20	184	40	4	1/2	456	8
FACCH, half rate	FACCH/H	40	184	40	4	1/2	456	6
SDCCH, SACCH			184	40	4	1/2	456	4
BCCH, NCH, AGCH, PCH		235	184	40	4	1/2	456	4
RACH		235	8	6	4	1/2	36	1
SCH			25	10	4	1/2	78	1
CBCH		235	184	40	4	1/2	456	4



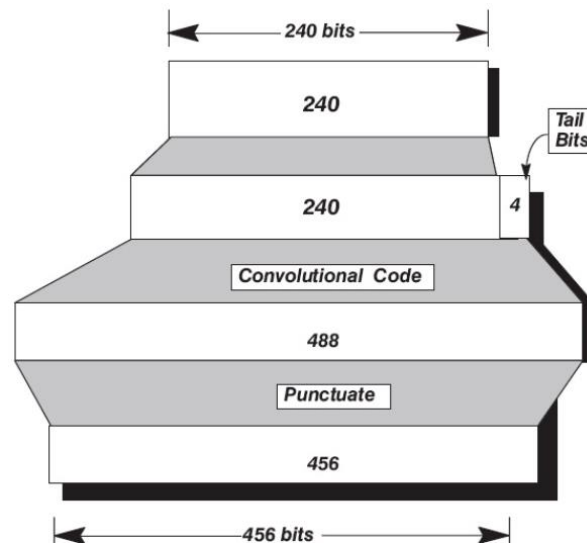
Sl.4.6 Kodiranje govornog kanala [17]

Prilikom kodiranja kanala signala koristi se sekvenca od 184 bita s dodavanjem 40 redundantnih bitova i 4 bita koji predstavljaju registre. Tih 228 bita postupkom konvolucijskog kodiranja prelazi u sekvencu od 456 bita (slika 4.7).



Sl.4.7 Kodiranje signalnog kanala [17]

Kodiranjem podatkovnog kanala (slika 4.8) sekvenci od 240 bita s dodatkom 4 bita repa preko konvolucijskog postupka kodiranja dobije se sekvenca od 488 bita. Blok od 488 bita reducira se brisanjem 32 bita kako bi dobili sekvencu od 456 bita prikladnu za daljnju obradu. Brisanje se obavlja na način da prvo obrišemo 11-ti bit, a zatim svaki 15-ti kroz sekvencu.



Sl.4.8 Kodiranje podatkovnog kanala [17]

U kodiranju kanala koristimo blok-kodiranje i dodavanjem paritetnih bitova dobivene sekvence prolaze konvolucijsko kodiranje nad različitim tipovima kanala korištenjem generatora polinoma (tablica 4.2) konvolucijskih kodova (tablica 4.3).

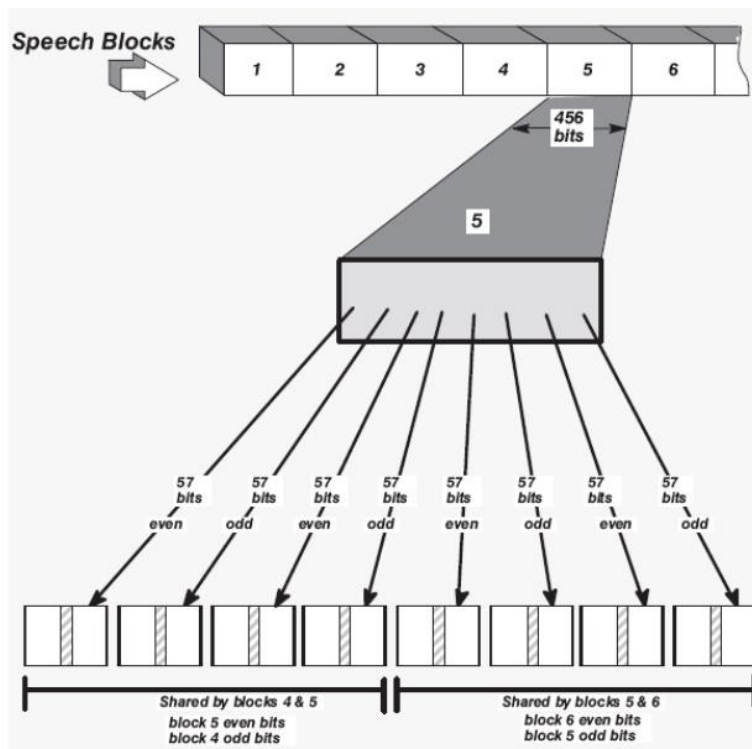
Tablica 4.2 Generatori polinoma konvolucijskog koda [4]

Type	Polynomial
G0	$1 + d^3 + d^4$
G1	$1 + d + d^3 + d^4$
G2	$1 + d^2 + d^4$
G3	$1 + d + d^2 + d^3 + d^4$
G4	$1 + d^2 + d^3 + d^5 + d^6$
G5	$1 + d + d^4 + d^6$
G6	$1 + d + d^2 + d^3 + d^4 + d^6$

Tablica 4.3 Primjena generatora polinoma po tipovima kanala [4]

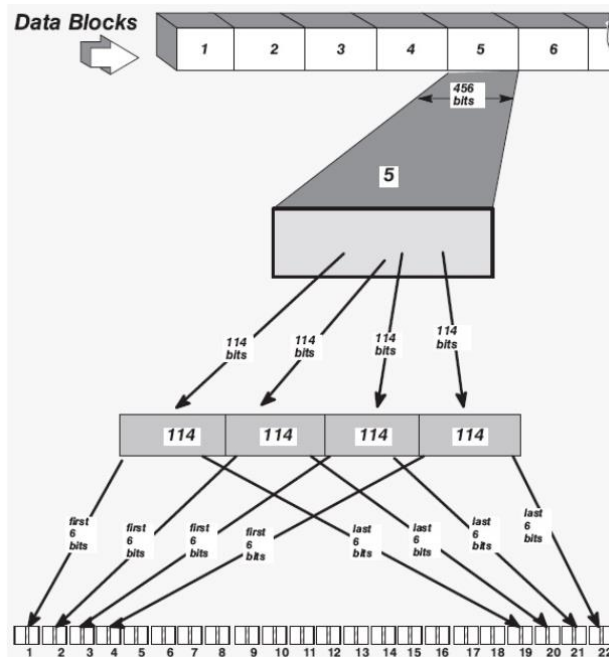
Channel type	Generator polynomial						
	G0	G1	G2	G3	G4	G5	G6
TCH, full rate, speech							
Class I	█						
Class II							
TCH, half rate, speech							
Class I					█		
Class II							
TCH, full rate, 14.4 kbit/s	█						
TCH, full rate, 9.6 kbit/s	█						
TCH, full rate, 4.8 kbit/s		█			█		
TCH, half rate, 4.8 kbit/s	█	█			█		
TCH, full rate, 2.4 kbit/s		█			█		
TCH, half rate, 2.4 kbit/s		█			█		
FACCHs	█						
SDCCHs, SACCHs	█						
BCCH, AGCH, PCH	█						
RACH	█						
SCH	█						

Nakon postupka konvolucije i formiranja blokova sekvenci od 456 bita, nad blokovima obavlja se postupak ispreplitanja. Dvije se vrste ispreplitanja koriste. Dijagonalno ispreplitanje se koristi u ispreplitanju govora i podataka, a pravokutno ispreplitanje u kontrolnom ispreplitanju. Nakon postupka kodiranja dobivamo slijed govornih blokova (slika 4.9) od 456 bita. Blokovi se dijele na 8 podblokova od 57 bita. Svaki blok sadržavat će samo bitove iz parnih položaja bita odnosno iz neparnih položaja bita. Kako svaki prasak sadrži 114 bitova, dijele ga dva govorna bloka. Svaki blok podijelit će četiri rafala s prethodnim blokom i četiri rafala s blokom koji ga naslijedi.



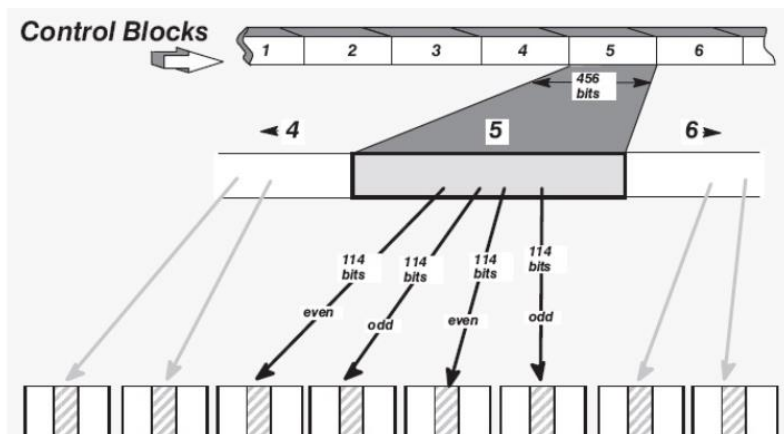
Sl.4.9 Postupak ispreplitanja govornog kanala [17]

Blokovi podataka (slika 4.10) nakon prethodno opisanog kodiranja sadrže 456 bita koji su podijeljeni u četiri podbloka od 114 bita. Ti se blokovi zatim međusobno isprepliću. Prvih 6 bitova smješteno je u prvi prasak. Prvih 6 bitova iz drugog bloka ide u drugi prasak itd. Svaki blok od 114 bita raspodijeljen je na 19 rafala, a ukupni blok će se raširiti na 22 rafala. Kaže se da podatkovni kanali imaju dubinu ispreplitanja 22, premda se to ponekad zove i dubina ispreplitanja 19.



Sl.4.10 Postupak ispreplitanja podatkovnog kanala [17]

Kontrolni blok (slika 4.11) od 456 bita dijelimo u četiri bloka od 114 bita. Svaki blok sadržava bitove za parne i neparne položaje. Rafali će se proizvesti pomoću ovih blokova.



Sl.4.11 Postupak ispreplitanja kontrolnog kanala [17]



## 5. PRIJENOS PUTEM KOMUNIKACIJSKOG KANALA

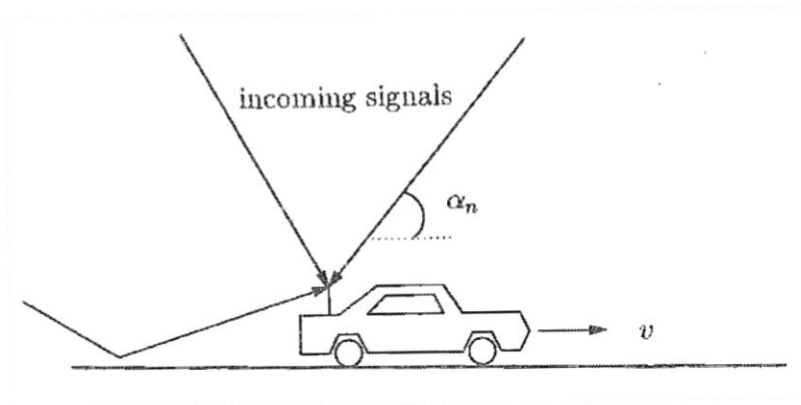
Prilikom bežičnog prijenosa, propagacija signala odvija se komunikacijskim kanalom koji je vremenski promjenjiv. Kako BER ukazuje na kvalitetu performansi pojedinog sustava potrebno odabrati takav model komunikacijskog kanala koji će zadovolji uvjete za stabilnost prijenosnog sustava. Mehanizmi propagacije koji utječu na vrijednost signala osim slabljenja u slobodnom prostoru su difrakcija, refleksija, refrakcija i raspršenje.

Difrakcija (*engl. diffraction*) se pojavljuje kada na putu propagacije između predajnika i prijemnika postoji prepreka sa velikim dimenzijama tijela u odnosu na valnu duljinu ( $\lambda$ ) elektromagnetskog radio vala i time formira sekundarne elektromagnetske valove iza tijela prepreke. Ovaj mehanizam objašnjava pojavu propagacije elektromagnetske energije bez postojanja optičke vidljivosti. Često se ovaj mehanizam naziva i mehanizam radio-sjene (*eng. shadowing*), zbog toga što difraktirani valovi mogu doći do prijemnika čak i u slučaju da je on u sjeni propagacijskih prepreka kroz koje ne može proći val. Raspršenje (*engl. scattering*) se dešava u slučajevima kada elektromagnetski val na svom putu prostiranja prema prijemniku pada na velike neravne površine ili bilo koje površine čije su dimenzije reda veličine njegove valne duljine ili manje, a kao posljedicu ima raspršivanje radio vala u svim pravcima. Refleksija (*engl. reflection*) se pojavljuje u slučajevima kada radio val na svom pravcu prostiranja pada na glatke površine koje imaju vrlo velike dimenzije u odnosu na njegovu valnu duljinu. Refrakcija (*engl. refraction*) se pojavljuje u slučaju kada dio elektromagnetskog radio vala prolazi kroz drugi medij različitih električnih osobina te mijenja svoj smjer prostiranja. Različiti načini propagacije vala stvaraju tzv. višestaznu okolinu (*engl. multipath environment*). Kao posljedica višestaznog širenja vala, dolazi do kašnjenja pojedinih komponenti i disperzije odaslanog signala te kolebanje u razini signala, odnosno fedinga (*engl. fading*). Višestazno prostiranje opisujemo preko optičke vidljivosti (*engl. LOS – line of sight*) i bez optičke vidljivosti (*engl. NLOS – non line of sight*). Upoznavajući fenomen fedinga, prijemni signal je izložen s tri razmjera prostorne varijacije kao što su brzi i spori feding i daljinska ovisnost. Za brzi feding kod kojeg replike originalnog signala dolaze iz svih pravaca bez obzira u kojem se pravcu kreće mobilna stanica koristi se termin feding na maloj prostornoj razmjeri (*engl. small-scale fading*). Kao rezultat promjene konfiguracije prepreka koje okružuju mobilnu stanicu za vrijeme njenog kretanja kroz okolinu propagacije, pojavljuju se varijacije oko prosječne vrijednosti signala oko koje se dešavaju brze fluktuacije signala. Te varijacije se dešavaju na razdaljinama koje su reda dimenzija samih okruženja zgrada. Feding koji se pojavljuje na ovakvim razdaljinama je poznat kao feding sjene, spori feding ili lognormalni feding. Općenito se za njega koristi termin feding na velikoj prostornoj razmjeri (*eng. large-scale fading*). Pored navedene osnovne klasifikacije fedinga uvodi se i klasifikacija po pitanju selektivnosti fedinga u pogledu širine frekvencijskog opsega. Tako da mobilni komunikacijski kanal ima neselektivan-ravan feding ako ima konstantno pojačanje i linearni fazni odziv na širini frekvencijskog opsega koja je veća od frekvencijske širine signala koji se prenosi preko tog kanala. Neselektivni – ravni feding se pojavljuje u slučajevima kada je frekvencijska širina signala  $B_t$  koji se prenosi manja od koherentne frekvencijske širine komunikacijskog kanala  $B_c$ ,

$$B_t \ll B_c \quad (5-1)$$

Koherentna frekvijska širina  $B_c$  predstavlja frekvijski opseg na kojim se komunikacijski kanal može smatrati „ravnim“ odnosno neselektivnim odnosno približni maksimalni frekvijski opseg na kojem će sve frekvencije signala najvjerojatnije biti pod utjecajem koreliranog fedinga. U suprotnom slučaju feding se naziva selektivnim.

Feding na maloj prostornoj razmjeri zovemo još Rayleighev feding. Kod velikog broja reflektiranih komponenti, anvelopu prijemnog signala uz nepostojanje komponente direktne zrake statistički opisujemo Rayleighovom distribucijom ili razdiobom, a uz postojanje komponente direktne zrake anvelopu opisujemo Riceovom distribucijom odnosno govorimo o Riceovom fedingu.



Sl.5.1 Model prijemnog uređaja u pokretu [7]

Mobilni uređaj brzine  $v$  (slika 5.1) u bilo kojem trenutku prima  $N$  komponenti signala s različitim upadnim kutom kojeg možemo prikazati linearnom superpozicijom vektora valova s slučajnim faznim pomakom na čije frekvencije utječe Dopplerov pomak  $f_n$  prijenosne frekvencije. Pomak je funkcija brzine, prijenosne frekvencije i upadnog kuta [7],

$$f_n = \frac{v}{\lambda} \cos \alpha_n \quad (5-2)$$

gdje je  $\alpha_n$  upadni kut dolaznog vala,  $v$  brzina mobilnog uređaja, a  $\lambda$  valna duljina frekvencije odašiljača. Maksimalni Dopplerov pomak događa se kod upadnog kuta jednakom nuli i definiran je izrazom,

$$f_D = \frac{v}{\lambda}. \quad (5-3)$$

Prijemni signal  $e(t)$ , kao zbroj  $N$  upadnih vektora signala opisan je izrazima

$$e(t) = E \sum_{n=1}^N e_n \cos(2\pi f_c t + \theta_n), \quad (5-4)$$

$$\theta_n = 2\pi f_n t + \phi_n, \quad (5-5)$$

gdje je  $\phi_n$  slučajni fazni kut ravnomjerno raspoređen od 0 do  $2\pi$ . Komponente  $e_n$  daju srednju vrijednost koja jednaka  $E[\sum_{n=1}^N e_n^2] = 1$ . Iz toga proizlazi da  $E^2/2$  predstavlja prosiječnu snagu na prijemniku. Za statističku analizu prijemnog signala jednadžba (5-4) prelazi u oblik,

$$e(t) = T_c(t) \cos 2\pi f_c t - T_s(t) \sin 2\pi f_c t, \quad (5-6)$$

gdje je,

$$T_c(t) = E \sum_{n=1}^N e_n \cos(2\pi f_n t + \phi_n), \quad (5-7)$$

$$T_s(t) = E \sum_{n=1}^N e_n \sin(2\pi f_n t + \phi_n). \quad (5-8)$$

Za veliki  $N$  granični teorem, vrijednosti  $T_c(t)$  i  $T_s(t)$  opisuje Gausovim slučajnim procesom. Označavajući  $T_c(t)$  i  $T_s(t)$  kao slučajne varijable  $T_c$  i  $T_s$  uz fiksni  $t$  sa srednjom varijancom jednakom nuli, vrijedi sljedeće:

$$E[T_c^2] = E[T_s^2] = \frac{E^2}{2} \quad (5-9)$$

$$E[T_c T_s] = 0. \quad (5-10)$$

Varijable  $T_c$  i  $T_s$  opisane su Gausovom funkcijom gustoće vjerojatnosti oblika

$$p(x) = \frac{1}{\sqrt{2\pi b}} e^{-\frac{x^2}{2b}}, \quad -\infty < x < \infty \quad (5-11)$$

gdje je  $b = E^2/2$  srednja snaga, a  $x = T_c$  ili  $T_s$ . Funkcija gustoće vjerojatnosti anvelope uz fiksni  $t$ ,

$$u = \sqrt{T_c^2 + T_s^2} \quad (5-12)$$

od  $e(t)$  jednaka Rayleighovoj razdiobi,

$$p(u) = \begin{cases} \frac{u}{b} e^{-\frac{u^2}{2b}}, & u \geq 0 \\ 0, & u < 0 \end{cases} . \quad (5-13)$$

Gustoća vjerojatnosti faze,

$$\phi = \tan^{-1} \frac{T_s}{T_c} \quad (5-14)$$

od  $e(t)$  je uniformno definirana,

$$p(\phi) = \frac{1}{2\pi}, \quad 0 \leq \phi < 2\pi . \quad (5-15)$$

Autokorelacijska funkcija od  $u(t)$  kod pretpostavke izotropnog raspršenja opisana je kao,

$$E[u(t)u(t + \tau)] = \frac{E^2}{2} J_0(2\pi f_D \tau) \quad (5-16)$$

gdje je  $J_0$  Besselova funkcija nultog reda. U analizi performansi komunikacijskog sustava uobičajeno polazište modela kanala je kanal s aditivnim bijelim Gausovim šumom (AWGN, *engl. additive white gaussian noise channel*). Shannon je izveo poznatu relaciju za granični kapacitet AWGN kanala,

$$C = B \log_2(1 + \Gamma) \quad \text{bit/s}, \quad (5-17)$$

gdje je  $B$  širina pojasa kanala, a  $\Gamma = E_s/N$  odnos signal – šum sustava. Relacija najbolje opisuje sustav uz poznate parametre  $\Gamma$  i  $B$ . Kanal ima beskonačni kapacitet kada  $\Gamma$  teži u beskonačnost odnosno ne može postići beskonačni kapacitet kad  $B$  teži u beskonačnost jer se snaga šuma povećava s povećanjem širine pojasa. Ako je  $N = N_0 B$ , gdje je  $N_0$  snaga šuma po hercu, a širina pojasa teži u beskonačnost jednadžba kapaciteta je jednaka,

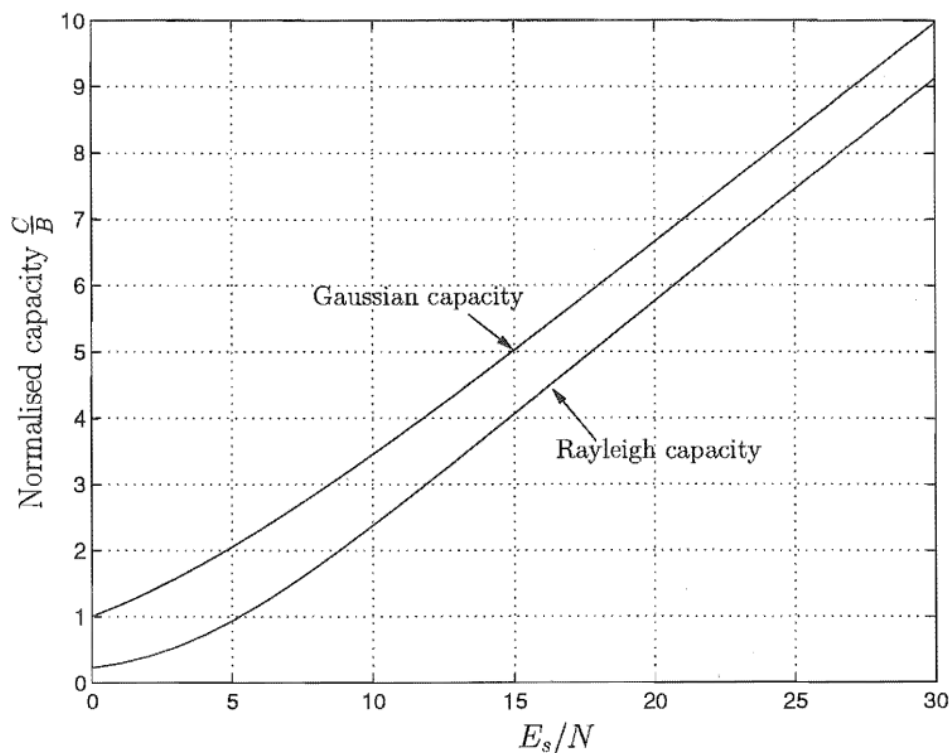
$$\lim_{B \rightarrow \infty} C = \frac{1}{\log_e 2} \frac{E_s}{N_0} \approx 1.44 \frac{E_s}{N_0} . \quad (5-18)$$

Ovo definira Shannovu granicu od -1.6 dB ispod koje komunikacija bez pogrešaka nije moguća na bilo kojoj pojasnoj širini.

Rayleighov fading možemo opisati kao konvencionalni AWGN kanal s vremenskim promjenjivim omjerom signal-šum (SNR, *engl. signal to noise ratio*) koji sadrži Rayleighovu razdiobu. Kapacitet Rayleighovog kanala možemo dobiti usrednjavanjem trenutnog AWGN kapaciteta preko Rayleighove razdiobe. Derivacija daje prosječni kapacitet Rayleighovog kanala za  $\Gamma > 2$ ,

$$C = B \log_2 e \cdot e^{-1/\Gamma} \left( -\gamma + \ln \Gamma + \frac{1}{\Gamma} \right) \quad (5-19)$$

gdje je  $\gamma$  Eulerova konstanta 0.5772.



Sl.5.2 Kapacitet Gaussovog i Rayleighovog kanala [7]

Iz granica kapaciteta kanala jednađbi (5-17) i (5-19) vidimo da je potrebni SNR Rayleighovog kanala veći za 2.5 dB (slika 5.2) za postizanje istog kapaciteta kao u Gaussovom kanalu za velike SNR. Za neograničenu širinu pojasa kapacitet Rayleighovog kanala jednak je Gaussovom.

Povećanje brzine vlakova i povećanje broja kvalitetnih usluga korisnicima željezničke infrastrukture ima za posljedicu pogoršanje prijenosnih uvjeta u komunikacijskom kanalu. Povećanje brzine utječe na pouzdanost komunikacijske veze povećanjem vrijednosti BER-a, Dopplerovog pomaka frekvencije, pojavom prijarnih pogrešaka i gubitka ortogonalnosti podnosilaca u postupku OFDM-a (OFDM, *engl. orthogonal frequency division multiplexing*) što dovodi do interferencije signala. OFDM je glavni modulacijski postupak dugoročnog razvoja bežične komunikacije za željeznicu (LTE-R, *engl. long term evolution for railway*). Prilikom mjerenja kvalitete prijenosa signala putem komunikacijskog kanala osim SNR-a, zbog prisustva interferencije između radiosustava potrebno je razmotriti omjer signala prema šumu i interferenciji (SINR, *engl. signal to interference plus noise ratio*) koji je opisan relacijom [18]:

$$SINR = \frac{P_D}{P_I + P_N} = \frac{\sigma^2 P}{ICI + n_0 W} \quad (5-20)$$

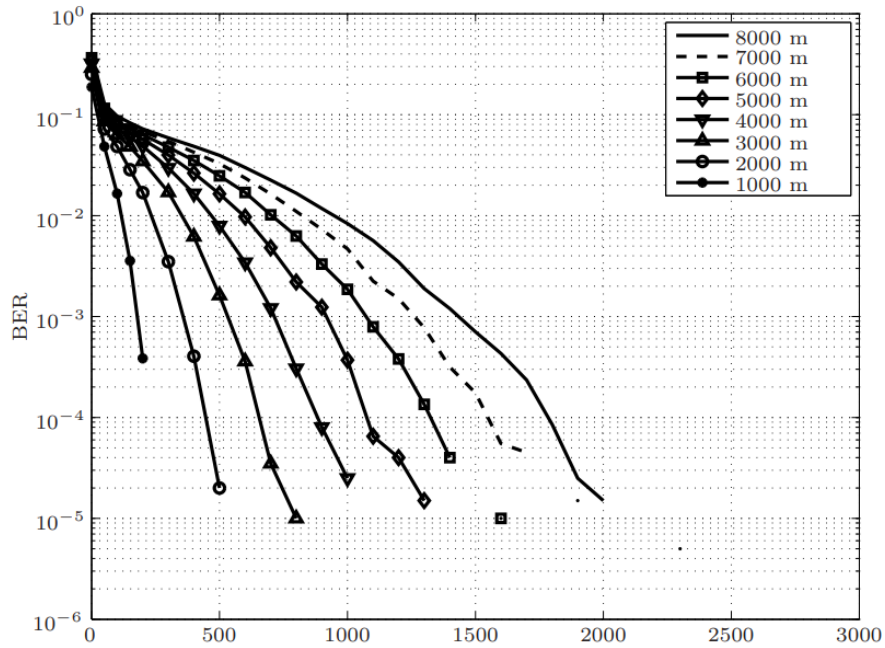
gdje je ICI interferencija između podnosilaca (ICI, *engl. inter carrier interference*),  $P$  odašiljačka snaga,  $n_0$  spektralna gustoća snage šuma, a  $W$  širina pojasa.

Tablica 5.1 Vrijednosti SINR-a prema modulacijskim postupcima i prijenosa podataka [18]

MCS Scheme	SINR(dB)	Data Rate (Mbps/MRU)
QPSK, R=1/2	2.1	18.637
QPSK, R=3/4	3.0	27.956
QPSK, R=7/8	4.7	32.615
16QAM, R=1/2	6.8	37.274
16QAM, R=3/4	7.0	55.911
64QAM, R=3/4	10.6	83.867

Parametri mreže trebaju biti odabrani tako da se njihovom kombinacijom može postići zahtijevani BER. To uključuje odabir modulacijskog postupka i omjera koda (MCS, *engl. modulation and coding scheme*). Tablica 5.1 prikazuje za različite kombinacije MCS-a vrijednost SINR-a za postizanje BER-a reda veličine  $10^{-5}$ . Povećanjem spektralne učinkovitosti modulacijskog postupka raste zahtijevana vrijednost SINR-a. Isto tako zahtijevani SINR raste i povećanjem omjera koda tj. smanjenjem stupnja zaštite od pogrešaka.

Zbog pojave interferencije signala sa susjednim sustavima LTE određena je minimalna duljina razmaka između LTE bazne stanice i GSM-R mobilne stanice (slika 5.3). Na slici vidimo ovisnost vrijednosti BER-a prema udaljenosti između LTE bazne stanice i GSM-R mobilne stanice i radijusa ćelije GSM-R sustava. S radijusom ćelije od 7 km minimalna udaljenost je oko 1500 m koju moramo ostvariti kako bi sustav radio bez smetnji i ostvario vrijednost BER reda veličine  $10^{-4}$ .



Sl. 5.3 Odnos BER-a prema udaljenosti između LTE<sub>BS</sub> i GSM-R<sub>MS</sub> u metrima [19]

Tablica 5.2 sadrži minimalne razine jakosti signala u dBm-ima za pojedine brzine prijenosa podataka uz ispunjavanje uvjeta za vrijednosti BER-a.

Tablica 5.2 Minimalne vrijednosti signala za granične vrijednosti BER-a [20]

	9600 bits/sec	4800 bits/sec	2400 bits/sec
BER < 0.01	-104 dBm	-106 dBm	-109 dBm
BER < 0.001	-101 dBm	-104 dBm	-106 dBm
BER < 0.0001	-98 dBm	-101 dBm	-103 dBm

## 6. ZAKLJUČAK

Mobilne komunikacije postale su bitan element sigurnog promet i automatskog upravljanja vlakova velikih brzina. Europske željeznice razvile su novu generaciju komunikacijske mreže bazirane na GSM tehnologiji nazvanu GSM-R s ciljem stvaranja jedinstvene komunikacijske platforme koja će osigurati internu operativnost željezničkog prometa kao temelj europskog sustava upravljanja vlakova. Velike brzine vlakova imaju potrebu za visokim stupnjem pouzdanosti komunikacijskog sustava koji omogućava smanjenje vanjskih fizikalnih utjecaja na kvalitetu komunikacije pri prijenosu podataka. Visok stupanj pouzdanosti je postignut implementacijom raznih tehnika ili postupaka kodiranja kanala u svrhu otkrivanja i ispravljanja pogrešaka koje se pojavljuju u komunikaciji. GSM-R je željeznička verzija sustava GSM te koristi tehnike slične kao i u sustavu GSM. GSM sustav koristi kombinaciju nekoliko postupaka. Uz blok-kodove koji generiraju bitove pariteta za otkrivanje pogreški i konvolucijskih kodova koji dodaju redundanciju tu je postupak ispreplitanja koji smanjuje utjecaj skupnih pogrešaka. Ove tehnike omogućavaju pouzdani prijenos i u slučaju negativnih pojava u komunikacijskom kanalu.



## 7. LITERATURA

- [1] Y. Jiang, A Practical Guide to Error-Control Coding Using MATLAB, Artech House, 2010.
- [2] A. Neubauer, J. Freudenberger, V. Kühn, Coding Theory algorithms, architectures, and applications, John Wiley & Sons, 2007.
- [3] S. Grgić, G. Šišul, Zabilješke s predavanja na predmetu Željeznički informacijsko komunikacijski sustavi, Fakultet elektrotehnike i računarstva, 2014.
- [4] J. Eberspächer, H. J. Vögel, C. Bettstetter, Ch. Hartmann, GSM Architecture, Protocols and Services, John Wiley & Sons, 2009.
- [5] J. Montelius, GSM Network and Services,  
<https://people.kth.se/~johanmon/attic/2g1723/lectures.html> (pristup, svibanj 2020.)
- [6] M. Nižetić „Zaštitno kodiranje signala,  
<https://personal.oss.unist.hr/~mnizetic/Za%C5%A1titno%20kodiranje%20signala-skripta.pdf> (pristup, ožujak 2019.)
- [7] R. van Nobelen, Coding for the Rayleigh Fading Channel, doktorski rad, 1996.  
<https://ir.canterbury.ac.nz/handle/10092/6060> (pristup, ožujak 2020.)
- [8] M. Hamidović, Simulacijski modeli u povećanju efikasnosti planiranja 2G/3G mobilnih mreža, magistrski rad, Univerzitet u Sarajevu, Elektrotehnički fakultet u Sarajevu, 2011.
- [9] B. Sklar, The Characterization of Fading Channels,  
[https://ptgmedia.pearsoncmg.com/images/art\\_sklar5\\_fading/elementLinks/art\\_sklar5\\_fading.pdf](https://ptgmedia.pearsoncmg.com/images/art_sklar5_fading/elementLinks/art_sklar5_fading.pdf) (pristup: srpanj 2019.)
- [10] B. Zabin, I. A. Imon, Performance comparasion between different channel models with channel estimation and adaptive aqualization using Rayleigh fading channel,  
<http://dspace.bracu.ac.bd/xmlui/bitstream/handle/10361/469/Performance%20comparison%20between%20different%20channel.pdf?sequence=1&isAllowed=y>  
(pristup: studeni 2019.)
- [11] N. Rožić, Informacija i komunikacije, kodiranje s primjenama, Alinea, Zagreb, 1992.
- [12] I. S. Pandžić, Uvod u teoriju informacije i kodiranje, Element, Zagreb, 2007.
- [13] D. Petrović, „Dekodiranje Reed Solomon kodova pomoću dekodera s tvrdom odlukom“, diplomski rad, Sveučilište Josipa Jurja Strossmayera u Osijeku, ETF, 2012.  
<https://pdfslide.net/documents/konvolucijski-kodovi.html>
- [14] D. Žagar, Bilješke s predavanja na predmetu Kodovi i kodiranje, ETF Osijek, 2011.
- [15] A. Sniady, Communication Technologies Support to Railway Infrastructure and Operations, PhD. Thesis, 2015.  
[file:///E:/Downloads/alesn\\_PhD\\_Thesis\\_final\\_version\\_with\\_covers\\_compressed.pdf](file:///E:/Downloads/alesn_PhD_Thesis_final_version_with_covers_compressed.pdf)  
(pristup: siječanj 2020.)

- [17] <http://teletopix.org/category/gsm/>
- [18] Z. Yuzhe, A. Bo, Quality of Service Improvement for High-Speed Railway Communications, China Communications, vol. 11, November 2014, str. 156-167.
- [19] F. Vihlborg, On Models For Interference Calculations between Radio Communication Systems, Master's Degree Project Stockholm, Sweden December 20112011. <http://www.diva-portal.org/smash/get/diva2:467170/FULLTEXT01.pdf> (pristup: veljača 2020.)
- [20] G. Dalton, GSM-R Implementation and Procurement Guide, 2009. [https://uic.org/IMG/pdf/2009gsm-r\\_guide.pdf](https://uic.org/IMG/pdf/2009gsm-r_guide.pdf) (pristup: veljača 2020.)
- [21] M. Zhan, Z. Pang, D. Dzung M. Xiao, Channel Coding for High Performance Wireless Control in Critical Applications: Survey and Analysis, IEEE Access, vol. 6, May 2018, str. 29648-29664.

## SAŽETAK

### POSTUPCI ZAŠTITE OD PRIJENOSNIH POGREŠAKA U SUSTAVU GSM-R

U ovom radu su obrađene tehnike zaštite od pogrešaka implementirane u globalnom mobilnom komunikacijskom sustavu za željeznice. Opisana su dva tipa blok-kodiranja, *fire*-kod i paritetni-kod, konvolucijsko kodiranje i ispreplitanje. Predstavljene su karakteristike GSM-R sustava kroz širinu i raspodjelu frekvencijskog pojasa, tipove komunikacijskih kanala i pripadajuće tehnike zaštite od pogrešaka zajedno s parametrima za svaki tip kanala.

Ključne riječi: konvolucijski kod, Viterbijev algoritam, Rayleighov kanal, Dopplerov pomak, ispreplitanje, generator polinoma, odnos signal-šum

## **ABSTRACT**

### **METHODS OF PROTECTION OF TRANSMISSION ERROR IN THE GSM-R SYSTEM**

This paper deals with error protection techniques implemented in the global mobile communication system for railway. Two types of block-coding, fire-code and parity-code, convolutional coding and interleaving, are described. The characteristics of the GSM-R system through the bandwidth and frequency allocation, the types of communication channels and the associated error protection techniques for each channel type are presented.

Keywords: convolution code, Viterbi algorithm, Rayleigh channel, Doppler shift, interleaving, polynomial generator, signal-to-noise ratio

## ŽIVOTOPIS

Darko Petrović rođen 09.03.1973. u Vinkovcima. Nakon drugog razreda srednje tehničke škole u Vinkovcima odlazi u Željezničku tehničku školu Zagreb. Nakon završetka srednje škole zaposlen je na Dionici telekomunikacije Osijek u Hrvatskim željeznicama (Sekcija signalizacije i telekomunikacije) kao elektrotehničar TK (kabel monter) gdje boravi do 1996. g. kada prelazi na Dionicu telekomunikacije Vinkovci. Upisuje 1997.g. izvanredni stručni studij na Elektrotehničkom fakultetu Osijek kojeg završava 2003.g. 2005.g. prelazi na novo radno mjesto inženjera vođa mjerne grupe u servisnoj Dionici signalno sigurnosnog uređaja Vinkovci. Po završetku stručnog studija nastavlja izvanredno studiranje na sveučilišnom studiju kojeg završava 2012.g. 2013.g. prelazi na novo radno mjesto Glavnog inženjera za SS uređaje Područne radne jedinice održavanja SS i TK uređaja istok.

## **BIOGRAPHY**

Darko Petrović was born on March 9.1973 in Vinkovci. After the second grade of the secondary technical school in Vinkovci, he moved to the Railway Technical School in Zagreb. After graduating from high school, he got a job at the Institute of Telecommunications Osijek in the Croatian Railways (Department of Signaling and Telecommunications) as an electrician TK (cable installer) where he stayed until 1996 when he moved to the Department of Telecommunications Vinkovci. In 1997 he enrolled in part-time professional studies at the Faculty of Electrical Engineering in Osijek, which he completed in 2003. In 2005. he moved to a new job as an engineer, head of the measuring group in the service part of the signal safety device Vinkovci. After completing his professional studies, he continued his part-time studies at the university, which he completed in 2012. In 2013. he transferred to the new position of Chief Engineer for Regional Work Units of SS Devices for Maintenance of SS and TK Devices East.