UNIVERZITET U BEOGRADU

MATEMATIČKI FAKULTET

OCENA ENTROPIJE TELEPRINTERSKOG JEZIKA I PRIMENA NA KANAL SA PRISLUŠKIVANJEM

MAGISTARSKI RAD

Mentor:

DR. ZORAN IVKOVIĆ

Kandidat:

MILAN RADULOVIĆ

BEOGRAD 1999.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

OCENA ENTROPIJE TELEPRINTERSKOG JEZIKA I PRIMENA NA KANAL SA PRISLUŠKIVANJEM

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

1. TELEPRINTERSKI JEZIK

Cilj rada je da se korišćenjem naučnih metoda statistike i teorije informacija oceni entropija teleprinterskog jezika i da se pokaže kako taj i slični rezultati mogu imati primenu u zaštiti komunikacionog kanala koji se prisluškuje (u literaturi poznatog kao WIRE-TAP CHANNEL).

Osnovni rezultati rada su ocene entropije teleprinterskog jezika, uopštenje rezultata iz [2] i na osnovu toga određivanje kodova koji u uslovima prisluškivanja kanala čuvaju tajnost sadržaja komunikacije. Potrebna statistička istraživanja sprovedena su na uzorku srpskog jezika novinarskog stila, što naizgled ovom radu daje uži praktični značaj. Međutim, opštost leži u primenjenom metodu zaštite komunikacionog sistema i korišćenim kodovima koji ne zavise od direktnog posmatranja jezika i stila.

U *prvoj* sekciji definisaćemo pojam teleprinterskog jezika, opisati komunikacioni sistem sa kanalom za prisluškivanje u okviru koga ćemo taj jezik posmatrati.

Druga sekcija daje osnovne pojmove i stavove vezane za proučavanje statističko-informacionih karakteristika jezika, sa težištem na entropiji kao važnom parametru jezika i elementu izučavanja u ovom radu.

U *trećoj* sekciji izložen je koncept WIRE-TAP CHANNEL-a za prislušni kanal sa šumom i dato uopštenje problema koje se sastoji u tome da se posmatraju i izvori sa raspodelom izlaznog niza koja nije ravnomerna raspodela.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

O statističkoj oceni entropije i drugih parametara teleprinterskog jezika govori se u *četvrtoj* sekciji. Sprovedena je statistička obrada uzorka srpskog jezika i u ovom delu rada izloženi su dobijeni rezultati .

Peta sekcija daje objašnjenje postupaka konstrukcije kodova i daje primere kodova otpornih na prisluškivanje u posmatranom komunikacionom sistemu.

Prilozi koji slede vezani su za odgovarajuće sekcije i objašnjeni izlaganjem u tim sekcijama.

Dati spisak literature sadrži samo najvažnije radove potrebne da pruže dovoljne reference za izloženu materiju.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

1.1 Teleprinterski jezik

Pod teleprinterskim jezikom podrazumevaćemo prirodni jezik u pisanom obliku, kodiran određenim teleprinterskim kodom i time zakonito transformisan u binarni niz. Takav oblik jezika prisutan je na svim teleprinterskim (telegrafskim) i teleks vezama.

Intezivan saobraćaj pisanih poruka zahtevao je da se postupci slanja poruka mehanizuju radi postizanja veće brzine, tajnosti i sigurnosti prenosa. Teleprinter je prvi telegrafski uređaj koji je to omogućio. Namenjen je za ručnu ili automatsku predaju, automatski prijem i štampanje pisanih poruka na daljinu (primopredajni uređaj). Mehaničke teleprinterske uređaje sve više zamenjuju elektronski, ali se osnovni princip prenosa poruka nije promenio. Razmatranje problema prenosa kodirane informacije ima za cilj da se daju teorijski i praktični rezultati primenjivi u ovoj i drugim oblastima komunikacija, u konstrukciji i primeni odgovarajućih komunikacionih uređaja .

Posmatraćemo fizički uređaj - teleprinter kao jedan izvor informacija koji generiše poruke sazdane od slova, reči, rečenica, pasusa, paragrafa itd., a iz određenog skupa mogućih poruka na datom jeziku. Kako su poruke sastavljene od elemenata koji mogu biti: slova, cifre, znaci interpunkcije ili neki drugi znaci, potrebno je svakom od njih pre slanja poruke dodeliti, po jednom unapred dogovorenom postupku, određenu

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

kodnu zamenu sačinjenu od simbola kanala veze. U principu kodiranje se sastoji u korišćenju dva elementarna stanja (npr. isključen i uključen napon, neizbušena ili izbušena rupa, itd.), koja označavamo binarnim ciframa 0 i 1 . Svakom znaku pisane poruke dodeljujemo kodnu reč koja se sastoji od određenog broja i rasporeda elementarnih stanja. Skup svih takvih kodnih reči sa korespodentnim slovima, ciframa, znacima interpunkcije i specijalnim znacima daje odgovarajuću kodnu transformaciju, odnosno teleprinterski kod.

Posmatraćemo petobitni kod dat u prilogu 1[1)] poznat pod nazivom CCITT[2)] kod N°2 . Mogućih 5-bitnih kodnih zamena ima $2^5=32$, što je dovoljan broj da se svakom slovu, cifri i specijalnom znaku dodeli kodna reč, koristeći sistem režima slova i režima cifara kojim se svakoj kodnoj reči dodeljuju dva znaka. Specijalnim znacima (kolica nazad, novi red, prelaz na

---

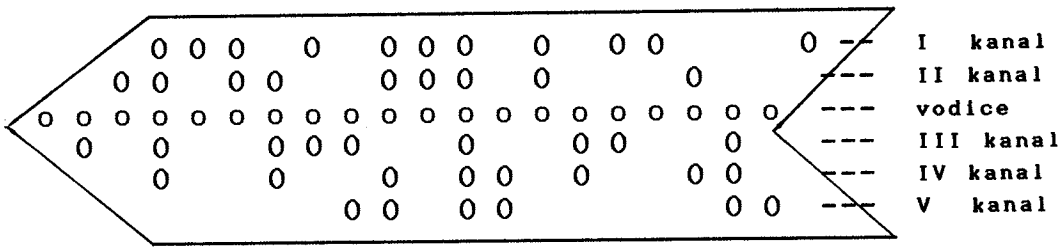
[1)] *Pored 5 kodnih impulsa, pri prenosu poruka, svakoj kodnoj reči prethodi jedan bestrujni impuls (0) koji se zove startni, a završava se strujnim impulsom (1), koji se zove stopni . Na taj način, svaki znak se sastoji od 7 impulsa. Posvetićemo pažnju samo kodnim impulsima koji se dodeljuju slovima, ciframa, znacima interpunkcije i specijalnim znacima kao nosiocima informacije. Startni i stopni bit služe za sinhronizaciju predajnog i prijemnog uređaja u asinhronom telegrafskom sistemu i nisu informacioni deo poruke.*

[2)] *Međunarodni konsultativni komitet za telefoniju i telegrafiju (CCITT) je zvanično telo u kome organizacije za pružanje telekomunikacionih usluga odlučuju o međusobnoj saradnji. Deo je Međunarodne telekomunikacione unije (ITU) u Ženevi i organ UN. CCITT objavljuje preporuke koje nemaju moć standarda, ali u praksi stiču tu moć širokim prihvatanjem preporuka od strane korisnika i proizvođača telekomunikacione opreme.*

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

slova, prelaz na cifre, razmak, vođica) obezbeđuje se korektan rad teleprintera pri prenosu poruke[3)].

Otkucani znak na teleprinteru moguće je izbušiti na papirnu traku tako da izbušena rupa označava cifru 1, a neizbušena cifru 0. Pored pet bitova na traci se buši jedna manja rupa za vođenje trake (vođica). Svaka rupica znaka koji se buši pripada po jednom *kodnom kanalu*. Redosled kodnih kanala je određen u odnosu na vođicu, kao što je to prikazano na slici 1, a znaci se nižu s leva na desno.



Sl. 1 Kanali bušene trake

Osnovni oblik toka informacije na teleprinterskom kanalu veze je serijski tok petobitnih kodnih blokova. Imajući u vidu postojanje navedene fizičke predstave niza kodnih bitova i paralelnog toka bitova kodnih kanala u uređaju prirodno se nameće i posmatranje binarnih nizova po kodnim kanalima.

---

3) *Da li se kodnoj reči dodeljuje slovo ili znak-cifra definisano je poslednjim pojavljivanjem specijalnog znaka prelaza na slova (A...) ili prelaza na cifre (1...) u kodnom nizu koji prethodi posmatranoj kodnoj reči. Samo specijalni znaci u režimu slova i režimu cifara imaju isto značenje. Pri prelasku u režim slova ili cifara teleprinter u njemu ostaje sve dok se odgovarajućim specijalnim znakom režim ne promeni.*

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Uočimo skup $\mathbb{A}$ koji čine slova, znaci, i cifre, tj. svi karakteri koje kodiramo uočenim teleprinterskim kodom CCITT $N^0 2$ (Prilog 1.):

$\mathbb{A}=\{A,B,C,\ldots,Y,Z,-,?,:,\ldots,6,+,1\ldots,A\ldots,\_,<,=,@\}$, $card(\mathbb{A})=58$.

Funkcija kodiranja zadata tablicom je oblika :

$$f : \mathbb{A} \longrightarrow (\mathbb{Z}_2)^5 \quad , \text{ tj. } f(x)=z \ , \ x\in\mathbb{A} \ , \ z\in(\mathbb{Z}_2)^5$$

$$z = (z_1 z_2 z_3 z_4 z_5)\in (\mathbb{Z}_2)^5 \ , \ z_i \in \mathbb{Z}_2 = \{0,1\} \ , \ i=\overline{1,5} \ .$$

Tako je na primer: f(A)=(11000) , f(B)=(10011),... Te kodne petorke predstavljaju slova alfabeta:

$CCITT_{32}$= { 11000, 10011, 01110, ... , 00100, 00000 } .

Uneta reč prirodnog jezika na izlazu teleprintera daje niz binarnih petorki i taj niz predstavlja reč teleprinterskog jezika T.

Slično tome definišemo teleprinterski jezik $T_i, i=\overline{1,5}$ sužavajući funkciju kodiranja tako da :

$f_i : \mathbb{A} \longrightarrow \mathbb{Z}_2$,tj. $f_i(x)=z_i$, $x\in\mathbb{A}$, $z_i\in\mathbb{Z}_2 = \{0,1\}$, $i=\overline{1,5}$.

Tako je na primer: $f_1(A)=(1)$, $f_1(B)=(1),\ldots$

$f_2(A)=(1)$, $f_2(B)=(0),\ldots$

$f_3(A)=(0)$, $f_3(B)=(0),\ldots$

$f_4(A)=(0)$, $f_4(B)=(1),\ldots$

$f_5(A)=(0)$, $f_5(B)=(1),\ldots$

Skup $\mathbb{Z}_2$= {0 , 1} je alfabet jezika T_i, a kodirana reč prirodnog jezika daje reč teleprinterskog jezika T_i. Time tekst jezika T_i predstavlja podniz teksta jezika T nastao izdvajanjem i-tog kanala kodnih zamena. Zbog toga ćemo ravnopravno koristiti

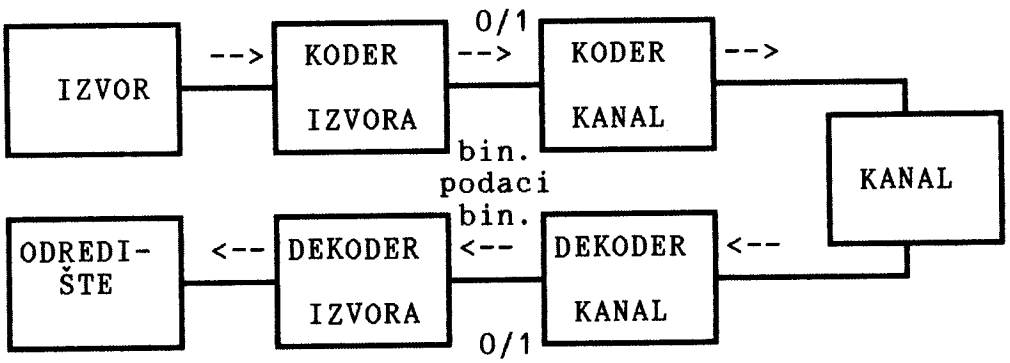
Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

termine kanal *i* i jezik T_i jer se odnose na iste sadržaje.

Očigledno da tekst jezika T, posmatrajući kodne petorke bitova, predstavlja samo transkripciju i malu promenu prirodnog jezika (npr. proširen je specijalnim znacima) pa zadržava, uz male promene, osobine jezičkog niza, dok binarni jezik T_i bitno menja osobine u odnosu na prirodni jezik.

1.2 Komunikacioni sistem

Radi jednostavnosti proučavanja izvora i kanala komunikacionog sistema uobičajno je izvršiti razdvajanje uticaja izvora na kanal komunikacionog sistema. To se postiže razdvajanjem kodera i dekodera na dve prirodne celine kao što je to prikazano na slici 2 :



Sl. 2 Blok dijagram komunikacionog sistema sa razdvojenim koderom i dekoderom na dva dela

Praktična vrednost razdvajanja kodera i dekodera (slika 2.), je da se korišćenjem binarnih podataka mogu različiti izvori

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

povezati na isti kanal. Takav jednostavniji prikaza komunikacionog sistema koristićemo u daljem izlaganju. Izvor i koder izvora posmatraćemo objedinjeno kao binarni izvor, a koder kanala nazivaćemo koder. Slično tome, dekoder izvora i odredište posmatramo objedinjeno kao binarni izlaz, a dekoder kanala nazivaćemo dekoder.

Takvim predstavljanjem jasno je da teleprinter možemo posmatrati kao diskretan binarni izvor jer generiše poruke u vidu nizova od dva različita električna signala, koje smo označili binarnim ciframa 0 i 1. Svaki signal koji generiše izvor nastao je pridruživanjem simbolu određenog petobitnog bloka bitova. Da li će se kao različiti elementi posmatrati dva različita binarna stanja, ili 32 različite petobitne kombinacije ili bilo koji drugi blok bitova, zavisi od problema koji se razmatra. U svakom od tih slučajeva definiše se odgovarajući konačan alfabet A izvora informacija

$$A = \{ a_1, a_2, \ldots, a_s \} \ , \ s=2^j \ , \ j \in \{1,2,3,4,5\}$$

čiji elementi (tj. slova u širem smislu) grade poruke C kao n-člane nizove oblika :

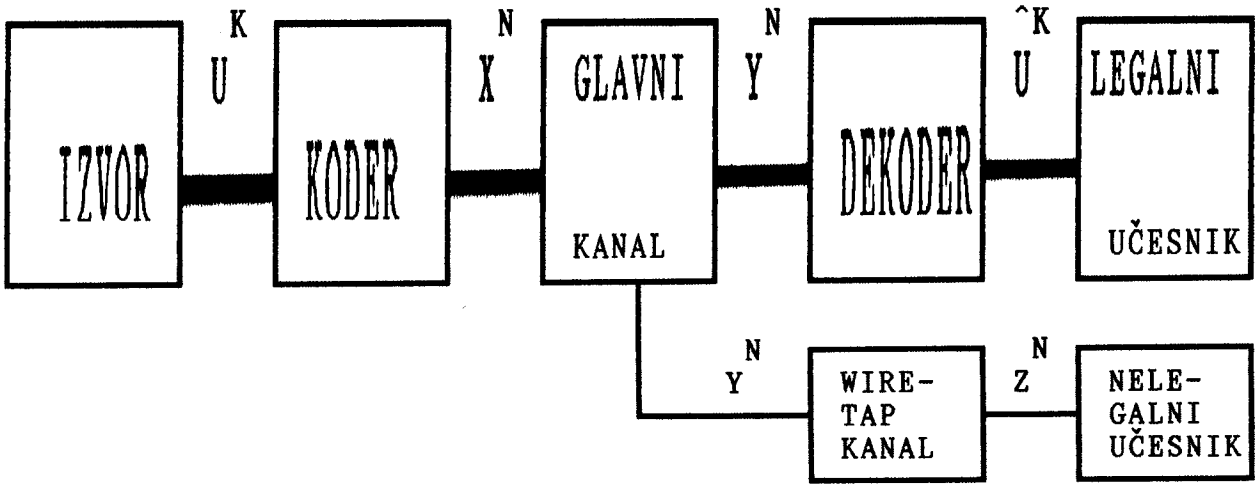
$$C = (x_1 x_2 \ldots x_n) \ .$$

U daljim razmatranjima od interesa će nam biti samo slučajevi kada je j=1 (teleprinterski jezik T_i) i j=5 (teleprinterski jezik T), ali ćemo određenim metodama problem svesti samo na binarni nivou, što bitno pojednostavljuje naš zadatak izučavanja teleprinterskog jezika.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

1.3 Komunikacioni sistem sa prisluškivanjem

Teleprinterski jezik posmatraćemo kao izvor komunikacionog sistema sa prisluškivanjem[4] čiji opšti oblik je prikazan na slici 3 :



Sl. 3 Komunikacioni sistem sa prisluškivanjem

Pri izgradnji ovog sistema vodilo se računa o zahtevu za obezbeđenje informacija od prisluškivanja u fazi prenosa. To je ostvareno, u odnosu na osnovni oblik komunikacionog sistema, unošenjem dodatnih informacionih procesa kodiranja i dekodiranja. Kodirana informacija prenosi se pomoću diskretnog kanala bez memorije, takvog da sadrži prislušni, tj. wire-tap (WT) kanal kao prijemnik.

Kodiranje poruke omogućeno je predajnoj, a dekodiranje prijemnoj strani. Kod koji se koristi u komunikacionom sistemu

---

[4] *Taj oblik komunikacionog sistema u literaturi prvi je razmatrao A.D.Wyner u radu* [1].

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

u potpunosti je poznat WT učesniku. Prednost legalnog učesnika nad njim je samo u tome što je prislušni kanal zašumljen. Kako u sistemu ne postoje nikakvi tajni elementi onaj ko dizajnira koder-dekoder formira takav kod koji omogućava maksimalnu brzinu prenosa i maksimalnu neodređenost na prislušnoj strani u odnosu na produkciju izvora. Znači, cilj je da se u komunikacionom sitemu dobije maksimalna informacija za legalnog učesnika, a minimalna za nelegalnog učesnika i time ostvari određeni nivo zaštite od prisluškivanja.

Sada ćemo dati kratak opis elemenata komunikacionog sistema sa kanalom za prisluškivanje.

Izvor je definisan nizom $\{U_k\}$, gde su U_k slučajne promenljive koje uzimaju vrednosti iz konačnog skupa U i imaju poznatu raspodelu i entropiju $H(U_k)=H(U)$. Niz od K podataka koje emituje izvor označavamo K-vektorom : $U^K=(U_1,U_2,\ldots,U_K)$.

Glavni kanal je diskretan kanal bez memorije sa konačnim alfabetima: ulaznim X i izlaznim Y, verovatnoćama prelaza $P_M(y|x)$, $x\in X$, $y\in Y$ i verovatnoćeom prelaza za N-vektore :

$$P_M^{(N)}(y|x) = \prod_{i=1}^{N} P_M(y_i|x_i) \ .$$

Wire-tap kanal (WT) je diskretan kanal bez memorije sa konačnim ulaznim alfabetom Y, i konačnim izlaznim alfabetom Z i verovatnoćama prelaza $P_W(z|y)$, $y\in Y$, $z\in Z$.

Koder sa parametrima (K,N) je poseban kanal sa ulaznim alfabetom U^K, izlaznim alfabetom X^N i verovatnoćama prelaza

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

$p_E(x|u)$, $u \in U^K$, $x \in X^N$. Ako su K slučajnih promenljivih izvora $U^K=(U_1,U_2,\ldots,U_K)$ ulaz kodera, izlaz je slučajni vektor $X^N=(X_1,X_2,\ldots,X_N)$. Neka su Y^N i Z^N respektivno izlazi kanala sa verovatnoćama prelaza $P_M^{(N)}$ i $P_{MW}^{(N)}$, kada je ulaz X^N. Nelegalni učesnik ocenjuje ekvivokaciju izvora po simbolu izvora na sledeći način :

$$D \triangleq \frac{1}{K} * H(U^K|Z^N) \quad .$$

Veličinu D uzimamo za kriterijum WT neodređenosti i koder se dizajnira tako da se ona učini što većom. Kada je D=K kažemo da je ostvarena apsolutna tajnost, tj. potpuna zaštita.

Dekoder je preslikavanje : $f_D : Y^N \rightarrow \hat{U}^K$.

Neka je $\hat{U}^K = (\hat{U}_1,\hat{U}_2,\ldots,\hat{U}_K) = f_D(Y)$. Paru koder-dekoder pridružujemo ratu greške P_e definisanu sa :

$$P_e = \frac{1}{K} * \sum_{k=1}^{N} P(U_k \neq \hat{U}_k) \quad .$$

Na ovaj način imamo definisan sistem koder-dekoder koji označavamo uređenom četvorkom : (K, N, D, P_e)

Ovakav oblik komunikacionog sistema koristićemo u daljim razmatranjima. U pogledu organizacije prenosa razmotrićemo *serijski prenos* (koristi se jedan prenosni kanal zajednički za sve kodne kanale, a time i jedan sistem komunikacije) i *paralelni prenos* (koristi se 5 kanala prenosa, po jedan za svaki kodni kanal, tj. 5 paralelnih sistema komunikacije).

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

$p_E(x|u)$, $u \in U^K$, $x \in X^N$. Ako su K slučajnih promenljivih izvora $U^K=(U_1,U_2,\ldots,U_K)$ ulaz kodera, izlaz je slučajni vektor $X^N=(X_1,X_2,\ldots,X_N)$. Neka su Y^N i Z^N respektivno izlazi kanala sa verovatnoćama prelaza $P_M^{(N)}$ i $P_{MW}^{(N)}$, kada je ulaz X^N. Nelegalni učesnik ocenjuje ekvivokaciju izvora po simbolu izvora na sledeći način :

$$D \triangleq \frac{1}{K} * H(U^K|Z^N) \quad .$$

Veličinu D uzimamo za kriterijum WT neodređenosti i koder se dizajnira tako da se ona učini što većom. Kada je D=K kažemo da je ostvarena apsolutna tajnost, tj. potpuna zaštita.

Dekoder je preslikavanje : $f_D : Y^N \rightarrow \hat{U}^K$.

Neka je $\hat{U}^K = (\hat{U}_1,\hat{U}_2,\ldots,\hat{U}_K) = f_D(Y)$. Paru koder-dekoder pridružujemo ratu greške P_e definisanu sa :

$$P_e = \frac{1}{K} * \sum_{k=1}^{N} P(U_k \neq \hat{U}_k) \quad .$$

Na ovaj način imamo definisan sistem koder-dekoder koji označavamo uređenom četvorkom : (K, N, D, P_e)

Ovakav oblik komunikacionog sistema koristićemo u daljim razmatranjima. U pogledu organizacije prenosa razmotrićemo *serijski prenos* (koristi se jedan prenosni kanal zajednički za sve kodne kanale, a time i jedan sistem komunikacije) i *paralelni prenos* (koristi se 5 kanala prenosa, po jedan za svaki kodni kanal, tj. 5 paralelnih sistema komunikacije).

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

2. ENTROPIJA JEZIK

2.1. Statistički model jezika

Generisanje tekstova, koje produkuje izvor komunikacionog sistema, nastaje kao rezultat međusobnog dejstva više promenljivih (sistem, norma, uzusi jezika i dr.), zavisi od situacije u kojoj se tekst realizuje, individualnih osobina stvaraoca teksta i operatera na komunikacionom uređaju. Zbog takve kompleksnosti jezika nemoguće je konstruisati dobar

generator poruka koji bi obuhvatio sve karakteristike i zakonitosti jezika.

Da bi se prevazišao ovaj problem vrši se modeliranje jezika. Model jezika u svakom konkretnom slučaju omogućava da se korišćenjem reprezentativnog uzorka i obradom na računaru brzo i pouzdano izdvoje potrebni elementi jezika, izuče njihove međusobne veze. Centralno pitanje koje se pri tome postavlja jeste izbor reprezentativnog uzorka, obrada i intepretacija dobijenih rezultata. Izbor uzorka mora se vršiti po principu slučajnosti, tj. mora se omogućiti da svi elementi osnovnog skupa mogu sa jednakom verovatnoćom ući u uzorak.

Različiti naučni problemi nametnuli su potrebu izučavanja i matematičkog modeliranja izvora informacija, a time i jezika, kao izrazito važnog izvora informacija. Matematički model jezika nikad nije identičan sa samim jezikom i predstavlja samo određenu aproksimaciju prirodnog jezika, prilagođenu konkretnom problemu, čime je omogućeno proučavanje onih karakteristika jezika za koje je taj model prilagođen.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

$$P(C) = P(x_1, x_2, \ldots, x_n) \ , \ \sum_C P(C)=1 \ , \ n=1,2,\ldots$$

Obeležavajući sa F presek svih σ-polja koja sadrže sve trajektorije dobijamo traženi prostor verovatnoće (Ω, F, P). Na taj način, zadavanjem alfabeta A , raspodele verovatnoće P i određivanjem klase F definisan je slučajan proces kojim opisujemo jezik L.

Ovako konstruisan model jezika, u vidu diskretnog izvora informacija,potiče od Mc-Millana i označava se parom (A,P) gde je A alfabet tog izvora ili jezika, a P raspodela verovatnoće n-članih nizova ili tekstova posmatranog jezika.

Diskretni binarni izvor informacija definišemo parom (A,P) koji čine alfabet $A = \{ a_1, a_2 \} = \{ 0,1 \}$ i raspodela verovatnoća P n-članih nizova koji su proizvod tog izvora.

2.2. Entropija jezika

Definicija 1

Za jezik L nad alfabetom A kaže se da poseduje *svojstvo stacionarnosti* (ili da je *stacionaran*) ako je za svako h=0,1,... i za svaku realizaciju $(a_{k_1} a_{k_2} \ldots a_{k_n})$, $a_{k_i} \in A$:

$$P(x_1 \ x_2 \ \ldots \ x_n) = P(x_{1+h} \ x_{2+h} \ \ldots \ x_{n+h})$$

tj. verovatnoća određenog teksta ne zavisi od mesta tog odsečka u sveukupnom jeziku.

Polazeći od toga da jezik L sa alfabetom A posmatramo kao stacionaran diskretan izvor informacija (A,P), definisaćemo entropiju jezika i navesti neke njene osnovne osobine.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Konstruišu se razni fizički i logičko-matematički modeli koji predstavljaju jedno od glavnih sredstava u proučavanju raznih osobina i zakonitosti jezika. Među svim dosad uvedenim modelima jezika značajno mesto zauzimaju verovatnosno-statistički modeli, koji koriste metode teorije verovatnoće i matematičke statistike. Oni omogućuju uspešno proučavanje statističke strukture jezika čije poznavanje ima veliku praktičnu primenu. Takav pristup verovatnosno-statističkog modeliranja polazi od pretpostavke da se tekst posmatra kao slučajni proces, a jedinice teksta kao slučajni događaji.

Proizvod svakog izvora informacija možemo posmatrati kao slučajni proces. Jezik L sa alfabetom $A = (a_1, a_2, \ldots, a_s)$, $s \in N$ intepretiramo kao diskretan slučajni proces $X(t)$, $t \in T \equiv D$, gde je D skup celih brojeva a realizacije procesa su nizovi (x_t), $t \in D$ koji predstavljaju tekstove jezika L nad alfabetom A.

Konstruišimo verovatnosni prostor (Ω, F , P), pri čemu je skup svih mogućih ishoda $\Omega = \{ (x_t) , t \in E \}$, a elementarni događaji $\omega \in \Omega$ su nizovi oblika $(x_t), t \in D$. Za fiksirano $\omega \in \Omega$, proizvoljno $n \in N$ i $t_1, t_2, \ldots, t_n \in D$ definišemo *realizaciju* ili *trajektoriju* slučajnog procesa:

$$C = (x_1, x_2, \ldots, x_n) \quad \text{gde je} \quad x_1 = a_{t_1}, x_2 = a_{t_2}, \ldots, x_n = a_{t_n}$$

$$t_1 < t_2 < \ldots < t_n \quad , \quad a_{t_1}, a_{t_2}, \ldots, a_{t_n} \in A.$$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Konstruišu se razni fizički i logičko-matematički modeli koji predstavljaju jedno od glavnih sredstava u proučavanju raznih osobina i zakonitosti jezika. Među svim dosad uvedenim modelima jezika značajno mesto zauzimaju verovatnosno-statistički modeli, koji koriste metode teorije verovatnoće i matematičke statistike. Oni omogućuju uspešno proučavanje statističke strukture jezika čije poznavanje ima veliku praktičnu primenu. Takav pristup verovatnosno-statističkog modeliranja polazi od pretpostavke da se tekst posmatra kao slučajni proces, a jedinice teksta kao slučajni događaji.

Proizvod svakog izvora informacija možemo posmatrati kao slučajni proces. Jezik L sa alfabetom $A = (a_1, a_2, \ldots, a_s)$, $s \in N$ intepretiramo kao diskretan slučajni proces $X(t)$, $t \in T \equiv D$, gde je D skup celih brojeva a realizacije procesa su nizovi (x_t), $t \in D$ koji predstavljaju tekstove jezika L nad alfabetom A.

Konstruišimo verovatnosni prostor (Ω, F , P), pri čemu je skup svih mogućih ishoda $\Omega = \{ (x_t) , t \in E \}$, a elementarni događaji $\omega \in \Omega$ su nizovi oblika $(x_t), t \in D$. Za fiksirano $\omega \in \Omega$, proizvoljno $n \in N$ i $t_1, t_2, \ldots, t_n \in D$ definišemo *realizaciju* ili *trajektoriju* slučajnog procesa:

$$C = (x_1, x_2, \ldots, x_n) \quad \text{gde je} \quad x_1 = a_{t_1}, x_2 = a_{t_2}, \ldots, x_n = a_{t_n}$$

$$t_1 < t_2 < \ldots < t_n \quad , \quad a_{t_1}, a_{t_2}, \ldots, a_{t_n} \in A.$$

Svakoj realizaciji pridružujemo verovatnosnu karakteristiku P tako da je za svako fiksirano n :

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Aproksimacija modela, u odnosu na realni jezik, je što ćemo pretpostaviti da slučajni proces koji opisuje jezik ima stacionarni karakter, tj. pretpostavlja se nepromenljivost kompleksa uslova u vremenu tokom produkcije sistema. Realni tekstovi su realizacija nestacionarnog slučajnog procesa. Razlog tome su počeci i završetci tekstova (pasusa) gde je narušena stacionarnost (npr. poznati standardni počeci teksta), a što se više odmičemo od početka osobina stacionarnosti je sve bolja. Zbog složenosti primene matematičkog aparata u izučavanju nestacionarnih slučajnih procesa, uzima se pretpostavka o stacionarnosti jezika, pa ćemo dalje posmatrati samo stacionarni jezik i podrazumevati da je njemu odgovarajući izvor stacionaran izvor.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Definicija 2

Stacionarni *jezik* L *je reda* m ako je m najmanji prirodan broj za koji važi :

$$P(a_n|a_1a_2\cdots a_{n-1}) = P(a_n|a_{n-m}a_{n-m+1}\cdots a_{n-1})$$

za svaku realizaciju

$$(\alpha_{k_1} \alpha_{k_2} \cdots \alpha_{k_n}) , \alpha_{k_i} \in A ,$$

za koju postoje navedene uslovne verovatnoće.

Intuitivno je jasno, a eksperimentalno potvrđeno, da na verovatnoću slova na n-tom mestu najviše utiče slovo na (n-1)-om mestu, nešto manje slovo na (n-2)-om mestu i tako sve manje do slova na nekom (n-m-1)-om mestu koje više ne utiče na

utiče samo n-gram $(a_{n-m}a_{n-m+1}\cdots a_{n-1})$. Prema tome, u jeziku reda m na verovatnoću narednog slova utiče samo m prethodnih slova. Za izvor (A,P) koji generiše jezik reda m kažemo da je izvor sa veličinom memorije m.

Za poznat red jezika m[1] pojednostavljeno je izračunavanje verovatnoća n-grama jer je :

$$P(x_1\ldots x_n)=P(x_1\ldots x_m)P(x_{m+1}|x_1\ldots x_m)P(x_{m+2}|x_2\ldots x_{m+1})*$$

$$*P(x_{m+3}|x_3\ldots x_{m+2})\ldots P(x_{n-1}|x_{n-m-1}\ldots x_{n-2})P(x_n|x_{n-m}\ldots x_{n-1}) \ .$$

Ovim je pokazano da je jezik L, tj. njemu odgovarajući izvor (A,P) potpuno određen ako je data respodela verovatnoća tekstova dužine m+1, jer je tada određena i raspodela tekstova bilo koje dužine $n>m+1$. Znači, sve statističke osobine stacionarnog jezika reda m kondezuju se u strukturama $(x_1x_2\cdots x_{m+1})$.

U proučavanju jezika od značaja su uslovne verovatnoće :

$$P(x_n|x_1x_2\ldots x_{n-1}) = \frac{P(x_1\ x_2\ \ldots x_n)}{P(x_1\ x_2\ \ldots x_{n-1})} \quad , \quad P(x_1x_2\ldots x_{n-1}) > 0.$$

Statističke verovatnoje n-grama utvrđuju se na osnovu dovoljno dugačkog uzorka tekstova. Ali, već za tetragrame, a posebno za n-grame kada je n>5 to predstavlja nedostižan zadatak i uz upotrebu najsavremenije računarske tehnike jer je praktično

---

[1] *Praktično je teško utvrditi red* m *nekog konkretnog jezika, pa se u praksi uzima vrednost koja dovoljno dobro aproksimira realno stanje (za prirodne jezike obično se uzima* m *oko 30).*

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

nemoguće dobiti potpune statističke podatke za odgovarajuće n-grame. Zbog toga su pronađene metode za ocenu entropije jezika izvođenjem statističkog eksperimenta.

Definicija 3

Entropija jezika na jednu poruku dužine n definiše se :

$$H_n = H(x_1x_2\ldots x_n) = -\sum_C P(C)\,\log(P(C)) =$$

$$= -\sum_{x_i\in A} P(x_1\ldots x_i\ldots x_n)\,\log P(x_1\ldots x_i\ldots x_n) \quad ,$$

Entropija H_n zavisi samo od n, alfabeta A i raspodele verovatnoća n-torki tog jezika. Ona predsavlja meru neodređenosti na jedan n-člani niz i izražava se u bitima na jedan niz (bit/niz).

Teorema 1

Za stacionarni jezik L, tj. stacionarni izvor (A,P) sa konačnim alfabetom i svaki prirodni broj n postoji granična vrednost i jednaka je entropiji na slovo jezika :

$$H = \lim_{n\to\infty} H(x_n|x_1x_2\ldots x_{n-1}) < \infty \quad .$$

Dokaz. Polazeći od nejednakosti $H(C|AB)\le H(C|B)$ i smene $x_n=C$, $x_2\ldots x_{n-1}=B$, $x_1=A$ dobijamo $H(x_n|x_1x_2\ldots x_{n-1}) \le H(x_n|x_2\ldots x_{n-1})$. Višestrukom primenom ovog postupka imamo da je

$$H(x_n|x_{n-1}) \ge H(x_n|x_{n-2}x_{n-1}) \ge \ldots \ge H(x_n|x_1x_2\ldots x_{n-1})$$

Ovo je monotono nerastući niz brojeva za koji važi za svako n:

$$0\le H(x_n|x_1x_2\ldots x_{n-1}) \le H(x_n) \le H_0 = \log s \quad .$$

Kako je ovaj niz nerastući i monotono ograničen on je

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Na osnovu osobine stacionarnosti prirodnog jezika neposredno sledi da je i teleprinterski jezik stacionaran. Time je omogućeno da postavimo odgovarajuće statističke modele u obliku diskretnog izvora informacija (A,P) i teleprinterski jezik posmatramo kao proizvod takvog izvora informacija. Poznavajući odgovarajuće raspodele P, koristeći prethodne teoreme vršićemo statističko određivanje potrebnih entropija teleprinterskog jezika.

Za jezik T nije moguće jednostavnim postupkom odrediti entropju jer je po svojstvima blizak prirodnom jeziku te poseduje memoriju veličine *m*. To znači da na verovatnoću n-tog slova utiče *m*-gram koji mu prethodi :

$$P(x_n|x_1x_2\cdots x_{n-1}) = P(x_n|x_{n-m}x_{n-m-1}\cdots x_{n-1}) \quad .$$

Zbog toga su definisane i koriste se razne metode posrednog određivanja entropije izvođenjem eksperimenata koji su u skladu sa pojmom entropije jezika [4]. Najpoznatiji je Šenonov metod i njegove varijante kojima se ocena entropoje vrši eksperimentom pogađanja slova nepoznatog teksta i naknadnom matematičkom obradom rezultata. Zbog nepodesnosti slovčanog nivoa jezika za korišćenje u komunikacionom kanalu i lakog korišćenja kodiranog oblika, naše interesovanje je usmereno na binarne nizove jezika.

Formiranje binarnog izvora moguće je kodiranjem teksta nekim binarnim kodom. Karakteristika tih izvora, verovatnoća $p_0 = P(u_i = 0)$, određena je iz primenjenog koda i jezika kome pripada tekst. U našem slučaju vrši se kodiranje tekstova

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

srpskog jezika CCITT $N^0 2$ kodom, što određuje karakteristike posmatranih binarnih izvora. Za razliku od jezika T, određivanje entropije binarnih jezika T_i, $i = \overline{1,5}$ moguće jednostavnijim postupkom. Razlog tome je što je kodiranjem i izdvajanjem kanala redukovan alfabet, a time i složena jezička struktura jezika T.

Ako uočimo niz slova teleprinterskog jezika T_i, na osnovu utvrđenog postojanja memorije niskog reda, vršićemo separaciju jezika T_i reda m na m+1 podnizova. Time dobijamo podnizove sastavljene od međusobno nezavisnih bitova $x_1,\ldots,x_n$, koji imaju raspodelu verovatnoća :

$$P(x_j=a_i)=P(a_i)=p_i \ , \ j=1,2,\ldots,n \ , \ i=0,1 \ .$$

Tako separisani nizovi teleprinterskog jezika emituje slova u skladu sa raspodelom verovatnoća (p_0,p_1) pa zbog toga važi :

$$P(x_1x_2\ldots x_n)=P(x_1)P(x_2)\ldots P(x_n) \ , \ x_j \in A \ , \ j=1,2,\ldots,n$$

kao i da je :

$$H(x_1) = H(x_2) = \ldots = H(x_n) \ .$$

Na osnovu ovog dobijamo entropiju n-članog niza :

$$H(x_1x_2\ldots x_n) = H(x_1) + H(x_2) + \ldots + H(x_n) = nH(x_1)$$

i entropiju na slovo :

$$H = \lim_{n\to\infty} \frac{H_n}{n} = \lim_{n\to\infty} \frac{H(x_1\ldots x_n)}{n} = H(x_1) = -\sum_{i=0}^{1} p_i \log p_i \ .$$

Vrednost te entropije poklapa se sa entropijom H_1^i jezika T_i na poruku dužine jednog slova, što pojednostavljuje određivanje vrednosti entropije.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Rezultati određivanja raspodele, testiranja nezavisnosti, određivanja entropije za posmatrane jezike prikazani su u poglavlju (4) i odgovarajućim prilozima.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

koder-dekoder sa parametrima k i n tako da je :

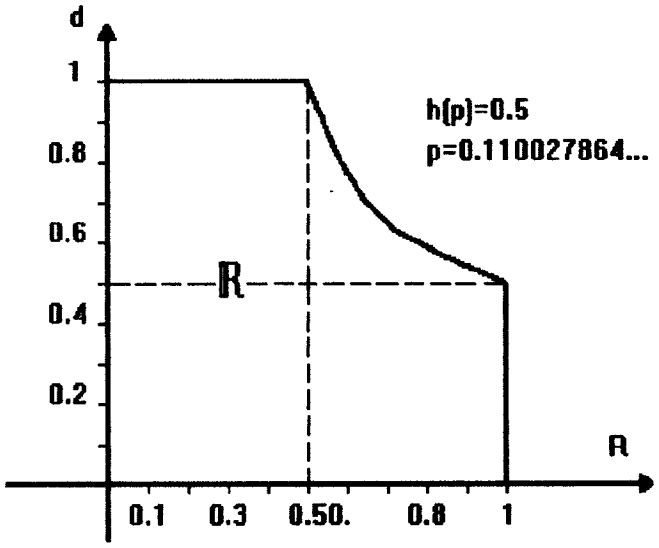
$$\frac{k}{n} \geq R - \varepsilon \quad , \quad \frac{H(U|Z)}{k} \geq d-\varepsilon \quad , \quad P_e \leq \varepsilon$$

gde je R rata prenosa , d ekvivokacija i P_e rata greške u bitovima za legitimnog učesnika. Posmatramo slučaj kad je glavni kanal bez šuma : $P_e=0$. Za ovakav specijalni slučaj komunikacionog sistema Winer je dokazao da je par (R,d) dopustiv akko je :

$$R \leq h(p) \equiv -p \log p - (1-p) \log (1-p) \qquad (1)$$

$$0 \leq d \leq 1 \ , \ 0 \leq R \leq 1 \ .$$

Skup $\mathbb{R}$ parova (R,d) koji su dopustivi prikazan je na slici 7 za slučaj h(p)=0.5 :



Slika 7. Oblast $\mathbb{R}$ dostižnih tačaka (R,d) za h(p)=0.5

Očigledno, ako je h(p)=0.5 ekvivokacija d=1 može se postići za R≤0.5 koristeći odgovarajući kod jer je ispunjen uslov (1). I za slučajeve h(p)≥0.5 lako se postiže apsolutna tajnost (d=1) koristeći odgovarajući kod rate R=0.5 (na primer kod čije kodne

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

reči čini $k=\frac{n}{2}$ bitova vektora u i $\frac{n}{2}$ slučajnih bitova).

Naizgled za $h(p)\leq 0.5$ nije moguće zaštititi ulazni niz u . Sledeća teorema (osnovni rezultat iz [2]) daje uslove pod kojima je i tada moguće kodiranjem potpuno zaštiti vektor u, tj. postići apsolutnu tajnost, koristeći (n,n-m) linearni kod :

Teorema 3

Neka je s *m*-dimenzionalna projekcija od u :

$$s = u\,P$$

gde je P proizvoljna $n\times m$ matrica, ranga m i gde je u slučajni binarni n-vektor. Za P fiksirano, posmatramo linearni kodni skup rate R=1 sa funkcijom kodiranja i dekodiranja :

$$x = u\,A^{-1} \quad , \quad u = x\,A$$

gde se A bira slučajno i uniformno iz skupa regularnih $n\times n$ binarnih matrica. Nad tim kodnim skupom svaka m-dimenzionalna projekcija s vektora u potpuno je zaštićena od prisluškivanja:

$$P\{\ A : H(S|Z) \geq m(1-\Delta)\ \} = 1-\delta(n) \text{ za } \forall\Delta>0 \quad , \quad (2)$$

samo ako je WT kanal dovoljno zašumljen, tj. :

$$h(p) \geq \frac{m}{n} \qquad (3)$$

gde $\delta(n)\longrightarrow 0$ za $n\longrightarrow\infty$.

Dokaz teoreme dat je u [2] i sastoji se u dokazivanju tri leme. Taj dokaz dajemo na kraju ove sekcije (3.3) jer svojim elementima omogućava bolje razjašnjavanje sadržaja i postupaka u daljem izlaganju.

Pomenuli smo da se za $h(p)\geq 0.5$ ($p\geq 0.11003$) može koristiti metod kojim se informativnim bitovima pridodaje skup slučajnih bitova, sa ciljem izazivanja konfuzije kod nepozvanog

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

učesnika . Teorema omogućuje ekonomičniji postupak: svih n bitova kodnog vektora koriste se za prenos informacije u kodiranom obliku, a za nepozvanog učesnika i u tajnom obliku. U sistemu nema nepoznatih ili kriptografskih elemenata, već je nepozvanom učesniku onemogućava korektno dekodiranje postojanjem samo odgovarajućeg nivoa šuma na prislušnom kanalu.

U tom sistemu komunikacije posmatramo linearne kodove sa ratom kodiranja R=1, tj. posmatramo u vektore dužine *n* koji se kodiraju u *n*-vektore x. Tako, u slučaju $h(p) \geq 0.5$,možemo podeliti vektor u na dva dela s_1 i s_2 koji će biti potpuno zaštićeni na individualnoj osnovi : $H(S_1|Z) = H(S_2|Z) = \frac{n}{2}$. Ako je $h(p) < \frac{1}{2}$, tada ne možemo potpuno zaštititi s_1 i s_2. Ako je pak $\frac{1}{3} \leq h(p) < \frac{1}{2}$, tada se u podelom na 3 dela s_1, s_2 i s_3 može potpuno zaštititi.

Očigledno, prethodna teorema uključuje particiju vektora u kao specijalni slučaj dobijen njenom višestrukom primenom :

Posledica teoreme 3

Neka su :

$$s_i = uP_i \quad , \quad i=1,2,\ldots,M$$

m-dimenzionalne projekcija od u, gde su $P_1, P_2, \ldots, P_M$ proizvoljne *nxm* matrice projektovanja (*m*-dimenzionalni operatori projektovanja), ranga *m* i gde je u slučajni binarni *n*-vektor. Posmatramo linearni kodni skup rate R=1 sa funkcijom kodiranja i dekodiranja :

$$x = u\,A^{-1} \quad , \quad u = x\,A$$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

gde se A bira slučajno i uniformno iz skupa regularnih $n \times n$ binarnih matrica. Nad tim kodnim skupom sve m-dimenzionalne projekcija s_i vektora u potpuno su zaštićene :

$P\{ A : H(S_i|Z) \geq m(1-\Delta), i=1,2,\ldots,M \} \geq 1-M\delta_1(n) = 1-\delta(n)$ za $\forall \Delta > 0$,

samo ako je WT kanal dovoljno zašumljen, tj. :

$$h(p) \geq \frac{m}{n} \qquad (3)$$

gde $\delta(n) \longrightarrow 0$ za $n \rightarrow \infty$.

Ako je $mM=n$, tada npr. možemo uzeti za s_1 prvih m bitova iz u, za s_2 drugih m bitova, itd., pri čemu su sve projekcije zaštićene na individualnoj osnovi, ako je $h(p) \geq \frac{m}{n}$.

Postupak particije omogućava da se svih n bitova kodnog vektora iskoriste za prenos informacije u obliku zaštićenom od prisluškivanja. Taj postupak omogućava i rešavanje problema zaštite u slučaju malog šuma na prislušnom kanalu, smanjivanjem dimenzije m projekcija s_i.

3.2 Uslov zašumljenosti i redundanca

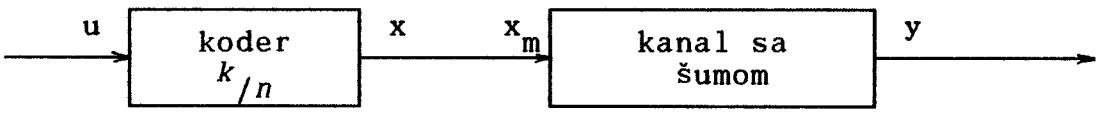
Prema teoremi 3 pretpostavlja se da je vektor u slučajan i zbog toga bez redundance . Kako vektore teleprinterskog jezika karakteriše neuniformna raspodela to je potrebno izvršiti proširenje rezultata prethodne teoreme .

Posmatraćemo **blok kodere**, tj. takve kodere koji primaju podatke u obliku nizova jednake dužine k: $u=(u_1 u_2 \ldots u_k)$. Ako je broj različitih ulaznih simbola q, tada je $M=q^k$ različitih blokova dužine k i za svaki od njih koder daje određenu kodnu reč. Svaka kodna reč $x=(x_1,\ldots,x_n)$ je niz od n ulaznih slova

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

kanala (slika 8). Broj n naziva se dužina bloka koda. Izlaznom nizu kodera dodeljujemo broj m , a odgovarajuću kodnu reč označavamo x_m. Izlazni niz kanala sa šumom, koji odgovara ulaznoj kodnoj reči x_m,označimo $y=(y_1,\ldots,y_n)$. Neka je $P_n(y|x_m)$ verovatnoća prijema niza $y=(y_1,\ldots,y_n)$ kad je x_m preneta kodna reč. Za diskretan kanal bez memorije ta verovatnoća prenosa kanalom biće :

$$P_n(y|x_m) = \prod_{i=1}^{n} P(y_i|x_{m,i}) \quad .$$



Slika 8. Kodiranje kanala sa šumom

Ovo izlaganje dajemo u opštem obliku, a na kraju ćemo razmotriti specijalni slučaj binarnih nizova (q=2).

Teorema 5 (teorema kodiranja kanala sa šumom)

Neka je $P_n(y|x)$ verovatnoća prenosa za diskretan kanal dodeljena nizu dužine $n\geq 1$. Neka je $Q_n(x)$ verovatnoća dodeljena skupu ulaznih nizova kanala, za dati broj $M\geq 2$ kodnih reči dužine n posmatranog kodnog skupa, iz koga se kodne reči biraju nezavisno sa verovatnoćom $Q_n(x)$. Pretpostavljamo da proizvoljna poruka m, $1\leq m\leq M$ ulazi u koder, uz minimalnu verovarnoću greške dekodiranja. Tada je srednja verovatnoća greške dekodiranja, po tom kodnom skupu, ograničena za svaki izbor ρ, $0\leq\rho\leq 1$:

$$\overline{P}_{e,m} \leq (M-1)^{\rho} \sum_{y} \Big[\sum_{x} Q_n(x)\, P_n(y|x)^{\frac{1}{1+\rho}} \Big]^{1+\rho} \quad .$$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Dokaz teoreme dat je u [3].

Posledica teoreme 5 (za diskretan kanal bez memorije) : Ako diskretan kanal bez memorije ima: $P_n(y|x) = \prod_n P(y_n|x_n)$; ograničen ulazni alfabet kanala sa verovatnoćama slova $Q(k)$, $k=0,1,\ldots,K-1$; verovatnoće ulaznih nizova kanala $Q_n(x) = \prod_{i=1}^{n} Q(x_n)$, za svaku kodnu reč sa slovima koja se biraju nezavisno, tada važi:

$$\overline{P}_{e,m} \le (M-1)^{\rho} \sum_{y_1}\ldots\sum_{y_n}\left[\sum_{x_1}\ldots\sum_{x_n}\prod_{i=1}^{n} Q(x_n)\,P(y_n|x_n)^{\frac{1}{1+\rho}}\right]^{1+\rho} =$$

$$=(M-1)^{\rho}\prod_{i=1}^{n}\sum_{y_n}\left[\sum_{x_n} Q(x_n)\,P(y_n|x_n)^{\frac{1}{1+\rho}}\right]^{1+\rho} =$$

$$=(M-1)^{\rho}\left\{\sum_{j=0}^{J-1}\left[\sum_{k=0}^{K-1} Q(k)\,P(j|k)^{\frac{1}{1+\rho}}\right]^{1+\rho}\right\}^{n}$$

Teorema 6 (objedinjena teorema kodiranja za izvor i kanal)

6.1. Neka je $P_n(y|x)$ uslovna verovatnoća nizova dužine n diskretnog kanala i posmatramo kodni skup, unutar koga se M kodnih reči bira nezavisno sa verovatnoćom $Q_n(x)$. Verovatnoće poruka, koje se kodiraju u te kodne reči, označimo $P(m)=q_m$, $1\le m\le M$. Neka je $q_m P(y|x_m)$ maksimum aposteriorne verovatnoće dekodiranja y za izabrano m . Ako označimo sa :

$$\overline{P}_e = \sum_m q_m \overline{P}_{e,m}$$

srednju verovatnoću greške dekodiranja po skupu poruka i po kodnom skupu, tada je za svaki izbor ρ , $0\le\rho\le 1$:

$$\overline{P}_e \le \left[\sum_{m=1}^{M} q_m^{\frac{1}{1+\rho}}\right]^{1+\rho}\sum_y\left[\sum_x Q_n(x)\,P_n(y|x)^{\frac{1}{1+\rho}}\right]^{1+\rho} \qquad (4)$$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

je U diskretan izvor bez memorije uprošćenog komunikacionog sistema sa prisluškivanjem. Tada uz uslov:

$$\lambda H(U) < C \ , \ \lambda = 1$$

imamo da je za kanal sa šumom :

$$H(U) < 1 - h(p)$$

i na osnovu teoreme 6.4 sledi da WT može smanjiti ekvivokaciju, tako da $H(U|Z) \rightarrow 0$ koristeći zajednički kod izvora i kanala. Ako taj uslov nije ispunjen biće :

$$H(U) \geq 1 - h(p) \qquad (22)$$

ili za poruke u dužine n :

$$H_n(U) \geq n[1 - h(p)] \ .$$

Na osnovu uslova (22) u obliku $h(p) \geq 1 - H(U)$ i uslova (3) svaka *m*-dimenzionalna projekcuja s od u može biti potpuno zaštićena ako je :

$$h(p) \geq \frac{m}{n} + [1 - H(U)] \qquad (23)$$

ili :

$$0 < m \leq nh(p) - [\, n - H_n(U) \,] \ . \qquad (23')$$

Izraz $n - H_n(U)$ je redundanca (suvišnost) prisutna u poruci u i značajno utiče na oblik informacionog toka do WT. Otklanjajući uticaj redundance smanjujemo maksimalnu veličinu projekcije *m* koja se može potpuno zaštititi.

Teorema 6 omogućava proširenje tvrđenja teoreme 3 na neslučajne nizove uz zamenu uslova (3) oštrijim uslovom (23) i na taj način dobijamo sledeću teoremu :

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Teorema 3'

Neka je s m-dimenzionalna projekcija od u :

$$s = u\,P$$

gde je P proizvoljna $n \times m$ matrica, ranga m i gde je u binarni n-vektor bez memorije. Za P fiksirano, posmatramo linearni kodni skup rate R=1 sa funkcijom kodiranja i dekodiranja :

$$x = u\,A^{-1} \quad , \quad u = x\,A$$

gde se A bira slučajno i uniformno iz skupa regularnih $n \times n$ binarnih matrica. Nad tim kodnim skupom je m-dimenzionalna projekcija s vektora u zaštićena od prisluškivanja:

$$P\{\, A : H(S|Z) \geq m(1-\Delta) \,\} = 1-\delta(n) \text{ za } \forall \Delta > 0 \quad ,$$

samo ako je WT kanal dovoljno zašumljen, tj. :

$$h(p) \geq \frac{m}{n} + [1 - H(U)] \qquad (23)$$

gde $\delta(n) \longrightarrow 0$ za $n \longrightarrow \infty$.

Očigledna posledica i za teoremu 3' je mogućnost particije vektora u, na m-dimenzionalne vektore, korišćenjem skupa operatora projektovanja : $P_1, P_2, \ldots, P_M$:

Posledica teoreme 3'

Neka su : $s_i = uP_i$, $i=1,2,\ldots,M$

m-dimenzionalne projekcija od u, gde su $P_1, P_2, \ldots, P_M$ proizvoljne $n \times m$ matrice projektovanja (m-dimenzionalni operatori projektovanja), ranga m i gde je u binarni n-vektor bez memorije. Posmatramo linearni kodni skup rate R=1 sa funkcijom kodiranja i dekodiranja :

$$x = u\,A^{-1} \quad , \quad u = x\,A$$

gde se A bira slučajno i uniformno iz skupa regularnih $n \times n$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

binarnih matrica. Nad tim kodnim skupom sve m-dimenzionalne projekcija s_i vektora u potpuno su zaštićene :

$P\{ A : H(S_i|Z) \geq m(1-\Delta), i=1,2,\ldots,M \} \geq 1-M\delta_1(n) = 1-\delta(n)$ za $\forall\Delta>0$,

samo ako je WT kanal dovoljno zašumljen, tj. :

$$h(p) \geq \frac{m}{n} + [1 - H(U)]$$

gde $\delta(n) \longrightarrow 0$ za $n \rightarrow \infty$.

Posmatrajući niz (x_r), $r=0,1,2,\ldots$, koji poseduje memoriju reda m, očigledno je, na osnovu definicije memorije reda m (2.2 def.2), da se izdvajanjem M podnizova dužine k:

$$x_i\ x_{i+M}\ x_{i+2M}\cdots x_{i+(k-1)M}\ , \quad M \geq m+1\ ,\ i=0,1,\ldots,M-1 \tag{24}$$

dobijaju disjunktni podnizovi među čijim elementima nema zavisnosti od prethodnih elemenata istog podniza, tj. nema memorije (memorija podnizova je reda m=0). Minimalan broj nezavisnih podnizova, za niz sa memorijom reda m, je M=m+1. Zbog jednostavnije podele i manje složenosti koda koji ćemo konstruisati u daljem izlaganju uglavnom ćemo koristiti minimalnu particiju niza sa memorijom reda m na m+1 podnizova :

$$x_i\ x_{i+(m+1)}\ x_{i+2(m+1)}\cdots x_{i+(k-1)(m+1)}\ , \quad i=0,1,\ldots,m. \tag{25}$$

Korišćenjem specijalnih operatora projektovanja P_i^* , koji ostvaruju particiju oblika (25), moguće je formirati projekcije $s_i = uP_i^*$, koje čine proizvoljni disjunktni podskupovi bitova. Na taj način moguće je primeniti postupak zaštite kodiranjem i na binarne vektore u sa memorijom reda m . Možemo postaviti sledeću teoremu koja sledi iz prethodnog izlaganja:

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Teorema 4

Neka su :

$$s_i = uP_i^* \quad , \quad i=1,2,\ldots,M$$

m-dimenzionalne projekcija koje čine M proizvoljnih disjunktnih podskupova bitova od u, gde su $P_1^*, P_2^*, \ldots, P_M^*$ specijalni m-dimenzionalni operatori projektovanja ranga m i gde je u binarni n-vektor memorije najviše reda M-1. Posmatramo linearni kodni skup rate R=1 sa funkcijom kodiranja i dekodiranja :

$$x = u\,A^{-1} \quad , \quad u = x\,A$$

gde se A bira slučajno i uniformno iz skupa regularnih $n \times n$ binarnih matrica. Nad tim kodnim skupom sve m-dimenzionalne projekcija s_i vektora u potpuno su zaštićene :

$P\{ A : H(S_i|Z) \geq m(1-\Delta), i=1,2,\ldots,M \} \geq 1-M\delta_1(n) = 1-\delta(n)$ za $\forall \Delta > 0$,

samo ako je WT kanal dovoljno zašumljen, tj. :

$$h(p) \geq \frac{m}{n} + [1 - H(U)]$$

gde $\delta(n) \longrightarrow 0$ za $n \longrightarrow \infty$.

Na osnovu Teoreme 4 formiraćemo kodova koji omogućuju zaštitu teleprinterskog jezika od prisluškivanja.

3.3 Dokaz teoreme 3

Dokaz teoreme sastoji se u dokazivanju sledeće tri leme:

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Lema 1

Neka je H = AP , gde je P fiksirana $n \times m$ binarna matrica ranga m. Ako A biramo uniformno iz skupa nesingularnih $n \times n$ matrica, tada je H uniformno raspodeljeno na skupu svih $n \times m$ binarnih matrica ranga m.

Dokaz : Iako je tvrđenje leme očigledno, daćemo kompletan dokaz zbog elemenata koji će se koristiti u sledećim dokazima.

Dokažimo prvo Lemu 1 za specijalan slučaj:

$$P = \begin{bmatrix} 1 & 0 & . & . & . & 0 \\ 0 & 1 & . & . & . & 0 \\ . & . & . & . & . & . \\ 0 & 0 & . & . & . & 1 \\ 0 & 0 & . & . & . & 0 \\ . & . & . & . & . & . \\ 0 & 0 & . & . & . & 0 \end{bmatrix} = P^*$$

gde operator preslikavanja preslikava prvih m komponenti vektora u (s = uP). U tom slučaju, stubci od H su prvih m stubaca od A u istom poretku (H = AP).

Broj nesingularnih $A_{n \times n}$ matrica je

$$(2^n-1)(2^n-2)(2^n-4)\ldots(2^n-2^{n-1})$$

jer postoji 2^n-1 izbora za prvi stubac od A (odbacuje se Ø-vektor); 2^n-2 izbora za drugi stubac (prvi izabrani stubac pripada jednodimenzionom potprostoru od 2 vektora; k-dimenzionalnom potprostoru pripada 2^k vektora); 2^n-2^2 izbora za treći stubac (prethodno izabrani stubci pripadaju dvodimenzionalnom potprostoru od 2^2 vektora);itd. Da bi matrica H bila ranga m, slično prethodnom, izbora ima :

$$(2^n-1)(2^n-2)(2^n-4)\ldots(2^n-2^{m-1})$$

jer su u H linearno nezavisni n-vektori. U specijalnom slučaju

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

izbora $P=P^*$ stubci H su prvih m stubaca od A, a njihov broj je:

$$(2^n-2^m)(2^n-2^{m+1})\ldots(2^n-2^{n-1})$$

preslikanih iz A u svako H. To je dokaz Leme 1 za specfijalni slučaj izbora matrice P.

Pretpostavimo sad da je P_{nxm} proizvoljna matrica reanga m. Tada postoji nesingularna matrica B_{nxn} ($\det B \neq 0$), koja nije jedinstvena, tako da su prvih m stubaca matrica B i P jednaki:

$$P = BP^* \quad .$$

Tada se familija H matrica generiše sa

$$H = AP = (AB)P^*$$

gde A, kao i AB, uzima vrednosti iz prostora svih nesingularnih nxn matrica. Zato su H matrice uniformno raspodeljene u prostoru svih binarnih matrica ranga m, kao za $P=P^*$.

Lema 2

Prizvoljna matrica provere H dimenzije $n \times m$, ranga m, uniformna po svim mogućim vrednostima određuje isti kodni skup kao i $(n-m)xn$ generatorna matrica G, ranga $n-m$, uniformna po svim svojim mogućim vrednostima.

Dokaz : Za datu matricu G, kod generise $(n-m)$-dimenzioni podprostor razapet nad redovima matrice G. Kako su redovi G n-dimenzionalni vektori to za (n,n-m) kod, zaključujući kao u dokazu Leme 1, moguće je generisati različitih matrica G:

$$(2^{n-m}-1)(2^{n-m}-2)(2^{n-m}-4)\ldots(2^{n-m}-2^{n-m-1}).$$

Birajući uniformno matrice G iz skupa svih $(n-m)xn$ matrica sa maksimalnim rangom je ekvivalentno izboru koda uniformno iz svih $(n,n-m)$ linearnih kodova.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Slično, izbor stubaca matrice pariteta H određuje :

$$(2^m-1)(2^m-2)(2^m-4)\ldots(2^m-2^{m-1})$$

kodova, gde svakoj matrici H odgovara jedan (n,n-m) kod. Zbog toga je izbor H uniformno ekvivalentan uniformnom izboru (n,n-m) koda.

Lema 3

Ako je $(n-m)\times n$ generatorna matrica G ranga $n-m$ izabrana uniformno po svim mogućim vrednostima, u ako je H njoj pridružena matrica provere, tada za svako $\Delta>0$:

$$P\{ G : H(EH) \geq n(h(p)-2\Delta) \} = 1-\delta(n)$$

gde je $\frac{m}{n}$ fiksirano, $h(p) < 1 - R = \frac{m}{n}$ i p rata greške, u bitovima, za e.

Dokaz : Dokaz izvodimo u dva koraka.

Prvo ćemo pokazati da ako je **G** izabrano uniformno iz skupa (n-m)xn matrica maksimalnog ranga tada, sa verovatnoćom $1-\delta(n)$, kod generisan matricom G je "dobar" kod, za $R < C = 1 - h(p)$,na BSC sa ratom greske p ($0<p\leq\frac{1}{2}$). Tada je blok grešaka P(e) tog koda koji se koristi za korekciju gresaka :

$$P(e) < \varepsilon \quad , \varepsilon > o \ .$$

Primetimo da je $P(e)\neq P_e$. P_e je bit rata greške legitimnog učesnika i na kanalu bez šuma $P_e=0$. P(e) ima drugačije značenje jer kod generisan matricom G nije korektivni za oba kanala, nego izaziva konfuziju na kanalu prisluškivača.

Ako G biramo uniformno iz skupa svih $(n-m)\times n$ matrica proizvoljnog ranga, primenom teoreme kodiranja za kodove

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Iz datih lema i nekoliko sledećih činjenica sledi dokaz Teoreme 3 :

Izbor notacije vektora m-dimenzionalne projekcije $\mathbf{s}=\mathbf{u}P$ je određen time što ćemo $\mathbf{s}$ indentifikovati sa sindrom vektorom:

$$\mathbf{s} = \mathbf{u}P = (\mathbf{x}A)P = \mathbf{x}(AP) = \mathbf{x}H .$$

Wire-tapper prijemnik prima vektor

$$\mathbf{z} = \mathbf{x} \oplus \mathbf{e}$$

tako da je

$$\mathbf{s} = (\mathbf{z} \oplus \mathbf{e})H = \mathbf{z}H \oplus \mathbf{e}H$$

gde je $\mathbf{e}$ sa raspodelom svojstvenom binarnom simetricnom kanalu sa verovatnoćom greške p. Kako su $\mathbf{z}$ i $\mathbf{e}$ nezavisni, raspodela $\mathbf{s}$ za dato $\mathbf{z}$ je translacija sa raspodelom $\mathbf{e}H$:

$$H(\mathbf{S}|\mathbf{Z}) = H(\mathbf{E}H) . \qquad (27)$$

Posmatramo H kao matricu pariteta za $(n,n-m)$ linearni kod, $\mathbf{e}H$ kao sindrom vektor. Ako je taj linearni kod dobar korekcioni kod važi da je :

$$R < C = 1-h(p)$$

ili ekvivalentno :

$$h(p) < 1 - R = \frac{m}{n} \qquad (28).$$

Kako je nama cilj da onemogućimo postojanje korekcionog svojstva, tj. informativnosti sindroma postavljamo suprotan uslov da je $R \geq C$ pa umesto (28) imamo pretpostavku (3) teoreme:

$$h(p) \geq \frac{m}{n} .$$

Tada je na osnovu Leme 3 i (27) očigledno tvrđenje (2) i važi:

$I(S;Z) = H(S) - H(S|Z) = m - H(S|Z) = m - H(EH) \leq m - nh(p) \leq 0$

odakle sledi da je $I(S;Z) = 0$. Q.E.D.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

3.4 Dokaz teoreme 6

Dokaz teoreme 6.1.:

Lema: Neka je $P(A_1),\ldots,P(A_M)$ skup verovatnoća dodeljen skupu događaja $A_1,\ldots,A_M$. Za verovatnoću njihove unije važi :

$$P(\bigcup_m A_m) \le \Big[\sum_m P(A_m)\Big]^\rho \ , \ 0 < \rho \le 1 \ , \ m=1,2,\ldots,M \qquad (10)$$

Dokaz leme: Jedna od osnovnih osobina verovatnoće je :

$$P(\bigcup_1^\infty A_m) \le \sum_1^\infty P(A_m) \quad \text{(lema o pokrivanju).} \qquad (11)$$

Za konačan skup događaja biće :

$$P(\bigcup_1^M A_m) \le \begin{cases} \sum_1^M P(A_m) & (12) \\ 1 & (13) \end{cases}$$

Ako je $\sum_m P(A_m) < 1$ tada stepenovanjem sa ρ iz (12) sledi (10). Ako bi bilo $\sum_m P(A_m) \ge 1$, stepenovanjem dobijamo da je $\Big[\sum_m P(A_m)\Big]^\rho \ge 1$, pa se na osnovu gornje granice verovatnoće (13) dobija (10). Time je lema dokazana.

Označimo sa $P(y)$ verovatnoću prijema niza y na skupu kodnih reči x_m:

$$P(y) = \sum_{x_m} Q_n(x_m) P_n(y|x_m)$$

Tada je verovatnoća greške dekodiranja :

$$\bar{P}_{e,m} = \sum_{x_m} \sum_y Q_n(x_m)\ P_n(y|x_m)\ P(\text{greška}|m,x_m,y) \qquad (14)$$

gde je $P(\text{greška}|m,x_m,y)$ uslovna verovatnoća greške dekodiranja za poruku m, dodelu odgovarajućeg kodnog niza x_m poruci m i

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

prijem niza y. Sumiranje je respektivno po svim ulaznim i izlaznim nizovima kanala dužine n.

Za dato m , x_m, y definišemo događaj $A_{m'}$, za svako $m' \neq m$, kao događaj da se kodna reč $x_{m'}$ izabere tako da je

$$q_{m'} P_n(y|x_{m'}) \geq q_m P_n(y|x_m) \quad .$$

Tada imamo za svako ρ , $0<\rho\leq 1$:

$$P(\text{greška}|m,x_m,y) \leq P\left(\bigcup_{m'} A_{m'}\right) \leq \left[\sum_{m'} P(A_{m'})\right]^{\rho} \quad , \; m' \neq m \; . \qquad (15)$$

Iz definicije $A_{m'}$, imamo za neko $s > 0$

$$P(A_{m'}) \leq \sum_{x_{m'}:\, q_{m'} P_n(y|x_{m'}) \geq q_m P_n(y|x_m)} Q_n(x_{m'}) \leq \sum_{x_{m'}} Q_n(x_{m'}) \frac{q_{m'}^s P_n(y|x_{m'})^s}{q_m^s P_n(y|x_m)^s} \qquad (16)$$

Promenljiva $x_{m'}$ u (10), je privremena promenljiva sumiranja i indeks m' možemo ukloniti posmatrajući promenljivu x, pa smenom (16) u (15) imamo :

$$P(\text{greška}|m,x_m,y) \leq \left[q_m^{-s} P_n(y|x_m)^{-s} \right]^{\rho} \left[\sum_x q_m^s \, Q_n(x) P_n(y|x)^s \right]^{\rho}$$

Smenjujući poslednju nejednakost i oslobađajući se privremene promenljive sumiranja x_m , transformišemo verovatnoću greške dekodiranja (14) na sledeći način :

$$\bar{P}_{e,m} = \sum_{x_m} \sum_y Q_n(x_m) \, P_n(y|x_m) \, P(\text{greška}|m,x_m,y) \leq$$

$$\leq \sum_y \left[\sum_{x_m} q_m^{-s\rho} Q_n(x_m) \, P_n(y|x_m)^{1-s\rho} \right] q_m^{-s\rho} \left[\sum_x q_m^s \, Q_n(x) P_n(y|x)^s \right]^{\rho} \leq$$

$$\leq \sum_y \left[\sum_x q_m^{-s\rho} Q_n(x) \, P_n(y|x)^{1-s\rho} \right] \left[\sum_x q_m^s Q_n(x) P_n(y|x)^s \right]^{\rho}$$

Dobijeni izraz smenjujemo u :

$$\bar{P}_e = \sum_m q_m \bar{P}_{e,m} \leq$$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

$$\sum_{m=1}^{M} q_m^{\frac{1}{1+\rho}} = \sum_{j=1}^{A} \Pi(j)^{\frac{1}{1+\rho}} \quad . \qquad (19)$$

Pretpostavićemo da tvrđenje (18) važi za k=k, k∈ℕ :

$$\sum_{m=1}^{M} q_m^{\frac{1}{1+\rho}} = \Big[\sum_{j=1}^{A} \Pi(j)^{\frac{1}{1+\rho}}\Big]^k \quad , \; M=A^k \; . \qquad (20)$$

Pokažimo da važi i za k=k+1 ,pri čemu je $M=A^{k+1}$.

$$\sum_{m=1}^{M} q_m^{\frac{1}{1+\rho}} = \Big[\sum_{j=1}^{A} \Pi(j)^{\frac{1}{1+\rho}}\Big]^{k+1} = \Big[\sum_{j=1}^{A} \Pi(j)^{\frac{1}{1+\rho}}\Big]^k \sum_{j=1}^{A} \Pi(j)^{\frac{1}{1+\rho}} =$$

$$=(\text{smena sa (20)}) = \sum_{m=1}^{A^k} q_m^{\frac{1}{1+\rho}} \sum_{j=1}^{A} \Pi(j)^{\frac{1}{1+\rho}} = \sum_{m=1}^{A^{k+1}} q_m^{\frac{1}{1+\rho}} \; , \; M=A^{k+1}.$$

Prelaskom na eksponencijalni zapis dobija se (5).

Dokaz teoreme 6.3. :

Za ρ=0 je $\sum_{i=0}^{A-1} \Pi(i)^{\frac{1}{1+\rho}} = \sum_{i=0}^{A-1} \Pi(i) = 1$, pa je očigledno $E_s(0)=0$.

Drugu osobinu funkcije $E_s(\rho)$ dobijamo određivanjem izvoda po ρ te složene funkcije.

$$\frac{\partial E_s(\rho)}{\partial \rho} = E_s'(\rho) = \Big(\ln\Big(\sum_{i=0}^{A-1} \Pi(i)^{\frac{1}{1+\rho}}\Big)\Big)' + \Big(\rho \ln\Big(\sum_{i=0}^{A-1} \Pi(i)^{\frac{1}{1+\rho}}\Big)\Big)' =$$

$$= \Big(\sum_{i=0}^{A-1} \Pi(i)^{\frac{1}{1+\rho}}\Big)^{-1} \Big(\sum_{i=0}^{A-1} \Pi(i)^{\frac{1}{1+\rho}}\Big)' +$$

$$+ \ln\Big(\sum_{i=0}^{A-1} \Pi(i)^{\frac{1}{1+\rho}}\Big) + \rho\Big(\sum_{i=0}^{A-1} \Pi(i)^{\frac{1}{1+\rho}}\Big)^{-1} \Big(\sum_{i=0}^{A-1} \Pi(i)^{\frac{1}{1+\rho}}\Big)' =$$

$$= (1+\rho)\Big(\sum_{i=0}^{A-1} \Pi(i)^{\frac{1}{1+\rho}}\Big)^{-1} \sum_{i=0}^{A-1} \Big(-\frac{1}{(1+\rho)^2} \Pi(i)^{\frac{1}{1+\rho}} \ln\Pi(i)\Big) + \ln\Big(\sum_{i=0}^{A-1} \Pi(i)^{\frac{1}{1+\rho}}\Big)$$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

uslov zašumljenosti

$$\left.\frac{\partial E_s(\rho)}{\partial \rho}\right|_{\rho=0} = \left(\sum_{i=0}^{A-1}\Pi(i)\right)^{-1}\sum_{i=0}^{A-1}\left(-\Pi(i)\ln\Pi(i)\right) + \ln\left(\sum_{i=0}^{A-1}\Pi(i)\right) =$$

$$= -\sum_{i=0}^{A-1}\Pi(i)\ln\Pi(i) = H(U)$$

Funkcija $E_s(\rho)$ je strogo rastuća jer je očigledno $E_s'(\rho)>0$ za $0\le\rho\le1$ $(\Pi(i)\neq1)$.

Dokaz teoreme 6.4. : Iz (5) dobijamo:

$$\overline{P}_e \le \exp\{-nE_0(\rho,Q) + kE_s(\rho)\} = \exp\left\{-n\left(E_0(\rho,Q) - \frac{k}{n}E_s(\rho)\right)\right\}$$

Srednja verovatnoća greške $\overline{P}_e \to 0$ za $n\to\infty$ i izabrane, fiksirane $Q(k)$ (za koje važi $\sum_k Q(k)=1$), ako je funkcija $E(\rho)=E_0(\rho,Q)-\lambda E_s(\rho)$ rastuća pozitivna funkcija.

Za $n\to\infty$ funkcija $E(\rho)\to E_0(\rho,Q)$ jer $\lambda E_s(\rho)\to0$ pa je $E(\rho)\ge0$, zato što je $E_0(\rho,Q)\ge0$, $\rho\ge0$ (to sledi neposredno primenom $(\sum_i P_i a_i)^r \ge \sum_i P_i a_i^r$, $r<1$, $\sum_i P_i=1$ na drugu sumu iz $E_0(\rho,Q)$, tj. na: $\sum_{k=0}^{K-1} Q(k)\,P(j|k)^{\frac{1}{1+\rho}}$ za $\rho>0$,a za $\rho=0$ očigledno važi tvrđenje).

Srednja verovatnoća greške dekodiranja može se zapisati i u obliku sledeće granice ([3] ,(5.6.15)):

$$P_e \le \exp\left\{-n\left(E_0(\rho,Q) - \rho R\right)\right\} \quad .$$

Označimo sa $E_0'(\rho,Q)=\frac{\partial E_0(\rho,Q)}{\partial\rho}$ i uočimo da je $(E_0(\rho,Q)-\rho R)\big|_{\rho=0}=0$.

Funkcija $E_0(\rho,Q)$ ima osobine ([3] st.142):

$$E_0(\rho,Q)\ge0 \ , \ \frac{\partial E_0(\rho,Q)}{\partial\rho}>0 \ , \ \frac{\partial^2 E_0(\rho,Q)}{\partial\rho^2}\le0 \ , \quad \rho\ge0 \qquad (21)$$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Tada je:

$$E_0'(\rho,Q)-R > 0 \text{ , tj. } E_0'(\rho,Q) > R$$

na osnovu fundamentalne teorema 5.6.4 ([3] st.143) da bi bilo ispunjeno $\max_{\rho,Q}[E_0(\rho,Q)-\rho R]>0$ za $0\le R<C$.

Funkcija $E(\rho)$ biće rastuća ako je $\frac{\partial E(\rho)}{\partial \rho} = E_0'(\rho,Q)-\lambda E_s'(\rho)>0$, a to je ispunjeno jer, imajući u vidu osobine (8), (21) i pretpostavku $\lambda H(U) < R$, važi :

$$E_0'(\rho,Q)-\lambda E_s'(\rho) \ge E_0'(\rho,Q)-\lambda E_s'(\rho)\Big|_{\rho=0} > R - \lambda H(U) > 0 . \qquad \text{Q.E.D.}$$

3.5 Dokaz teoreme 4

Na osnovu prethodnog izlaganja i dokazanih teorema sledi neposredno i dokaz teoreme 4, s tim što je ostalo samo još da pokažemo da važi:

$$I(S_i;Z) = 0 \text{ , } i=1,2,\ldots,M .$$

$I(S_i;Z) = H(S_i) - H(S_i|Z) =$

$= H(S_i) - (H(S_iZ) - H(Z)) = H(S_i) - (H(Z|S_i) + H(S_i) - H(Z)) =$

$= H(S_i) - [H(Z|XH_i) - (H(Z) - H(S_i))] =$

$= H(S_i) - [H(Z|X)-(H(Z)-H(UP_i^*))] \le m - [nh(p)-(n - H(U))]=$

$= m - nh(p) + (n - H(U)) \le 0 \text{ , } i=\overline{1,M}$,

pri čemu smo iskoristili: uslov (23'), $H(Z)\le n$ i $H(Z|X)=nh(p)$. Poslednja jednakost važi, bez obzira na raspodelu X, jer su X,Z ulazi i izlaz binarnog simetričnog kanala . Na osnovu prethodnog sledi da je :

$$I(S_i;Z) = 0 \text{ , } i=\overline{1,M}. \qquad \text{Q.E.D.}$$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

4. OCENA ENTROPIJE

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

postaju i ostaju približno konstantne kad dužina tekstova neograničeno raste. Otud je pri analizi jezičkog materijala korišćen obiman materijal da bi dobijeni rezultati bili verodostojni. Pored ocena dati su i intervali poverenja parametara da bi se dobila što savršenija ocena parametra.

Pri ispitivanju zakonitosti jezika došlo se do zaključka da u okviru nekog konkretnog jezika treba razlikovati podjezike, kao što su na primer : literarni, novinski, telegrafski, tehnički, vojni telegrafski, jezik određene specijalnosti i dr. Šenon je zato uveo pojam čistog jezika za jezik određene specijalnosti ili područja, a jezik u celini se naziva jezikom smeše. U našem razmatranju nije potrebno ispitivati jezik u celini, već samo telegrafski jezik. Pošto je razmatranje spušteno na nivo teleprinterskog koda za taj jezik usvojili smo, kao prikladniji, naziv teleprinterski jezik, da bi istakli uticaj postupka kodiranja teleprinterskim kodom CCITT 2 u njegovom nastanku. Postupkom kodiranja fonetska i fonološka jezička svojstva su oslabljena i izmenjena, ali je termin jezika, za teleprinterski jezik i jezike teleprinterskih kanala, uzet da bi se imalo u vidu poreklo tih nizova, koji su od prirodnog jezika nasledili karakterističnu raspodelu i niz drugih osobina.

Kao što je već rečeno, nemoguće je jednim modelom obuhvatiti svu raznovrsnost i bogatstvo jezika u pogledu njegovih mogućih realizacija. U tom smislu pogodna je situacija što nas interesuje određeni podjezik (teleprinterske

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

komunikacije) i to na nivou koda. Time se mnogo uprošćava potreban model jezika jer smo potpuno odvojeni od fonetskih i fonoloških svojstava jezika, a u statističkom smislu takav prilaz omogućava da se na manjim uzorcoma dobiju pouzdani rezultati za raspodele verovatnoća pojedinih obeležja.

Objasnićemo detaljno model jezika koji je korišćen u ovim razmatranjima. Prva transformacija pisanog jezika u teleprinterski jezik (samo za uzorak srpskog jezika) je bigramiranje karakterističnih glasova našeg jezika:

č=CC ć=CS ž=ZZ š=SS lj=LJ nj=NJ đ=DJ dž=DZ .

Na uzorcima teksta srpskog i engleskog jezika, pisanim slovčano-znakovnim alfabetom A teleprinterske tastature, izvršena je glavna transformacija postupkom kodiranja CCITT kodom. Postupkom kodiranja dolazi do svođenje ulaznog alfabeta pisanog jezika od 58 znakova na 32 kodna slova CCITT koda, što podrazumeva i uvođenja karakterističnih teleprinterskih znakova (specijalni znaci). Na taj način dobija se teleprinterski jezik T blizak pisanom jeziku, a iz njega se, izdvajanjem teleprinterskih kanala, dobijaju jezici T_i. Drugim rečima, posmatra se model teksta napisan pomoću alfabeta CCITT N^O2 koda iz priloga 1 :

$CCITT_{32}$= { 11000, 10011, 01110, ... , 00100, 00000 } ,

a u tablici je vidljiva uspostavljena korespodencija sa alfabetom pisanog teksta. U suštini, reč je o šest modela na kojima je vršena obrada teksta, jedan model za slovčani nivo sa alfabetom $CCITT_{32}$ i pet modela sa alfabetom {0,1} za kanale

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

CCITT koda (isti uzorak teksta programski je rastavljen na kanale). Pomenute modele posmatramo zato što su prisluškivaču dostupni samo podaci sa linije, a to su nizovi elemenata ili nizovi kanala CCITT koda. Tim modelima omogućena je analiza entropijskih i drugih zakonitosti koje se manifestuju u tekstu na binarnom nivou.

Istraživanje ima za cilj određivanje raspodela verovatnoća i na osnovu njih entropije kodnih elemenata jezika. Za ta i dalja razmatranja, potrebna nam je raspodela verovatnoća teleprinterskog jezika T data u prilozima 2 i 4. U prilogu 4 dat je pregled statističkih verovatnoća za slova (režim slova), znake (režim cifara) i specijalne znake, ali je najznačajniji stubac zbira verovatnoća p_i+p_j koji predstavlja raspodelu verovatnoća za 32 kodna slova teleprinterskog jezika T. Njima odgovarajući intervali poverenja su u prilogu 4a. Pregleda statističkih verovatnoća, za uzorak srpskog jezika sa alfabetom A, dat je u prilogu 2. Može se uočiti da i pored prihvatanja opisanog modela teleprinterskog jezika , najveća težina prisutnosti je u slovčanom delu alfabeta. Zadržana je karakteristična, izrazito neravnomerna, raspodela slova srpskog jezika (poređenje sa rezultatima priloga 1 iz [7]). Tako je razmak najverovatniji , slede grupa slova A,E,I,O sa najvećim verovatnoćama, a zatim i sledeće grupe sa bliskim verovatnoćama u okviru grupe: S,N,R,J,U,T; D,V,K,C,L,M i najmanje verovatna grupa Z,P,G,B,H,F sa ostalim znacima alfabeta A. Prilog 9 pokazuje postojanje neravnomerne raspodele slova engleskog

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

jezika i odgovarajućih verovatnosnih grupa za izabrani model teleprinterskog engleskog jezika sa alfabetom $\mathbb{E}_{32}$= $CCITT_{32}$.

Zbog oblika i potrebe primene ovog modela jezika samo na posmatrani sistem telegrafskih komunikacija nisu od interesa neka šira razmatranja strukture i karakteristika jezika T slovčanog nivoa. Kako slovčani nivo jezika nije primenljiv na posmatrani postupak zaštite kanala od prisluškivanja, značajnije je razmatranje binarnog nivoa i određivanje binarnih entropija (prilozi 5-8 , 10, 11).

Rezultati ocene entropije po kanalima dati su u prilogu 5 i pružaju najinteresantnije i najpotrebnije podatke. Uočava se ujednačenost entropija od 1. - 4. kanala i veliko odstupanje entropije 5. kanala. To, intuitivno neočekivano, ponašanje koda izazvano je postavkom CCITT koda, gde je kao kriterijum konstrukcije koda postavljena optimalnost koda, saglasno slovčanoj raspodeli, u smislu minimiziranja strujnih i mehaničkih inpulsa koji realizuju binarne 1. Tvorci koda su slova teleprinterskog alfabeta $CCITT_{32}$, na uzorku engleskog jezika, uredili po opadajućim frekvencijama pa su im dodelili kodne zamene uređene po rastućim Hemingovim težinama. Tako na primer razmak=00100, E=10000 i T=00001, kao najfrekventiji imaju kodne zamene minimalne Hemingove težine w=1, a malo frekventno X=10111 i Q=11101 Hemingove težine w=4. Postignuto je minimizovanje 1, što je vidljivo iz priloga 10 i odnosa p_0^k verovatnoće 0 prema p_1^k verovatnoći 1. Taj pozitivan efekat za teleprintersku komunikaciju je manji u slučaju korišćenja našeg

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

jezika (poređenje priloga 5 i 10), što je i očekivano jer su tvorci standarda kod optimizovali za engleski jezik.

Poređenjem rezultata iz priloga 5 i 10, za srpski i engleski jezik, vidljiva je približnost korespodentnih vrednosti raspodele i entropije samo između trećeg i petog kanal. To je osobina koja je zakonita i uočena je i za druge indoevropske jezike. Može se videti da važi :

$$H_k > H_5 \ , \ k=1,2,3,4 \quad ili$$

$$H_{min} = H_5 = 0.88 \ ;$$

$$H_{max} = H_3 = 1.00 \ .$$

Što se tiče vrednosti entropija kanala 1,2 i 4, ne može se uočiti neka stalnost ponašanja, već su kod različitih jezika vrednosti drugačije, ali sigurno veće od 0.92.

Iz postupka formiranja CCITT koda jasno je da on nije zasnovan na nekoj zavisnosti kanala, ali postavkom svake kodne zamene uspostavlja se fiksni odnos između vrednosti njenih bitova pa je to dovelo do određenih korelacionih veza izmađu kanala (prilog 7). Vidljivo je da je stepen linearne zavisnosti između teleprinterskih kanala X i Y mali, tj. $|R_{XY}| \leq 0.29$ i najveću vrednost dostiže za kanale 1 i 3 : $|R_{13}| = 0.29$.

Entropija jezika T, tj. niza koji čine nadoveze kodne reči, data je u prilogu 8 i 11. Prikaz je dat po serijama različite dužine (binarni nivo), gde zbog mešanja kanala i uticaja osobina jezičkog niza imamo skokovite promene entropija. Najizrazitiji "defekti" entropije su za slučajeve poklapanja serija sa kodiranim monogramima, bigramima i ostalim

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

n-gramima jezičkog niza (slovčani nivo teleprinterskog jezika n= 5, 10, 15,...). Na taj način, možemo formirati niz vrednosti H_0, H_1, H_2 entropija odgovarajućeg reda, za srpski i engleski jezik teleprinterski kodiran. U prilozima su, kao poslednji stubac, dati odgovarajući rezultati jezičkih merenja iz [9] i uočljivo je slaganje rezultata, uz očekivanu veću entropiju teleprinterskog jezika.

Pomenuli smo postojanje monogramske binarne raspodele, koja karakteriše telprinterski jezik T_i, date u prilogu 5, ali nismo razmatrali raspodelu i pitanje postojanja zavisnosti među n-gramima tih nizova. Teleprinterski jezik će biti izvor sa nezavisnim generisanjem simbola akko važi :

$$P(x_1x_2\ldots\ x_n) = P(x_1)P(x_2)\ldots P(x_n), \qquad (1)$$

$$x_j\in\{0,1\},\ j=1,2,\ldots,n\ ,\ P(x_j)=p_i, i=1,2.$$

Osobina nezavisnosti nije ispunjena, što jasno pokazuju raspodele n-torki, tj. serija dužina n=2,3,4,5, date u prilozima 12. Već na primeru serija dužina 2 i verovatnoće serije 00 jasno je da postoji zavisnost sledbenika u nizu od prethodnika jer je, na primer, $P(00) \neq P(0)P(0)$. Preciznu potvrdu nepostojanja nezavisnosti i raspodele (1) sa $P(1)=p_1=p$, $P(0) = p_2 = 1-p$, daje Pirsonov χ^2 test.

Pirsonov χ^2 test saglasnosti polazi od pretpostavke da posmatrano obeležje X ima nepoznatu funkciju raspodele F(x). Testiramo hipotezu :

$$H_0 : F(x) \equiv F_0(x)\ ,\quad x=(x_1x_2\ \ldots\ x_n)$$

na osnovu uzorka, gde je $F_0(x)$ data funkcija raspodele, u

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

našem slučaju oblika (1). Koristimo χ^2 statistiku :

$$\chi^2 = \sum_{k=1}^{r} \frac{(n_k - np_{0k})^2}{np_{0k}} = \frac{1}{n} \sum_{k=1}^{r} \frac{n_k^2}{p_{0k}} - n ,$$

koja ima asimtotski χ^2_{r-1} raspodelu. Kritična oblast testiranja za H_0 određuje se velikim vrednostima te statistike:

$$W : \chi^2 \geq C$$

gde se, za dati nivo značajnosti α, C određuje iz uslova

$$P(\chi^2 \geq C) = \alpha, \text{ odnosno } C = \chi^2_{r-1;1-\alpha} .$$

Rezultati χ^2 testa dati u prilozima 12 pokazuju značajno odstupanje od kritične vrednosti i odbacivanje hipoteze o saglasnosti sa raspodelom oblika (1), a time i nepostojanje nezavisnosti bitova teleprinterskog jezika T_i, tj. kanala teleprinterskog jezika T.

U prilozima 13 dati su rezultati χ^2 testa po kanalima za podnizove oblika :

$x_i\ x_{i+(m+1)}\ x_{i+2(m+1)} \cdots x_{i+k(m+1)}$, i=1,...,m+1 ; k=1,2,...

za m=4, ili u razvijenom obliku to je 5 podnizova:

$$\begin{aligned}
&x_1\ x_6\ x_{11} \cdots x_{1+5k} && - \quad \text{1. podniz} \\
&x_2\ x_7\ x_{12} \cdots x_{2+5k} && - \quad \text{2. podniz} \\
&x_3\ x_8\ x_{13} \cdots x_{3+5k} && - \quad \text{3. podniz} \qquad (2) \\
&x_4\ x_9\ x_{14} \cdots x_{4+5k} && - \quad \text{4. podniz} \\
&x_5\ x_{10}\ x_{15} \cdots x_{5+5k} && - \quad \text{5. podniz} .
\end{aligned}$$

Testovi pokazuju slaganje sa hipotezom (prilozi 13), što govori o postojanju nezavisnosti bitova u posmatranim podnizovima. Formiranje m+1 podnizova, za m=4, pokazuje da je memorija

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

posmatranih kanala manja ili jednaka 4. Tačnije, za kanale 3 i 4 pokazuje se postojanje memorije reda m=3 i za ostale kanale reda m=4, ali zbog zajedničke zaštite svih pet kanala i ujednačavanja podele uzećemo navedenu podelu kanala na 5 podnizova. Tako dobijeni podnizovi su sa nezavisnim elementima i raspodelom koja se lako određuje, bez ove podele na podnizove, direktno iz monogramske raspodele nizova. Znači, niz ima složenu raspodelu zbog postojanja uticaja jezičke zavisnosti između elemenata niza, a definisani podnizovi imaju raspodelu koja odgovara monogramskoj raspodeli 0 i 1 polaznog niza.

Praktično korišćenje ovih i prethodnih rezultata izloženo je u sledećem poglavlju. Osnovni metod će biti postupak particije informacionog niza kojim se pojednostavljuje zahtev za poznavanje entropije, tako da nam je potrebna samo entropija monograma. Vrednosti ocena tih entropija izdvajamo u sledećoj tabeli :

jezik	H(U)
T	0.98292
T_1	0.98046
T_2	0.99673
T_3	0.99978
T_4	0.98377
T_5	0.87863

.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

4.2 Statistička ocena entropije

Za ocenu verovatnoće p_i nekog događaja A_i , kao što je poznato, uzima se relativna frekvencija f_i događaja A_i u N nezavisnih eksperimenata :

$$\bar{p}_i = f_i = \frac{S_N^i}{N}, \quad S_N^i = \sum_{k=1}^{N} I_k, \quad I_k = \begin{cases} 1 & A_i \text{ se realizuje} \\ 0 & A_i \text{ se ne realizuje} \end{cases}, \quad k=1,N$$

Ta ocena je centrirana, postojana i najefikasnija za svako N.

Ocena entropije neke slučajne promenljive X definiše se statistikom:

$$\bar{H}(X) = -\sum_{i=1}^{n} \frac{S_N^i}{N} \log \frac{S_N^i}{N}$$

što je, u suštini, statistička ocena matematičkog očekivanja slučajnje promenljive $-\log p_i$ definisane za slučajnu promenljivu X :

$$X = \begin{pmatrix} x_1 & x_2 \cdots & x_n \\ p_1 & p_2 \cdots & p_n \end{pmatrix} .$$

Od svih osobina ove ocene istaći ćemo samo jednu osobinu značajnu za naše izlaganje, a to je da se entropija neke slučajne promenljive malo menja za male promene verovatnoća. Pretpostavimo da su se u nekoj raspodeli P promenile vrednosti verovatnoća p_i i p_j tako da je :

$$p_i' = p_i + d \quad , \quad p_j' = p_j - d$$

pri čemu je :

$$p_i' + p_j' = p_i + p_j \quad , \quad 0 \le p_i' \le 1 \quad , \quad 0 \le p_j' \le 1 \quad .$$

Tako dobijena nova raspodela :

$$P' = (p_1, p_2, \ldots, p_i, \ldots, p_j, \ldots, p_n)$$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

imaće entropiju koja će se razlikovati od entropije raspodele P u razlici vrednosti odgovarajućih sabiraka :

$$\Delta H = H(P) - H(P') =$$

$$= -p_i' \log p_i' - p_j' \log p_j' - (-p_i \log p_i - p_j \log p_j)$$

$$= d \log \frac{p_j - d}{p_i - d} - p_i \log\left(1 + \frac{d}{p_i}\right) - p_j \log\left(1 - \frac{d}{p_j}\right),$$

što pokazuje da male promene verovatnoća daju male promene entropije :

$$\Delta H \to 0 \quad \text{za} \quad d \to 0 .$$

Značaj ove osobine je u tome što, iako ocene $\frac{S_N^i}{N}$ verovatnoća p_i na osnovu uzorka uvek manje ili više odstupaju od tih verovatnoća, ta kolebanja imaju mali uticaj na ocenu entropije. Koliki je taj uticaj i kolika je preciznost ocene tog parametra odredićemo izračunavanjem odgovarajućih intervala poverenja.

4.3 Interval poverenja za verovatnoću p

Iako nam ocene verovatnoća nisu neposredno potrebne, zbog potpunije analize teleprinterskog jezika date su i ocene verovatnoća i njihovi intervali poverenja. Koristili smo interval poverenja za verovatnoću p sa nivoom poverenja β oblika :

$$[\hat{p}_1, \hat{p}_2] = \left[\frac{N}{N+z_\beta^2} \left(f + \frac{z_\beta^2}{2N} - \frac{z_\beta}{N} \sqrt{Nf(1-f) + \frac{1}{4} z_\beta^2} \right), \right.$$

$$\left. \frac{N}{N+z_\beta^2} \left(f + \frac{z_\beta^2}{2N} + \frac{z_\beta}{N} \sqrt{Nf(1-f) + \frac{1}{4} z_\beta^2} \right) \right]$$

gde je N obim uzorka, f relativna frekvencija posmatranog

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

događaja, $\Phi(z_\beta) = \frac{\beta}{2}$(entropija H ima oblik sume slučajnih veličina pa njoj, po centralnoj graničnoj teoremi, pripada asimtotski normalna raspodela).

4.4 Ocena parametara za sistem slučajnih promenljivih

Uočimo n nezavisnih realizacija dve slučajne promenljive (X,Y) :

$$(X_1,Y_1) , \ldots ,(X_n,Y_n) \quad .$$

Na osnovu tog realizovanog uzorka mogu se naći ocene za matematičko očekivanje $m_X=E(X)$ i $m_Y=E(Y)$, disperziju $D_X=\sigma^2(X)$ i $D_Y=\sigma^2(Y)$ i korelacioni moment K_{XY} koristeći statistike:

$$m_X' = \bar{X}_n = \frac{1}{n}\sum_1^n X_k \quad , \quad m_Y' = \bar{Y}_n = \frac{1}{n}\sum_1^n Y_k \qquad \text{(sredine uzorka)}$$

$$D_X' = S'^2_{n,X} = \frac{1}{n-1}\sum_1^n (X_k - m_X')^2 \qquad \text{(popravljene disperzije uzorka)}$$

$$D_Y' = S'^2_{n,Y} = \frac{1}{n-1}\sum_1^n (Y_k - m_Y')^2$$

$$R_{XY}' = \frac{K_{XY}}{\sqrt{D_X' D_Y'}} \quad ; \quad K_{XY} = \frac{1}{n}\sum_1^n X_k Y_k - \bar{X}_n \bar{Y}_n \quad .$$

Analogno se posmatra sistem od više slučajnih promenljivih i određuju ocene za m_i, D_i , K_{ij} (i,j=1,2,...,m) i odgovarajući koeficijent korelacije R_{ij} pa bi se time dobila i korelaciona matrica na osnovu koje bi se utvrđivao stepen linearne zavisnosti u posmatranom sistemu od m slučajnih promenljivih.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

4.5 Ocena parametara za funkciju slučajnih promenljivih

Neka je data funkcija $Y=H(X_1,\ldots,X_m)$ slučajnih promenljivih $X_1,\ldots,X_m$ sa matematičkim očekivanjem $a_i= E(X_i)$, disperzijom $\sigma^2(X_i)$ i korelacionom matricom $K_{ij}(j>i=1,2,\ldots,)$. Kako je i Y slučajna promenljiva mogu se naći ocene parametara te slučajne promenljive, a posebno su interesantni matematičko očekivanje i disperzija . U tom cilju može se primeniti metod linearizacije, koji se sastoji u tome da se funkcija Y razvije u Tejlorov red u okolini tačke $a(a_1,\ldots,a_m)$ pa je :

$$Y = H(a_1,\ldots,a_m) + \sum_{i=1}^{m}\left(\frac{\partial H}{\partial x_i}\right)_a (X_i-a_i) + o(X-a).$$

Na ovu linearnu funkciju primenjuje se operator matemetičkog očekivanja E i disperzije σ^2 pa se dobija :

$$E(Y) = H(a_1,\ldots,a_m) \qquad (3)$$

$$\sigma^2(Y) = \sum_{i=1}^{m}\left(\frac{\partial H}{\partial x_i}\right)_a^2 \sigma^2(X_i)+2\sum_{i<j}\left(\frac{\partial H}{\partial x_i}\right)_a\left(\frac{\partial H}{\partial x_j}\right)_a K_{ij}$$

ili u slučaju nekorelisanih slučajnih promenljivih ($K_{ij}=0$, $i\neq j$)

$$\sigma^2(Y)=\sum_{i=1}^{m}\left(\frac{\partial H}{\partial x_i}\right)_a^2 \sigma^2(X_i) \ . \qquad (4)$$

Ako imamo ocene za a_i i $\sigma^2(X_i)$ (za neki broj od opažanja) tada možemo dobiti linearne ocene matematičkog očekivanja i disperzije funkcije Y koristeći (3) i (4). Za preciznije ocene E(Y) i $\sigma^2(Y)$ treba u Tejlorov razvoju uzeti i naredne članove. Ako se uzme još jedan (kvadratni) član tada je Tejlorov razvoj funkcije $Y=H(X_1,\ldots,X_m)$ u okolini tačke $a(a_1,\ldots,a_m)$:

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

i ocene za elemente korelacione matrice $\bar{K}_{ij}, i<j=\overline{1,n}$. Zamenjujući matematička očekivanja i disperzije njihovim ocenama dobijamo sledeće ocene :

$$\bar{E}(H) = -\sum_{i=1}^{n} \bar{p}_i \log_2 \bar{p}_i$$

$$\bar{\sigma}^2(H) = \frac{1}{N \cdot \ln^2 2} \sum_{i=1}^{n} (\ln \bar{p}_i + 1)^2 \bar{p}_i \bar{q}_i +$$

$$+ \frac{1}{\ln^2 2} \sum_{i<j} (\ln \bar{p}_i + 1)(\ln \bar{p}_j + 1) \bar{K}_{ij}$$

Da bi se dobile preciznije ocene popravke, zbog nelinearnosti funkcije H, potrebno je koristiti sledeće članove Tejlorovog razvoja funkcije $Y=H(X_1,\ldots,X_m)$.

Ako su slučajne promenljive međusobno nekorelisane, tj. $\bar{K}_{ij}=0$

$$\bar{\sigma}^2(H) = \frac{1}{N \cdot \ln^2 2} \sum_{i=1}^{n} (\ln \bar{p}_i + 1)^2 \bar{p}_i \bar{q}_i$$

Na osnovu ocena za $\bar{E}(H)$ i $\bar{\sigma}^2(H)$ može se približno odrediti interval poverenja za entropiju H sa nivoom poverenja β :

$$I = \{ H : (\bar{E}(H) - z_\beta \sqrt{\bar{\sigma}^2(H)} \ , \ \bar{E}(H) + z_\beta \sqrt{\bar{\sigma}^2(H)}) \}$$

jer H ima oblik sume slučajnih veličina, pa prema centralnoj graninoj teoremi ima asimtotski normalnu raspodelu.

4.7 Interval poverenja za koeficijenat korelacije

Da bi se dobila dobra ocena za interval poverenja koeficijenta korelacije na osnovu i nevelikog obima uzorka od n elemenata za slučajne promenljive sa normalnom raspodelom, uvodi se slučajna promenljiva :

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

$$Z = \frac{1}{2} \ln \frac{1+r'}{1-r'} \qquad (5)$$

gde je r' statistička vrednost koeficijenta korelacije izračunata na osnovu uzorka. Za slučajnu promenljivu Z važi da ima normalnu raspodelu $N(E(Z),\sigma^2(Z))$:

$$E(Z) = \frac{1}{2} \ln \frac{1+r}{1-r} + \frac{r}{2(n-1)} \quad , \quad \sigma^2(Z) = \frac{1}{n-3} \quad .$$

Relacija za E(Z) važi i daje približnu vrednost očekivanja i kad se r zameni sa ocenom r' za koeficijenat korelacije.Tada je interval poverenja za Z :

$$I_b(Z) = \left(M(Z) - t_b\sqrt{\sigma^2(Z)} \; ; \; M(Z) + t_b\sqrt{\sigma^2(Z)}\right)$$

pa se na osnovu veze (5) između r i Z odredi inverzna funkcija

$$r = th(Z) = \frac{e^{2Z} - 1}{e^{2Z} + 1}$$

i odredi interval poveranja :

$$I_b(r) = (r_1, r_2) \quad , \quad r_{1,2} = th\left(M(Z) \mp t_b\sqrt{\sigma^2(Z)}\right) .$$

Ocena intervala poverenja za koeficijent korelacije u slučaju sistema od dve slučajne promenljive može se izvršiti i na sledeći način:

Slučajna promenljiva r'_{XY} za veliko n i malo r ima približno normalnu raspodelu $N(r',\sigma^2_{r'})$ gde je :

$$\sigma_{r'} = \frac{1 - r'^2}{\sqrt{n}} \quad .$$

Kako najčešće ne znamo matematičko očekivanje r', zamenjujemo ga sa r'_{XY} ocenom dobivenom realizacijom uzorka, tako da gruba ocena za interval poverenja koeficijenta korelacije bi bila :

$$I_b(r) = (r' - t_b\sigma_{r'} \; ; \; r' + t_b\sigma_{r'}) \; .$$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

5. KONSTRUKCIJA KODOVA I PRIMERI

5.1 Primeri kodova otpornih na prisluškivanje

Ovo razmatranje obuhvata postupke zaštitnog kodiranja zasnovane na primeni teoreme 4 .

Za ostvarivanje zaštitnog kodiranja potrebno je konstruisati odgovarajuće linearne kodove polazeći od nekog poznatog linearnog koda. Kvalitet konstruisanog koda nije zasnovan na tome kojoj klasi pripada osnovni kod, pa je moguće, kao osnovu, ravnopravno koristiti bilo koji linearni kod. Zbog toga, a i zbog konciznosti izlaganja, opredelili smo se za prikaz postupka korišćenja kao osnove samo jedne klase lineanih kodova. Daćemo primere zasnovane na klasi Hemingovih kodova, a razlog ovakvog izbora leži u tome što su Hemingovi kodovi:

- pogodni da se određenim metodama iz njih formiraju drugi linearni kodovi,
- jednostavni za kodiranje i dekodiranje,
- prva i široko poznata klasa linearnih kodova (konstruisani su 1950. godine),
- široko korišćeni za korigovanje i otkrivanje grešaka u digitalnim telekomunikacionim i memorijskim uređajima.

Binarni kod Heminga najjednostavnije se zadaje matricom provere H. Matrica H sadrži m redova i 2^m-1 stubaca, koje čine svi nenulti binarni vektori dužine m. Može se dati sledeća karakterizacije Hemingovih (n,k) kodova :

dužina kodnih reči	$n=2^m-1$
broj informacionih bita	$k=2^m-m-1$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

odgovarajućeg operatora projektovanja P ($s_{1xm} = uP$).

Konstrukciju koda počinjemo tako što izaberemo operator projektovanja P_{nxm}. Sam kod određujemo izborom matrice A_{nxn}, koja treba da je regularna ($\det(A) \neq 0$) i da ispuni uslov da je $H=AP$ dobra matrica pariteta Hemingovog koda. Najjednostavniji postupak izbora A je ako se elementi matrice biraju na slučajan način, čime se obezbeđuje uniformni izbor iz skupa svih nxn regularnih matrica.

U ovom primer uzećemo jednostavnu matricu projektovanja P_{nxm}, koja daje izdvajanje m=3 informaciona bita vekora u na pozicijama prve tri bita vektora:

$$P = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{vmatrix}$$

Ako je izabrana matrica :

$$A = \left|\begin{array}{ccc|cccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{array}\right|, \quad \text{tada je: } A^{-1} = \left|\begin{array}{ccccccc} 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right\} G', \quad \det(A) \neq 0.$$

H^T F

Provera H=AP pokazuje da je H dobra matrica provere Hemingovog (7,4) koda, koji je ukomponovan u formirani linearni kod definisan matricom A i funkcijom kodiranja i dekodiranja:

$$x = u\,A^{-1} \quad , \quad u = x\,A \; .$$

Elementi pomenutog Hemingovog koda, matrica provere H i

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

broj bita provere	$m=n-k$
broj ispravljivih grešaka	$t=1$ (min. težina $d=3$)
broj kodnih vektora	2^k

pri čemu je $m=2,3,4,...$ Vrednost ovih parametara za prvih 10 Hemingovih kodova data je u prilogu 14.

Kod Heminga, dužine n, može se formirati i ako matricu H sačinimo tako da $n \leq 2^m-1$. Minimalna težina biće 3 nezavisno od izbora tih n stubaca matrice H. To znači da za svako n postoji

Hemingov kod koji ispravlja sve pojedinačne greške i optimalan je za binarni simetrični kanal.

PRIMER 1.

Razmotrimo prvo jedan jednostavan primer koda dužine n=7, zasnovanog na Hemingovom (7,4) kodu sa parametrima :

dužina kodnih reči	$n=7$
broj informacionih bita	$k=4$
broj bita provere	$m=n-k=3$.

Polazeći od ovog koda realizuje se kod kojim se štiti m=3 bita informacionog vektora u (broj zaštićenih bitova odgovara broju korekcionih bitova polaznog koda). Metod omogućava potpunu zaštitu informacije, ako se vektor u formira tako da nosi samo 3 informaciona bita, preostali deo vektora dopuni pseudoslučajnim bitovima, a zaštite se samo pozicije informativnih bitova. Tako formiran kod, sa parametrima (7,3), nije ekonomičan jer je njegova rata kodiranja $R=\frac{m}{n}=\frac{3}{7}$, a zasnovan je na direktnom korišćenju teoreme 4 , tako da se štiti samo m pozicija informacionih bitova postavkom

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

generatorna matrica G, dati u sistematskom obliku, su :

$$H = AP = \left|\begin{array}{cccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right| = |Q^T I_3| \quad ,$$

$$Q^T \qquad I_3$$

$$G' = \left|\begin{array}{ccccccc} 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{array}\right| \overset{(KE)}{\cong} G = \left|\begin{array}{cccc|ccc} 1 & & & 0 & 1 & 1 & 0 \\ & 1 & & & 1 & 0 & 1 \\ & & 1 & & 0 & 1 & 1 \\ 0 & & & 1 & 1 & 1 & 1 \end{array}\right| = |I_4 Q| \quad .$$

$$I_4 \qquad Q$$

Iz datog primera, saglasno projekciji P, vidljivo je da je matrica H_{nxm} ustvari podmatrica matrice A, sačinjena od prva m=3 stupca te matrice u transponovano obliku. Generatorna matrica Hemingovog koda G_{kxn} ($GH^T=0$) dobija se iz podmatrice G', koju čine prvih k=4 reda matrice A^{-1}, ograničenim brojem elementarnih transformacija (G i G' su kombinatorno ekvivalentne (KE) i daju isti kod).

Postupak dekodiranja je interesantan sa stanovišta ostvarenja zaštite vektora u. Dekodiranje možemo posmatrati po podmatricama dekodirajuće matrice A :

$$u = x\,A = x\,|H^T|F| = |xH^T|xF| = |xAP|xF| = |s|xF|$$

pa je vidljivo da će prvih m bitova dati projekcija s = uP , a u našem slučaju to su informacioni bitovi na prvih m pozicija vektora. Prislušna strana, zbog postojanja šuma, neće dobiti ispravan oblik kodnog vektora x, pa postupkom dekodiranja neće dobiti ispravnu informacionu sekvencu.

Za dati primer koda, jedini kriterijum upotrebljivosti u našem komunikacionom sistemu je nivo šuma na prislušnom kanalu. Prema teoremi 4, binarni simetrični kanal je dovoljno zašumljen

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

za upotrebu konstruisanog koda ako je :

$h(p) \geq \frac{m}{n} + (1-H(U)) = \frac{3}{7} + (1-H(U)) = 0.42857 + (1-H(U))$.

Analizu odnosa šuma, entropije i parametara koda daćemo posle navođenja primera pogodnih za korišćenje u posmatranoj teleprinterskoj komunikaciji.

Izbor projekcije P ne utiče na kvalitet koda i može biti diktiran potrebom ostvarivanja određenog oblika kodiranja, kao što je slučaj u sledećim primerima sa particijom informacionog vektora.

PRIMER 2.

Navodimo primer konstrukcije koda dužine n=6, zasnovanog na Hemingovom (6,3) kodu sa parametrma :

dužina kodnih reči	n=6
broj informacionih bita	k=3
broj bita provere	m=n-k=3 .

Primer nije najpogodniji sa stanovišta istih vrednosti parametara k i m, ali pošto nama nije cilj posmatranja ovog Hemingovog koda kao korekcionog i odnosa njegovih parametara, jednostavnost koda poslužiće za prikaz postupka kodiranja sa particijom vektora u. Ovde je to particija vektora u na 2 dela:

$$u = |s_1 \vdots s_2| = |u_1 u_2 u_3 \vdots u_4 u_5 u_6| ,$$

što znači da će u konstrukciji koda biti korišćena dva Hemingova koda i time ostvarena individualna zaštita particija s_1 i s_2, svaka sa zasebnim Hemingovim kodom. Time je omogućena zaštita svih bitova vektora u, što znači da kod ima

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

maksimalnu ekonomičnost kad u sadrži svih n informacionih bitova.

Ovaj metod konstrukcije koda zasnovan je na dvostrukoj primeni teoreme 4 i dobar je uvod za objašnjenje sledećih konstrukcija kodova sa složenijim postupcima particije.

Konstrukciju koda počinjemo izborom operatora projektovanja P_i, i=1,2. Sam kod određujemo izborom matrice A_{nxn}, koja treba da je regularna (det(A)≠0) i da ispuni uslov da su $H_i=AP_i$ dobre matrice pariteta Hemingovog koda. Najjednostavniji postupak izbora A je ako se elementi matrice biraju na slučajan način, čime se obezbeđuje uniformni izbor iz skupa svih nxn regularnih matrica.

Odabrali smo jednostavne operatore projektovanja P_1 i P_2, kojima se vrši podela vektora u na dva dela s_1 i s_2 , gde prvi deo čine prvih m=3 bita vektora u, a drugi preostala 3 bita:

$$P_1 = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{vmatrix} \quad , \quad P_2 = \begin{vmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}$$

Ako je izabrana matrica A :

$$A=\left|\begin{array}{ccc:ccc} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right|, \text{ tada je: } A^{-1}=\left|\begin{array}{cccccc} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ \hdashline 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{array}\right| \Big\} G \quad \text{i } \det(A)\neq 0.$$

H_1^T H_2^T

Provera $H_i=AP_i$, i=1,2 pokazuje da su H_i dobre matrice provere Hemingovih (6,3) kodova, koji su ukomponovani u formirani

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

linearni kod definisan matricom A i funkcijom kodiranja i dekodiranja:

$$x = u\,A^{-1} \quad , \quad u = x\,A\,.$$

Konstruisani linearni kod omogućava potpunu zaštitu informacionog vektora u, pa pretstavlja linearni kod sa parametrima (n,n).

Binarni simetrični kanal našeg komunikacionog sistema je dovoljno zašumljen za upotrebu konstruisanog koda ako je :

$$h(p) \geq \frac{m}{n} + (1-H(U)) = \frac{3}{6} + (1-H(U)) = 0.5 + (1-H(U)).$$

Elementi korišćenih Hemingovih kodova, matrice provere H_i i generatorne matrice G_i, za i=1,2, su :

$$H_1 = AP_1 = \begin{vmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{vmatrix} \quad , \quad H_2 = AP_2 = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{vmatrix} \quad ;$$

$$G = \begin{vmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{vmatrix}.$$

gde je G zajednička generatorna matrica dva ekvivalentna koda.

PRIMER 3.

Za praktičnu upotrebu i zaštitu našeg komunikacionog sistema potrebni su kodovi veće dužine i brojnije particije. Tako za zaštitu kodnog kanala teleprinterskog jezika odgovarajući kod je kod dužine n=25, zasnovan na Hemingovom (25,20) kodu sa parametrma :

dužina kodnih reči	n=25
broj informacionih bita	k=20
broj bita provere	m=5 .

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Poznato je da za uklanjanje uticaja memorije moramo izvršiti particiju nizova teleprinterskih kanal i da smo se radi ujednačavanja postupka kodiranja opredelili za podelu na M=5 podnizova. Prema prethodnoj konstrukciji vidljivo je da vršimo particije vektora u na delove dužine m, pa traženi kod treba da zadovoljava :

$$n = Mm \ , \quad n \leq 2^m \ .$$

Proverom za m=1,2,3,... (prilog 14) dobijamo da je za m=5 (naravno i za m > 5) zadovoljen prethodni uslov, tj. da postoje Hemingov kod (25,20) koji se može koristiti za konstrukcije potrebnog koda. To je linearni (25,25) kod kojim ostvarujemo particiju niza teleprinterskog jezika na 5 podnizova oblika (4.1 (2)), sa nezavisnim elementima u okviru podniza. Time su ostvareni uslovi za primenu teoreme 4 .

U konstrukciji koda koristimo pet Hemingovih kodova i ostvarujemo individualnu zaštitu particija s_i, i=1,2,3,4,5 :

$$s_1=(u_1u_6u_{11}u_{16}u_{21}) \ , \ s_2=(u_2u_7u_{12}u_{17}u_{22}) \ , \ s_3=(u_3u_8u_{13}u_{18}u_{23}) \ ,$$
$$s_4=(u_4u_9u_{14}u_{19}u_{24}) \ , \ s_5=(u_5u_{10}u_{15}u_{20}u_{25}) \ .$$

Konstrukciju koda počinjemo izborom operatora projektovanja P_i, $i=\overline{1,5}$,koji ostvaruju projekcije s_i. Sam kod određujemo izborom matrice A_{nxn}, koja treba da je regularna ($\det(A)\neq 0$) i da ispuni uslov da su $H_i=AP_i$ dobre matrice pariteta Hemingovog koda. Najjednostavniji postupak izbora A je ako se elementi matrice biraju na slučajan način, čime se obezbeđuje uniformni izbor iz skupa svih nxn regularnih matrica.

Ogovarajući operatori projektovanja P_i, $i=\overline{1,5}$ su :

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

$P_1=$
10000
00000
00000
00000
00000
01000
00000
00000
00000
00000
00100
00000
00000
00000
00010
00000
00000
00000
00000
00001
00000
00000
00000
00000

$P_2=$
00000
10000
00000
00000
00000
00000
01000
00000
00000
00000
00000
00100
00000
00000
00000
00010
00000
00000
00000
00000
00001
00000
00000
00000

$P_3=$
00000
00000
10000
00000
00000
00000
00000
01000
00000
00000
00000
00000
00100
00000
00000
00000
00010
00000
00000
00000
00000
00001
00000
00000

$P_4=$
00000
00000
00000
10000
00000
00000
00000
00000
01000
00000
00000
00000
00000
00100
00000
00000
00000
00010
00000
00000
00000
00000
00001
00000

$P_5=$
00000
00000
00000
00000
10000
00000
00000
00000
00000
01000
00000
00000
00000
00000
00100
00000
00000
00000
00010
00000
00000
00000
00000
00001

Ako je izabrana matrica A :

$A =$

1	0	0	1	1	0	0	1	0	0	0	1	1	1	1	0	1	0	1	0	0	0	0	0	0
0	1	0	0	1	1	0	0	0	1	0	0	1	1	1	0	0	0	0	0	0	0	0	1	1
1	0	1	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	1
0	1	1	0	0	0	1	1	1	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	0	0	1	0	0	0	1	0	0	1	0	0	1	1	0	1	0	0	0	0	0	1	1	1
0	1	0	0	0	1	1	1	0	1	1	0	0	0	1	0	1	1	0	1	0	0	0	1	0
1	1	1	1	1	1	0	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	1
0	1	1	0	1	0	0	1	0	0	0	0	1	1	0	1	1	1	1	1	0	0	0	0	0
1	1	1	1	0	0	0	0	1	1	0	0	0	0	1	1	1	0	1	0	0	1	1	0	1
0	1	1	0	1	1	0	1	1	1	0	1	1	1	1	1	0	0	0	1	0	1	0	1	0
1	1	1	0	0	1	1	0	1	0	0	0	1	1	1	1	0	0	0	0	0	1	0	0	0
0	1	1	0	0	0	1	0	0	1	1	1	1	0	0	1	1	1	1	1	0	0	0	0	0
1	1	1	0	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	1	0	0	0	0	0
0	0	0	1	1	1	1	0	1	1	1	0	0	0	1	1	1	0	0	0	0	0	1	1	0
1	0	1	1	0	1	1	0	0	1	1	0	0	0	1	1	0	1	0	0	0	0	1	0	0
0	0	1	0	0	0	1	1	1	0	0	1	0	1	0	0	0	0	1	1	1	1	1	0	1
1	0	0	0	1	0	0	1	0	0	0	0	1	0	0	0	0	0	1	0	1	1	1	1	0
0	0	0	1	1	1	1	1	1	0	0	1	0	1	0	0	1	0	0	1	1	0	0	1	1
1	0	0	1	1	1	1	0	0	1	0	0	0	0	0	0	0	1	0	0	1	1	1	1	0
0	0	0	1	1	0	1	1	0	0	1	1	1	0	1	0	0	1	1	1	1	0	0	1	0
1	0	1	1	1	0	0	1	1	0	1	1	1	1	1	0	0	0	1	0	1	0	1	0	1
0	1	0	1	1	1	0	0	1	1	1	0	1	1	0	0	0	0	0	0	1	1	1	0	1
1	0	0	1	0	1	0	0	0	0	1	0	1	1	1	0	1	1	0	1	1	1	0	0	0
0	1	1	0	1	0	1	0	0	1	0	1	1	1	0	1	0	0	0	1	1	0	1	0	0
1	1	0	1	0	0	1	0	0	1	0	1	0	0	0	1	0	1	1	0	1	1	0	0	1

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

koja je regularna. Tada je njena inverzna matrica A^{-1} :

$$A^{-1}=\begin{vmatrix}
1&1&1&0&0&1&0&1&1&0&1&0&1&1&0&0&0&0&0&0&0&1&0&1&0\\
1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&1&1&0&0&1&1\\
0&1&1&1&0&1&1&0&1&1&0&1&0&1&1&1&0&1&1&1&0&0&1&1&0\\
0&1&1&1&1&0&0&1&0&0&0&0&1&0&1&1&1&0&1&1&1&1&1&1&0\\
1&1&1&1&0&1&0&1&1&0&0&1&0&0&0&1&0&0&1&0&1&1&1&1&0\\
0&0&1&0&1&0&1&1&0&0&0&1&0&0&1&1&0&1&1&0&0&0&0&0&1\\
0&0&1&0&0&1&1&1&1&1&1&1&1&0&0&0&1&1&0&1&1&0&0&1&1\\
0&0&0&1&0&1&0&0&1&1&0&0&1&0&0&1&0&0&1&1&1&0&1&0&1\\
1&0&0&1&1&0&0&0&1&0&1&1&1&0&1&0&0&1&1&1&0&0&0&0&1\\
0&0&1&1&1&1&0&1&0&0&0&1&1&1&0&0&0&0&0&0&1&1&0&0&0\\
0&0&1&0&0&0&0&1&0&1&1&0&1&0&0&1&0&0&1&1&1&0&0&1&1\\
1&0&0&0&0&1&0&0&0&0&1&1&0&1&1&0&1&0&1&0&1&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&0&1&0&0&1&0&1&1&0&1&0&1&0\\
0&1&0&1&1&1&1&1&1&1&1&1&1&0&0&1&1&0&1&0&1&0&1&0&1&1\\
1&1&1&0&1&0&0&1&0&0&1&0&1&1&1&0&0&0&1&1&1&1&1&0&1\\
0&0&1&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&1&1&0&1&1&0&0\\
1&0&1&0&0&0&1&0&0&0&0&1&0&1&1&0&0&0&1&1&0&1&0&0&1\\
0&0&1&1&0&0&0&1&0&0&1&1&0&1&1&1&1&1&0&0&1&1&0&0&1\\
0&0&1&0&1&1&1&1&0&0&0&1&0&1&1&0&0&0&0&0&1&0&1&0&0\\
1&1&1&1&0&1&1&1&0&0&1&1&0&0&0&1&1&0&1&1&1&0&0&0&1\\
0&0&1&1&0&1&0&1&1&0&1&0&1&0&0&1&0&0&1&1&0&0&0&1&1\\
0&0&1&1&0&0&1&1&1&0&1&0&1&1&0&1&1&0&1&0&1&1&0&1&0\\
0&0&0&0&0&0&1&0&1&0&0&0&0&1&0&1&1&0&0&0&0&0&0&1&1\\
0&1&1&0&1&1&0&1&0&1&1&1&0&1&1&1&1&1&0&1&0&0&0&1&1\\
1&1&0&1&1&0&1&0&0&0&1&1&1&1&1&0&1&0&1&1&0&1&1&0&1
\end{vmatrix}.$$

Provera $H_i=AP_i$, $i=\overline{1,5}$ pokazuje da je H_i dobra matrica provere Hemingovog (25,20) koda:

$$H_1=\begin{vmatrix}
1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0\\
0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0\\
0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1
\end{vmatrix},$$

$$H_2=\begin{vmatrix}
0&1&0&1&0&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&0&1&1\\
0&0&0&1&0&1&0&0&0&0&1&1&0&1&1&1&0&1&1&1&0&0&0&1&1\\
1&0&1&0&0&0&1&0&0&1&0&1&1&0&0&1&0&1&0&1&1&0&0&1&1\\
1&0&0&0&1&1&0&1&1&0&0&1&1&1&0&0&0&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&0&1&1&1&0&0&0&0&1&1&0&1&0&0&1&1&0&1
\end{vmatrix},$$

$$H_3=\begin{vmatrix}
0&0&1&1&0&0&1&1&1&1&1&1&1&0&1&1&0&0&0&0&1&0&0&1&0\\
1&0&0&1&1&1&0&1&0&1&0&0&1&0&0&1&1&1&0&1&1&0&0&0&0\\
1&1&0&0&0&0&0&1&0&1&1&1&0&0&0&0&1&0&0&1&1&1&1&1&0\\
0&0&0&1&0&1&1&1&0&0&0&1&0&0&1&0&0&0&1&1&0&0&1&0&1\\
0&0&0&0&1&0&0&0&1&0&0&0&0&1&1&1&1&0&1&0&1&1&0&1&0
\end{vmatrix},$$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

$$H_4=\begin{vmatrix}1&0&0&0&1&0&1&0&1&0&0&0&0&1&1&0&0&1&1&1&1&1&1&0&1\\0&0&1&1&0&0&1&0&1&1&1&0&1&1&0&1&0&1&0&0&1&1&0&0&0\\1&1&0&0&1&0&0&1&0&1&1&0&0&0&0&1&0&1&0&0&1&1&1&1&0\\1&0&0&0&0&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&0&1\\0&1&1&0&1&1&0&0&0&1&0&0&0&1&0&0&1&1&1&1&0&0&0&0&0\end{vmatrix},$$

$$H_5=\begin{vmatrix}1&1&0&0&0&0&1&1&0&1&0&0&0&1&0&0&1&1&1&1&1&1&0&1&0\\0&1&0&1&0&1&0&0&1&1&0&1&0&1&1&0&0&0&1&0&0&1&0&1&1\\1&1&0&0&1&1&0&0&1&1&1&0&0&1&1&0&0&0&0&1&1&0&1&0&0\\0&0&0&0&0&1&0&1&0&1&0&1&1&0&0&1&0&1&0&1&0&0&1&1&0\\0&1&1&0&1&0&1&0&1&0&0&0&0&0&0&1&0&1&0&0&1&1&0&0&1\end{vmatrix}.$$

Hemingovi (25,20) kodovi, definisani ovim matricama pariteta, ukomponovani su u formirani linearni kod definisan matricom A i funkcijom kodiranja i dekodiranja:

$$x = u\,A^{-1}, \qquad u = x\,A\,.$$

Konstruisani linearni kod omogućava potpunu zaštitu informacionog vektora u, pa pretstavlja ekonomičan kod sa parametrima (25,25).

Binarni simetrični kanal našeg komunikacionog sistema je dovoljno zašumljen za upotrebu konstruisanog koda ako je :

$$h(p) \geq \frac{m}{n} + (1-H(U)) = \frac{5}{25} + (1-H(U)) = 0.2 + (1-H(U)).$$

Pre nego iznesemo sledeći primer daćemo još neka objašnjenja i uopštenja postupka konstrukcije koda koji daje particiju vektora u.

Primetimo da su matrice P_i vrlo "slične", tj da se sledeća projekciona matrica dobija iz prethodne cikličnim šiftom stubaca za jedan korak na niže. Uvedimo sledeću oznaku za tu operaciju:

P_i=ciksift(P_{i-1},1) ili P_i=ciksift(P_1,i-1), i=1,2,...,M ,

gde je ciksift(*,*) oznaka operacije za ciklicno siftovanje stubaca matrice, gde je prvi argument matrica projetovanja čiji

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

se stupci šiftuju, a drugi argument broj koraka šiftovanja stupca na dole.

Kako su projekcione matrice koje su nama potrebne "prazne" matrice, tj. sa puno nula i malo jedinica, pogodan je i njihov zapis navođenjem samo pozicija sa jedinicom. Na primer za matricu P_1 :

$$P_1=\begin{cases} p(1,1)=1 \ ; \ p(6,2)=1 \ ; \ p(11,3)=1 \ ; \ p(16,4) \ ; \ p(21,5)=1 \\ \text{inače} \quad 0 \end{cases}$$

Uopštenje ovog zapisa i oblika pogodnih matrica projektovanja je :

$$P_j=\begin{cases} p(M(i-1)+j,i) = 1 \\ \text{inače} \qquad\quad 0 \end{cases} , \ i = \overline{1,m} \ , \ j = \overline{1,M} \ .$$

Iz izabrane matrice A jednostavno se određuju matrice H_i imajući u vidu da je $H_i=AP_i$. Tako se j-ti red matrice H_1 dobija iz i-tog stubaca matrice A za koje je p(i,j)=1 u matrici P_1. U ovom primeru to su redom 1.,6.,11.,16.,21.stubac matrice A, koji se preslikavaju u 1.,2.,...,5. red matrice H. Uopšteno važi za elemente matrice H_i:

$H_i(j,k) = A(\ k \ , \ M(j-1)+i \ )$ $\qquad i=1,M \ ; \ j=1,m \ ; \ k=1,n \ .$

Za određenje Hemingovih kodova koje koristimo u konstrukciji dovoljno je dati samo matricu H, ali lako se opisuje i generatorna matrica korišćenih ekvivalentnih kodova:

$G_i(j,k) = A^{-1}(j, \ k \ )$ $\qquad i=1,M \ ; \ j=1,n-m \ ; \ k=1,n \ ,$

koja je zajednička za korišćene kodne osnove u konstrukciji.

Kako su za brojnije particije potrebni kodovi veće dužine to je binarni zapis glomazan i nepregledan pa je jednostavnije koristiti heksadecimalni zapis, kao što je to u sledećem

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

primeru učinjeno. Pri tom je oblik zapisa vidljiv iz sledećeg primera (u binarnim četvorkama težine bitova rastu u desno) :

(1011101010010111) = (1011 ¦ 1010 ¦ 1001 ¦ 0111) = D5 9E =D59E .

PRIMER 4.

Za objedinjenu zaštitu svih pet kanala teleprinterskog jezika daćemo primer odgovarajućeg koda koji ima kodne reči dužine n=200, a zasnovan na Hemingovom (200,192) kodu sa parametrma :

dužina kodnih reči	n=200
broj informacionih bita	k=192
broj bita provere	m=8 .

Konstruisani kod treba da izvrši particiju niza teleprinterskog jezika T na 5 podjezika teleprinterskih kodnih kanala i u okviru svakog kanala na 5 podniza zbog postupka uklanjanja memorije reda 4. To znači da je potreban kod koji daje particiju na M=25 delova. Particije vektora u vršimo na delove dužine m, pa traženi kod treba da zadovoljava :

$$n = Mm \ , \quad n \leq 2^m \ .$$

Proverom za m=1,2,3,... dobijamo da je za m=8 (naravno i za m > 8) zadovoljen prethodni uslov, tj. da postoji Hemingov kod (200,192) koji se može koristiti za konstrukcije potrebnog koda. To je linearni kod kojim ostvarujemo particiju vektora $u=(u_1u_2...u_{200})$ teleprinterskog jezika T na 25 podnizova, pa su projekcija vektor u oblika :

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

$$s_1 = (u_1 u_{26} u_{51} u_{76} u_{101} u_{126} u_{151} u_{176}) ,$$

$$s_2 = (u_2 u_{27} u_{52} u_{77} u_{102} u_{127} u_{152} u_{177}) ,$$

.....

$$s_{25} = (u_{25} u_{50} u_{75} u_{100} u_{125} u_{150} u_{175} u_{200}) .$$

Konstrukciju koda počinjemo izborom operatora projektovanja P_i, $i=\overline{1,25}$, koji ostvaruju projekcije s_i. Jednostavniji zapis matrica projektovanja dimenzije 200x8 je :

$$P_j = \begin{cases} p(M(i-1)+j,i) = 1 , & i = \overline{1,m},\ j = \overline{1,M} . \\ \text{inače} \qquad\qquad 0 \end{cases}$$

Kod određujemo izborom matrice $A_{200x200}$, koja treba da je regularna ($\det(A)\neq 0$) i da ispuni uslov da su $H_i=AP_i$ dobre matrice pariteta Hemingovog koda. Postupak izbora A je realizovan programom datim u prilogu 15. Metod koji je korišćen je pseudoslučajno generisanje elemenata matrice, posle čega sledi provera da li formirana matrica zadovoljava potrebne uslove. Jedan od mogućih izbora matrice A je:

748E	D0C1	2881	34E8	F2	29	9B	CC	4E	36	6F	ED	49	BBD2	2148	048E	6AC2
6461	1E31	E6A7	0E5E	A9	01	5C	BF	40	18	0A	8D	3F	4612	68D3	661E	4C11
3DBB	A16B	7419	8FFF	53	5B	7E	80	A4	F2	EE	54	0B	6B7A	D850	9604	06D0
88C1	949D	F7E7	CFFD	5A	50	EA	F4	78	9A	BA	2C	DD	EEAB	47AD	8120	1400
910D	0FD1	802D	729C	E2	42	93	D3	40	C9	A6	4C	88	2E30	AE0A	A492	892A
2E26	5731	C278	49FF	B3	7E	94	F7	00	1B	E3	95	AD	CE72	3330	6209	8D18
3489	BCB6	3C91	4032	5C	03	EC	8A	70	3A	11	80	E5	87D1	F42E	4406	2224
6300	50C5	B002	85CB	01	F1	D8	F9	EE	F1	02	B4	E2	4F10	819B	4280	2A42
329A	89D4	491A	2739	3D	8C	68	C5	86	B9	09	00	5D	1E51	0541	6025	E28B
875B	9C78	1C07	1865	E3	90	CC	C6	44	12	46	44	2E	E799	8200	4308	DF40
98E3	CC2F	D4F7	31F9	8C	B1	61	E2	F0	6A	9C	60	6E	971A	1D16	0420	0152
CB31	AB58	A6DC	6095	83	B3	14	3B	AA	F9	DF	D8	D8	4ED0	31A8	1481	8483
771D	D042	7C70	DBCB	B2	9A	30	01	76	01	04	84	D0	AC50	2688	45A1	5B00
2A4F	9FEB	784B	F994	36	88	DB	33	40	7F	D7	35	58	F143	F104	202C	51B0
D8A8	03BA	6F78	DD3D	6C	C3	83	0A	C4	E6	F4	50	D7	5770	22A0	A4B2	1A90
082C	4000	261E	9AA5	49	18	A6	CC	09	84	41	31	08	64BB	49BC	50BD	962B
B42B	EFDA	9D4C	18E9	0E	64	B5	08	FF	D6	49	B0	28	F6E1	1A60	C099	2876
62F2	1667	625A	1A67	7F	7E	39	93	5D	0B	11	E8	88	F17B	11E8	359D	3200
BDBE	7E6F	99CD	8779	D9	7D	03	43	8F	0A	99	48	83	0263	4211	7022	DD15
CDEE	50C8	60C2	E13F	F1	68	B5	7D	5B	63	0A	CC	ED	7641	693C	1735	03A9
5723	3A1D	E7F1	5536	D7	14	55	23	A3	C8	22	F1	9A	0A21	91CC	80DC	46EA

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

C3D6 B57D CC08 DC84 34 3B 88 E8 B5 F3 9B 98 5D AC02 6723 4031 296A
90AA 81FB 72FF D42E 52 7C 76 03 D9 FB 36 19 51 9BAA 920C C108 F524
6A87 76C6 9A74 2FE1 FE C9 14 67 69 5D 8C 9C F2 09E3 1271 4415 9142
312A 6BCE CBFB 3090 86 80 9B F9 F5 4C DB 34 41 A122 40C3 9076 58CC
CAA1 6AF7 BBBF A4C6 DF F4 E9 C6 01 62 7F 98 FE D30A 0A83 8190 E8C6
D307 6232 6D77 812F 9F C7 64 24 57 00 F4 2D 93 45A2 12C8 2693 3687
60D5 825E 17F4 5085 48 8B 96 FC BD 61 0C A4 7A 5892 9C78 5480 9E80
7134 5C13 7D9E DAB4 6A A1 DA 0C AF B3 CF 68 84 0F4A 1821 1244 8505
8714 2429 89CC EC54 26 C7 63 E2 97 34 E6 08 6A 1681 944D 6242 F0E9
78A2 4BF2 E648 53C7 2D A4 F5 F4 FB 6A B3 20 16 65C8 A480 9120 B40C
E19E 334D 156F 0E42 97 59 04 4B 32 20 63 B3 78 DEA2 4615 406F 9029
3FD2 5395 ED0F 3A28 FA 63 57 A3 C4 20 C0 5A 56 1732 C2C9 87D8 7001
81AF E3A0 4C3D B295 B4 20 02 88 84 39 90 2B 7B A7C8 6303 3721 B8B4
397A EE66 33ED B092 E2 2D 30 26 08 90 61 5E CC E792 0194 6059 461B
E12B 7585 013B 7880 F5 62 D8 65 56 57 AD 67 17 2FD1 4394 0251 94C9
946E 8DCC B804 C90D ED 6A 93 4D E8 9E 94 57 48 F350 4161 2145 2409
6DDC 0422 BCCF 4F57 44 14 60 BD 4C C1 39 57 6E 4772 2BEA 0490 2287
1FD9 4B72 A08E 6458 5F 5A AF EC 92 B5 C3 B7 B6 5203 4F67 8501 01F4
6FA2 2E86 9193 9FCB 16 CA 4B 98 56 A6 08 D6 EC 0179 4133 110C CB08
1A0E BD9F AEB3 336E 28 A1 4B 30 42 D9 50 AA C1 9CE1 4C86 1251 4A52
88DB 3569 5DAE A727 55 90 61 D5 32 C9 03 FB 04 1F01 D116 7051 A05B
F433 E164 2052 9BE6 3A 9B EF F3 EA F9 0A 7A E8 BC90 4318 A578 40AC
EF8B 1D82 55AC 6210 58 9C 04 8F D8 B8 DC 23 3A 01B0 89A1 113C A145
7DAE 4B9C C58E D419 CB 8B C2 08 A8 A8 9D 03 09 B742 6942 811B 1244
204E D0BB 29A8 6809 C4 EF 45 68 44 2D 27 47 A1 6EE8 4C8A 2102 1060
553A AD3B 9384 CA93 C7 F2 9D 57 0A 0C 64 7E CD 2312 4714 6181 133D
835F AA84 52E9 83B0 33 5C 38 66 F9 20 83 2A 27 FC43 9E30 7080 8F89
9062 3958 3174 3CD4 16 63 64 99 45 CC 2E 9A E2 6CD1 A6E2 80C0 34F8
2460 E462 8670 BC67 C7 23 06 9E 7B C5 CD 12 00 8039 9C08 C444 6314
38CA FDE3 CDB4 1C00 F7 71 39 54 85 F7 09 3E 65 0949 4172 004D 5B69
EEBC 8983 4F83 5190 05 07 70 C6 AF 05 0C 2E 80 A049 DACC 05C8 1705
381D 518B 9366 474A 90 0E 4E A9 BF 95 7B 72 3B DEFB CC13 0040 54AE
0653 1066 0B87 598E 4B 22 B0 91 5D F8 1A 93 4E 3451 08C7 10AB 46DF
D875 20E2 9762 D66A C4 19 A8 41 5F A2 FD B7 55 AFE2 7521 8216 E850
AF14 86CB 2A39 8B63 F6 BC 82 40 75 21 27 4E A5 1D20 1510 D211 8D58
50E8 AE94 5D08 3F3E FC 97 08 95 0D AE 5E 3A BE C002 8C08 C536 8C20
E461 7174 A86D AF31 6D CA 15 66 63 12 88 C7 A4 40C0 A244 D47A BC96
5800 16E4 D5C4 B0BA 8A F5 8E 5D F1 83 18 5E 71 56E2 3361 B493 2722
2DBC A495 FC19 DF99 0C F7 A9 2F 73 5E 54 FE 89 2E60 2C84 9581 C25C
FEE5 0FC9 85CC E5E4 41 EB 7A 24 7B 87 F3 66 1F 5598 4180 A26D E698
A66F F0B6 8AB7 EB6D 6D B9 4A 9D 97 58 57 83 18 A460 0D1C 5149 D404
3380 9EA3 E93E E11E 55 FF 9D B1 81 B6 41 17 12 F5D1 B018 508C 5F60
C63A FF82 0EDB 2283 A1 5B CD FB 22 D3 AC D4 E9 7EE6 0223 E169 812C
9F4D E252 3341 0895 CF 61 AF 20 38 7C A4 25 C6 F125 1555 31A4 5442
0AF8 BC77 7B7D 3E08 21 1C 8E EE 16 AE 2D A8 F7 9474 836A A520 382E
5EB0 2DB5 5E1F A901 ED 40 8F B8 22 54 7D 69 12 94B4 420A 0316 746C
830B 41DC FE4D 5A79 A7 3C F2 3E 78 77 96 01 11 CADF 28A8 2199 0A21
146D 219B A125 EDFA BA 52 C3 1C 80 7B D3 68 F9 1785 94E5 80D6 34E2
E7FB DE36 64DB 52C1 CD 7F EB 08 A8 D4 12 68 A3 E5CE 68A1 B02B 68DE
3A4C 873F 1406 F4EB 83 1F 73 7E BE 8D AD 15 0C 794E 2842 E1A5 2938
0F35 F943 8139 0E37 FB CA 8F 3A 0C 5C C1 B0 D8 005F 936C 800C 0230
D1DE 2F50 1FFC 188E 3C FF 28 1D 24 8E BC A1 67 406C 086D 304F 0208
6584 18E8 CD66 0E41 DC A4 28 0E 90 40 1B 50 04 8396 DAA0 1367 08B1

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

7A79 5722 09C2 A028 0C 8B 33 A7 16 2A 98 A4 C6 3A27 EAB4 4570 0365
670C 99DE B23C FF12 5B 8C 29 73 B6 3F 34 AC 8E 85EF 3C46 F684 2012
DF76 B608 DCC0 C45A F8 F8 EA 01 68 EA 3E 9D D3 60E7 9436 6486 0B12
E2F3 CDF2 E3AB 6E27 67 B1 A1 32 CE CE 6E D5 38 AD84 0204 803B 4C1D
B525 6DB0 050A 6EC2 65 DE 4A 6A D2 98 E2 D0 AF FD86 6840 9124 0A51
C959 E557 5966 1D42 FC 76 48 DB 93 D5 9F 2D 5A 97DC 80E3 10CA 20D2
9B31 384D 344A AE39 CF 2B 97 A0 33 9D 05 69 62 F754 3813 52C2 80C5
6C2B 15E3 AE72 9778 9A 5C 25 1A 47 77 4B 28 0A 2EA5 8870 55B6 4D0D
FC72 0BA7 F2BE 9668 39 17 1C 02 27 3A CA E1 A0 D3E4 BA92 821A C0A0
01EF 170D 1EE5 E1EF 41 7B 94 DC 77 17 BC EC 0F 0BED C960 4020 2D64
7D60 8600 4A99 FA14 9A 78 5E 21 63 24 81 80 54 B935 1116 07EE 0171
8AA7 CD6D 9FB3 FE07 79 27 B4 27 DB 22 64 8C 1B 60DC C188 52A4 ACC9
508B 0DBB D2C1 55C5 80 0A 14 07 3B C7 55 E9 73 C1CC 0489 44C2 34C2
0334 1D17 AF3D AD67 5B C3 5B 7F A9 0D 22 A5 97 A3CD 0090 820A 8418
912F 27DC B811 ADFE 2A F8 30 82 C5 70 51 F9 88 36D4 0BD2 14F4 4DC5
AEBD 76B3 569F B709 D9 86 73 41 2D 31 DD 2D 0B 8C87 6B40 9730 06D0
D04E BB6A 8CDC 2DEC 5F BF B6 C8 99 DC E5 55 85 393F D428 3640 B811
4526 F48C 74B8 FA82 4B 82 7C D5 A9 2D F8 C5 55 BA15 B048 2114 328D
1DD1 D95F B631 CFB7 6C C5 3A BC B7 0C D1 04 D7 0337 A061 6282 0010
0BBC BA31 D292 58A4 2A 9D D8 03 DD 36 E1 A0 75 2344 43C5 7660 74C1
D93D 01FE E3A2 4CC9 CB AC 6B B3 BD AA 24 6C F0 2E24 A427 C1AE 2020
075C 904D A42F B14B 1A 41 D2 3C AC 57 14 D3 98 020C 20ED 8624 4412
181C 20DD 0F83 26D8 7E 13 B7 9B 56 37 76 03 66 4BA5 2320 24F0 BA47
6F20 5F34 5DA2 175D 05 5E 9D CB 6A 41 6C EE 64 A91C 9055 1002 015D
F8D8 8EB1 A5FE 07B5 11 23 07 2B 72 81 FC BA D2 8475 9110 9080 5F1A
E676 F3C8 6514 7995 3C 16 B7 21 C0 30 EE 33 6E 58AF 3E0B 4101 8120
1B0A EB9E FD46 4DB8 C7 66 35 10 56 CA 33 07 64 794F F409 5146 A902
C193 1D64 1ACA E2FB 50 2C C0 6B E2 F2 6A D6 75 4CA6 1052 A24D 2512
FC49 DB30 180F DFBB ED 2C 1A 01 B8 D3 3C 8B CF BEFF 40E1 3068 3818
05BD 94C7 6172 0117 C1 F0 77 FB F0 E8 F5 23 06 9AA4 3602 0051 5915
DF69 6CD2 6ECF B676 05 EA C4 FF 76 51 70 0A 27 6D65 B625 8100 9DA0
027C 33B0 D39D 25C6 D0 BC 4F 10 02 AE 97 17 3A D304 01B7 E24E 9071
745B 3F2D 7507 0907 2A E3 AD 1B 36 AF 08 C7 85 5564 2A8F 2699 6803
47F2 7486 085D F46F 32 E2 30 3E 0A 75 3D 2F 35 89F6 579B 6051 C826
F395 7481 B0C6 65AC 19 F7 0C 43 56 8F D3 3A B1 8F4F 2402 6380 5143
E3AC A7E5 442D CE34 B4 E5 56 94 9A 61 34 07 32 A267 563A 3552 2587
B246 86ED 2140 E4A7 06 99 A1 5F E0 23 32 B3 83 2046 08A7 20F9 82AB
A77C 864A 4BE4 9664 81 10 13 F8 C3 B0 90 2B 5C 811C 5868 F60A 4332
1475 7C05 2D4B 090C F6 2E 83 36 05 EB 6E EA 87 378F 0543 8140 409C
414B 0276 8E75 910A E5 0D E4 CC 05 C9 2C 6A 82 2D64 B900 2608 038B
31E6 257B E727 06D6 94 69 54 8C 95 0F 03 6A CA 4616 3767 D401 3254
66F2 341D 7B07 DB83 92 4A FC CF 05 46 EA 4A BB 68A4 C271 E21A 0816
77FB 0759 CB78 73B2 B3 4F 60 2C 15 E5 90 5A D3 283C 46EF 1560 2985
A638 90F4 0F95 476A 9F 51 AD A1 9F 30 BD CF 48 BBFC 828C A306 1288
3668 D62E 949B F6FC 21 3D 89 CC 3D F6 B8 76 A6 CC8F 1404 30C0 5491
A218 7AC4 F1B8 0150 36 FE 37 5A 43 3F E6 2E DB 7346 0C22 80E5 806E
D1FD B709 DEC4 B138 F9 E3 B6 38 B9 0B 12 27 37 3875 4006 0217 40AB
AD46 C03B 426B 9253 89 DB 90 03 81 8E DA CB FC 42B4 A004 4484 5416
FFE4 C922 6914 08EE 00 85 66 BF 77 B9 C3 AA 36 DDD7 E861 5018 2803
CB9A 2A0B 76AB 6142 CD E1 37 88 53 D6 84 4B 54 80CF 5296 5003 425C
D6A7 D509 B03B 7AC8 2E CD 6C F2 53 5A 5D 1B F0 C635 0017 82ED A022
68F2 4361 B5D8 4DB9 55 9C 30 D4 8F 3A 32 C7 30 108F 18BA 8687 22C0
7579 F82E 4231 DE2B 34 BB 1F E2 51 D6 70 33 6D 533D 3014 15C6 8756

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

083A	981C	8AF1	0C65	98	18	9A	16	22	AE	D9	85	BB	A860	5026	1A55	B3C8
1889	6B9C	E4BD	A027	D8	73	26	B9	26	DA	EB	14	D9	D412	3469	488A	282A
85EF	943A	5627	26AA	8A	1F	56	34	64	6C	89	55	1B	CC62	0A08	0981	EF40
7880	7BE5	13CC	2267	B6	06	5C	6C	9C	FE	0A	24	39	CF98	6C18	4A20	8B40
A459	D649	CEC6	E723	34	24	44	F0	3A	24	4A	B9	C8	28D1	8C90	3D4E	9611
5C82	5A87	9619	428C	82	0C	44	75	D6	3B	83	91	20	D0B3	4152	1A40	82D2
2007	8F3B	3888	6175	36	26	05	E4	40	CE	46	BC	73	8F9B	00DA	0B84	D2C0
5112	B7BF	244D	F790	37	25	2F	21	0A	EE	E3	20	8D	A219	DC00	6946	893C
2586	43D9	4AA2	2EE3	2A	AF	A4	A3	EA	2D	D2	50	98	B85B	8D04	5800	240D
DD10	2185	DB64	11F3	B5	D4	44	64	AC	45	9B	B1	B0	23F3	18E2	B857	1190
4BD3	0136	CAFC	A2C3	A2	D4	81	E6	32	07	7B	51	3B	1DBA	882E	0DCE	A324
F39D	9424	5966	365F	21	E8	B4	15	04	F3	DB	E9	AC	0C0A	0212	AE38	C222
0EDD	10CE	19E0	4CDB	BD	DD	03	EB	50	E8	06	D5	01	9A43	90A2	EA30	0202
1BC7	C790	CBFB	EEBB	46	B3	5C	FB	2C	51	AE	9D	D9	B782	1569	5940	0048
29D1	B93E	C476	D982	10	9A	28	01	7A	5F	70	F5	9E	BE21	EB8B	3B3C	C880
FEF4	7DBA	B245	EAB9	73	A2	D8	E6	B8	E9	2E	CD	06	5073	6390	1808	5490
22E7	D253	30D6	A9DD	E6	42	7B	C3	C9	DC	FC	29	4D	DD6A	9460	EB4C	0C38
DD85	89CD	425E	1334	4F	35	D4	38	E7	54	71	CD	2F	7638	0490	49C7	1845
2051	AD62	6AC5	1FBD	F0	17	AF	FB	01	F7	10	58	85	1630	0F2C	AE31	030F
F5E1	26F5	BAD9	B52F	23	14	70	88	FD	D6	02	80	E5	93E3	C808	AA20	AEA2
0D52	7F48	8E42	7AE5	65	76	18	17	93	47	27	14	F2	9161	B814	6DB2	0125
B034	EE1D	4D34	FBB4	A6	70	FF	47	8D	B1	93	00	8B	448B	B045	0A1A	6068
66A2	3B3C	1FA3	5840	20	04	23	DD	6D	CD	01	C0	3C	4553	8154	6C48	9427
DABC	78F1	06D2	E07E	62	43	52	90	8D	BF	3E	4D	20	37BB	0804	28CF	03B5
0D3E	CA46	2858	B9F8	08	EC	A4	D7	9D	96	31	D8	38	7882	A306	8889	7216
F127	D215	5049	B3AC	8A	A8	8A	5D	E7	C1	BC	C0	85	AA90	8236	BA3B	C101
AA60	C1AF	5F9A	8838	BF	D2	C2	51	39	18	E7	39	A9	3FA0	9486	0A0D	B2E6
F049	E879	DFA1	8602	F8	9F	1B	DE	29	08	83	74	19	CDF2	2D6C	0802	0187
A3DE	2B0B	38B0	7DB8	2F	F3	03	90	8D	07	4C	DC	12	D123	70E9	288C	9C1C
5F0B	E188	CDDB	51CB	41	8F	D2	6E	C9	98	19	B4	A7	E751	0245	8990	45C4
0F2D	F2E8	E350	64D8	36	97	9B	19	45	85	BC	99	57	5033	03E4	1838	26DF
DAFF	3E60	EDB4	D149	53	C9	3D	5F	21	56	C0	15	D1	8240	9C01	9B62	0898
C8FA	90CF	B610	3CCF	88	28	8B	DA	32	41	71	72	A7	3AA0	6A08	4A52	6869
F3A1	EC12	B71A	8D37	56	55	6B	4D	9C	D1	27	5E	3E	6090	8A15	483B	813B
AE17	23E5	EF00	878A	CB	3A	73	EF	AC	61	31	12	6D	BAA9	0898	EABC	880A
1688	ABB1	4BC9	BE11	7E	60	9C	3E	AA	7E	D4	A2	1A	C821	3100	1E8D	D4C3
C98B	D341	44FB	43F7	C9	6F	F3	91	96	79	4F	03	16	0848	318B	CF0C	2046
5E20	50DC	EA3B	D752	9D	4E	84	32	EA	19	E2	CB	30	985A	48E7	C966	006C
E301	C4A7	60E6	D95C	0C	22	09	F6	86	40	61	D6	65	D3B3	3D19	9D01	E5D1
3CA2	6D3F	AA73	4284	E9	1E	81	6A	EE	4D	E4	5B	C8	6882	A56E	BD30	1100
8A14	760F	13C5	1523	96	F5	97	98	9A	4E	1F	DF	DA	3703	6D81	08B0	A50C
BE05	38D0	DB6E	1916	3A	C4	3B	20	88	C6	CA	73	B1	C153	C491	1E7E	0422
AE97	7726	3A0B	B55D	0B	D0	EF	B0	12	24	EF	93	3F	4D19	D48A	2E04	D023
78D3	0AEE	EB27	9A5D	69	E9	DC	A8	A4	12	DF	BA	37	FA38	194E	2E80	03A3
E325	A2DB	BD3D	683D	DD	DC	D2	0B	D0	25	50	CF	06	E520	E188	CB26	7020
9D57	CC1A	3426	D173	31	F5	92	B5	6A	90	43	12	24	C020	A228	2E31	B7A1
2B72	C27B	1993	473D	83	B8	68	46	1E	08	EC	FE	65	2063	BC8C	6910	AC3C
3684	EC67	158E	E4A4	C6	A4	F4	C9	4C	18	8D	FE	C0	D129	0D11	58C1	4D04
C2D4	69C5	433B	B2EA	D7	2B	E4	4D	AB	8B	7F	7A	10	01B8	AC44	0FA1	6161
5D86	6E1A	AB01	3355	2C	41	25	54	C9	4B	70	32	21	F8C9	435A	2959	0B0C
65CB	EB24	F231	2F80	49	11	ED	75	33	09	CB	86	E2	55D0	2E30	0D23	A609
BE92	1A60	6500	8A89	EE	16	D9	83	71	84	17	62	00	1802	4084	EEF2	A300
8E9D	01DD	8051	CDF2	E5	36	E3	72	57	91	4C	CF	E4	4CEA	037D	D800	4D08

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

1A54 68DD 94D8 4D4E 3A 56 EC AD 4F A3 1B 1B 3B F299 764D EC03 5105
0D45 A6EE C795 E4C7 E3 44 FB EE D9 55 2A 1F 93 B913 071C 8A10 500A
FD5C E3F4 5C97 CBDD CD 21 79 02 A9 2A 38 A3 55 FEE1 5412 1F63 9D81
87DC 2E11 B1F8 AE7B BC C5 0B 60 71 16 C5 8A 5E 6812 4090 0C28 50B4
1EE2 C982 3636 BB76 C8 EB 8C 5C F1 34 EA 43 83 DBAB 0050 9BEC 54D0
E97F CD3C ADE0 1795 0A CC 73 D4 45 A0 AB 2A F0 320A 2E81 5F89 0A22
97CB 5EBE 64FF 3880 7C 8D 68 68 35 04 E0 DF EE 1919 D610 2806 983E
4B94 7CC7 A1F6 447E 2B B7 6B CF 9F 49 01 CF EC 50B1 0001 0A22 64EA
DCC1 27C3 B5B3 F30A F9 E1 02 1D AB 67 D3 E3 AE BE92 4A00 0D53 8794
0007 54A0 1269 50B2 1D DC C9 12 35 CF 35 32 EE FEC9 0428 08D1 0684
D4F1 F73F 13E0 E81A F2 C0 F0 97 0F 61 AC D7 41 999A 20BB 88A2 284D
84C9 B9D8 DDD2 B06E 71 02 0F 05 C8 28 1D CD 1A 355C 4353 0C6A 0971
73CF 9A08 310E B448 B5 5C CF 86 AC 9C C1 74 89 2D2D B196 5801 0253
42E4 DB3B 6A23 12CE D6 3A 67 1E FC A3 E5 ED FC 78B4 0111 1845 0080
F279 DB69 F306 0B94 B2 69 45 65 5A 6D 26 88 FE 6184 045B 0D51 5981
847B 4F5A 37B8 6F4A 04 35 CC 77 52 E2 20 24 4D 43F5 4788 8E11 7A72
38D8 F098 CAAB 7A92 26 38 5B CA 1A AE DE EC C1 2807 E099 BA2E C80A
CFD5 163A FB75 62F1 7E 26 6B BF F8 10 34 65 7E 64D7 0746 1CF0 7380
9F96 483E 294D 6545 81 52 AD 20 44 97 A2 55 67 0AFF A063 0B8A 0020
8B47 4085 47EC 1D7D 99 95 F7 00 EE A0 8D 95 C3 531F 7290 298A 58B8

Matrica A je regularna te postoji inverzna matrica A^{-1} :

3CE7 0019 4F03 0668 10 FB 00 84 65 35 A8 11 B7 F80B B66D 5495 D690
7FB0 C1DC 061B E486 83 98 FC E0 F2 5B BB 2B 1E 5EAA FA7D D656 8393
9DEB AA39 2D95 50EA 2F 04 BB 71 2D 78 6F 4B 4F 1DB8 E9FF B265 A40F
8621 04CC F913 A50E 47 D6 9E D0 BA 00 98 AE 6C C686 4703 0868 E487
42A0 4D21 A908 0D4A DD C5 51 49 F0 1C B7 9C 60 789F 0CF2 D290 7389
99DA A381 47F9 1009 48 55 A3 86 5D A3 E7 28 74 D023 6C2A 72CD DB04
4A2C 05A3 E364 AC49 65 C8 BA BD 1E 04 4B A5 B8 3E65 5F20 F5FB A9A1
BC4B 3C90 7528 B599 84 CD 1B 14 63 6F 7D FF E2 1257 1B9F 8A7E 0D84
E1D8 5ED3 B500 14CB A9 CF 4D 97 00 65 72 49 A1 F76A A523 5F2A 45A0
A5DC FD9C 3A59 ACO2 27 BE DB 9F E3 E0 F0 2B 8C 0E4F E8CA 0E03 812A
43D8 291F CD67 00DE 2A 69 CD 7E 7E A6 BC 15 F1 13DE 240B 6E56 9126
3ECD C49C 7DB9 7D4B 83 23 6B 1F 5A 91 50 E3 48 06A2 0E92 A3F1 4010
4B2B 158C 4363 0E47 C4 E8 86 BF 47 2C 5A BE AE 8E27 528A BA3F 490F
8B19 2177 5560 E1ED AD 4A 53 F3 62 B9 7F A8 97 0127 D33D 02D0 4BDA
F4FD 7194 90DD 8C22 C2 63 2D 11 62 61 72 4C 1A 7E91 4D66 9407 E1EA
155A C84F 249D 4597 7C F1 1A 02 6B BB CC A7 72 2C04 EC6C 557A A849
38D0 9969 1655 BCB4 E6 35 2F 96 D8 14 1D E1 6B AE2C 38F6 469E C6E2
0BB9 F249 5E79 CA63 E0 CB 15 77 E6 E5 EA BD 61 2ECE 1882 660F 0652
F22F BCAA 57C0 6013 B5 91 B2 AC 92 FF AE 6B 5B EB4A 6C80 8F20 F6C9
8F19 9591 2EAD C8F8 CB 9B ED 99 9A CF 7D 55 EB 747C 4676 8692 D933
8C89 F403 7178 5624 57 03 4B 5F 13 A6 19 74 2A A381 8635 FCDA 06DF
9844 EDB6 FE2E 3E36 B5 E6 C5 C3 A4 72 2C 93 16 43FE 735D FF93 0793
F353 6DC0 4B42 8551 70 CF 0E 3D 95 08 D0 32 1F 7358 1D3F 2D95 837E
4931 691E D9AC 978C 89 CA 13 B8 24 90 BA 96 81 4848 1DF0 02ED 6AD5
852F C057 A559 2993 74 0D D1 54 A0 93 2C 09 06 9340 C493 FFBB 9A67
CFBE 72E3 C433 A6A5 F6 1D 07 7E F5 33 E0 A1 B2 83E4 FDA5 E454 123D
1A43 C2B0 2096 8EB4 EC 73 90 4D EE 86 A9 94 54 A307 B20F 4616 6EAD
169A D5FC C2BD 6014 BD 27 83 43 FA 54 2F C8 38 0E79 E13F 6993 D247
CDDA B379 1C76 FDE1 FF D5 23 55 B2 1F 0E 00 76 FB27 6594 F389 E235
FA7B AD60 E0FD 13A0 3B F2 9D FB C4 D9 B6 D3 68 37BE EC76 55C5 2203

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

5B03	B0B0	E0E2	222B	7B	EA	2A	33	F0	C6	F7	93	9B	66BA	32C0	3F39	26EB
0325	676C	F8FC	CC4C	1F	D8	97	11	5D	62	01	B9	12	B24B	F612	B329	C9BC
83E9	374B	332C	B720	7D	A6	A0	44	1C	4D	20	AA	CC	021E	1843	390A	5E63
0DA2	B52F	16F4	9426	DC	B3	02	8A	C6	94	D6	F5	A2	3120	BE26	3713	2790
03A5	303B	349C	1D43	3B	22	81	10	CC	8B	60	8C	28	D708	67DD	C45E	A9F1
C9A8	5277	B95C	70F8	F1	2C	7D	AB	F4	06	C9	8D	8C	C20B	4074	6F6F	70DE
61CF	5078	3479	968F	8B	89	8B	D0	D6	A1	65	C7	33	E6E5	1A12	0B33	7A67
D317	3FAE	893A	57E5	73	27	96	D9	0D	93	14	81	5F	26FA	B2EE	EE61	016D
DD74	30AE	44DE	6234	5A	9F	10	7B	33	97	9F	06	3A	BCC6	8F8D	C754	847E
9FC5	2639	F637	C837	CE	C7	FE	CE	48	1E	6F	A5	A9	BF81	7CB2	9960	81FF
74D2	F615	E22E	6BA6	CB	09	9E	2A	BC	85	09	0B	7C	5D70	B650	9EDB	C7F8
0D7C	B1B7	82C9	B6EF	56	67	68	9E	36	A1	44	1A	44	E375	C93D	3C4C	EC84
A0D9	714B	6FB2	1F5D	02	A2	BF	77	62	3C	2E	99	7E	6BD9	9289	9DB8	4A1A
A4E3	12AA	D390	90ED	92	8B	5B	6E	B9	B6	70	E1	28	398B	D438	2221	8A2E
0916	6A2D	D717	ADAC	18	93	7B	0B	6F	6E	45	2B	9B	6E2F	1C0A	4C03	8023
99C3	88E6	3136	652D	8F	D8	4C	F0	FB	E5	A3	6C	41	10AC	FC97	7529	0975
54E6	EBF3	29ED	77AE	EC	D2	25	81	BE	71	EB	8F	FA	0269	B9D3	5F01	06DA
71F0	0D17	5212	E330	1C	DA	A1	CC	88	E6	70	4D	74	8866	B6D7	F4AF	43C9
AAB0	5CEE	0B9B	999A	67	60	FB	00	3B	10	96	0F	7C	DEB7	4DF2	1906	C843
0A7A	F083	2D65	3E8D	4A	D0	94	D4	B1	8D	76	BF	62	9D35	DD2C	953B	EC6A
9B5C	E280	9DBF	0C89	74	84	33	71	78	13	18	37	8E	89AB	1B98	1591	2FC3
4855	10DC	9BF7	ED48	C2	94	4B	9D	D3	01	BC	E9	0F	6D1F	CB27	6553	1064
F25B	2006	B8E5	A5D7	89	B8	F4	DF	50	35	F9	83	5A	0620	8767	87E6	7566
479B	ACBD	9A31	E345	75	54	D6	58	E7	D5	1B	32	42	5E5F	3364	8ECC	7923
5F51	F084	8B37	FA77	E0	42	4A	E6	49	A9	E5	59	1B	A209	B4F9	15EA	3530
092D	4254	1305	C6F5	23	06	42	FF	B2	38	CF	B9	E2	42B4	79C3	AE11	4ED3
8584	6953	6FF0	EF8D	19	AE	A6	78	D6	F7	DA	3C	A4	0FF8	CCB9	495D	104A
D7B9	1679	FFD7	CB2D	7B	27	41	D3	31	D2	A6	B2	E3	7BE8	E927	5F97	BC22
162F	1B46	5EEF	1495	3D	83	01	25	59	6C	10	DE	5C	ABF5	8405	AF57	48A4
7B0B	0CE6	04D5	0CCD	59	63	DF	30	CD	15	94	67	53	4E0E	ACED	0A2A	0DA1
60C3	54EE	9336	A557	7B	55	90	1D	32	D9	EB	E4	58	3535	DFFD	FB44	D47E
EAF3	E9AC	D5FC	E2BB	69	BE	34	E3	68	C8	A2	0F	E0	F6AD	4B81	90B1	8431
4C60	CED2	3A43	39B0	5D	6B	C1	D2	BC	BC	74	39	8F	9F6D	6830	3D80	47C3
3EF7	B9AC	11AC	74F5	24	3D	B1	3B	21	BC	66	62	55	27A3	1429	5166	8F31
DB67	AD33	EC44	D997	6F	B4	34	B1	52	EB	9E	CB	37	C51A	B541	918B	E2BF
0C64	9C77	2CDD	C2CC	A6	92	E4	65	EB	65	2D	AD	4E	D3AD	7718	A4F0	1F32
6D66	9472	418C	1162	4C	AF	40	74	FF	9C	81	1F	8B	5426	EB06	2BD9	E118
E6B7	A935	2989	22BA	96	08	40	5C	A0	5A	3D	03	2B	C843	2A7B	612C	FA64
01B1	A4F1	5FDE	0441	C6	70	81	6D	DD	76	8F	2B	F6	7076	E342	10C5	554C
6814	62D5	21C9	33A0	D9	72	66	35	44	58	41	69	08	4F40	69B5	BFFE	7F55
ED94	4C0A	AE58	FB00	DD	55	75	44	22	7F	55	1C	DE	43B8	4B5F	B337	6E7F
CF64	A24F	B7D4	0455	84	54	EF	61	8C	22	FB	3C	90	F029	A758	60D9	AFFD
FDA7	3046	E925	C9AC	A8	D9	F6	C5	59	E3	9B	51	7B	7A6F	7051	638D	6259
C526	F645	8324	D33D	3D	E4	42	B1	C0	54	85	EF	4B	E762	C07A	5C2E	6FDC
A7A7	5307	E871	0CB0	E4	ED	44	AC	0A	D5	F3	8D	37	1657	583D	E442	A071
4E1A	64B7	28A2	BA0F	CD	27	63	C5	D8	1D	6C	74	22	9064	F8B1	BAC2	A000
4BF0	6843	A329	AF2C	BE	5B	65	D8	98	06	7A	95	D1	D487	2F75	B98F	00A9
AAAF	11CA	3F11	4594	B2	63	2E	6A	49	B6	DF	D6	CC	D4D7	C052	B112	5CAB
5049	F9F6	998D	B5C2	22	A5	6F	EF	2B	49	9B	18	0E	70CD	B753	7742	2C4C
62D0	4C36	A221	BEB7	87	C5	CE	08	C7	F7	2D	83	32	7FE8	A066	FAF3	7824
9179	8B90	D40A	8A21	E3	23	17	3A	3E	69	A2	FF	4F	4BEB	F5FF	5FD3	5BF9
F92D	CF75	F9A6	5EC9	01	22	CB	FF	BD	1A	87	CF	67	192A	BFDE	AD64	490A
50B7	11DB	239D	77B4	D2	AC	5C	47	81	5E	96	98	83	E9D7	1FBD	F03C	4E42

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

73D9	01A3	4C50	DB49	C6	6C	F4	A9	CC	13	C8	B8	DA	4750	49D2	3962	9F69
6704	B900	6B06	6EA8	7B	BB	0D	C9	A4	1C	92	49	26	1384	06C3	C4CF	EE00
E4D1	EEE7	2ED7	CBC9	30	20	C6	C6	F1	34	61	AE	9A	82EA	35B7	A725	7561
76D2	A1DE	4BFD	60A2	18	7C	1A	13	9E	B3	87	EC	2B	A082	31EA	B948	BEEE
E943	1EA6	3C53	283C	C3	FF	FB	2F	86	BE	28	55	6E	C5B2	50C7	082F	8A10
4771	16B9	372A	DD30	6A	6E	13	DE	B1	91	A8	13	C6	F9CA	193B	8D9D	F01A
3272	9AE9	659D	B811	1F	FE	4C	5F	86	33	6A	72	01	7A0F	08E5	E82B	B43A
1E12	3627	AF80	2D05	91	58	EC	A8	30	C9	F9	47	B7	CCC4	92FB	4EA6	EE25
C601	D8B1	A2F8	87A6	92	69	18	CA	C6	AE	B9	08	A6	82E2	0CFA	4ACD	53DF
6F6D	7186	FBD4	B158	42	B7	44	E8	1A	6C	A4	8B	C4	78EE	CA3D	3ACD	95A9
1EF5	373C	1072	2F80	6B	E3	FF	24	BF	89	9C	0A	CB	D12C	C42D	5A39	C72A
F1BC	A7BF	A5ED	0311	E2	0B	68	41	1B	92	DA	C6	78	DC34	9CE2	AFFA	3DBA
D2ED	F5BF	003D	F781	F9	E0	20	52	D9	01	98	82	C6	CE32	5DD0	EC55	9166
FEE9	79AA	7598	D6D3	25	98	F2	BD	54	C0	39	0A	4C	BE3C	69D2	43BA	6726
4AB2	7588	9DA1	86E9	DD	4F	79	91	0A	DD	F8	57	A2	A639	AA41	94EC	07A0
DCEF	5025	C4A4	63F3	72	E8	5D	7C	7E	A0	E7	E1	3F	F42D	4C09	A0FC	FEEF
820F	32F2	77BA	296A	86	36	A5	6B	49	BD	C0	DC	1F	6E04	F153	28D3	ECAE
A386	CCFC	22AF	0ED9	CE	ED	1E	54	27	BD	ED	32	6C	D51E	212E	DD55	FAC1
34D0	2D26	CCF2	1857	BD	17	D4	F3	B8	1A	12	05	96	9531	A796	CE56	24D5
7197	6B11	F310	C6D8	47	BF	AE	10	51	D4	E8	7D	59	4EAF	8E49	56B5	2BD5
A5E3	7EB5	34A5	06A6	91	E6	B7	F5	6F	98	3E	A5	21	D24A	2C51	025A	6E98
DDAB	1819	C6FC	DB88	18	F2	B4	3D	B3	3A	9E	95	B3	5ED1	2FF1	4DAC	07B0
E7EE	9A06	F080	E147	6A	E9	58	66	E5	FD	B2	4E	79	17E0	F691	0A94	E126
6243	90C4	D55D	2240	8B	24	E0	AE	5E	DC	AF	00	61	15D5	B644	9763	83F0
681B	A496	4320	C501	57	53	54	99	70	4E	8A	A0	E8	24E3	91A0	D03C	5AB6
6517	5B99	69DD	C7AB	0C	27	44	5B	DA	F4	37	C6	67	95F4	3184	70A6	5C60
7920	A1F0	EF7E	50D3	C9	8F	E6	5A	55	C5	3D	18	C9	3E20	CB1D	E722	8F5D
F57A	C549	08D9	36AB	6C	93	E7	52	9E	1E	91	B9	D9	253D	CAB4	6784	CA08
7E16	97B4	3244	8F3B	F8	4E	3D	94	17	AC	45	4B	49	A223	9821	5E54	EB52
774C	8BE7	95A3	8121	73	E6	84	47	F7	0A	BC	DB	F5	786C	2E0B	37C1	15CB
D8DF	C57B	C917	E19D	ED	20	97	C3	3E	59	7C	4F	F1	EFCC	4667	FCFB	F198
77C9	D086	8794	F36A	8E	D8	2B	C6	A3	60	D1	5B	F4	0D2A	DE3C	20CB	CF5F
A729	C192	1C5A	6AC1	93	77	F6	30	29	07	17	08	EF	1887	BAD0	8C6F	B55C
E8D7	9A1F	DA7C	BEC8	40	BB	F4	EC	8F	49	EE	E2	BA	5DA1	D5BB	34A6	20E2
F52F	87A1	000B	7493	B0	DA	ED	B5	BE	05	D4	C0	03	50DD	D759	6DE1	9833
245F	CF56	99DB	C04D	87	66	64	32	A2	42	35	BE	7B	2613	15FF	1866	997E
1A90	21FF	EC49	4339	6D	30	A4	CC	58	A9	0A	46	88	4A9A	60BD	F227	D07C
1187	B7CB	1FC1	136C	9C	EE	66	8E	D6	5A	3F	E2	5F	E230	DED6	8384	0E1A
32F5	F394	BE69	D74B	83	A9	06	58	73	90	2E	6E	D5	5ED1	A620	0C9A	BCF1
4B75	2FAE	F0FD	A708	1F	00	18	56	2A	60	1B	7A	48	CC88	81CC	CD83	5EAF
CECD	90C3	F818	95B5	4F	F3	7F	C3	A6	06	FA	4A	3C	C0A3	DB68	8DD2	380B
CBDB	A6AA	C9AC	B5AD	4D	87	FB	D1	71	84	5F	FB	F0	B935	11C5	A8BC	F0FA
FBAC	1E70	02BA	C683	2A	34	B9	09	FE	B7	33	21	EB	3CCB	8335	4314	04C0
9218	CE29	F1AC	1B84	0C	7E	F8	D3	86	05	55	70	BC	D98E	65FD	9429	6A8C
61AE	DA39	93C7	C818	83	E3	4B	B3	55	80	E9	86	32	CFB5	7189	F074	ECEE
15DE	9220	7691	BBD3	49	54	4C	76	98	2F	C1	72	CD	5D10	B9EA	4F6B	47BF
E941	89C1	DF86	A1CC	09	F0	9F	49	D6	3C	80	DA	30	6820	F35F	9912	7831
84B2	F3AD	D72D	B412	9D	42	ED	5B	2F	8F	B8	14	3D	BCC1	B3A9	EB4F	F2FF
BFA6	C443	06B1	C5FA	CE	AF	28	46	96	DB	4E	55	AA	584B	FA58	57C0	8AA0
1D74	EDDE	9B43	61EF	F4	6D	7A	94	0A	E9	BC	C8	88	D317	F40C	C5DB	7C42
45B9	57AB	D73D	CA1C	63	62	D3	0E	36	70	BF	62	A8	6B26	BA48	CABB	13F1
A744	45A7	9E6F	34C0	68	55	6C	A2	8A	E3	99	A2	E5	8056	564F	9EA0	9A18
0A81	32BD	DC85	55FD	D5	66	60	DB	92	F9	5C	E9	06	0E49	5CBA	B772	167A

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

8F08	610D	CE93	1B6A	D2	3C	FB	A2	39	22	12	F0	21	40AD	5DA1	22B7	75AE
06DB	AFEA	D06C	2BA3	41	15	BC	57	57	8F	AC	7C	1C	5D72	051A	3CF9	0C8E
AAEE	58BD	592F	E20F	24	69	6C	99	68	23	F9	BC	B2	9A65	1903	1DBD	7856
F368	EADE	02D1	BF05	B7	E3	C5	22	BA	3F	D7	D0	F7	F855	C049	7595	7610
1A8D	7622	8C06	CEE3	F4	D1	FF	09	77	4D	FC	59	F0	373A	861A	6639	05AF
6623	45B9	4C0F	54FB	CF	3F	72	B0	E9	A3	44	52	CA	FAA9	1031	93CC	F559
03E7	59D4	BB26	833D	BA	9C	D8	20	D3	93	96	FC	20	30A2	F81C	A430	7D3A
F086	A848	FD2F	7BC8	D0	4D	75	31	09	64	22	62	03	978B	296A	D650	B3B8
8FF8	579B	53D7	A170	03	A8	97	FD	6A	D6	4E	55	90	466C	3E10	393D	5E8A
EAB7	A271	B841	05CB	21	BF	AF	8F	B8	DF	9C	97	2F	7A89	DE78	02E5	C058
D39E	53FD	571B	1A34	93	B5	83	F2	A7	90	75	FC	F4	BFF4	C977	DDDD	3ECE
EB28	2AAA	653F	C37B	D4	CA	EE	F9	47	62	8E	CF	2A	500A	826F	BE5C	64A7
E22B	0DB8	230E	243E	B5	37	7C	E6	32	90	17	96	B3	AA49	8A29	356C	E7B2
F795	2CC0	ACFF	227E	5C	82	8A	80	99	8C	35	79	86	06D8	5BA3	C703	A074
2C9B	EC6B	9BB3	43A7	60	22	A6	84	DB	E7	7E	5C	44	FF60	4E08	0A5A	6BAB
053D	A38F	A6AF	2105	81	49	58	B1	F3	2B	F8	DB	F6	0764	FB07	E597	7E86
722C	1631	0C26	5F11	35	62	E1	2F	7B	C4	49	1D	40	5F00	33DA	5B68	FE17
7B46	462B	46EA	C765	F2	CB	F7	B5	99	AE	EA	EB	00	3F1E	DE60	3E5B	E768
CBB7	1386	ED46	E172	C7	3B	4D	F0	3B	66	D3	92	93	1612	06C0	1329	EF66
6552	2422	DE1E	8173	C1	60	DF	EB	6D	2D	1A	1D	42	3E23	1ED4	7232	9F14
23E9	D830	59F9	7F64	C1	DD	EA	E5	0A	37	3C	B0	BD	152E	356E	54F5	79C9
C41A	4449	A50B	A80D	8B	E8	75	3D	62	97	10	31	8A	BAB8	105B	3681	CF63
8FFE	D13A	549F	71E0	14	BB	56	5E	89	9D	9C	78	65	3F88	7A74	0D40	E9A4
C26D	3C78	84B2	7227	34	CD	F9	BF	E2	76	D1	A6	A0	6F67	D70D	39E2	FBAB
5B7B	DDF2	7DC2	3B97	5E	D1	97	F3	6C	44	6B	D4	D8	9C66	C40D	282C	060E
1DAB	0220	4662	3B45	E0	19	30	4A	83	80	D0	78	7C	610B	8A5F	EBD1	82E5
F032	5C6A	138F	F837	EE	23	8B	A0	03	29	51	25	83	38C9	661C	FC54	FBE6
6C31	2918	4630	AEB4	F1	0F	06	BB	08	48	86	2A	3F	636B	E5C6	25C3	BBA5
C332	EA9F	91DB	4AEE	D9	80	17	C4	E9	26	97	14	56	93CA	95B9	8D0C	F0AB
FABD	EA96	8035	CA01	30	08	6E	13	8E	A7	13	7E	73	3D4F	8877	B624	AF70
84BE	8135	DB44	6FBC	CC	75	55	79	8A	04	17	6C	47	DF15	A160	3769	EBF1
1C9A	E68C	4699	8525	6A	D1	64	44	5A	51	3C	DA	2A	9BB8	7FA9	D66C	CC61
E907	4BE9	21D0	F90A	A6	31	24	B0	5B	25	FC	4B	07	5700	45C6	93CB	25F0
1244	B0DC	7A92	8B00	79	5B	BC	B5	C3	00	E9	9D	EB	2F47	C9A2	3AE8	F37C
C5B0	3D35	7559	2C0E	21	2D	8B	E9	56	6A	0F	83	2B	F91B	615D	5A97	5809
6A42	2E6D	DDAA	9DF6	20	98	0E	C9	34	EF	73	3A	2E	F4D0	AC87	7287	6B1E
5D2F	BC45	6D93	60C4	96	02	CD	BA	EC	59	BB	73	85	B4F8	9BD4	EF59	02F2
9689	46A6	9398	F706	5F	FA	EF	AF	B1	A4	9C	F8	B5	6E2B	5191	5B2E	7AAE
63CB	6F02	0C19	32DB	99	BF	38	E0	67	2A	1E	B5	76	43A2	F658	175B	3354
82AC	F5F9	6E5C	95DF	70	82	DE	2A	74	0E	CE	BF	D3	D663	77A7	18D2	4A11
6B42	2D6E	27F7	4C63	30	AD	A1	53	4D	26	59	E7	1B	2C06	845B	20E3	1D5C
29A9	C7CD	A6C1	60F9	9D	8A	C3	E7	31	6C	EE	CB	22	DD48	2B55	749E	3B1C
ED82	0322	9BD4	6CD6	72	21	46	55	2B	78	8D	A6	7D	29DE	562D	12BD	8A8D
5733	CF8A	1F7C	93F7	72	A4	46	54	62	BD	8A	59	73	91EF	FC7D	6760	4681
1E38	6A0C	F9B4	0D1A	B3	10	CE	1A	5D	18	E5	7C	4E	4D8C	9310	4472	E995
9B08	593B	688C	B8A5	4B	3C	0E	AF	D0	00	F6	00	5A	B6D6	E32C	69BC	0FEC
09BA	6E35	1B08	1DEF	64	10	51	54	0E	FB	1C	5D	4B	1637	23A8	B7C9	CC23
C1B7	AF40	4AB7	F083	85	71	95	B2	E2	0C	C8	77	7C	1FEB	7D02	E8D5	E1A0
7716	24B2	5E9F	649F	D1	A1	FA	08	B8	0A	69	FD	2A	59FC	3FEE	E8E7	A240
6B71	7D5D	B747	3B4C	4A	E3	2B	B6	D6	1B	DD	92	4F	E876	2A7F	7708	F1DB
8C20	DA12	16FE	D288	0F	31	AD	21	4F	CF	A4	20	52	F67E	0C72	8BB3	9D2A
CEC3	C32F	2611	44F7	EF	24	31	CE	3C	E7	03	BF	B0	BDFE	C34A	F2A1	E50D
B678	E873	FA3C	CCAC	67	C5	27	42	56	5E	B2	DF	52	EA43	5985	E203	EF55

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

9951	867A	6CE1	CD37	2D	D4	59	1F	F6	B1	4F	0E	A7	2A3E	AC6A	5F1E	335F
09E7	3072	7F4C	BC23	15	5B	C6	9A	C6	8C	0B	7F	82	B505	31CE	ADEF	7450
C555	4F48	BBD1	400F	D5	38	D1	DA	67	5F	AF	E9	69	B7A9	C189	39B8	D7A2
471F	0A32	A65A	4A5B	2F	DC	A9	E4	BF	51	1F	36	5D	C27E	8284	2F32	82D1
D944	1FB3	7CA5	0D5B	79	77	FF	31	BC	1E	DD	3C	4C	03D6	ABC9	71A3	262C
CFE7	EA8E	2639	D237	C4	29	F8	C1	8F	92	EE	46	93	566B	4146	9388	61B0
5D05	6B24	39BD	A210	99	3E	82	FB	00	BF	31	3F	5A	C155	768E	105B	003B
9F45	AD3F	9B15	C7C9	CD	58	05	D5	51	E0	EE	B8	59	B270	DE04	54B4	8B84
EDC6	1E6B	A274	2271	B1	26	AB	D0	29	EF	45	73	C8	EB1B	5045	109A	1404
67D2	8391	AE01	F66D	AB	05	03	5C	0E	37	87	19	ED	519D	98BF	9C37	5BA2
10EE	CEC8	B3B8	9455	76	4B	31	53	9C	D5	65	35	09	7894	BFAB	EAAD	BAD2

Provera $H_i=AP_i$, $i=\overline{1,25}$ pokazuje da je H_i dobra matrica provere

Hemingovog (200,192) koda:

H(1)

5555	5555	5555	5555	55	55	55	55	55	55	55	55	55	5555	5555	5555	5555
6666	6666	6666	6666	66	66	66	66	66	66	66	66	66	6666	6666	6666	6666
8787	8787	8787	8787	87	87	87	87	87	87	87	87	87	8787	8787	8787	8787
08F7	08F7	08F7	08F7	08	F7	08	F7	08	F7	08	F7	08	F708	F708	F708	F708
0008	FFF7	0008	FFF7	00	08	FF	F7	00	08	FF	F7	00	08FF	F700	08FF	F700
0000	0008	FFFF	FFF7	00	00	00	08	FF	FF	FF	F7	00	0000	08FF	FFFF	F700
0000	0000	0000	0008	FF	FF	FF	FF	FF	FF	FF	F7	00	0000	0000	0000	08FF
0000	0000	0000	0000	00	00	00	00	00	00	00	08	FF	FFFF	FFFF	FFFF	FFFF

H(2)

7E13	789D	DAC3	E9A7	06	E6	61	20	E4	4F	CF	66	CA	4E63	F036	F664	2051
59B3	FEBC	4560	7E61	B8	BA	32	5D	9A	1E	6B	02	C8	88FC	4EA1	DEC7	89C0
C80F	C663	696D	2CE7	45	C1	FB	B9	06	9E	A4	34	94	2F4D	7473	6DCE	1D10
7CC4	4ACB	5053	F4DF	16	52	DA	4B	50	47	67	F5	3C	8134	C798	493C	D1C8
1891	D14F	8C74	A5AB	64	CE	F7	01	73	FB	0A	CB	9D	2290	18CF	2BA1	85C9
FB23	88D0	CF06	CCED	14	CB	8A	E5	23	E2	0E	1A	72	8794	C51A	86A2	CCBF
C068	2425	2802	E101	8E	98	8E	48	A5	09	17	86	4E	6815	00A1	6C91	7E1C
210C	BB70	D2F1	0C70	C1	42	60	B0	18	C6	80	58	00	D2A1	1B3C	1352	03C2

H(3)

3885	ABED	8AC5	8479	42	FB	65	C4	E6	D3	A1	D7	45	7456	5D93	C834	A572
9D16	9C34	B99B	CDDF	C1	A6	64	B4	D9	B7	0A	00	5D	9554	2B63	D887	DB09
CA57	C944	0B78	8BB7	41	88	AC	79	ED	61	BB	92	86	1A79	95BB	33B5	31CC
4785	22C2	9D47	B3BD	0F	5C	DE	E0	F1	D1	99	34	7A	0FA4	E3A7	08C1	9826
5835	72D3	BA02	DF12	2C	D2	E0	3F	11	51	F7	42	71	515F	92B6	4681	E63C
B180	EE63	707C	D8D0	63	89	B6	34	64	99	FB	E1	82	4D3C	A21D	CE8B	E861
46C2	3DC3	0028	AC44	19	A1	51	C0	EB	9A	64	8E	14	9981	A4C2	6205	4018
805F	C21C	20C0	0239	36	66	A3	3E	14	04	09	01	40	C2E0	163D	996C	9C03

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

H(4)

81E4	D66A	A1E8	9C2B	92	1F	52	74	C6	1F	0A	F1	A0	5455	FCBA	B9CC	6DCE
FB42	672B	9036	C985	6D	08	FE	2B	58	47	D1	B3	CF	1855	F8EE	8E89	8568
E119	680D	3AFC	0DBA	AA	A6	73	A1	76	1A	C7	25	ED	65B1	50E5	4A7C	31E3
0210	7566	428A	89D4	A6	BC	62	67	A7	23	3D	43	EF	B0FA	439D	95CB	E29A
9888	FC85	43CD	A711	9E	03	0E	EE	24	82	06	12	CC	1F4F	E17D	1F17	8D7B
A097	0FEC	B480	0557	E9	0B	0F	8F	42	AB	89	FB	7A	338A	C6D9	780F	2862
3787	8204	2201	14E4	86	C4	50	AD	99	51	60	64	50	0689	C8CE	8B21	241D
0000	011B	D170	F12B	01	78	15	52	1F	A6	1D	0D	85	3916	0C01	1454	1B62

H(5)

49A1	C35B	FE8D	0884	9A	BD	99	9F	2B	9B	61	F4	2C	73D8	9392	833E	E01E
4447	7CF5	4E96	EF0E	3F	CA	6C	65	09	98	64	E4	27	AE28	A81E	E712	D5A6
F814	4F2A	0E21	75B1	2D	AF	7E	75	75	BF	46	0E	AC	C160	CA79	26AB	A09C
521B	EE88	4DCB	0D2F	AE	D5	B5	56	26	34	FD	2F	29	C208	5DA5	CA00	7271
FEB2	1E03	E5D0	43AE	DB	8C	F0	7A	96	98	0E	C7	51	4B7D	25D1	458A	1016
2E60	98AA	2ECA	5978	23	16	54	06	B3	B3	84	7F	43	70DE	2933	73B1	E366
E40A	C218	BD77	C501	42	64	82	62	05	8A	81	D8	45	0640	8809	B05D	4989
198D	31E0	120C	92C4	95	89	37	15	50	45	0C	27	32	209C	8168	4C40	360E

H(6)

0AB3	2B62	1C98	8A0F	FE	C3	1A	2A	A1	BF	8F	C1	00	ED06	A77B	BEC9	D07E
8C50	6BB8	D959	02F2	E6	88	DA	9D	3B	C6	BE	0C	55	F25B	382F	6CA7	E40C
E22F	3A0B	9B46	7AB2	F9	BE	1B	D7	85	42	90	4F	08	8FAB	A852	D0ED	54C9
7B83	BD95	D10C	C225	84	40	DF	FB	BD	8A	C8	BE	60	4DD5	47E8	D546	2409
5CD6	86AF	3CCB	4E14	B1	C1	63	B6	9A	EE	1F	4A	ED	C425	00E0	A005	3DE9
9CD7	8EBA	7B54	5648	39	59	15	87	F7	08	4B	A5	92	09C0	062E	06AC	E6EF
4D22	0586	10A8	B134	29	69	E2	C5	61	10	A2	60	8C	AACB	3414	BB00	4015
0299	BA48	E535	4ACB	86	32	00	00	8A	C4	48	9B	20	103C	3052	0D35	23F0

H(7)

7621	D102	1FC5	AAAB	5B	A5	61	A9	AC	D8	97	65	A9	94DA	0365	35FE	5D86
C0E6	D79A	0137	1901	85	A1	96	DD	91	4C	C5	BD	BE	8693	EB0D	C393	6CF7
E7D6	C113	668D	90F4	99	81	31	11	FF	12	4D	32	06	DD3D	A2D3	F39C	B64B
C459	B466	4668	D681	96	F3	22	F5	99	C4	AB	D3	1C	4A6B	04B0	3EB7	E42E
49C6	9FB4	8270	728A	DB	2B	24	58	2F	92	B5	85	76	DFF2	1CFE	1012	87C0
8F85	E961	4C56	98B8	3B	C5	48	5D	44	45	FD	29	9C	53E1	3D0C	14A2	F379
9ADA	A300	EFE5	4C43	38	00	83	32	50	A0	70	00	09	072A	42CE	C492	08B2
3504	405A	0003	0670	43	3B	7D	05	21	2A	82	96	94	3095	5C11	9065	CD0D

H(8)

C2CE	C824	5EB1	CDC1	7C	49	73	27	75	10	00	EA	51	B79C	2FAD	73D7	B10F
CC63	5CA9	4BAC	15D0	F4	99	D6	B3	27	61	8C	93	63	DC42	F818	B72D	1FD2
D67C	FD41	1078	2C73	8D	42	F8	53	47	9F	07	5E	FA	15FD	B098	8F88	9A0A
EC72	0567	9A73	910B	87	0D	09	AE	0A	32	E1	41	E1	1D55	21B0	EEE7	E6FB
C99C	1701	4FF1	775D	26	1F	14	44	4F	69	35	EC	56	CC6F	1310	19C1	22BD
F614	C650	A01F	4DC9	A3	15	8E	E3	06	D5	99	1C	76	A971	7F22	7217	149D
8325	5E68	B64C	9068	68	62	40	32	98	D2	C3	80	20	4628	1B10	01B3	698A
741A	A919	0980	6415	5D	B5	23	9C	03	20	0A	3F	86	3A14	A0E1	B000	5021

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

H(9)

40B1 628B 566C 8F88 6A 5B 58 2F DA E9 9B 9E 84 F6AD 8C28 6BCD A4C7
FC8F A565 5752 18A4 B3 82 78 9D C9 55 D8 C3 16 0C68 8E37 E178 F1F6
FA61 782E 0E50 3D03 87 2D EC 5C 32 B8 4E E9 4A F88E 0F83 699F 98BE
9F2E 92B5 8545 0ECC FB 03 92 4A B2 54 B6 38 08 6439 3BCD EDE3 169C
0B93 AE81 A672 E949 85 88 BC A8 74 D7 79 50 09 77A7 9AB5 88B3 8764
6864 49E6 B688 1315 72 DD BE 21 DC 36 FD 58 22 2691 8BD8 E02B 5B4E
8551 028E 041E 3D92 11 81 04 44 89 93 5D 00 DC 0930 640E 3E27 62C2
322A 3508 58C1 C22F 8A 1A 49 04 06 6C A0 41 90 6E0F B2F0 1018 380D

H(10)

62CC F535 E945 B4BB 6B 47 FB B6 A8 BA D7 5F 20 0C4F 3E15 8200 34E0
E257 A755 30A9 C0D4 E2 2B 45 A6 A9 7A C9 F4 B8 7331 77E3 5866 486B
DBCB 1AB5 E84C 92C9 17 14 84 D7 D7 25 C5 43 2D BFA9 9BA4 0CE6 6263
1146 F136 1D76 40AC 5F C2 38 24 F9 6C 1E 84 06 A823 CEBE 30FE AA7F
D666 F625 8900 44FD A1 D3 E6 0E 17 65 DC BF 57 62EC 8448 581D 03A5
A674 8225 DE2C 4E31 34 F4 89 C3 BF D8 14 F4 04 4E72 1BB2 E38C C3E6
6148 90A1 069B A392 86 F4 F0 30 80 4C 28 42 EC 32E4 4C3B 4E20 2100
802F 6CDE B007 D126 71 00 04 C2 5C 31 46 28 82 141A A044 A10F 50CA

H(11)

A062 A280 572A 7633 37 5B C1 49 C4 FC F5 76 A0 AFE0 EC00 4B2F 7DFB
ABC0 5B36 1F15 65E7 89 A3 6E 5F 41 21 6D 1B 91 37C0 4F35 D0BB A943
CAFD F8C4 2B27 28AA DE 22 9E 2D EE C4 80 2E DA FDE0 0DD8 E35E 200E
D10E 4493 3D51 2943 FF 45 19 6D DC 2A 18 DC 34 8827 FBB8 B18A A93B
100E 1812 8D06 F195 FE 9A BD CB 10 E1 CD AC EE 3AFE 864C B04A 5355
F3FA B3AA 6BC5 039B 0D 8E A2 38 84 28 CA 2C FC 6B1B 607C 2009 CBF2
6A48 C888 C86C 4906 10 41 79 10 62 A2 80 87 C3 4492 1032 14BE 5C79
1C10 3666 33A0 3461 67 88 86 C6 17 42 41 4B 38 2049 2A8A 8B60 8482

H(12)

D454 EEAC 3EA1 C095 62 32 86 23 4A 83 C1 D3 79 EF56 8CD4 6CF8 DD37
8014 51FB D8A7 D755 39 7E 0A 04 F9 6C DB 42 40 D103 6778 DE5A ADDE
6E01 A56C 4A74 2F5C 0D 9F 8A 99 0E F4 E3 E4 F8 F344 49B9 198B 9FA1
66A8 9DCC 14C6 316C 78 00 F7 C0 F9 73 EA D5 FF 5139 0449 6C31 18FC
A7D2 6D14 21F7 1292 3D D7 58 C5 09 61 78 7B 7F 8E06 61CD 0E34 8A51
1056 B4AA 1579 0B4D 75 4C 51 D0 8D 60 1A 56 19 AFFC AA2B 4477 FF28
868C BA81 0F88 5448 AB 79 A0 4D 14 3E C9 4A 10 B920 D205 01A0 0604
3033 4532 5850 6787 52 02 60 1A 48 C9 14 B0 22 4609 1942 AC8B 90CB

H(13)

E5E3 19E0 A4E8 0723 9B 4E B6 35 0E 51 31 15 B2 EB70 57B2 F1A2 6FDA
A28C 2DB4 401C AF0A F0 92 EF 27 12 38 E3 BC E9 35F6 6A7D 7832 16EB
E3AE A7E7 2370 3217 18 12 8F 53 E8 FF 54 48 53 48F5 1896 F617 B86C
FC32 2231 8C5C 45DF 7A BD 49 87 24 61 86 0D 44 0FA1 5E52 726F DA97
84C6 6674 2391 07D3 C3 F9 84 B9 5D BF 07 3F 08 7A3D 1B68 C855 0B03
D12B B214 E14F 968E 16 47 3B D6 25 16 BB 18 8C 131C 393C C21F 2B73
7010 39D2 1701 D260 3D 9C A0 BB 26 08 D1 40 13 1903 C305 4891 1846
03B8 4CAF A8A8 0CBB 00 00 5A 40 91 B4 08 0D E7 6242 B07A 2364 4101

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

H(14)

5272 FF5C F9FF 520A 82 13 E6 D0 83 C4 E1 AB 2F 298A 9DA4 6370 729C
E4ED 13CD 32B1 E4D9 C6 35 BA E9 F1 52 76 92 B5 0287 6DB0 8547 7988
FB55 D440 1D13 07D6 A5 51 F0 7C 37 81 36 57 21 CD6C BF22 EA4D 8DB8
AB82 A094 0A74 725E CD 9A A8 8D 19 FE 18 5B B1 41BE FECB 21B0 37A2
D304 056E C206 1D09 74 97 8A C6 FF 96 BE 06 14 2F9C 3A37 2A16 76E6
EAAE B0EC 470A 117D 96 15 56 00 93 70 CC 65 71 0C1B C356 F5BD 92EA
A88D 2174 D292 9281 83 68 4E 1A 04 E4 03 82 82 9610 A2A9 B248 2499
0363 CE01 0C8C E84C 04 41 A1 10 EB 1B 21 0C 64 30A4 511E 4DD5 0942

H(15)

130B CACB 231B 8D83 1D B5 8A FE 98 2F 50 71 2A CD1D 9628 BD9F A23E
1437 5A73 3332 CABE E0 79 AB 50 37 98 B3 58 8A F1EB E565 F214 2827
D613 EF68 BCE8 5914 09 B9 6B 68 D2 A3 DB 1E D6 9620 6659 9909 4F7A
AAC2 8BD6 D65A 01AD FC C6 1B 0D CA 98 13 55 FF B530 0167 71AB 40C6
52AE 107B 5494 2597 49 06 66 F3 FA 11 98 6D 9E 6A10 ACC7 FBB8 5131
9663 3638 6159 A516 F2 AE 5D A0 6C AB 06 C9 7F 8BC0 D563 D517 1700
A810 4A3B 3D80 0748 13 18 14 0F A5 F4 D1 41 10 0301 859B 1481 AC65
5C3D A1C0 4A1D E2C5 88 55 00 A0 50 0C 62 8E E3 E06C 2200 4170 2392

H(16)

553F D418 E7BF C19A B7 D8 A4 7E 5D 7A 2F 9C B0 C00C CFC0 00AC 68D1
46DD 2DF1 A850 788E 6A 90 6B F3 C8 A0 2F 4F 11 2B5D AF95 8AAF D982
3337 AA07 F158 483A E9 1F 42 13 94 C2 3D 15 CE FCE7 E244 51DB CD53
9B78 CABE 856E CC68 24 8C 88 E0 2A 1D AC 07 C3 BD2B 7D36 0EBA F0C1
C3C6 4A57 B589 2429 9D 5C C1 E3 C8 29 8F E8 3D 5901 7645 7628 753D
5C66 2C75 FBA5 4C05 17 AE DD 43 31 F9 3A 44 42 39C6 E10A BC22 5CD8
2D40 0230 2E33 5308 64 89 51 14 8A E7 59 9B 03 F208 3085 6014 0C56
E2A8 45C5 C108 9B77 51 02 AE 3A 42 12 04 24 A8 0C42 834A 17A4 9300

H(17)

BE23 EB09 90B2 536E 2A E1 B8 EB AE E1 9E 1D E5 CE86 1E89 3040 CE73
A345 0DF8 E0BA 7D26 29 BA EA 8D 68 0A 69 AD 38 F303 C487 D928 F7AB
D52C EDA1 D7A7 6E37 5A AF 9A E5 1F 20 30 92 10 0DB4 45F4 CCE6 5D22
FF78 22B6 3EE0 B31E 60 48 90 D5 38 1A E6 C7 9A AD6E C8AA 6543 A413
169A 723D C62B 6D07 6D 28 35 73 09 A1 42 49 35 709B 69BA 6D69 AB38
FFF4 D52B F727 05C8 81 68 F8 9F 1C 23 5A 25 46 9374 3D2A 4005 338C
844A 850A C434 82A2 19 D3 01 0E 20 74 47 BD 08 20AF 7315 4AC3 0012
3B25 52B0 2818 4C34 A6 27 A2 50 5D D0 81 40 74 0A50 8C20 0694 6CC9

H(18)

4480 5B7A E87C 74BA 79 1D 10 F2 91 F3 D8 94 54 16E7 C77C BC3F 8D01
82C7 FDDE 4248 3569 B2 79 B4 40 4B 9D 31 3A C4 FFFC 13CE 1089 EE0E
33E1 C978 F107 6D58 DF 29 35 24 0D 2A F3 B8 71 B821 78AD 8ECE 157C
2B93 ED18 93E4 17DE 00 D9 0F A6 FE 55 82 60 1D CBAB 36B0 8D61 8DC2
FBA2 873F 046A 1B13 83 2F 68 00 93 25 D8 72 DF F5C5 6099 7963 3145
AFFD 924F F27B 1FCF 63 8E 30 34 46 51 74 41 72 6B37 6108 A0A4 0B12
9D89 A5C2 1242 A016 E8 10 06 C8 81 CA 03 02 72 2360 C8A6 E393 06C1
6246 5000 6434 3EA1 0E AF 09 69 6E 28 D4 A4 85 1C0C 8612 0208 5998

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

H(19)

1A49 D875 F443 612A 9A 4E 02 A1 A5 91 1C 67 D9 0D8D 739F 2F35 F6ED
B4C0 C5B3 4EBF C24B 02 53 C7 E6 72 39 0E 9A DA A966 E5CA 060F ED89
6AB8 E16C 852D E22F FE 86 DA E4 6D 19 27 B2 04 D4D0 A5A5 EBA6 8B1C
27E6 6D2A 50CC A0A8 AC EE 6E 16 7A D5 98 6D 08 ADA9 4D67 82C6 86B3
51E7 0CE3 8187 BC9A F4 9B 96 6C FC A2 3A 81 02 8D84 B2DC 6EC8 0E6B
DB91 0F89 807A 5D88 84 46 A1 E4 BF 91 A7 58 EA EA08 78E5 60DE 5735
4088 E095 28B8 0AE6 12 BC 32 72 65 0A 45 CC 89 1700 1646 1484 3033
050A 970A 2446 515C ED 60 C1 04 80 BC 08 11 14 68C7 2811 FB08 E88C

H(20)

D4F3 1680 615E E89E 3E 8B 03 CB CD 0E 06 7D A6 4B39 7BD2 8726 3C71
F562 4578 FA18 8AAA FB 02 8F 39 14 F2 F6 AD 35 0562 51CD EAB6 4327
D3A3 3D7B 5C4D 7A40 9D 82 39 DE 11 C4 9B 01 6F 2D55 B678 3E43 A463
B238 88E5 C7AC E0F3 A5 70 8E 89 00 96 F5 4A 63 748B 5572 0B33 BDF2
F0D0 DAB1 8AC1 F778 64 7B E0 A0 E6 C0 B6 29 F0 7D04 9388 7EA7 3C09
7FFD 2080 DBC4 3305 E8 28 13 D1 64 88 43 75 DF 3436 5313 782B CDAE
2316 6042 616E 0049 B6 91 00 C3 16 EF A6 00 84 DAE6 9024 6351 4009
5860 1B32 84B3 5E84 53 4C 97 32 30 21 48 8E 63 0111 2BC3 0800 9C90

H(21)

4396 161C B5F5 D129 CD DE EE 55 A7 62 41 53 5E 37B2 A1E4 28A4 3DE0
A87A A479 9E71 870E 46 6E 72 2E 7F 51 D4 A1 A8 4B96 2197 7F04 D971
0456 3B7E AF26 FCB6 D2 7E 10 41 B5 16 7A 87 C6 9991 A25B 8CDC 42B3
3C8C 9299 2F83 31CA EF 3C A8 49 7A DC ED D0 50 8172 5F7C CC03 D123
4A8E 1F38 5F64 77DC 0C 27 00 58 C2 25 05 05 BB B3A8 EF3E 7F13 461C
C30C 7D58 1A92 2DCA 70 D1 E1 45 DE D2 A3 3D 21 3EF4 EA62 CF84 90B4
2E39 5E8A 402C 283E 04 C1 B6 07 81 A9 C0 E0 5C 8992 08B1 86C1 2010
5096 81F2 A648 1321 03 28 56 B2 00 16 37 1A 03 1644 6742 410C 936A

H(22)

2386 79FC 7C09 085D 16 51 C1 72 E5 6E 2D 92 DF 09CB 96E8 E27E 45F2
A1E8 5CEB 77A5 5367 E5 B8 C8 68 C5 FB E2 50 F4 7E31 040A D506 D05E
A45C 78E5 15D1 02F2 5B F9 7B FF 94 41 02 B9 38 8018 F8E7 F07D F30A
8441 B6DE 8CA8 2FC3 B4 EC 96 47 5D 53 47 D5 C1 A6C8 2898 A2EA D2E3
984A 31DD A4FC C591 7B D8 FC 36 E8 8D 7C 54 C6 5A00 6940 5E54 23B3
5697 F805 AB1B D7EE AE 99 DE 12 45 D7 2A D8 A8 9CC2 4581 12B4 0A86
C104 1534 1441 3CF9 2F 86 48 2C 42 38 DA 03 00 D868 15A7 80C3 1481
2098 C04B D3AC C200 80 66 33 D2 38 67 25 50 88 00B6 5A52 6925 0C50

H(23)

A762 7A03 CBB4 68DD 66 5F AF B0 6A DF D5 11 A6 45E1 041E 251A E782
439E 763F F6AB 08BD EA 96 59 E8 46 B2 1D A3 57 2158 31D1 BC09 429D
CAE9 6728 06EC 4CDE A7 1F E1 52 B8 2D 0E 2E 30 B3F1 E23C A3E1 82BD
CCC1 1B9D 0169 A9E9 D6 91 DD AD 6E 54 04 58 B8 3752 7C65 496C 533A
51E4 E101 DB66 09E9 43 26 D4 DC 22 40 F7 A2 28 E63E D81F 9EC0 DD37
94A8 1CCE E0D2 156D C3 AF EE 30 9E 80 96 E2 C3 314D 7836 08B5 97E6
8021 A424 3DC7 809A F4 64 21 A4 81 13 13 04 A6 2B90 0587 8A34 314C
19D8 1B60 4230 0360 33 89 04 08 53 CF A8 75 11 C06A 62F0 7002 E091

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

je u savremenim komunikacionim sistemima, sa brzinama od 400 i 800 Bd, zanemarljivo.

Još nam preostaje da, saglasno statističkim ocenama entropije teleprinterskog jezika, razmotrimo odnos nivo šuma i parametara različitih kodova pogodnih za zaštitno kodiranje.

Pri zaštiti teleprinterskog jezika na veličinu projekcije koja se može potpuno zaštititi značajno utiče redundanca, pa navodimo ocenjene vrednosti tog parametra jezika :

jezik	1 - H(U)
T	0.01708
T_1	0.01954
T_2	0.00327
T_3	0.00022
T_4	0.01623
T_5	0.12137

.

Da bi ove vrednosti mogli koristiti jedan od uslova je da se ostvari particija jezičkog niza koja uklanja memoriju. Za jezik T_i, $i=\overline{1,5}$ tu particiju ostvarujemo već objašnjenim postupkom. U slučaju jezika T može se vršiti particija koja uključuje podelu na kanale (jednostavniji postupak korišćen u primeru 4) ili particija saglasno memoriji jezika T po kodnim petorkama. Zbog složenosti postupka određivanja memorije jezika T u ovom izlaganju nećemo se baviti ocenjivanjem tog parametra. Ipak, prema poznatim jezičkim istraživanjima ([4] , [9]), to je

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

sigurno memorija reda $m \geq 30$ pa su potrebne brojnije particije. Odgovarajuće particije mogu imati oblik kao u sledećem primeru:

PRIMER 5.

$$M=40 \; ; \; m=10 \; ; \; n=Mm=400 \; (\; n \leq 2^m \;) \; ;$$

$$u=(u_1 u_2 \ldots u_{400}) \quad \text{za kod } (400,390) \; ;$$

$$s_1 = (u_1 u_2 u_3 u_4 u_5 \; u_{201} u_{202} u_{203} u_{204} u_{205}) \; ,$$

$$s_2 = (u_6 u_7 u_8 u_9 u_{10} \; u_{206} u_{207} u_{208} u_{209} u_{210}) \; ,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$s_{40}=(u_{196} u_{197} u_{198} u_{199} u_{200} \; u_{396} u_{397} u_{398} u_{399} u_{400}) \; .$$

Koristeći ovaj oblik particije moguće je, polazeći od Hemingovog koda (400,390), formirati dobar (400,400) linearni kod koji daje potpunu zaštitu od prisluškivanja. Za ovu, i bilo koju drugu, particiju obavezan je takav oblik vektora s_i koji uključuje preslikavanje celih kodnih petorki jezika T.

Vrednosti redundance, za neki posmatrani jezik, smatramo konstantnim pa na nivo šuma potrebnog za ispunjenje uslova:

$$h(p) \geq \frac{m}{n} + (1-H(U))$$

promenljivo utiče odnos $\frac{m}{n}$ parametara izabranog koda. Kako je uzeta podelu vektora u na M jednakih delova i kako je tada :

$$M = \frac{n}{m} \quad \text{ili} \quad \frac{m}{n} = \frac{1}{M} \; ,$$

to možemo formirati sledeću tablicu po kanalima teleprinterskog jezika, sa prikazom potrebnog šuma za neke od mogućih vrednosti za M ($M \geq 5$):

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

M	T_1 jezik		T_2 jezik		T_3 jezik	
	$h(p)\geq$	$p\geq$	$h(p)\geq$	$p\geq$	$h(p)\geq$	$p\geq$
5	0.21954	0.03514	0.20327	0.03179	0.20022	0.03117
6	0.18621	0.02838	0.16994	0.02524	0.16689	0.02467
7	0.16240	0.02382	0.14613	0.02084	0.14308	0.02029
8	0.14454	0.02055	0.12827	0.01769	0.12522	0.01717
9	0.13065	0.01810	0.11438	0.01534	0.11133	0.01483
10	0.11954	0.01620	0.10327	0.01351	0.10022	0.01302
11	0.11045	0.01468	0.09418	0.01206	0.09113	0.01159
12	0.10287	0.01345	0.08660	0.01088	0.08355	0.01042
13	0.09646	0.01242	0.08018	0.00991	0.07714	0.00945
14	0.09097	0.01156	0.07470	0.00909	0.07165	0.00864
15	0.08621	0.01082	0.06994	0.00839	0.06689	0.00795
16	0.08204	0.01019	0.06577	0.00779	0.06272	0.00736
17	0.07836	0.00964	0.06209	0.00727	0.05904	0.00684
18	0.07510	0.00915	0.05883	0.05883	0.05578	0.00639
19	0.07217	0.00872	0.05590	0.00641	0.05285	0.00599
20	0.06954	0.00833	0.05327	0.00605	0.05022	0.00564
25	0.05954	0.00691	0.04327	0.00472	0.04022	0.00433

M	T_4 jezik		T_5 jezik	
	h(p)≥	p≥	h(p)≥	p≥
5	0.21623	0.03445	0.32137	0.05848
6	0.18290	0.02773	0.28804	0.05039
7	0.15909	0.02321	0.26423	0.04488
8	0.14123	0.01996	0.24637	0.04089
9	0.12734	0.01753	0.23248	0.03788
10	0.11623	0.01564	0.22137	0.03552
11	0.10714	0.01414	0.21228	0.03363
12	0.09956	0.01292	0.20470	0.03208
13	0.09315	0.01190	0.19829	0.03078
14	0.08766	0.01105	0.19280	0.02968
15	0.08290	0.01032	0.18804	0.02874
16	0.07873	0.00969	0.18387	0.02792
17	0.07505	0.00914	0.18019	0.02721
18	0.07179	0.00866	0.17693	0.02658
19	0.06886	0.00824	0.17400	0.02602
20	0.06623	0.00786	0.17137	0.02551
25	0.05623	0.00645	0.16137	0.02363

Iz tablica je vidljivo da je u slučaju malog šuma potrebno birati kodove brojnije particije.

Što se tiče zaštite teleprinterskog jezika T pogodni oblici particije su, u slučaju particija koje uključuju podelu na teleprinterske kanale, M=5k, k=5,6,7,... . Za najmanju podelu M=25 dobijamo : $h(p) \geq 0.16137$ ili $p \geq 0.02363$, što

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

daje praktičnu upotrebljivost kodovima sa ovom ili brojnijom particijom. U slučaju particije bez podele na teleprinterske kanale ta upotrebljivost je i bolja, što je vidljivo iz sledeće tablice za neke moguće vrednosti particije M :

M	T jezik bez podele na kanale n=10M		T jezik sa podelom na kanale n=mM	
	h(p)≥	p≥	h(p)≥	p≥
30	-	-	0.15470	0.02240
35	■	■	0.14994	0.02153
40	0.04208	0.00457	0.14637	0.02088
45	0.03930	0.00421	0.14359	0.02038
50	0.03708	0.00393	0.14137	0.01999

Broj particija vektora u teorijski možemo neograničeno uvećavati a time $\frac{m}{n} \to 0$, pa se uslov teoreme 4 svodi na :

$$h(p) \geq 1 - H(U) \ , \ \frac{m}{n} \to 0 \quad .$$

U tom slučaju mogu se odrediti vrednosti h(p) , a time i verovatnoće p za koje izloženi postupci kodiranja ne omogućavaju zaštitu (donja granica upotrebljivosti) :

jezik	h(p) <	p <
T	0.01708	0.00159
T_1	0.01954	0.00186
T_2	0.00327	0.00024
T_3	0.00022	0.00001
T_4	0.01623	0.00150

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRIMER 6.

Izabrali smo primer zaštite teleprinterskog jezika T sa parametrima :

- M = 25 ; koristi se kod (200,200) iz primera 4. sa kodnom osnovom (200,192)
- dužina niza bitova: 2000
- nivo šuma (p≥0.02363): p = 0.024
- broj zašumljenih bitova: 48
- pozicije zašumljenih bita: 123 1779 955 51 1467 1603 859 1635

331 1347 1083 1939 315 611 1227 563 1019 995 891 1107

43 99 1675 1171 987 1523 1179 355 1451 867 1003 259 1035 1731

747 483 1339 1715 11 627 1963 419 395 291 507 1443 1499 1075

kodirana informacija

@INU<CT@C PRGBO D@JH<KT^QR<L ^@XGKNFOLDL
^QRCOSZZ<KR AGWP@VDK=KGTBFAXXFFMW@KVX@Q=
SHSWMDIMMYQFC NRB@LNFRKZKBWQUA<XSGR@X<WE
KKGA^DVBWEKZ^H^TRP\B=HZIRXO X@OHHGR=SMKO
\NXNNIGLGEMIVEAIQ^DFGLTQKJEAL@K@BN@XOT<H
LH<K DJAH=Z FK@O\ADI SA PJ\VF\NDJG=IYSQF
RD=CZ UOFPDWUHBAFR@YAWSRP^ =HVILKZDBEMUX
RWIGMJTSEVIL D^MZSE\NZ K@TP U=KBNBLL X Y
HXWY^ZQWSKCOKCJDHGH NXIW\HXSERGULD CHEB=
L\VA IEHMRTTXVD \AEA=@TPMEYCJY=G^=XG LAR

poslata informacija

dekodirao legalni učesnik

^U GRADU SSENGDU NA JUGOZAPADU KINE U NE

DELJU JE PROGLASSENO<=VANREDNO STANJE\M^

U UTORAK SE IZ DOBRO OBAVESSTENIH IZVOR

A IZ<=HONGKONGA SAZNAJE DA JE TAMO POCIN

dekodirao prisluškivač

VAZPCKRYQGCI@CE=Z Z\OO<CZ Y< DVB== \FSJO

O@GHL^FGU\C^\ Q<S<CXOGALJGKFFBBWBT UFJLC

OTW<J\QH\N B^BKFZKR^CFVRXQHVABAQJV=FT=^J

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

BA^SMJGJBLTK@W^HQSDCO=NFASUXGLJNVOGM FDQ

ULO NAJMANJE \EPP ^OSOBA\M<=^TAKODJE SE
IDXKRSIWGIJGCJVCDWPKUOXLZVAPGEH YY=ZIE\

SAZNAJE DA SU U PONEDELJAK POSLE INTERVE
FJBTC HTC BGBSEMI=DCEA^UCZFUOUA<<L LXBUL

NCIJE JEDINICA<=PROTIV DEMONSTRANATA\N ^
LNNMQC=LVVCBNU CXKSBGWILGWMCFB\LJOHGS NI

IZBILI \S^NEREDI\SM ^PREMA OVIM IZVORIMA
SUI^OJW^<FAGJ PIPLKSYFQWOKSGQ\OTML^IB<@U

<=^NEREDI I DALJE TRAJU\M ^U SSENGDU JE
YYEECRQGJFMLFQ<V^JSSUSVEDQCWE CZOGJIXOMU

RANJENO VISSE OD HILJADU<=OSOBA\M ^PREKI
AVPGOXK CARUNBGGJK<SV@KXGTZUFBE\DXDWIYS^

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Uticaj šuma u ovom primeru simuliran je "kvarenjem" kodnih bitova na pseudoslučajnim pozicijama, saglasno postavljenom nivou šuma. Korišćen je jednostavan pseudoslučajni generator zasnovan na linearnom kongruentnom metodu:

$X(0)=123$; $X(k+1) = (921X(k) + 496) \bmod 2000$; $k=1,2,...,47$.

* * *

Ovim su izloženi potrebni uslovi i primeri za realizovanje zaštite teleprinterske komunikacije. Za svaki konkretan komunikacioni sistem (ne mora biti teleprinterski niti CCITT kodiran) potrebno je, imajući u vidu korišćeni kod, izvršiti statistička merenja entropije. U slučaju prenosa informacija koje nemaju redundantnost postupak je mnogo jednostavniji jer je potrebno samo postići zadovoljenje uslova $h(p) \geq \frac{m}{n}$, a to je uglavnom moguće izborom odgovarajuće particije vektora u.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

6. PRILOZI

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

P R I L O G 1

C C I T T N°2 (Mirejeva azbuka)

slova	znaci,cifre	kodna zamena		dekad.vrednost
A	-	1 1 0 0 0		24
B	?	1 0 0 1 1		19
C	:	0 1 1 1 0		14
D	ko je tamo?(#)	1 0 0 1 0		18
E	3	1 0 0 0 0		16
F	%	1 0 1 1 0		22
G	h	0 1 0 1 1		11
H	n	0 0 1 0 1		5
I	8	0 1 1 0 0		12
J	zvono(;)	1 1 0 1 0		26
K	(	1 1 1 1 0		30
L	)	0 1 0 0 1		9
M	.	0 0 1 1 1		7
N	,	0 0 1 1 0		6
O	9	0 0 0 1 1		3
P	0	0 1 1 0 1		13
Q	1	1 1 1 0 1		29
R	4	0 1 0 1 0		10
S	' '	1 0 1 0 0		20
T	5	0 0 0 0 1		1
U	7	1 1 1 0 0		28
V	=	0 1 1 1 1		15
W	2	1 1 0 0 1		25
X	/	1 0 1 1 1		23
Y	6	1 0 1 0 1		21
Z	+	1 0 0 0 1		17
	CIFRE(\ ili 1...)	1 1 0 1 1		27
	SLOVA(^ ili A...)	1 1 1 1 1		31
	RAZMAK(raz.)	0 0 1 0 0	specij.	4
	KOL.NAZAD(] ili <)	0 0 0 1 0	znaci	2
	NOVI RED([ili ≡)	0 1 0 0 0		8
	VOĐICA(@)	0 0 0 0 0		0
KANAL KODNE ZAMENE		1 2 3 4 5		

i	A_i	ASCII	f_i	p_i
1	raz.	32	30769	0.12308
2	A	65	22464	0.08986
3	I	73	17834	0.07134
4	O	79	17748	0.07099
5	E	69	17182	0.06873
6	S	83	14207	0.05683
7	N	78	12921	0.05168
8	R	82	9577	0.03831
9	J	74	9330	0.03732
10	U	85	8567	0.03427
11	T	84	8288	0.03315
12	D	68	7658	0.03063
13	V	86	7218	0.02887
14	K	75	7171	0.02868
15	C	67	6310	0.02524
16	L	76	6235	0.02494
17	M	77	6214	0.02486
18	Z	90	5578	0.02231
19	P	80	5471	0.02188
20	^	94	4153	0.01661
21	\	92	4147	0.01659
22	]	93	3815	0.01526
23	[	91	3815	0.01526
24	G	71	3282	0.01313
25	B	66	2438	0.00975
26	,	44	1779	0.00712
27	.	46	1690	0.00676
28	H	72	1291	0.00516
29	@	64	609	0.00244
30	F	70	516	0.00206
31	"	34	434	0.00174
32	-	45	213	0.00085
33	0	48	210	0.00084
34	1	49	154	0.00062
35	9	57	103	0.00041
36	:	58	103	0.00041
37	8	56	82	0.00033
38	2	50	80	0.00032
39	5	53	76	0.00030
40	4	52	57	0.00023
41	3	51	50	0.00020
42	7	55	47	0.00019
43	(	40	32	0.00013
44	)	41	32	0.00013
45	6	54	23	0.00009
46	?	63	23	0.00009
47	X	88	2	0.00001
48	Q	81	1	0.00000
49	W	87	1	0.00000
50	Y	89	0	0.00000
51	/	47	0	0.00000
52	%	33	0	0.00000
53	n	38	0	0.00000
54	h	37	0	0.00000
55	=	61	0	0.00000
56	+	43	0	0.00000
57	#	35	0	0.00000

Prilog 2.
Raspodela frekvencija f_i i verovatnoća p_i po alfabetu A (uzorak srpskog jezika)

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 4.

Raspodela frekvencija f_i i verovatnoća p_i kodnih zamenamau režimu slova i raspodela frekvencija f_j i verovatnoća p_j kodnih zamena u režimu cifara

(uzorak srpskog jezika; 250 000 karaktera)

slovo i	f_i	p_i	znak j	f_j	p_j	$p_i + p_j$
A	22464	0.08986	-	213	0.00085	0.09071
B	2438	0.00975	?	23	0.00009	0.00984
C	6310	0.02524	:	103	0.00041	0.02565
D	7658	0.03063	#	0	0.00000	0.03063
E	17182	0.06873	3	50	0.00020	0.06893
F	516	0.00206	%	0	0.00000	0.00206
G	3282	0.01313	h	0	0.00000	0.01313
H	1291	0.00516	n	0	0.00000	0.00516
I	17834	0.07134	8	82	0.00033	0.07167
J	9330	0.03732	zv;	0	0.00000	0.03732
K	7171	0.02868	(	32	0.00013	0.02881
L	6235	0.02494	)	32	0.00013	0.02507
M	6214	0.02486	.	1690	0.00676	0.03162
N	12921	0.05168	,	1779	0.00712	0.05880
O	17748	0.07099	9	103	0.00041	0.07140
P	5471	0.02188	0	210	0.00084	0.02272
Q	1	0.00000	1	154	0.00062	0.00062
R	9577	0.03831	4	57	0.00023	0.03854
S	14207	0.05683	"	434	0.00174	0.05857
T	8288	0.03315	5	76	0.00030	0.03345
U	8567	0.03427	7	47	0.00019	0.03446
V	7218	0.02887	=	0	0.00000	0.02887
W	1	0.00000	2	80	0.00032	0.00032
X	2	0.00001	/	0	0.00000	0.00001
Y	0	0.00000	6	23	0.00009	0.00009
Z	5578	0.02231	+	0	0.00000	0.02231
] (<)	3815	0.01526				0.01526
[(≡)	3815	0.01526				0.01526
^ (A...)	4153	0.01661	specijalni			0.01661
\ (1...)	4147	0.01659	znaci			0.01659
razmak	30769	0.12308				0.12308
@	609	0.00244				0.00244

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 4.a

Intervali poverenja za verovatnoće p_i+p_j (Prilog 4.) sa nivoom poverenja β po kodnim rečima sa CCITT dekadnim vrednostima k

CCITT k	β = 0.90	β = 0.95	β = 0.99
24	[0.08977, 0.09166]	[0.08959, 0.09184]	[0.08924, 0.09220]
19	[0.00952, 0.01018]	[0.00946, 0.01024]	[0.00935, 0.01037]
14	[0.02514, 0.02618]	[0.02504, 0.02628]	[0.02485, 0.02648]
18	[0.03007, 0.03121]	[0.02996, 0.03132]	[0.02975, 0.03153]
16	[0.06810, 0.06977]	[0.06794, 0.06993]	[0.06763, 0.07025]
22	[0.00192, 0.00222]	[0.00189, 0.00225]	[0.00184, 0.00231]
11	[0.01276, 0.01351]	[0.01269, 0.01358]	[0.01255, 0.01373]
5	[0.00493, 0.00541]	[0.00489, 0.00545]	[0.00481, 0.00555]
12	[0.07081, 0.07252]	[0.07065, 0.07268]	[0.07034, 0.07300]
26	[0.03670, 0.03795]	[0.03658, 0.03807]	[0.03635, 0.03831]
30	[0.02826, 0.02937]	[0.02816, 0.02948]	[0.02796, 0.02969]
9	[0.02456, 0.02559]	[0.02446, 0.02569]	[0.02427, 0.02589]
7	[0.03104, 0.03220]	[0.03093, 0.03231]	[0.03072, 0.03253]
6	[0.05803, 0.05958]	[0.05788, 0.05973]	[0.05760, 0.06003]
3	[0.07056, 0.07226]	[0.07040, 0.07242]	[0.07009, 0.07274]
13	[0.02224, 0.02322]	[0.02214, 0.02332]	[0.02197, 0.02351]
29	[0.00054, 0.00071]	[0.00053, 0.00073]	[0.00050, 0.00076]
10	[0.03791, 0.03918]	[0.03779, 0.03930]	[0.03755, 0.03954]
20	[0.05779, 0.05934]	[0.05765, 0.05949]	[0.05736, 0.05979]
1	[0.03287, 0.03405]	[0.03276, 0.03417]	[0.03254, 0.03440]
28	[0.03386, 0.03506]	[0.03375, 0.03518]	[0.03353, 0.03541]
15	[0.02832, 0.02943]	[0.02822, 0.02954]	[0.02802, 0.02975]
25	[0.00027, 0.00039]	[0.00026, 0.00040]	[0.00024, 0.00043]
23	[0.00000, 0.00000]	[0.00000, 0.00001]	[0.00000, 0.00002]
21	[0.00006, 0.00013]	[0.00006, 0.00014]	[0.00005, 0.00016]
17	[0.02183, 0.02281]	[0.02174, 0.02290]	[0.02156, 0.02309]
27	[0.01486, 0.01567]	[0.01478, 0.01575]	[0.01464, 0.01591]
31	[0.01486, 0.01567]	[0.01478, 0.01575]	[0.01464, 0.01591]
4	[0.01619, 0.01704]	[0.01612, 0.01712]	[0.01596, 0.01729]
2	[0.01617, 0.01702]	[0.01609, 0.01710]	[0.01594, 0.01726]
8	[0.12200, 0.12416]	[0.12179, 0.12437]	[0.12139, 0.12478]
0	[0.00228, 0.00261]	[0.00225, 0.00264]	[0.00219, 0.00271]

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 6.

Interval poverenja za entropiju H kanala i sa nivoom poverenja β

(Prilog 5.)

i	β= 0.90	β = 0.95	β = 0.99
1	(0.97934, 0.98157)	(0.97913, 0.98179)	(0.97871, 0.98220)
2	(0.99568, 0.99777)	(0.99548, 0.99797)	(0.99509, 0.99836)
3	(0.99875, 1.00081)	(0.99855, 1.00101)	(0.99816, 1.00139)
4	(0.98267, 0.98488)	(0.98246, 0.98509)	(0.98205, 0.98550)
5	(0.87716, 0.88011)	(0.87687, 0.88039)	(0.87632, 0.88095)

Interval poverenja za entropiju H_1 jezika T sa nivoom poverenja β

(Prilog 8.)

n	β= 0.90	β = 0.95	β = 0.99
1	(0.98242,0.98341)	(0.98233, 0.98350)	(0.98214, 0.98369)

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Prilog 7.

Koeficjent korelacije R_{XY} za kanale X i Y

(uzorak srpskog jezika)

X \ Y	1	2	3	4	5
1	1	0.12422	-0.28957	-0.14676	-0.25738
2	0.12422	1	-0.03153	-0.02942	-0.06555
3	-0.28957	-0.03153	1	-0.09661	-0.20045
4	-0.14676	-0.02942	-0.09661	1	0.27182
5	-0.25738	-0.06555	-0.20045	-0.27182	1

Interval poverenja za koeficijent korelacije R_{XY} kanala X i Y sa nivoom poverenja β

X Y	β=0.90	β=0.95	β=0.99
1 2	(0.12098, 0.12746)	(0.12036, 0.12808)	(0.11915, 0.12929)
1 3	(-0.29258,-0.28655)	(-0.29316,-0.28597)	(-0.29428,-0.28484)
1 4	(-0.14998,-0.14354)	(-0.15060,-0.14292)	(-0.15180,-0.14172)
1 5	(-0.26045,-0.25431)	(-0.26104,-0.25371)	(-0.26219,-0.25256)
2 3	(-0.03482,-0.02824)	(-0.03545,-0.02761)	(-0.03668,-0.02638)
2 4	(0.02613, 0.03271)	(0.02550, 0.03334)	(0.02427, 0.03457)
2 5	(-0.06883,-0.06227)	(-0.06945,-0.06164)	(-0.07068,-0.06042)
3 4	(-0.09987,-0.09335)	(-0.10049,-0.09272)	(-0.10171,-0.09150)
3 5	(-0.20361,-0.19729)	(-0.20421,-0.19668)	(-0.20539,-0.19550)
4 5	(0.26877, 0.27486)	(0.26818, 0.27545)	(0.26704, 0.27659)

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 8.

Pregled entropija jezika T po bitovima i slovima

(dužina teksta 250 000 slova; uzorak srpskog jezika)

binarni nivo (zajedno $T_i, i=\overline{1,5}$)		slovčani nivo	
dužina serije	H_n	$H_0=H_{max}=5.000$ s=32	$H_0=4,95$ s=31
n = 1	0.98292		
n = 2	0.98207		
n = 3	0.97981		
n = 4	0.97777		
n = 5 $H_5=4.407$	0.88137	$H_1=4.407$	$H_1=4.18$
n = 6	0.96928		
n = 7	0.96297		
n = 8	0.95517		
n = 9	0.94674		
n =10 $H_{10}=7.834$	0.78345	$H_2=3.917$	$H_2=3.45$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Prilog 9.

Raspodela frekvencija f_i i verovatnoća p_i po alfabetu

$\{A_i, i=1,32\}=E_{32}$ (uzorak engleskog jezika)

i	A_i	ASCII	f_i	p_i
1	raz	32	14301	0.14301
2	E	69	9234	0.09234
3	T	84	6997	0.06997
4	A	65	6298	0.06298
5	I	73	6148	0.06148
6	N	78	5995	0.05995
7	O	79	5751	0.05751
8	S	83	4992	0.04992
9	R	82	4864	0.04864
10	H	72	3505	0.03505
11	[	91	3011	0.03011
12	]	93	2950	0.02950
13	L	76	2796	0.02796
14	D	68	2788	0.02788
15	@	64	2456	0.02456
16	C	67	2317	0.02317
17	F	70	2007	0.02007
18	M	77	1888	0.01888
19	U	85	1806	0.01806
20	^	94	1779	0.01779
21	P	80	1768	0.01768
22	G	71	1482	0.01482
23	W	87	1166	0.01166
24	Y	89	985	0.00985
25	B	66	974	0.00974
26	V	86	813	0.00813
27	K	75	492	0.00492
28	Q	81	191	0.00191
29	J	74	125	0.00125
30	X	88	116	0.00116
31	\	92	4	0.00004
32	Z	90	1	0.00001
	UKUPNO		100000	1.00000

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 10.

Raspodela binarnih frekvencija f_0, f_1 ; verovatnoća p_0^k, p_1^k i entropije H po kanalima k (uzorak engleskog jezika)

k	f_0	f_1	p_0^k	p_1^k	H
1	67040	32960	0.67040	0.32960	0.93460
2	64940	35060	0.64940	0.35060	0.93460
3	50895	49105	0.50895	0.49105	0.99977
4	65655	34345	0.65655	0.34345	0.92808
5	69782	30218	0.69782	0.30218	0.88394

Interval poverenja za p_0^k (verovatnoća bitova 0) po kanalu k

sa nivoom poverenja β

k	p_0^k	β=0.90	β=0.95	β=0.99
1	0.67040	[0.66795,0.67285]	[0.66747,0.67331]	[0.66655,0.67422]
2	0.64940	[0.64691,0.65188]	[0.64643,0.65236]	[0.64550,0.65328]
3	0.50895	[0.50634,0.51156]	[0.50584,0.51205]	[0.50487,0.51303]
4	0.65655	[0.65407,0.65902]	[0.65359,0.65949]	[0.65267,0.66041]
5	0.69782	[0.69542,0.70021]	[0.69496,0.70067]	[0.69406,0.70155]

Interval poverenja za p_1^k (verovatnoća bitova 1) po kanalu k

sa nivoom poverenja β

k	p_1^k	β=0.90	β=0.95	β=0.99
1	0.32960	[0.32715,0.33205]	[0.32669,0.33253]	[0.32578,0.33345]
2	0.35060	[0.34812,0.35309]	[0.34764,0.35357]	[0.34672,0.35450]
3	0.49105	[0.48844,0.49366]	[0.48795,0.49416]	[0.48697,0.49513]
4	0.34345	[0.34098,0.34593]	[0.34051,0.34641]	[0.33959,0.34733]
5	0.30218	[0.29979,0.30458]	[0.29933,0.30504]	[0.29845,0.30594]

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 11.

Pregled entropija jezika T po bitovima i slovima

(dužina teksta 250 000 slova; uzorak engleskog jezika)

binarni nivo (zajedno $T_i, i=\overline{1,5}$)		slovčani nivo	
dužina serije	H_n	$H_0=H_{max}=5.000$ s=32	$H_0=4.76$ s=27
n = 1	0.945		
n = 2	0.945		
n = 3	0.944		
n = 4	0.943		
n = 5 $H_5=4.375$	0.875	$H_1=4.375$	$H_1=4.03$
n = 6	0.937		
n = 7	0.932		
n = 8	0.924		
n = 9	0.914		
n =10 $H_{10}=7.716$	0.772	$H_2=3.858$	$H_2=3.32$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 12.1

Raspodela serija dužine n i vrednosti χ^2 testa saglasnosti za 1. kanal na uzorku dužine 250 000 bitova

verovatnoće serija dužine n=1 :

0	1
.58211	.41789

n = 1 H=0.98046

verovatnoće serija dužine n=2 :

00	01	10	11
.32996	.25215	.25216	.16574

n = 2 H=0.97998 χ^2_3 = 334.25 ($\chi^2_{3;0.99}$ = 11.34)

verovatnoće serija dužine n=3 :

000	001	010	011	100	101	110	111
.18004	.14992	.13956	.11260	.14992	.10223	.11260	.05314

n = 3 H=0.97787 χ^2_7 =2565.39 ($\chi^2_{7;0.99}$ = 18.48)

verovatnoće serija dužine n=4 : 0000 0001 0010 ... 1111

.10148	.07856	.07963	.07029	.08418	.05537	.07720	.03539
.07856	.07137	.05993	.04230	.06574	.04686	.03539	.01775

n = 4 H=0.97655 χ^2_{15}=5316.98 ($\chi^2_{15;0.99}$= 30.58)

verovatnoće serija dužine n=5 : 00000 00001 00010 ... 11111

.05898	.04251	.04264	.03592	.04719	.03244	.04836	.02193
.04445	.03973	.03393	.02144	.04372	.03349	.02312	.01227
.04251	.03605	.03699	.03438	.03700	.02293	.02885	.01346
.03411	.03163	.02599	.02087	.02202	.01337	.01227	.00548

n = 5 H=0.97559 χ^2_{31}=8408.34 ($\chi^2_{31;0.99}$= 52.19)

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 12.2

Raspodela serija dužine n i vrednosti χ^2 testa saglasnosti za 2. kanal na uzorku dužine 250 000 bitova

verovatnoće serija dužine n=1 :

0	1
.53366	.46634

n = 1 H=0.99673

verovatnoće serija dužine n=2 :

00	01	10	11
.27397	.25969	.25968	.20666

n = 2 H=0.99605 $\chi^2_3 = 472.49$ ($\chi^2_{3;0.99} = 11.34$)

verovatnoće serija dužine n=3 :

000	001	010	011	100	101	110	111
.13117	.14280	.14505	.11464	.14280	.11689	.11464	.09201

n = 3 H=0.99517 $\chi^2_7 = 1598.11$ ($\chi^2_{7;0.99} = 18.48$)

verovatnoće serija dužine n=4 : 0000 0001 0010 ... 1111

.06753	.06364	.07768	.06512	.07905	.06600	.06409	.05054
.06364	.07916	.06737	.04951	.06375	.05089	.05054	.04147

n = 4 H=0.99443 $\chi^2_{15} = 3236.79$ ($\chi^2_{15;0.99} = 30.58$)

verovatnoće serija dužine n=5 : 00000 00001 00010 ... 11111

.03533	.03220	.03721	.02644	.04202	.03566	.03674	.02838
.03401	.04504	.03697	.02903	.03475	.02934	.02762	.02292
.03220	.03144	.04047	.03869	.03703	.03035	.02735	.02216
.02964	.03412	.03041	.02048	.02900	.02154	.02292	.01855

n = 5 H=0.99381 $\chi^2_{31} = 5198.79$ ($\chi^2_{31;0.99} = 52.19$)

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 12.3

Raspodela serija dužine n i vrednosti χ^2 testa saglasnosti

za 3. kanal na uzorku dužine 250 000 bitova

verovatnoće serija dužine n=1 :

0	1
.49120	.50880

n = 1 H=0.99978

verovatnoće serija dužine n=2 :

00	01	10	11
.24732	.24389	.24388	.26491

n = 2 H=0.99957 $\chi^2_3 = 145.78$ ($\chi^2_{3;0.99} = 11.34$)

verovatnoće serija dužine n=3 :

000	001	010	011	100	101	110	111
.11170	.13562	.11444	.12945	.13561	.10828	.12944	.13546

n = 3 H=0.99816 $\chi^2_7 = 1660.14$ ($\chi^2_{7;0.99} = 18.48$)

verovatnoće serija dužine n=4 : 0000 0001 0010 ... 1111

.05424	.05745	.06579	.06983	.06316	.05128	.06090	.06855
.05745	.07816	.04865	.05962	.07245	.05699	.06855	.06691

n = 4 H=0.99717 $\chi^2_{15} = 3614.03$ ($\chi^2_{15;0.99} = 30.58$)

verovatnoće serija dužine n=5 : 00000 00001 00010 ... 11111

.02626	.02798	.02518	.03227	.03578	.03001	.03178	.03805
.02606	.03711	.02082	.03046	.03379	.02711	.03272	.03583
.02798	.02947	.04061	.03755	.02738	.02127	.02912	.03050
.03140	.04105	.02783	.02916	.03867	.02988	.03583	.03109

HI R-1 31

N= 5 E= 4.98117 E/n

n = 5 H=0.99623 $\chi^2_{31} = 6113.18$ ($\chi^2_{31;0.99} = 52.19$)

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 12.4

Raspodela serija dužine n i vrednosti χ^2 testa saglasnosti

za 4. kanal na uzorku dužine 250 000 bitova

verovatnoće serija dužine n=1 :

0	1
.57485	.42515

n = 1 H=0.98377

verovatnoće serija dužine n=2 :

00	01	10	11
.30714	.26771	.26771	.15743

n = 2 H=0.98047 χ^2_3 =2275.27 ($\chi^2_{3;0.99}$ = 11.34)

verovatnoće serija dužine n=3 :

000	001	010	011	100	101	110	111
.17399	.13316	.16989	.09781	.13316	.13456	.09782	.05961

n = 3 H=0.97870 χ^2_7 =5469.62 ($\chi^2_{7;0.99}$ = 18.48)

verovatnoće serija dužine n=4 : 0000 0001 0010 ... 1111

.09783	.07616	.08796	.04519	.08424	.08565	.05857	.03924
.07616	.05700	.08193	.05263	.04891	.04891	.03924	.02037

n = 4 H=0.97756 χ^2_{15}=8874.60 ($\chi^2_{15;0.99}$= 30.58)

verovatnoće serija dužine n=5 : 00000 00001 00010 ... 11111

.05388	.04395	.05003	.02612	.04156	.04640	.02602	.01917
.04835	.03589	.05204	.03361	.02721	.03137	.02582	.01342
.04395	.03221	.03793	.01907	.04268	.03925	.03256	.02007
.02780	.02111	.02989	.01902	.02170	.01754	.01342	.00695

n = 5 H=0.97667 χ^2_{31}=12642.54 ($\chi^2_{31;0.99}$= 52.19)

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 12.5

Raspodela serija dužine n i vrednosti χ^2 testa saglasnosti

za 5. kanal na uzorku dužine 250 000 bitova

verovatnoće serija dužine n=1 :

0	1
.70216	.29784

n = 1 H=0.87864

verovatnoće serija dužine n=2 :

00	01	10	11
.49388	.20828	.20828	.08957

n = 2 H=0.87863 $\chi^2_3 = 4.21$ ($\chi^2_{3;0.99} = 11.34$)

verovatnoće serija dužine n=3 :

000	001	010	011	100	101	110	111
.35171	.14218	.14312	.06516	.14218	.06609	.06516	.02441

n = 3 H=0.87836 $\chi^2_7 = 282.32$ ($\chi^2_{7;0.99} = 18.48$)

verovatnoće serija dužine n=4 : 0000 0001 0010 ... 1111

.25492	.09678	.09846	.04371	.09771	.04541	.04734	.01782
.09679	.04539	.04465	.02144	.04447	.02068	.01782	.00659

n = 4 H=0.87805 $\chi^2_{15} = 815.42$ ($\chi^2_{15;0.99} = 30.58$)

verovatnoće serija dužine n=5 : 00000 00001 00010 ... 11111

.18327	.07165	.06706	.02973	.06628	.03218	.03125	.01247
.06624	.03147	.03108	.01433	.03217	.01517	.01278	.00503
.07166	.02513	.03140	.01399	.03142	.01323	.01610	.00535
.03055	.01392	.01357	.00711	.01231	.00551	.00503	.00156

n = 5 H=0.87778 $\chi^2_{31} = 1468.31$ ($\chi^2_{31;0.99} = 52.19$)

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 13.1

Raspodela serija dužine n i vrednosti χ^2 testa saglasnosti za 1. kanal na 5 podnizova uzorka od 250 000 bitova

verovatnoće serija dužine n=1 : 0 1

0.58285 0.41715 1.podniz $\chi^2_1 = 0.04$

0.58240 0.41760 2.podniz $\chi^2_1 = 0.00$

0.58045 0.41955 3.podniz $\chi^2_1 = 0.23$ $(\chi^2_{1;0.99} = 6.64)$

0.58120 0.41880 4.podniz $\chi^2_1 = 0.07$

0.58370 0.41630 5.podniz $\chi^2_1 = 0.20$

verovatnoće serija dužine n=2 : 00 01 10 11

0.34037 0.24251 0.24251 0.17461
1.podniz $\chi^2_3 = 0.22$

0.34192 0.24051 0.24051 0.17706
2.podniz $\chi^2_3 = 2.45$

0.33937 0.24106 0.24106 0.17851
3.podniz $\chi^2_3 = 2.52$ $(\chi^2_{3;0.99}=11.35)$

0.33862 0.24256 0.24256 0.17626
4.podniz $\chi^2_3 = 0.38$

0.34307 0.24061 0.24066 0.17566
5.podniz $\chi^2_3 = 2.28$

verovatnoće serija dužine n=3 : 000 001 010 011 100 101 110 111

0.20017 0.14021 0.14081 0.10171 0.14021 0.10231 0.10166 0.07291
1.podniz $\chi^2_7 = 1.58$

0.20267 0.13926 0.13606 0.10446 0.13926 0.10126 0.10446 0.07256
2.podniz $\chi^2_7 = 12.05$

0.19797 0.14141 0.13986 0.10121 0.14136 0.09966 0.10121 0.07731
3.podniz $\chi^2_7 = 6.47$ $(\chi^2_{7;0.99} = 18.48)$

0.19857 0.14001 0.14151 0.10106 0.14001 0.10256 0.10106 0.07521
4.podniz $\chi^2_7 = 2.55$

0.20412 0.13896 0.13936 0.10126 0.13896 0.10166 0.10131 0.07436
5.podniz $\chi^2_7 = 8.00$

verovatnoće serija dužine n=4 : 0001 0010 0011 ... 1110 1110

0.11807 0.08211 0.08201 0.05821 0.08081 0.06001 0.06066 0.04106
0.08211 0.05811 0.05881 0.04351 0.05941 0.04226 0.04101 0.03185
1.podniz $\chi^2_{15} = 8.03$

0.12177 0.08091 0.07931 0.05996 0.07756 0.05851 0.06151 0.04296
0.08091 0.05836 0.05676 0.04451 0.06171 0.04276 0.04296 0.02955
2.podniz $\chi^2_{15} = 26.93$

0.11727 0.08071 0.08191 0.05951 0.08106 0.05876 0.05756 0.04366
0.08071 0.06066 0.05796 0.04171 0.06031 0.04091 0.04366 0.03366
3.podniz $\chi^2_{15} = 15.09$ $(\chi^2_{15;0.99} = 30.58)$

0.11607 0.08246 0.08216 0.05786 0.08106 0.06046 0.05801 0.04306
0.08246 0.05756 0.05936 0.04321 0.05896 0.04211 0.04306 0.03215

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 13.2

Raspodela serija dužine n i vrednosti χ^2 testa saglasnosti za 2. kanal na 5 podnizova uzorka od 250 000 bitova

verovatnoće serija dužine n=1 : 0 1

0.53208 0.46793 1.podniz $\chi^2_1 = 0.41$

0.53468 0.46533 2.podniz $\chi^2_1 = 0.16$

0.53550 0.46450 3.podniz $\chi^2_1 = 0.54$ ($\chi^2_{1;0.99} = 6.64$)

0.53365 0.46635 4.podniz $\chi^2_1 = 0.00$

0.53325 0.46675 5.podniz $\chi^2_1 = 0.03$

verovatnoće serija dužine n=2 : 00 01 10 11

0.28401 0.24809 0.24806 0.21984
1.podniz $\chi^2_3 = 1.32$

0.28554 0.24914 0.24916 0.21616
2.podniz $\chi^2_3 = 0.42$

0.28881 0.24666 0.24669 0.21784
3.podniz $\chi^2_3 = 3.84$ ($\chi^2_{3;0.99} = 11.35$)

0.28449 0.24919 0.24916 0.21716
4.podniz $\chi^2_3 = 0.06$

0.28584 0.24744 0.24739 0.21934
5.podniz $\chi^2_3 = 1.48$

verovatnoće serija dužine n=3 : 000 001 010 011 100 101 110 111

0.15302 0.13101 0.13344 0.11466 0.13099 0.11709 0.11461 0.10519
1.podniz $\chi^2_7 = 9.70$

0.15302 0.13254 0.13411 0.11501 0.13254 0.11661 0.11504 0.10114
2.podniz $\chi^2_7 = 1.71$

0.15729 0.13154 0.13061 0.11606 0.13151 0.11514 0.11606 0.10179
3.podniz $\chi^2_7 = 10.19$ ($\chi^2_{7;0.99} = 18.48$)

0.15252 0.13199 0.13491 0.11424 0.13199 0.11719 0.11426 0.10291
4.podniz $\chi^2_7 = 5.37$

0.15432 0.13154 0.13251 0.11489 0.13149 0.11591 0.11489 0.10446
5.podniz $\chi^2_7 = 7.04$

verovatnoće serija dužine n=4 : 0001 0010 0011 ... 1110 1110

0.08381 0.06921 0.07019 0.06083 0.06931 0.06413 0.06008 0.05456
0.06921 0.06178 0.06326 0.05383 0.06168 0.05293 0.05453 0.05063
1.podniz $\chi^2_{15} = 26.51$

0.08219 0.07084 0.07209 0.06043 0.07136 0.06273 0.06121 0.05381
0.07084 0.06171 0.06203 0.05458 0.06116 0.05388 0.05381 0.04733
2.podniz $\chi^2_{15} = 4.56$

0.08694 0.07036 0.07071 0.06083 0.06904 0.06153 0.06253 0.05353
0.07034 0.06118 0.05991 0.05523 0.06248 0.05358 0.05353 0.04826
3.podniz $\chi^2_{15} = 25.83$ ($\chi^2_{15;0.99} = 30.58$)

0.08176 0.07076 0.07164 0.06033 0.07071 0.06421 0.06008 0.05416

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 13.3

Raspodela serija dužine n i vrednosti χ^2 testa saglasnosti za 3. kanal na 5 podnizova uzorka od 250 000 bitova

verovatnoće serija dužine n=1 : 0 1

0.48730 0.51270 1.podniz $\chi^2_1 = 1.23$

0.48775 0.51225 2.podniz $\chi^2_1 = 0.97$

0.48915 0.51085 3.podniz $\chi^2_1 = 0.34$ ($\chi^2_{1;0.99} = 6.64$)

0.49050 0.50950 4.podniz $\chi^2_1 = 0.04$

0.49200 0.50800 5.podniz $\chi^2_1 = 0.05$

verovatnoće serija dužine n=2 : 00 01 10 11

0.23661 0.25071 0.25066 0.26201
1.podniz $\chi^2_3 = 2.66$

0.23566 0.25211 0.25206 0.26016
2.podniz $\chi^2_3 = 3.49$

0.23626 0.25291 0.25291 0.25791
3.podniz $\chi^2_3 = 3.58$ ($\chi^2_{3;0.99} = 11.35$)

0.23466 0.25581 0.25581 0.25371
4.podniz $\chi^2_3 = 11.23$

0.23741 0.25456 0.25456 0.25346
5.podniz $\chi^2_3 = 6.94$

verovatnoće serija dužine n=3 : 000 001 010 011 100 101 110 111

0.11361 0.12301 0.12331 0.12736 0.12301 0.12766 0.12736 0.13466
1.podniz $\chi^2_7 = 5.53$

0.11536 0.12031 0.12576 0.12631 0.12031 0.13176 0.12631 0.13386
2.podniz $\chi^2_7 = 9.37$

0.11441 0.12186 0.12586 0.12706 0.12186 0.13106 0.12701 0.13086
3.podniz $\chi^2_7 = 7.26$ ($\chi^2_{7;0.99} = 18.48$)

0.11216 0.12251 0.12966 0.12616 0.12246 0.13331 0.12616 0.12756
4.podniz $\chi^2_7 = 13.64$

0.11616 0.12126 0.12851 0.12606 0.12121 0.13331 0.12606 0.12741
5.podniz $\chi^2_7 = 16.33$

verovatnoće serija dužine n=4 : 0001 0010 0011 ... 1110 1110

0.05621 0.05741 0.05931 0.06371 0.05916 0.06416 0.06126 0.06611
0.05741 0.06561 0.06401 0.06361 0.06386 0.06351 0.06611 0.06856
1.podniz $\chi^2_{15} = 16.70$

0.05741 0.05796 0.06041 0.05986 0.06066 0.06511 0.06096 0.06536
0.05796 0.06236 0.06531 0.06646 0.05966 0.06666 0.06536 0.06851
2.podniz $\chi^2_{15} = 17.26$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 13.4

Raspodela serija dužine n i vrednosti χ^2 testa saglasnosti za 4. kanal na 5 podnizova uzorka od 250 000 bitova

verovatnoće serija dužine n=1 : 0 1

0.57513 0.42487 1.podniz $\chi^2_1 = 0.01$

0.57465 0.42535 2.podniz $\chi^2_1 = 0.00$

0.57411 0.42589 3.podniz $\chi^2_1 = 0.07$ $(\chi^2_{1;0.99} = 6.64)$

0.57492 0.42508 4.podniz $\chi^2_1 = 0.00$

0.57843 0.42157 5.podniz $\chi^2_1 = 1.75$

verovatnoće serija dužine n=2 : 00 01 10 11

0.33097 0.24421 0.24415 0.18067
1.podniz $\chi^2_3 = 0.04$

0.32699 0.24765 0.24768 0.17768
2.podniz $\chi^2_3 = 5.87$

0.32846 0.24565 0.24565 0.18025
3.podniz $\chi^2_3 = 0.87$ $(\chi^2_{3;0.99} = 11.35)$

0.33044 0.24451 0.24448 0.18058
4.podniz $\chi^2_3 = 0.00$

0.33559 0.24289 0.24280 0.17872
5.podniz $\chi^2_3 = 4.08$

verovatnoće serija dužine n=3 : 000 001 010 011 100 101 110 111

0.19202 0.13898 0.13958 0.10462 0.13898 0.10519 0.10459 0.07604
1.podniz $\chi^2_7 = 3.13$

0.18666 0.14030 0.14405 0.10360 0.14036 0.10735 0.10360 0.07409
2.podniz $\chi^2_7 = 12.05$

0.19025 0.13817 0.14207 0.10357 0.13823 0.10744 0.10357 0.07670
3.podniz $\chi^2_7 = 7.18$ $(\chi^2_{7;0.99} = 18.48)$

0.18990 0.14054 0.14204 0.10243 0.14054 0.10396 0.10243 0.07817
4.podniz $\chi^2_7 = 2.76$

0.19514 0.14048 0.14099 0.10186 0.14048 0.10234 0.10183 0.07688
5.podniz $\chi^2_7 = 8.28$

verovatnoće serija dužine n=4 : 0001 0010 0011 ... 1110 1110

0.11200 0.08004 0.07884 0.06013 0.07905 0.06055 0.06129 0.04333
0.08004 0.05896 0.06073 0.04447 0.05995 0.04465 0.04330 0.03269
1.podniz $\chi^2_{15} = 9.76$

0.10547 0.08121 0.08175 0.05854 0.08250 0.06156 0.06061 0.04300
0.08121 0.05911 0.06228 0.04507 0.05782 0.04579 0.04300 0.03110
2.podniz $\chi^2_{15} = 22.24$

0.11086 0.07941 0.07911 0.05905 0.07995 0.06213 0.05926 0.04432
0.07941 0.05878 0.06291 0.04453 0.05830 0.04528 0.04432 0.03239

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 13.5

Raspodela serija dužine n i vrednosti χ^2 testa saglasnosti za 5. kanal na 5 podnizova uzorka od 250 000 bitova

verovatnoće serija dužine n=1 : 0 1

0.70243 0.29758 1.podniz $\chi_1^2 = 0.01$

0.70483 0.29518 2.podniz $\chi_1^2 = 1.35$

0.69978 0.30023 3.podniz $\chi_1^2 = 1.09$ ($\chi^2_{1;0.99} = 6.64$)

0.70030 0.29970 4.podniz $\chi_1^2 = 0.67$

0.70078 0.29923 5.podniz $\chi_1^2 = 0.37$

verovatnoće serija dužine n=2 : 00 01 10 11

0.49365 0.20879 0.20879 0.08878
1.podniz $\chi_3^2 = 0.07$

0.49427 0.21056 0.21054 0.08463
2.podniz $\chi_3^2 = 8.41$

0.48842 0.21136 0.21136 0.08885
3.podniz $\chi_3^2 = 3.66$ ($\chi^2_{3;0.99} = 11.35$)

0.48862 0.21169 0.21169 0.08800
4.podniz $\chi_3^2 = 4.33$

0.48987 0.21091 0.21089 0.08833
5.podniz $\chi_3^2 = 2.09$

verovatnoće serija dužine n=3 : 000 001 010 011 100 101 110 111

0.34721 0.14644 0.14546 0.06331 0.14644 0.06236 0.06331 0.02548
1.podniz $\chi_7^2 = 3.37$

0.34603 0.14824 0.15017 0.06038 0.14824 0.06231 0.06038 0.02425
2.podniz $\chi_7^2 = 15.72$

0.34006 0.14836 0.14809 0.06326 0.14839 0.06298 0.06326 0.02560
3.podniz $\chi_7^2 = 8.55$ ($\chi^2_{7;0.99} = 18.48$)

0.34173 0.14689 0.15034 0.06133 0.14689 0.06481 0.06133 0.02668
4.podniz $\chi_7^2 = 11.00$

0.34171 0.14816 0.14879 0.06211 0.14814 0.06276 0.06211 0.02623
5.podniz $\chi_7^2 = 4.52$

verovatnoće serija dužine n=4 : 0001 0010 0011 ... 1110 1110

0.24356 0.10364 0.10209 0.04433 0.10167 0.04381 0.04576 0.01755
0.10364 0.04281 0.04338 0.01898 0.04476 0.01855 0.01755 0.00793
1.podniz $\chi_{15}^2 = 11.97$

0.24209 0.10394 0.10567 0.04258 0.10574 0.04443 0.04268 0.01770
0.10397 0.04428 0.04448 0.01780 0.04251 0.01788 0.01770 0.00655

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

PRILOG 14.

Parametri prvih 10 Hemingovih (n,k) kodova

za $n=2^m-1$

m	n	k	d
2	3	1	3
3	7	4	3
4	15	11	3
5	31	26	3
6	63	57	3
7	127	120	3
8	255	247	3
9	511	502	3
10	1023	1013	3
11	2047	2036	3

```
C                          P R I L O G  1 5.
C     PROGRAM PRINT25H
C     ------------------------------------------------------------
C     formiranje matrice A za postupak particije i prov.det(A)<>0
C     Hi=APi - matrice u hexa zapisu
C     --------  MAKSIMALNI KOD  ( 200 , 192 ) ,     N=200 ---------
C     ============================================================
C     SPECIJ.SLUC. podele na 25 delova, tj. m=25 => (200,192) kod
C     jer je kod (n,n-m) gde je m-broj bitova  provere,  podelu
C     na 25 podnizova dobija se uzimanjem svakog 25. elementa
C                FORMIRANJE STAMPE I PRIKAZ KODA
C           =======================================
      INTEGER*2 MAT(200,200),N,M,P(200,200),H(200,200),A(200,200)
     *,AI(200,400)
      INTEGER*2 IND,IJ,U,V
      INTEGER*2 PERM(200),INDIND,BIT
      INTEGER*4 R
C
      PRINT '(A30\)',' UNESI POC. VRED. GENERATORA '
      READ '(I12)',R
      PRINT '(A38\)',' UNESI DIMENZIJU n (kodnog vekt.):'
      READ '(2I3)',N
      DO 110 MM=8,2,-1
      N1=2**MM-1
      IF( N.LE.N1) M=MM
110   CONTINUE
      MM=N/M
      PRINT '(1X,A16,I3,A1,I3,A1)','Formira se kod (',N,',',N-M,')'
      DO 5 I=1,N
      DO 5 J=1,M
5     P(I,J)=0
C
      DO 6 I=1,M
      J=I*MM-(MM-1)
6      P(J,I)=1
C
C     P matrica
C     prvi podniz 1. 26. 51. 76. 101. 126. 151. 176.  za (200,192)
C      P1(1,1)=1      P1(26,2)=1      P1(51,3)=1      P1(76,4)=1 ...
C
                                CALL PISIP(P,N,M)
C     formiranje H-matrice
                                CALL HMAT(N,M,H)
      INDIND=0
500   DO 190 I=1,N
      DO 190 J=1,M
C
      JJ=J*MM-(MM-1)
      A(I,JJ)=H(I,J)
190   AI(I,J)=1
C
C     pocetni deo  A  je napunjen podmatricom  nxm  identicnom H
C     (POCETNI DEO SU STUPCI 1.26.51.76... PRVOG PODNIZA PODELE)
C     preostale podmatrice (po preostalim podnizovima) sirine m
C     (zadnja <m) pune se permutovanim redovima H na slucajan na-
C     cin, a onda provera det<>0
          DO 200 LL=2,MM
C         punjenje iza STUBACA 1 og podniza sirine M
```

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

```
      DO 310 K=1,N
310   PERM(K)=PERM(K)+1
      PRINT '(20I3)',(PERM(K),K=1,N)
C
      DO 320 I=1,N
      U=PERM(I)
      DO 320 J=1,M
C
      JJ=LL+J*MM-MM
C     zadnja podmatrica moze biti manja od M - zato ovaj  USLOV
C      USLOV=LL+J-1 ; IF(USLOV.GT.N)GO TO 320  - NIJE OVDE AKTIVIRANO
      BIT=0
      IF(BTEST(U,J-1)) BIT=1
      A(I,JJ)=BIT
320   CONTINUE
C
200             CONTINUE
      DO 606 U=1,N
      DO 606 V=1,N
606   MAT(U,V)=A(U,V)
C
      CALL REGULA(MAT,N,IJ)
      IF(IJ.EQ.0) GOTO 500
C
      CALL PISIH(A,N,N)
           PRINT *,' A ^'
           READ *,KLK
      CALL INVERZ(A,N,AI)
      CALL PISIH(AI,N,N)
                PRINT *,' AI *'
                     READ *,KLK
      CALL MNOMAT(A,P,H,N,M)
                     CALL PISIHT(H,N,M)
                PRINT *,' H ^'
      CALL KONTRA(H,N,M,IND)
      IF(IND.EQ.0) STOP 'kontrola H nije zadovoljena '
                READ *,KLK
C     obicna podela: s1=prvih m bitova ; s2=drugih m bitova u, itd.
C     specijalna podela SVAKI m. elemenat - m podnizova
C
C      m podnizova    - kontrola Hi matrica   i=2,N/m (prva H
C      matrica kontrolisana je pri I kontroli formirane A matrice
C
          DO 700 LL=2,MM
      DO 15 I=1,N
      DO 15 J=1,M
15     P(I,J)=0
      DO 16 J=1,M
16    P(LL+J*MM-MM,J)=1
C
      CALL MNOMAT(A,P,H,N,M)
      CALL PISIHT(H,N,M)
                PRINT *,' Hi = A*Pi     ^^^'
                PRINT *,' PROVERA MATRICE H(',LL,')'
      CALL KONTRA(H,N,M,IND)
      IF(IND.EQ.0) STOP 'kontrola H nije zadovoljena '
700         CONTINUE
C
```

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

```
      SUBROUTINE PERMUT(NIZOSN,OSN      ,IND)
C     ------------------------------------------------------
C     BAZA permutovanja OSN=broj elem. permut.
C     NIZOSN(1 do OSN) ; punjenje poc.postavke
C     uvecanje NIZOSN za po 1; kontrola da su svi rezlic. elem. i
C     da su elementi <=OSN ; UVECANJE preko broja R*4 => ograniceno
C     ------------------------------------------------------
      INTEGER*2 OSN,MM,NN,NIZOSN(200), IND
      INTEGER*4 R,RR,OST,RO ,KRAJ, RRR
C
      IF(IND.EQ.1) GOTO 410
      IND=1
      IF(OSN.GT.9) THEN
            PRINT *,' PROGRAM DOPUSTA SAMO OSN<10 '
            PAUSE
      END IF
C
      KRAJ=0
C     punjenje pocetne postavke - permutacije bez ponavlanja
      DO 110 MM=OSN,1,-1
      NN=OSN-MM+1
110   NIZOSN(NN)=MM-1
      R=NIZOSN(1)
      KRAJ=NIZOSN(OSN)
      RRR=1
      DO 111 MM=2,OSN
      RRR=RRR*10
      KK=OSN-MM+1
      NN=MM-1
      KRAJ=KRAJ+NIZOSN(KK)*RRR
      R=R+NIZOSN(MM)*RRR
111   CONTINUE
      PRINT '(10I3)',(NIZOSN(K),K=1,OSN)
      PRINT *,R,KRAJ
C
C     formiranje permutacija
400   RO=R
C     rastav na cifre i provera da su elementi razliciti
201   DO 210 I=1,OSN
      RR=RO/10
      OST=RO-RR*10
      IF(OST.GE.OSN) GOTO 410
      NIZOSN(I)=OST
210   RO=RR
C
      DO 300 I=1,OSN-1
      DO 300 J=I+1,OSN
      IF(NIZOSN(I).EQ.NIZOSN(J)) GOTO 410
300   CONTINUE
      RETURN
410   R=R+1
      IF(R.GT.KRAJ) STOP
      GOTO 400
```

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

```
      SUBROUTINE SPUNI(R,N,M,ADR)
C     punjenje slucajnih permutacija - P(N)
C     start generatora =R , M-samo za pretkorake, ADR-niz permut.
C     ------------------------------------------------------------
      INTEGER*4 R
      INTEGER*2 I,N,M, J ,ADR(200), NIZ(200),A
C
C     set KONTROLE istih
      DO 15 I=1,N
15    NIZ(I)=0
C     pretkoraci generatora
      DO 20 I=1,40
      R=ISHFT(R,1)
      IF(BTEST(R,3).NEQV.BTEST(R,31)) R=IBSET(R,0)
20    CONTINUE
C
C     punjenje ADR
10    DO 30 I=1,N
44    DO 40 J=1,M
      R=ISHFT(R,1)
      IF(BTEST(R,3).NEQV.BTEST(R,31)) R=IBSET(R,0)
40    CONTINUE
      A=MOD(R,N)
      IF(A.LT.0) A=(-1)*A
C     sprecavanje istih
      IF(NIZ(A+1).EQ.1) GO TO 44
      NIZ(A+1)=1
      ADR(I)=A
30    CONTINUE
      RETURN
      END



      SUBROUTINE REGULA(MAT,N,IND)
C     provera da li je matrica regularna
C     metod: svi elementi dijagonale <>0 dijagon,matrice
C
      INTEGER*2 MAT(200,200),N,IND,I,J,L,K,NN,MS
      A(I,J)=MAT(I,J)
30    CONTINUE
C
C     provera det(A)<>0 -  na dijadonali sve <>0
C     svodjenje na dijagonalni oblik
      IND=0
      DO 50 K=1,N
      IF(MAT(K,K).EQ.1) GOTO 55
C     izbor vodeceg elementa
      DO 80 L=K+1,N
      IF(MAT(L,K).NE.1) GOTO 80
C     zamena redaka
            DO 70 MS=1,N
            NN=MAT(L,MS)
            MAT(L,MS)=MAT(K,MS)
70          MAT(K,MS)=NN
      GOTO 55
```

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

```
      SUBROUTINE PISIT(MAT,N,M)
C     ispis matrice ali u transponovanom obliku
      INTEGER*2 MAT(200,200),N,M
      DO 40 J=1,M
      PRINT '(40I2)',(MAT(I,J),I=1,N)
40    CONTINUE
      RETURN
      END

      SUBROUTINE PISIP(MAT,N,M)
C     ispis specijalnih P matrica
      INTEGER*2 MAT(200,200),N,M
C     na osnovu P1 punjenje ostalih is skupa projekcija
C
      DO 20 I=1,N
      DO 20 J=M+1,N
20    MAT(I,J)=0
      DO 30 J=1,N-M
      DO 30 I=1,N-1
      IF(MAT(I,J).EQ.1) MAT(I+1,J+M)=1
30    CONTINUE
C     stampa
      IF(M.GT.5) GOTO 50
      DO 40 I=1,N
      PRINT '(5(5I2,5X))',(MAT(I,J),J=1,N)
40    CONTINUE
      RETURN
50    DO 44 I=1,N
      PRINT '(8I2)',(MAT(I,J),J=1,8)
44    CONTINUE
      RETURN
      END

      SUBROUTINE PISIH(MAT,N,M)
C     stampa u heksa formatu (Z2)
      INTEGER*2 MAT(200,200),N,M,IHEX, NIZ(8)
      DATA NIZ/4,5,6,7,0,1,2,3/
C
      DO 40 I=1,N
      IHEX=0
      DO 44 J=1,M,8
         DO 50 K=1,8
         IF(J+K-1.GT.M) GOTO 50
         IF(MAT(I,J+K-1).EQ.1) IHEX=IBSET(IHEX,NIZ(K))
50    CONTINUE
      PRINT '(1X,Z2\)',IHEX
      IHEX=0
44    CONTINUE
      PRINT '(A1)',' '
40    CONTINUE
      RETURN
      END
```

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

```
      SUBROUTINE PISIHT(MAT,N,M)
C     ispis matrice ali u transponovanom obliku
C     stampa u heksa formatu (Z2)
      INTEGER*2 MAT(200,200),N,M,IHEX, NIZ(8)
      DATA NIZ/4,5,6,7,0,1,2,3/
C
      DO 40 J=1,M
      IHEX=0
      DO 44 I=1,N,8
         DO 50 K=1,8
         IF(I+K-1.GT.N) GOTO 50
         IF(MAT(I+K-1,J).EQ.1) IHEX=IBSET(IHEX,NIZ(K))
50    CONTINUE
      PRINT '(1X,Z2\)',IHEX
      IHEX=0
44    CONTINUE
      PRINT '(A1)',' '
40    CONTINUE
      RETURN
      END

      SUBROUTINE MNOMAT(A,P,H,N,M)
C     H(N,M)=A*P
      INTEGER*2 A(200,200),P(200,200),H(200,200)
      INTEGER*2 M,N,I,J,K
C
      DO 10 J=1,M
      DO 10 I=1,N
      H(I,J)=0
C
      DO 20 K=1,N
      H(I,J)=H(I,J)+A(I,K)*P(K,J)
20    CONTINUE
      H(I,J)=MOD(H(I,J),2)
10    CONTINUE
      RETURN
      END

      SUBROUTINE INVERZ(A,N,A1)
C     Gaus-Zordanova metoda
      INTEGER*2 A(200,200),N, N2,A1(200,400)
C
      DO 10 I=1,N
      DO 10 J=1,N
      A1(I,J)=A(I,J)
10    CONTINUE
C
      N2=2*N
      N1=N+1
      DO 20 I=1,N
      DO 20 J=N1,N2
      A1(I,J)=0
      IF(J.EQ.N+I) A1(I,J)=1
20    CONTINUE
      PRINT *,' MATRICA A :'
```

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

```
      CALL ZORDAN(A1,N,N2,IND)
      GOTO(25,30),IND
25    PRINT *,' MATRICA A NEMA INVERZNU'
      RETURN
30    DO 35 I=1,N
      DO 36 J=1,N
36    A1(I,J)=A1(I,J+N)
35    CONTINUE
      RETURN
      END

      SUBROUTINE ZORDAN(A,N,M,IND)
      INTEGER*2 A(200,400),N,M
C
      DO 10 K=1,N
      K1=K+1
      IF(K.EQ.N) GOTO 20
      AMAX=ABS(A(K,K))
      L=K
      DO 30 I=K1,N
      IF(AMAX.GE.ABS(A(I,K))) GOTO 30
      AMAX=ABS(A(I,K))
      L=I
30    CONTINUE
      IF(L.EQ.K) GOTO 20
      DO 40 J=1,M
      P=A(K,J)
      A(K,J)=A(L,J)
40    A(L,J)=P
20    IF(A(K,K).EQ.0) GOTO 50
      DO 10 I=1,N
      IF(I.EQ.K) GOTO 10
      DO 70 J=K1,M
      A(I,J)=A(I,J)-A(I,K)/A(K,K)*A(K,J)
      A(I,J)=ABS(A(I,J))
      A(I,J)=MOD(A(I,J),2)
70    CONTINUE
10    CONTINUE
      IND=2
      DO 80 I=1,N
      J1=M-N
      DO 80 J=1,J1
80    A(I,N+J)=A(I,N+J)/A(I,I)
      RETURN
50    IND=1
      RETURN
      END
```

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

LITERATURA

[1] A.D.Wyner
"The wiretap chanel", Bell System Technical Journal, vol. 54, oktobar 1975., str. 1355-1387.

[2] A.B.Carleial, M.E.Hellman
"A Note on Winer's Wiretap Channel", IEEE Trans. on Information Theory, maj 1977,str. 387-390.

[3] R.Gallager
"Information Theory and Reliable Communication", Wiley, New York, 1968.

[4] Раймонд Г. Пиотровский
"Информационные измерения языка", Наука, Ленинград, 1968.

[5] Е.С.Венцель
"Теория вероватностей", Наука, Москва, 1964.

[6] Robert Ash
"Information Theory", Interscience, New York, 1965.

[7] W.Peterson
"Error correcting codes", John Wiley & Sons Inc., New York, London, 1961.

[8] M.Obradović, D.Lazić, J.Golić, M.Milosavljević, V.Šenk
"Zaštitno kodovanje sa statističkim prepoznavanjem oblika", Beograd, VINC, 1989.

[9] Milojko Koković
"Statističko-informacione karakteristike jezika i njihova primena u teoriji kodiranja", magistarski rad, Prirodno-matematički fakultet, Beograd, 1970.

[10] J.Željković
"O zasnivanju matematičke teorije informacija", magistarki rad, Prirodno-matematički fakultet, Beograd, 1972.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs