Simulaciona analiza kodova za cikličnu proveru redundanse

Srđan Brkić, Elektrotehnički fakultet Beograd

***Sadržaj* – Većina savremenih telekomunikacionih sistema koriste postupak ciklične provere redundanse (*cyclic redundacy check*)- CRC kao sredstvo za detekciju grešaka nastalih prilikom prenosa kroz telekomunikacioni kanal. U ovom radu uz pomoć Monte Karlo simulacione analize biće ispitane osobine nekih, u praksi korišćenih, CRC kodova na dva tipa kanala: binarnom simetričnom kanalu i Gilbert-Eliotovom modelu kanala.**

***Ključne reči* – ciklična provera redundanse, simulacija.**

I. UVOD

Kodovi za cikličnu proveru redundanse (CRC) predstavljaju specifičnu potklasu sistematskih linearnih blok kodova koja služi isključivo za otkrivanje grešaka nastalih prilikom prenosa kroz šumni kanal. U slučaju ovih kodova, za početak ili za kraj binarne informacione poruke (dužine *k* bita) dodaje se *n* – *k* bita za proveru parnosti. Na taj način se dobijaju kodne reči dužine *n*, deljive sa generišućim polinomom za taj kod $g(x)$, a odgovarajući kod označava se sa (*n*,*k*). Posebnu pogodnost korišćenja CRC kodova predstavlja mogućnost korišćenja ovih kodova u sistemima koji koriste različite dužine kodne reči, kao i mogućnost kombinovanja ovog postupka sa drugim tehnikama zaštitnog kodovanja koji imaju mogućnost da ispravljaju greške, gde CRC služi kao konačna provera da li je poslati paket informacionih bita ispravno primljen [1].

Iako u opštem slučaju CRC kodovi ne pripadaju klasi cikličnih kodova matematički aparat su upravo nasledili od njih [2], pa su u potpunosti opisani generišućim polinomom $g(x)$. Kako je CRC postupak veoma rasprostranjen u telekomunikacionim sistemima to je postojala potreba za korišćenjem više različitih generišućih polinoma. Najčešće se koriste polinomi između četvrtog i trideset drugog stepena, međutim koristi se i više polinoma istog stepena tako da, na primer, postoje dva CRC-12 polinoma, u upotrebi je i deset CRC-16 polinoma, kao i četiri CRC-32 koda. Najčešće primenjivani polinomi su osmog, dvanaestog i šestnaestog stepena. Polinom CRC-16-CCITT je dosta korišćen pa se može naći u Blutut (*Bluetooth*), CDMA (*Code Division Multiple Access*), WLAN (*Wireless Local Area Network*), PPP (*Point-to-Point Protocol*), HDLC (*High-Level Data-Link Control Protocol*) kao i mnogim drugim sistemima. Od polinoma osmog stepena treba istaći CRC-8-ATM koji služi za otkrivnaje grešaka u zaglavlju paketa korišćenih u ATM (*Asychronous Transfer Mode*) tehnici prenosa i CRC-8-WiMAx koji je u upotrebi u WiMax (*Worldwide Interoperability for Microwave Access*) bežičim mrežama. Pomenuti polinomi osmog stepena zajedno sa polinomom CRC-12 korišćenim u UMTS (*Universal Mobile Telecommunications System*) biće prikazani u poglavlju IV gde će se performanse kodova koje oni generišu biće ispitane simulacionom analizom. Analiza je uopštena i može se primeniti na bilo koji drugi CRC kod.

S. S. Brkić, Tošin Bunar 143, Beograd, Srbija (telefon: 381-64-5707143, e-mail: brka05@gmail.com).

II. TEORIJSKA ANALIZA CRC KODOVA

Performanse nekog CRC koda (a i uopšte bilo kog drugog zaštitnog koda koji služi za otkrivanje grešaka) primenjenog na nekom kanalu određuju se preko verovatnoće neotkrivene greške P_u, koja predstavlja verovatnoću događaja da šum u kanalu jednu kodnu reč prevede u drugu [3]. U ovom odeljku biće izložena teorijska analiza CRC kodova koričćenih na binarnom simetričnom kanalu BSC (*Binary Simmetric Channel*).

Imajući u vidu definiciju neotkrivene (zaostale) greške ona se, za neki CRC kod u oznaci (*n*,*k*), matematički može prikazati u zavisnosti od verovatnoće greške u kanalu (*p*) i spektra kodnih rastojanja $[A_0, A_1, \dots, A_n]$ [3]:

$$P_u(p) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}\,, \qquad (1)$$

gde A_i predstavlja broj kodnih reči sa Hemingovom težinom *i*. Dakle, za potpuno poznavanje nekog CRC koda potrebno je znati raspodelu težina u kodu što nekada nije lak zadatak. Glavni nedostatak predstavlja računarsko vreme potrebno da se izvrše operacije određivanja spektra. U modernim sistemima dužine kodne reči mogu biti više stotina (pa i hiljada) bita dok, kako je naglašeno u poglavlju I, redundantni deo CRC koda retko sadrži više od trideset dva bita pa je vrlo nepraktično analizirati svaku od 2^k kodnih reči. Znatno je lakše posmatrati dualni kod (koji ima mnogo manje kodnih reči), pa je pronađena veza između njegovog spektra i spektra originalnog koda opisana preko Mekvilijamsovih identiteta (*MacWilliams identities*) (u potpunosti opisanih u [4]):

$$A(z) = 2^{-(n-k)}(1+z)^n B\left(\frac{1-z}{1+z}\right), \qquad (2)$$

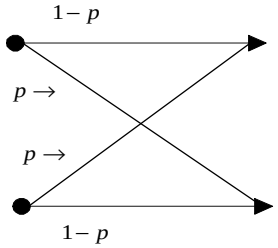
gde su $A(z)$ i $B(z)$ polinomski zapisi spektra originalnog i dualnog koda (na primer $A(z) = A_0 + A_1 z + \cdots + A_n z^n$). Verovatnoća zaostale greške se onda može pisati kao [3]:

$$P_u(p) = 2^{-(n-k)} B(1-2p) - (1-p)^n. \quad (3)$$

Navedena formula je korišćena i u ovom radu za teoretsko određivanje verovatnoće greške i provere verodostojnosti simulacije na BSC modelu i rezultati dobijeni teoretski su na slici 4 poređeni sa onim dobijenim numeričkim putem.

III. SIMULIRANI TELEKOMUNIKACIONI KANALI

U ovom radu biće simulirana dva modela kanala: binarni simetrični kanal BSC (*binary simmetric channel*) i Gilbert-Eliotov kanal (*Gilbert-Elliot channel*). BSC je najjednostavniji model diskretnog kanala koji je bez memorije i pojava greške ne zavisi od prethodno emitovanih simbola niti prethodnih grešaka. Simetričnost (koja stoji u nazivu kanala) se ogleda u tome što su verovatnoće da se emitovani bit 0 pogrešno primi kao bit 1 i da se bit 1 primi kao 0 međusobno jednake (p). Tada će biti jednake i verovatnoće ispravnog prenosa ($1 - p$). Ovakav način nastajanja grešaka karakterističan je za kanal u kome deluje samo beli aditivni Gausov šum, a čiji opseg je toliko širok da nema međusimbolske interferencije niti drugih tipova smetnji (inpulsni šum, feding itd). Kako su vrednosti susednih amplituda kod belog Gausovog šuma statistički nezavisne, to su i greške nastale pod uticajem ovog šuma takođe nezavisne, dok se zbog simetrije Gausove raspodele oko srednje vrednosti prag za odlučivanje nalazi na sredini između dva amplitudska nivoa koja odgovaraju bitima 0 i 1. Na slici 1 je prikazan graf koji odgovara ovom tipu kanala.



Slika 1 Graf koji odgovara BSC modelu

Verovatnoće greške i ispravnog prenosa su date kanalnom matricom:

$$P_{BSC} = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}. \quad (4)$$

Gilbert-Eliotov model je nešto složeniji i on se sastoji od dva binarna simetrična kanala koji predstavljaju dva stanja u opisu ovog modela teorijom Markovljevih procesa. Stanja su dobro i loše sa stacionarnim verovatnoćama P_D i P_L , respektivno. Mogu se definisati i verovatnoće da će kanal ostati u stanju u kome se prethodno nalazio ili da će preći u drugo stanje i tada će važiti:

$$P_{DD} + P_{DL} = 1, \quad (5)$$

$$P_{LD} + P_{LL} = 1, \quad (6)$$

gde je veličina P_{AB} verovatnoća da se iz stanja A pređe u stanje B. Uvedeni parametri kanala su grafički prikazani na slici 2. Kada su poznate tranzicione (prelazne) verovatnoće date izrazima (5) i (6) jednostavno se dolazi i do stacionarnih verovatnoća stanja:

$$P_D = P_{LD}/(P_{LD} + P_{DL}), \quad (7)$$

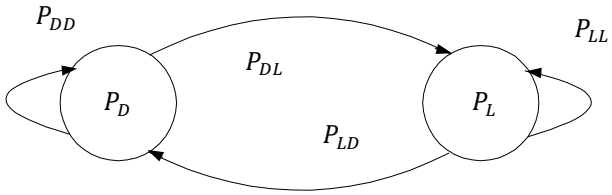
$$P_L = P_{DL}/(P_{LD} + P_{DL}). \quad (8)$$

Kao što je već rečeno svako stanje odgovara jednom BSC kanalu pa model ima još dva nezavisna parametra verovatnoću greške u dobrom stanju p_d i verovatnoću greške u lošem stanju p_l pa je prosečna verovatnoća greške:

$$p_{sr} = p_d P_D + p_l P_L. \quad (9)$$

Od posebnog interesa za simulaciju su i prosečno trajanje svakog od stanja u bitima koje je obrnuto proporcionalno verovatnoći da se to stanje napusti:

$$T_D = 1/P_{DL}, T_L = 1/P_{LD}. \quad (10)$$

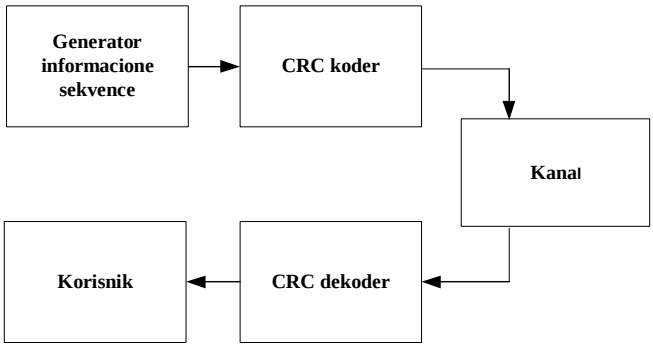


Slika 2 Gilbert-Eliotov model kao Markovljev proces

Fizička interpretacija ovog modela je kanal u kome, pored aditivnog belog Gausovog šuma (dobro stanje), deluje i impulsni šum i njegovo trajanje se predstavlja trajanjem lošeg stanja i obično se smatra da je u lošem stanju verovatnoća greške $p_l = 0.5$ [1].

IV. SIMULACIONA ANALIZA CRC KODOVA

Da bi se izvršila simulaciona analiza CRC kodova i ispitale njihove performanse (mogućnost detekcije grešaka) potrebno je napraviti simulacioni model prikazan na slici 3. Prvo je formiran izvor grešaka koji odgovara binarnom simetričnom kanalu.



Slika 3 Model sistema za simulaciju

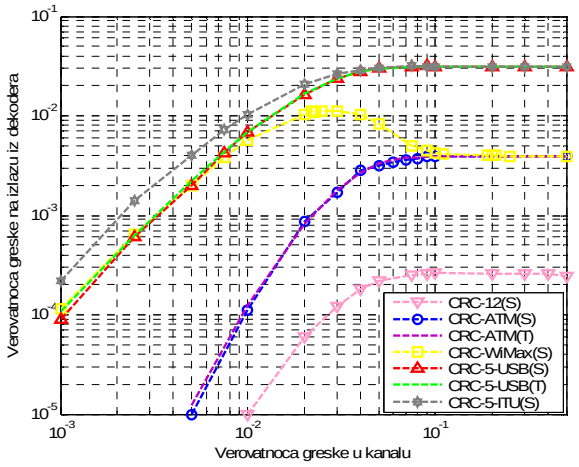
Ispitivano je pet CRC kodova čiji su generišući polinomi dati u tabeli 1. Pored tri polinoma pomenuta u prvom poglavlju u tabeli se nalaze još dva polinoma petog stepena i to CRC-5-USB koji je standardizovan specifikacijom USB

2.0 i CR-5-ITU standardizovan ITU (*International Telecommunication Union*) preporukom G.704.

Tabela 1 Generišući polinomi posmatranih kodova

Naziv	Generišući polinom
CRC-5-ITU	$x^5 + x^4 + x^2 + 1$
CRC-5-USB	$x^5 + x^2 + 1$
CRC-8 (WiMax)	$x^8 + x^2 + 1$
CRC-8-ATM	$x^8 + +x^2 + +1$
CRC-12	$x^{12} + x^{11} + x^3 + x^2 + x + 1$

Monte Karlo simulacionim postupkom [1], koji se temelji na teoriji verovatnoće, određena je zavisnost zaostale greške za vrednosti greške u kanalu u opsegu $p \in [0.001,0.5]$ i rezultati su grafički prikazani na slici 4. Kako se CRC kodovi mogu koristiti na informacionim porukama promenljive dužine moguće je za sve kodove iz tabele 1 izabrati istu dužinu kodne reči i porediti njihove osobine. Ovde je izabrano da dužina kodnih reči bude $n = 100$ bita.



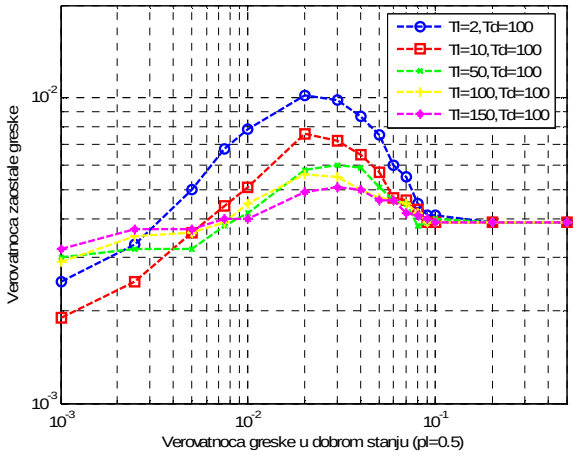
Slika 4 Performanse CRC kodova na BSC tipu kanala

Očigledno je da je najbolje rezultate pokazao kod sa najviše redudantnih bita CRC-12. Interesantnije je, međutim, poređenje kodova generisanih polinomima istog stepena. Tako se pokazalo da je CRC-5-USB efikasniji od CRC-5-ITU, dok je CRC-8-ATM na ovoj dužini kodnih reči znatno superiorniji u odnosu na CRC-8 WiMax. Kako je simulacija pokazala, funkcija verovatnoće zaostale greške je monotono rastuća i ne prelazi graničnu vrednost 2^{n-k} za sve kodove izuzev za CRC-8 WiMax. Takvi kodovi su, kako se to navodi u [3], pravilni dok je CRC-8 WiMax nepravilan na zadatoj dužini kodne reči što je glavni razlog za njegovu inferiornost. Treba napomenuti da ako se pokaže da je neki kod pravilan na nekoj dužini kodne reči ne može se zaključiti da je pravilan za sve dužine. Na primer kod CRC-12 je nepravilan na nekim kraćim dužinama gde ima veću verovatnoću neotkrivene greške nego u slučaju simuliranom ovde [5].

Kako se verovatnoća greške na BSC tipu kanala može izračunati i teorijski (kako je to pokazano u odeljku II), izvršeno je poređenje vrednosti dobijenih simulacijom sa teorijskim vrednostima. Na slici 4 su prikazani teorijski rezultati za dva koda i to CRC-5-USB i CRC-8-ATM (krive koje njima odgovaraju u legendi sadrže oznaku (T), dok su one dobijene simulacijom označene sa (S)) i može se primetiti da su skoro identični sa rezultatima simulacije za koju se tada može reći da je verodostojna.

Simulacija Gilbert-Eliotovog kanala se obavlja istovetno samo se menja statistika sekvence grešaka. BSC je unosio statistički nezavisne greške dok se ovde u greške uvodi statistička zavisnost i simuliraju se paketi grešaka.

Na slikama 5, 6 i 7 su prikazani rezultati simulacije ovog kanala. Kao što je već rečeno sama simulacija se obavlja na isti način, ali se cilj simulacije promenio. Sada se simulira samo jedan kod (CRC-8 WiMax) a menjaju se parametri kanala. Gilbert-Eliotov model ima četiri nezavisna parametra: prosečno trajanje dobrog stanja (T_D), prosečno trajanje lošeg stanja (T_L), verovatnoća greške u dobrom stanju (p_d) i verovatnoća greške u lošem stanju (p_l). Njihovom promenom menjaju se i performanse zaštitnog koda primenjenog na ovom kanalu. Izabrano je da verovatnoća greške u lošem stanju bude konstantna i iznosi $p_l = 0.5$ dok se verovatnoća greške u dobrom stanju menja u opsegu $p_d \in [0.001,0.5]$. Trajanje dobrog stanja takođe je konstantno ($T_D = 20$ bita) dok se familija krivih prikazanih na slikama 5 i 6 dobija promenom trajanja lošeg stanja koje može da iznosi 2, 10, 50, 100 i 150 bita.

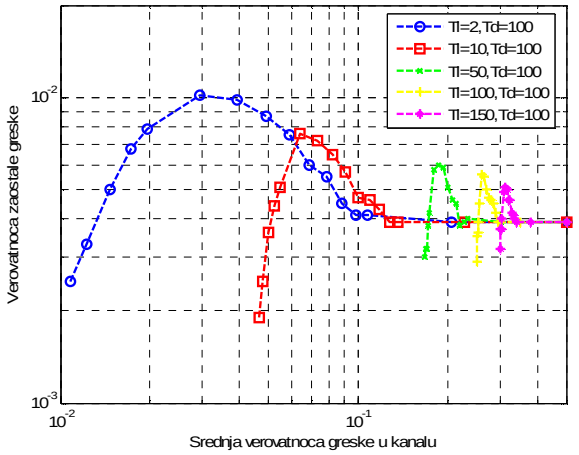


Slika 5 CRC-8 WiMax na Gilbert-Eliotovom kanalu (zavisnost P_u od verovatnoće greške u dobrom stanju)

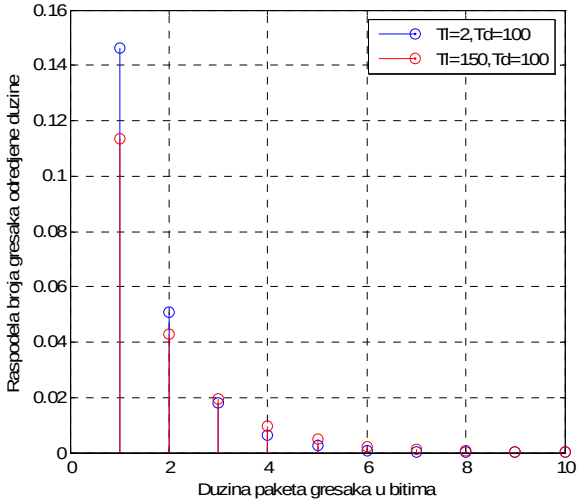
Na slici 5 je prikazana zavisnost verovatnoće neotkrivene greške od verovatnoće greške u dobrom stanju. Može se zapaziti da se sa povećanjem trajanja lošeg stanja vrednosti zaostale greške izjednačavaju i daljim povećavanjem parametra T_L izgubila bi se zavisnost od p_d i preovladalo bi loše stanje (a samim tim ne bi bilo nikakvog prenosa) a funkcija $P_u(p_l, p_d)$ postala konstanta i bila jednaka $P_u(p_l) \approx 2^{n-k} = 0.0039$.

Međutim, slika 5 ne nosi direktnu informaciju o performansama posmatranog koda jer je, pre svega, od interesa analiza koja uključuje prosečnu verovatnoću greške u kanalu (datu formulom (9)) koja još zavisi i od stacionarnih verovatnoća stanja. Upravo, slika 6 u potpunosti

opisuje ponašanje CRC koda. Može se zapaziti da se zbog fiksiranja parametra $p_l$opseg crtanja krivih razlikuje tako da se funkcija dobijena za $T_D = 2$ bita nalazi u domenu $p_{sr} \in [0.01,0.5]$ dok je za $T_D = 150$ bita interval znatno manji i iznosi $p_{sr} \in [0.3,0.5]$.



Slika 5 CRC-8 WiMax na Gilbert-Eliotovom kanalu (zavisnost $\boldsymbol{P_u}$ od srednje verovatnoće greške u kanalu)



Slika 6 Raspodela sekvence grešaka za dve različite vrednosti trajanja lošeg stanja

Interesantno je uočiti, posmatrajući krive na slici 6, da postoje intervali gde je verovatnoća zaostale greške manja ako je veće trajanje lošeg stanja. Ta naizgled zbunjujuća pojava može se lako objasniti poznajući sposobnosti CRC kodova da otkrivaju paketski tip grešaka. Naime, dva Gilbert-Eliotova modela kanala različitih trajanja lošeg stanja a iste srednje verovatnoće greške u sekvenci grešaka imaju isti broj jedinica samo su one drugačije raspoređene, kanal sa dužim lošim stanjem stvara više paketskih grešaka. Na slici 7 je prikazana raspodela paketa grešaka za dva granična slučaja kada je $T_D = 2$ i $T_D = 150$ bita. Može se primetiti da se povećanjem trajanja lošeg stanja smanjuje broj paketa dužina 1 i 2 na račun povećanja paketa veće dužine. Zaštitni kod CRC-8 WiMax ne može imati Hemingovo rastojanje veće od 4 na dužini kodne reči od 100 bita (to je maksimalno Hemingovo rastojanje koje može imati bilo koji CRC kod sa 8 redundantnih bita na pomenutoj dužini kodne reči [6]) pa može detektovati samo 3 statistički nezavisne greške. Ali poznato je da CRC kod sa $n - k$ zaštitnih bita može da otkrije sve paketske greške iste ili manje dužine od $n - k$ kao i jedan broj paketa veće dužine [1]. Tada kada paketske greške budu dominantne CRC kod će ih lakše otkrivati ali daljim povećavanjem broja grešaka (preko povećavanja verovatnoće greške u dobrom stanju) izlazi se iz pomenutog intervala i kanal sa kraćim trajanjem lošeg stanja postaje pogodniji za prenos.

Na kraju treba istaći i neke loše strane Monte Karlo simulacionog metoda koji je u ovom radu korišćen. Za pouzdanu simulaciju potrebno je veoma veliko računarsko vreme koje zavisi i od primenjenog koda. Neki bolji kodovi sa više redundantnih bita imaju manje vrednosti verovatnoće neotkrivene greške pa je za njihov pronalazak potrebno generisati veoma velike dužine sekvence grešaka. Simulacija CRC-16 i CRC-32 kodova je veoma nepraktična pa treba koristiti neki drugi simulacioni postupak.

LITERATURA

[1] D. Drajić, P. Ivaniš, "*Uvod u teoriju informacija i kodovanje*", treće izdanje, Akademska misao, Beograd, 2009

[2] F. Manganiello, „Computation of the Weight Distribution of CRC Codes", Applicable Algebra in Engineering, Communication and Computing, Vol. 19, No. 4. (2008), pp. 349-363.

[3] G. Castagnoli, J. Ganz, P. Graber, "Optimum Cyclic Redundancy-Check Codes with 16-bit Redundancy", IEEE Trans. Commun., Vol. 38 (1990), pp. 111-114

[4] R. E. Blahut, *Theory and Practise of Error Control Codes*, Addison-Wesley Publishing Company, Reading, Massachusetts, 1983

[5] K. A. Witzke, C. Leung, "A Comparison of Some Error Detecting CRC Code Standards", *IEEE Trans. Commun.*, Vol. COM-33 (1985), pp. 996-998

[6] P. Koopman, T. Chakravaty, "*Cyclic Redudancy Code (CRC) Polynomial Selection For Embedded Networks*", Intl. Conf. Dependable Systems and Networks (DNS), Washington DC, 2004.

ABSTRACT

Most of modern telecommunication systems use the process of cyclic redundancy check - CRC as a tool for detecting the errors incurred during the transmission through the telecommunications channel. In this paper using the Monte Carlo simulation analysis are examined properties of some common used CRC codes. The numerical results are presented on two types of channels: the binary symmetric channel and Gilbert-Elliot's channel model.

A SIMULATION ANALYSIS OF CYCLIC REDUNDANCY CHECK CODES

Srdjan Brkic, Faculty of Electical Engineering, Belgrade