

## PROCENA PERFORMANSI DEKODOVANJA BCH KODOVA POMOĆU TRELISA I BCJR ALGORITMA

### PERFORMANCE EVALUATION OF BCH CODES WITH BCJR TRELIS DECODING

Tanja Živković Jovanović, *Telenor d.o.o, Beograd*  
Predrag Ivaniš, *Elektrotehnički fakultet, Beograd*

**Sadržaj** – BCH kodovi predstavljaju jednu od najpoznatijih klasa cikličnih kodova. Dosadašnje algoritme za dekodovanje BCH kodova karakteriše velika kompleksnost, uz ograničenje da ih nije moguće primeniti za dekodovanje drugih linearnih blok kodova. BCJR algoritam za dekodovanje linearnih blok kodova sa maksimalnom verodostojnošću, se može primeniti na bilo koji kod za koji je moguće formirati trellis dijagram. Takođe, poznato je da je za svaki BCH kod moguće kreirati trellis. U ovom radu, analiziran je generalni princip BCJR dekodovanja linearnih blok kodova pomoću trellisa za BCH kodove: BCH (7,4), BCH (15,7) i BCH (15,5). Na osnovu dobijenih simulacionih dijagrama, data je procena performansi BCJR dekodovanja navedenih BCH kodova u odnosu na nekodovani prenos. Analiziran je kanal sa prisustvom aditivnog belog Gauss-ovog šuma i BPSK modulacijom.

**Abstract** – BCH codes are the most important group of cyclic codes. Decoding algorithms of BCH codes are characterized by exceptional complexity, with the limitation that they can not be applied for decoding of other linear block codes. Maximum-likelihood BCJR decoding algorithm of linear block codes, can be applied to any code for which it is possible to form trellis. Also, it is known that for every BCH code, trellis can be formed. In this paper, the general approach of BCJR decoding of linear block codes is analyzed, using trellis and BCH codes: BCH (7,4), BCH (15,7) and BCH (15,5). Based on the obtained simulation diagrams, performance evaluation of BCJR decoding of BCH codes is presented, in comparison to uncoded transmission. Additive white Gaussian noise channel model with BPSK modulation is analyzed.

**Ključne reči** – Linearni blok kodovi, BCJR dekodovanje, trellis dijagram, BCH kodovi, ML dekodovanje.

**Keywords** – Linear block codes, BCJR decoding, trellis, BCH codes, ML decoding.

#### 1. UVOD

Linearni blok kodovi spadaju u grupu zaštitnih kodova. Dobro je poznato da zaštitno kodovanje predstavlja efikasan mehanizam pomoću kojeg se može omogućiti pouzdan prenos podataka u otežanim uslovima prenosa. Linearne blok kodove karakteriše jednostavan matematički opis. Ciklični kodovi predstavljaju podklasu linearnih blok kodova i oni imaju važnu ulogu u savremenim telekomunikacionim sistemima [1]. BCH (*Bose-Chaudhuri-Hocquenghem*) kodovi su najpoznatiji ciklični kodovi. Pronađeni su nezavisno od strane Hokenhema [2] s jedne, i Bouza i Čodhurija [3] s druge strane.

Generalno, postoje dva načina za dekodovanje linearnih blok kodova, tvrdo i meko [1]. Meko dekodovanje daje bolje rezultate u pogledu verovatnoće grešaka zaostalih nakon dekodovanja i ima veći kodni dobitak. Način dekodovanja blok kodova podrazumeva dekodovanje jedne reči nezavisno od druge, tako da ne postoji propagacija grešaka.

Tehnika dekodovanja linearnih blok kodova pomoću trellisa poseduje veliki potencijal da doprinese značajnom poboljšanju performansi u postojećim komunikacionim i informacionim sistemima, kao što su mobilni i radio sistemi, magnetni i optički uređaji za čuvanje podataka, itd. Preduslov

za implementaciju ovakvog načina dekodovanja jeste dobro poznavanje strukture trellis dijagrama.

Dosadašnje algoritme za dekodovanje BCH kodova [1] karakteriše izuzetna kompleksnost, uz činjenicu da implementiranje ovakvih algoritama ima ograničenu primenu isključivo na BCH kodove i nije ih moguće koristiti za dekodovanje drugih linearnih blok kodova. Korišćenje algoritama za dekodovanje koji su bazirani na trellis dijagramu, kao što su dekodovanje na bazi Viterbijevog [4] i BCJR algoritma [5], donosi nekoliko suštinskih prednosti:

1. Predstavljanje linearnog blok koda pomoću trellisa je najjednostavniji način za grafičku prezentaciju koda.

2. Predstavljanjem linearnog blok koda ( $n,k,d$ ) pomoću trellisa, se može analizirati kompleksnost samog koda. Kompleksnost minimalnog trellisa određuje kompleksnost koda za razliku od parametara koda  $n$  (dužina kodne reči) i  $k$  (dužina informacione reči), koji to ne obezbeđuju.

3. Algoritmi za dekodovanje, koji su bazirani na trellis dijagramu, predstavljaju jedan od najefikasnijih poznatih metoda za postizanje dekodovanja sa minimalnom verovatnoćom zaostale greške. U slučaju kada su apriorne verovatnoće pojavljivanja simbola u kanalu jednake, ovaj način dekodovanja se svodi na dekodovanje sa maksimalnom

verodostojnošću (*ML-Maximum-Likelihood*). Dok se u opštem slučaju svodi na dekodovanje sa maksimalnom aposteriornom verovatnoćom (*MAP – Maximum Aposteriori Probability*).

4. Korišćenje ovih algoritama obezbeđuje uniformnost u pristupu dekodovanja, jer je ove algoritme moguće sprovesti nad bilo kojim treliis dijagramom, a poznato je da se za svaki linearan blok kod može formirati treliis.

U narednom odeljku je opisan način dobijanja treliis dijagrama za BCH kodove, predložen u [6]. Analizirani su kodovi: BCH (7,4), BCH (15,5) i BCH (15,7). U radu je opisan simulacioni model za implementaciju BCJR algoritma dekodovanja u slučaju mekog i tvrdog dekodovanja sa različitim brojem kvantizacionih nivoa. Na osnovu dobijenih rezultata, data je procena performansi dekodovanja BCH kodova korišćenjem treliisa i BCJR algoritma, u uslovima delovanja aditivnog belog Gausovog šuma i BPSK modulacije.

## 2. FORMIRANJE TRELIIS DIJAGRAMA ZA BCH KODOVE

Osnovna karakteristika BCH kodova je da se dobijaju konstruktivnim putem. Nakon što se postavi zahtev u pogledu korekcionih sposobnosti koda, množenjem odgovarajućih minimalnih polinoma može se doći do generišućeg polinoma. Generišući polinom  $g(x)$ , BCH koda  $(n,k)$  je stepena  $n-k$ .

Struktura treliis dijagrama svih cikličnih kodova je analizirana u [6]. Ako se posmatra  $(n,k)$  ciklični kod  $C$  nad poljem  $GF(2)$  sa generišućim polinomom

$$g(X) = 1 + a_1X + a_2X^2 + \dots + a_{n-k}X^{n-k-1} + X^{n-k}, \quad (1)$$

generišuća matrica  $G$  ovog koda ima oblik

$$G = \begin{bmatrix} 1 & a_1 & a_2 & \dots & \dots & a_{n-k-1} & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & a_1 & a_2 & \dots & \dots & a_{n-k-1} & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 & a_1 & a_2 & \dots & \dots & a_{n-k-1} & 1 \end{bmatrix}. \quad (2)$$

Da bi se olakšalo formiranje treliisa, generišuća matrica  $G$  se transformiše u specijalnu formu. Neka je

$$v = \{v_0, v_1, \dots, v_{n-1}\} \quad (3)$$

nenultna binarna  $n$ -torka. Prva nenultna komponenta  $n$ -torke  $v$  se naziva vodeća jedinica, a poslednja nenultna komponenta se naziva poslednja jedinica. Na primer, u reči  $(0,1,0,1,0,1,0,1,0)$  vodeća i poslednja jedinica su  $v_1$  i  $v_7$ . Za generišuću matricu  $G$  koda  $C$  se kaže da je u *treliis orijentisanjoj formi (TOF)* ako su zadovoljeni sledeći uslovi:

1. Vodeća jedinica svake vrste matrice  $G$  se pojavljuje u koloni pre vodeće jedinice svake naredne vrste, odnosno vrste ispod nje.

2. Ni jedne dve vrste nemaju poslednje jedinice u istim kolonama.

Vidi se da je generišuća matrica koda  $C$ , navedena u relaciji (2), već u *TOF*. Stoga se svaka generišuća matrica koda  $C$  može transformisati u *TOF* pomoću koraka Gausovog algoritma (ili elementarnim operacijama nad vrstama matrice). Može se zapaziti da generišuća matrica u *TOF* nije neophodno u sistematskoj formi.

U knjizi [6] je pokazan način za formiranje treliis dijagrama na osnovu generišuće matrice u *TOF*. Za svaku

vremensku instancu  $i$  je potrebno pronaći prema instrukcijama navedenim u [6]:  $G_i^s$  - aktivni vremenski raspon;  $a^*$  - trenutni ulazni informacioni bit;  $a^0$  - najstariji informacioni bit sačuvan u memoriji kodera u trenutku  $i$ ;  $A_i^s$  - podskup informacionih bita koji odgovaraju vrstama iz  $G_i^s$ . Informacioni biti iz  $A_i^s$  definišu stanje kodera u vremenskoj instanci  $i$ .

U [6] se pokazuje da je za bilo koji ciklični kod  $(n,k)$ , maksimalan broj stanja u treliisu na određenoj dubini jednak  $\min\{k, n-k\}$ . Tako su za BCH kod (7,4), koji ispravlja jednu grešku, i ima generišući polinom

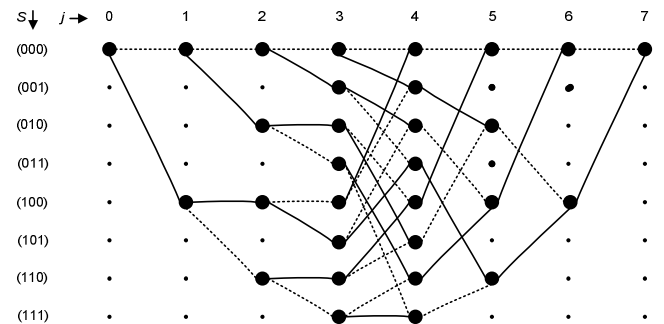
$$g(x) = x^3 + x + 1, \quad (5)$$

navedene vrednosti prikazane u tabeli 1.

Tabela 1: Informacije koje definišu stanja i oznake stanja za BCH kod (7,4)

$i$	$G_i^s$	$a^*$	$a^0$	$A_i^s$	Oznaka stanja
0	$\emptyset$	$a_0$	-	$\emptyset$	(000)
1	$\{g_0\}$	$a_1$	-	$\{a_0\}$	$(a_000)$
2	$\{g_0, g_1\}$	$a_2$	-	$\{a_0, a_1\}$	$(a_0 a_1 0)$
3	$\{g_0, g_1, g_2\}$	$a_3$	$a_0$	$\{a_0, a_1, a_2\}$	$(a_0 a_1 a_2)$
4	$\{g_1, g_2, g_3\}$	-	$a_1$	$\{a_1, a_2, a_3\}$	$(a_1 a_2 a_3)$
5	$\{g_2, g_3\}$	-	$a_2$	$\{a_1, a_3\}$	$(a_2 a_3 0)$
6	$\{g_3\}$	-	$a_3$	$\{a_3\}$	$(a_3 0 0)$
7	$\emptyset$	-	-	$\emptyset$	(0000)

Na osnovu podataka prikazanih u tabeli 1, dobija se treliis dijagram za BCH (7,4), prikazan na slici 1.



Slika 1: Treliis dijagram za kod BCH (7,4)

U radu je analiziran BCH kod (15,5), koji može da ispravi sve kombinacije od tri greške u kodnoj reči dužine 15 bita. Njegov generišući polinom je:

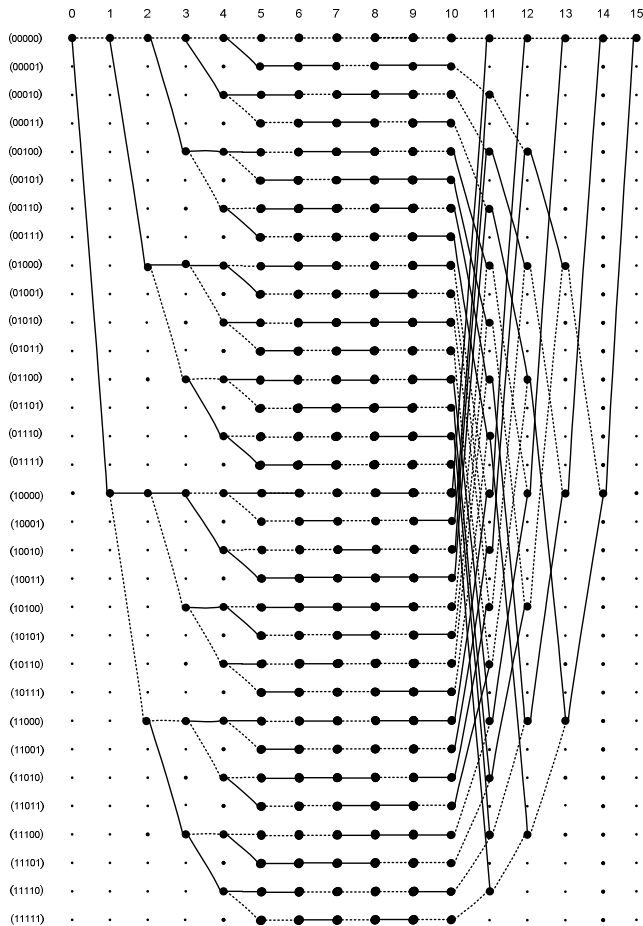
$$g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1. \quad (6)$$

Identičnim algoritmom, koji je naveden za BCH (7,4) kod, se nalazi treliis dijagram za BCH kod (15,5), koji je prikazan na slici 2. Maksimalan broj stanja treliis dijagrama je  $2^5 = 32$ .

U narednom poglavlju, procena efikasnosti se radi i za BCH kod (15,7), koji može da ispravi sve kombinacije od dve greške u kodnoj reči. Njegov generišući polinom je

$$g(x) = x^8 + x^7 + x^6 + x^4 + 1. \quad (7)$$

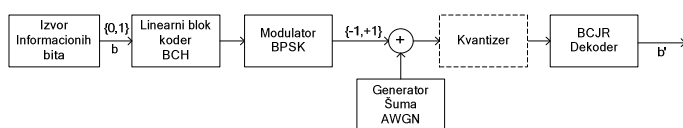
Broj stanja u trelis dijagramu za kod BCH (15,7) je  $2^7 = 128$ . Dakle, upravo iz strukture trelis dijagrama se može izvesti zaključak, da je BCH kod (15,7) u značajnoj meri kompleksniji od koda BCH (15,5), iako to osnovni parametri koda  $n$  i  $k$  ne pokazuju. Uz to, kod sa manjom kompleksnošću BCH (15,5) ispravlja veći broj grešaka u odnosu na kod sa većom kompleksnošću BCH (15,7).



Slika 2: Trelis dijagram BCH koda (15,5)

### 3. PROCENA PERFORMANSI BCH KODOVA SA MEKIM I TVRDIM BCJR DEKODOVANJEM SA RAZLIČITIM BROJEM KVANTIZACIONIH NIVOA

U radu je izvršena procena performansi za tri različita BCH koda: BCH (7,4), BCH (15,5) i BCH (15,7). Korišćena je BPSK modulacija i analiziran je kanal sa prisustvom aditivnog belog Gausovog šuma. U dekoderu je implementiran BCJR algoritam dekodovanja, predstavljen u [5]. BCJR algoritam dekodovanja koristi trelis dijagrame dobijene u prethodnom odeljku. Korišćen je simulacioni model, prikazan na slici 3.

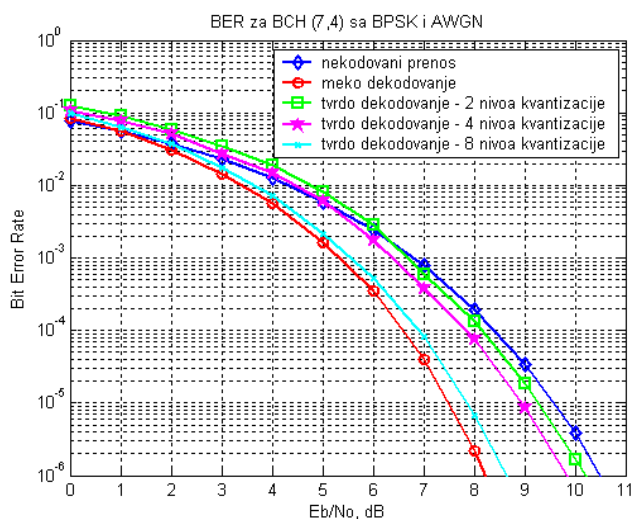


Slika 3: Simulacioni model za BCJR dekodovanje

Na slici 3 je prikazan simulacioni model za meko BCJR dekodovanje, kada se u BCJR dekoder, dovodi kvantizovani signal nastao superponiranjem aditivnog belog Gausovog šuma. Ovaj simulacioni model odgovara slučaju postizanja optimalnog dekodovanja sa maksimalnom verodostojnošću. Model je realizovan korišćenjem kvantizera na ulazu dekodera, sa različitim brojem kvantizacionih nivoa. U slučaju kada kvantizer ima dva nivoa, dekodovanje se naziva tvrdim jer se zasniva na tzv. „tvrdom odlučivanju“. U slučaju kada kvantizer ima teorijski beskonačan broj nivoa (odgovara slučaju kada se ukloni kvantizer) u pitanju je tzv. „meko dekodovanje“.

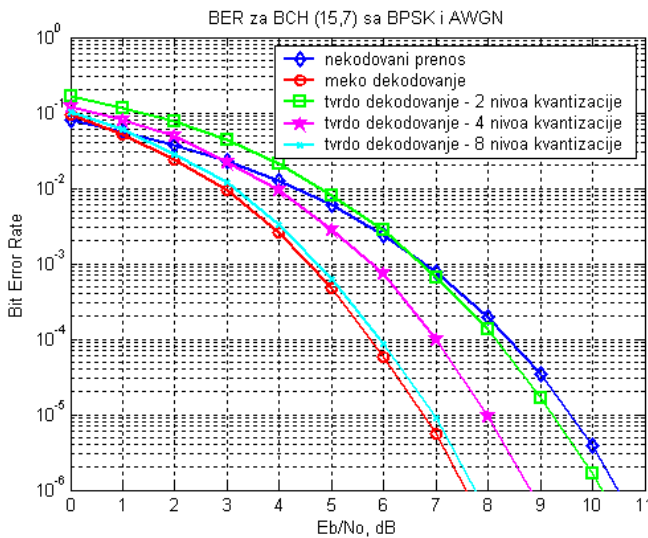
Procena performansi dekodovanja navedenih BCH kodova, je realizovana analizom dobijenih vrednosti BER-a (*Bit Error Rate*) za slučajeve nekodovanog prenosa, kodovanog BCH prenosa sa mekim BCJR dekodovanjem i kodovanog BCH prenosa sa tvrdim BCJR dekodovanjem u slučaju korišćenja dva, četiri i osam kvantizacionih nivoa. Na slikama 4, 5 i 6, su respektivno prikazane dobijene vrednosti BER-a, za kodove BCH (7,4), BCH (15,7) i BCH (15,5).

Na slici 4 se može videti da se za BCH (7,4) kod, bolje vrednosti BER-a za slučaj tvrdog dekodovanja sa dva kvantizaciona nivoa u odnosu na nekodovani prenos, dobijaju počev od vrednosti  $E_b/N_0 = 6.4$  dB. Povećavanjem broja kvantizacionih nivoa, vrednosti BER-a se približavaju vrednosti koja je dobijena za meko dekodovanje. Ova vrednost odgovara ML dekodovanju i u tom slučaju se granica boljitka korišćenja kodovanog prenosa, pomera na  $E_b/N_0 = 1$  dB.



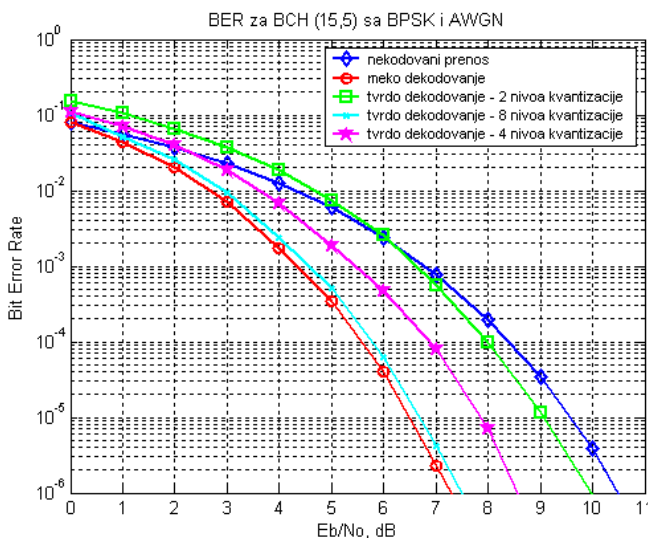
Slika 4: Vrednosti BER-a za BCH (7,4) sa BPSK i AWGN

Na slici 5, su prikazane dobijene vrednosti BER-a za BCH kod (15,7). U istoj vrednosti  $E_b/N_0 = 6.4$  dB, kodovani prenos sa tvrdim dekodovanjem, počinje da pokazuje bolje performanse za prenos signala, u odnosu na nekodovani prenos, kao i kod BCH (7,4). U slučaju mekog dekodovanja ova granica je u značajnoj meri povoljnija, i iznosi  $E_b/N_0 = 0.7$  dB. Vrednosti BER-a za meko dekodovanje su niže u odnosu na kod BCH (7,4). Može se zapaziti, da tvrd dekodovanje sa osam kvantizacionih nivoa, skoro dostiže vrednosti BER-a sa mekim dekodovanjem.



Slika 5: Vrednosti BER-a za BCH (15,7) sa BPSK i AWGN

Na slici 6, su prikazane dobijene vrednosti BER-a za BCH kod (15,5). Za vrednost  $E_b/N_0 = 6.1$  dB, kodovani prenos sa tvrdim dekodovanjem, počinje da pokazuje bolje performanse za prenos signala, u odnosu na nekodovani prenos, dok je u slučaju mekog dekodovanja ova granica značajno pomerena, i iznosi  $E_b/N_0 = 0.05$  dB. Vrednosti kodnih dobitaka za verovatnoću greške od  $10^{-6}$  su prikazane u tabeli 2.



Slika 6: Vrednosti BER-a za BCH (15,5) sa BPSK i AWGN

Tabela 2: Vrednosti kodnih dobitaka G [dB]

BER	G [dB]		
	BCH(7,4)	BCH(15,7)	BCH(15,5)
$10^{-3}$	1.5 dB	2.3 dB	2.5 dB
$10^{-4}$	1.8 dB	2.7 dB	2.9 dB
$10^{-5}$	2.1 dB	2.8 dB	3.0 dB
$10^{-6}$	2.3 dB	3.0 dB	3.2 dB

Može se primetiti, da su vrednosti BER-a za meko dekodovanje za kod BCH (15,5) niže u odnosu na vrednosti BER-a za kod BCH (15,7), što i odgovara činjenici da kod BCH (15,5) ispravlja tri greške pri prenosu, za razliku od koda BCH (15,7) koji ispravlja dve. Dobici koji se ostvaruju pri mekom dekodovanju u odnosu na tvrdo dekodovanje iznose 2.5 dB za kodove BCH (15,5) i BCH (15,7), dok za kod BCH (7,4) ovaj dobitak iznosi 2 dB.

Ukoliko se analizira ponašanje dobijenih BER vrednosti u slučaju postojanja kvantizera na ulazu BCJR dekodera, može se primetiti da za vrednost od osam kvantizacionih nivoa, dijagrami BER-a se u značajnoj meri približavaju dobijenim dijagramima za meko dekodovanje, ali bi preporuka bila da se u implementacionim dekoderima koriste kvantizeri sa šesnaest kvantizacionih nivoa.

Na osnovu komparativne analize svih predstavljenih parametara, može se zaključiti da od analiziranih kodova, kod BCH (15,5) ostvaruje najbolje performanse pri dekodovanju pomoću treliisa i BCJR algoritma.

#### 4. ZAKLJUČAK

U radu je analizirano dekodovanje BCH kodova pomoću BCJR algoritma koji je zasnovan na treliis dijagramu. Procenjene su performanse BCH kodova: BCH (7,4), BCH (15,5) i BCH (15,7). Primenjena je BPSK modulacija i analiziran je kanal sa prisustvom aditivnog belog Gausovog šuma. Pokazan je način formiranja treliis dijagrama za ciklične blok kodove, jer je poznavanje treliis strukture neophodno za sprovođenje BCJR dekodovanja, koje obezbeđuje dekodovanje sa maksimalnom verodostojnošću.

Procene performansi dekodovanja BCH kodova, pokazuju da se ostvaruju značajni kodni dobitci u odnosu na nekodovani prenos, u vrednosti od 1.5 do 3.2 dB, u zavisnosti od analiziranog BCH koda. Analizirano je ponašanje BER vrednosti u slučaju postojanja kvantizera na ulazu BCJR dekodera, sa različitim brojem kvantizacionih nivoa. Na osnovu dobijenih vrednosti se vidi da se sa povećanjem broja kvantizacionih nivoa, vrednosti BER-a približavaju vrednostima dobijenim za meko dekodovanje.

Predloženi metod za dekodovanje na osnovu treliisa i BCJR algoritma, obezbeđuje uniformni pristup dekodovanju linearnih blok kodova.

#### LITERATURA

- [1] D. Drajić, P. Ivaniš, *Uvod u teoriju informacija i kodovanje*, Akademsaka misao, Beograd, 2009.
- [2] A. Hocquenghem, "Codes correcteurs d'erreurs", *Chiffres*, Vol. 2, pp. 147-156, 1959.
- [3] R. C. Bose, D. K. Ray-Chaudhuri, "On a Class of Error Correcting Binary Group Codes", *Inform. Control*, Vol. 3, pp. 68-79, 1960.
- [4] A. J. Viterbi, "Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm", *IEEE Trans. Inform. Theory*, Vol. 13, pp. 260-269, 1967.
- [5] L. R. Bahl, J. Cocke, F. Jelinek, J. Raviv, "Optimal Decoding of Linear Codes for Minimizing Symbol Error Rate", in *IEEE Trans. on Inf. Theory*, pp. 284-287, March 1974.
- [6] S. Lin, D. J. Costello, *Error Control Coding (Second edition)*, Prentice Hall, 2004.