UNIVERZITET SINGIDUNUM

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

DOKTORSKE AKADEMSKE STUDIJE

STUDIJSKI PROGRAM: NAPREDNI SISTEMI ZAŠTITE

NOVA KLASA GENERATORA SLUČAJNIH NIZOVA ZASNOVANA NA ZVUČNOJ KARTICI

- doktorska disertacija -

Mentor: **Student:**

Mladen Veinović **Slaviša Nikolić, master**

Broj indeksa: 460049/2010

Beograd, 2016

UNIVERSITY OF SINGIDUNUM

DEPARTMANT OF POSTGRADUATE STUDIES

DOCTORAL STUDIES

PROGRAM: ADVANCED PROTECTION SYSTEMS

A NEW CLASS OF RANDOM SEQUENCE GENERATORS BASED ON A SOUND CARD

- doctoral dissertation -

Mentor:

Mladen Veinović

Student:

Slaviša Nikolić, master

Index number: 460049/2010

Belgrade, 2016

Podaci o mentoru i članovima komisije

Mentor:

Prof. dr Mladen Veinović, redovni profesor **Univerzitet Singidunum**

_____

Članovi komisije:

Prof. dr Mladen Veinović, redovni profesor **Univerzitet Singidunum**

_____

Prof. dr Milan Milosavljević, redovni profesor **Univerzitet Singidunum**

_____

Prof. dr Branko Kovačević, redovni profesor **Univerzitet u Beogradu, Elektrotehnički fakultet**

_____

Datum odbrane:

_____

Podaci o doktorskoj disertaciji

Naziv disertacije: **Nova klasa generatora slučajnih nizova zasnovana na zvučnoj kartici**

Rezime

Proces generisanja kvalitetnih nizova slučajnih brojeva je najosetljiviji i najvažniji činilac svakog kriptografskog sitema tako da način dizajna i provera karakteristika generatora zahtevaju pažljiv i studiozan pristup. Najveći uticaj na kvalitet generisanih nizova kod generatora slučajnih vrednosti zasnovanih na zvučnoj kartici imaju visina entropije izvora slučajnosti i primenjeni postupak postprocesiranja. Primenom ovog postupka postprocesiranja vrši se destilacija digitalizovanog oblika slučajnog analognog signala čiji je posledica dobijanje niza istinski slučajnih brojeva ravnomerne odnosno uniformne raspodele. Predmet ove disertacije je analiza postojećih i predstavljanje nove klase generatora slučajnih nizova zasnovane na zvučnoj kartici.

Nizovi slučajnih brojeva su nezaobilazni činioci širokog spektra oblasti, od kriptografije, simulacija, igara na sreću, uzorkovanja, donošenja odluka, medicine i estetike, pa sve do umetnosti. Najviše korišćen generator slučajnih vrednosti je generator pseudoslučajnih brojeva (PRNG). Generator pseudoslučajnih brojeva je matematički algoritam koji stvara deterministički, periodični niz brojnih vrednosti određenih početnim stanjem čiji je naziv SID. Generatori istinski slučajnih brojeva (TRNG) su, za razliku od PRNG, zasnovani na nedeterminističkim prirodnim pojavama poput zvučnih šumova, radioaktivnog raspadanja, termalnih šumova generisanih poluprovodnikom, termalnih šumova otpornika, fotoelektričnih efekata i raznih kvantnih fenomena, i njihov proizvod su neperiodični istinski slučajni brojevi.

Na zvučnim karticama, u cilju dobijanja što boljih slučajnih brojeva, vršena su mnogobrojna istraživanja. Većina ovih istraživanja koristila je pristupe koji su se zasnivali na potrebama PRNG-a ili njihovim konstrukcijama.

U ovoj disertaciji razvijen je pristup dobijanja istinski slučajnih bita zasnovan na zvučnoj kartici hardvera računarskih uređaja, koja se pobuđuje slučajnim signalima buke u životnoj sredini, i postprocesiranju odnosno destilaciji novim postupkom mešanja ulaznog niza i XOR-ovanja susednih bita (MiBiS&XOR).

Predstavljeni postupak post-procesiranja obezbeđuje jednostavno i efikasano razdvajanje i udaljavanje susednih bita ulaznog niza, između kojih postoji određena korelacija, a zatim u novodobijenom nizu XOR-ovanje susednih bita, smanjujući autokorelaciju, povećavajući

entropiju i redukujući bias niza izlaznih bita.

Ispitivanja sprovedena statističkim testovima slučajnosti pokazala su da ova klasa generatora ima odlične karakteristike i da u veoma kratkom vremenskom periodu generiše veliku količinu istinski slučajnih brojeva visokog kvaliteta slučajnosti.

U prvom delu disertacije (glave 2 i 3) izložena je teorijska osnova neophodna za razumevanje originalnih doprinosa izloženih u drugom delu. Iz tog razloga prvo su u glavi 2 u potrebnoj meri uvedeni pojmovi slučajnog procesa, slučajnog signala i stohastičkog izvora slučajnih signala, kao neophodnih činioca u procesu dobijanja nizova istinski slučajnih brojevaa zatim u glavi 3 osnove zvučnih kartica i šuma buke u životnoj sredini.

U drugom delu disertacije (glave 4 i 5) prikazani su originalni rezultati istraživanja. Prvo su u glavi 4 izloženi rezultati postignuti na razvoju novih postupaka dobijanja slučajnih nizova kao i osnovne karakteristike generatora istinski slučajnih brojeva. Detaljno je objašnjen princip rada generatora istinski slučajnih brojeva, klasifikacija i karakteristike, najnovija istraživanja i dizajni kao i faze u njegovom radu. Prikazane su, takođe, različite tehnike post-procesiranja, njihova efikasnost, prednosti i mane. U glavi 5 prikazani su rezultati primene nove destilacione tehnike. Posebno mesto zauzima značaj i razvoj novog postupka dobijanja istinski slučajnih nizova u cilju dobijanja generatora slučajnih brojeva koji su brzi, efikasni i jeftini a samim tim i pristupačni širokom auditorijumu. U okviru disertacije je posebna pažnja posvećena razvoju novih efikasnih postupaka dobijanja slučajnih nizova baziranih na korišćenju hardverskog potencijala personalnog desktop računaraskog sistema i novih tipova laptopava, tablet PC-a i smart telefonskih uređaja. Pokazano je da je prikazani sitem efikasan jer omogućava veoma brzo generisanje slučajnih vrednosti uz zadovoljavajuću nepredvidljivost i da je stoga, iako prevashodno namenjen u kriptografske svrhe, veoma pogodan za korišćenje u mnogim aplikacijama koje zahtevaju razne oblasti.

Ostvareni rezultati predstavljaju dobru podršku razvoju korišćenja hardverskog okruženja i sofverske osnove za dalji proces unapređenja generatora slučajnih nizova.

Ključne reči: Generator istinski slučajnih brojeva, miksovanje bita u koracima a zatim XOR-ovanje susednih bita, buka životne sredine, zvučna kartica, entropija, statistički testovi.

Information about the thesis

Title of thesis: **A new class of random sequence generators based on a sound card**

Summary

The process of generating high-quality series of random numbers is the most sensitive and most important factor of any cryptographic system so that the way of design and verification of the characteristics of generators require careful and studious approach. The greatest impact on the quality of generated sequences in random value generators based on the sound card have the height of the randomness source of entropy and the applied post-processing procedure. Using this postprocessing procedure, distillation of digitized form of random analog signal is done, with the result of obtaining a set of truly random numbers of uniform distribution.The subject of this dissertation is the analysis of existing and presentation of a new class of random sequence generators based on a sound card.

Sequences of random numbers are unavoidable factors of a wide range of areas, from cryptography, simulation, games of chance, sampling, decision-making, medicine and aesthetics, to the art. Most used random values generator is the pseudorandom number generator (PRNG). Pseudorandom number generator is a mathematical algorithm that creates a deterministic, periodic array of numerical values determined by the initial state under the name of SID. A true random number generator (TRNG) were, unlike the PRNG, based on non-deterministic natural phenomena such as sound noise, radioactive decay, thermal noise generated by semiconductor, thermal noise of resistors, photoelectric effects and a variety of quantum phenomena, and their products are non-periodic true random numbers.

On sound cards, in order to obtain the best possible random numbers, many researches have been carried out. Most of these researches have used the approaches that were based on the needs of the PRNGs or their structures.

In this dissertation an approach was developed in order to obtain true random bits based on the sound card of computer hardware, which is induced with random signal noise in the environment, and postprocessing (distillation) with a new process of mixing the input string and XOR-ing neighboring bits (Mibis & XOR).

The presented method of post-processing provides a simple and efficient separation and removal of adjacent bits of the input string, between which there is a correlation, then in the

newly obtained set, the XOR-ing of neighboring bits, reducing the autocorrelation, increasing entropy and reducing bias of output bits set.

Examinations conducted with statistical tests of randomness have shown that this class of generators has excellent characteristics and that in a very short period of time generates a large amount of true random number of high quality randomness.

In the first part of the dissertation (Chapters 2 and 3) a theoretical basis necessary for understanding the original contributions set out in the second part is presented. For this reason,firstly, in Chapter 2, to the extent necessary, concepts of random process, random signal and stochastic signal sources are introduced, as necessary factors in the process of obtaining a true random series of numbers and then in the Chapter 3 basics of sound cards and environmental noise signals.

The second part of the dissertation (Chapters 4 and 5) shows the original research results. First, in Chapter 4 the results achieved in the development of new methods of obtaining random sequences as well as basic characteristics of a true random number generators are presented. The working principle of a true random number generators, classification and characteristics, the latest research, designs and stages in his work are explained in detail. A variety of post-processing techniques, their effectiveness, advantages and disadvantages are also displayed. In Chapter 5 the results of application of the new distillation techniques are presented. A special place is occupied by the significance and development of the new process of obtaining true random sequences in order to obtain random number generators, which are fast, efficient and cheap and therefore accessible to a wide audience. Within the dissertation special attention is given to the development of new effective methods of obtaining random sequences based on the use of hardware potential of personal desktop systems and new types of lap-tops, tablets and smartphone devices. It is shown that an efficient system is presented because it allows rapid generation of random values with sufficient unpredictability and therefore, although intended for the cryptographic purposes, is very suitable for use in many applications that various fields require.

The achieved results represent a good use of support to the development of hardware and software-environment basis for further process improvements of random sequence generators.

Keywords: True Random Number Generator, Mixing Bits in Steps and XOR-ing of Adjacent Bits, Environmental noise, Sound card, Entropy, Statistical tests.

Spisak slika

Slika 2.1. *Ponašanje determinističkih prostoperiodičnih signala* *10*

Slika 2.2. *Slika 2.2. Prikaz talasnih oblika signala jednog izvora signala izmerenih instrumentom u različitim vremenskm intervalima* *10*

Slika 2.3. *Talasni oblici dva različita slučajna signala šuma* *11*

Slika 2.4. *Slučajni signal buke životne sredine korišćen u ovom eksperimentu* *13*

Slika 2.5. *Rezultati merenja osciloskopom signala iz četiri izvora šuma* *14*

Slika 2.6. *Grafički prikaz funkcije gustine raspodele uniformne slučajne promenljive koja ima parametre* $a=1$ *i* $b=4$ *29*

Slika 2.7. *Grafički prikaz funkcije gustine raspodele eksponencijalne slučajne promenljive čiji je parametar* $\lambda \in \{1,2\}\}$ *30*

Slika 2.8. *Grafički prikaz normalne raspodele čiji su parametri* $\mu=0$ *i* $\sigma \in \{1,2,3\}\}$ *31*

Slika 3.1. *Sferni i ravni zvučni talasi: a) lopta koja pulsira stvarajući sferne talase, b) stvaranje zvučnih talasa pomoću membrane* *43*

Slika 3.2. *Zvučni pritisak (p) i promene u vremenu* *43*

Slika 3.3. *Karakteristike jednog složenog zvuka a)Vremenski oblik signala složenog zvuka b)Frekvencijska karakteristika složenog zvuka* *43*

Slika 3.4. *Uticaj različitih temperatura i promene pravca prostiranja zvučnog talasa: a) tokom dana, b) u toku noći* *41*

Slika 3.5. *Refleksija i apsorcija jednog zvučnog talasa* *42*

Slika 3.6. *Zvučna PCI kartica računarskog sistema* *43*

Slika 3.7. *Studijski mikrofon* *49*

Slika 3.8. *Specijalni mikrofon sa talasovodom – često se naziva i puška mikrofon ili samo puška, zbog svog fizičkog oblika i karakteristika usmerenosti.* *50*

Slika 3.9. *Frekvencijska karakteristika diferencijalnih mikrofona* *51*

Slika 3.10. *Buka životne sredine* *55*

Slika 3.11. *Zvučni signal grmljavine* *56*

Slika 3.12. *Zvučni govorni signal jednog od učesnika razgovora* *57*

Slika 3.13. *Zvuk buke životne sredine izazvan zbirom različitih izvora buke* *58*

Slika 3.14. *Korekcija nivoa zvuka filtrima A, B i C.* *58*

Slika 3.15. *Podela ukupnog opsega signala na podopsege B* *61*

Slika 3.16. *Trodimenzionalni prikaz signala buke životne sredine* *61*

Slika 3.17. *Spektar signala buke dobijen primenom konstantnih filtara. Vrednost svake tačke dobijena je iz po jednog filtra* *62*

Slika 3.18. *Prikaz spektralne analize sa slike 3.17 u logaritamskoj razmeri* *63*

Slika 3.19. *Definisanje proporcionalnih frekvencijskih opsega* *64*

Slika 3.20. *Rezultati spektralne analize 1/3 oktavnim filtrima* *65*

Slika 3.21. *Prikaz rezultata oktavnih (gornja linija), tercnih (srednja linija) i linearnih (donja linija) spektara istog zvučnog signala* *66*

Slika 3.22. *Primeri predstavljanja proporcionalnih spektara zvučnog signala* *67*

Slika 3.23. *Primer spektrograma koji prikazuje deo zvuka. Uočljive su harmonijske komponente zvuka (horizontalne linije) i promene spektra u vremenu.* *68*

Slika 3.24. *Primer slapa signala zvuka. U pitanju je isti signal kao na slici 3.23* *68*

Slika 3.25. *Prikaz spektralne analize belog i roze šuma: a) spektri sa konstantnim opsezima b) spektri sa proporcionalnim opsezima.* *69*

Slika 3.26. *Merni lanac za merenje i analizu buke* *70*

Slika 3.27. *Standardizovane N krive* *72*

Slika 4.1. *Prikaz grafičke analize rezultata kod TRNG-a (levo) i PRNG-a (desno)* *8*

Slika 4.2. *Blok šema procesa rada generatora istinski slučajnih brojeva* *83*

Slika 4.3. *Dobijene vrednosti izlazne sekvence* m_{izlaz} *u odnosu na* m_{ulaz} *i N kod T flip-flopa* *89*

Slika 5.1. *Slučajni signali mešovite buke* *96*

Slika 5.2. *Šum na izlazu iz ADC-a* *97*

Slika 5.3. *Histogram šuma odnosno funkcije gustine verovatnoće amplituda* *98*

Slika 5.4. *Postupak destilacije mešanjem i XOR-ovanjem bita* *99*

Slika 5.5. *Grafičko predstavljanje ukupnog broja bita, stepena razdvajanja bita i novoubačenog broja bita u zavisnosti od koraka miksovanja* *102*

Slika 5.6. *Princip raspoređivanja bita i dobijanja izlaznog bitskog niza metodom MiBiS&XOR* *103*

Slika 5.7. *Postupak stvaranja slučajnih nizova u realnom vremenu* *104*

Slika 5.8. *Grafičko predstavljanje rezultata ispitivanja primenjenog MiBiS&XOR postupka korišćenjem buke miksovanog zvuka #5, zvuka sa žurke #4, zvuka iz podzemnog prolaza #3, zvuka iz prometne šetačke zone #1 i zvuka saobraćajne buke #2* *106*

Slika 5.9. *Grafički prikaz rezultata testiranja dobijenih različitim metodama* *108*

Slika 5.10. *Vrednosti entropije dobijene primenom različitih metoda u poređenju sa entropijom dobijenom metodom XOR10* *109*

Slika 5.11. *Grafičko predstavljanje apsolutnih srednjih vrednosti autokorelacija miksovanog signala buke pre i nakon post-procesiranja prikazanim postupcima* *110*

Slika 5.12. *Komparativna analiza iskorišćenja ulaznih bita* *110*

Slika 5.13 *Prikaz uniformne raspodele slučajnih brojeva matrice [80x100] sa vrednostima u rasponu od 0 do 1* *112*

Spisak tabela

Tabela 2.1. *Određivanje t za dati nivo poveranja* *23*

Tabela 3.1. *Vrednosti podataka za praktičnu primenu PCM-a* *47*

Tabela 3.2. *Vrednosti standardnih centralnih frekvencija proporcionalnih filtara* *65*

Tabela 3.3. *Maksimalni dozvoljeni nivoi buke u životnoj sredini* *72*

Tabela 3.4. *Dozvoljeni nivoi buke u životnoj sredini izraženi N kriterijumima i u dBA* *73*

Tabela 3.5. *Dozvoljeni nivoi buke (pri kojima postoji mogućnost obavljanja određenih delatnosti) izraženi N kriterijumima i u dBA* *73*

Tabela 4.1. *Pregled osnovih razlika karakteristika između TRNG-a i PRNG-a* *79*

Tabela 4.2. *Prikaz rada Nojmanovog korektora, tehnike pariteta niza i XOR tehnike* *88*

Tabela 5.1. *Prikaz rasporeda nizova bita dobijenih u prvih pet koraka miksovanja* *100*

Tabela 5.2. *Ukupan broj bita u zavisnosti od broja koraka, broj novoubačenih bita u određenom koraku i stepen razdvajanja bita posle određenog koraka miksovanja* *101*

Tabela 5.3. *Rezultati ispitivanja različitih uzoraka zvučnog signala buke u životnoj sredini posle primenjenog postupka MiBiS&XOR* *105*

Tabela 5.4 *Rezultati testiranja dobijeni primenom različitih metoda post-procesiranja korišćenjem slučajnog signala buke životne sredine (#5)* *107*

Tabela 5.5. *Autokorelacija i bias* *109*

Tabela 5.6. *Brzine proizvodnje bita TRNG-a korišćenjem različitih metoda destilacije* *111*

S A D R Ž A J

1. UVOD 1

2. SLUČAJNI NIZOVI 7

2.1. SLUČAJNI BROJEVI 8

2.1.1. Osnove slučajnih signala 9

2.1.2. Korelacina svojstva slučajnog signala 14

2.1.3. Karakteristike korelacionog spektra slučajnog signala 16

2.2. SLUČAJNI NIZOVI I SLUČAJNI PROCESI 18

2.2.1. Statistička metoda 21

2.2.2. Definisanje tačkastih ocena parametara 21

2.2.3. Određivanje intervalnih ocena parametara 22

2.2.4. Načini testiranja statističkih hipoteza 23

2.2.4.1. Provera hipoteza parametarskim testovima 24

2.2.4.2. Provera hipoteza neparametarskim testovima 25

2.2.5. Veza entropije i informacije 25

2.3. TEORIJA VEROVATNOĆE U FUNKCIJI SLUČAJNOSTI 26

2.3.1. Osnovne karakteristike slučajnosti i verovatnoće 26

2.3.2. Pregled najčešćih apsolutno neprekidnih raspodela verovatnoće slučajnih promenljiva 29

2.3.2.1. Uniformna raspodela slučajnih promenljiva 29

2.3.2.2. Eksponencijalna raspodela slučajnih promenljiva 30

2.3.2.3. Normalna raspodela slučajnih promenljiva 31

3. ZVUČNA KARTICA I ZVUK BUKE U ŽIVOTNOJ SREDINI 32

3.1. ZVUČNI TALASI 33

3.1.1. Zvučni pritisak 34

3.1.2. Talasna dužina 35

3.1.3. Intenzitet zvuka 36

3.1.4. Prost i složen zvuk 37

3.1.5. Istovremeno zračenje više izvora 38

3.1.6. Slabljenje zvuka 39

3.1.7. Difrakcija i refrakcija 40

3.1.8. Koeficijenti refleksije i apsorpcije 41

3.2. ZVUČNA KARTICA 42

3.2.1. Vrste, tipovi i priključci zvučnih kartica 43

3.2.2. MIDI protokol 44

3.2.3. Digitalni zvuk i formati zvučnih zapisa 45

3.2.4. Impulsno-kodna modulacija PCM (Pulse Coded Modulation) 47

3.2.5. Ograničenja koja se odnose na frekvencijski opseg ... *47*
3.2.6. Ograničenje dinamike ... *48*
3.2.7. Mikrofoni ... *49*
3.2.7.1. Faktor elektroakustičkog pretvaranja (osetljivost mikrofona) ... 50
3.2.7.2. Dinamički opseg mikrofona ... 51
3.2.7.3. Usmerenost mikrofona ... 52
3.2.7.4. Akustička i električna podela mikrofona ... 52
3.3. BUKA U ŽIVOTNOJ SREDINI ... 55
3.3.1. Vrste i tipovi buke ... *56*
3.3.2. Izvori i načini prostiranja buke u životnoj sredini ... *57*
3.3.3. Merenje nivoa i spektra buke životne sredine ... *58*
3.2.3.2. Nivo i spektar buke životne sredine ... 59
3.2.3.3. Karakteristike zvuka buke u frekvencijskom domenu ... 60
3.2.3.4. Primeri karakterističnih spektralnih oblika zvučnog signala ... 69
3.2.3.5. Instrumenti za merenje buke životne sredine ... 70
3.2.3.6. Dozvoljeni nivoi buke životne sredine ... 71
4. GENERATORI SLUČAJNIH NIZOVA ... 74
4.1. GENERISANJE SLUČAJNIH BROJEVA ... 75
4.1.1. Tipovi generatora brojeva slučajnih vrednosti ... *77*
4.1.2. Razlike između TRNG-a i PRNG-a ... *79*
4.1.2.1. Klasifikacija generatora istinski slučajnih brojeva ... 80
4.1.2.2. Potreba za generatorima istinski slučajnih brojeva ... 81
4.1.2.3. Bazna zasnovanost dizajna generatora istinski slučajnih brojeva ... 81
4.2. POSTUPAK DOBIJANJA ISTINSKI SLUČAJNIH BROJEVA ... 82
4.2.1. Prvi deo procesa rada generatora istinski slučajnih brojeva ... *83*
4.2.2. Drugi deo procesa rada generatora istinski slučajnih brojeva ... *84*
4.2.2.1. Entropija generatora slučajnih brojeva ... 85
4.2.2.2. Bias ... 85
4.2.2.3. Autokorelacija niza slučajnih brojeva ... 86
4.2.2.4. Različite tehnike post-procesiranja ... 87
4.3. ISPITIVANJE SLUČAJNOSTI NIZOVA SLUČAJNIH BROJEVA ... 89
4.3.1. Statistički testovi slučajnosti ... *91*
4.3.1.1. Test frekvencija (monobitski test) ... 91
4.3.1.2. Test serija (dvo bitski test) ... 92
4.3.1.3. Poker test ... 92
4.3.1.4. Ran test ... 92
4.3.1.5. Autokorelacioni test ... 93
4.3.1.6. Mauerov univerzalni test slučajnosti ... 93
4.3.1.7. Ostali važni testovi slučajnosti ... 93
- Test za određivanje približne entropije ... 93
- Test najdužih uzastopnih ponavljanja jedinica u bloku ... 94
- Test podjednake učestalosti u bloku ... 94
- Test preklapanja uzoraka ... 94

- Test uzastopnog ponavljanja istog bita u nizu 94
- Test sa diskretnom Furijeovom transformacijom 94
- Test slučajnog kumulativnog zbira 94

5. PRIMENA METODE MIBIS&XOR U POSTUPKU DESTILACIJE SLUČAJNIH NIZOVA 95

5.1. POSTUPAK MEŠANJA BITA SLUČAJNOG NIZA 96

5.2. UPOREĐIVANJE REZULTATA SA POZNATIM METODAMA POST-PROCESIRANJA 107

5.3. DISKUSIJA DOBIJENIH REZULTATA 111

6. ZAKLJUČAK 113

Naučni doprinosi 114

Pravci budućih istraživanja 115

7. LITERATURA 116

Prilog *124*

Izvorni kod MiBiS&XOR algoritma u C# programskom jeziku *124*

1 UVOD

Današnje doba potencira red i potrebu ljudi za uvođenjem nekakvog reda u svojim životima, tako da deluje možda malo čudno što je kao tema ove disertacije izabrana sasvim suprotna problematika – slučajnosti i primena nereda ili drugačije posmatrano – haos.

Ovaj haos, neverovatno međutim nepobitnim činjenicama dokazano, svojom velikom primenom utiče na mnoge segmente naših života. Njegov uticaj je dominantan u najnaprednijim i najzahtevnijim razvojnim oblastima gde se primenjuje u cilju predviđanja svih mogućih uticaja, posledica i rešenja, sprovođenjem simulacija, u eksperimentima, medicini, kao i u kriptografiji.

Nizovi slučajnih brojeva su nezaobilazni činioci širokog spektra oblasti, od kriptografije [1], simulacija [2], igara na sreću [3], uzorkovanja [4], donošenja odluka, medicine i estetike [5], pa sve do umetnosti.

U današnjem svetu komunikacija postoji stalna potreba za povećanjem bezbednosti pri prenosu informacija. U cilju obezbeđivanja sigurne komunikacije, korišćenjem savremenih sistema komunikacije, podatke je potrebno šifrovati. Održavanje bezbednosti kriptografskog sistema ne postiže se tajnošću postupka šifrovanja nego čuvanjem tajnog ključa. Očuvanje tajnosti ključa postiže se korišćenjem kvalitetnih, nepredvidljivih nizova slučajnih brojeva. Zajednička karakteristika kriptografskih sistema je proizvodnja ključeva slučajnim procesom, pa otud i potreba u kriptografiji za generatorima slučajnih brojeva [6].

Pouzdane slučajne vrednosti moguće je jedino dobiti iz slučajnih prirodnih pojava i situacija sa nepredviljivim rezultatima, (npr. slučaj bacanja simetričnog novčića). U praksi se međutim primenjuju i fizički i aplikativani postupci stvaranja slučajnih vrednosti kojima se dobijaju brojevi većeg ili manjeg kvaliteta slučajnosti. Za proveru slučajnosti nizova brojeva koriste se skupovi statističkih testova koji proveravaju određene karakteristike slučajnosti posmatranih nizova brojeva. Na osnovu rezultata testiranja donosi se zaključak da li nizovi zadovoljavaju karakteristike slučajanosti koje se očekuju od nizova slučajnih brojeva.

Nizove slučajnih brojeva proizvode, stvaraju ili generišu generatori slučajnih brojeva. Ovi generatori slučajnih brojeva se dele na dve vrste i to na generatore istinski slučajnih brojeva TRNG (true random number generator) i generatore pseudoslučajnih brojeva PRNG (pseudo-random number generator). Generator istinski slučajnih brojeva za svoj rad koristi prirodne pojave koje su slučajne, tako da su i njegove generisane vrednosti istinski slučajne, dok pseudo-slučajni generatori koriste računarske postupke za stvaranje nizova prividnih slučajnih brojeva, čije vrednosti se ustvari posle određenog vremena ponavljaju, i zato se zovu pseudo-slučajni.

Generalno, gde je neophodno dati prvenstvo nepredvidljivosti, fizički generator koji generiše istinski slučajne brojeve pogodniji je od generatora pseudoslučajnih vrednosti.

Najčešće korišćeni generator slučajnih vrednosti je ipak generator pseudo-slučajnih brojeva. Na PRNG-ima su obavljena mnoga istraživanja [7]. Generator pseudoslučajnih brojeva je matematički algoritam koji stvara deterministički, periodični niz brojnih vrednosti određenih početnim to jest inicijalnim stanjem čiji je naziv SID [8]. Šenonova entropija izlaza zavisi od entropije SID-a i nikada je ne može nadmašiti. Po definiciji ovakvi generatori nisu dokazivo slučajni. Reproduktivnost PRNG-a, to jest mogućnost ponovnog generisanja iste izlazne sekvence, ima velike prednosti kod simulacija. Sa druge strane, njegova karakteristika zavisnosti entropije i način izbora SID-a predstavljaju prepreku njegovoj univerzalnoj eksploataciji. Ove generatore za svoj rad koriste mnoge aplikacije. Ali se dešava i to, da za neke slučajeve, generisane vrednosti ne ispunjavaju zahtevane vrednosti statističkih karakteristika slučajnosti. U ovakvim situacijama, npr. u kriptografiji ili igrama na sreću, oni se zamenjuju generatorima istinski slučajnih brojeva.

TRNG generatori su, za razliku od PRNG, zasnovani na nedeterminističkim prirodnim pojavama poput zvučnih šumova [9], radioaktivnog raspadanja [10], termalnih šumova generisanih poluprovodnikom [11], termalnih šumova otpornika [12], fotoelektričnih efekata i raznih kvantnih fenomena [13]. Haotično ponašanje uzrokovano ovakvim pojavama može se iskoristiti kao izvor entropije u dizajnu TRNG-a. Signale takvih prirodnih pojava najčešće treba pojačati, izvršiti njihovu A/D konverziju i digitalno ih očitati, ili se koristi neki drugi način prikupljanja zavisno od fizičke prirode signala.

Istinski slučajani brojevi se dobijaju iz istinski slučajnog bitskog niza u kome su biti nezavisni i nepristrasni. Pošto se slučajni brojevi koriste u različite svrhe, postavljaju se različiti zahtevi koji se odnose na kvalitet generisane sekvence. Na primer, kod aplikacija za simulacije obično je dovoljno da su ispunjeni uslovi nezavisnosti brojeva i ravnomernaraspodela. Međutim, u kriptografiji je jedan od glavnih zahteva nemogućnost pogađanja sledećeg broja u nizu. Kriptosistemi visokog stepena bezbednosti ne mogu se zamisliti bez TRNG-a koji predstavljaju fundamentalne blokove takvih sistema osiguravajući svojim kvalitetom bezbednost ključa a samim tim i sigurnost celog sistema [14].

Možda je najkritičnija komponenta TRNG-a entropija izvora jer ona značajno određuje entropiju izlaznog niza. Sa druge strane, jasno je da neki fizički izvori, na primer atmosferski šum ili nuklearno raspadanje, nisu uvek održivi i pristupačni, osim za prilično ograničene aplikacije ili online distribucione servise. Određivanje raspoložive entropije i njenih tačnih statističkih osobina kao i ispitivanje dugoročnih efekata koji mogu izazvati pogoršanje kvaliteta entropije izvora su sledeći važni zadaci kod određivanja dizajna TRNG-a. Međutim, iako su

mnogobrojne aktivne monitoring tehnike za detekciju kvarova na raspolaganju, suptilnije greške je u praksi vrlo teško otkriti i predvideti.

Za postizanje dobrog kvaliteta TRNG-a potrebna je i primena post-procesne obrade, premda postoje dizajni kod kojih to nije neophodno (na primer TRNG-i bazirani na kvantnim fenomenima). Primarni cilj primene post-procesiranja je eliminisanje pristrasnosti ili međuzavisnosti u entropiji izvora ili mehanizmu ekstraktovanja [15]. Sekundarni cilj, koji je dosta dobio na značaju zbog aktivnih direktnih i bočnokanalnih zlonamernih napada, je da se obezbedi otpornost na promene u okruženju i falsifikovanje od strane potencijalnih protivnika [16]. Dobra strana ovih generatora je što se generisane vrednosti ne ponavljaju, odnosno nemaju periodične karakteristike. Mana im je brzina generisanja koja je uslovljena A/D konverzijom ali i potreba za preciznim pojačavačem koji će detektovati i pojačati signal što povećava potrošnju. Oni ustvari koriste slučajnosti prirodnih fizičkih procesa, za koje se veruje da se ponašaju na nedeterministički način, što ove generatore čini boljim kandidatima za generisanje istinski slučajnih brojeva.

Do sada je predložen veliki broj dizajna TRNG-a [18]. Ovi projekti se značajno razlikuju po izboru izvora entropije ali i po načinu primene tehnike postprocesiranja. Svaki dizajn ima svoje prednosti i mane. Neke od ovih karakteristika se odnose na performanse a neke na bezbednost. Sa praktične tačke gledišta od suštinskog je značaja da TRNG-i budu dizajnirani na bazi jeftinog raspoloživog procesa. Štaviše, veoma je poželjno da se za dizajniranje TRNG-a koriste isključivo tehnička rešenja digitalnog tipa. Međutim, procena kvaliteta dizajna TRNG-a nije lak zadatak. Ipak, primarni cilj procene kvaliteta jeste utvrđivanje entropije po slučajnom bitu ili tačnije dobitak od entropije po slučajnom bitu [25].

TRNG-i se mogu pohvaliti mnogim prednostima u poređenju sa PRNG-ima. Prva prednost odnosi se na karakteristiku nepredvidljivosti što za posledicu ima dobijanje boljih slučajnih vrednosti. Druga prednost TRNG-a je nepostojanje periodičnosti, što je od izuzetne važnosti kod šifrovanja. Međutim, zbog prirode nedeterminističkih izvora TRNG-i su veoma osetljivi na neželjene determinističke izvore buke, uključujući buku napajanja, varijacije temperature a u ekstremnim slučajevima i na zlonamerno izazvane napade buke.

U ovoj disertaciji, u cilju dobijanja nizova istinski slučajnih brojeva koji ispunjavaju sve potrebne karakteristike slučajnosti, opisan je postupak korišćenja zvučne kartice koja je sastavni deo osnovnog hardverskog potencijala personalnog desktop računaraskog sistema i novih tipova laptopava, tablet PC-a ili smart telefonskih uređaja, koja se slučajnim analognim signalima buke u životnoj sredini pobuđuje koristeći mikrofon. Vrednosti odmeraka dobijene velikom

frekvencijom odmeravanja imaju nedovoljno dobre korelacione karakteristike, jer se odmeravaju kontinualni signali čije se amplitude ne menjaju dovoljno brzo u odnosu na frekvenciju odmeravanja. Iz tog razloga je bila neophodna primena postupka destilacije, čiji je primenjeni princip rada takođe prikazan u ovom radu i koji se izvodi mešanjem bita u koracima a zatim XOR-ovanjem susednih bita (MiBiS&XOR). Posledice primene ovog postupka su dobijanje niza kod koga je smanjena korelacija između bita, smanjen bias a povećana entropija Statistički testovi slučajnosti, iako je slučajnost nemoguće u potpunosti dokazati, nakon ispitivanja minimalno 1 Mbita elemenata niza korišćenih za svaki uzorak potvrdili su odličan kvalitet TRNG-a odnosno veoma dobre karakteriske slučajnosti generisanih nizova.

Disertacija je organizovana na sledeći način. U uvodnom delu doktorske disertacije istaknuta je aktuelnost teme i izvršena kratka analiza do sada objavljenih rezultata u ovoj oblasti. Ukratko su navedene karakteristikegeneratora istinski slučajnih brojeva, princip rada, potreba za slučajnim brojevima kao i najčešće oblasti korišćenja. Naglašene su prednosti ovakvih generatora u odnosu na generatore pseudoslučajnih brojeva kao i njihove razlike. Poseban osvrt napravljen je na različite dizajne generatora istinski slučajnih brojeva, njihove specifičnosti, karakteristike, mane i procene kvaliteta. U nastavku je ukratko objašnjen princip radanove klase generatora slučajnih nizova zasnovanoj na zvučnoj kartici računara i ukazano je na pozitivne rezultate ispitivanja karakteristika istinski slučajnih brojeva dobijenih ovom novom metodom.

U prvom delu drugog poglavlja date su osnovne karakteristike šuma sa kojim se srećemo na ulazu generatora istinski slučajnih brojeva sa naglaskom na slučajneprocesepririodnih fizičkih izvora slučajnosti. Drugi deo ovog poglavlja daje opis karakteristika slučajnih signala i njihovo matematičko predstavljanje. Pažnja je posvećena teoriji verovatnoće sa pregledom apsolutno neprekidnih raspodela neophodnih za razumevanje procesa rada generatora istinski slučajnih nizova. Pored toga uveden je pojam entropije kao mere neizvesnosti i dat je opis entropije složenih sistema. Posebna pažnja je posvećena uvođenju pojma stohastičkih izvora zračenja, kao izvora slučajnosti i karakteristikama slučajnih signala.

U trećem poglavlju izložena je teorijska osnova slučajnog signala šuma buke u životnoj sredini a opisana je i struktura hardverskih komponenata korišćenih u ovom radu, od kojih su svakako najvaznije zvučna kartica i mikrofon. Detaljno su prikazane karakteristike zvuka buke u životnoj sredini u frekvencijskom domenu a obrađeni su i nivoi buke kao i instrumenti za merenje buke.

U naredna dva poglavlja prikazani su originalni naučni rezultati istraživanja. Prvi deo četvrtog poglavlja odnosi se na generatore istinski slučajnih brojeva, njihovu klasifikaciju, potrebu za generatorima istinski slučajnih brojeva i njihove najnovije dizajne. Pokazano je da su razvijeni i primenjeni modeli generatora istinski slučajnih brojeva efikasniji od najčešće korišćenih aplikativnih generatora pseudoslučajnih brojeva [48] i da je njihova upotreba nezamenljiva u jakim kriptografskim i kriptoanalitičkim izazovima. U drugom delu ovog poglavlja prikazan je princip rada generatora istinski slučajnih brojeva kao i faze u njegovom radu. Prikazane su, takođe, različite tehnike post-procesiranja, njihova efikasnost, prednosti i mane.

Peto poglavlje predstavlja centralni deo disertacije u kome je prikazan najveći broj ostvarenih naučnih doprinosa. U prvom delu ovog poglavlja prikazan je novi način poboljšavanja karakteristika slučajnog niza dobijenog na izlazu ADC konvertora zvučne kartice računara mešanjem bita u koracima čiji rezultat predstavlja odličnu osnovu za drugi deo post-procesiranja koji se izvodi XOR-ovanjem susednih bita u novodobijenom nizu slučajnih bita. U drugom delu prikazani su rezultati dobijeni primenom metode MiBiS&XOR, provera tih rezultata primenom statističkih testova slučajnosti i poboljšanja koja se primenom ove nove metode dobijaju.Posebno mesto zauzima značaj i razvoj novog postupka dobijanja istinski slučajnih nizova u cilju dobijanja generatora slučajnih brojeva koji su brzi, efikasni i jeftini a samim tim i pristupačni širokom auditorijumu. Pokazano je da je prikazani sitem efikasan jer omogućava brzo generisanje slučajnih vrednosti uz zadovoljavajuću nepredvidljivost i da je stoga, iako namenjen u kriptografske svrhe, veoma pogodan za primenu u aplikacijama raznih oblasti od simulacija do igara na sreću.

Šesto poglavlje sadrži zaključke o najvažnijim naučnim rezultatima predstavljenog rada i smernice za dalja istraživanja u ovoj oblasti.

Na kraju disertacije (sedmo poglavlje), dat je pregled literature koja je korišćena za naučno-istraživački rad i pisanje same disertacije a u prilogu je dat i originalni kod algoritma predstavljene metode post-procesiranja.

2 SLUČAJNI NIZOVI

Ne postoji značajna razlika između istinski slučajnih podataka kao što su istinski slučajni biti, istinski slučajne sekvence bita, istinski slučajni brojevi ili istinski slučajne sekvence brojeva. Slučajna sekvenca bita može biti tako konstruisana nizanjem slučajnih bita. Slučajni broj iz intervala [*0, n*] može se konvertovati iz slučajne sekvence dužine $\lceil \log_2 n \rceil + 1$ (novu sekvencu treba uvek koristiti kada je *n* prekoračeno). Slučajna sekvenca brojeva može tako biti konstruisana nizanjem slučajnih brojeva. Shodno tome, ne postoji značajna razlika između odgovarajućih generatora ovakvih tipova slučajnih podataka.

Tumačenje slučajnog binarnog niza najlakše se može predstaviti rezultatom koji se dobija kada se baci novčić čije dve strane pisma i glave predstavljaju istu verovatnoću rezultata (0 i 1) približne vrednosti 0,5. Ovo je primer savršenog generatora s obzirom na to da su slučajne vrednosti rezultata ravnomerno raspoređene odnosno imaju uniformnu raspodelu. Što se tiče generisanja elemenata niza oni su statistički nezavisni jedni od drugih i ne postoji mogućnost predviđanja narednih vrednosti niza, nezavisno od broja prethodno generisanih vrednosti.

Na osnovu gore navedenog obrazloženja, može se smatrati da po svojoj prirodi, slučajni nizovi (sekvence) predstavljaju nizove slučajnih brojeva.

2.1. Slučajni brojevi

Slučajni brojevi su brojevi koji se generišu slučajno i čije vrednosti ne možemo predvideti. Na osnovu toga se niz slučajnih brojeva može definisati kao niz brojeva u kome se učestalost pojave određenog broja može unapred predvideti ali se ne može predvideti mesto kao ni raspored tog broja jer se brojevi ređaju bez bilo kakve zavisne zakonitosti.

Računarski sistemi i uređaji najčešće proizvode brojeve koji su pseudoslučajni, odnosno koje je moguće predvideti iz razloga njihove prirode nastanka koja je bazirana na matematičkim algoritmima. Karaktetistično za nizove ovih brojeva je i to da se posle određenog vremena ponavljaju što znači da poseduju svojstvo periodičnosti.

Međutim, postoji i vrsta generatora istinski slučajnih brojevnih vrednosti koji brojeve slučajnih vrednosti formiraju na osnovu vrednosti dobijenih iz slučajnih fizičkih procesa. Neki

od jednostavnijih primera su vremenske razlike pri pritiskanju dva tastera tastature ili promene koordinata pri pomeranju miša. Međutim, mora se biti pažljiv pri izboru izvora slučajnosti. Dobar broj računara poseduje aplikacije koje memorišu prethodno pritiskanje tastera, tako da to podrazumevaju jednim pritiskom, gubeći element slučajnosti. Mnogo bolji primeri su generatori istinski slučajnih brojeva na bazi atmosferskog šuma, detektovanja raspada radioaktivnih elemenata, termalnih šumova kod poluprovodnika i otpornika, fotoelektričnih efekata ili raznih kvantnih fenomena, kao i novi primeri generisanja istinski slučajnih brojeva poput onih koji koriste fotografije sa mehurićima lava lampe [26].

Karakteristika ovih istinski slučajnih brojeva je da im je reprodukcija nemoguća, periodično se ne ponavljaju, brzina dobijanja im je manja u odnosu na pseudoslučajne brojeve a proces njihovog kreiranja zahteva posebnu opremu.

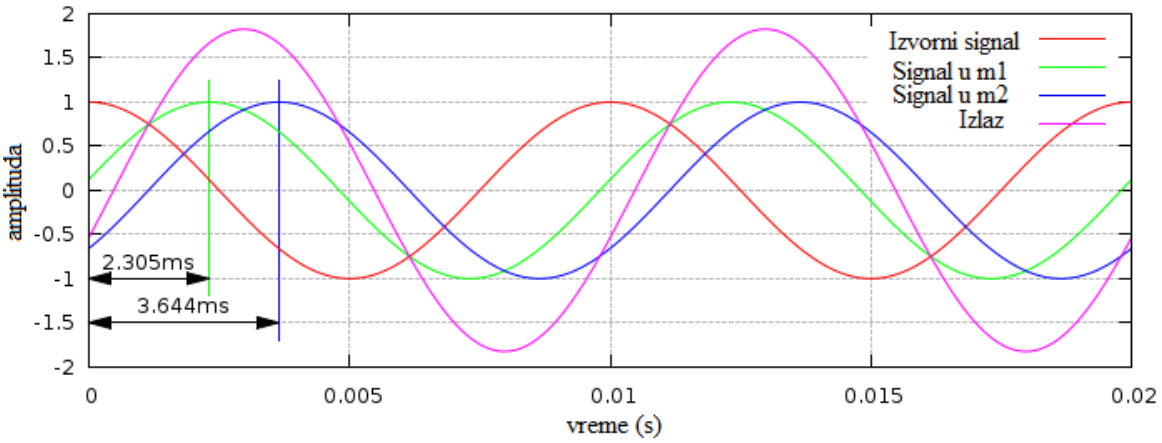
Mada se stiče utisak da se generatori slučajnih signala odnosno slučajnih impulsa razlikuju u svojstvima od generatora slučajnih bita i generatora slučajnih brojeva i da se radi o potpuno drugačijim vrstama generatora, tu prosto nema istine. Slučajne brojeve lako dobijamo grupisanjem bita a koji se opet dobijaju na osnovu slučajnih impulsa.

Velika potreba za slučajnim brojnim vrednostima primetna je posebno u kriptografiji. Zajednička karakteristika svih kriptografskih sistema je potreba generisanja ključa slučajnih svojstava. Veliki broj kriptografskih protokola, autentifikacionih protokola kao i protokola na osnovu kojih se generišu digitalni potpisi su korisnici istinski slučajnih ili pseudoslučajnih brojeva. Kriptografski slučajni brojevi moraju biti statistički slučajni i nepredvidivi.

Slučajni brojevi se kod generatora istinski slučajnih brojeva dobijaju deskretizacijom slučajnog kontinualnog signala i digitalizacijom tih diskretnih vrednosti, odnosno očitavanjem bita diskretizovanih signala.

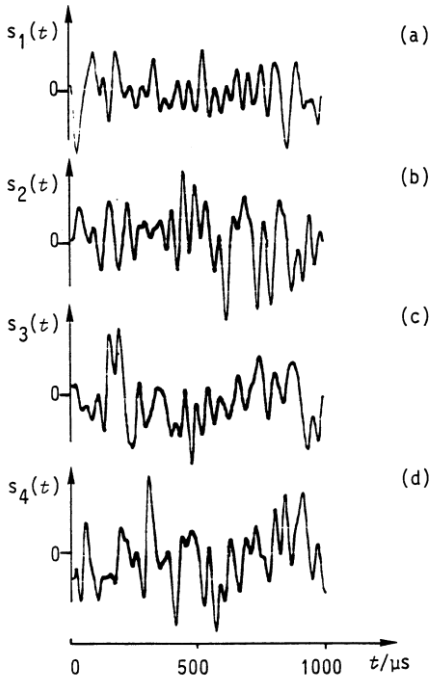
2.1.1. Osnove slučajnih signala

Odavno je poznato da deterministički izvori slučajnosti emituju signale koji su poznati u toku vremena, odnosno signale koji mogu biti opisani funkcijama zavisnosti koje određuju u bilo kom trenutku vremena najvažnije karakteristike signala, što se može videti na slici 2.1. Za razliku od determinističkih izvora u prirodi se vrlo često sreću i izvori zračenja čiji način emitovanja signala nije poznat i čije su funkcije opisivanja signala veoma složene da bi se mogle opisati klasičnim načinom. Ovo je slučaj takozvanih slučajnih pojava, izvora i signala.



Slika 2.1. *Ponašanje determinističkih prostoperiodičnih signala*

Mada se funkcionalni oblik slučajnog signala ne može egzaktnim načinom opisati, moguće je matematičkim funkcijama opisati njegovu srednju vrednost odnosno odrediti njegove verovatne karakteristike koristeći se funkcijama gustine verovatnoća.



Slika 2.2. *Prikaz talasnih oblika signala jednog izvora signala izmerenih instrumentom u različitim vremenskm intervalima [27]*

Predstavljeni izvori prikazanih signala predstavljaju osnovne izvore slučajnosti. Slika 2.2 prikazuje talasne oblike signala u vremenu istog izvora signala izmerenih pomoću osciloskopa u četiri različita vremenska trenutka. Primetno je da mada potiču iz jednog izvora oblici signala su različiti za različite vremenske intervale. Zato se može smatrati da koristeći vremenske, izvornog oblika direktne izmerene, vrednosti signala slučajnog izvora bez njihovog dodatnog obrađivanja ne možemo dobiti korisne informacije kojima bi opisali karakteristične parametre slučajnih

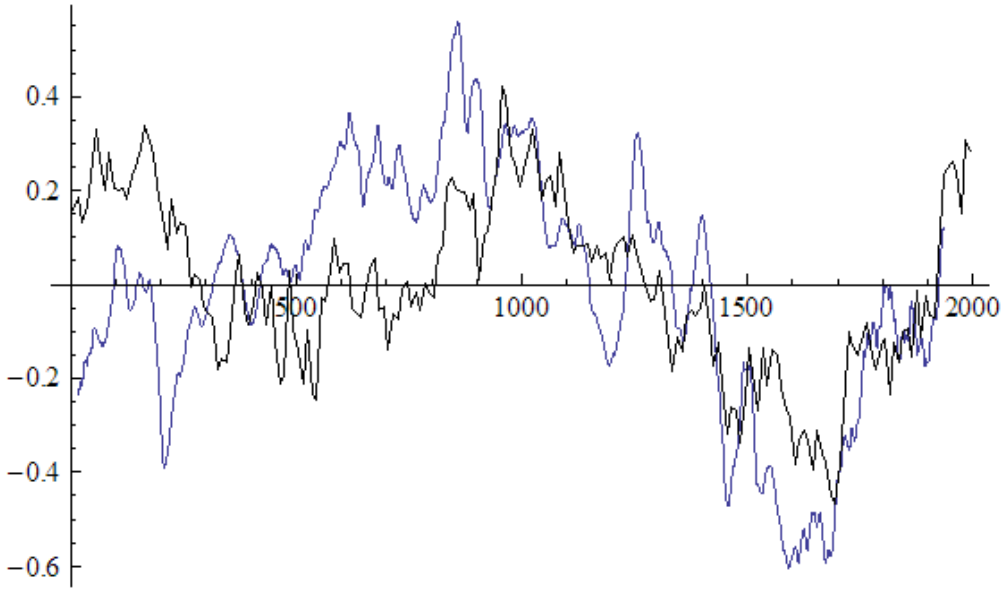
signala. Mnogostruko korisnija informacija, kojom se može opisati karakteristika slučajnog signala predstavlja parametar srednje vrednosti signala u vremenu, koji se dobija dodatnim obradama vrednosti koje su već izmerene. Zato se u cilju karakterizacije slučajnog najčešće upotrebljava veličina pod nazivom srednja kvadratna vrednost signala $s(t)$ nekog vremenskog intervala konačne dužine T i vremenskog centra intervala u trenutku t_1.

$$\bar{s}^2(t,t_1,T)=\frac{1}{T}\int_{t_1-T/2}^{t_1+T/2}s^2(t)dt\,. \tag{2.1}$$

Vrednost ove veličine zavisi koliko od dužine vremenskog intervala, toliko i od položaja tog vremenskog intervala na vremenskoj osi. Iz ovoga proizilazi da, mada se radi o istom slučajnom signalu i o istoj dužini intervala usrednjavanja, navedena srednja vrednost signala u intervalu konačne dužine može biti različita u različitim vremenskim položajima tog intervala. Iz tog razloga je važno definisati srednju kvadratnu vrednost signala $s(t)$ u nekom vremenskom intervalu beskonačne dužine ($T\to\infty$)

$$\bar{s}^2(t)=\lim_{T\to\infty}\frac{1}{T}\int_{-T/2}^{+T/2}s^2(t)dt\,, \tag{2.2}$$

nezavisnu od položaja intervala na vremenskoj osi a koja opisuje na sveobuhvatniji način slučajne signale. Pošto ne poznajemo vremensku promenu signala $s(t)$, direktno matematičko rešavanje integrala u jednačini (2.2) je nemoguće, ali se može aproksimovati merenjima u konačnom ali dovoljno dugom periodu T (predstavljanjem dužeg perioda integraljenja T aproksimacija merenjem će biti tačnija).



Slika 2.3. *Talasni oblici dva različita slučajna signala šuma*

Posmatranjem prirode nekog slučajnog procesa, može se zaključiti da slučajni proces možemo nazvati stacionarnim u slučaju statističkih osobina signala (na primer srednjih kvadratnih vrednosti ili varijanse signala) nepromenljivih u vremenu. U slučaju mogućnosti određivanja statističkih osobina signala na osnovu posmatranja signala u dovoljno dugom vremenskom periodu onda takav stacionarno slučajni proces možemo smatrati i ergodičkim [132]. Suprotno od postupka kojim se određuju srednje kvadratne vrednosti slučajnog signala zasnovanog na integraciji signala u vremenu, ova vrednost se može odrediti sledećim postupkom: Prvo se formira ansambl N mernih sistema potrebnih za paralelno merenje signala N istih izvora slučajnih signala koji daju signale $s_n(t)$, n=1,2,...N, a zatim se u istom odabranom trentku t_1 izvrši merenje trenutnih vrednosti signala svakog izvora. Korišćenjem ovih N paralelnih uzoraka određuje se ansambl srednje kvadratnih vrednosti signala za N uzoraka

$$\left(s^2\left(N,t_1\right)\right)=\frac{1}{N}\sum_{n=1}^{N}s^2(t_1), \tag{2.3}$$

koji je zavisan od broja identičnih test objekata N i vremenskog trenutka uzorkovanja t_1. Teorijskim uzimanjem beskonačno mnogo uzoraka ($N\to\infty$) može se definisati ansambl srednje kvadratnih vrednosti signala koji nije zavisan od broja uzoraka, već jedino od vremena

$$\left\langle s^2(t)\right\rangle=\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}s^2(t). \tag{2.4}$$

U slučaju da je ansambl srednje kvadratnih vrednosti slučajnog signala nepromenljiva u vremenu, takvi signali pripadaju grupi stacionarnih slučajnih signala. Isto tako, u slučaju da je ansambl srednje kvadratne vrednosti stohastičkog signala jednak srednje kvadratnoj vrednosti tog signala dobijenoj usrednjavanjem u vremenskom domenu

$$\left\langle s^2(t)\right\rangle=\bar{s}^2(t), \tag{2.5}$$

tada je taj slučajni signal pored toga što je stacionaran još i ergodički.

Osim srednje kvadratne vrednosti signala, moguće je, u smislu opisivanja srednje vrednosti signala, definisati opšti slučaj odnosno srednju vrednost k-tog stepena signala

$$\bar{s}^k(t)=\lim_{T\to\infty}\frac{1}{T}\int_{-T/2}^{+T/2}s^k(t)dt. \tag{2.6}$$

Primenom ansambla usrednjavanja $\langle s^k(t)\rangle$ bi predstavljao k-ti moment signala. A k-ti moment devijacije signala srednje vrednosti $\langle(s(t)-\langle s(t)\rangle)^k\rangle$ naziva se k-ti centralni moment.

Jedan drugi centralni moment ima veoma važnu ulogu u istraživanjima i eksperimentima koja se odnose na analizu šuma. Njega najčešće obeležavamo sa σ^2 i nazivamo varijansa ili disperzija

$$\sigma^2 = \left\langle \left(s(t) - \langle s(t) \rangle \right)^2 \right\rangle \tag{2.7}$$

Kvadratni koren varijanse nazivamo standardnom devijacijom ili efektivnom vrednošću slučajnog signala $s(t)$

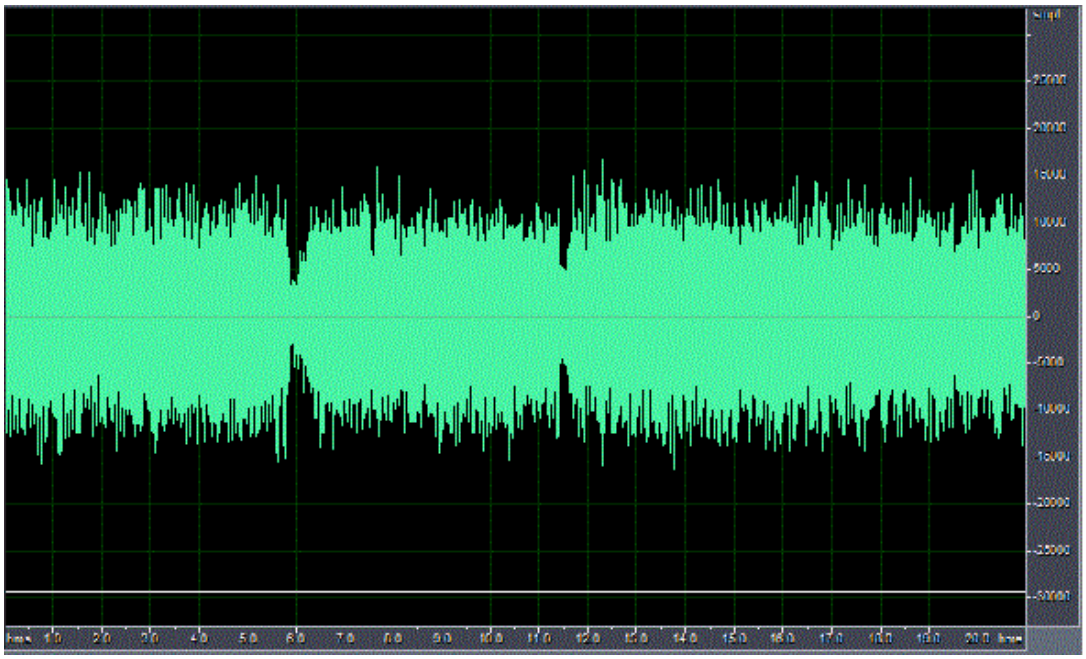
$$\sigma = \sqrt{\left\langle \left(s(t) - \langle s(t) \rangle \right)^2 \right\rangle} \tag{2.8}$$

Za slučajni signal šuma nulte srednje vrednosti, koga nazivamo belim šumom, važi

$$\sigma = \sqrt{\left\langle s^2(t) \right\rangle} \qquad , \langle s(t) \rangle = 0 \tag{2.9}$$

Slučajne signale šuma u većini slučajeva u potpunosti karakteriše njihova varijansa σ^2. Kada je u pitanju ergodički slučajni signal tada važi izraz

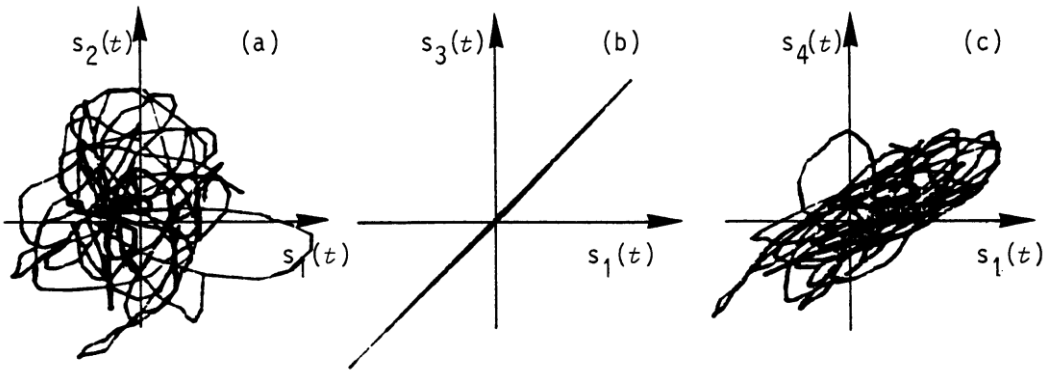
$$\left\langle s^k(t) \right\rangle = \lim_{T \to \infty} \frac{1}{T} \int_{-T/2}^{+T/2} s^k(t) dt \,. \tag{2.10}$$



Slika 2.4. *Slučajni signal buke životne sredine korišćen u ovom eksperimentu*

2.1.2. Korelacina svojstva slučajnog signala

Predpostavimo da se posmatrana tačka u prostoru nalazi u okruženju dva ili više slučajnih izvora, tada u toj tački nastaje pojava superpozicije signala tih izvora. Korelaciju ili statističku zavisnost tih signala možemo smatrati posebno značajnom za karakterizaciju procesa superpozicije u toj tački. Za primer karakterizacije statističke zavisnosti signala više slučajnih izvora merenjem, uzet je osciloskop čija je uloga merenje četiri izvora šuma za tri različite kombinacije: prve kod dovođenja na *x* kanal osciloskopa signala šuma $s_1(t)$ a na *y* kanal $s_2(t)$, druge kod dovođenja na *x* kanal osciloskopa signala šuma $s_1(t)$ a na *y* kanal $s_3(t)$ i treće na *x* kanal osciloskopa signala šuma $s_1(t)$ a na *y* kanal $s_4(t)$ (slike 2.5(a)-(c) respektivno).



Slika 2.5. *Rezultati merenja osciloskopom signala iz četiri izvora šuma [27]*

Signali $s_1(t)$ i $s_2(t)$ su signali fizički nezavisnih izvora šuma tako da se očekuje da su nekorelisani i statistički nezavisni jedni od drugih. Rezultat merenje na slici 2.5a pokazuje takvu činjenicu. Izmerene vrednosti signala $s_1(t)$ nisu prejudicirale niti uticale da se izvede zaključak šta se može očekivati po pitanju izmerenih vrednosti signala $s_2(t)$ i obratno. Kod slučajnog šuma $\langle s_1(t)\rangle = 0$ i $\langle s_2(t)\rangle = 0$, tako da za uslov statističke nezavisnosti važi

$$\langle s_1(t)\cdot s_2(t)\rangle = 0\,. \tag{2.11}$$

Signali $s_1(t)$ i $s_3(t)$ su signali fizički zavisnih izvora šuma tako da se očekuje da su korelisani i statistički zavisni. Rezultati merenje na slici 2.5b pokazuje da su ovi signali linearno zavisni odnosno da važi $s_3(t) = a\cdot s_1(t)$, tako da se njihova korelisanost može izraziti kao

$$\langle s_1(t)\cdot s_3(t)\rangle = a\cdot\langle s_1(t)\cdot s_1(t)\rangle = a\sigma_1^2 \neq 0\,. \tag{2.12}$$

Poslednji je slučaj signala $s_1(t)$ i $s_4(t)$ gde se signal $s_4(t)$ dobija linearnom superpozicijom

signala $s_1(t)$ i $s_2(t)$, odnosno gde važi $s_4(t) = as_1(t) + bs_2(t)$. Rezultat merenje na slici 2.5c pokazuje da dijagram rasipanja signala ispunjava elipsu sa promenljivim osama. Takva njihova korelisanost može se izraziti kao

$$\langle s_1(t) \cdot s_4(t) \rangle = \langle a \cdot s_1(t) \cdot s_1(t) + b \cdot s_1(t) \cdot s_2(t) \rangle = a \cdot \langle s_1(t) \cdot s_1(t) \rangle = a\sigma_1^2 \neq 0 \tag{2.13}$$

Veličina stepena korelisanosti dva signala određuje se preko korelacionim koeficijentom definisanog kao [27]

$$k_{ij} = \frac{\langle s_i(t) \cdot s_j(t) \rangle}{\sqrt{\langle s_i^2(t) \rangle \cdot \langle s_j^2(t) \rangle}} \tag{2.14}$$

Za signale $s_1(t)$ i $s_2(t)$ dobija se

$$k_{12} = 0, \tag{2.15}$$

što znači da su signali $s_1(t)$ i $s_2(t)$ nekorelisani.

Za signale $s_1(t)$ i $s_3(t)$ dobija se

$$k_{13} = 1, \tag{2.16}$$

što znači da su signali $s_1(t)$ i $s_3(t)$ u potpunosti korelisani.

Posmatranjem signala $s_1(t)$ i $s_4(t)$, pošto važi

$$\langle s_4^2(t) \rangle = a^2\sigma_1^2 + b^2\sigma_2^2 \tag{2.17}$$

korelacioni koeficijenat je

$$k_{14} = \frac{a\sigma_1^2}{\sqrt{\sigma_1^2(a^2\sigma_1^2 + b^2\sigma_2^2)}} = \frac{a}{|a|} \frac{1}{\sqrt{1 + \frac{b^2\sigma_2^2}{a^2\sigma_1^2}}} < 1, \tag{2.18}$$

što znači da su signali $s_1(t)$ i $s_4(t)$ delimično korelisani. Uopšte za korelacioni koeficijent dva signala važi

$$0 \leq |k_{ij}| \leq 1. \tag{2.19}$$

Vrlo često se u praksi dešava da u nekoj tački u prostoru dođe do superpozicije signala dva stacionarna slučajna izvora, gde jedan signal ima vremensko kašnjenje u odnosu na drugi τ. Označimo signal jednog izvora sa $s_i(t)$, a signal drugog izvora sa $s_j(t)$. Između dva stacionarna slučajna izvora može se definisati korelaciona funkcija $c_{ij}(\tau)$ na sledeći način

$$c_{ij}(\tau) = \left\langle s_i(t) \cdot s_j(t-\tau) \right\rangle . \tag{2.20}$$

Korelaciona funkcija stacionarnih stohastičkih signala ne zavisi od vremena *t*. U slučaju ergodičkih slučajnih signala ansambl srednje vrednosti proizvoda dva signala se mogu zameniti srednjim vrednostima proizvoda dva signala u vremenu i obrnuto, pa se korelacina funkcija može izaraziti u obliku

$$c_{ij}(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{-T/2}^{+T/2} s_i(t) \cdot s_j(t-\tau) dt . \tag{2.21}$$

Ako je u formuli (2.21) $i = j$ (slučaj istog signala) onda se dobija autokorelaciona funkcija slučajnog signala, dok za $i \neq j$ (slučaj signala dva različita izvora) funkcija predstavlja kros-korelacionu funkciju dva različita slučajna signala.

2.1.3. Karakteristike korelacionog spektra slučajnog signala

Stacionarne slučajne signale nije moguće opisati u zatvorenom funkcionalnom obliku tako da proračun integrala tih signala nije moguć. Iz tog razloga klasični amplitudski spektar koji egzistira kod determinističkih signala nije moguće izračunati kod slučajnih signala. Međutim, ako se uzme uzorak signala u nekom određenom vremenskom intervalu konačne dužine na tom uzorku se može primeniti spektralna analiza [27]. Pretpostavimo da je segment signala $s(t)$ trajanja T označen sa $s_T(t)$ i da se definiše kao

$$s_T(t) = \begin{cases} s(t) & , \quad -\dfrac{T}{2} < t < +\dfrac{T}{2} \\ 0 & , \quad |t| \geq \dfrac{T}{2} \end{cases} \tag{2.22}$$

Ovakvim načinom definisan signal je vremenski odsečen signal ili signal odsečen u prozoru. Furijeova transformacija ovakvog signala se može definisati kao

$$S_T(f) = \int_{-\infty}^{+\infty} s_T(t) e^{-2\pi j f t} dt . \tag{2.23}$$

Odgovarajuća inverzna Furijeova transformacija se u skladu sa tim može izraziti u obliku

$$s_T(t) = \int_{-\infty}^{+\infty} S_T(f) e^{2\pi j f t} df . \tag{2.24}$$

Imajući u vidu (2.22) korelacionu funkciju definisanu sa (2.21) možemo predstaviti i kao

$$c_{ij}(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{-\infty}^{+\infty} s_{iT}(t) \cdot s_{jT}(t-\tau) dt . \tag{2.25}$$

Ako $N \to \infty$ integrali koji su dati u (2.21) i (2.25) postaju jednaki. Primenom inverzne Furijeove transformacije date sa (2.20) na (2.21) dobijamo

$$c_{ij}(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{-\infty}^{+\infty} \left[\int_{-\infty}^{+\infty} S_{iT}(f) e^{2\pi j f t} df \right] \cdot s_{jT}(t-\tau) dt , \tag{2.26}$$

a posle zamene sekvence oba integrala dobijamo

$$c_{ij}(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{-\infty}^{+\infty} S_{iT}(f) \cdot \left[\int_{-\infty}^{+\infty} s_{jT}(t-\tau) e^{2\pi j f t} dt \right] df . \tag{2.27}$$

Posle uvođenja zamene $t - \tau = t'$ i $dt = dt'$ dobijamo

$$c_{ij}(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{-\infty}^{+\infty} S_{iT}(f) e^{2\pi j f \tau} \cdot \left[\int_{-\infty}^{+\infty} s_{jT}(t') e^{2\pi j f t'} dt' \right] df . \tag{2.28}$$

Hermitovim transponovanjem jednačine (2.23) za Furijeovu transformaciju i spektar signala S_{jT} dobijamo

$$S_{jT}^{*}(f) = \int_{-\infty}^{+\infty} s_{jT}(t) e^{2\pi j f t} dt . \tag{2.29}$$

Ako se (2.29) primeni u delu (2.28) dobijamo

$$c_{ij}(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{-\infty}^{+\infty} S_{iT}(f) \cdot S_{jT}^{*}(f) e^{2\pi j f \tau} df . \tag{2.30}$$

Furijeovom transformacijom korelacione funkcije $c_{ij}(\tau)$ dobija se funkcija $C_{ij}(f)$ koja se naziva korelacioni spektar [27,28]

$$C_{ij}(f) = \int_{-\infty}^{+\infty} c_{ij}(\tau) e^{-2\pi j f \tau} d\tau . \tag{2.31}$$

Primenom (2.31) na (2.30) dobijamo

$$C_{ij}(f) = \lim_{T\to\infty} \frac{1}{T} \int_{-\infty}^{+\infty} S_{iT}(f) \cdot S_{jT}^{*}(f) \left[\int_{-\infty}^{+\infty} e^{2\pi j f \tau} e^{-2\pi j f \tau} d\tau \right] df , \tag{2.32}$$

odnosno

$$C_{ij}(f)=\lim_{T\to\infty}\frac{1}{T}\int_{-\infty}^{+\infty}S_{iT}(f)\cdot S_{jT}^{*}(f)df\ . \tag{2.33}$$

S obzirom da $S_{iT}(f)$ ne postoji za granični slučaj $T\to\infty$ integraciju na desnoj strani (2.33) moramo zameniti ansamblom usrednjavanja proizvoda $S_{iT}(f)\cdot S_{iT}^{*}(f)$ u skladu sa (2.20) i (2.21)

$$C_{ij}(f)=\lim_{T\to\infty}\frac{1}{T}\left\langle S_{iT}(f)\cdot S_{jT}^{*}(f)\right\rangle. \tag{2.34}$$

U slučaju da u prostoru imamo N ergodičkih slučajnih izvora zračenja međusobni uticaj njihovih zračenja se može opisati preko njihovih korelacionih spektara signala koji se predstavljaju korelacionom matricom signala [27, 28]

$$\mathbf{C}(f)=\begin{bmatrix}C_{11}(f) & C_{12}(f) & \cdots & C_{1N}(f)\\ C_{21}(f) & C_{22}(f) & \cdots & C_{2N}(f)\\ \vdots & \vdots & & \vdots\\ C_{N1}(f) & C_{N2}(f) & \cdots & C_{NN}(f)\end{bmatrix}. \tag{2.35}$$

Ako se korelacioni spektri ergodičkih slučajnih signala proračunavaju u izabranim tačkama u prostoru onda se često ovako definisana korelaciona matrica naziva prostornom korelacionom matricom slučajnih signala. Ovako definisana korelaciona matrica **C** po svojoj fizičkoj suštini odgovara korelacionoj matrici $\mathbf{R_{xx}}$ koja je ranije definisana preko determinističkih signala, tako da se i ona na potpuno isti način može iskoristiti za proračun korišćenjem odgovarajućih algoritama koji su zasnovani na korelacionoj matrici signala.

2.2. Slučajni nizovi i slučajni procesi

Pretpostavimo da svakog trenutka $t\in T$, gdje je $T\subset R$, posmatramo neku karakteristiku X u sistemu i neka ona ima slučajni karakter. U tom slučaju $X(t)$ predstavlja neku slučajnu promjenljivu u svakom trenutku t. Tada svi elementi skupa $\{X(t),t\in T\}$, koji su slučajne promenljive, mogu se posmatrati kao jedna slučajna veličina koja se menja tokom vremena.

Pri ovakvim okolnostima skup $\{X(t),t\in T\}$ nazivamo slučajnim procesom.

Slučajni proces se može definisati i na sledeći način. Neka je (Ω*; F; P*) određeni prostor verovatnoće i T neprazni skup, pri čemu je svakom $t\in T$ pridružena određena slučajna

promenljiva $X(t): \Omega \to R$. Tada se familija slučajnih promenljivih $\{X(t), t \in T\}$ naziva slučajni proces.

Skup *T* naziva se parametarski skup slučajnog procesa $\{X(t), t \in T\}$, a pojedina vrednost $t \in T$ naziva se parametar.

Važno je uočiti da je slučajni proces $\{X(t), t \in T\}$ funkcija sa skupa $T \times \Omega$ u skup realnih brojeva R odnosno, funkcija dva paramatra ω i *t*. Za svako određeno $t \in T$ dobijamo jednu slučajnu promenljivu koja opisuje posmatranu slučajnu pojavu u trenutku *t*. Ukoliko odredimo da je $\omega \in \Omega$ dobićemo funkciju koja je jedna realna funkcija definisana u okviru skupa *T* i koju nazivamo realizacijom slučajnog procesa. Primećujemo da za $T = \{1\}$ dobijamo slučajnu promenljivu, za $T = \{1,2,...k\}$ dobijamo *k*-dimenzionalni slučajni vektor, dok za $T = R$ dobijamo slučajnu funkciju.

Radi jasnijeg razumevanja problematika se može predstaviti na sledeći način.

Sretanje sa veličinama slučajno promenljivim u vremenu je vrlo česta pojava. Tako da slučajni proces predstavlja familiju sa slučajnim promenljivama $X(t) = X(t, \omega)$ koje su zadate i deo su prostora verovatnoće *(Ω; F; p)* zavisnog od vremena $t \in T$. Tako da slučajni proces označen kao $\{X(t), t \in T\}$ predstavlja funkciju u prostoru $R \times \Omega$ i ima vrednosti u *R* (*t; X*(t, ω_0)), gde je *t* vreme a $X(t, \omega_0)$ trajektorija ili putanja $\{X(t), t \in T\}$.

Pretpostavimo da je *T* skup koji se može prebrojati, neka su na primer u pitanju celi brojevi, onda se takav skup može nazvati slučajnim nizom. Pretpostavimo da se radi o realnom intervalu $T = [a, b]$ ili delu na realnoj pravi, tada bi se radilo o slučajnom procesu sa neprekidnim vremenom.

Posebnom vrstom slučajnih procesa smatramo Markovljeve slučajne procese. Pretpostavimo da su $A_1, A_2, ...$ i $\sum A_i = \Omega$ rezultati određenog eksperimenta, pri čemu je $A_j^{(n)}$ rezultat A_j realizovan u nekom eksperimentu koji se *n*-ti put (*n* =1,2,...) iznova ponavlja. Tada niz eksperimenata predstavlja Markovljev lanac pod uslovom da proizvoljni *r*, *n*, $k_i \in N$, $n > k_1 > k_2 > ... > k_r$, i proizvoljni događaji $A_j^{(n)}, A_{i_1}^{(k_1)}, ..., A_{i_r}^{(k_r)}$ koji su deo skupa mogućih rezultata $\{A_i\}$ ispunjavaju uslov:

$$p\left(A_j^{(n)} / A_{i_1}^{(k_1)}, ..., A_{i_r}^{(k_r)}\right) = p\left(A_j^{(n)} / A_{i_1}^{(k_1)}\right) \tag{2.36}$$

Za verovatnoću koja predstavlja prelaz sistema iz jednog stanja x_i u trenutku vremena *n* u

drugo stanje x_j u trenutku vremena m, važi relacija:

$$p_{ij}(n,m) = p\left(X_m = x_j / X_n = x_i\right), \quad 0 \le n \le m \tag{2.37}$$

U slučaju da $p_{ij}(n,m)$ koja predstavlja funkciju od m i n koja je zavisna jedino od razlike $m-n$ onda to predstavlja homogeni Markovljev lanac. Može se, u slučaju homogenih Markovljevih lanaca, postaviti pitanje mogućnosti određivanja verovatnoća prelaza $p_{ij}(n)$, n = 2,3,... za n koraka, ukoliko je poznata verovatnoća prelaza p_{ij}, i,j=1,2,... u jednom koraku. U tom slučaju odgovor daju sledeće jednačine:

$$p_{ij}(n) = \sum_k p_{ik}(m)p_{kj}(n-m); \;\; 1 \le m \le n; \; i, \; j = 1,2,... \tag{2.38}$$

Ovo je moguće zapisati matrično kao:

$$P_n = P_m P_{n-m}, \quad 1 \le m \le n \tag{2.39}$$

jer je $P_n = \left\lfloor p_{ij}(n) \right\rfloor$; $P_1 = \left\lfloor p_{ij} \right\rfloor$; $i, j = 1,2,...; \; n = 2,3,...$

Tako da se P_n može smatrati matricom verovatnoće prelaza iz jednog stanja x_i u drugo x_j za n koraka sa elementima brojeva $[0,1]$.

Ovde važi pravilo zbira elemanata bilo koje vrste u P_n da je jednako 1, kao i da se P_n može dobiti stepenovanjem iz P.

Potreno je pomenuti i ergodičnu teoremu kod Markovljevih lanaca sa konačnim brojem stanja, koja se odnosi na ponašanje verovatnoće prelaza $p_{ij}(n)$ pri neograničenom povećavanju broja koraka n, a koja se definiše na sledeći način:

Neka je za $n = n_0$ svaki element u matrici P_{n_0} pozitivan, $p_{ij}(n_0) > 0; \; \forall i, \; j = 1,2,...,s$,onda za svako j=1,2,..., s važi relacija:

$$\lim_{n \to \infty} p_{ij}(n) = p_j^* \tag{2.40}$$

gde su p_j^* finalne verovatnoće nezavisne od $i = 1,2,...,s$.

Brojeve p_j^* dobijamo iz uslova

$$p_1^* + p_2^* + ... + p_s^* = 1 \tag{2.41}$$

kao i iz sistema jednačina

$$p_j^* = \sum_k p_k^* p_{kj} \qquad j = 1,2,...,s \tag{2.42}$$

2.2.1. Statistička metoda

Neka je $X_k = X(\omega_k), \quad k = 1,2,...,n$ je tada slučajni uzorak sa $\omega_1, \omega_2, ..., \omega_n$ slučajnim rezultatima kod kojih posmatramo karakteristiku *X* čime dobijamo *n*-dimenzionalnu slučajnu veličinu $(X_1, X_2, .., X_n)$. Označimo sa $x_1, x_2, ..., x_n$ realizovane vrednosti uzorka $(X_1, X_2, .., X_n)$.

Pod slučajnim uzorkom smatra se prost uzorak kada je skup slučajnih promenljivih $X_1, X_2, ..., X_n$ međusobno nezavisan i kada sve promenljive imaju istu *F*(*X*) odnosno funkciju raspodele. Na osnovu uzorka $(X_1, X_2, ..., X_n)$ može se definisati empirijska funkcija raspodele $F_n^*(X)$ kao:

$$F_n^*(X) = \frac{1}{n}\sum_{k=1}^{n} I(X_k \langle x), \quad x \in R \qquad \left(I_A = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases} \right), \tag{2.43}$$

odnosno:

$$P\left(F_n^*(x) = \frac{k}{n} \right) = \binom{n}{k} (F(x))^k (1 - F(x))^{n-k}, \quad k = 0,...,n \tag{2.44}$$

Centralnom teoremom matematičke statistike definisano je:

$$p\left(\sup \left| F_n^*(x) - F(x) \right| \to 0\right) = 1, \tag{2.45}$$

gde *F*(*X*) predstavlja teorijsku funkciju raspodele karakteristike *X*.

2.2.2. Definisanje tačkastih ocena parametara

Pretpostavimo da karakteristika *X* ima određenu vrstu raspodele, binomnu ili normalnu, onda je potrebno izvšiti ocenu parametara funkcije raspodele *F*. Na primer, ako je *X* funcija $N(m, \sigma)$ potrebno je oceniti parametre *m* i σ.

Ako θ smatramo nepoznatim parametrom funkcije raspodele $F(x,\theta)$ karakteristike *X*, onda bismo sa $\theta_n = U(X_1, X_2, ..., X_n)$ označili odabranu statistiku kojom ocenjujemo parametar θ.

Ovako definisana ocena zove se tačkasta ocena parametara. Kod tačkastih ocena

parametara postavljaju se sledeći zahtevi:

- da je ocena nepristrasna, što znači da je centrirana $E(U)=\theta$,
- da je ocena korektna, što znači da je *U* asimptotski centrirano $E(U)\to\theta$, za $n\to\infty$,
- da je ocena konzistentna, što znači da $\sigma_U^2=E(U-\theta)^2\to 0$, za $n\to\infty$, predstavlja najmanju moguću disperziju ocene u odnosu na dati raspored.

U postupku dobijanja tačkastih ocena parametra θ najčešće se koristimo metodom maksimalne verodostojnosti. Pretpostavimo da je

$$f(x,\theta)=\begin{cases} p_\theta(x_k) \\ f_\theta(x) \end{cases} \tag{2.46}$$

skup dozvoljenih raspodela karakteristike *X*. Funkcija verodostojnosti *L* se tada može definisati kao

$$L(\theta)=f(x_1,\theta)f(x_2,\theta)...f(x_n,\theta) \tag{2.47}$$

Može se reći da za ocenu parametra θ, dobijenu metodom maksimalne verodostojnosti, smatramo onu vrednost θ za koju funkcija $L(\theta)$ ima maksimalnu vrednost.

Određivanje maksimuma funkcije *L* moguće je obaviti na dva načina:

- tako što se izvrši izjednačavanje izvoda funkcije po θ sa nulom ili
- tako što se prvo izvrši logaritmovanje a tek onda diferenciranje i izjednačavanje sa nulom.

2.2.3. Određivanje intervalnih ocena parametara

Postupak ocene nepoznatog parametra θ,u određenoj raspodeli karakteristike nepoznate, moguće je uraditi koristići slučajni uzorak i određivanjem intervala $[u_1,u_2]$ u kome se nalazi taj parametar, kao:

$$p(u_1\le\theta\le u_2)=p(\theta\in I(X_1,X_2,...,X_n))=1-\alpha, \tag{2.48}$$

gde 1 – α predstavlja koeficijenat pouzdanosti.

Za određivanje intervala poverenja kod nepoznatog matematičkog očekivanja *m* koje je funkcija $X:N(m,\sigma)$, važi:

$$I = \left[\bar{x}_n - t\frac{\sigma}{\sqrt{n}}, \bar{x}_n + t\frac{\sigma}{\sqrt{n}} \right], \quad l = \frac{2t\sigma}{\sqrt{n}} \tag{2.49}$$

gde *l* predstavlja širinu intervala a $\bar{x}_n$ sredinu uzorka.

Kod datog nivoa poverenja $1-\alpha$ parametar *t* se određuje tablicom kao u tabeli 2.1.

Tabela 2.1. Određivanje *t* za dati nivo poveranja

$1-\alpha$	0.8	0.9	0.95	0.96	0.98	0.99
t	1.28	1.645	1.96	2.05	2.33	2.58

Prilikom određivanja ocene nepoznate *m* potrebno je koristiti veličinu

$$t = \frac{\bar{x}_n - m}{\bar{s}_n}\sqrt{n-1} \tag{2.50}$$

gde $\bar{s}_n$ predstavlja standardnu devijaciju uzorka. Tako da za interval poverenja sada važi:

$$I = \left[\bar{x}_n - t_0\frac{\bar{s}_n}{\sqrt{n-1}}, \bar{x}_n + t_0\frac{\bar{s}_n}{\sqrt{n-1}} \right], \quad l = \frac{2t_0\bar{s}_n}{\sqrt{n-1}} \tag{2.51}$$

Kod određivanja intervalnih ocena za σ^2 koristimo tablicu χ^2 raspodele sa $n-1$ stepenom slobode i datim nivoom poverenja $1-\alpha$, određujemo $\chi^2_{\alpha_1}$ i $\chi^2_{\alpha_2}$ $\left(\chi^2_{\alpha_1} \langle \chi^2_{\alpha_2}\right)$ i dobijamo:

$$p\left(\frac{n\bar{s}_n^2}{\chi^2_{\alpha_2}} \langle \sigma^2 \langle \frac{n\bar{s}_n^2}{\chi^2_{\alpha_1}} \right) = 1-\alpha; \tag{2.52}$$

gde su:

$$1-\alpha = \beta, \qquad F\left(\chi^2_{\alpha_1}\right) = \frac{1+\beta}{2}, \qquad F\left(\chi^2_{\alpha_2}\right) = \frac{1-\beta}{2} \tag{2.53}$$

2.2.4. Načini testiranja statističkih hipoteza

Pod statističkom hipotezom, $H: \theta \in A$, podrazumeva se bilo kakva pretpostavaka o raspodeli karakteristike *X*, odnosno o pripadnosti raspodele, kao delu nekog podskupa *A*, skupu dozvoljenih raspodela $F(x,\theta)$. Suprotnu hipotezu, $H: \theta \in A^C$, zovemo alternativnom hipotezom.

Pored toga što se hipoteza odnosi na oblik raspodele karakteristike odnosi se i na:

- vrednosti nekih parametara raspodele,
- jednakost parametara u slučaju većeg broja raspodela,
- međusobne nezavisnosti uzoraka,
- jednakost raspodele kod dve različite karakteristike.

Za hipotezu važi da je prosta u slučaju jednočlanog skupa *A*, odnosno da je složena ukoliko je sastavljena iz nekoliko prostih hipoteza.

Verifikovanje hipoteze vrši se statističkim testom na sledeći način.

Uoči se skup $C \subset R^n$, koga nazivamo kritičnom oblašću hipoteze *H*, i ako je:

- određeni realizovani uzorak $(x_1, x_2, ..., x_n)$ deo oblasti *C*, hipoteza se odbacuje,
- realizovani uzorak $(x_1, x_2, ..., x_n)$ deo neke druge hipoteze i nije deo *C*, hipoteza se ne odbacuje i prihvata se.

Prilikom verifikacija hipoteza postoji mogućnost pojave grešaka koje se dele na:

- greške prve vrste, koje opovrgavaju tačnu hipotezu i
- greške druge vrste, koje prihvataju netačnu hipotezu.

Vrednost verovatnoće pojave grešaka prve vrste se najčešće kreće od 0.01 do 0.05, naziva se nivo nivo značajnosti i obeležava sa α.

2.2.4.1. Provera hipoteza parametarskim testovima

Pri proveri hipoteza, onih koje se bave raspodelama i vrednostima njihovih parametara, koristimo parametarske testove. Navešćemo primer testiranja hipoteze $H_0(m = m_0)$ protivno hipotezi $H_1(m \neq m_0)$ u slučaju poznate disperzije σ kao parametra karakteristike $X : N(m, \sigma)$:

$$p\left(\left|\overline{X}_n - m_0\right| \geq \left|\bar{x}_n - m_0\right|\right) = 1 - 2\Phi\left(\frac{\left|\bar{x}_n - m_0\right|}{\sigma / \sqrt{n}}\right) = \alpha^* \tag{2.54}$$

U slučaju $\alpha^* \leq \alpha$ hipotezu *H* odbacujemo, ako je suprotno hipotezu prihvatamo.

Drugi primer je testiranje hipoteze $H_0(m = m_0)$ protiv $H_1(m \neq m_0)$ za nepoznato σ:

$$\bar{t}_{n-1} = \frac{\bar{x}_n - m_0}{\bar{s}_n}\sqrt{n-1} \tag{2.55}$$

Računa se odgovarajuća vrednost iz uzorka i poredi sa $t'_{n-1,\alpha}$ iz tablica Studentove raspodele. U slučaju $|t'_{n-1}| > t'_{n-1,\alpha}$ hipoteza *H* se odbacuje, ako je suprotno hipotezu prihvatamo.

2.2.4.2. Provera hipoteza neparametarskim testovima

Provera hipoteza koje se bave oblikom funkcije raspodele karakteristične nepoznate vrši se statističkim neparametarskim testovima. Najčešće se koristi Pirsonov test χ^2. Treba:

- izvršiti podelu na *r* podskupa, koji su disjunktivni, skupa svih mogućih vrednosti *X*,
- izvršiti određivanje verovatnoća 1 p_k i 2 da vrednosti *X* budu u intervalu S_k, k=1,2,...,r
- označiti sa m_k broj x_j u skupu $(x_1, x_2, ..., x_n)$ iz S_k; $m_1 + m_2 + ... + m_r = n$ je obim uzorka.

Karakteristično za kritičnu oblast, kod datog nivoa značajnosti, je da je to skup tačaka sa:

$$\overline{A} = \sum_{k=1}^{n} \frac{(m_k - np_k)^2}{np_k} \geq \chi^2_{r-1,\alpha} \tag{2.56}$$

U slučaju da je $\overline{A} \geq \chi^2_{r-1,\alpha}$ hipotezu odbacujemo, u suprotnom hipoteza se prihvaća.

2.2.5. Veza entropije i informacije

Neka skup slučajnih događaja $A_1, A_2, ..., A_n$ označava različita stanja fizičkog sistema *X* koji je u funkciji prelaska iz jednog stanja u drugo, onda svako stanje može dobiti brojnu vrednost a *X* dobija status slučajne promenljive, stim da su p_i verovatnoće stanja A_i. Znači:

$$X : \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ p_1 & p_2 & \dots & p_n \end{pmatrix}, \quad \sum_{i=1}^{n} p_i = 1 \tag{2.57}$$

Pojam entropije odnosi se na meru neodređenosti nekog sistema čija je funkcija prelazak iz jednog u drugo stanje.

Posmatranjem komunikacionih sistema može se primetiti da su njihovi signali i šumovi statističkog karaktera, to jest da imaju određene raspodela verovatnoća. Tip raspodele određuje srednju informaciju signala što drugačije nazivamo merom informacije. Matematički izraz entropije, odnosno neodređenosti pri izboru jedne vrednosti iz skupa mogućih vrednosti (gde svaka vrednost ima verovatnoću izbora p_i), je po američkom matematičaru, elektro inženjeru i kriptologu Šenonu (Claude Elwood Shannon):

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i \tag{2.58}$$

Ako imamo slučaj istih verovatnoća p_i, važi izraz:

$$H\left(\frac{1}{n},\frac{1}{n},...,\frac{1}{n}\right) = \log_2 n \tag{2.59}$$

Možemo entropiju $H(X)$ za neku slučajnu veličinu X izraziti i kao:

- očekivanu količinu informacije koja je sadržana u jednoj realizaciji X,
- neizvesnost ili neodređenost u odnosu na rezultat relizacije X,
- očekivanu vrednost bita potrebnih da se opiše jedna realizacija X.

Ako se posmatraju složeni sistemi (X,Y) onda je mogućnost svih stanja realizacija dvodimenzionalnih slučajnih promenljiva.

U vezi sa komunikacionim sistemima se onda uvode veličine koje se odnose na:

- neizvesnost ulaza u kanal X i izlaza iz kanala Y, $H(X)$ i $H(Y)$,
- neizvesnost da se pojavi uređeni par (X,Y), $H(X,Y)$,
- pojam uslovne entropije, odnosno srednju neizvesnost ulaza X uz poznavanje izlaza Y

$$H(X/Y) = -\sum_{i}\sum_{j} p_{ij} \log_2 q_{j/i} \tag{2.60}$$

- količinu informacije, kao srednja uzajamna informacija X i Y:

$$I(X,Y) = H(X) - H(X/Y) = H(Y) - H(Y/X) \tag{2.61}$$

2.3. Teorija verovatnoće u funkciji slučajnosti

2.3.1. Osnovne karakteristike slučajnosti i verovatnoće

Označimo sa Ω neki skup elementarnih događaja odnosno sve moguće rezultate određenog eksperimenta. Za elemente Ω podrazumevamo događaje označene sa $\omega_1, \omega_2, \ldots$.

Slučajni događaj A smatramo podskupom skupa elementarnih događaja Ω. Njegovi članovi su elementarni događaji čije karakteristike definišu događaj A.

Pod σ poljem nad Ω podrazumeva se podskup $\mathcal{F}$ partitivnog skupa $P(\Omega)$, gde je partitivni $P(\Omega)$ ustvari skup svih podskupova skupa Ω, ako važi:

a) uslov pripadnosti $\Omega \in \mathcal{F}$,

b) da je ispunjen uslov komplementiranja $B \in \mathcal{F} \Rightarrow B^C \in \mathcal{F}$,

c) ispunjenost uslova prebrojive unije $\{B_i\}_{\in \mathbb{N}} \subseteq \mathcal{F} \Rightarrow U_{i=1}^{\infty} B_i \in \mathcal{F}$.

Skupom Ω sa σ poljem $\mathcal{F}$, $(\Omega,\mathcal{F})$, nazivamo prostorom σ polja.

Pod Borelovim σ poljem, $\mathcal{B}=\mathcal{B}(\mathbb{R})$, podrazumevamo σ polje u kome su sadržani svi zatvoreni skupovi skupa realnih brojeva.

Ako $(\Omega,\mathcal{F})$ predstavimo prostorom koje ima σ polje, tada se funkcija $P:\mathcal{F} \rightarrow [0,1]$ naziva verovatnoćom na prostoru $(\Omega,\mathcal{F})$ pod uslovom da važi:

- da je ispunjen uslov $P(\omega)=1$,
- ispunjenost uslova $\{B_i\}_{i \in \mathbb{N}} \subseteq \mathcal{F}, B_i \cap B_j \neq \emptyset, i \neq j, i,j=1,2,\ldots \Rightarrow P(U_{i=1}^{\infty} B_i) = \sum_{i=1}^{\infty} P(B_i)$.

Tada uređenu trojku $(\Omega,\mathcal{F},P)$ nazivamo prostorom verovatnoća.

Pod presekom događaja A i B podrazumevamo skup $A \cap B$ koji može biti realizovan ako su realizovani i A i B događaji.

Događaje A i B smatramo nezavisnim ako je ispunjena jednakost

$$P(A \cap B) = P(A)P(B) \tag{2.62}$$

Funkciju $X:\Omega \rightarrow \mathbb{R}$ zovemo slučajnom promenljivom u prostoru verovatnoća $(\Omega,\mathcal{F},P)$ pod uslovom da se na svako $B \in \mathcal{B}$ odnosi $X^{-1}(B) \in \mathcal{F}$.

Za slučajnu promenljivu X kažemo da je diskretna jedino pod uslovom postojanja prebrojivog skupa sa različitim vrednostima $R_X=\{x1,x2,\ldots\}$ takvog da $P\{\overline{R_x}\}=0$, $\overline{R_x}$ zovemo komplementarnim skupom R_x. Ako se verovatnoća događaja $\{X=xi\}$ označi sa $p(xi)$, onda je:

$$p(x_i) = P\{\omega \in \Omega | X(\omega) = x_i\} = P\{X = x_i\}, i = 1,2,... \tag{2.63}$$

Par sastavljen iz skupa vrednosti diskretne slučajne promenljive $\{x_{1,2},\ldots\}$ i odgovarajuće verovatnoće $p(x_i)$, $i=1,2,\ldots$, je uslov zakona raspodela slučajnih promenljiva X.

Funkciju (x): $\mathbb{R} \rightarrow [0,1]$ nazivamo funkcijom raspodele slučajne promenljive X ako je:

$$F_X(x) = P\{\omega \in \Omega | X(\omega) \langle x\} = P\{X \langle x\}, \tag{2.64}$$

Slučajnu promenljivu X smatramo apsolutno neprekidnom pod uslovom postojanja funkcije (x), $-\infty<x<\infty$, takve da za svaki skup S važi uslov pripadnosti $S\in\mathcal{B}(\mathbb{R})$

$$P(X \in S) = \int_S \varphi_X(x)dx \tag{2.65}$$

Funkciju (x) nazivamo gustinom raspodele verovatnoća slučajne promenljive X.

Najjednostavnija slučajna promenljiva je indikator događaja $B\in\mathbb{F}$, I_B, koga defnišemo sledećom funkcijom:

$$I_B(\omega) = \begin{cases} 1, \omega \in B, \\ 0, \omega \in B^C \end{cases} \tag{2.66}$$

Slučajnu promenljivu $X: \Omega\rightarrow\mathbb{R}$ nazivamo prostom slučajnom promenljivom u slučaju postojanja konačno mnogo vrednosti realnih brojeva $x_1,\ldots$, tako da važi $\sum_{i=1}^{n} p(x_i)=1$. U tom slučaju važi $\Omega=\sum_{i=1}^{n} A_i$, gde je $A_i=\{\omega \mid X(\omega)=x_i\}$ i $X=\sum_{i=1}^{n} x_i I_A$.

Definisanje integrala prostih slučajnih promenljiva X možemo izraziti sa:

$$\int X dP = \sum_{i=1}^{n} x_i P(X = x_i) = \sum_{i=1}^{n} x_i P(A_i) \tag{2.67}$$

Definisanje pojma očekivanja slučajnih promenljiva X, koje se obeležava kao (X), vrši se u dva slučaja, i to:

1) Ako se radi o slučajnoj promenljivi X koja je diskretna i ako je ispunjen uslov da je $\sum_{k=1}^{\infty}|x_k|p(x_k)<\infty$, onda važi

$$E(X) = \sum_{k=1}^{\infty} x_k\, p(x_k) \tag{2.68}$$

2) Ako se radi o slučajnoj promenljivi X koja je apsolutno neprekidna i ako je ispunjen uslov $\int_{-\infty}^{\infty}|x|\varphi_x(x)dx<\infty$, onda važi

$$E(X) = \int_{-\infty}^{\infty} x\varphi_X(x)dx \tag{2.69}$$

Pojam centralnog momenta reda k slučajnih promenljiva X moguće je definisati iz izraza u vezi sa X i (X) kao $(X-(X))^k$.

Pod centralnim momentom drugog reda slučajnih promenljiva X podrazumevamo disperziju ili varijansu slučajnih promenljiva X, a njegova oznaka je $D(X)$ odnosno $\sigma^2(X)$.

Pod standardnim odstupanjem ili standardnom devijacijom slučajnih promenljiva X podrazumeva se

$$\sigma(X) = \sqrt{D(X)} \tag{2.70}$$

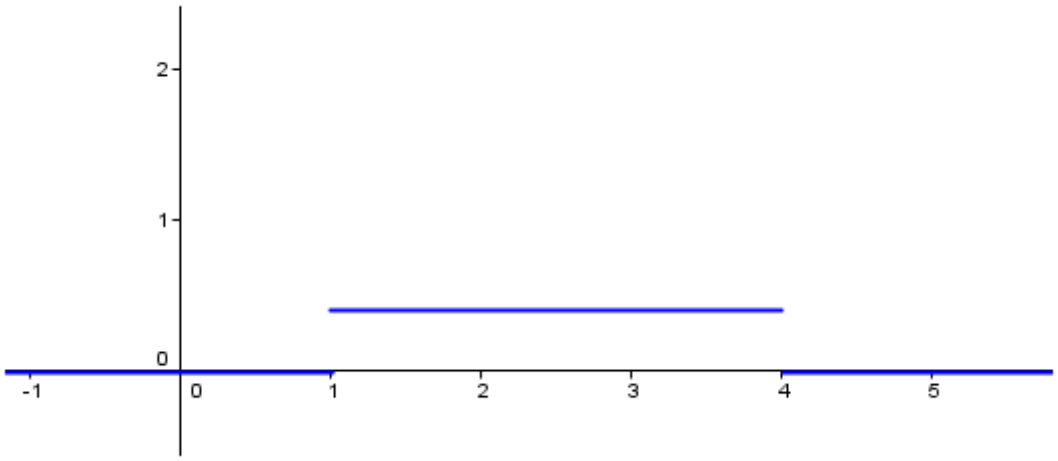
2.3.2. Pregled najčešćih apsolutno neprekidnih raspodela verovatnoće slučajnih promenljiva

Ova disertacija, u čijoj osnovi je stvaranje nizova istinski slučajnih brojeva, bavi se pretvaranjem nizova slučajnih brojeva koji imaju normalnu raspodelu u nizove istinski slučajnih brojeva sa uniformnom raspodelom. Kako se u jednom i u drugom slučaju radi o apsolutno neprekidnim raspodelama bilo je potrebno upoznati se sa karakteristikama i predstaviti grafičke oblike najčešće korišćenih apsolutno neprekidnih raspodela verovatnoća slučajnih promenljiva.

2.3.2.1. Uniformna raspodela slučajnih promenljiva

Za uniformnu raspodelu važi da je jedna od najčešće korišćenih apsolutno neprekidnih raspodela slučajnih promenljiva. Slučajna promenljiva X ima uniformnu raspodelu verovatnoća na intervalu $[a,b]$, $a < b$, odnosno X: $U(a,b)$, pod uslovom da njena gustina raspodele ima oblik

$$\varphi(x) = \begin{cases} \dfrac{1}{b-a}, & x \in [a,b] \\ 0, & inace \end{cases} \tag{2.71}$$



Slika 2.6. *Grafički prikaz funkcije gustine raspodele uniformne slučajne promenljive koja ima parametre* ***a= 1 i b= 4***

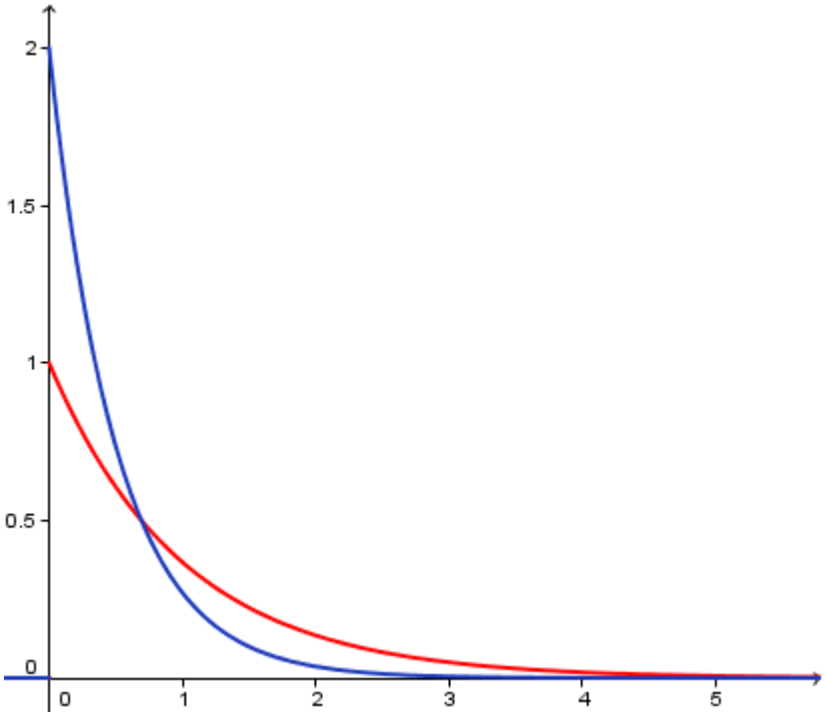
Za funkciju raspodele slučajne promenljive X koja ima uniformnu raspodelu na intervalu $[a,b]$ važi:

$$F_X(x)=\begin{cases}0, & x\in[a,b]\\ \dfrac{1}{b-a}x-\dfrac{a}{b-a}, & a\le x\langle b\\ 1, & x\ge b\end{cases} \tag{2.72}$$

2.3.2.2. Eksponencijalna raspodela slučajnih promenljiva

Za slučajnu promenljivu se kaže da ima eksponencijalnu raspodelu $\varepsilon(\lambda)$, λ>0, odnosno $X:\varepsilon(\lambda)$, ako za njenu gustinu raspodele važi:

$$\varphi(x)=\begin{cases}\lambda e^{-\lambda x} & x\ge 0\\ 0, & x<0\end{cases} \tag{2.73}$$



Slika 2.7. *Grafički prikaz funkcije gustine raspodele eksponencijalne slučajne promenljive čiji je parametar* $\lambda\in\{1,2\}$

Kod funkcije raspodele slučajne promenljive $X:\varepsilon(\lambda)$ važi da je:

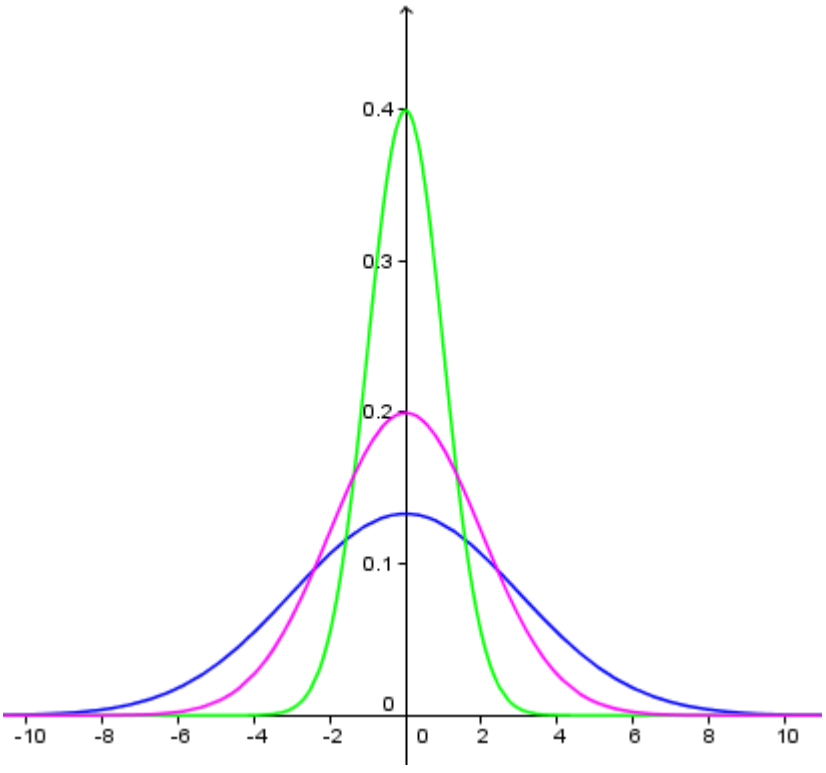
$$F_X(x)=\begin{cases}1-e^{-\lambda x} & x\ge 0\\ 0, & x\langle\ 0\end{cases} \tag{2.74}$$

2.3.2.3. Normalna raspodela slučajnih promenljiva

Za slučajnu promenljivu X se kaže da ima normalnu raspodelu, odnosno X: $N(\mu, \sigma^2)$, ako je $\mu \in \mathbb{R}$ a $\sigma>0$. Ako su parametri $\mu=0$ i $\sigma=1$ dobijamo $N(0,1)$ raspodelu, koja predstavlja standardizovanu normalnu raspodelu i koja se često koristi u teoriji verovatnoće i matematičkoj statistici zbog njenih dobrih karakteristika. Za funkciju gustine normalne raspodele važi:

$$\varphi(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}, x \in R \tag{2.75}$$

gde je μ matematičko očekivanje slučajne promenljive X, a σ njeno standardno odstupanje. Oblici normalnih raspodela sa vrednošću $\mu=0$, za različite vrednosti σ, dati su sledećim grafikom:



Slika 2.8. *Grafički prikaz normalne raspodele čiji su parametri* $\mu=0$ *i* $\sigma \in \{1,2,3\}$

Kod funkcije raspodele slučajne promenljive X koja ima normalnu raspodelu $N(\mu, \sigma^2)$, važi:

$$F_X(x) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{(x-\mu)^2}{2\sigma^2}} dt, x \in R \tag{2.76}$$

3 ZVUČNA KARTICA I ZVUK BUKE U ŽIVOTNOJ SREDINI

Zvuk nastaje, po međunarodno usvojenoj definiciji, kada u elastičnoj sredini nastupi pod dejstvom sile promena položaja čestica određene sredine. Prostiranje zvuka, a samim tim i njegovo nastajanje, moguće je jedino u čvrstim, tečnim i gasovitim sredinama dok u vakumu to nije moguće. U ovoj disertaciji se za stvaranje slučajnih nizova koristi zvuk koji se prostire u vazduhu tako da se u tekstu koji sledi jedino razmatra pojava prostiranja zvuka u vazdušnoj sredini. Zvučni talasi u vazduhu nastaju tako što se čestice vazduha poveraju prenoseći to pomeranje sa jedne na drugu česticu. Na ovaj način stvoreno kretanje čestica vazduha stvara oscilacije čija frekvencija (broj oscilacija u jednoj sekundi) u čujnom opsegu inosi od 20 Hz do 20 KHz. Pojave kretanja čestica koje imaju frekvenciju ispod 20 Hz nazivaju se infra zvuk a one iznad 20 KHz ultra zvuk.

3.1. Zvučni talasi

Postoje dve vrste zvučnih talasa: sferni i ravni. Najčešće se u prirodi susrećemo sa sfernim talasima koji nastaju iz tačkastih zvučnih izvora. Njihova osobina je da se oni u prostoru šire od zvučnog izvora u svim pravcima prostiranja. Tačkaste izvore zvuka moguće je zamisliti kao loptu koja se pulsirajuće povećava, potiskujući čestice vazduha na svojoj površini i koja na taj način stvara zvučne talase.

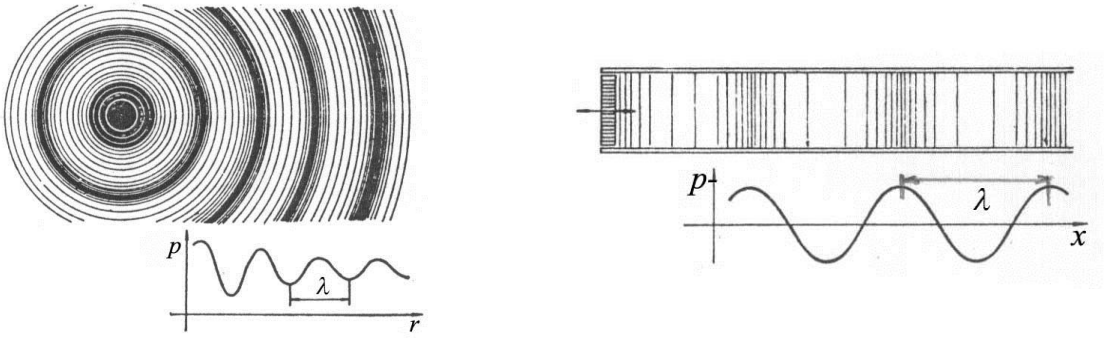
Drugu vrstu zvučnih talasa predstavljaju ravni talasi i njih u prirodi mnogo ređe susrećemo nego sferne. Osobina ovih talasa je da njihova površina osciluje u ravni a ne u obliku sfere kao što je to bilo u slučaju sfernih zvučnih talasa. Ovi talasi su veoma pogodni za laboratorijska eksperimentisanja, jer se veoma lako stvaraju i kontrolišu, čime su posebno dobili na važnosti. Važno je pomenuti i to da udaljavanje od zvučnog izvora sfernog talasa dovodi do toga da sferni talasi prelaze u ravne, što se iz njihove prirode prostiranja i može zaključiti. Ravni talasi se mogu stvoriti pomoću krute ploče (membrane) pomeranjem napred-nazad.

Na slici 3.1 prikazan je način stvaranja i oblik sfernih i ravnih zvučnih talasa.

Brzina prostiranja zvučnih talasa u prostoru u normalnim uslovima (normalni atmosferski pritisak 1 atm, temperatura 20^0 C) iznosi

$$c = 343 m/s \tag{3.1}$$

Temperatura sredine utiče na brzinu prostiranja tako što povećanje temperature dovodi do povećavanja brzine zvučnog talasa. Inače, brzina prostiranja zvučnih talasa ne zavisi od veličine frekvencije niti od toga kakva je složenost zvučnog signala.



a) b)

Slika 3.1. *Sferni i ravni zvučni talasi: a) lopta koja pulsira stvarajući sferne talase, b) stvaranje zvučnih talasa pomoću membrane*

Zvučni talasi prilikom prostiranja prenose akustičku energiju česticama vazduha, koje inače osciluju oko njihovog ravnotežnog položaja. Najvažnije karakteristike ovog oscilovanja su pomeraj čestica ξ i brzina oscilovanja. Što se brzine oscilovanja tiče nju obeležavamo sa v naglasivši njenu vrednost kao vrednost mnogo manju (nekoliko stotina puta) od vrednosti koju ima brzina prostiranja zvučnih talasa.

Relacija koja povezuje pomeraj čestica i brzinu oscilovanja je:

$$\xi = \frac{v}{\omega} \tag{3.2}$$

gde je $\omega = 2\pi f$ kružna frekvencija.

Iz relacije (3.2) može se zaključiti da će se pomeraj čestice smanjivati povećavanjem frekvencije ako je brzina v stalna.

3.1.1. Zvučni pritisak

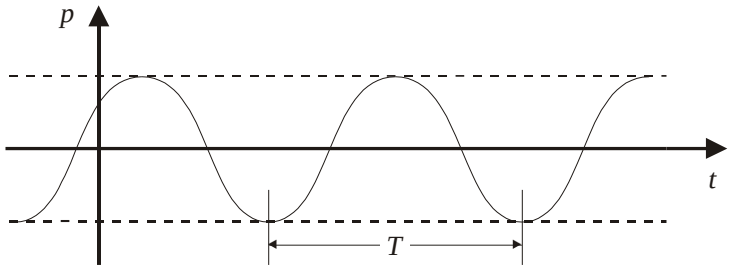
Zvučni pritisak se uvek javlja prilikom pomeranja čestica vazduha, u uslovima postojanja zvučnog talasa, i to važi za sve pravce prostiranja. On se obeležava sa *p* i osnovni je parametar koji karakteriše pojavu zvuka i zvučnog polja.

Za vazduh je karakteristično da je on stalno pod uticajem nekog atmosferskog pritiska (p_{atm}). Kada se ovom pritisku doda zvučni pritisak, u uslovima postojanja zvučnog polja, dobija se relacija za izračunavanje ukupnog pritiska

$$p_u = p_{atm} + p \tag{3.3}$$

Jedinica atmosferskog pritiska je mb (milibar) i njegova vrednost iznosi oko 1000 mb. Vrednost zvučnog pritiska je mnogo manja. Miđutim, usled brzih promena atmosferskog pritiska u kombinaciji sa relativno malim zvučnim pritiskom, dolazi do stvaranja zvučnog pritiska veoma pogodnog za reagovanje našeg čula sluha, stvarajući predispozicije za pravljenje audio uređaja (mikrofona) koje pravimo tako da budu osetljivi baš na te male promene atmosferskog pritiska.

Na slici 3.2 prikazan je prostoperiodični oblik promene zvučnog pritiska u funkciji vremena *t*, gde $T = \frac{1}{f}$, $[T] = s$, predstavlja periodu signala.



Slika 3.2. *Zvučni pritisak (p) i promene u vremenu*

Veličina zvučnog pritiska izražava se jedinicom paskal i označava sa Pa. Sada možemo povezati paskal i bar sledećom relacijom: 1 Pa = 1 N/m^2 = 10^{-5} bar.

3.1.2. Talasna dužina

Talasna dužina je jedna od osnovnih veličina koja karakteriše zvučne talase. Njena oznaka je malo grčko slovo λ. Osvrtom na sliku 3.2 možemo da definišemo talasnu dužinu kao rastojanje između dva maksimalna ili minimalna položaja signala zvučnog pritiska.

Sobzirom da znamo da je *c* brzina prostiranja zvučnog talasa i da je to konstanta, možemo da definišemo relacije

$$c = \lambda \cdot f\ ,\ \lambda = \frac{c}{f},\ \lambda = cT\ . \tag{3.4}$$

Akustika proučava talasne dužine u širokom rasponu granica. Kod najnižih frekvencija vrednost talasne dužine je 17m, dok je kod najviših frekvencija njen iznos 1,7cm. Veličina talasne dužine kao i ogroman raspon vrednosti, od vrlo malih do veoma velikih, su veoma važne

karakteristike zvučnog talasa i veoma su bitne u akustici. Na primer, karakteristike zvučnika, kao vrlo važnog elektroakustičkog pretvarača, veoma mnogo zavise od odnosa talasnih dužina i dimenzije membrane kod tog zvučnika.

3.1.3. Intenzitet zvuka

Zvučni pritisak i intenzitet zvuka su dve veličine akustike od posebne važnosti jer njihove vrednosti ukazuju na promene kod prostiranja zvučnog talasa. Sam intenzitet zvuka označava onu količinu akustičke energije koja prolazi kroz jediničnu površinu, koja je normalna na pravac kojim se prostire zvučni talas, u posmatranoj jedinici vremena. Svi zvučni izvori stvaraju u svojoj okolini intenzitete zvuka koji opadaju udaljavanjem od izvora.

Relacija koja povezuje zvučni pritisak i intenzitet zvuka je

$$J = \frac{p^2}{\rho c} \tag{3.5}$$

gde je ρc konstanta karakteristične sredine.

Navedena relacija važi i kod ravnih i kod sfernih talasa i veoma je korisna u praksi.

Zavisnost intenziteta zvuka i snage izvora zvuka (Pa), koja je izražena W, kreće se u opsegu vrlo malih vrednosti. Ako uzmemo primer ljudskog glasa koji stvara nivo od 64 dB na rastojanju 1m od govornika, tada je vrednost akustičke snage govora oko $10\,\mu W$. Akustičkom snagom se predstavljaju osobine zvučnih izvora i ona predstavlja energiju koja u jedinici vremena prođe kroz površinu obuhvaćenu izvorom.

Sada je moguće, poznavanjem snage zvučnog izvora, odrediti intenitet zvuka na rastojanju *r*, koristeći relaciju:

$$J = \frac{P_a}{4\pi r^2},\ [J] = \mathrm{W/m^2}. \tag{3.6}$$

Iz date relacije primećujemo opadanje intenziteta zvuka sa kvadratom rastojanja, što je vrlo važna karakteristika zvuka. Kako je zvučni pritisak na kvadrat srazmeran intenzitetu zvuka (3.5), on će linearno opadati sa rastojanjem od zvučnog izvora. Tako da sada možemo definisati izraz koji povezuje zvučni pritisak i rastojanje od zvučnog izvora (*r*), kao

$$p \cdot r = const. \tag{3.7}$$

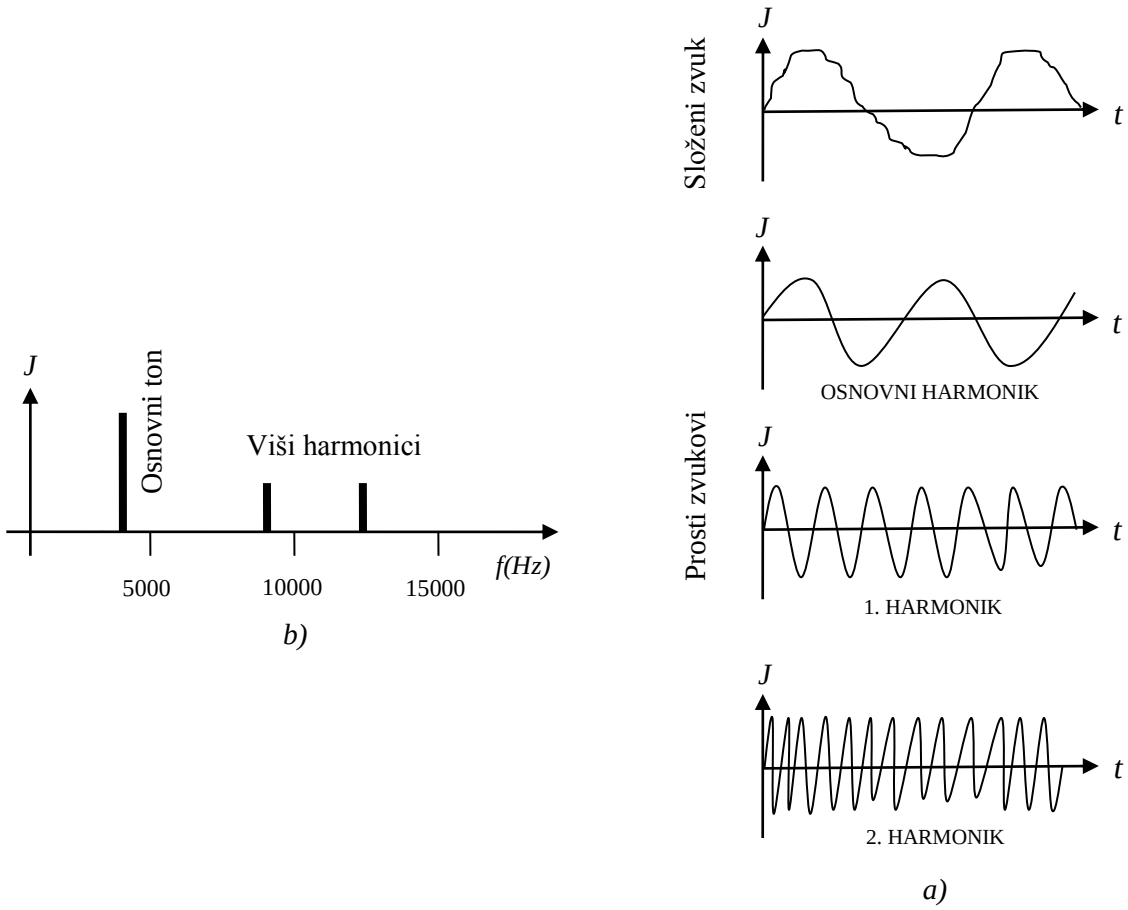
Izraz (3.6) intenziteta zvuka, ima u imeniocu $4\pi r^2$ (površina loptaste sfere), odnosi se na sferne talase, to jest na zvučne izvore koji zrače u svim pravcima podjednako. 4π predstavlja konstantu, odnosno veličinu punog prostornog ugla zračenja izvora zvuka. Ovaj ugao nije uvek pun jer izvor zračenja može da koristi samo deo raspoloživog prostora. Ukoliko imamo takav slučaj dolazi do promene izraza u imeniocu, koji će se smanjiti, čime se pri istoj snazi zvučnog izvora dobija povećanje intenziteta. Ukoliko, na primer, zvučnik koji zrači približimo zidu smanjićemo mu na pola prostorni ugao zračenja (koji sada iznosi 2π), u pitanju je zračenje u polusferi, tada se intenzitet zvuka duplo povećava sa izvorom koji ima istu snagu i na istom rastojanju od njega.

3.1.4. Prost i složen zvuk

U zavisnosti od spektralog sadržaja zvuka razlikujemo prosti i složeni zvuk.

Prost zvuk je onaj zvuk čiji spektar sačinjava samo jedna komponenta određene frekvencije i određenog intenziteta (nivoa). Prikazuje ga jedna linija linijskog spektra (slika 3.3) i u prirodi se veoma retko sreće. Primer prostog zvuka je recimo kratak ujednačeni zvižduk. Prost zvuk se inače proizvodi generatorom pojedinačnih tonova koji se naziva ton generator. Na vremenskoj osi predstavljen prost zvuk je jedna čista, prosta sinusna oscilacija. Ovakav zvuk se ne može razložiti.

Složeni zvuk predstavlja kombinaciju prostih zvukova. Razlikujemo dve vrste složenih zvukova. Prvu vrstu čine dve ili više komponenti različitih frekvencija, čije se vrednosti intenziteta u zavisnosti od frekvencije (spektri) prikazuju linijskim spektrima. Na primer odsviran akord na gitari, koji predstavlja skup čistih tonova istovremeno proizvedenih, ili zvuk koji proizvodi automobilska sirena sa više tonova. Drugu vrstu složenih zvukova čine oni koji imaju kontinualni spektar frekvencija. Zavisnost intenziteta zvuka od frekvencije prikazuje se neprekidnom krivom obvojnicom što praktično znači da signal zvuka sadrži ogroman broj komponenata sa različitom frekvencijom a samim tim i sa različitim intenzitetom za svaku komponentu. U prirodi se zvuk sa kontinualnim spektrom najčešće sreće. Ovakav složeni zvuk nazivamo šum (na primer šum buke u životnoj sredini).



Slika 3.3. *Karakteristike jednog složenog zvuka a)Vremenski oblik signala složenog zvuka b)Frekvencijska karakteristika složenog zvuka*

Razlaganjem složenog zvuka na više prostih zvukova primećujemo zvuk najniže frekvencije koji se naziva osnovni ton ili osnovni harmonik a ostali prosti zvukovi su viši harmonici.

3.1.5. Istovremeno zračenje više izvora

U prirodi se najčešće sreću slučajevi istovremenog zračenja više izvora a ređe zračenja pojedinačnih izvora. To je pogotovo primetno u urban sredinama velikih gradova gde se zvučno polje formira zračenjem velikog broja različitih izvora zvuka, od saobraćajne buke, preko buke koju stvaraju industriska postrojenja do buke šetača na ulicama. Da bi se znalo kojim intenzitetom zvuka raspolažemo, u takvim uslovima, i da bi se odredio zvučni pritisak u uslovima istovremenog emitovanja zvuka više izvora, potrebno je poznavati sledeća pravila.

Zvuk koji ima određeni intenzitet stvaraju svi zvučni izvori zračećoko sebe u prostoru. U slučaju zračenja većeg broja izvora dolazi do sabiranja zvučnih egergija pojedinačnih izvora što

podrazumeva sabiranje njihovih intenziteta.

Jednačina za izračunavanje ukupnog intenziteta zvuka, koga stvara više izvora zračenja istovremeno zračeći zvuk u prostoru, mogla bi se odrediti kao:

$$J = J_1 + J_2 + J_3 + \cdots + J_n, \qquad [J] = \mathrm{W/m^2} \tag{3.8}$$

odakle se vidi da je ukupan intenzitet jednak zbiru pojedinačnih intenziteta.

Kod zvučnog pritiska treba imati u vidu činjenicu srazmernosti intenziteta zvuka sa kvadratom pritiska, tako da je:

$$p = \sqrt{p_1^2 + p_2^2 + p_3^2 + \cdots + p_n^2}\,, \quad [p] = \mathrm{P_a}. \tag{3.9}$$

Pošto se intenziteti mnogo lakše sabiraju nego pritisci u praksi je praktičnije izračunati ukupni intenzitet pa tek onda, na osnovu dobijenih rezultata za intenzitet, izračunati ukupni zvučni pritisak.

3.1.6. Slabljenje zvuka

Poznato je da prilikom prostiranja zvučnih tasa, intenziteti zvuka opadaju sa kvadratima rastojanja, što znači da pritisci opadaju sa rastojanjem, a razlog tome je činjenica da se talasi šire i pritom prenose akustičku energiju na sve veći broj čestica vazduha. Ovo pravilo uvek važi i do slabljenja usled širenja talasa uvek dolazi. Talasi sačinjeni od viših frekvencija više slabe dok niže frekvencije imaju manje slabljenje.

Pored ovog osnovnog slabljenja, koje je prouzrokovano širenjem talasa, postoji još jedno dodatno slabljenje koje se javlja zbog neizbežnih gubitaka koji se javljaju prilikom prostiranja talasa naročito zbog gubitaka akustičke energije. Faktori koji utiču na ovo dodatno slabljenje su, pre svega, uticaji viskoznosti vazduha, procesi odvođenja toplote kao i pojava rezonansija u molekulima.

Što se faktora viskoznosti tiče, treba naglasiti da je on stalno prisutan i on nastaje međusobnim trenjem čestica vazduha, usled njihovog oscilovanja različitim brzinama. Porast ovih gubitaka je evidentan sa rastom frekvencije, tako da na visokim frekvencijama postoji njihova izraženost. Toplotni gubici nastaju sabijanjem i razređivanjem čestica vazduha kroz koga se zvučni talasi prostiru. I za ove gubitke važi pravilo da se povećavaju na višim frekvencijama.

Posebno važnu ulogu kod gubitaka usled rezonansije u molekulima, koji takođe nastaju

kao posledica sabijanjem i razređivanjem čestica vazduha, ima uticaj vlažnosti. U uslovima veće vlažnosti ovi gubici rastu, dok su pri manjoj vlažnosti i oni mali.

Za intenzitet zvuka u realnim uslovima, uzimajući u obzir navedene faktore slabljenja na nekom rastojanju *x*, sada je moguće koristiti sledeći izraz:

$$J = J_0 \mathrm{e}^{-mx}, \tag{3.10}$$

gde je J_0 – intenzitet zvuka, na nekom rastojanju *x*, bez dodatnih faktora slabljenja, dok *m* predstavlja koeficijent slabljenja zavistan od frekvencije i koji se daje tablično.

Sam proračun slabljenja, u realnim uslovima, je vrlo delikatan posao i zahteva ozbiljan pristup i analizu.

3.1.7. Difrakcija i refrakcija

Poznato je da se slobodnim prostorom zvučni talasi šire bez smetnji. Važe već navedena pravila intenziteta zvuka i zvučnog pritiska sa promenom rastojanja od izvora zračenja. Međutim, u slučaju nailaska na neku prepreku prilikom prostiranja zvučnog talasa, zvučni talas menja pravac prostiranja. Ove fizičke prepreke direktno utiču na pravolinijsko kretanje talasa ali na takvo njegovo kretanje imaju uticaj i promene temperature vazduha koje su naročito izražene u slojevima vazduha u blizini zemljine kore i neposredno iznad vodenih površina.

Postoje dve vrste pojava koje utiču na promenu pravca zvučnog talasa, i to: difrakcija i refrakcija.

Kod difrakcije je karakteristično to da se ona javlja u slučaju talasa zvuka manje talasne dužine od dimenzija prepreke. U slučaju veće prepreke od talasne dužine imamo veću izraženost difrakcije. Kada je slučaj takav da je vrednost talasne dužine veća od dimenzije prepreke dolazi do pojave zaobilaženja zvučnog talasa prepreke, bez ikakvog ometanja ili promene pravca.

Difrakcija dovodi do poremećaja koje objašnjavamo na sledeći način. Dolaskom zvučnog talasa do prepreke dolazi do njegovog reflektovanja i stvaranja veće koncentracije zvuka na prednjoj strani prepreke, to znači da dolazi do povećanja nivoa zvuka usled sabiranja direktnog i reflektovanog talasa. Na drugoj strani prepreke dolazi do stvaranja tzv. ''mrtve zone'' sa znatno smanjenim nivoom zvuka, što pogotovo važi za visoke frekvencije iz razloga male talasne dužine u odnosu na dimenzije prepreke.

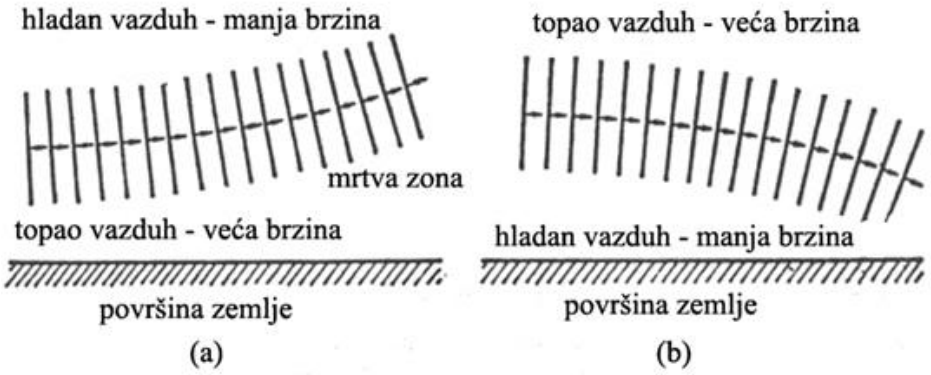
Difrakcija ponekad može biti i poželjna, na primer ukoliko se želi smanjivanje nivoa

zvuka neke zone može se postaviti prepreka čije će dimenzije biti veće nego što je to talasna dužina dužina neželjenog izvora zvuka.

Kod refrakcije je karakteristično to da ona takođe utiče na promenu pravca kretanja zvučnih talasa ali se javlja kao posledica različitih brzina zvuka u različitim slojevima vazduha.

Na brzinu prostiranja zvučnih talasa pre svega utiče temperatura vazduha. U slučajevima toplijeg vazduha dolazi do povećanja brzine prostiranja i obratno što je vazduh hladniji brzina je manja. Zavisnost brzine prostiranja od temperature dovodi do toga da prenošenje akustičke energije, koju stvara zvučni izvor u prostoru oko sebe, odstupa od pravolinijskog kretanja. Prave linije, po kojima se zvučni talasi prostiru, postepeno se savijaju. Pojava refrakcije zvučnih talasa prikazana je slikom 3.4.

Refrakcija zvučnih talasa dovodi do toga da se mogu pojaviti mrtve zone u kojima se zvuk mnogo slavije čuje ili da ga čak uopšte nema.



Slika 3.4. *Uticaj različitih temperatura i promene pravca prostiranja zvučnog talasa: a) tokom dana, b) u toku noći*

3.1.8. Koeficijenti refleksije i apsorpcije

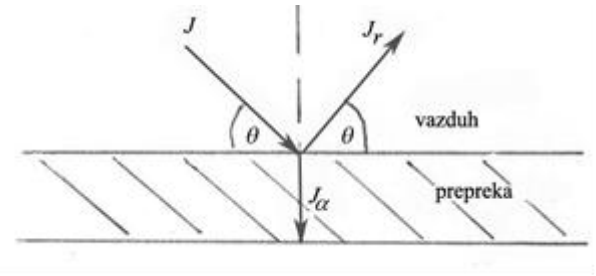
Kada zvučni talasi naiđu na neke prepreke delovi njihovih energija se reflektuju dok se jedan deo apsorbuje. U praksi je veoma važan taj odnos reflektovane i apsorbovane energije. Materijal prepreke, u pogledu njegovih različitih karakteristika, može u mnogo čemu uticati na apsorciju i refleksiju zvučnog talasa. U cilju brojnog izračunavanja pojava apsorcije i refleksije uvedeni su koeficijenti za apsorciju i refleksiju.

Susret zvučnog talasa sa preprekom prikazan je na slici 3.5. Intenzitet ovog talasa, odnosno njegovu snagu, označavamo sa *J*. Nailaskom na prepreku intenzitet ovog talasa biće

delom reflektovan (J_r), a delom apsorbovan od strane prepreke (J_α).

Tako da dobijamo da je:

$$J = J_r + J_\alpha, \quad [J] = \text{W/m}^2 \tag{3.11}$$



Slika 3.5. *Refleksija i apsorcija jednog zvučnog talasa*

Deljenjem svih članova jednačine (3.11) sa *J*, dobija se:

$$1 = \frac{J_r}{J} + \frac{J_\alpha}{J} \tag{3.12}$$

gde su $\frac{J_r}{J} = r$, i $\frac{J_\alpha}{J} = \alpha$, koeficijenti refleksije i apsorpcije, respektivno.

Zamenom u gornjoj jednačini uspostavlja se veza

$$\alpha + r = 1 \tag{3.13}$$

Što znači da je zbir ovih koeficijenata uvek jedak jedinici. U slučaju da se jedan povećava drugi se smanjuje i obratno. Njihovi iznosi se mogu kretati u granicama od 0 do 1 tako da važi: $0 \le \alpha \le 1$ i $0 \le r \le 1$.

3.2. Zvučna kartica

Zvučna kartica je deo matične ploče računara, sastavljen iz više analogno-digitalnih konvertora koji omogućuju obradu digitalnog zvučnog signala u računaru.

Zvučna kartica kod kućnih računara proizvodi zvuk koristeći dve potpuno različite tehnike. Prva tehnika se zasniva na sintezi zvuka, slično kao kod muzičkih sintisajzera, - tako što se reprodukuje MIDI zapis (na primer .mid ili .rmi), dok se kod druge tehnike reprodukuje PCM zapis zvučnih signala (na primer .wav ili .au).

Slika 3.6. *Zvučna PCI kartica računarskog sistema*

Kod savremenih računara zvučne kartice su već ugrađene na matičnoj ploči ili postoje posebni slotovi u koje se dodatno ubacuju PCI (Peripheral Component Interconnect) zvučne kartice.

Kada se reprodukuje MIDI (Musical Instrument Digital Interface) zapis šalju se standardizovani kodovi (vrste muzike, nota, tempa, jačine panorama, glasnoće, brzine udaranja tipki ili različitih efekata) na odgovarajući MIDI procesor koji je zadužen da proizvodi određeni zvuk.

U zavisnosti od toga koji se MIDI procesor koristi dobijaju se različiti kvaliteti zvuka, međutim nemoguće je izvršiti zapis ili reprodukciju instrumenata, koji ne obuhvataju standardni skup MIDI instrumenata, ili vokala. Kod PCM zapisa moguće je zapisivanje kao i reprodukcija praktično svih vrsta zvučnih signala.

3.2.1. Vrste, tipovi i priključci zvučnih kartica

Skoro svi proizvođači prave matične ploče sa ugrađenim zvučnim karticama tako da njihove karakteristike i mogućnosti (obično veoma skromne) zavise od proizvođačevog izbora, ali je dobro to što na matičnim pročama postoje slotovi u kojima je moguće dodati zvučnu karticu prema sopstvenim potrebama.

Postoje dve vrste zvučnih kartica koje se ugrađuju, u zavisnosti od vrste slota, i to ISA i PCI. ISA kartice su već zastarele, tako da se danas skoro isključivo koriste PCI kartice sa svojom sopstvenom memorijom i neuporedivo boljim karakteristikama.

Na spoljnoj strani zvučne kartice postoji nekoliko ulaznih bananica za priključak

mikrofona, spoljnjeg audio uređaja i izlazni priključci za zvučnike. Sa unutrašnje strane zvučnih kartica (kućište računara) nalaze se pored sintetizatora, pojačala, DSP procesora, CD konektora i A/D i D/A konvertori.

Savremene zvučne kartice podržavaju i obradu audio signala u realnom vremenu uz mogućnost dodavanja 3D efekta, za šta je zadužen DSP procesor. Zvučna kartica može i da snima zvuk, tako da joj je uz reprodukciju kompletirana mogućnost emitovanja i obrade audio signala. Pri snimanju zvuka se može koristiti već postojeći mikrofon računara, ili se koristi dodatni, a potreban je i neki od mnogobrojnih programa za snimanje.

3.2.2. MIDI protokol

MIDI protokol je nastao 1982 godine kada se koristio za potrebe muzičara i kompozitora, tako da je vrlo brzo postao najčešće korišćeni protokol muzičkih studija. Njegovim korišćenjem bila je omogućena razmena informacija između muzičkih instrumenata, međutim kako nije postojao standard bilo je omogućeno proizvođačima da protokol realizuju kako njima odgovara, što je za posledicu imalo neusklađenost opreme i nemogućnost međusobne komunikacije. Standardizovanjem ovog protokola definisan je raspored ogromnog broja instrumenata čime su postavljene osnove za korišćenje kompletne MIDI opreme.

Jednostavnim rečima opisano, MIDI protokol se može smatrati skupom uputstava korišćenja muzičke opreme. On se ne sastoji iz digitalizovanog zvuka već iz kolekcije nota i skupa efekata koji se mogu koristiti prilikom njigove realizacije. MIDI kompozicija sadrži uputstvo kako se svira određeni ton kao i to koji se efekti mogu upotrebiti.

Tehničkim jezikom rečeno, podaci MIDI toka predstavljaju asinhrone jednosmerne tokove bita, čija je brzina 31,25 Kbit/s, koji se prenose u paketu od po 10 bita. Osam bita su zadužena za nošenje korisne informacije dok su prvi start a poslednji stop biti. Prenos podataka je serijski tako da postoji kašnjenje prilikom reprodukcije tonova koji se sviraju istovremeno, međutim, to kašnjenje iznosi svega par milisekundi i kao takvo je zanemarljivo sobzirom na to da ga ljudsko uvo ne može registrovati.

Najvažniji zadaci MIDI računarske opreme su što vernija reprodukcija zvuka svakog realnog instrumenta i mogućnost sintetizovanja zvuka električnih instrumenata. Složenost akustičkih zakona kao i subjektivni doživljaj koji ostavlja zvuk na slušaoce, čine ove postupke veoma teškim za realizaciju. Tehničke karakteristike zvuka, oblici i jačine rasta tonova kao i vreme opadanja tonova, predstavljaju činioce koji u najvećoj meri utiču na kvalitet zvuka čime

se procesi sinteze dodatno komplikuju.

Tehnika sinteze bazirana je na korišćenju ROM-a zvučnih kartica računara, u kojima se smeštaju digitalizovani podaci svakog realnog instrumenta, i ima za cilj njihovu što verniju reprodukciju. Kako dobar kvalitet digitalizovanih audio podataka zahteva trošenje dobrog dela raspoložive memorije, neophodno je korišćenje posebnih tehnika radi uštede memorijskog prostora. Iz tog razloga se na primer ne vrši digitalizacija čitavih zvučnih opsega koje neki instrumenti proizvode, već se upotrebljava sistem tehnike visinskog pomeraja tona. Naime, prvo se vrši smeštanje samo jednog tona određenog instrumenta a zatim se pristupa menjanju visine tog tona. I to se radi za svaki ton koji proizvodi taj instrument čime se pravi njegova grupa tonova. Isti postupak važi za sve korišćene instrumente. Napravljene grupe se u obliku tabela smeštaju u memoriji kartice i potpuno su spremne za brzu upotrebu.

Treba naglasiti i to da je za dobijanje zvuka visokog kvaliteta proces sinteze neophodan, a to se može postići ili korišćenjem kvalitetnih ali skupljih zvučnih kartica, ili kupovinom jeftinijih zvučnih kartica i dodatnom nabavkom aplikacije koja softverski stvara sintezu, uz korišćenje jakog procesora.

3.2.3. Digitalni zvuk i formati zvučnih zapisa

Pretvaranje anolognog signala zvuka u digitalni oblik obavlja se u tri faze. U prvoj fazi vrši se odmeravanje ili uzorkovanje, u drugoj kvantovanje a u trećoj kodovanje. Sklop koji vrši postupak pretvaranja naziva se analogno-digitalni (AD) konvertor. AD konvertor prvo vrši odmeravanje analognog signala (važno je istaći da su ti vremenski razmaci uvek isti i da predstavljaju *n*-ti deo sekunde), nakon čega se dobijaju odmerci određenih vrednosti *m*, koji se zatim u postupku kvantovanja zaokružuju na neke približne vrednosti, a onda se tako dobijenim vrednostima dodeljuju određeni binarni kodovi. Na taj način se decimalne vrednosti svakog odmerka pretvaraju u binarne podatke, koje računar koristi za svoj rad, a kontinualni analogni signal se pretvara u digitalni impulsni signal.

Podaci dobijeni konvertovanjem se u binarnom obliku čuvaju u određenom audio fajlu, a zvučna kartica ih koristi prilikom rekonstrukcije zvučnog signala tako što preko svojih digitalno-analognih konvertora (DA) vrši inverzan postupak, u ovom slučaju pretvaranje digitalnog signala u analogni zvučni signal.

Nabrojaćemo najvažnije karakteristike postupka analogno-digitalne konverzije.

- Brzina odmeravanja – to je broj odmeraka koji se uzima u jednoj sekundi (jedinica za merenje je Hz). Standardna brzina odmeravanja je: 11.025KHz, 22.05KHz ili 44.1KHz.
- Vrednost odmerka – to je broj bita koji se koristi za opisivanje odmerka, na primer odmerak koji ima 8 bita poseduje mogućnost od 256 kombinacija za predstavljanje odmeraka. Kvalitet zvuka se povećava sa većom brzinom odmeravanja i većim brojem uzoraka.
- Veći kvalitet zvuka podrazumeva i porast veličine fajlova.
- Veličina digitalnog zvučnog fajla (u bajtima) određuje se formulom: brzina odmeravanja X posmatrano vreme (sekundi) X (vrednost odmerka/8) X M. Kod mono snimaka M = 1 a kod stereo snimaka M = 2. Na primer, zvuk trajanja 10 sec. koji se snima brzinom 22,05KHz i odmercima veličine 8-bita veličina fajla je 22050 X 10 X 8/8 X 1 = 220.500 bajta.

Potrebno je navesti i ogromnu razliku MIDI fajla i digitalnog audio fajla. Naime, u slučaju digitalnog fajla digitalne kompozicije su originali snimljeni u binarnom zapisu, dok su u slučaju MIDI-ja kompozicije raščlanjene po pojedinačnim instrumentima i mogu se pojačavati, smanjivati, odnosno nezavisno obrađivati. Digitalni muzički fajlovi su veličine reda nekoliko MB dok MIDI zauzimaju prostor od oko 50 KB. Međutim, dok digitalna kompozicija može sadržati i glas vokala, MIDI kompozicija to ne može jer se ne može sintetizovati. Praktično, MIDI fajlovi su muzičke matrice pesama i imaju mogućnost editovanja svakog instrumenta.

Format zvučnog zapisa

Najpoznatiji audio formati koje računari koriste su: .wav, .au, .ra, komprimovani formati kao na primer .mp3 itd.

- midi .mid MIDI formati
- wave .wav Majkrosoftovi formati digitalnih zvučnih fajlova
- audio interchange file format .aif Mekintošovi formati digitalnih fajlova
- CD format .cda Formati zvučnog zapisa na CD-u
- sun audio .au Sun-ov kompresovani digitalni format
- windows media audio codec .wma Majkrosoftov kompresovani format
- mpeg audio layer 3 .mp3 Kompresovani formati

Kod komprimovanja zvučnih fajlova neophodna je posebna šema kompresije tzv. kodek. Ima više vrsta kodeka ali je nekoliko verzija MPEG verovatno najpopularnije za audio zapise.

3.2.4. Impulsno-kodna modulacija PCM (Pulse Coded Modulation)

PCM tehnika omogućuje zapisivanje i reprodukciju praktično svih vrsta zvučnih signala. Međutim, postoje i ograničenja i to:

- ograničenja koja se odnose na frekvencijski opseg, i
- ograničenja koja se odnose na dinamiku.

Filter propusnik niskih frekvencija i korišćena frekvencija odmeravanja f_{sr}, su odlučujući faktori kojima se određuje raspoloživost frekvencijskog opsega dok je gustina kvantnih nivoa ograničavajući faktor korisne dinamike zvučnih signala.

U zavisnosti od zahtevanog kvaliteta zapisa zvučnog analognog signala različite su i vrednosti gornje granične frekvencije zvučnog signala f_m, frekvencije odmeravanja f_{sr} i gustine kvantovanja kod određenog bitskog zapisa odmerka sa brojem bita *n*. Podaci ovih karakterističnih parametata, za pomenutu praktičnu primenu PCM, prikazani su u tabeli 3.1.

Tabela 3.1. Vrednosti podataka za praktičnu primenu PCM-a

Namena PCM-a	f_m [KHz]	f_{sr} [KHz]	Kvantovanje [bita]
Telefonija	3,400	8	8
CD	20	44,1	16
DAT	22	48	16
Muzički uređaji	do 44	do 96	18, 20, 24, 32

3.2.5. Ograničenja koja se odnose na frekvencijski opseg

Gornju graničnu frekvenciju f_m praktično određuje frekvencija odmeravanja f_{sr} koju koristimo prilikom impulsno-kodne modulacije.

Prigušenje većih frekvencija od f_m je veoma izraženo a krivicu za to snosi niskopropusni filter i njegova oštra pravougaona karakteristika. Niskopropusni filter je inače nezaobilazan

element u postupku filtriranja ulaznih signala, odnosno sprečavanja pojave neželjenih izobličenja koje se javljaju ukoliko ulazni signali sadrže komponente čije su frekvencije veće od $f_{sr}/2$.

Praktično, vrednosti f_m su nešto manje jer na nju utiču utiču parazitne kapacitivnosti elektronskih sklopova zvučnih kartica. Uobičajeno se za frekvenciju odmeravanja, kod standardne zvučne kartice, koristi frekvencija f_{sr} = 44,1 KHz sa gornjom graničnom frekvencijom f_m = 20 KHz.

Vrdenost donje granične frekvencije je na ulazu za spoljne audio uređaje (line in) standardne zvučne kartice oko 5 Hz, dok je na ulazu za mikrofon (mic in) oko 15 Hz. Na veličinu ove granične frekvencije utiču kondenzatori raspoređeni neposredno iza ovih priključaka zvučne kartice.

Postavljanje kondenzatora na ulazima zvučnih kartica je u fukciji brisanja jednosmernih komponenata ulaznih audio signala. To praktično znači da se zapis izvornih signala u računaru vrši bez jednosmernih komponenata i sa prigušenjem niskih frekvencija koje su mane od f_d jačinom 20 dB/dekadi.

3.2.6. Ograničenje dinamike

Zbog ograničenja gustine kvantnih nivoa, na osnovu kojih se vrši kvantovanje izvornog signala, u procesu kvantovanja dolazi do pojave grešaka koje smatramo kvantizacijskim šumom. Ako se svakom od nivoa kvantovanja dodeli jedna od kombinacija dužine *n* bita, onda se kontinualni amplitudni opseg, koji poseduje izvorni signal, treba preslikati ograničenim skupom od 2*n* različitih nivoa amplituda, kojima se potom dodeljuje binarni kod. Iz tog razloga, sve amplitude koje se nalaze u istom diskretnom intervalu dobijaju isti binarni broj. Pojava kvantizacijskog šuma prati svaki proces PCMa i utiče na ograničenje korisne dinamike. Kod gustine kvantovanja, kod koje je *n* = 16 bita, odnos signal-šum (S/N) iznosi 98,08 dB, dok je kod 8 bitskog kvantovanja taj odnos mnogo manji i iznosi 49,93 dB. Zapis amplituda signala, sa 16-to bitskom gustinom kvantovanja, u računaru se vrši 16-to bitskim intidžer brojevima, to jest u opsegu od -32768 ÷ +32767. Najmanja brojna vrednost odgovara najvećoj vrednosti negativne amplitude a najveća brojna vrednost odgovara najvećoj vrednosti pozitivne amplitude.

Osim šuma kvantizacije na korisnu dinamiku zvučnih kartica utiču i klasični šumovi koje stvaraju elektronske komponente i sklopovi same zvučne kartice, tako da je praktično njihova korisna dinamika oko 80 dB pri 16-to bitskoj gustini kvantovanja.

3.2.7. Mikrofoni

Mikrofoni su elektroakustički pretvarači koji akustičku energiju pretvaraju u električnu. Preciznija definicija je da su to uređaji koji vrše pretvaranje zvučnog pritiska, kao ulazne veličine, u električne signale na njihovom izlazu. Može se reći i to da je radna sredina mikrofona vazduh, pre svega zato što je to medij koga zvučni talasi koriste za svoje prostiranje.

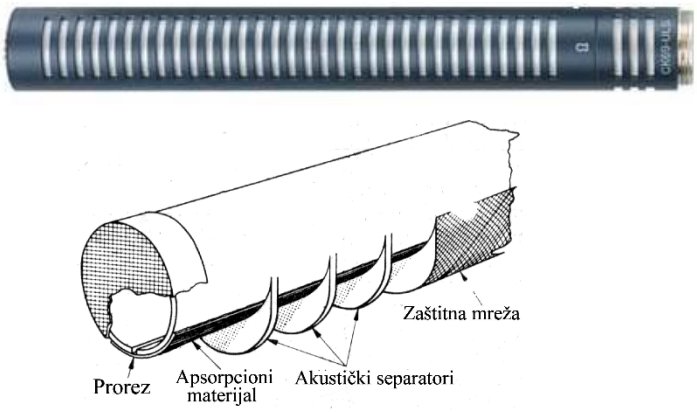
Slika 3.7. *Studijski mikrofon*

Mikrofon je uređaj koji u praksi ima široku primenu. Glavni deo mikrofona je mikrofonska kapisla, u kojoj se obavlja proces pretvaranja, ali sadrži i druge delove koji su takođe važni za njegov rad a koji su zaduženi za obavljanje različitih funkcija. To su, pored ostalih, zaštitne mrežice kapisla, kućišta prilagođena određenim namenama, konektori za povezivanja sa kablovima, itd. Neki mikrofoni u svom sastavu imaju transformatore koji vrše prilagođavanje impedansi, neki sadrže pojačavače a neki sklopove jednostavnih filtarskih kola.

Što se savremenog razvoja tiče, on se kreće u dva smera. Prvi se zasniva na težnji za vrhunskim kvalitetom pretvaranja, tako da se današnji kvalitetni mikrofoni mogu pohvaliti odličnim prenosnim karakteristikama. Danas se izrađuju mikrofoni sa donjom graničnom frekvencijom manjom od 1 Hz a postoje i oni kod kojih je gornja granična frekvencija nekoliko stotina KHz pa i veća. Neretko se može sresti mikrofon koji registruje zvuk nivoa preko 170 dB ili mikrofon koji registruje nivo zvuka ispod 0 dB.

Razvoj mikrofona koji ide drugim smerom zasniva se na težnji pravljenja što jeftinijeg mikrofona, koji bi se masovno proizvodio, koji bi imao odlične karakteristike i koji bi se mogao koristiti za različite svrhe. Mikrofone takvih karakterisika već uveliko koriste razne oblasti, kao

što su na primer telefonija, multimediji i druge slične oblasti.



Slika 3.8. *Specijalni mikrofon sa talasovodom – često se naziva i puška mikrofon ili samo puška, zbog svog fizičkog oblika i karakteristika usmerenosti*

Postoje tri najvažnija parametara koja definišu mikrofone kao elektroakustičke pretvarače, i to:

- faktor elektroakustičkog pretvaranja (osetljivost mikrofona),
- dinamički opseg mikrofona (odnos najvišeg i najnižeg nivoa zvuka) i
- usmerenost mikrofona.

3.2.7.1. Faktor elektroakustičkog pretvaranja (osetljivost mikrofona)

Faktorom pretvaranja opisuje se osnovne odlike, odnosno karakteristike, mikrofonskih uređaja prilikom pretvaranja zvučnog signala u električni signal. Njime se definiše veza između ulaznih i izlaznih veličina u procesu pretvaranja, to jest on predstavlja parameter sposobnosti mikrofona da pobudni pritisak pretvori u elektromotornu silu. Ovaj faktor često nazivamo osetljivošću mikrofona i obeležavamo ga malim slovom *s*.

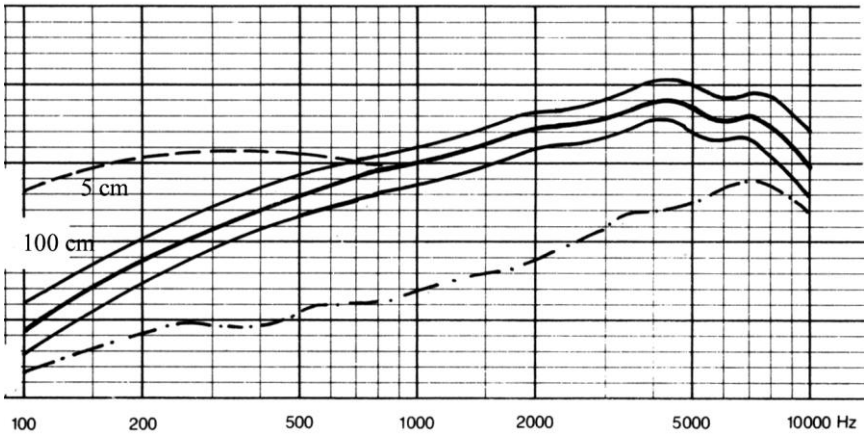
Faktor mikrofona zavisi od mnogo činioca. Prvo, on zavisi od veličine membrane koja svojom površinom utiče na silu pritiska zvučnog signala koji deluje na nju.

Drugo, on zavisi i od mehaničkih parametara membrane, odnosno od njene osetljivosti na mehaničke podude. Ulazne veličine membrane, kao osnovnog faktora prenosa u procesu pretvaranja, su sile koje na nju deluju a izlazne veličine su pomeraji i brzine oscilovanja.

Ovaj faktor je zavistan i od samog mehaničkog mehanizma rada membrane.

3.2.7.2. Dinamički opseg mikrofona

Ovaj parametar određuje granice upotrebljivosti mikrofona odnosno raspon nivoa zvuka na koji on deluje. Ovaj raspon se kreće od najmanjeg nivoa zvuka, koji se korektno pretvara u električni signal (donja granica dinamičkog opsega), do najvećeg nivoa zvučnog signala, koga mikrofon u okviru razumnih izobličenja pretvara u električni signal (gornja granica dinamičkog opsega). Treba reći i to da gornju granicu određuju linearnosti mehaničkog odziva membrana. Kao što je poznato, svaka membrana ima ograničene mogućnosti kretanja, odnosno ograničenu brzinu oscilovanja kao i fizički raspon mehaničkog pomeraja, tako da kada se dostignu te mehaničke granice dobija se izlazni signal sa ogromnim izobličenjima. Zato svaki mikrofon ima granice svoje upotrebljivosti koje pre svega zavise od njegovih mehaničkih karakteristika.



Slika 3.9. *Frekvencijska karakteristika diferencijalnih mikrofona*

Donju granicu osetljivosti mikrofona određuju sopstveni termogeni šumovi mikrofona. Naime, mikrofon u kombinaciji sa određenim pojačavačem predstavlja strujno električno kolo. Ovo električno kolo osim generatora željenog signala *ep* sadrži i generator termičkog šuma sa elektromotornom silom *eN*. Tako da veličina donje granice osetljivosti mikrofona osim od mehaničkih karakteristika mikrofona zavisi i od parametara njihovih električnih kola.

U svakom slučaju, električni signal, koji se dobija pretvaranjem željenog zvučnog signala, mora biti dosta veći u odnosu na sopstveni termogeni šum kako bi se izobličenja zadržala u razumnim okvirima.

Međutim, problem svih mikrofona kao elektroakustičkih pretvarača je u njihovom niskom nivou dobijenog električnog signala zvog čega je ostavljen veliki prostor štetnom delovanju termičkog šuma.

3.2.7.3. Usmerenost mikrofona

Usmerenost mikrofona se odnosi na upadni ugao pod kojim zvučni talas dolazi do mikrofona. Ovaj ugao se računa u odnosu na osu membrane mikrofona i može biti različite veličine, što pre svega zavisi od tipa mikrofona odnosno njegove namene.

Usmerenost mikrofona, odnosno njegova maksimalna osetljivost, je najveća kod zvučnih talasa čiji pravci normalno padaju na osu membrane dok je za ostale zvučne talase, čiji su pravci prostiranja različiti u odnosu na njega, manje vrednosti. Upravo takve pojave, kod kojih je osetljivost mikrofona različita za različite pravce, definišu usmerenost mikrofona.

3.2.7.4. Akustička i električna podela mikrofona

Usmerenost mikrofona, kao mera osetljivosti mikrofona u zavisnosti od pravca kojim zvučni talasi deluju na membranu, je odlučujući faktor kod akustičke podela mikrofona. Prema ovoj podeli, koja pre svega deli mikrofone u odnosu na njihove dijagrame usmerenosti, postoje tri tipa mikrofona, i to:

- presioni mikrofoni,
- gradijentni mikrofoni, i
- kombinovani mikrofoni.

Kod presionih mikrofona je karakteristično to da je njihova konstrukcija takva da je membrana, sa druge strane u odnosu na pravac dolaska zvučnog talasa, potpuno zatvorena. Tako da je delovanje zvučnog polja ograničeno samo na jednu stranu membrane. Delovanjem zvučnog pritiska na membranu dolazi do njenog oscilovanja, čija je brzina v proporcionalna sa pritiskom koji pobuđuje membranu. Kako se radi o pritisku kao skalarnoj veličini nebitno je iz kog pravca dolazi zvučni talas, tako da je dijagram usmerenosti ovakvih mikrofona u obliku kruga, odnosno u pitanju su neusmereni mikrofoni.

Međutim, ovo važi samo za talase niskih frekvencija odnoso onda kada je talasna dužina pobudnih zvučnih talasa mnogo veća od dimenzija presionih mikrofona. U slučaju da mikrofon pobuđuju zvučni talasi visokih frekvencija, čije su talasne dužine približno jednake ili manje od

dimenzija mikrofona, dolazi do promena u zvučnom polju i do neželjenih pojava poput refleksija i difrakcija. Tako da na ovim frekvencijama, usled delovanja difrakcije, dijagram usmerenosti više nije krug već dobija svoju usmerenost u jednom pravcu, a mikrofon postaje potpuno neosetljiv za zvuk koji dolazi sa zadnje strane membrane, čime dolazi do smanjenja odziva kod ovakve vrste mikrofona.

Kod gradijentnih mikrofona, nazivaju se još i dvosmernim mikrofonima, je karakteristično to da njihova mehanička izvedba omogućuje ujednačenost delovanja zvučnog polja sa obe strane membrana.

U slučaju dovoljne udaljenosti zvučnog izvora od mikrofona amplitude oba pritiska koji deluju na membranu, jedan sa prednje a drugi sa zadnje strane membrane, su jednake (jer dolazi do zanemarivanja putne razlike koja se javlja obilaskom oko membrane sobzirom na mnogo veći put koji talas prolazi od izvora do mikrofona) i na kretanje membrane utiče jedino rezultantna sila određena njihovom faznom razlikom. Fazna razlika je najmanja kada je upadni ugao talasa oko 90^0 u odnosu na osu membrane i tada je kretanje membrane vrlo neprimetno, a kada je upadni ugao tačno 90^0 onda nema fazne razlike i membrana miruje. Sa druge strane, kada je upadni ugao 0^0, odnosno u osi membrane, fazna razlika je maksimalna pa je i osetljivost mikrofona maksimalna.

Kombinacijom karakteristika usmerenosti presionog i gradijentnog mikrofona dobija se nova karakteristika usmerenosti koja odgovara kombinovanim mikrofonima. Naime, postavljanjem gradijentnog i presionog mikrofona na jedno isto mesto, sa poklapajućim osama, u slučaju dolaska zvuka u pravcu njihovih osa na izlazu takve kombinacije dobijamo dvostruko veću vrednost izlaznog signala. I suprotno, za zvuk koji dolazi sa druge strane u pravcu osa membrana, signali imaju jednake amplitude ali su u protiv fazi, dolazi do poništavanja i vrednost izlaznog signala je jednaka nuli.

Druga podela mikrofona odnosi se na primenjeni postupak pretvaranja zvučnog signala u električni. Na osnovu toga mikrofone delimo na tri vrste, i to: elektrostatičke (kondenzatorske), elektret i elektrodinamičke mikrofone.

Kod elektrostatičkih mikrofona kombinacija zadnje metalne ploče i membrane (čiji je materijal provodni) predstavlja kondenzator kapaciteta zavisnog od njihovih površina i rastojanja na kome se nalaze.

Delovanjem zvučnog signala dolazi do vibriranja membrane i do promena rastojanja između ploča kondenzatora adekvatnih promenama sile zvučnog pritiska. Promenom rastojanja između ploča dolazi do promene kapaciteta električnog kondenzatora čime se vrednosti

vremenski promenljivog zvučnog pritiska pretvaraju u vrednosti vremenski promenljivog kapaciteta. Menjanjem kapaciteta dolazi do promene količine naelektrisanja na pločama, koje predstavlja promenljivu komponentu električne struje u kolu, čijim proticanjem kroz redni otpornik dolazi do stvaranja promenljivog napona na njegovim krajevima a koji ustvari predstavlja korisni signal.

Osnovu elektret mikrofona čini stalno naelektrisani materijal u obliku folije sa mnogo slobodnih nepokretnih elektrona, izdvojenih posebnim tehnološkim procesom iz atoma, koji se naziva elektret. Postavljanjem ovakve folije na nepokretnu ploču elektrostatičkog mikrofona utiče se na povećanje kapaciteta kondenzatora koji je sada polarisan i bez električnog napajanja. Veoma mali naponi napajanja dovoljni su za dobijanje velikih vrednosti korisnog izlaznog signala, tako da su ovi mikrofoni našli široku primenu u mnogim oblastima a posebno kod računara, mobilnih telefona i mnogih drugih elektronskih uređaja.

Princip rada elektrodinamičkih mikrofona zasniva se na principu elektrodinamičkog pretvaranja. Membrane se kod ovih mikrofona fiksiraju se za cilindre sa namotajima koji se nalaze u magnetnim poljima.

Konstrukcija ovih mikrofona veoma je slična onima kod zvučnika sa tom razlikom da su njene dimenzije i mehaničke karakteristike prilagođene ulaznoj pobudi kao i potrebi za većom osetljivošću.

Međutim, koliko se god teži smanjivanju dimenzija, zbog samog principa rada i postojanja kalema sa namotajem a pre svega zbog dimenzija konstrukcije, postoji određena krutost membrane kod ovakvih mikrofona. Membrane kod elektrodinamičkih mikrofona su mnogo veće i krutije od membrana kondenzatorskih mikrofona, čime je smanjena i njihova osetljivost na pobudni signal. U poređenju sa kondenzatorskim mikrofonima, elektrodinamički mikrofoni su pretvarači sa mnogo manjom osetljivošću i sa frekvencijskim odzivom koji vrlo često odstupa od linearnosti.

Bez obzira na to što ovakva konstrukcija mikrofona doprinosi nedostacima u radu elektrodinamičkih mikrofona, ona ima i svoje prednosti. Jedna od prednosti ovih konstrukcija je to da elektrodinamički mikrofoni ustvari predstavljaju pasivne sisteme bez potrebe za spoljašnjim napajanjem. Namotaji kalema indukuju elektromotornu silu adekvatnu dejstvu pobudnog signala, usled kretanja provodnika koji je izložen stalnom dejstvu magnetnog polja. Druga prednost je da su ovi mikrofoni veoma otporni na spoljne uticaje, na primer na vlagu ili manje mehaničke potrese. Zbog svega ovoga ovi mikrofoni imaju veliku primenu od ozvučavanja govora pa sve do živih muzičkih izvođenja na koncertima.

3.3. Buka u životnoj sredini

Svakodnevne i uobičajene aktivnosti ljudi, pre svega u urbanim sredinama, sprovode se u skladu sa prisutnim i intenzivnim civilizacijskim napretkom, koji podrazumeva sve veće prisustvo i korišćenje kako tehničko-tehnoloških sredstava tako i drugih rezultata naučno istraživačkog rada. Mnogobrojne koristi skoro uvek su praćene postojanjem nečega što je u manjoj ili većoj meri nepovoljno za čoveka, proces rada, sredstva rada i prirodu. Jedna od takvih manifestacija je zvučna (buka životne sredine).

Slika 3.10. *Buka životne sredine*

Šum buke predstavlja neprijatno, nepoželjno i ometajuće postojanje zvuka. Praktično, sve zvučne pojave koje nepovoljno i ometajuće utiču na proces rada ili odmora mogu se smatrati bukom. Da bi se zvuk smatrao bukom potrebno je da on ima dovoljnu jačinu, da se izdvaja od drugih i da se dobro čuje. U nekim slučajevima i posebnim okolnostima, buku može predstavljati i skup tihih zvukova, kao što su razgovori grupe ljudi ili šapati gledaoca u bioskopu ili na pozorišnoj predstavi.

U cilju merenja štetnosti uvedene su kategorije poželjnog i nepoželjnog zvuka, čime je jasno napravljena razlika između zvuka buke i onog koji to nije. To praktično znači, da se status buke ne dodeljuje na osnovu vrednosti jačine zvuka već na osnovu toga koliki je njegov ometajući faktor. Na primer, buku predstavlja svaka, pa i tiha, ometajuća muzika iz susednih prostorija, dok se bukom ne smatra izrazito jaka muzika koja se može čuti na rok koncertima, u nekim kafićima ili na žurkama.

3.3.1. Vrste i tipovi buke

Buka se, na osnovu porekla najstajanja, deli na buku koju stvaraju prirodni izvori i na buku koju stvaraju ljudi. U prirodnu buku spadaju razni šumovi vode, zavijanja vetrova, grmljavine i slično. Ova buka, uglavnom, nije štetna po zdravlje ljudi i kako nije dominantna u urbanim sredinama, nije predmet značajnog razmatranja u ovom radu.

Sa druge strane, buka urbane sredine se prema mestu delovanja deli na dva dela, i to na buku radne sredine i buku životne sredine. Buku životne sredine često nazivamo i komunalnom bukom.

Slika 3.11. *Zvučni signal grmljavine*

Buku radne sredine predstavljaju svi oni zvukovi koje, tokom procesa proizvodnje, stvaraju aparati, uređaji ili mašine za rad. Ovu buku stvaraju kako mašine sa radnih mesta, tako i mašine iz ostalih radnih pogona, kao i neproizvodni izvori buke kao što su ventilatori, klima uređaji i slično.

Pod bukom životne sredine podrazumevaju se svi oni zvukovi koji se javljaju van radnih mesta, kao što su na primer: stanovi, ulice, vozila, mesta za rekreaciju, škole, bolnice. Jasno je da do ovih mesta stižu različite vrste buke, od saobraćane i industrijske buke, preko buke građevinsko-komunalnih mašina, buke iz kafića i restorana, buke koju stvaraju šetači ili razni ulični svirači, pa sve do buke u domaćinstvima koja nastaje pri obavljanju stalnih kućnih poslova korišćenjem različitih aparata i uređaja.

Buka se na osnovu trajanja deli na kontinualnu ili stalnu, diskontinualnu ili povremenu i na buku pojedinačnih zvukova ili šumova.

Slika 3.12. *Zvučni govorni signal jednog od učesnika razgovora*

U zavisnoti od promene jačine buke tokom vremena trajanja postoje sledeće vrste buke, i to: buka iste jačine, buka promenljive jačine, impulsna buka i isprekidana buka.

3.3.2. Izvori i načini prostiranja buke u životnoj sredini

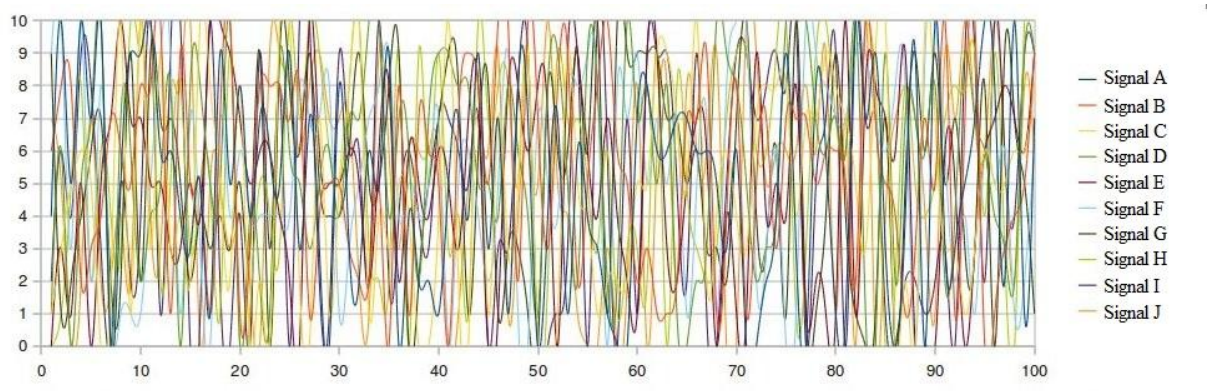
Postoji veliki broj različitih izvora buke u životnoj sredini. Izvorom vrlo jake buke može se na primer smatrati kompletan saobraćaj nekog grada ili jednog dela grada. Posebni izvori buke u sklopu saobraćaja su autobusi, automobili ili druga motorna vozila. Takođe su u okviru samih vozila posebni izvori buke motor vozila, auspuh, sirena ili radio na primer.

Svaki izvor buke ima specifične osobine koje se mogu razlikovati po svojim vremenskim, prostornim i akustičkim osobinama. Prema ponašanju buke koju proizvode u toku vremena postoje izvori sa stalnom bukom i izvori sa promenljivom bukom. Prema načinu delovanja u prostoru dele se na stacionarne i mobilne izvore buke. Najvažnija akustička svojstva ovih izvora opisujemo jačinom, spektralnim karakteristikama i karakteristikama usmerenosti.

Kojim načinom se buka prostire od njenog izvora nastajanja do posmatranog prijemnog mesta, zavisi pre svega od toga koje i kakve se putanje koriste. Put kojim se buka kreće je takođe od velike važnosti i kada se donosi odluka kojim tehničkim zaštitnim sredstvima je najpogodnije odbraniti se od određene buke. Od izuzetne važnosti je dali na svom putu zvuk prolazi kroz čvrste prepreke, tečne prepreke ili se direktno prostire kroz vazduh.

Pod prijemnim mestom ili prijemnikom buke, u širem smislu značenja, smatra se različiti

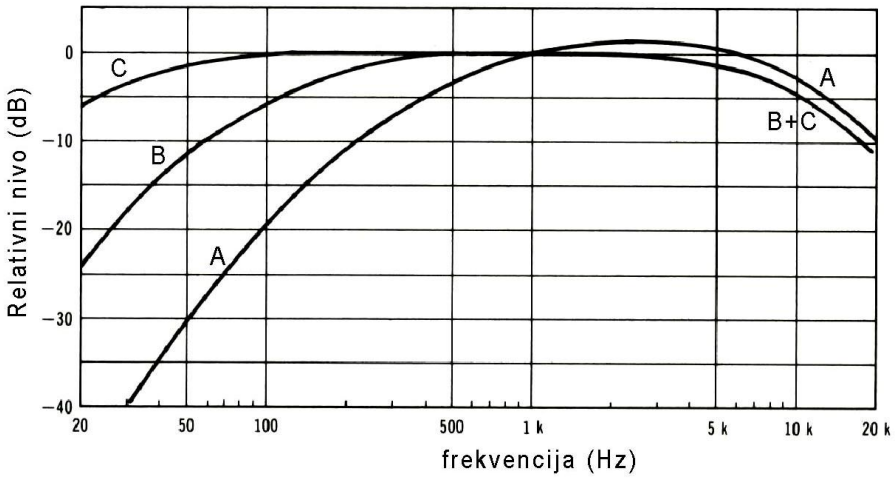
prostor koji je označen kao cilj posmatranja.



Slika 3.13. *Zvuk buke životne sredine izazvan zbirom različitih izvora buke*

3.3.3. Merenje nivoa i spektra buke životne sredine

Životna sredina čoveka ispunjena je zvukovima sa relativno malim zvučnim pritiskom u odnosu na atmosferski pritisak, i njegova veličina je najčešće manja od jednog paskala dok se vrednosti atmosferskog pritiska kreću oko 10^5 paskala. Najmanja vrednost zvuka koga ljudsko čulo sluha može da registruje (prag čujnosti) iznosi $p_0 \approx 20\mu Pa$, tako da je njena vrednost za $5x10^9$ manja od vrednosti koju ima atmosferski pritisak.



Slika 3.14. *Korekcija nivoa zvuka filtrima A, B i C*

Sobzirom na to da ljudsko čulo sluha reaguje na zvuk logaritamskom karakteristikom, za razlike u veličini zvuka u vazduhu uvedena je veličina nivo zvuka ili nivo zvučnog pritiska, koja u svojoj osnovi ima logaritamsku skalu. Nivo zvuka, je prema tome, logaritamski odnos ukupnog pritiska i pritiska najmanje vrednost zvuka koga ljudsko čulo sluha može da registruje, odnosno

$$L = 20\log\frac{p}{p_0} \tag{3.14}$$

Jedinica za merenje nivoa zvuka je decibel. Nivo zvuka od 0 dB odgovara pritusku praga čujnosti $p_0 = 20\mu Pa$. Za tihe zvukove životne sredine ova vrednost iznosi $20 \div 30\,\text{dB}$, kod normalnog govora je $60 \div 70\,\text{dB}$ a kod veoma glasnih zvukova, na primer kod glasne muzike, nivo zvuka je iznad 100 dB.

Međutim, zbog nelinearnih karakteristika ljudskog čula sluha a u cilju realne procene nivoa zvuka, kao i njegovog lakšeg merenja, uvodi se korekcija čiji je cilj simuliranje nelinearnog frekvencijskog osećaja ljudskog uha. Ova korekcija izvodi se uključivanjem jednog filtra, sa nešto drugačijom frekvencijskom karakteristikom od uva, pre merenja nivoa zvuka mernim instrumentom. Ovaj filtar ima oznaku A filtar (slika 3.14), na osnovu čega je i jedinica za merenje nivoa zvuka, na ovaj način, dobila naziv decibel a (dBA).

3.2.3.2. Nivo i spektar buke životne sredine

U cilju zaštite od štetnog delovanja buke, u konkretnim slučajevima i za određene uslove, neophodno je merenjem odrediti vrednosti određenih parametara buke. Najvažnije je utvrditi vrednosti nivoa buke, vremensku promenu kao i amplitudski spektar buke u životnoj sredini. Za merenje ovih veličina koriste se instrumenti sa posebnim karakteristikama, koji su vrlo precizni i koji su kao takvi u širokoj upotrebi. Njihova izrada je prilagođena različitim potrebama, tako da se oni koriste kod kratkotrajnih ili stalnih merenja, kod merenja na terenu ili u istraživačkim laboratorijumima, u normalnim ili ekstremnim uslovima merenja.

Veoma je važno poznavati i ujednačiti uslove merenja kako bi rezultati merenja bili što tačniji i kako bi smo ih mogli međusobno upoređivati.

Najčešće se vrše merenja ukupnog nivoa buke zato što se ovi podaci najviše traže i na osnovu njih je vrlo lako odrediti mnoge druge parametre. Do vrednosti nivoa buke dolazi se, kao što znamo, merenjem zvučnog pritiska posle čega se na osnovu izraza (3.14) dobija vrednost za nivo zvuka u dBA.

Nivo buke životne sredine je promenljiva veličina i menja se u vremenu. U cilju procene dejstva takve promenljive veličine uvodi se pojam ekvivalentnog nivoa buke životne sredine L_{Aeq}. To je onaj nivo buke čiji je štetni uticaj isti kao kod vremenski promenljivog izmerenog nivoa buke i obračunava se na sledeći način:

$$L_{Aeq} = 10 \log \sum_{i=1}^{n} \frac{1}{100} \left(t_i \cdot 10^{0,1 \cdot L_i} \right), \quad \text{dBA} \tag{3.15}$$

gde su t_i vremena trajanja i-tih nivoa L_i.

Ekvivalentni nivo buke se izražava procentualno i odnosi se na ukupni vremenski interval merenja buke.

Prilikom analize štetnog uticaja buke životne sredine važno je poznavati i njene frekvencijske karakteristike, pre svega veličinu i raspored njenih frekvencijskih komponenata. To se postiže razlaganjem buke životne sredine filtrima propusnicima određenih opsega učestanosti.

Analizu je moguće uraditi i korišćenjem filtara propusnika opsega učestanosti sa bilo kojom širinom opsega, ali da bi došlo do ujednačavanja rezultata merenja najčešće se koriste oktavni ili trećinsko-oktavni filtri.

3.2.3.3. Karakteristike zvuka buke u frekvencijskom domenu

Vremenski promenljiva vrednost $p(t)$ je u principu veoma složena funkcija. Najčešće ona predstavlja sumu pojedinačnih harmonijskih komponenata, tako da važi:

$$p(t) = \sum_{n} p_n(t) \tag{3.16}$$

gde $p_n(t)$ predstavlja komponentu zvučnog pritiska na učestanostima f_n, ili prikazana u obliku kontinualne funkcije učestanosti

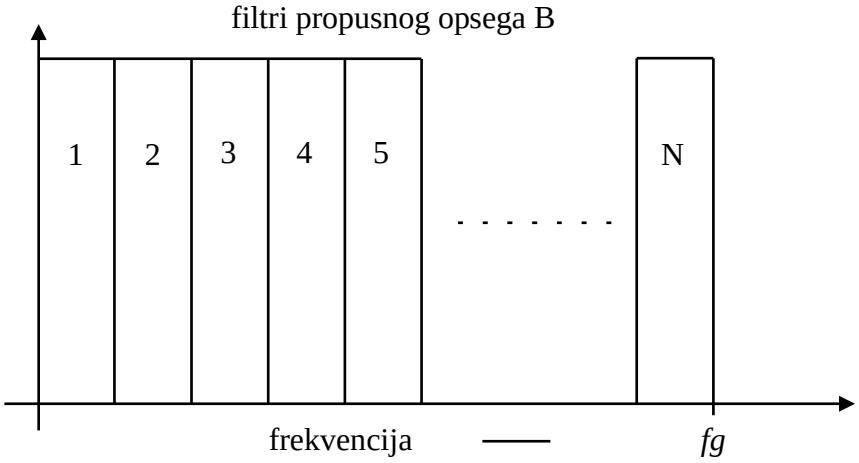
$$p(t) = \int_{-\infty}^{\infty} W(f) e^{-j 2 \pi f t} dt \tag{3.17}$$

gde funkcija $W(f)$ predstavlja spektralnu funkciju pritiska.

Na ovaj način prikazan zvučni signal podrazumeva njegovu trenutnu vrednost $p(t)$ i efektivnu vrednost $p_{eff}(t)$, definisanu za bilo koji opseg učestanosti.

U suštini, spektralna analiza predstavlja podelu opsega učestanosti signala zvuka na određeni broj manjih opsega učestanosti. Ovaj postupak prikazan je na slici 3.15. Ovi manji opsezi, ili bolje rečeno podopsezi ukupnog frekvencijskog opsega signala, imaju određenu širinu, kao i broj koji zavisi od usvojene širine opsega B kao i od ukupne širine opsega učestanosti signala. Praktično, preciznost spektra, zajedno sa rezolucijom spektralne analize u zavisnosti je

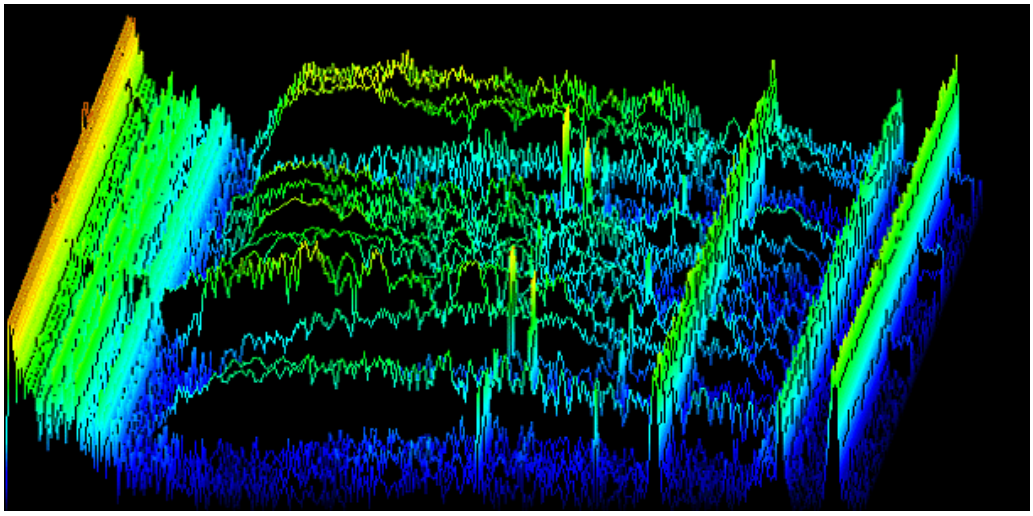
od usvojene vrednosti širine podopsega.



Slika 3.15. *Podela ukupnog opsega signala na podopsege B*

Svaki filtar na svom izlazu daje određenu srednju kvadratnu to jest efektivnu vrednost amplitude posmatranog signala, za grupu frekvencija koje su u njegovom opsegu. Ovako dobijena vrednost predstavlja jednu tačku spektra a ukupan spektar se dobija određivanjem srednjih kvadratnih vrednosti na izlazima svih filtara. Na osnovu ovako dobijenih vrednosti izračunava se i vrednost nivoa zvuka.

Spektralnom analizom se u principu dobijaju vektorske vrednosti frekvencijskih komponenata posmatranog signala, sa mogućnošću očitavanja skalarnih vrednosti amplituda tih komponenata. Što se sabiranja pojedinačnih komponenti tiče, ono se jedino može vršiti sa srednjim kvadratnim vrednostima tih komponenata, kada se kao rezultat dobija ukupna energija posmatranog signala. Numeričke vrednosti za nivo zvuka izraženog u dB se ne sabiraju.



Slika 3.16. *Trodimenzionalni prikaz signala buke životne sredine*

Iznešena tvrdnja, u vezi sabiranja vrednosti pojedinačnih komponenata, može se dokazati

na vrlo jednostavan način. Pretpostavimo da su pritisci p_1 i p_2 frekvencijski podopsezi, tada je:

$$p(t) = p_1(t) + p_2(t) \tag{3.18}$$

gde je *p(t)* ukupni zvučni pritisak. Srednju kvadratnu vrednost računamo kao:

$$\overline{p^2} = \overline{p_1^{\,2}} + \overline{p_2^{\,2}} + 2(\overline{p_1 p_2}) \tag{3.19}$$

Pošto je srednja vrednost proizvoda pritisaka p_1 i p_2 jednaka nuli, jer se spektralne komponente ne mogu množiti, dobija se izraz

$$\overline{p^2} = \overline{p_1^{\,2}} + \overline{p_2^{\,2}} \tag{3.20}$$

Ako prikazani postupak primenimo na *N* podopsega dobija se:

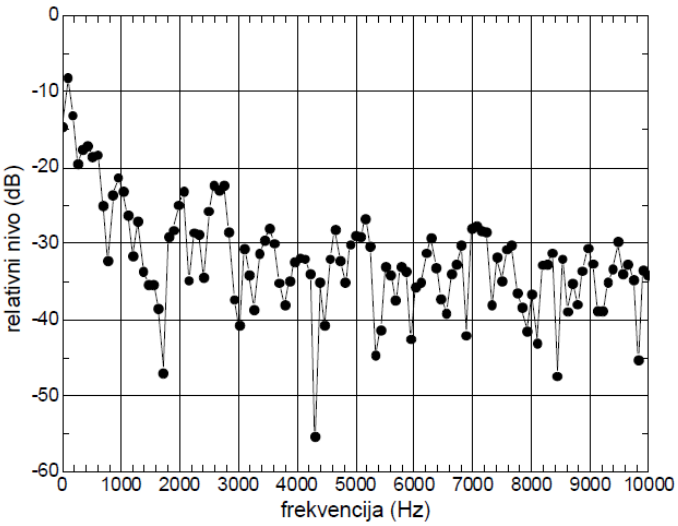
$$\overline{p^2}(t) = \sum_{i=1}^{N} \overline{p_i^{\,2}} \tag{3.21}$$

Dobijeni rezultat dokazuje da je ukupna energija posmatranog signala jednaka zbiru energija pojedinačnih komponenata spektra signala.

Pri spektralnoj analizi širinu podopsega praktično određuje broj filtara, pa je:

$$B = \frac{f_g}{N} \tag{3.22}$$

gde f_g predstavlja gornju graničnu učestanost posmatranog signala zvuka. Spektralnu analizu koja koristi konstantne filtre vršimo pomoću FFT algoritma (slika 3.17).



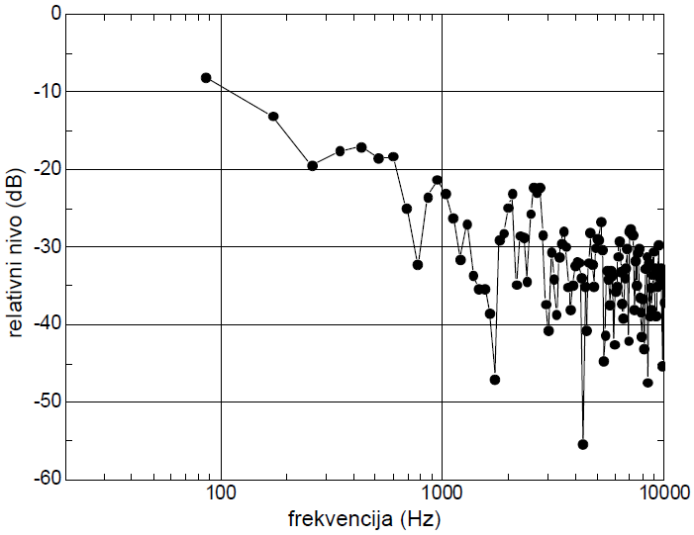
Slika 3.17. *Spektar signala buke dobijen primenom konstantnih filtara. Vrednost svake tačke dobijena je iz po jednog filtra*

Sa slike 3.17 se može primetiti približno jednaka udaljenost između tačaka spektra, u

slučaju predstavljanja frekvencijske ose linearnom razmerom, što je osnovna karakteristika analize koja koristi konstantne filtre.

Zbog logaritamske karakteristike ljudskog uha nameće se potreba prikazivanja rezultata spektralne analize u logaritamskoj razmeri ali se tada, pri korišćenju konstantnih filtara, dobija nejednaka gutoća tačaka što se može videti na slici 3.18 koja odgovara slici 3.17.

Na ovoj slici, kod koje je osa učestanosti prikazana u logaritamskoj razmeri, primetna je povećana gustina zgušnjavanja tačaka na visokim učestanostima i smanjenje gustine tačaka na niskim učestanostima, što je loša osobina ovakvog načina predstavljanja.



Slika 3.18. *Prikaz spektralne analize sa slike 3.17 u logaritamskoj razmeri*

U cilju usklađivanja rezolucije sa logaritamskom skalom vrši se spektralna analiza kojom se dobijaju proporcionalni frekvencijski opsezi kao na slici 3.15. Na ovaj način dobijene širine frekvencijskih opsega iznose:

$$B = f_2 - f_1 \tag{3.23}$$

za svaki frekvencijski opseg, pri čemu je

$$\frac{f_2}{f_1} = const\,. \tag{3.24}$$

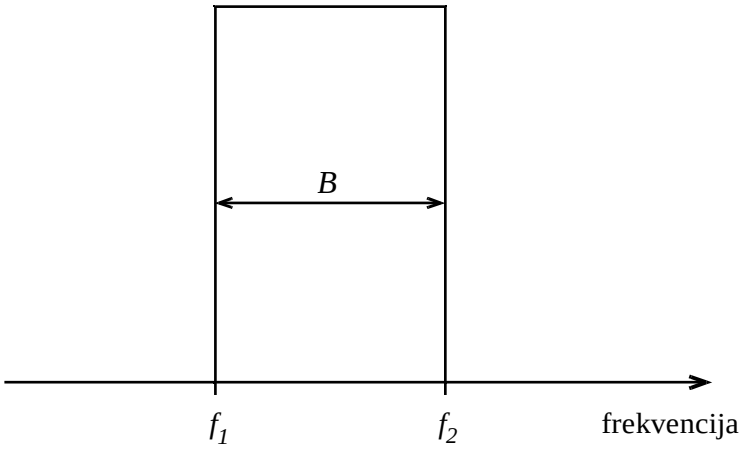
Očigledno je da proporcionalni frekvencijski opsezi umesto zadate širine B u hercima imaju širinu koju određuje konstanta (3.24). Iz tog razloga širene opsega zavise jedino od odnosa gornjih i donjih graničnih frekvencija i duž frekvencijske ose se menjaju proporcionalno. Njihova širina je na nižim frekvencijama prilično mala i proporcionalno se povećava porastom frekvencije.

Definisanje opsega proporcionalnih filtara se uvek vrši konstantom *n*, koja se naziva red

proporcionalnog filtra i čija je osnova 2, tako da je:

$$\frac{f_2}{f_1} = 2^n \tag{3.25}$$

Filtri kod kojih je konstanta n = 1 zovu se oktavni jer njihov odnos gornje i donje granične frekvencije iznosi 2 a u muzici se takav interval tonova čija je odnos frekvencija 2:1 naziva oktava. Vrednost konstante n = 1/3 imaju tercni filtri i njihova širina opsega iznosi trećina oktave. Filtri čija je konstanta n = 1/2 ili poluoktavni filtri se veoma retko koriste.



Slika 3.19. *Definisanje proporcionalnih frekvencijskih opsega*

Realizacija 1/3 oktavnog spektra prikazana je na slici 3.20 na kojoj se vidi jasna razlika rasporeda tačaka na niskim frekvencijama u odnosu na sliku 3.18. To je jedan od najvažnijih razloga standardne primene proporcionalnih filtara u spektralnoj analizi zvučnog signala.

Iz razloga precizne definisanosti odnosa gornjih i donjih graničnih frekvencija, moguće je pojednostavljivanje uvođenjem frekvencije koja se nalazi tačno na sredini opsega, frekvencijske ose predstavljene logaritamskom razmerom, odnosno između graničnih frekvencija i koja se naziva centralna frekvencija proporcionalnog opsega.

Relacija na osnovu koje se određuje vrednost centralne frekvencije je:

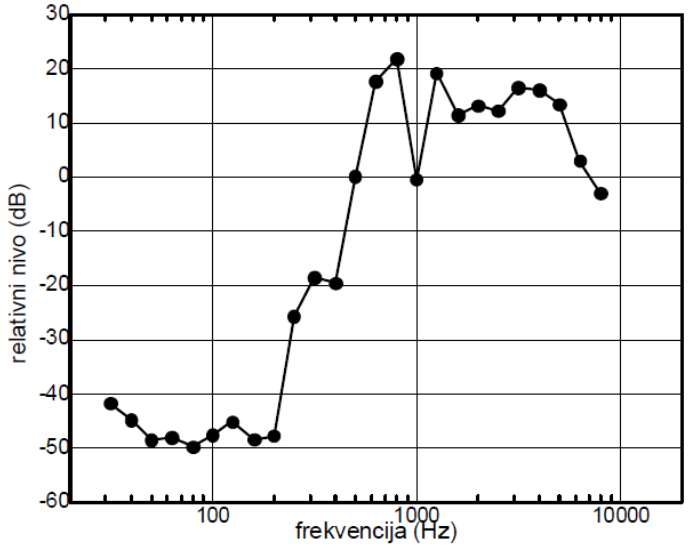
$$f_0 = \sqrt{f_1 f_2} \tag{3.26}$$

Vrednost donje granične frekvencije, uz poznatu centralnu frekvenciju oktavnog opsega, računa se pomoću izraza:

$$f_1 = \frac{f_0}{\sqrt{2}} \tag{3.27}$$

To praktično znači da se centralnom frekvencijom, lako i u potpunosti, određuju propusni

opsezi oktavnih filtara. Istim postupkom određuje se i veličina centralne frekvencije kod 1/3 oktavnih opsega.



Slika 3.20. *Rezultati spektralne analize 1/3 oktavnim filtrima*

U cilju poređenja različitih sprektara koji se dobijaju pomoću proporcionalnih filtara, neophodno je standardizovati centralne frekvencije njihovih opsega. Tako su, na automatski način, i za uže proporcionalne opsege određene vrednosti njihovih centralnih frekvencija.

Standardizovane vrednosti centralnih frekvencija, za proporcionalne filtre sa oktavnim i tercnim opsezima, prikazane su tabelom 3.2.

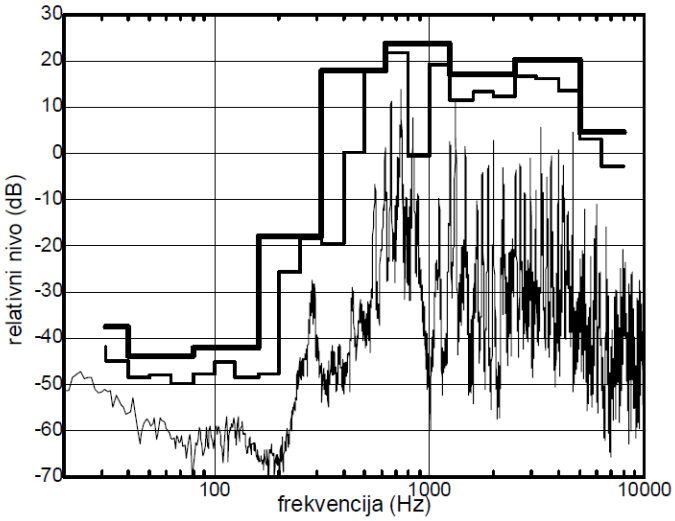
Tabela 3.2. Vrednosti standardnih centralnih frekvencija proporcionalnih filtara

oktavni	1/3 oktavni	oktavni	1/3 oktavni
31,5Hz	25Hz 31,5Hz 40Hz	1000Hz	800Hz 1000Hz 1250Hz
63Hz	50Hz 63Hz 80Hz	2000Hz	1600Hz 2000Hz 2500Hz
125Hz	100Hz 125Hz 160Hz	4000Hz	3150Hz 4000Hz 5000Hz
250Hz	200Hz 250Hz 315Hz	8000Hz	6300Hz 8000Hz 10000Hz
500Hz	400Hz 500Hz 630Hz	16000Hz	12500Hz 16000Hz 20000Hz

Potrebno je reći i to da je poređenje različitih frekvencijskih spektara, dobijenih

proporcionalnim filtrima, skoro nemoguće bez standardizacije njihovih centralnih frekvencija i bez sprovođenja ispravnog postupka definisanja standardnih frekvencija. Ovaj postupak, kojim se ispravno definišu vrednosti standardne frekvencije za svaki podopseg učestanosti ukupnog opsega posmatranog signala zvuka buke, izvodi se tako što se za polaznu tačku uzima frekvencija vrednosti jedan herc i njoj se dodeljuje uloga centralne frekvencije jednog oktavnog podopsega. Zatim se ostale vrednosti centralnih frekvencija opsega određuju povećavajući ili smanjujući vrednost frekvencije za oktavu.

Radi ilustracije razlika do kojih dolazi prilikom primene različite spektralne analize na isti zvučni signal, na slici 3.21 prikazani su spektri dobijeni korišćenjem oktavnih filtara, 1/3 oktavnih filtara i linearnih, takozvanih filtara po hercu, kod kojih širina opsega iznosi 1 Hz.



Slika 3.21. *Prikaz rezultata oktavnih (gornja linija), tercnih (srednja linija) i linearnih (donja linija) spektara istog zvučnog signala*

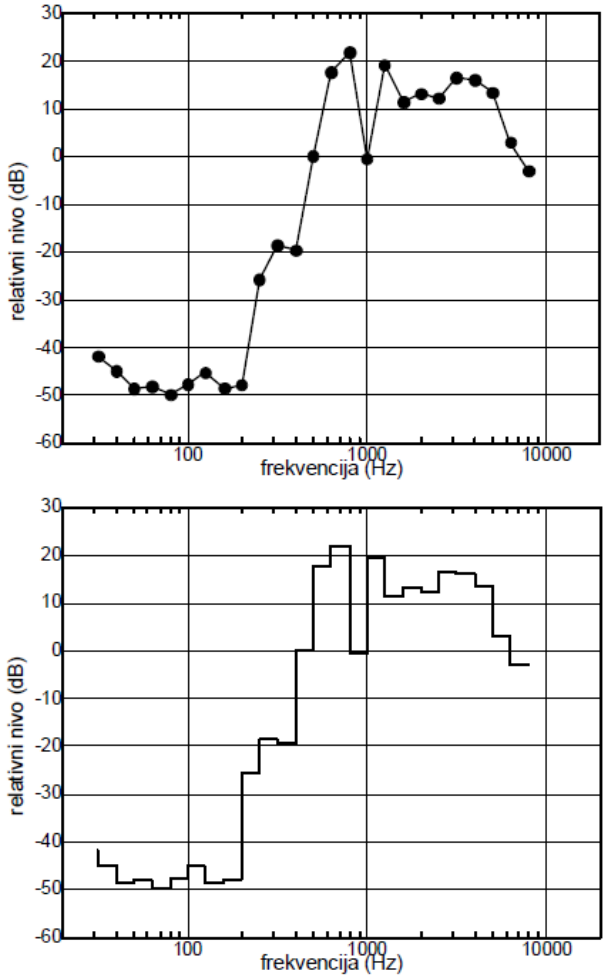
Proporcionalne spektre moguće je predstaviti na dva različita načina, kao što je to prikazano slikama 3.22. Prvi način prikazan je na gornjoj slici na kojoj se dijagram spektra crta spajanjem spektralnih tačaka.

Drugi način prikazivanja proporcionalnih spektara prikazan je na donjoj slici i izvodi se crtanjem horizontalnih linija celom dužinom ose propusnih frekvencijskih opsega svih filtara koji se koriste u spektralnoj analizi.

Kod prikazivanja vremenskih promena spektralnih karakteristika signala zvuka buke životne sredine u polju sa dimenzijama vremena, frekvencije i intenziteta, neophodno je korišćenje posebnih oblika grafičkog prikazivanja i za takve potrebe se najčešće koriste spektogrami i slapovi.

Primer prikaza analize jednog dela signala zvuka čije je trajanje 0,45 sekundi prikazan je

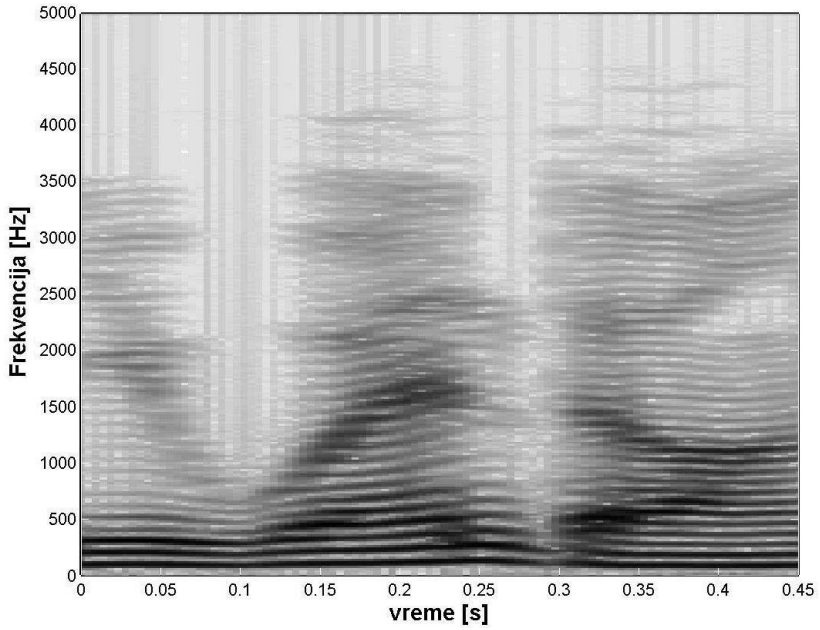
spektogramom na slici 3.23. Kod prezentacija na ovaj način obično je apcisna osa zadužena za prikazivanje intervala vremena a ordinatna osa za frekvencije, dok se za prikazivanje intenziteta koristi kodovanje skalom različitih boja ili se koristi kodovanje skalom crne boje odnosno većim ili manjim zatamnjenjem, što je slučaj u ovom primeru. Pojačano zatamnjenje označava veću vrednost intenziteta posmatranog dela signala i obratno, manje zatamnjenje znači da se radi o manjem intenzitetu. Prikazivanje spektogramima predstavlja uobičajeni način grafičke prezentacije rezultata spektralne sadržine pri analizi slučajnih zvučnih signala kao što je govor ili, u našem konretnom slučaju, buka životne sredine. Treba naglasiti i to da se spektogrami koriste kod skoro svih analiza buke životne sredine, jer je jedino sa njihovog prikaza moguće sagledati određene specifičnosti ovih, najčešće nepoželjnih signala.



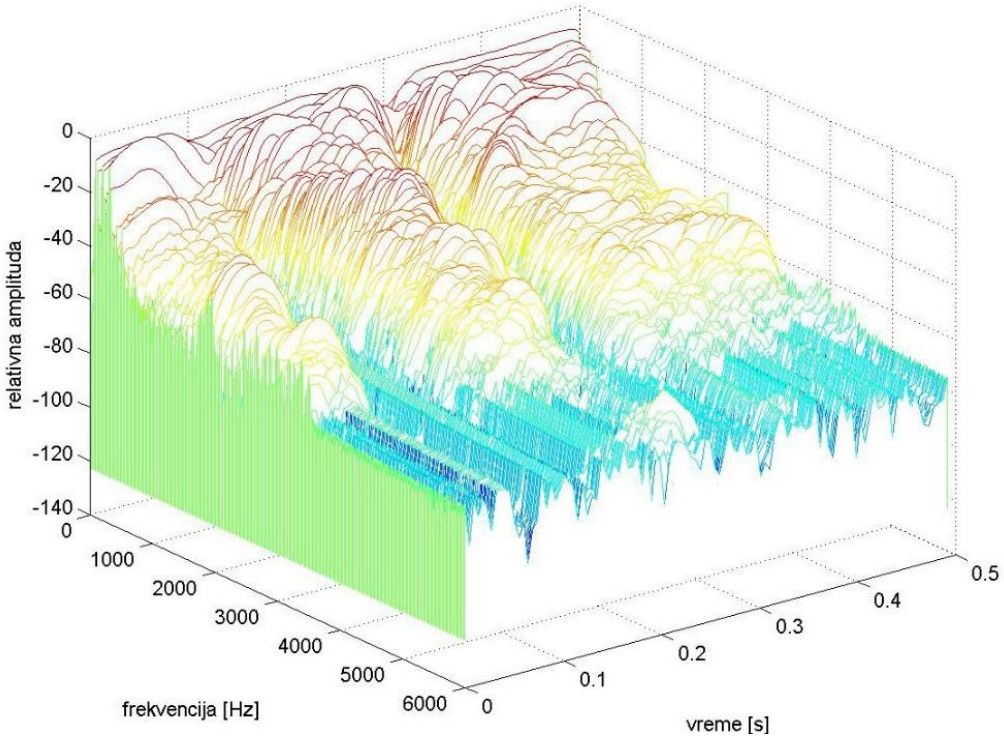
Slika 3.22. *Primeri predstavljanja proporcionalnih spektara zvučnog signala*

Drugi takođe često korišćen način trodimenzionalne predstave promena frekvencijske sadržine zvuka tokom vremena je slap. On predstavlja grafičko prikazivanje promene sadržaja spektra u vremenu posmatrano iz određene perspektive. Obično se kod ovakvog prikaza vremenske i frekvencijske ose nalaze u horizontali dok je nivo signala u vertikalnoj ravni.

Na slici 3.24 prikazan je slap jednog signala zvuka. Radi se o prikazu istog zvučnog signala koji je spektogramom prikazan na slici 3.23.



Slika 3.23. *Primer spektrograma koji prikazuje deo zvuka. Uočljive su harmonijske komponente zvuka (horizontalne linije) i promene spektra u vremenu.*



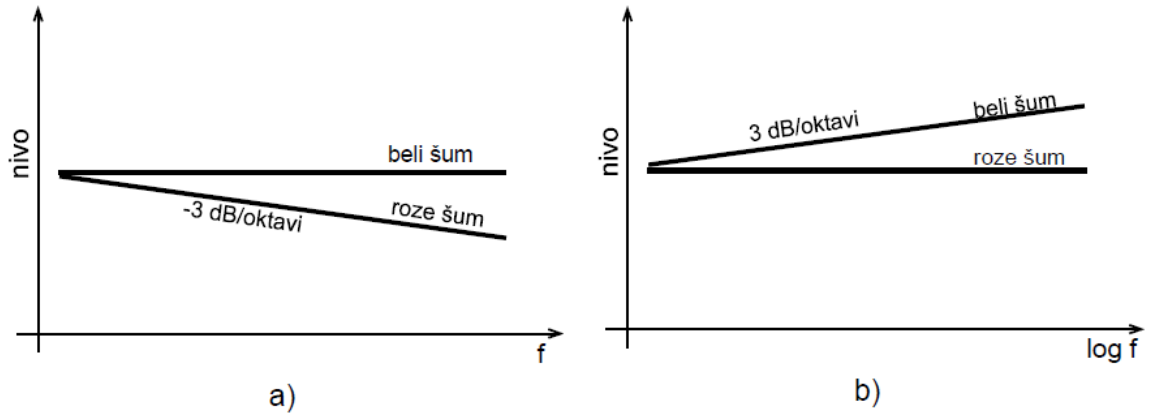
Slika 3.24. *Primer slapa signala zvuka. U pitanju je isti signal kao na slici 3.23*

Problem prikazivanja vremenskog sadržaja signala slapom odnosi se na njegovu preglednost i grafičku čitljivost. U slučaju slike 3.24 može se reći da se radi o primeru slapa koji je veoma pregledan i čitljiv. Međutim, u mnogim slučajevima slike su predstavljene grupama krivih linija, nejasne su i nisu dovoljno pregledne.

3.2.3.4. Primeri karakterističnih spektralnih oblika zvučnog signala

Akustički prenosni sistemi prilikom svojih testiranja imaju potrebu za specifičnim signalima čiji frekvencijski sprektar ima određeni oblik. Iz tog razloga ponekad postoji potreba za generisanjem zvučnog pritiska, odnosno zvučnog signala čiji je spektar potpuno ravan. Ali kako se postupak kojim se određuju spektri razlikuje, tako i ravan spektar nije precizno definisan već njegov oblik zavisi od toga kojom se metodom vrši spektralna analiza. Zato je bilo potrebno definisati zvučne signale i njihove različite spektralne sadržaje i prilagoditi ih sprovođenju procedure dobijanja spektara pomoću konstantnih ili proporcionalnih filtara.

Nastajanje belog šuma, koje iniciraju termički procesi u provodniku, ima za posledicu stvaranje signala sa ravnim spektrom. To znači da se proces spektralne analize sprovodi formiranjem konstantnih opsega. Kod ovakvih opsega spektralna gustina je konstantna, i izražava se u W/Hz, što je karakteristika ravnog spektra. Primenom proporcionalnih filtara u procesu spektralne analize belog šuma, za razliku od korišćenja konstantnih filtara, dobija se spektar koji je neravan odnosno monotono rastući sa porastom frekvencije.



Slika 3.25. *Prikaz spektralne analize belog i roze šuma: a) spektri sa konstantnim opsezima b) spektri sa proporcionalnim opsezima*

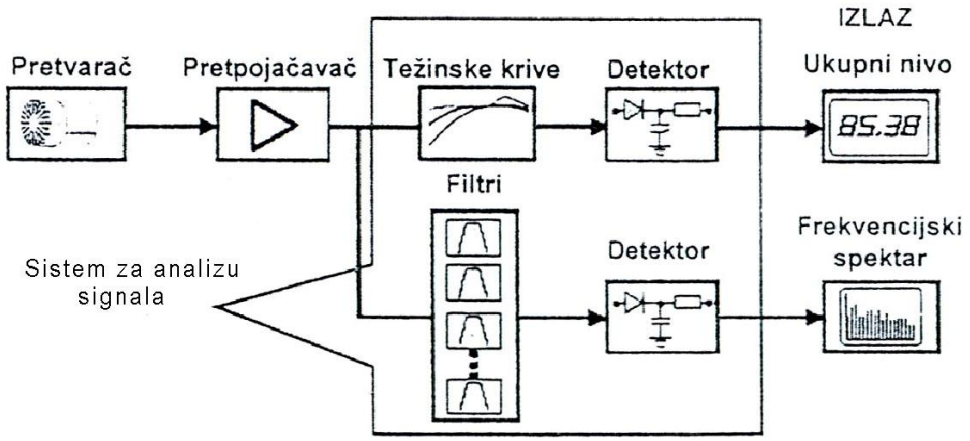
Posmatranjem oktavnih filtara može se zaključiti da kod svakog sledećeg višeg filtra na frekvencijskoj osi dolazi do dvostrukog povećanja širine frekvencijskog opsega u odnosu na prethodni. To znači da spektralnom analizom belog šuma pomoću oktavnih filtara dobijamo energiju na izlazu svih filtara koja je duplo veća u odnosu na energiju izlaza prvih susednih nižih filtara. Ovako duplirano povećanje energije po filtru, sa dvostrukim povećanjem frekvencije, za posledicu ima nagibanje linije spektra za 3 dB po oktavi kao što je to prikazano na slici 3.25.

Kako razna merenja imaju potrebu za signalom sa ravnim spektrom, pri upotrebi proporcionalnih filtara, bilo je potrebno definisati posebnu vrstu signala pod nazivom roze šum. Ovo ime dodeljeno je na osnovu sličnosti sa analizom svetlosti i njenim spektralnim sadržajem čiji jedan deo zauzima roze boja. S obzirom na to, da kod nijednog prirodnog procesa ne postoji generisanje takvog oblika signala, roze šum je moguće dobiti propuštanjem belog šuma kroz roze filtar. Specifičnost ovog filtra je da konstantna opadajuća frekvencijska karekteristika sa nagibom 3 dB po oktavi.

Analizom spektralnog sadržaja roze šuma spektralnom analizom sa konstantnim filtrima dobijamo monotono opadajući spektar čiji je nagib 3 dB po oktavi, kao na slici 3.25a. Primenom analize koja koristi proporcionalne filtre dolazi se do ravnog spektra, kao što to prikazuje slika 3.25b. Koji će se šum, beli ili roze, koristiti u postupku analize akustičkog prenosnog sistema, zavisi od toga koju metodu spektralne analize ćemo koristiti. U praksi se najčešće koristi spektralna analiza sa proporcionalnim filtrima, tako da se praktično kao pobuda za razna merenja i ispitivanja u akustičkim sistemima prenosa, roze šum koristi kao standarni signal i mnogo se češće koristi od belog šuma.

3.2.3.5. Instrumenti za merenje buke životne sredine

Postoji veliki broj različitih instrumenata koji se koriste za merenje buke kao i njenih amplitudskih, frekvencijskih i vremenskih karakteristika. Na slici 3.26 prikazani su osnovni delovi mernog lanca za merenje i analizu buke, mada se on može zasnivati na analognom i digitalnom principu ili može imati određeno softversko rešenje.



Slika 3.26. *Merni lanac za merenje i analizu buke*

Zadatak pretvarača je pretvaranje zvučnih oscilacija, koje izaziva zvučni talas, u električni signal. Tako dobijeni električni signal, koji ima veoma malu amplitudu, pojačava se u pretpojačavaču. U delu sa težinskim krivama vrši se ponderisanje signala u domenu učestanosti, tako da se dobijaju trenutni nivoi signala sa određenim ponderacijama. Sistem filtara koristi se za spektralnu analizu signala u domenu učestanosti, osnosno za dobijanje frekvencijskog spektra posvatranog zvučnog signala. Detektor ima funkciju određivanja efektivnih vrednosti signala koji se zatim mogu prikazati vizuelno preko displeja koje sadrži sam instrument ili korišćenjem uređaja poput štampača, plotera ili monitora.

Instrumente koji se koriste za merenje buke, zavisno od toga koji se delovi sastava koriste za analizu, moguće je podeliti u nekoliko grupa, i to: na instrumente koji mere ukupan nivo buke, koji u svom sastavu sadrže sistem težinskih kriva i detektor signala, na instrumente za dobijanje frekvencijskog spektra signala buke, koji u svom sastavu sadrže filtre i detektor, ili na instrumente koji predstavljaju kombinaciju prethodno nabrojanih grupa instrumenata, koji služe i za merenje nivoa buke i za frekvencijsku analizu signala.

Svaka promena u nivou buke životne sredine se konstantno snima, prati, registruje i prikazuje preko raznih monitora, plotera i štampača.

3.2.3.6. Dozvoljeni nivoi buke životne sredine

Postoje propisima utvrđeni dozvoljeni nivoi buke za stambene i poslovne objekte odnosno u boravišnim prostorijama stanova, koje su namenjene za odmor, i u radnim prostorijama koje zahtevaju koncentraciju pri radu ili su namenjene za komunikaciju.

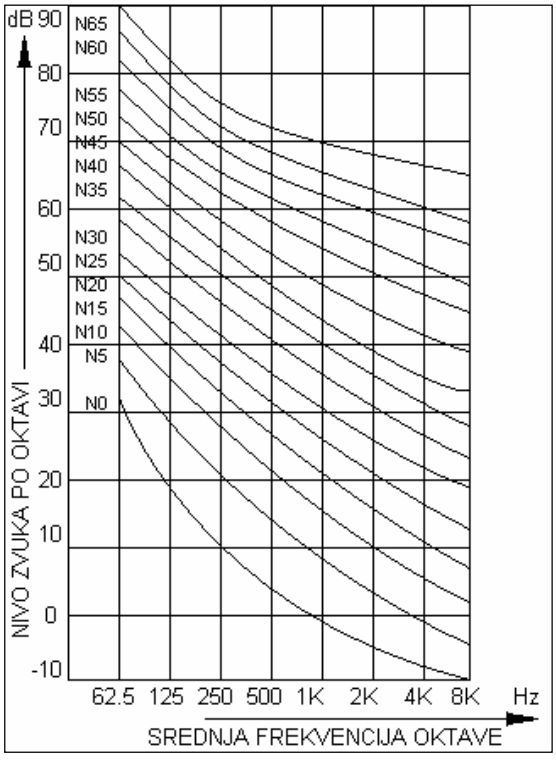
U tabeli 3.3 dati su utvrđeni dozvoljeni nivoi buke u boravišnim prostorijama i drugim vrstama objekata odnosno u hotelima, bolnicama, domovima, školama i tako dalje. Kao što se iz tabele može videti vrednosti dozvoljenih nivoa buke definisane su za one prostorije u kojima ljudi borave u dužem vremenskom periodu. Maksimalni nivo buke koji je dozvoljen se ne definiše za pomoćne prostorije, prostorije za komunikaciju, sanitarne čvorove i slične delove zgrada koji se samo povremeno koriste.

Pošto se utvrdi veća vrednost nivoa buke on one vrednosti koja je dopuštena treba uraditi oktavnu analizu buke. Ova procena zahteva korišćenje N krive (slika 3.27) čija je vrednost manja za 5 decibela od najvećeg dozvoljenog nivoa buke koji se izražava dBA vrednostima.

Tabela 3.3. Maksimalni dozvoljeni nivoi buke u životnoj sredini

Životna sredina	Najveće dozvoljene vrednosti stalnog nivoa buke u dBA	
	U toku dana (07–20h)	U toku noći (22–06h)
Stambene zgrade (prostorije za boravak) sa zatvorenim prozorima	40	35
Bolnice	35	30
Lekarske ordinacije	40	40
Prostorije u domovima za odmor dece i učenika	40	35
Škole, biblioteke, čitaonice, sale za bioskopske predstave	40	40
Pozorišta i koncertne sale	30	30
Hoteli	40	35

Vrednost na ordinati spektra koja je uzeta za nominalnu oznaku krive iznosi 1000 herca. Opadanje povećavanjem frekvencije, koje je karakteristično za sve krive, pokazuje da veće frekvencije utiču na jače ometanje.



Slika 3.27. *Procena ometanja pomoću standardizovanih N kriva*

Određivanje kriterijuma, to jest graničnih linija, za nivo buke određenih prostorija vrši se po tabeli 3.4. Nivo buke na osnovu propisa ne sme prelaziti date vrednosti kriva što podrazumeva položaj spektra buke ispod kriva usvojenih na osnovu određenih kritreijuma.

Tabela 3.4. Dozvoljeni nivoi buke u životnoj sredini izraženi N kriterijumima i u dBA

Objekti	Kriterijumi	Nivoi buke (dBA)
Radijski studiji	N15 – N20	20 - 25
Pozorišta, koncertne sale,	N20 – N25	25 - 30
Školske učionice, bioskopi, spavaće sobe	N25 – N30	30 - 40
Kancelarije, biblioteke	N30 – N40	40 - 45
Restorani, radnje	N45 – N50	50 - 55
Sportske sale, manifestacione hale	N55	60
Radionice, servisi	N65	70

Vrednosti dozvoljenih nivoa buke u prostorijama koje nisu označene tabelom 3.4, kao i u prilikom raznih drugih slučajeva kada je potrebno opisati subjektivnu ocenu buke i mogućnost obavljanja određenih delatnosti, date su u tabeli 3.5.

Tabela 3.5. Dozvoljeni nivoi buke (pri kojima postoji mogućnost obavljanja određenih delatnosti) izraženi N kriterijumima i u dBA

Kriterijumi	Nivoi buke (dBA)	Opisi slučajeva i posledica
N25 – N30	30 - 40	Veoma mirno stanje, sastanak moguć
N35 – N40	40 - 45	Mirna stanja, čujnost govora dobra do 10 m, telefonski razgovori normalni
N40 – N45	45 - 50	Bučnost zadovoljavajuća, čujnost govora dobra do 4 m, telefonski razgovori normalni
N45 – N55	50 - 60	Pojačani govori, razumljivost do 2 m, telefonski razgovori nešto otežani
N55 – N60	60 - 65	Mogući razgovori između dve osobe koje su vrlo blizu, telefonski razgovori veoma otežani
N60 – N65	65 - 70	Mogući umni rutinski radovi i radovi upravljani govornim komandama i signalima
N70	75	Mogući fizički radovi uz zadovoljavajući nivo preciznosti i koncentracije
N80	85	Mogući fizički radovi bez umnog napora

4 GENERATORI SLUČAJNIH NIZOVA

4.1. Generisanje slučajnih brojeva

Potreba za slučajnim brojevima je naglo porasla četrdesetih godina prošlog veka kada su oni bili neophodni za prve modele i simulacije nuklearnih eksplozija i stvaranje nuklearnog oružja. Već 1955 godine odštampana je prva knjiga slučajnih brojeva čijom kupovinom se za 10 dolara moglo dobiti 100.000 cifara. Izdanje se nastavilo sve do 2001 godine kada se knjiga mogla nabaviti za oko 90 dolara.

Dok su se pre koristile tablice slučajnih brojeva, razvojem računara one su zamenjene generatorima slučajnih brojeva. U začecima simuliranja, do slučajnosti se dolazilo ručnim tehnikama, poput bacanja novčića i kockice za igranje. Kasnije su mehanički uređaji spajani na računare jer je preovladavalo mišljenje da samo mehanički ili elektronski uređaji mogu proizvesti istinski slučajne nizove. Međutim, kako su mehaničke metode, ponekad, prespore za široku upotrebu, uz činjenicu da nizovi ne mogu biti reprodukovani (što može biti problem naročito kod simulacija), velika većina današnjih generatora slučajnih brojeva bazirana je na algoritmima koji se mogu jednostavno implementirati u računare. Dobri algoritamski generatori mogu da obezbede „skoro" sva važna statistička svojstva slučajnih nizova, bez obzira na to što su generisani determinističkim algoritmima. Međutim, ipak to nisu brojevi koji su istinski slučajni, već brojevi koji se takvima čine, jer načini na koji nastaju nisu slučajni. Zato brojeve nastale na taj način zovemo pseudoslučajnim brojevima.

U većini slučajeva je potrebno da generisani slučajni brojevi imaju približno uniformnu raspodelu na jediničnom intervalu (0, 1). Za tu distribuciju koristimo oznaku $U(0, 1)$. Uopšteno, koristimo oznaku $U(a, b)$ za označavanje neprekidne uniformne distribucije na intervalu (a, b). Ta raspodela je ne samo neophodna kod istinski slučajnih brojeva već je i generalno pogodna za upotrebu budući da postoji mnogo jednostavnih tehnika za transformaciju uniformnog uzorka u uzorke drugih raspodela.

Da bi slučajne brojeve mogli koristiti u svakodnevnim primenama, oni moraju biti realizacije nezavisnih i jednako raspodeljenih slučajnih varijabli, to jest za niz slučajnih varijabli U_1, U_2, ... mora važiti:

- Svaka $U_i \sim U(0, 1)$

- Sve U_i su međusobno nezavisne.

Ovo drugo svojstvo je veoma važno i uslovljava da bilo koje dve slučajne varijable moraju biti nekorelisane, ili još uopštenije, da se vrednost varijable U_i ne može pretpostaviti iz $U_1, ..., U_{i-1}$.

Generator slučajnih brojeva proizvodi konačan niz brojeva $u_1, u_2, \ldots, u_k$ na jediničnom intervalu. Generisane vrednosti delom zavise od parametara zadanih od strane korisnika. Dobar generator je onaj koji zadovoljava uslov da se mali segmenti (u odnosu na k) niza $u_1, u_2, \ldots, u_k$ne razlikuju od realizacija nezavisnih uniformnih slučajnih varijabli.

Uzimajući u obzir navedene uslove, prilikom konstruisnja generatora slučajnih brojeva potrebno je voditi računa o sledećim karakteristikama:

- **Dužina periode**. Kao što je već pomenuto, bilo koji generator pseudoslučajnih brojeva će se vremenom ponoviti. Prednost treba dati generatorima sa dužom periodom, to jest generatorima koji proizvode više različitih vrednosti pre ponavljanja ili svakako generatorima istinski slučajnih brojeva koji su neperiodični.

- **Reproduktivnost**. Jedan od nedostataka istinski slučajnog niza je taj da se ne može lako reprodukovati. Često je važno imati mogućnost ponovnog pokretanja simulacije koristeći jednake parametre kao i pre, ili da se jednaki parametri koriste u dve ili više simulacija.

- **Brzina**. S obzirom na veliku potrebu za slučajnim brojevima kao i na to da generator slučajnih brojeva može biti korišćen nekoliko hiljada puta prilikom jedne simulacije, važno je da bude brz. Kako je brzina današnjih računara velika, to ne bi trebalo da predstavlja poseban problem ali ne može biti ni opravdanje za generator sa lošijim distribucijskim svojstvima.

- **Prenosivost**. Algoritam za generisanje slučajnih brojeva treba proizvesti jednak niz nezavisno od računarske platforme. Želja za brzinom i dužinom periode povremeno dovodi do implementacija aplikacija koje zavise od specifičnih karakteristika pojedinog uredaja, tako da je potrebno testiranje takvih aplikacija prilikom prenosa na neku drugu računarsku platformu.

- **Slučajnost**. Najvažniji i najteže ostvarljiv uslov. Postoje dva opšta aspekta o kojima se vodi računa prilikom konstruisanja generatora slučajnih brojeva: teorijska svojstva i statistički testovi. Generatore sa dobrim teorijskim svojstvima neophodno je podvrgnuti statističkom testiranju.

4.1.1. Tipovi generatora brojeva slučajnih vrednosti

Brojevi slučajnih vrednosti se, korišćenjem računara, generišu na osnovu dva pristupa:

- **deterministčkog** – kod generatora pseudoslučajnih brojeva PRNG (*Pseudorandom Number Generator*) i
- **nedetermističkog** – kod generatora istinski slučajnih brojeva TRNG (*True Random Number Generator*).

Navedeni pristupi generisanja se u mnogo čemu razlikuju i imaju svoje prednosti i mane.

Princip rada TRNG-a je dosta drugačiji od rada PRNG-a, tako da postoji primetna razlika u njihovim karakteristikama. TRNG-i su dosta neefikasniji u poređenju sa PRNG-ima (u smislu brzine) i za proizvodnju iste količine slučajnih brojeva treba im znatno više vremena. Sa druge strane, vrednosti slučajnih brojeva dobijene TRNG-ima su potpuno nedeterminističke, što podrazumeva nemogućnost reprodukovanja proizvedenih nizova.

Pseudoslučajni generatori brojevnih vrednosti u principu predstavljaju algoritme kojima se na osnovu početnih ili inicijalnih stanja dobijaju nizovi brojeva prividno slučajnih vrednosti. Pomoću računara se u većini slučajeva proizvode takvi pseudoslučajni brojevi, odnosno brojevi koje je moguće predvideti, jer se sam proces proizvodnje zasniva na proračunu matematičkih formula. Tako da se poznavanjem početnog uslova koji se inače dobija iz TRNG, sve sledeće vrednosti brojeva mogu predvideti. Vrednosti ovih brojeva su periodične tako da se njihovi nizovi posle određenog perioda iznova ponavljaju. Do pre određenog vremena su se, uz upotrebu specijalnih metoda, ovakvi nizovi prilično lako razbijali. Međutim, u današnje vreme pravljenjem mnogo savršenijih algoritama, dobijaju se periodi ponavljanja vrednosti koji su mnogo duži i kojima se provaljivanje postupka generisanja mnogostruko otežava. Kako se karakterišu velikom brzinom generisanja veoma su praktični i imaju veliku primenu. Naravno, za šifrovanje podataka odnosno informacija od izuzetno velike važnosti i za koje je potrebna stroga tajnost, ove generatore zamenjujemo generatorima istinski slučajnih brojeva. Karakteristike generatora pseudoslučajnih vrednosti mogu biti veoma dobre, uz veoma pažljivo i oprezno biranje početnih stanja čime se prikrivaju deterministička svojstva koja se koriste u kriptoanalizi.

Generatori brojeva pseudoslučajnih vrednosti su veoma brzi, dosta ih je lako napraviti i izuzetno su pogodni za simulacije [121]. Međutim, kada je reč o kriptografiji, potrebno je veliku

pažnju pokloniti samom izboru generatora slučajnosti, njegovim karakteristikama i mogućim statističkim manama koje inače najčešće koriste potencijalni napadači pri kriptoanalizi. Što se testiranja generatora tiče, ona se izvode statističkim testovima slučajnosti i pomoću njih se utvrđuju karakteristike generisanih nizova brojeva a samim tim i osobine generatora. Ne postoji određena, precizno odabrana, grupa testova koja bi se kao univerzalna primenjivala za ispitivanje svih generatora slučajnih brojeva. Konstrukcija generatora pseudoslučajnih vrednosti se jednostavno izvodi tako što se na osnovu potencijalne namene prvo izvrši procena karakteristika koje bi taj generator trebao da zadovolji, pa se tek posle konstrukcije algoritma vrši njegovo statističko ispitivanje karakteristika i proverava ispunjenosti postavljenih zahteva.

Za razliku od matematičkih, postoje generatori istinski slučajnih brojevnih vrednosti koji brojeve slučajnih vrednosti formiraju na osnovu vrednosti dobijenih iz slučajnih fizičkih procesa. Neki od jednostavnijih primera su vremenske razlike pri pritiskanju dva tastera tastature ili promene koordinata pri pomeranju miša. Međutim, mora se biti pažljiv prilikom izbora spoljnog izvora slučajnosti. Mnogo bolji primeri su generatori istinski slučajnih brojeva na bazi atmosferskog šuma [29], detektovanja raspada radioaktivnih elemenata [30], termalnih šumova kod poluprovodnika [31] i otpornika [32], fotoelektričnih efekata ili raznih kvantnih fenomena [33]. Ovakve pojave čije ponašanje je nedeterminističko mogu biti izvori slučajnosti potrebni za dizajniranje TRNG-a. Ova ponašanja izvora su možda najvažnija za rad TRNG-a jer ona određuje raspoloživu entropiju. Pri određivanju dizajna TRNG-a vrlo je važno odrediti raspoloživu entropiju i njene tačne statističke osobine, kao i ispitati dugoročne efekte koji mogu uticati na izazivanje njenog pogoršanja odnosno na kvalitet koji izvor ima u pogledu njegove sposobnosti stvaranja entropije. Međutim, iako postoji mnogo tehničkih rešenja za praćenje i kontrolu rada ovakvih izvora, pojave i uzroci grešaka su veoma teški za otkrivanje i predviđanje.

Istinski slučajni brojevi se dobijaju iz istinski slučajnih bitskih nizova kod kojih važi pravilo nezavisnosti i nepristrasnosti bita. S obzirom na korišćenje slučajnih brojeva u različitim oblastima radi se o različitim zahtevima koji se odnose na kvalitet generisanih nizova. Za potrebe simulacija najčešće je potrebno samo ispuniti uslov nezavisnosti i identične distribucije brojeva. vrednosti. Dok je kod kriptografije neophodno ispuniti uslov nemogućnosti pogađanja narednog broja niza. Kriptografski sistem sa visokim stepenom bezbednosti nemoguće je realizovati bez kvalitetnog TRNG-a koji predstavlja njegovu najvažniju komponentu sigurnosti, obezbeđujući svojim radom garantovano bezbedan ključ [35], [37], [127]. Za dobar kvalitet TRNG-a potrebna je i post-procesna obrada [43], mada sprovođenje ovog postupka nije neophodno u svim dizajnima (na primer TRNG-i bazirani na kvantnim fenomenima).

Primarni cilj primene post-procesiranja je eliminisanje pristrasnosti ili međuzavisnosti u

entropiji izvora ili mehanizmu ekstraktovanja [36]. Sekundarni cilj, koji je dobio na značaju zbog aktivnih direktnih i bočnokanalnih zlonamernih napada, je da se obezbedi otpornost na promene u okruženju i otkloni mogućnost falsifikovanja od strane potencijalnih protivnika [44].

Treba napomenuti da fizičke generatore istinski slučajnih brojeva ne treba smatrati potpuno fizičkim iako za svoj rad koriste fizičke izvore slučajnih vrednosti. Razlog za to je što ovakvi generatori obično poseduju algoritam za destilaciju odnosno post obradu signala kojim se sve nesavršenosti otklanjaju, a sve u cilju konstantnog dobijanja izlaza većeg kvaliteta. Upotreba procesa destilacije je potrebna da bi se prevazišle slabosti u izvoru entropije koja dovodi do proizvodnje brojeva koji nisu slučajni (na primer pojava dugih nizova nula ili jedinica).

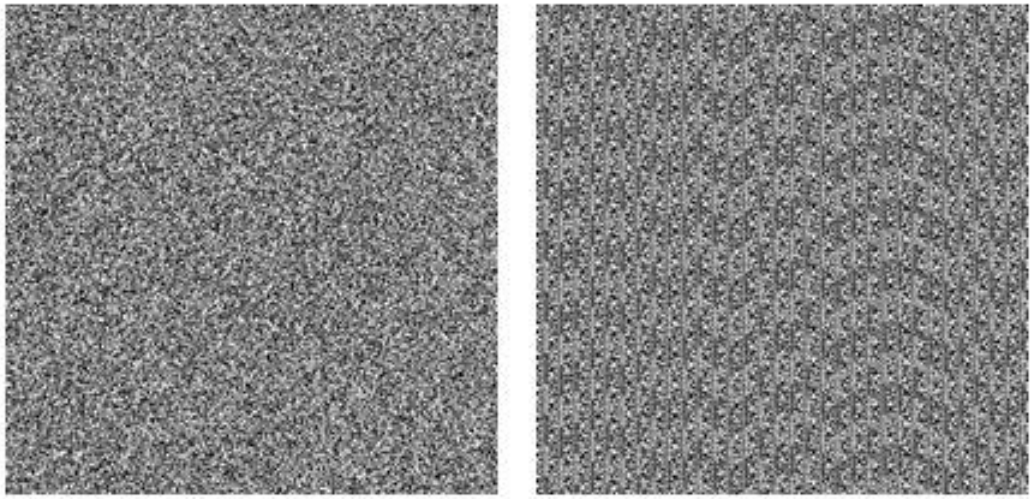
Generatoru istinski slučajnih brojeva je za generisanje istinski slučajnih brojeva potreban prirodan izvor slučajnosti odnosno entropije. Odmerci signala, ovakvog izvora entropije, obrađuju se u računaru i dobijaju se sekvence slučajnih brojeva. Izvor entropije se tipično sastoji od neke fizičke veličine, kao što je buka iz radija [46], proteklo vreme između emisije čestica tokom radioaktivnog raspadanja [47], termički šum kod poluprovodnika [48] ili frekvencija nestabilnosti kod oscilatora [49].

4.1.2. Razlike između TRNG-a i PRNG-a

Osnovne osobine generisanja slučajnih nizova TRNG dovode u bolju poziciju, u odnosu na PRNG, u pogledu podobnosti korišćenja kod kriptografskih sistema pri šifrovanju podataka i kod igara na sreću. Sa druge strane, mala brzina generisanja i nemogućnost ponovnog generisanja identičnog niza, čini ga nepogodnijim u odnosu na PRNG, koji se veoma često koristi u praksi kod velikog broja simulacija i pri modelovanju velikog broja aplikacija za koje je vrlo često potrebno proizvesti ogromnu količinu brojeva u vrlo kratkom vremenskom periodu.

Tabela 4.1. Pregled osnovih razlika karakteristika između TRNG-a i PRNG-a

Karakteristike generisanja	PRNG-i	TRNG-i
Velika brzina	da	ne
Deterministička svojstva	da	ne
Mogućnost ponavljanja	da	ne



Slika 4.1. *Prikaz grafičke analize rezultata kod TRNG-a (levo) i PRNG-a (desno)*

4.1.2.1. Klasifikacija generatora istinski slučajnih brojeva

Generatori istinski slučajnih brojeva se generalno dele u tri grupe. Prvu grupu čine fizički, drugu nefizički a treću grupu predstavljaju kombinovani generatori istinski slučajnih brojeva.

- **Fizički TRNG-i** – ili hardverski generatori slučajnih nizova, koriste kao izvore slučajnosti nedeterminističke efekte elektronskih kola, elemenata i uređaja (npr. šum proboja Zener diode, termalni šum kod poluprovodnika i otpornika, frekvencija nestabilnosti slobodnih oscilatora, količina elektriciteta koja se napuni u kondenzatorima formiranim na spojevima metala i poluprovodnika u fiksnom vremenu, turbulencija vazduha oko diskova koja rezultuje u fluktuaciji vremena očitavanja sektora na disku, zvuk i šumovi na ulazu u mikrofon ili video ulaz video kamera) ili fizičke eksperimente (npr. vreme proteklo između emitovanja čestica radioaktivnih izvora, fotoelektrični efekti ili razni kvantni slučajni procesi).
- **Nefizički TRNG-i** –ili softverski generatori slučajnih nizova, kao izvore slučajnosti koriste nedeterminističke događaje odnosno verovatnosnu prirodu nekih fenomena dostupnih programima koji se izvršavaju na tipičnom računaru kao što su sistemsko vreme, vreme proteklo između uzastopnih otkucaja tastature ili kretanja miša, sadržaj ulazno-izlaznih bafera, korisnički ulaz, neke veličine iz operativnog sistema, npr. opterećenje računara ili neka statistika iz mrežnog okruženja.

- **Kombinovani TRNG-i** – predstavljaju još jedan način generisanja istinski slučajnih brojeva koji za svoj rad koriste kombinovanje nekoliko nezavisnih izvora slučajnosti. Slučajnost i nezavisnost ovih kumulativnih izvora direktno zavisi od broja kombinovanih izvora, međutim, mogućnost nekih statističkih grešaka je još uvek prisutna a moguće ih je ublažiti kroz post-procesnu fazu.

U nekim slučajevima izvor slučajnosti ne proizvodi slučajne impulse u skladu sa potrebama korisnika. Iz ovog razloga se za modifikaciju generisanih slučajnih impulsa prema određenoj raspodeli koristi post-procesna faza destilovanja entropije izvora [51]. Ovo omogućuje fleksibilnost provere entropije direktno pre i posle post-procesne faze ostavljajući otvorena vrata za dizajniranje različitih post-procesnih algoritama.

4.1.2.2. Potreba za generatorima istinski slučajnih brojeva

Poznato je da PRNG-i odgovaraju potrebama mnogih aplikacija koje zahteva čitav niz oblasti, uključujući kriptografiju [52], simulacije [53], uzorkovanje [54], igre na sreću [55], [120], kao i problemi kod donošenja odluka, medicine i estetike [56,57] ili umetnosti, međutim, ponekad generisanim brojevima nedostaju jake statističke karakteristike. U ovakvim situacijama, korišćenje PRNG-a može da postane nepouzdano jer njegov niz postaje predvidljiv zbog njegovih deterministickih svojstava [58]. Takođe je primećeno da generator slučajnih bita kombinovan sa običnim klasičnim digitalnim kanalom (ova kombinacija se naziva „simetrični binarni kanal sa bukom") povećava kriptografski potencijal takvog kanala [61].

Zbog svega toga, kao i zbog danas česte upotrebe računarskih sistema, u ovom radu su istaknute prednosti primene potpuno nezavisnog generatora istinski slučajnih brojeva zasnovanog na arhitekturi zvučne kartice, izvoru buke životne sredine i post-procesnom metodu miksovanja i XOR-ovanja bita. Predstavljen je jednostavan i efikasan način generisanja TRNG-a bez namere kompromitovanja značaja PRNG-a.

4.1.2.3. Bazna zasnovanost dizajna generatora istinski slučajnih brojeva

Do sada je predložen veliki broj dizajna TRNG-a [64]. Ovi projekti se značajno razlikuju

po izboru izvora entropije ali i po načinu primene tehnike post-procesiranja. Svaki dizajn ima svoje prednosti i mane. Neke od ovih karakteristika se odnose na performanse a neke na bezbednost. Sa praktične tačke gledišta od suštinskog je značaja da TRNG-i budu dizajnirani na bazi jeftinog raspoloživog procesa. Štaviše, veoma je poželjno da se za dizajniranje TRNG-a koriste isključivo tehnička rešenja digitalnog tipa. Međutim, procena kvaliteta dizajna TRNG-a nije lak zadatak. Ipak, primarni cilj procene kvaliteta jeste utvrđivanje entropije po slučajnom bitu ili dobitak od entropije po slučajnom bitu.

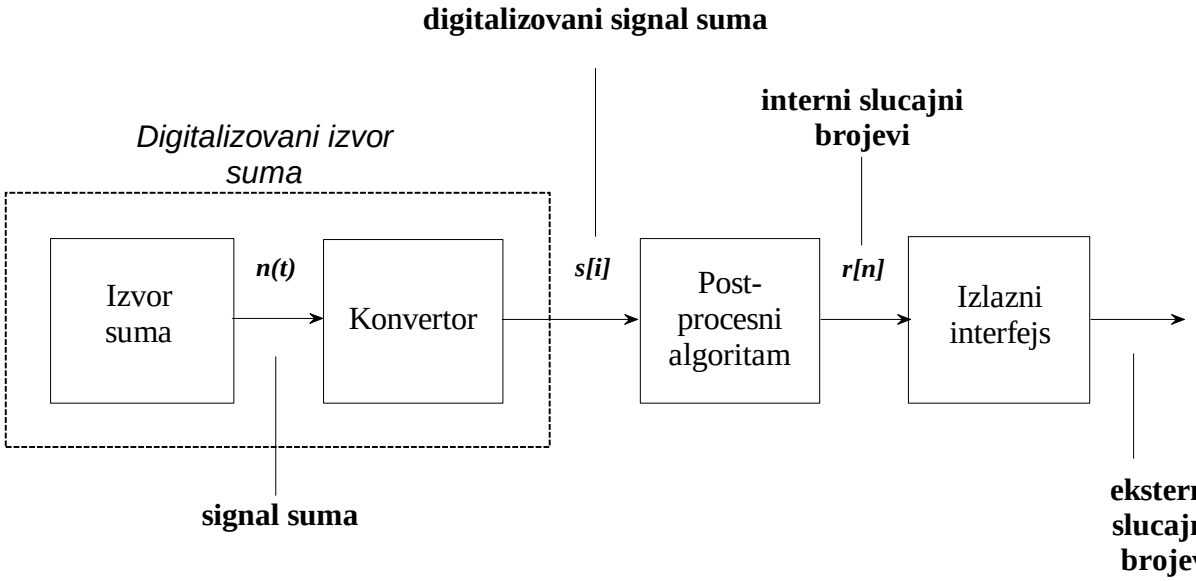
Istraživanja kod TRNG-a su koncentrisana na razvoj boljih fizičkih izvora šuma. Višestruki dizajni zasnovani na različitim izvorima slučajnosti i različite tehnike za generisanje slučajnih brojeva su već predložene [18]. Na primer, neke koriste kombinaciju analognih i digitalnih dizajna za generisanje i obradu belog termičkog šuma [38], [80], neke druge primenjuju jednostavnu arhitekturu stabilnih stanja kombinujući veliki broj kola [21], [49].

Većina postojećih pristupa za generisanje slučajnih brojeva zasniva se na PRNG-ima, bilo da su to grupe sesija ili korišćenje strukture stanja memorije koja se nalazi u arhitekturi zvučne kartice. Novi pristupi su se bavili istraživanjem osobina zvučnih i grafičkih kartica zasnovanoj na CUDA (Compute Unified Device Architecture). Po našem dosadašnjem saznanju, pristup koji je prikazan u ovom radu nije ranije dokumentovan.

4.2. Postupak dobijanja istinski slučajnih brojeva

Proces rada TRNG-a moguće je podeliti na tri zasebna dela (Slika 4.). U prvom delu generiše se digitalizovani signal (DAS), dobijen iz analognog slučajnog signala koga stvara neka prirodna pojava kao izvor slučajnosti, odnosno slučajni fizički proces (npr. atmosferski šum), i to tako što se periodično digitalizuje analogni kontinualni signal.

U drugom delu generišu se interni (unutrašnji) slučajni brojevi, ili DAS slučajni brojevi posle primene postupka post-procesiranja koji se vrši u cilju smanjivanja njihovih statističkih slabosti raspodele i poboljšanja karakteristika slučajnosti. U trećem delu dobijaju se tako zvani spoljašnji slučajni brojevi i ova faza odgovara konačnom rezultatu algoritma na osnovu koga se izvlače brojevi iz niza dobijenog post-procesiranjem. Ovakav princip BSI sertifikaciono telo je usvojilo 2001 godine i objavilo njihovom 31 AIS publikacijom [62].



Slika 4.2 *Blok šema procesa rada generatora istinski slučajnih brojeva*

4.2.1. Prvi deo procesa rada generatora istinski slučajnih brojeva

Prvi deo procesa rada TRNG-a odnosi se na pretvaranje slučajnih analognih veličina (signala) u veličine digitalnog oblika. Ovo prevođenje jednog oblika signala u drugi, zbog samog naziva analognih i digitalnih signala, zovemo analogno – digitalnom (A/D) konverzijom. Za sprovođenje ovog postupka zaduženi su A/D konvertori i on se obavlja u tri koraka. U prvom koraku vrši se odmeravanje analognih signala, odnosno njihovih amplituda, u tačno određenim vremenskim razmacima. U drugom koraku vrši se kvantovanje odmerenih vrednosti i na kraju, u trećem koraku vrši se kodiranje dobijenih vrednosti.

Postupak odmeravanja analognih kontinualnih signala *n(t)* (slika 4.2) obavlja se koristeći ritam koji diktira taktni signal bloka za uzorkovanje A/D konvertora, nakon čega dobijamo vremenski diskretizovani analogni signal. Predstavljanje vrednosti amplituda analognog kontinualnog signala sada vrši niz sa diskretnim odmercima uzetim u istim, unapred određenim, vremenskim intervalima. Frekvenciju uzorkovanja biramo u skladu sa Nyquist-ovom teoremom $f_{odm} \geq 2 f_{\max}$, da bi izbegli preklapanje kod spektra. U slučaju korišćenja manjih učestanosti imamo pojavu izobličenja, koja nisu poželjna, i svakako ih treba izbeći.

Postupak kvantizacije sprovodi se zaokruživanjem vrednosti odmerenih amplituda vrednostima najbližih, unapred odabranih, dozvoljenih nivoa u ukupnom opsegu vrednosti amplituda, ili postupak kojim se određuju približne vrednosti amplitudnih odmeraka. Gustina kvantizacionih nivoa zavisi od definisanog broja nivoa koga određuje izbor broja bita po uzorku.

Proces kodovanja obavlja koder, na osnovu definisanog koda, koji generiše digitalni signal *s[i]* prilagođen obradi, prenosu i zapisu digitalnih sistema odnosno računaru. Kodovanjem se praktično vrši dodeljivanje binarnih kodova kvantizacijskim nivoima, a samim tim i određivanje kombinacija 0 i 1 za svaki odmerak. Veći broj bita, korišćen za predstavljanje svakog odmerka, određuje veću gustinu nivoa odnosno manje odstupanje od realnih vrednosti.

4.2.2. Drugi deo procesa rada generatora istinski slučajnih brojeva

Drugi deo procesa rada TRNG-a odnosi se na post-procesiranje ili destilaciju niza bita dobijenog analogno-digitalnom konverzijom slučajnog analognog signala, odnosno na generisanje internih ili unutrašnjih slučajnih brojeva *r[n]* – slika 4.2. To je postupak eliminisanja loših karakteristika niza slučajnih bita koji se dobijaju na izlazu A/D konvertora, koje se pojavljuju kao posledica nesavršenosti ulaznih analognih signala, čime se popravlja entropija izvora po bitu. Proces destilacije mogli bi smo definisati i kao stvaranje sigurno nepredvidljivih nizova iz nesigurno nepredvidljivih izvora nizova.

Destilacija praktično predstavlja proces transformisanja digitalizovanog slučajnog signala u uniformno raspoređen niz slučajnih brojeva iako ulazni slučajni signal ima dosta statističkih nedostataka slučajnosti. Čak se destilacijom povećava entropija u delu kojim se onemogućuje pojavljivanje dugog niza 0 ili 1 što je redovna pojava kod signala na izlazu iz A/D konvertora.

Svrha sprovođenja procesa post-procesiranja je ispravljanje loših osobina slučajnosti TRNG-a poput male entropije, velike pristrasnosti ili biasa, i velike autokorelacije. Upotreba procesa destilacije je generalno potrebna da bi se prevazišle slabosti karakteristika slučajnosti izvora entropije, koje dovode do pojave vrednosti brojeva koje nisu slučajne kao što su na primer pojave dugih sekvenci 0 ili 1.

Glavni problemi koji se javljaju pri konstrukciji nedeterminističkog generatora slučajnih brojeva su statistički bias i korelacije između bita a radi boljeg razumevanja ovih pojmova kao i

pojma neizvesnosti objašnjena je i entropija kao mera neizvesnosti odnosno neodređenosti. Potpuno slučajne nizove brojeva karakteriše to da im bias i autokorelacijski koeficijent teže nuli a entropija jedinici kad posmatrana dužina niza teži beskonačnosti.

4.2.2.1. Entropija generatora slučajnih brojeva

Kvalitet generatora slučajnih brojeva određuje, u najvećoj meri, vrednost njegove entropije. Ona predstavlja meru za količinu neodređenosti sistema, u smislu prelaza u neko od mogućih stanja, odnosno meru nepredvidljivosti stanja slučajne promenljive. Pod entropijom, u teoriji informacija, podrazumeva se prosečna količina informacije koja je sadržana u generisanim porukama informacionih izvora.

Entropija kao mera neizvesnosti, u pogledu izbora jedne od mogućih vrednosti promenljive *X*, računa se iz izraza:

$$H_{(X)} = -\sum_{i=1}^{n} P(x_i) \log_b P(x_i) \tag{4.1}$$

gde je *X* diskretna slučajna promenljiva sa vrednostima iz skupa $\{x_1, x_2, x_i, \dots, x_n\}$, a $P(x_i)$ su verovatnoće pojavljivanja vrednosti x_i, $1 \leq i \leq n$.

Entropiju poruke u bitima računamo kao $\log_2 n$, gde n predstavlja moguća stanja. Za entropiju binarnih nizova podrazumeva se informacija po bitu. Poželjno je da entropija *H* bude vrednosti $H \approx 1$. Ona je ove vrednosti pri verovatnoći pojavljivanja 0 i 1 $P_{0/1} \approx 0.5$.

4.2.2.2. Bias

Neka je *X* diskretna slučajna promenljiva sa vrednostima $\{0,1\}$. Tada jednačina:

$$b = \left| P(0) - \frac{1}{2} \right| = \left| P(1) - \frac{1}{2} \right| \tag{4.2}$$

predstavlja *bias* od *X*.

Za dobar TRNG, bias bi trebalo da konvergira ka 0. To praktično znači da je poželjno da broj jedinica u slučajnom nizu bita, bude jednak broju nula.

4.2.2.3. Autokorelacija niza slučajnih brojeva

Autokorelacija predstavlja uzajamni odnos slučajnih vrednosti promenljivih veličina u nekom slučajnom procesu odnosno pokazuje kolika je zavisnost između vrednosti signala u različitim vremenskim trenucima t_1 i t_2.

Neka je $X(t)$ slučajni proces.

Autokorelacijska funkcija ovakvog procesa data je formulom:

$$R_{XX}(t_1,t_2) = E\left[X(t_1)X(t_2)\right] = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} x_1 x_2 f_{X(t_1),X(t_2)}(X_1, X_2)dx_1 dx_2 \qquad (4.3)$$

Često se umesto vremena t_1 i t_2 uzima vreme t_1 i t_1 pomereno za τ gde je $t_2 - t_1 = \tau$. U tom slučaju se autokorelacijska funkcija označava sa $R_{XX}(t,\tau)$ i računa kao $E\left[X(t)X(t+\tau)\right]$.

Za dobar TRNG, autokorelaciona funkcija bi trebalo da konvergira ka 0.

Kako se raspolaže konačnim brojem realizacija slučajnog procesa ne mogu se direktno koristiti definicijski izrazi (3) za računanje autokorelacijske funcije. Ukoliko želimo izvršiti procenu AKF potrebno je izvršiti njeno usrednjavanje odnosno izračunavanje njene srednje vrednosti, pa računamo:

$$R_{XX}(t_1,t_2) = E\left[X(t_1)X(t_2)\right] \approx \frac{1}{N}\sum_{i=1}^{N} X_i(t_1)X_i(t_2) \qquad (4.4)$$

Primetno je da se u ovom slučaju radi sa parom slučajnih uzoraka odnosno uzimaju se dva slučajna uzorka $X(t_1)$ i $X(t_2)$ iz iste realizacije.

Umesto trenutaka t_1 i t_2, mogu se uzeti vreme t i pomeraj τ kao nezavisne promenljive, s tim da je $t_1 = t$ i $t_2 - t_1 = \tau$.

$$R_{XX}(t,\tau) = E\left[X(t)X(t+\tau)\right] \qquad (4.5)$$

Tada se autokorelacija izračunava kao:

$$R_{XX}(t,\tau) = \lim_{N\to\infty}\frac{1}{N}\sum_{t=1}^{N} x(t)x(t+\tau) \approx \frac{1}{N}\sum_{i=1}^{N} X_i(t)X_i(t+\tau) \qquad (4.6)$$

Ovo je slučaj kada je X neprekidno (kontinualno) tako da se na ovaj način računa autokorelacija po bajtovima.

Od presudne važnosti za dobijanje dobrih rezultata je potpuno razumevanje autokorelacijske funkcije odnosno njena primena kao i način računanja u slučaju digitalnih podataka.

Ako je X digitalno i podaci se uzimaju po bitu, u intervalu $r\Delta t$, onda se autokorelacija računa kao:

$$R_{xx}(t, r\Delta t) = \frac{1}{N-r}\sum_{n=1}^{N-r} x_n(t)x_n(t+r\Delta t) \equiv \frac{1}{N-r}\sum_{n=1}^{N-r} x_n x_{n+1} \tag{4.7}$$

gde je $r = 0,1,2,3, \dots, m$ za $m < n$.

Ova skraćena autokorelacija se često naziva nepristrasna empirijska autokorelacija i posmatra se kao numerička procena pune autokorelacije.

4.2.2.4. Različite tehnike post-procesiranja

Pri ispunjavanju zahteva za tajnošću kriptografskih aplikacija, potrebno je da slučajni brojevi zadovolje stroge kriterijume slučajnosti, kao što su nepredvidljivost, nepristrasnost, nezavisnost jednih od drugih i uniformna distribucija. Tipičan TRNG koji koristi isključivo nedeterministički izvor entropije, ne može proizvoditi dovoljne statističke slučajnosti koje bi zadovoljile pomenute kriterijume. Zato se koristi zajednički pristup prevazilaženju nedostataka izlazlaznih nizova bita korišćenjem naknadnih tehnika destilacije odnosno post-procesiranja i poboljšavanja entropije izvora.

Najčešće primenjivane tehnike, koje su se pokazele vrlo efikasnim, su Nojmanova tehnika post-procesiranja [102], tehnika pariteta niza [104] i XOR tehnika [9], [105].

Von Neumann-ova tehnika se sastoji u prevođenju uzastopnih parova bita S_{2i} , S_{2i+1} u izlaz S_{2i} za $S_{2i} \neq S_{2i+1}$ a za ostale slučajeve u odbacivanju bitskih parova. Osnova ove tehnike je algoritam koji vrši mapiranje prelaza bitskih parova niza. Ispituje se svaki par bita niza i ukoliko je slučaj da ima prelaza između bita, npr. 01 ili 10, zadržava se samo jedan od njih a u slučaju da nema prelaza, 00 ili 11, vrši se odbacivanje oba bita.

Kompletan potupak je izmislio i učinio ostvarljivim naučnik Nojman (John von Neumann) tako da ga vrlo često nazivamo i Nojmanovim korektorom.

Tehnika pariteta niza izvodi se deljenjem nizova na parove bita a zatim se vrši određivanje pariteta svih parova. Svaki par kod koga su pariteti različiti, 10 i 01, se odbacuje a kod parova istih pariteta, 11 i 10, zadržava se jedan od njih.

Međutim, postoji nekoliko konsekvenci, naime, ove tehnike smanjuju protok bita u proseku za faktor 4 i izlazni strim će imati promenljivu brzinu bita zavisno od distribucije ulaznih parova bita.

Pokazalo se da tehnika zasnovana na operaciji XOR-ovanja može biti iskorišćena kao zadovoljavajući post-procesor. Jedan od primera je XOR10 post-procesor kod koga se XOR-uju bit najveće težine (eng. most significant bit MSB) i bit najmanje težine (eng. least significant bit LSB) svakog desetog odmerka [9]. Post-procesor, je osim toga, dodatno poboljšan tako da se može koristiti mnogo komplikovaniji XOR korektor, koji kombinovanjem mnogo više od dva bita ulaznog strima daje izlazni strim. XOR korektor se takođe može primeniti na bit strimove koji su generisani sa različitih RNG-a.

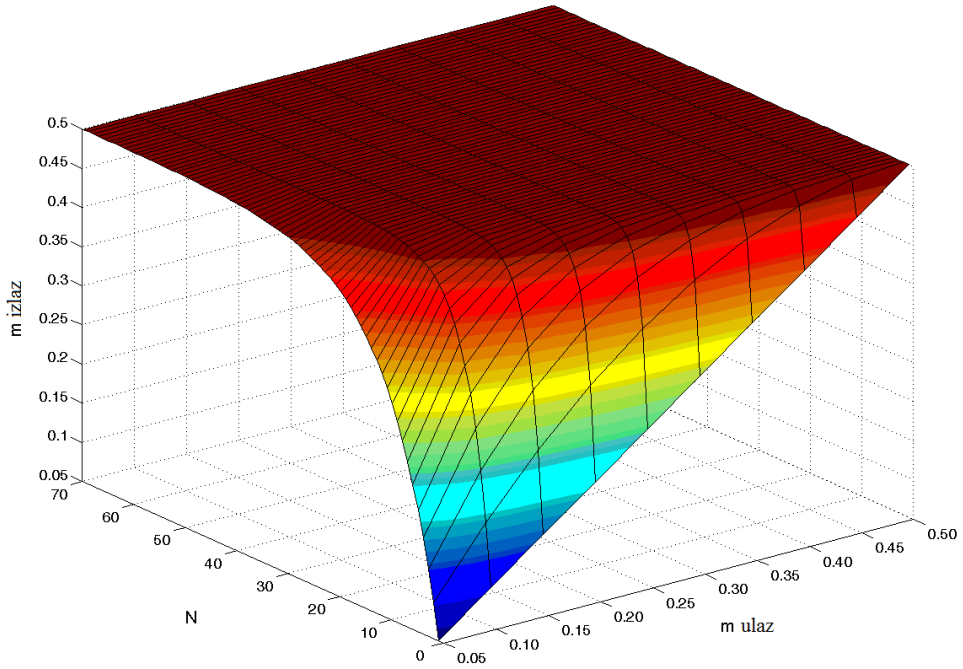
Postupak primene pomenutih tehnika, Nojmanovog korektora (transition mapping), Pariteta niza (stream parity) i XOR-ovanja, u slučajevima različitih mogućih kombinacija parova bita ulaznog niza, prikazan je u Tabela 4..

Tabela 4.2. Prikaz rada Nojmanovog korektora, tehnike pariteta niza i XOR tehnike

Parovi ulaza	Verovatnoća	Rezultat izlaznih bita		
		Nojman	Paritet	XOR
00	AA	ništa	0	0
01	AB	0	ništa	1
10	BA	1	ništa	1
11	BB	ništa	1	0

Pored navedenih, najčešće korišćenih postupaka u procesu uklanjanja bias-a iz izlaznih nizova, pre svega zbog nedovoljno slučajnih ulaznih sekvenci, vrlo često se kao post-procesor koristi i T tip flip-flopa.

Analiza efekta T flip-flopa prikazana je na slici 4.3 na kojoj je određena vrednost izlazne sekvence m_{izlaz} prikazana kao funkcija od m_{ulaz} i N, za $m_{ulaz} \in [0.05, 0.5]$. U ovom slučaju su m_{ulaz} i N određene vrednosti ulazne sekvence i broja bita izlazne sekvence, respektivno. Kao što je prikazano na slici, korišćenje T flip-flopa garantuje izlazni niz bita nepristrasno (bez bias-a) raspoređenih vrednosti [22].



Slika 4.3. *Dobijene vrednosti izlazne sekvence m_{izlaz} u odnosu na m_{ulaz} i N kod T flip-flopa [22]*

Upotrebom procesa destilacije povećava se entropija izvora i dobija niz bita sa mnogo boljim karakteristikama slučajnosti. Primenom prikazanih digitalnih post-obrada nizova obezbeđuje se uniformnost raspodele promenljivih i izlazni niz izbegava određene pristrasnosti i statistički je nezavisan od karakteristika izvora slučajnih signala.

4.3. Ispitivanje slučajnosti nizova slučajnih brojeva

Da bi se slučajni brojevi koristili direktno (bez dalje obrade), izlaz iz generatora istinski slučajnih brojeva mora da zadovolji stroge kriterijume slučajnosti merene statističkim testovima jer je nemoguće matematički dokazati da li su generisane sekvence slučajne. Međutim postoji mogućnost da slučajni niz TRNG-a ne može proći neka od statističkih ispitivanja.

Postupak ispitivanja kvaliteta generisanih slučajnih nizova zahteva primenu većeg broja testova [110]. Međutim, nema univerzalnog skupa testova koji sa sigurnošću dokazuju da je određeni generisani niz potpuno slučajan i da ispunjava sve kriterijume slučajnosti. Iz rezultata testiranja moguće je zaključiti da ispitivani niz poseduje neke od karakteristika kakve bi trebalo

da pokazuje niz dobijen idealnim generatorom. Sa druge strane, rezultati ispitivanja sa sigurnošću mogu navesti na zaključak da niz nije slučajan i da je rad generatora loš.

Ispitivanjem karakteristika slučajnog niza određuju se statističke vrednosti na osnovu kojih se donosi odluka o prihvatanju ili odbacivanju. Takođe je važno i određivanje kritičnih vrednosti koje ne smeju biti premašene. Kritične vrednosti predstavljaju granicu vrlo malih verovatnoća realizacije određenog dogadaja, odnosno to su statističke granične vrednosti slučajnosti koje se ne smeju prelaziti. Ukoliko su vrednosti generisanih nizova u okvirima ovih granica smatra se da se radi o generisanju slučajnih nizova a ako su ispod ili iznad granica, smatra se da su generatori nesigurni.

Pod merom sigurnosti prihvatanja ili ne prihvatanja generatora podrazumeva se vrednost nivoa značaja. Određivanjem prevelikih, ili premalih vrednosti ovih parametara možemo doći u situaciju koja nalaže odbacivanje slučajnog niza a samim tim i do ne prihvatanja generatora. Primenom svakog testa ispituje se određene karakteristike niza slučajnih brojeva na osnovu kojih se određuje kvalitet posmatranog generatora.

Obično se testovima proveravaju odnosno ispituju sledeće raspodele vrednosti:

- Očekivane raspodele vrednosti nekog prostora posmatranja i
- Očekivane raspodele učestalih pojava nekog događaja.

Odabir na koje će se anomalije obratiti pažnja, deli statističke testove prema oblasti primene generatora. Skup statističkih testova koji je definisan od strane Donalda Knutha [106], koristi se nad sekvencama koje se primenjuju za potrebe različitih simulacija, uglavnom kod pseudoslučajnih generatora, dok se NIST-ovi testovi [108] primenjuju za slučajne sekvence koje će kasnije naći primenu u kriptografiji.

Svi NIST-ovi testovi su zasnovani na matematičkim formulama i primenjuju se na izlazne binarne sekvence i to najčešće na uzorku ne manjem od 10.000 bita. Konačan rezultat svih testova predstavlja se vrednošću između nula i jedan. Rezultat testova predstavljen je sa vrednošću P (verovatnoća dobijanja date vrednosti), koja treba da ispuni uslov $P \geq 0{,}01$. Ukoliko je uslov ispunjen, generator se smatra slučajnim, što znači da daje slučajne nizove na svom izlazu. Međutim, poželjno je da vrednost P bude što veća ($P \approx 1$) kako bi na osnovu toga i generatori, koji se rangiraju po kvalitetu, bili višeg ranga.

Primenom serije testiranja može se doći do zaključka o posedovanju željenih karakteristika ispitivanog generatora i njegovom eventualnom prihvatanju i korišćenju u određenim oblastima za koje je namenjen.

4.3.1. Statistički testovi slučajnosti

Neka je $(X_1, X_2, ..., X_n)$ vremenska serija čiju slučajnost ispitujemo. Nulta hipoteza u testovima je hipoteza slučajnosti - da su slučajne promenljive $X_1, X_2, ..., X_n$ nezavisne i jednako raspodeljene. Izbor testa zavisi od alternativne hipoteze i svrhe korišćenja.

Skup statističkih testova, koji su prikazani u ovoj disertaciji, pripada skupu testova koji se najčešće primenjuju i koji su se pokazali veoma pouzdanim u postupku ispitivanja karakteristika generatora slučajnih brojeva i odnosi se, pre svega, na FIPS 140-1 (*Federal Information Processing Standard*) grupu statističkih testova i na veliku grupu NIST statističkih testova slučajnosti [109].

Najvažniji statistički testovi slučajnosti, kojima se u najvećoj meri određuje kvalitet slučajnog niza a samim tim i karakteristike slučajnosti generatora, su svakako sledećih šest bazičnih testova:

- Test frekvencija (monobitski test)
- Test serija (dvo bitski test)
- Poker test
- Ran test
- Autokorelacioni test
- Mauerov univerzalni test slučajnosti

4.3.1.1. Test frekvencija (monobitski test)

Namena ovog testa je utvrđivanje broja 1 i broja 0 u nizu, kao i toga da li je njihov broj približno isti. Koristi se statistika:

$$X_1 = \frac{(n_0 - n_1)^2}{n} \tag{4.8}$$

koja je raspodeljena kao χ^2 sa 1 stepenom slobode, za $n \geq 10$.

4.3.1.2. Test serija (dvo bitski test)

Namena ovog test je da utvrdi da li je raspodela bigrama 00, 01, 10, 11 ravnomerna, kao kod slučajnog binarnog niza. Koristi se statistika:

$$X_2 = \frac{4}{n}\left(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2\right) - \frac{2}{n}\left(n_0^2 + n_1^2\right) + 1 \tag{4.9}$$

$n_{00} + n_{01} + n_{10} + n_{11} = n - 1$ (usled preklapanja bigrama)

koja je raspodeljena kao χ^2 sa 2 stepena slobode za $n \geq 21$.

4.3.1.3. Poker test

Podelimo niz *s* u *k* nepreklapajućih delova, svaki dužine *m*.

Neka je zadovoljeno

$$\left\lfloor \frac{n}{m} \right\rfloor \geq 5 \cdot 2^m, k = \left\lfloor \frac{n}{m} \right\rfloor \tag{4.10}$$

Neka je n_i *broj pojavljivanja niza* $i-$*tog tipa,* $1 \leq i \leq 2^m$

Poker test ustanovljava da li se svi nizovi dužine m pojavljuju u onom broju koji bi se očekivao kod slučajnih nizova. Statistika

$$X_3 = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^2\right) - k \tag{4.11}$$

je raspodeljena χ^2 sa $2^m - 1$ stepena slobode.

4.3.1.4. Ran test

Očekivani broj ranova dužine i (ili jedinica ili nula) je

$$e_i = \frac{n - i + 3}{2^{i+2}} \tag{4.12}$$

Neka je k najveći ceo broj za koji je $e_i \geq 5$. Neka je B_i, G_i broj blokova i gepova dužine i u zadatom nizu, $1 \leq i \leq k$. Statistika

$$X_4 = \sum_{i=1}^{k} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{k} \frac{(G_i - e_i)^2}{e_i} \tag{4.13}$$

ima χ^2 raspodelu sa $2k-2$ stepena slobode.

4.3.1.5. Autokorelacioni test

Ako autokorelacionu funkciju predstavimo kao

$$A(d) = \sum_{i=0}^{n-d-1} S_i \oplus S_{i+d}\ , \quad 1 \le d \le \left\lfloor \frac{n}{2} \right\rfloor \tag{4.14}$$

onda statistika

$$X_5 = 2\left(A(d) - \frac{n-d}{2} \right) \Big/ \sqrt{n-d} \tag{4.15}$$

ima $N(0,1)$ raspodelu za $n-d \ge 10$.

4.3.1.6. Mauerov univerzalni test slučajnosti

Slučajni niz se ne može značajno komprimovati bez gubitka informacija.

Ako se neki niz može značajnije komrimovati on se odbacuje kao neslučajan niz.

Umesto komprimovanja, Muerov test izračunava veličine koje su u vezi sa dužinom komprimovane sekvence.

Univezalnost ovog testa se sastoji u svojstvu da detektuje gotovo sve opšte klase nedostataka pseudoslučajnih nizova pa se vrlo često naziva i Univerzalni test.

Zahteva znatno duže nizove nego standardni testovi.

Računski je vrlo efikasan.

4.3.1.7. Ostali važni testovi slučajnosti

- **Test za određivanje približne entropije**

Fokus ovog testa usmeren je na pojavu učestalosti mogućih preklapajućih n-bitskih

oglednih primeraka niza u cilju poređenja sa učestalošću kod očekivanog rezultata.

- **Test najdužih uzastopnih ponavljanja jedinica u bloku**

Ovim testom posmatra se dužina najvećeg uzastopnog ponavljanja jedinica n-bitskih blokova. Ima svrhu određivanja najdužih uzastopnih ponavljanja i proveru poklapanja sa očekivanom dužinom uzastopnih ponavljanja niza.

- **Test podjednake učestalosti u bloku**

U ovom ispitivanju vrši se posmatranje odnosa nula i jedinica n-bitskih blokova u cilju uočavanja i poređenja njihovih jednakosti u svakom od blokova.

- **Test preklapanja uzoraka**

Ovo ispitivanje odnosi se na posmatranje učestalosti pojave preklapanja mogućih n-bitskih oglednih primeraka celog ispitivanog niza. Ispitivanjem se otkriva broj preklapanja a zatim se vrši poređenje, koje bi trebalo da bude približno jednako, sa brojem preklapanja kod očekivanog niza.

- **Test uzastopnog ponavljanja istog bita u nizu**

Fokus kod ovog ispitivanja usmeren je na posmatranju ukupnog broja uzastopnog ponavljanja istih bita niza.

- **Test sa diskretnom Furijeovom transformacijom**

Ispitivanje ovim testom usmereno je na primeni diskretnih Furijeovih transformacija na nizove sa svrhom otkrivanja svih periodičnih funkcija kod nizova koje bi bile pokazivale odstupanja od pretpostavki slučajnosti. Cilj je otkrivanje da li se u količini najvećeg broja vrednosti, više od 95 procenata ukupnih vrednosti, dobijene vrednosti brojeva značajno razlikuju od preostalog broja vrednosti.

- **Test slučajnog kumulativnog zbira**

Ovo ispitivanje je bazirano na potrebi izračunavanja vrednosti kumulativnih zbirova pojedinih delova posmatranog niza i utvrđivanju da li su ove vrednosti previše male ili previše velike u poređenju sa vrednostima kumulativnih zbirova parcijalnih sekvenci očekivanog niza.

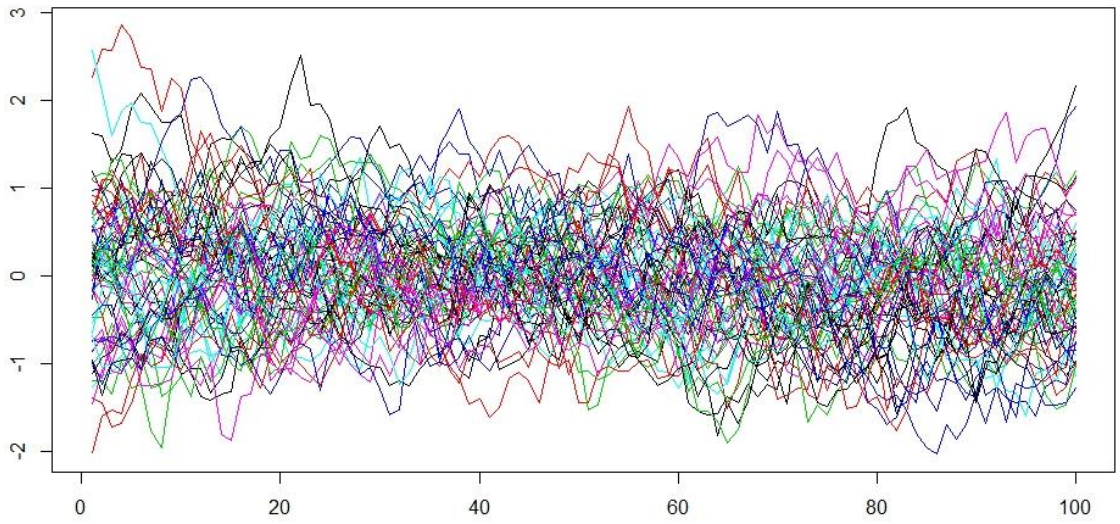
5 PRIMENA METODE MiBiS&XOR U POSTUPKU DESTILACIJE SLUČAJNIH NIZOVA

5.1. Postupak mešanja bita slučajnog niza

U ovoj disertaciji je predstavljen postupak rada generatora istinski slučajnih brojeva, odnosno novi princip proizvodnje istinski slučajnih nizova bita, koji se bazira na upotrebi zvučne kartice kao standardnom delu hardvera računara (desktop računari, lap topovi, mobilni telefoni), na koju se preko mikrofona dovodi slučajni šum buke iz životne sredine i na koji se, posle A/D konvertovanja, primenjuje novi metod destilacije ili postprocesiranja kojim se vrši mešanje bitskog niza u koracima a zatim XOR-ovanje dobijenih susednih bita (MiBiS&XOR). Primenom ovog postupka smanjuju se autokorelacija i bias a povećava entropija izlaznog bitskog niza.

Karakteristično za ovu metodu je korišćenje nesvakidašnjeg fizičkog izvora slučajno promenljivih veličina odnosno zvučnog signala stvorenog bukom u životnoj sredini. Korišćeni su sledeći slučajevi slučajnih zvučnih signala nastali:

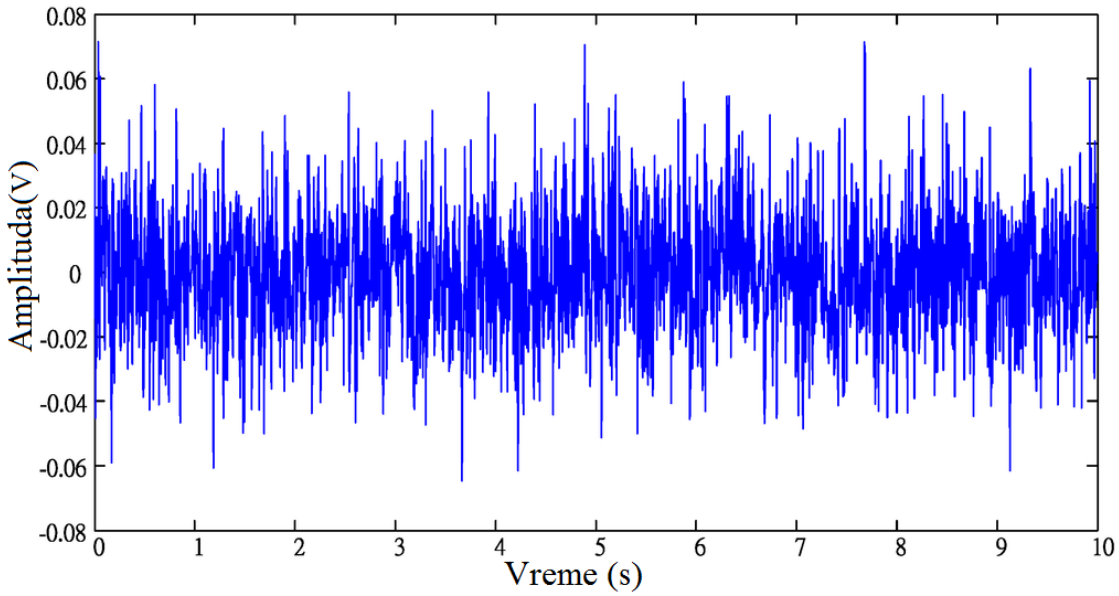
#1. Razgovorima brojnih šetača najprometnije pešačke zone grada,
#2. Saobraćajnom bukom,
#3. Bukom iz prometnog podzemnog pešačkog prolaza,
#4. Bukom na zabavi, kao posledica velike gužve, glasnih razgovora i snažne bučne muzike
#5. Mešovitom bukom nastalom zbirom saobraćajne buke, konverzacione buke brojnih učesnika, multimedijalnim zvucima i industrijskom bukom.



Slika 5.1. *Slučajni signali mešovite buke*

Kretanjem, to jest pomeranjem raznih objekata, saobraćajnom bukom, konverzacijskim razgovorima, bukom iz restorana, industrijskom bukom, kao i svom ovom superponiranom bukom, proizvodi se ogroman broj slučajnih signala zvuka sa različitim frekfencijama, amplitudama i fazama, koji prolaze kroz etar i odbijaju se od različitih prepreka stvarajući slučajno promenljivi zvučni pritisak koji detektuje mikrofon pretvarajući ga u električni signal nepredvidljivih amplitudnih vrednosti. Električni napon dobijen iz slučajnog analognog signala zvuka se zatim u A/D konvertoru zvučne kartice pretvara u diskretizovane odmerke (Slika 5.1 i Slika 5.2.) a zatim u skup digitalnih podataka predstavljenih binarnim nizom.

Iz dobijenog histograma uočljiva je normalna ili Gaussova raspodela čija je idealna karakteristika prikazana isprekidanom linijom. Kod signala sa ovakvom raspodelom verovatnoća da je broj amplitudskih odmeraka signala vrednosti nula je najveća, i postepeno se smanjuje za amplitude čije se apsolutne vrednosti povećavaju.

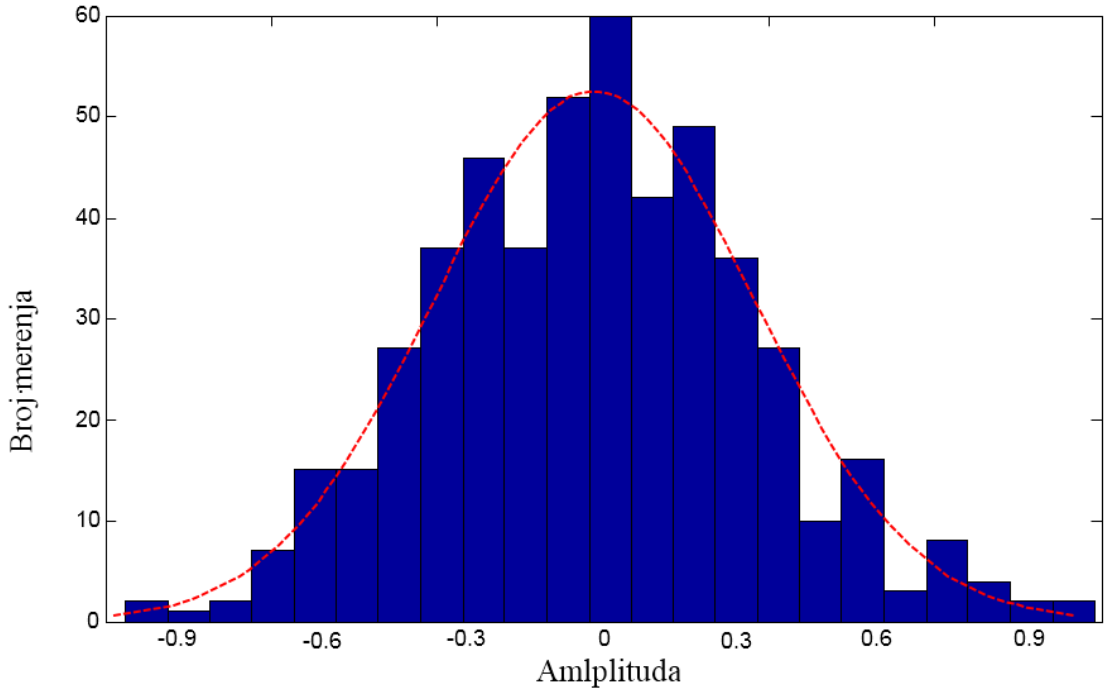


Slika 5.1. *Šum na izlazu iz ADC-a*

Ovakav tip raspodele kod kojih su verovatnoće dobijanja nekih vrednosti veće od verovatnoća dobijanja drugih vrednosti nije poželjna zbog toga što dobijene vrednosti niza nisu dovoljno slučajne odnosno nemaju zadovoljavajuće osobine slučajnosti.

Slučajne vrednosti kvalitetnih nizova moraju biti ravnomerno odnosno uniformno raspoređene, to jest moraju imati uniformnu a ne normalu raspodelu, da bi zadovoljili osnove kriterijume nepredvidljivosti, nepristrasnosti i nezavisnosti. Upravo zato se u ovom radu koristi pristup prevazilaženju nedostataka izlaznih bit sekvenci korišćenjem tehnike postprocesiranja.

Postprocesiranje ili destilacija u suštini predstavljaju proces transformisanja digitalizovanih vrednosti sa normalnom raspodelom u skup uniformno raspoređenih slučajnih vrednosti iako ulazni slučajni signal ima dosta statističkih nedostataka slučajnosti.



Slika 5.2. *Histogram šuma odnosno funkcije gustine verovatnoće amplituda*

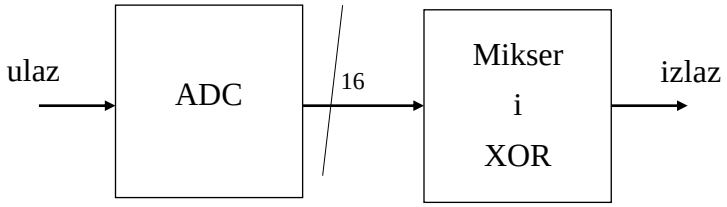
Ukoliko se za dobijanje istinski slučajnih impulsa koristi personalni računar onda se mikrofon sa neusmerenom karakteristikom prijema signala (elektrodinamički ili elektrostatički) preko 3,5 mm konektora direktno spaja na mikrofonski (MIC) ulaz računara. Ukoliko se koristi laptop (notebook computer) najbolje je koristiti laptopove sa ugrađenim (postojećim) elektrostatičkim mikrofonima koji se vrlo lako i bez ikakve dodatne opreme mogu koristiti za izvođenje eksperimenata na različitim lokacijama. Zbog svojih malih dimenzija i vrlo moćnih hardverskih i softverskih karakteristika za ove namene su takođe veoma pogodni tablet računari kao i smart mobilni telefoni novijih generacija.

Zavisno od modela kome pripada, zvučna kartica definiše dozvoljenu toleranciju ulaznog napona, frekvenciju očitavanja kao i rezoluciju očitavanja ulaznog zvučnog signala.

Dozvoljene maksimalne vrednosti ulaznog napona kreću se od [0.7 – 1] V. Frekvencije očitavanja su, uglavnom u području poznatih frekvencija odmeravanja: (22.05, 44.1, 96, 192) KHz. Moguće je izabrati rezoluciju očitavanja od 8, 16, 24 ili 32 bita. Ovi parametri očitavanja su izborni i podešavaju se odabirom ponuđenih opcija.

Vrednosti parametara pri izvođenju ovog eksperimenta bili su: 1V, 44.1 KHz, 16 bita.

Vrednosti odmeraka dobijene velikom frekvencijom odmeravanja imaju nedovoljno dobre korelacione karakteristike, jer se odmeravaju kontinualni signali čije se amplitude ne menjaju dovoljno brzo u odnosu na frekvenciju odmeravanja. Iz tog razloga je neophodna primena postupka destilacije, čiji je princip rada primenjen u ovom radu prikazan na Slika 3.4 i koji se izvodi mešanjem bita u koracima a zatim XOR-ovanjem susednih bita (MiBiS&XOR).



Slika 3.4. *Postupak destilacije mešanjem i XOR-ovanjem bita*

Prikazanom metodom prvo se u mikseru izvodi postupak mešanja niza bita, dobijenog na izlazu konvertora, a zatim se vrši XOR-ovanje susednih bita mešanjem dobijenog niza koji su se pre mešanja nalazili na velikoj geometrijskoj i vremenskoj razdaljini. Posledice primene ovog postupka su dobijanje niza kod koga je smanjena korelacija između bita, smanjen bias a povećana entropija.

Prvi korak mešanja izvodi se prihvatanjem miksera prvih dva bita dolazećeg niza iz ADC-a. Drugi korak predstavlja prihvatanje trećeg bita i njegovo smeštanje između između prva dva. Obeležavanjem bita brojevima dodeljenim na osnovu redosleda dolazaka, dobili bismo raspored bita $x1, \boldsymbol{x3}, x2$, gde je x promenljiva sa mogućim vrednostima [0,1]. Trećim korakom vrši se smeštanje četvrtog bita između bita 1 i 3 i smeštanje petog bita između 3 i 2. Dobijeni niz je sledećeg rasporeda $x1, \boldsymbol{x4}, x3, \boldsymbol{x5}, x2$. Četvrti korak predstavlja smeštanje šestog bita između prvog i četvtog, sedmog između drugog i petog, osmog između četvrtog i trećeg i devetog između petog i trećeg. Raspored dobijenog niza sada je $x1, \boldsymbol{x6}, x4, \boldsymbol{x8}, x3, \boldsymbol{x9}, x5, \boldsymbol{x7}, x2$ i prikazan je u Tabela 5.. Nastavljanjem postupka petim korakom nastaje niz sa rasporedom bita:

$$x1, \boldsymbol{x10}, x6, \boldsymbol{x12}, x4, \boldsymbol{x14}, x8, \boldsymbol{x16}, x3, \boldsymbol{x17}, x9, \boldsymbol{x15}, x5, \boldsymbol{x13}, x7, \boldsymbol{x11}, x2.$$

Šesti korak počinje smeštanjem 18-tog bita između 1 i 10, 19-tog između 2 i 11, 20-tog imeđu 10 i 6 a 21 između 7 i 11 itd. do raspoređivanja svih bita između postojećih bita iz prethodnog koraka.

Postupak raspoređivanja bita u sledećim koracima se ponavlja sve do raspoređivanja svih ulaznih bita između bita iz prethodnih koraka (Slika).

Prvi bit u završnom nizu je $x_{n-1}1$, gde je sa n označen korak datog niza pa bi $n-1$ značilo da se radi o prethodnom koraku, odnosno o nizu koji je dobijen u prethodnom koraku, a 1 da se radi o prvom bitu niza iz prethodnog koraka.

Tabela 5.1. Prikaz rasporeda nizova bita dobijenih u prvih pet koraka miksovanja

Redosled koraka	Redosled bita
1vi korak	$x1, x2$
2gi korak	$x1, x\mathbf{3}, x2$
3ći korak	$x1, x\mathbf{4}, x3, x\mathbf{5}, x2$
4ti korak	$x1, x\mathbf{6}, x4, x\mathbf{8}, x3, x\mathbf{9}, x5, x\mathbf{7}, x2$
5ti korak	$x1, x\mathbf{10}, x6, x\mathbf{12}, x4, x\mathbf{14}, x8, x\mathbf{16}, x3, x\mathbf{17}, x9, x\mathbf{15}, x5, x\mathbf{13}, x7, x\mathbf{11}, x2$

To je ujedno i prvi bit koji stiže iz ADC-a odnosno $x_{n-1}1 = x1$.

$x_n1, x_n2, x_n3, \dots, x_nm\text{-}1, x_nm$ su datim redosledom ubačeni biti *n*-tog koraka, gde je sa *m* označen poslednji ubačeni bit u posmatranom nizu.

$x_{n-1}r$ predstavlja *r*-ti bit niza prethodnog koraka a to je ujedno i treći bit iz ADC-a odnosno $x_{n-1}r = x3$.

$x_{n-1}s$ je poslednji bit niza prethodnog koraka kao i poslednji bit posmatranog niza a to je ujedno i drugi bit iz ADC-a odnosno $x_{n-1}s = x2$.

Izračunavanje ukupanog broja bita svakog niza vrši se primenom izraza:

$$y_n = 2^{n-1} + 1 \tag{5.1}$$

gde *n* predstavlja broj koraka sa mogućim vrednostima $n = 1,2,3, \dots, \infty$.

Za $n = 1$ dobija se $y_1 = 2^{1-1} + 1 = 2$, što znači da se primenom prvog koraka dobija bitski niz koji se sastoji iz dva člana a to su prva dva bita dobijena iz ADC-a. Posle drugog koraka dobija se 3 bita, posle trećeg 5, posle četvrtog 9 itd. kao što je prikazano u Tabela 5..

Broj koraka miksovanja miksera, na osovu poznatog broja bita niza koji treba izmešati, da bi se izvršilo mešanje svih bita izračunava se po formuli:

$$n = \log_2(y_n - 1) + 1 \tag{5.2}$$

Obrazac za određivanje ukupnog broja novih ubačenih bita svakog koraka (ne računajući prebačene bite dobijene prethodnim korakom) je:

$$m_n = 2^{n-2} \tag{5.3}$$

gde je n broj koraka.

Tako je broj ubačenih bita u drugom koraku $m_n = m_2 = 2^{2-2} = 1$, u trećem $m_3 = 2^{3-2} = 2$, u četvrtom $m_4 = 2^{4-2} = 4$, u petom $m_5 = 2^{5-2} = 8$, itd. kao u Tabela 5..

Prikazanom metodom miksovanja bita u koracima dobija se takav razmeštaj bita kojom se susedni dolazeći biti iz ADC-a, koji su u određenoj korelaciji, odvajaju jedan od drugog tako da se u novonastalom nizu slučajnih bita kao susedni pojavljuju biti koji su udaljeni jedni od drugih u smislu rasporeda koji su imali na ulazu u post-procesor.

Predstavljenim postupkom razmeštanja bita, rastojanje između susednih bita dolazećeg niza se primenom svakog sledećeg koraka mešanja sve više povećava.

Tabela 5.2. Ukupan broj bita u zavisnosti od broja koraka, broj novoubačenih bita u određenom koraku i stepen razdvajanja bita posle određenog koraka miksovanja

Broj koraka	Ukupan broj bita	Broj novoubačenih bita	Stepen razdvajanja bita
2	3	1	1
3	5	2	1
4	9	4	2
5	17	8	4
10	513	256	128
11	1025	512	256
20	524289	262144	131072
21	1048577	524288	262144
30	536870913	268435456	134217728
40	549755813889	274877906944	137438953472
50	562949953421313	281474976710656	140737488355328
100	1267650600228229401496703205377	316912650057057350374175801344	158456325028528675187087900672

Tako najmanje rastojanje (stepen razdvajanja bita) u rasporedu redosleda primljenih bita iz ADC-a, u novodobijenim nizovima sve do trećeg koraka miksovanja bita iznosi samo jedan. To je iz razloga rasporeda bita koji se dobija primenom trećeg koraka mešanja i koji je izgleda $x1, x4, x3, x5, x2$, sa najmanjim rastojanjem čija vrednost iznosi jedan. To znači da iako rastojanja između prvog i drugog bita u nizu $x1, x4$ (prvi i četvrti prihvaćeni biti iz ADC-a) i četvrtog i petog bita u nizu $x5, x2$ (peti i drugi prihvaćeni biti) iznose tri, najmanje rastojanje između redosledom prihvaćenih bita je jedan jer postoji par bita (drugi i treći bit odnosno $x4, x3$) čiji su se članovi kao četvrti i treći, znači uzastopno, pojavili na ulazu miksera.

Izgled rasporeda niza bita dobijen četvrtim korakom je $x1, x6, x4, x8, x3, x9, x5, x7, x2$ tako da je vrednost stepena razdvajanja dva, iz razloga pojavljivanja bita niza sa najmanjim rastojanjem u redosledu bita čiji je izvos dva ($x6, x4$ i $x5, x7$).

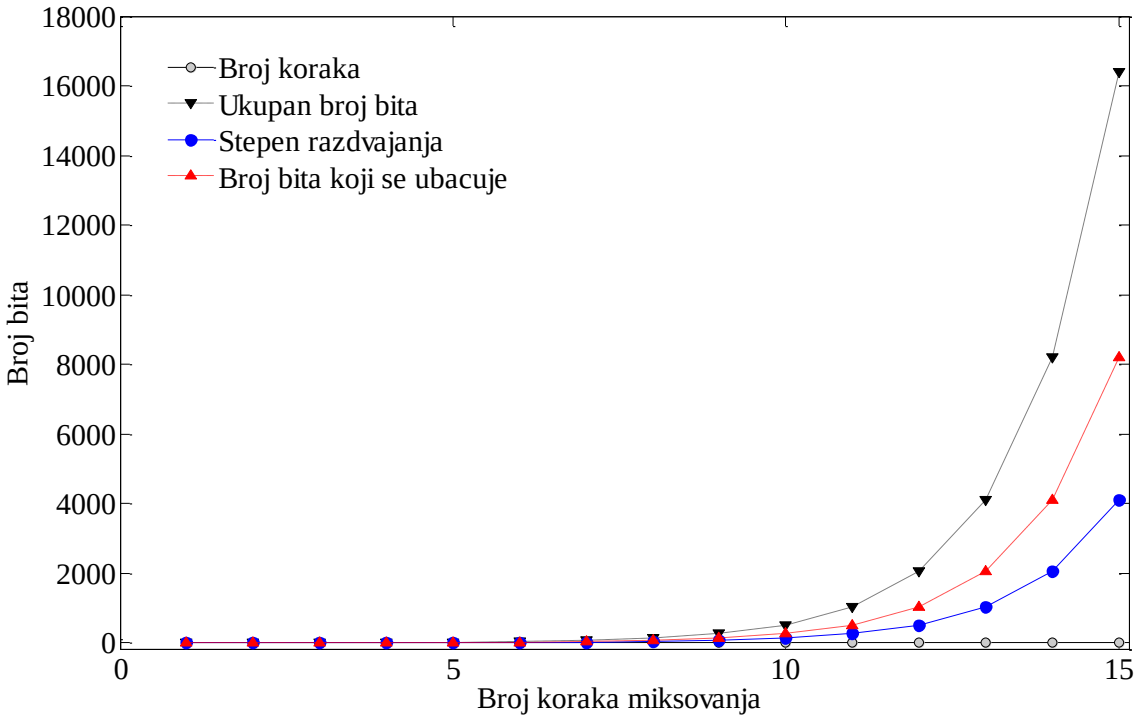
Ovo podrazumeva raspored bita, ovog novonastalog niza iz četvrtog koraka miksovanja, kod koga su susedni biti oni biti koji koje je kao svakog drugog prihvatio mikser iz ADC-a, u petom koraku su to svaki četvrti a, u na primer jedanaestom koraku su to svaki 256-ti.

Vrednosti stepena razdvajanja kod koji se dobijaju primenom prikazane metode mešanja bita dati su u Tabela 5..2 a grafički su prikazani na slici 5.5.

Matematički izraz, kojim se vrši izračunavanje stepena razdvajanja bita u nizovima sa slučajnim bitima koji se dobijaju ovim postupkom, nakon *n* primenjenih koraka mešanja je:

$$d_n = 2^{n-3} \tag{5.4}$$

gde n predstavlja broj koraka mešanja vrednosti $n = 3,4,5, \ldots, \infty$.



Slika 5.5. *Grafičko predstavljanje ukupnog broja bita, stepena razdvajanja bita i novoubačenog broja bita u zavisnosti od koraka miksovanja*

Konačni niz, čiji je raspored $p_1, p_2, p_3, \ldots p_n$ prikazan na slici 5.6 dobija se XOR-ovanjem susednih bita niza dobijenog na izlazu miksera. Funkcija XOR ima karakteristiku povećanja entropije nekorelisanih bita a povećanje dobiti XOR-ovanjem bita ogleda se i u redukovanju biasa. Pokazalo se da, čak i relativno gruba, tehnika zasnovana na operaciji XOR-ovanja može dati odlične rezultate. Slučajni izlazni bit strim lako se dobija propuštanjem statički nezavisnih ulaznih parova bita kroz logički XOR geit. U ovom slučaju se brzina protoka redukuje na pola bitske brzine ulaznog strima.

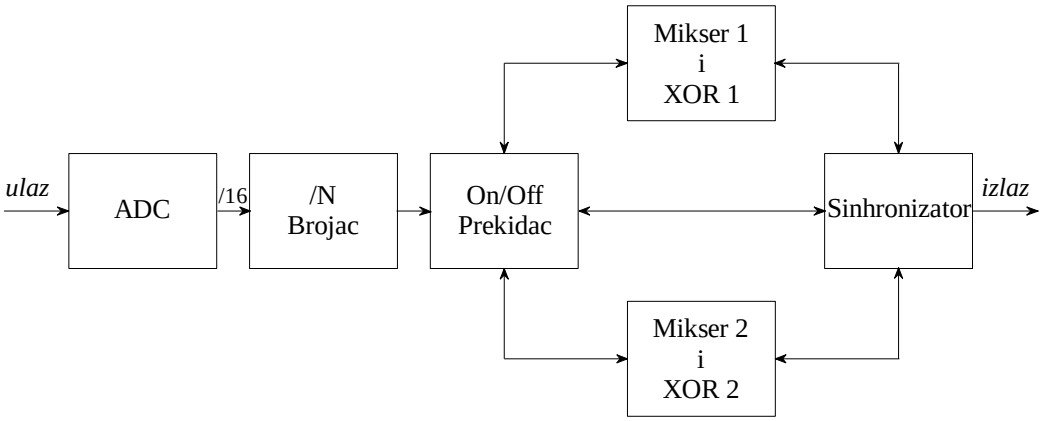
$$x1$$
$$x1x2$$
$$x1x\mathbf{3}x2$$
$$x1x\mathbf{4}x3x\mathbf{5}x2$$
$$x1x\mathbf{6}x4x\mathbf{8}x3x\mathbf{9}x5x\mathbf{7}x2$$
$$x1x\mathbf{10}x6x\mathbf{12}x4x\mathbf{14}x8x\mathbf{16}x3x\mathbf{17}x9x\mathbf{15}x5x\mathbf{13}x7x\mathbf{11}x2$$
$$x1x\mathbf{18}x10x\mathbf{20}x6x\mathbf{22}x12x\mathbf{24}x4x\mathbf{26}x14x\mathbf{28}x8x\mathbf{30}x16x\mathbf{32}x3x\mathbf{33}x17x\mathbf{31}x9x\mathbf{29}x15x\mathbf{27}x5x\mathbf{25}x13x\mathbf{23}x7x\mathbf{21}x11x\mathbf{19}x2$$
$$\vdots$$
$$\vdots$$
$$\vdots$$
$$x_{n-1}1, x_n\mathbf{1}, x_{n-1}2, x_n\mathbf{3}, \ldots, x_{n-1}r\text{-}1, x_n\boldsymbol{m}\text{-}\mathbf{1}, x_{n-1}r, x_n\boldsymbol{m}, x_{n-1}r{+}1, \ldots, x_n\mathbf{4}, x_{n-1}s\text{-}1, x_n\mathbf{2}, x_{n-1}s$$
$$\underbrace{x_{n-1}1 \oplus x_n 1}, \underbrace{x_{n-1}2 \oplus x_n 3}, \underbrace{x_{n-1}3 \oplus x_n 5}, \ldots, \underbrace{x_n 4 \oplus x_{n-1}s\text{-}1}, \underbrace{x_n 2 \oplus x_{n-1}s}$$
$$p_1 \quad , \quad p_2 \quad , \quad p_3 \quad , \ldots , \quad p_{n-1} \quad , \quad p_n$$

Slika 5.6. *Princip raspoređivanja bita i dobijanja izlaznog bitskog niza metodom MiBiS&XOR*

Ovakav način dobijanja slučajnih bita predstavlja primenu algoritma za postprocesiranje sa memorisanjem (eng. algorithmic postprocessing with memory). Iako daje dobre rezultate ovaj algoritam je dosta spor (npr. za ulazni broj bita 654896 vreme potrebno za miksovanje i XOR-ovanje svih bita iznosi 17 sekundi) i brzina mu se smanjuje sa povećanjem broja ulaznih bita. Međutim, kada se radi sa podacima odnosno informacijama od izuzetno velike važnosti i poverljivosti, za šifrovanje je neophodno korišćenje TRNG-a koji rade u realnom vremenu tj. primena algoritma za postprocesiranje bez memorisanja (eng. algorithmic postprocessing without memory).

Princip dobijanja istinski slučajnih bita u terminu realnog vremena, koristeći predstavljenu metodu, može se izvesti i ako se koriste samo po jedan mikser i XOR, međutim, takvim načinom mešanja i XOR-ovanja gubimo određenu količinu bita zbog potreba miksera da, posle određene količine skupljenih bita sa ulaza, prekine postupak prihvatanja ulaznih bita zbog sprovođenja postupka mešanja i XOR-vanja kao i nakon toga primanja novog bloka bita, za šta je potreban izvesni vremenski period. U tom periodu dolazi do nepovratnog gubljenja bita iz ADC-a. Ovaj problem je rešen upotrebom para nezavisnih miksera i XOR-a sa naizmeničnim radom – slika 5.7.

Primenom ovog rešenja prvo dolazni biti pune mikser1, količina ovih bita reguliše se podešavanjem brojača bita *N*, nakon čega se sinhronizatorom vrši isključivanje punjenja miksera1 i uključivanje punjenja miksera2. Završavanjem rada miksera1 svoj deo posla odrađuje XOR1 i vrši se slanje i punjenje izlaznog bafera dobijenim nizom. U međuvremenu je završeno punjenje miksera2, mikser1 preuzima punjenje i postupak se istim načinom nastavlja.



Slika 5.7. *Postupak stvaranja slučajnih nizova u realnom vremenu*

Sinhronizator ima zadatak ne samo da vrši kontrolu i automatsko uključivanje i isključivanje punjenja miksera već i da uskladi brzinu emitovanja bita iz kola za postprocesiranje sa brinom dolazećih bita iz ADC-a. Prikazanim načinom destilacije dolazi do redukovanja polovine ukupnog broja bita niza iz ADC-a i slanje bita novog niza prema izlazu brzinom koja je konstantna. Vreme mešanja i XOR-ovanja algoritma kod postupka bez memorisanja (2 miksera i 2 XOR-a) programskim jezikom C#, koristeći hardversku konfiguraciju: (Processor Intel (R) Pentium (R) CPU G2030@3.00GHz 3.00GHz; Instalirana memorija (RAM) 8.00 GB), kod koga je unapred određen broj bita u zavisnosti od izabranog broja koraka (jer se bitovi mešaju u blokovima), je vrlo kratko i iznosi na primer za blok veličine 1.048.577 bita 142 mili sekunde.

Algoritam programskog koda postprocesiranja jednog bloka bita metodom MiBiS&XOR:

Korak 1. Početna tačka aplikacije incijalizuje sve parametre i učitava audio fajl kao bajt niz. Pokreće se takođe i Štoperica.

Korak 2. Glavni program pravi bafer koji će sadržati miksovane bite na kraju operacije miksovanja. Dužina ovog bafera je definisana od strane korisnika.

Korak 3. Glavni program pravi odvojeni bafer koji sadrži šablon za bite. Ovaj bafer govori mikseru gde da postavi bite.

Korak 4. Glavni program poziva metod za računanje ukupnog broja koraka potrebnih za operaciju miksovanja. Ovaj metod koristi logaritamsku funkciju za to utvrđivanje.

Korak 5. Glavni program prolazi kroz svaki korak i izvršava operaciju miksovanja. Rezultati ovog metoda smeštaju se u bafer koji sadrži šablon za bite.

Korak 6. Algoritam za miksovanje pronalazi referentnu tačku koja je središna u trenutnom koraku miksovanja.

Korak 7. Algoritam za miksovanje popunjava šablon za bite levo od referentne tačke. Posle ovog koraka ceo bafer se ofsetuje na levo.

Korak 8. Algoritam za miksovanje pronalazi novu referentnu tačku na ofsetovanom baferu.

Korak 9. Algoritam za miksovanje popunjava šablon za bite desno od referentne tačke. Ceo bafer se ofsetuje na desno posle ovog koraka.

Korak 10. Glavni program poziva metod za postavljanje bita koji postavlja bite po izmiksovanom redosledu. Ovaj metod koristi bafer koji sadrži šablon za bite da bi odredio gde da postavi bite.

Korak 11. Glavni program poziva metod koji izvršava XOR operaciju nad miksovanim baferom.

Korak 12. Štoperica se zaustavlja i rezultati se ispisuju na konzoli.

Korak 13. Svi baferi se čiste a rezultat se smešta u bit niz.

Korak 14. Finalni bit niz se upisuje u fajl sa podacima.

Prikazanim načinom postprocesiranja proizvode se nizovi istinski slučajnih bita brzinom 352.8 Kb/s, što zadovoljava potreba aplikacija koje se koriste u mnogim oblastima.

Tabela prikazuje rezultate testiranja uzoraka zvuka buke u životnoj sredini, koji su uzeti na različitim lokacijama, posle primene destilacionog postupka MiBiS&XOR, dok su na slici 5.8 prikazani njihovi grafički izrazi.

Tabela 5.3. Rezultati ispitivanja različitih uzoraka zvučnog signala buke u životnoj sredini posle primenjenog postupka MiBiS&XOR

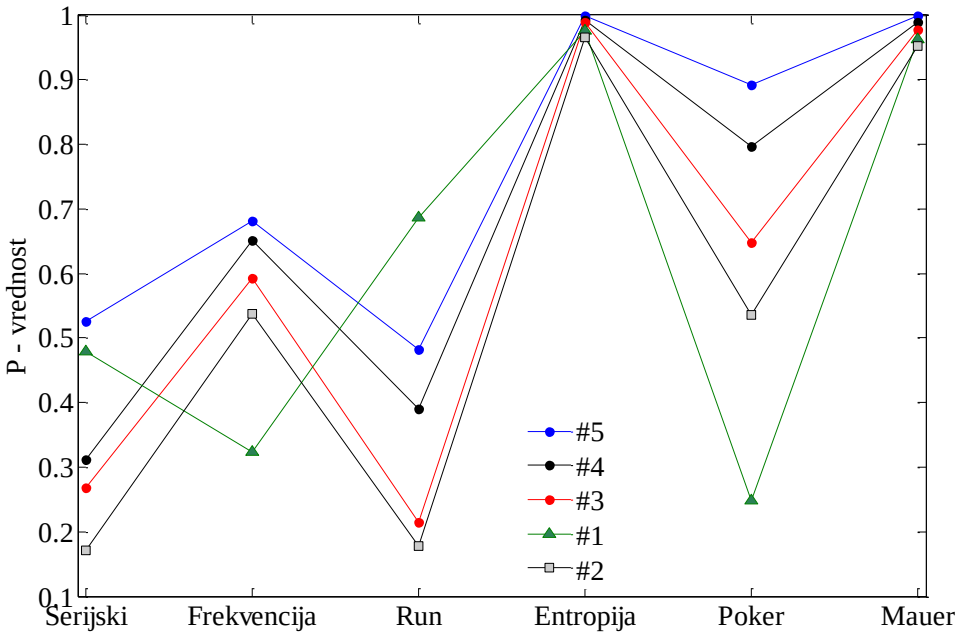
Uzorak	Statistički test					
	Serijski	Frekvencija	Run	Entropije	Poker	Mauer
#5	0.525	0.681	0.482	0.999	0.892	0.992
#4	0.311	0.651	0.390	0.993	0.797	0.989
#3	0.268	0.593	0.215	0.989	0.647	0.976
#1	0.478	0.323	0.686	0.976	0.249	0.961
#2	0.171	0.537	0.177	0.965	0.535	0.959

Iako je slučajnost nemoguće u potpunosti dokazati, nakon ispitivanja minimalno 1 Mbita elemenata niza korišćenih za svaki uzorak, dobijeni rezultati su prošli veliki broj NIST i FIPS statističkih testova slučajnosti (najbolje rezultate pokazali su korišćeni uzorci signala šuma miksovane buke životne sredine) a pored ostalih i sledeće testove:

- Test frekvencija (monobitski test)
- Test serija (dvo bitski test)

- Poker test
- Ran test
- Autokorelacioni test
- Test približne entropije
- Test najdužeg uzastopnog ponavljanja jedinica u bloku
- Test učestalosti u bloku
- Test preklapajucih uzoraka
- Test uzastopnog ponavljanja istog bita u nizu
- Test najdužih uzastopnih ponavljanja jedinica u bloku
- Test diskretne Furijeove transformacije
- Mauerov univerzalni test slučajnosti

Ovakav način miksovanja bita niza, odnosno uticaj na raspored bita dolaznog niza, dovodi do nastajanja takvog razmeštaja bita niza kojim je omogućeno odvajanje susednih bita, između kojih postoji određena korelacija, ubacivanje između njih velikog broja različito udaljenih bita koji nisu u korelaciji, i stvaranje idealnih uslova za XOR-ovanje bita dobijenog niza, koji su sada susedni biti, povećavajući na taj način vrednost entropije konačnog niza.



Slika 5.8. *Grafičko predstavljanje rezultata ispitivanja primenjenog MiBiS&XOR postupka korišćenjem buke miksovanog zvuka #5, zvuka sa žurke #4, zvuka iz podzemnog prolaza #3, zvuka iz prometne šetačke zone #1 i zvuka saobraćajne buke #2*

5.2. Upoređivanje rezultata sa poznatim metodama post-procesiranja

U Tabela 1.4 prikazani su rezultati testiranja slučajnog signala buke prirodne sredine (#5 – signal miksovane buke), dobijeni primenom različitih postprocesnih metoda a na slici 5.9 dat je njihov grafički prikaz. Primenjene metode su poznate i najčešće korišćene metode post-procesiranja i to: Nojmanov korektor (eng. Neumann's Corrector), Paritet niza (eng. Stream Parity), XOR-ovanje bita najmanje težina (LSB) i bita najveće težine (MSB) svakog desetog odmerka, i nova metoda MiBiS&XOR. Prethodno je u Tabela 4. za uporedne metode, dat pregled dobijanja izlaznih bita za različite moguće kombinacije ulaznih bita.

Tabela 1.4 Rezultati testiranja dobijeni primenom različitih metoda post-procesiranja korišćenjem slučajnog signala buke životne sredine (#5)

Statistički test	Metod post-procesiranja			
	Nojman	MiBiS&XOR	Paritet	XOR10
Serijski	0.513	0.525	0.082	0.541
Frekvencija	0.737	0.681	0.435	0.128
Run	0.189	0.482	0.078	0.101
Entropije	0.992	0.999	0.989	0.969
Poker	0.472	0.892	0.377	0.082
Mauer	0.983	0.992	0.957	0.932

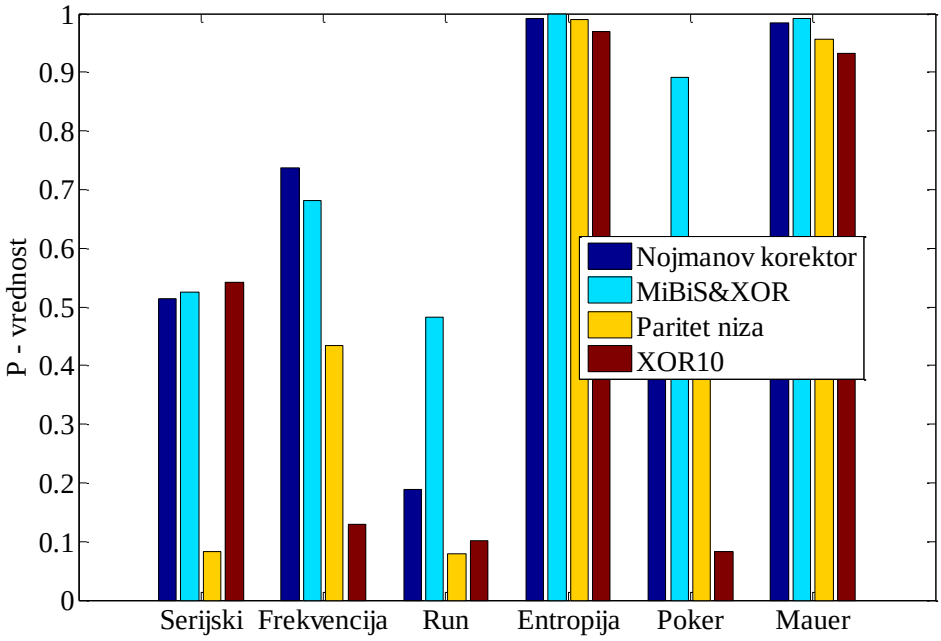
Kao što se iz rezultata testiranja vidi, potvrđuje se da se primenom svih četiri primenenjenih metoda dobijaju istinski slučajni biti. Rezultati koji se dobijaju novom metodom su očigledno odlični, posebno kada se razmatraju dva najvažnija statistička testa i to test približne entropije (eng. The Approximate Entropy Test) i Mauerov univerzalni statistički test (eng. Maurer's "Universal Statistical" Test).

Serijski test (eng. Serial Test) ima namenu da utvrdi da li je raspodela bigrama 00, 01, 10, 11 ravnomerna. S obzirom da se za $P \geq 0.01$ smatra da je sekvenca slučajna, testirani rezultati svih metoda prolaze ovaj test a najslabiji rezultati postižu se metodom Pariteta niza.

U fokusu frekvencijskog testa (eng. Frequency Test) je ispitivanje broja 1 i broja 0 u

dobijenom nizu bita odnosno njihova učestanost pojavljivanja. S obzirom da se za $P \geq 0.01$ smatra da je sekvenca slučajna testirani rezultati svih metoda prolaze ovaj test a najbolji rezultati dobijaju se primenom Nojmanovog korektora i metodom MiBiS&XOR.

Daleko najbolji rezultati Poker i Ran testa postižu se primenom metode MiBiS&XOR. Kod Poker testa se uzorci dužine 20.000 bita dele na 5.000 uzastopnih četvorobitnih segmenata nakon čega se vrši prebrojavanje pojavljivanja svake od mogućih 16 kombinacija 4-bitnih vrednosti.



Slika 5.9. *Grafički prikaz rezultata testiranja dobijenih različitim metodama*

Ran test inače ispituje odgovaranje broja uzastopnog ponavljanja 0 i 1 očekivanoj slučajnosti slučajnog niza. U svakom slučaju rezultati Poker i Run testa dobijeni svim metodama su bili dobri s obzirom da se već kada je $P \geq 0.01$ smatra da su sekvence slučajne.

Mauerovim testom ispituje se mogućnost komprimovanja niza bez gubitka informacije i ako se niz može značajnije komprimovati on se odbacuje kao neslučajan niz bita, prosto iz razloga efikasnije kompresije niza sa periodičnim svojstvima.

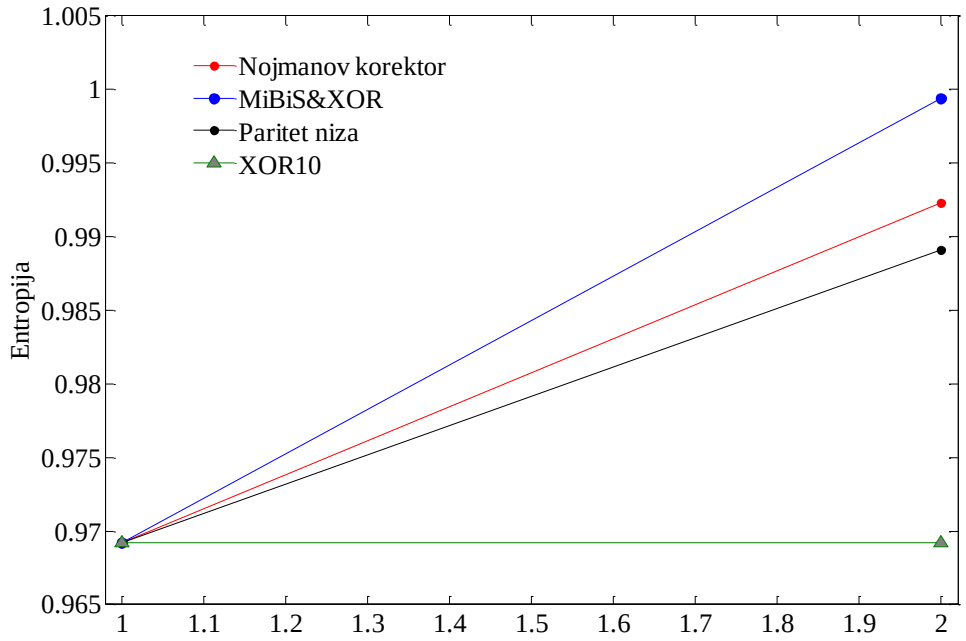
Rezultati Mauerovog testa očigledno pokazuju da su karakteristike niza dobijene svim metodama dobre a da su karakteristike niza dobijene Nojmanovim i metodom MiBiS&XOR najbolje. Međutim, vrednost entropije ipak predstavlja najvažniju karakteristiku svih generatora slučajnosti, to jest mogućnosti generisanja nizova istinski slučajnih brojevnih vrednosti, čime direktno utiče na određivanje kvaliteta TRNG-a.

Tabela 5.5. Autokorelacija i bias

Metod post-procesiranja	Autokorelacija ulaznog niza	Autokorelacija izlaznog niza	Bias
Nojmanov korektor	0.0032	0.0022	0.0005
Paritet niza	0.0032	0.0025	0.0004
XOR10	0.0032	0.0024	0.0021
MiBiS&XOR	0.0032	0.0019	0.0002

Na osnovu rezultata ispitivanja dolazi se do zaključka da je vrednost entropije dobijene predloženim postupkom MiBiS&XOR značajno veća nego kod vrednosti drugih uporednih metoda (slika 5.10).

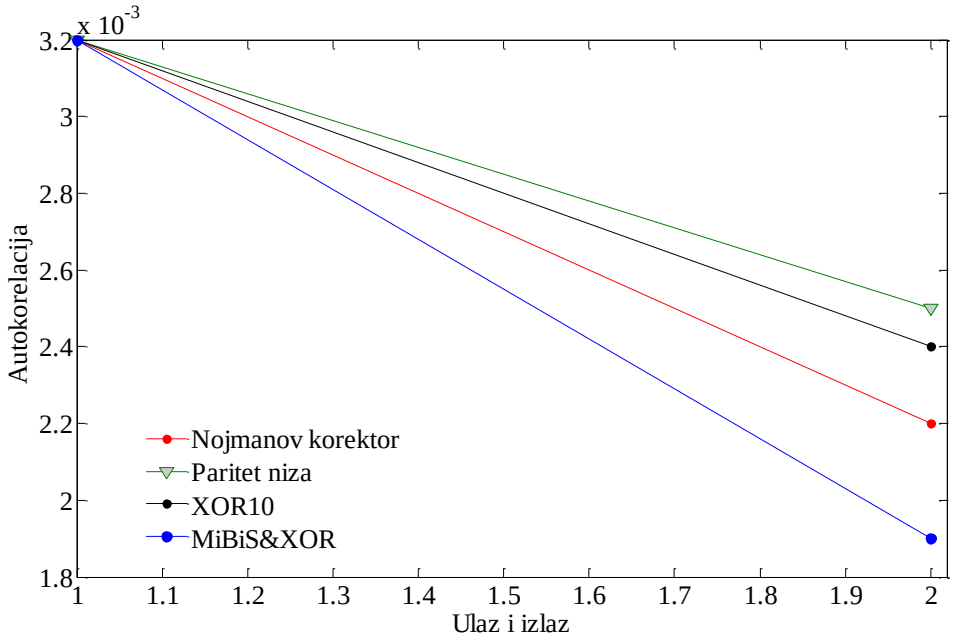
Od presudnog uticaja za dobijanje kvalitetnog niza, odnosno niza sa dobrom vrednošću entropije, su definitivno vrednosti autokorelacije i biasa. U Tabela 5.5. date su apsolutne srednje izmerene vrednosti autokorelacija na ulazu i izlazu post-procesora odnosno pre i posle post-procesiranja uporednim metodama, kao i vrednosti biasa posmatranog primera miksovanog signala buke životne sredine posle post-procesiranja uporednim metodama.



Slika 5.10. *Vrednosti entropije dobijene primenom različitih metoda u poređenju sa entropijom dobijenom metodom XOR10*

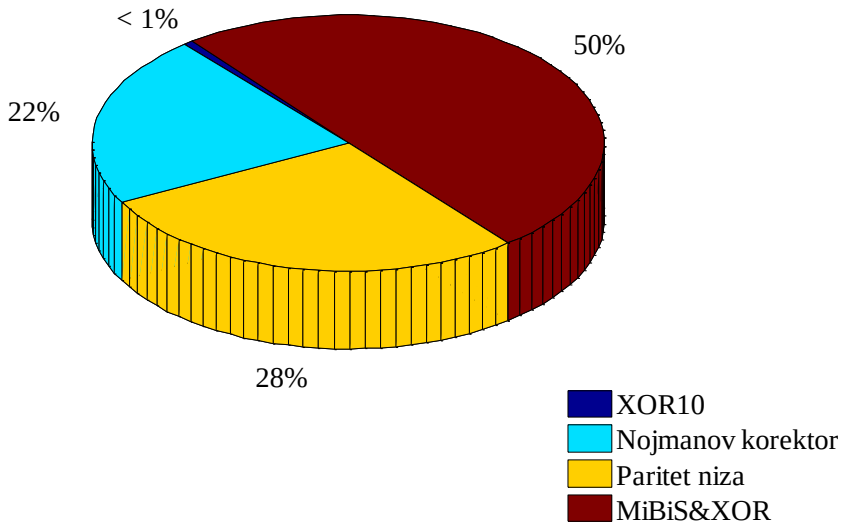
Kao što se sa slike 5.11 i tabele 5.5 može videti vrednost najmanje autokorelacije izlaznog niza dobijena je tehnikom MiBiS&XOR. S obzirom i na vrednost dobijenog biasa, čija vrednost je primenom ove metode takođe najmanja, apsolutno je jasan razlog zašto se primenom

ove metode dobija najveća vrednost entropije (slika 5.10).



Slika 5.11. *Grafičko predstavljanje apsolutnih srednjih vrednosti autokorelacija miksovanog signala buke pre i nakon post-procesiranja prikazanim postupcima*

Ako efikasnost generatora predstavimo procentom iskorišćenosti niza sa izlaza iz ADC-a, onda on metodom MiBiS&XOR iznosi 50%, što znači da je efikasnot ovakvih generatora najveća (Neumann-ov korektor oko 22%, Paritet niza oko 28%, XOR10 0.63%) – slika 5.12.



Slika 5.12. *Komparativna analiza iskorišćenja ulaznih bita*

Što se brzine proizvodnje, generisanja, odnosno stvaranja istinski slučajnih bita generatora tiče, ona kod predstavljene metode ima daleko najveću vrednost i iznosi 352.8 Kb/s. Upoređenja radi ona je kod Nojmanovog korektora 155 Kb/s, kod Pariteta niza 200 Kb/s a kod XOR10 4.41 Kb/s (za Nojmanovu i metodu Pariteta niza date vrednosti su približne) –tabela 5.6.

Tabela 5.6. Brzine proizvodnje bita TRNG-a korišćenjem različitih metoda destilacije

Metoda destilacije (post-obrade)	Brzina proizvodnje bita [Kb/s]
MiBiS&XOR	352.80
Neumann-ov korektor	155.00
Paritet niza	200.00
XOR10	4.41

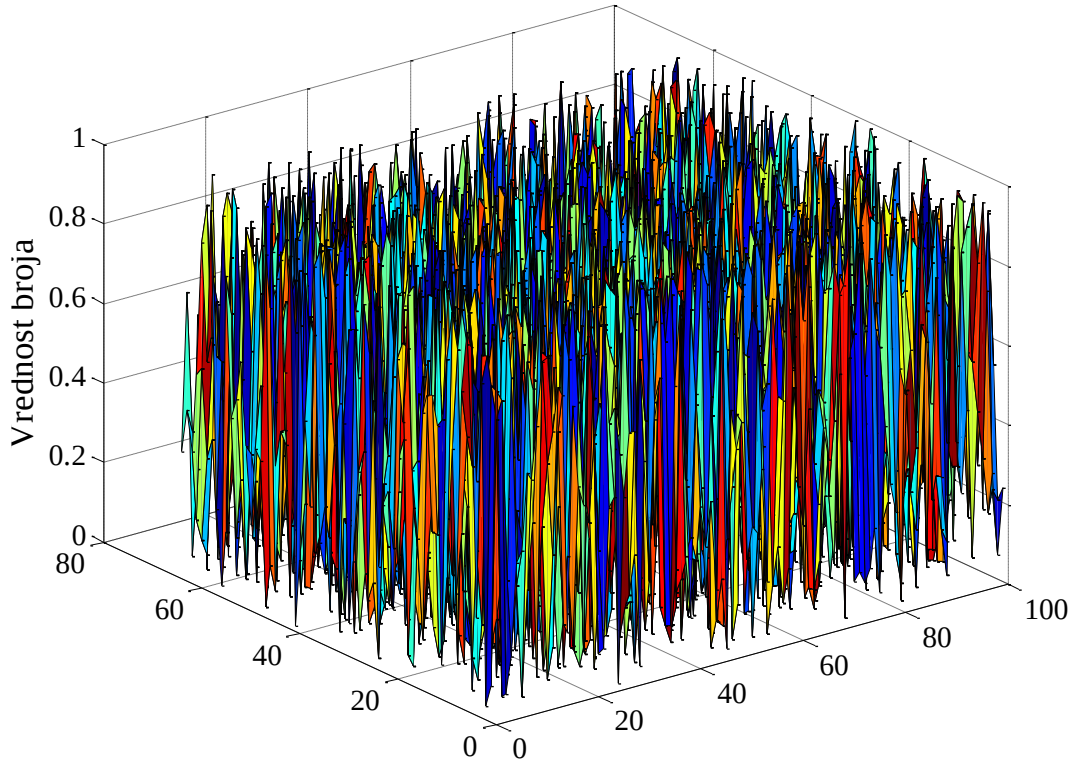
5.3. Diskusija dobijenih rezultata

Upoređujući rezultate dobijene statističkim testiranjima može se zaključiti da se novom, predloženom metodom MiBiS&XOR dobijaju odlični rezultati. Štaviše testiranja sa tendencijom sabotaža, forsiranja prostoperiodičnih fiksnih frekvencija na ulazu u mikrofon, nisu doprinela primetnom povećanju autokorelacije ili biasa. Proizvodnja bitske brzine vrednosti 352.8 Kbit/s, korišćenjem frekvencije odmeravanja 44.1 KHz, čini ovaj generator respektabilnim i primenljivim za veliki broj kriptografskih aplikacija. Prikaz primera niza, sa istinski slučajnim brojevima vrednosti od 0 do 1, dobijenim predstavljenom metodom dat je na slici 5.13.

U referenci za ovaj rad [9] objašnjene su dobiti koje se dobijaju XOR-ovanjem bita, pre svega one koje se odnose na popravljanje biasa i povećanja entropije. Međutim, kako se princip rada prikazan u [9] zasniva na XOR-ovanju MSB i LSB svakog desetog odmerka nemoguće je bilo smanjiti autokorelaciju između prvog i poslednjeg bita svakog odmerka (pre svega zbog visoke frekvencije odmeravanja – 44.100 odmeraka u sekundi) iako se autokorelacija između odmeraka smanjivala odbacivanjem određenog broja odmeraka. Predstavljenom metodom MiBiS&XOR se XOR-uju biti koji nisu u korelaciji, odnosno biti koji su se nalazili na ogromnom rastojanju u nizu bita iz ADC-a, čime se dobijaju mnogo bolje karakteristike slučajnosti i značajno unapređuje rad TRNG-a.

Ova metoda ima mnoge prednosti ali ima i manu. Nedostatkom se može smatrati to što je proces konstantnog generisanja bita moguće ostvariti tek nakon završetka prvog ciklusa miksovanja bita miksera1 i XOR-ovanja tog prvog izmešanog niza. Iz tog razloga uključivanje generatora ne podrazumeva i automatsko dobijanje konačnog izlaznog niza. U principu radi se o veoma kratkom vremenu kašnjenja koje je u prvom redu zavisno od dužine izabranog bloka niza a zatim od frekvencije taktnog generatora centralnog procesorskog modula računarskog sistema.

Nesumnjivo je ipak da predstavljeni generatori slučajnih nizova na bazi zvučne kartice generišu slučajne nizove sa elementima koji su nezavisni jedni od drugih, čime je ispunjen uslov statičke nezavisnosti, kao i to da je vrednost elemenata naredne sekvence nepredvidljiva, nezavisno od toga o kolikom se broju prethodno generisanih vrednosti radi.



Slika 5.13. *Prikaz uniformne raspodele slučajnih brojeva matrice [80x100] sa vrednostima u rasponu od 0 do 1*

6 ZAKLJUČAK

Predmet disertacije je nova klasa generatora slučajnih nizova zasnovana na zvučnoj kartici računara. Radi se o aktuelnoj temi dobijanja slučajnih brojeva koja je u fokusu velikog broja istraživača širom sveta. Do sada je razvijen veći broj pristupa i algoritama za rešavanje problema generisanja slučajnih brojeva koji su detaljno opisani u poglavlju 4. GENERATORI SLUČAJNIH NIZOVA ove disertacije. Glavni problem se ispoljava u kompromisu između između kvaliteta i brzine dobijanja rezultata. Iz navedenog razloga, u ovoj disertaciji razvijen je pristup zasnovan na zvučnoj kartici. Predloženi generatori slučajnih nizova su efikasni i odlikuju ih mogućnost obezbeđivanja visokog kvaliteta slučajnih brojeva kao i velika brzina generisanja, pa su kao takvi veoma pogodni za primenu u realnom vremenu. Performanse navedenih generatora verifikovane su testiranjem statističkim FIPS i NIST testovima slučajnosti i poređenjem sa rezutatima poznatih metoda post-procesiranja. Koristeći predloženi metod MiBiS&XOR, koji kao rezultat daje odličnu entropiju, svaki korisnik kućnog računara ima mogućnost generisanja kriptografski sigurnih slučajnih brojeva ne izlažući se bespotrebnim troškovima potrebnim za ugradnju ili korišćenje specijalnih hardverdskih komponenata.

Prednost predloženih generatora je da su nepredvidljivi, ne poseduju karakteristike periodičnosti, u finansijskom pogledu svakom dostupni i kao takvi, mada projektovani za potrebe kriptografskih aplikacija, odgovaraju zahtevima mnogih oblasti.

Naučno-stručni rezultati koji su obuhvaćeni ovom doktorskom disertacijom prezentovani su naučno-stručnoj javnosti saopštavanjem na međunarodnim i domaćim naučnim konferencijama i publikovanjem u međunarodnim naučnim časopisima.

Naučni doprinosi

Najznačajniji naučno-stručni doprinosi izloženi u okviru ove disertacije se mogu sistematizovati na sledeći način.

- Razvoj novog postupka za dobijanje slučajnih brojeva korišćenjem šuma buke životne sredine. Prikazan je efikasan način dobijanja slučajnih bita mešanjem bita ulaznog niza a zatim XOR-ovanjem susednih bita prethodno mešanjem dobijenog niza, čiji je raspored bita tako raspoređen da susedne bite čine oni koji su bili na velikim udaljenostima, nakon čega se kao rezultat dobija novi niz bita i povećava ukupna entropija bitskog niza.
- Razvoj nove klase generatora slučajnih brojeva sposobnih da u kratkom vremenskom roku obezbede značajnu količinu istinski slučajnih brojeva. Testiranja su pokazala da ova klasa generatora ima odlične karakteristike i da generiše istinski slučajne brojeva visokog kvaliteta slučajnosti.

- Razvoj novog postupka korišćenja zvučne kartice, koja je sastavni deo osnovnog hardverskog potencijala personalnog desktop računaraskog sistema i novih tipova laptopava, tablet PC-a ili smart telefonskih uređaja, koja se slučajnim analognim signalima buke u životnoj sredini pobuđuje koristeći mikrofon, u cilju dobijanja nizova istinski slučajnih brojeva koji ispunjavaju sve potrebne karakteristike slučajnosti.
- Razvoj novog modela post-procesiranja koji se sastoji iz dva paralelna miksera koji su konstruisani tako da istovremeno obavljaju sledeća dva scenarija:
    a) Punjenje bafera određenom količinom bita iz ADC-a zvučne kartice
    b) Obrada bita, metodom miksovanja u koracima a zatim XOR-ovanje susednih bita i slanje istinski slučajnog niza bita u izlazni bafer.
- Razvoj proceduralnog okruženja i sofverske osnove za dalji proces destilacije slučajnih brojeva kod generatora istinski slučajnih brojeva i za podršku razvoju i unapređenju generatora slučajnih nizova.

Pravci budućih istraživanja

Pravci budućih istraživanja u ovoj oblasti se mogu odnositi na:

- razvoj generatora istinski slučajnih nizova zasnovanih na zvučnoj kartici koji bi koristili predloženi metod post-procesiranja ali korišćenjem većeg broja miksera za mešanje bita, čime bi se maksimalno ubrzao rad generatora što može biti od presudne važnosti u mogim aplikacijama,
- istraživanje mogućnosti primene predložene metode MiBiS&XOR korišćenjem različitih izvora slučajnosti od atmosferskog šuma do kvantnih fenomena kao i različite kombinacije većeg broja izvora slučajnog signala. U ovom slučaju je neophodno razviti nove aplikacije koje bi za određene izvore slučajnosti postizale najveće moguće brzine uz zadržavanje odličnih karakteristika slučajnosti,
- razvoj nove metode post-procesiranja generatora slučajnih nizova zasnovanih na zvučnoj kartici koja bi istovremeno vršila mešanje dva ili više ulaznih slučajnih signala, čime bi bila povećana ulazna entropija a što bi za posledicu imalo povećanje entropije izlaznog slučajnog niza,
- razvoj novih modela generatora slučajnih brojeva zasnovanih na različitim delovima hardvera kućnog računara, od grafičke kartice do RAM memorije, koji bi za svoj rad koristili predloženi metod destilacije ili njegovu modifikovanu formu prilagođenu specifičnim karakteristikama određenog hardvera.

7 LITERATURA

[1] Menezes J, Vanstone A, Oorschot PV, *Handbook of applied cryptography*, Boca Raton, CRC Press, 1996.

[2] Xin Q, Zen X, et al, *Modeling and system simulation of truly random number generator*, Journal of System Simulation, 17(1), 53-56, 2005.

[3] Lotteries and Gaming Authority, *Remote gaming regulations*, Legal notice 176 of 2004, 110 of 2006, Malta, 2011.

[4] Kuriyama K et al., *A random parameter model with onsite sampling for recreation site choice: An Application to Southern California Shoreline Sportfishing*, Environmental and Resource Economics, 56(4): 481-497, 2013.

[5] Matsukawa Y et al., *Eye movement and random number in NP lupus evaluation*, Clinical Rheumatology, 27(2): 237-240, 2008.

[6] Maurer U, *Protocols for secret key agreement by public discussion based on common information*, Sci., Springer, vol 740, pp 461–470, 1993.

[7] Matsumoto M, Nishimura T, *Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator*, http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/emt.html.

[8] Gentle E, *Random number generation and Monte Carlo Methods*, 2nd edn. Springer, New York, 2004.

[9] Morrison R, *Design of a true random number generator using audio input*, Journal of Cryptology, 1(1), 1-4, 2001.

[10] Walker J, *HotBits: genuine random numbers, generated by radioactive decay*, 1996, https://www.fourmilab.ch/hotbits/.

[11] Tani M et al., *Photoconductive emission and detection of terahertz pulsed radiation using semiconductors and semiconductor devices*, Journ. of infrared, millimeter, and terahertz waves, 33(4): 393-404, 2012.

[12] Dollfus P et al., *Thermal noise in nanometric DG-MOSFET*, Journal of computational electronics, 5(4): 479-482, 2006.

[13] Stipcevic M & Rogina B, *Quantum Random Number Generator, ArXiv: quant-ph/0609043v2*, 2007, http://qrbg.irb.hr/0609043v2.pdf.

[14] Santoro R et al., *On-line monitoring of random number generators for embedded security*, Circuits and Systems, doi: 10.1109/ISCAS.2009.5118446, 2009.

[15] Golic DJ, *New methods for digital generation and post-processing of random data*, IEEE Trans. Comput, 55(10): 1217-1229, 2006.

[16] Nishioka M et al., *Design and analysis of fast provably secure public-key cryptosystems based on a modular squaring*, In: Information security and cryptology, LNCS (vol. 2288, pp.81–102), 2001.

[17] Barak B et al., *True random number generators secure in a changing environment*, In: Wolter C, Koc C, Paar C (eds), Cryptographic Hardware and Embedded Systems - CHES 2003, vol 2779, Springer, Cologne, pp 166-180.

[18] Bucci M, & Luzzi R, *Design of testable random bit generators*, In: Cryptographic Hardware and Embedded Systems, LNCS (vol. 3659, pp.147-156), 2005.

[19] Jun B & Kocher P, *The Intel random number generator*, 1999. www.cryptography.com/public/pdf/IntelRNG.pdf.

[20] Petrie C & Connelly J, *Modeling and simulation of oscillator-based random number generators*, IEEE International symposium on circuits and systems 4: pp. 324-327, 1996.

[21] Che W et al., *Scheme of truly random number generator application in RFID Tag*, 2007, http://www.autoidlabs.org/single-view/dir/article/6/231/page.html.

[22] Bucci M et al., *A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC*, IEEE Transactions on computers, 52(4), 403-409, 2003.

[23] Dichtl M, *How to predict the output of a hardware random number generator*, In: Workshop on Cryptographic Hardware and Embedded Systems, LNCS (vol. 2779, pp.181–188), 2003.

[24] Bucci M & Bagini V, *A design of reliable true random number generator for cryptographic applications*, Cryptographic Hardware and Embedded Systems, LNCS (vol. 1717, pp. 204-218), 1999.

[25] Molotkov NS, *Entropy uncertainty relations and stability of phase-temporal quantum cryptography with finite-length transmitted strings*, Journal of experimental and theoretical physics, 115(6): 969-985, 2012.

[26] Zhao QP, *Data acquisition and simulation of natural phenomena.* Science China Informat. Sciences, 54(4): 683-716, 2011.

[27] Russer P & Russer J, *Interference and Noise in Electromagnetics and Electromagnetic Compatibility*, ICEST 2011 Workshop, Faculty of Electronic Engineering, Niš, Serbia, 2011.

[28] Russer A., Asenov T and Russer P, *Sampling of Stochastic Electromagnetic fields*, IEEE MTT-S International microwave symposium digest, Montreal, pp 1-3, 2012.

[29] Mankad HS, Pradhan NS, *Application of software defined radio for noise reduction using empirical mode decomposition,* Advances in computer science, engineering & applications, 166(1):113-121, 2012.

[30] Mathews KC, Vasudeva Rao RP, *Radioactivity in monitoring materials processing,* Journal of radioanalytical and nuclear chemistry, 203(2):519-535, 1996.

[31] Jozwikowski K et al., *Numerical modeling of fluctuation phenomena in semiconductors and detailed noise study of mid-wave infrared HgCdTe-heterostructure devices,* Journal of electronic materials, 31(7):677-682, 2002.

[32] Pennetta C et al., *Excess thermal-noise in the electrical breakdown of random resistor networks, The European Physical Journal B - Condensed Matter and Complex Systems vol 12, Springer, Berlin, pp 61-65*, 1999.

[33] Gerhardt I et al., *Perfect eavesdropping on a quantum cryptography system,* ArXiv: 1011.0105v1, 18 March 2012.

[34] Stefanov A et al., *Optical quantum random number generator,* J. Mod. Opt. 47, 595–598, 2000.

[35] Schindler W, *Random Number generators for cryptographic applications*, In: Koc KC (ed.) Cryptographic engineering, Springer, Signals and Communication Theory, Berlin, pp 5-23, 2009.

[36] Roellgen B, *Visualisation of potential weakness of existing cipher engine implementations in commercial on-the-fly disk encryption software*, Global IP Telecommunications, Inc., 2008.

[37] Jun B & Kocher P, *The Intel random number generator*, Cryptography Research, 1999.

[38] Bucci M & Bagini V, *A design of reliable true random number generator for cryptographic applications*, CHES 1999, Lecture notes in computer science, vol 1717, Springer, Berlin, pp 204-218, 1999.

[39] Stipčević M, *Preventing detector blinding attack and other random number generator attacks on quantum cryptography by use of an explicit random number generator,* ArXiv: 1403.0143v3, 2014.

[40] Petrie S & Connelly A, *A noise-based IC random number generator for applications in cryptography,* IEEE Theor. Appl., 47(5): 615–621, 2000.

[41] Dichtl M & Golic D, *High-speed true random number generation with logic gates only,* in Cryptographic hardware and embedded systems, Springer, Berlin, pp.45–62, 2007.

[42] Lydersen L et al., *Secure gated detection scheme for quantum cryptography,* ArXiv: 1101.5698, 2011.

[43] Lacharme P, *Post processing functions for a biased physical random number generator,* in FSE, pp 334–342, 2008.

[44] Barak B et al., *True random number generators secure in a changing environment*, CHES, Springer, Berlin, pp 166–180, 2003.

[45] Sidorenko A & Schoenmakers B, *State recovery attacks on pseudorandom generators,* in Research in cryptology, Springer, Berlin, pp 53–63, 2005.

[46] Leland PR, *White noise in atmospheric optics, Acta Applicandae Mathematica, 35(1-2):103-130,* 1994.

[47] Lindroos M, Mc Elrath B, Orme C, Schwetz T, *Measuring neutrino mass with radioactivetions in a storage ring,* The European Physical Journal C, 64(4):549-560, 2009.

[48] Stipčević M & Rogina M, *Quantum random number generator based on photonic emission in semiconductors,* Rev. Sci. Instrum., vol 78, 1–7, 2007.

[49] Epstein M et al., *Design and implementation of a true random number generator based on digital circuit artifacts,* CHES 2003, vol 2779, Springer, Cologne, pp. 152-165, 2003.

[50] Evstaf'ev FF, *Instability of quartz crystal oscillator frequencies,* Measurement Techniques, 3(12):1042-1044, 1961.

[51] Dynes F et al., *A high speed, postprocessing free, quantum random number generator,* Applayd Physics. Letter 93, 031109, 2008.

[52] Ko K, Lee JW and Thomas T, *Towards generating secure keys for braid cryptography, Design.* Cod. and Cryptograph., 45(3): 317-333, 2007.

[53] *Parisi G & Rapuano F, Effects of the random number generator on computer simulations,* Physic. Letter B 157, 301–302, 1985.

[54] Viega J, *Practical random number generation in software,* ACSA, pp 129–140, 2003.

[55] Ferrenberg M et al., *Monte Carlo simulations: hidden errors from 'good' random number generators,* Physic. Letter 69, 3382–3384, 1992.

[56] Bennett H et al., *Experimental quantum cryptography,* Jour. of Cryptol. 5(1), 3–28, 1992.

[57] Qi B et al., *High speed quantum random number generation by measuring phase noise of single mode laser,* Op. Letter 35, 312–314, 2010.

[58] Boyar J, *Inferring sequences produced by a linear congruential generator missing low-order bits*, Jour. of Cryptol, 1(3): 177–184, 1989.

[59] Krawczyk H, *How to predict congruential generators*, Journal of Algorithms, 13(4):138-15, 1992.

[60] Ecuyer P & Simard R, *Test U01: A C library for empirical testing of random number generators*, ACM 33(4), Art. 22, 2007.

[61] Schindler W & Killmann W, *Evaluation criteria for true (physical) random number generators used in cryptographic applications*, CHES 2002, vol 2523, Springer, Heidelberg, pp 431–449, 2003.

[62] Schindler W & Killmann W, *AIS 31: Functionality classes and evaluation methodology for true (physical) random number generators*, version 3.1, BSI, Bonn, 2001.

[63] Lozi R, *Emergence of randomness from chaos*, Intern J Bifurcat Chaos 22(02): 1250021, 2012.

[64] *Figotin A et al.*, Random number generator based on the spontaneous alpha-decay, U.S.

[65] Proykova A, *How to improve a random number generator*, CPC 124, 125–131, 2000.

[66] Brederlow R et al, *A low-power true random number generator using random telegraph noise of single oxide-traps*, IEEE ISSCC, pp. 1666–1675, 2006.

[67] Che W et al., *A random number generator for application in RFID tag*, Springer, Berlin, pp 279–287, 2008.

[68] C.H. Vincent, *The generation of truly random binary numbers*, J. Phys. E: Sci. 3, 594–598, 1970.

[69] Beenakker J & Büttiker M, *Suppression of shot noise in metallic diffusive conductors*, PRB 46, 1889–1892, 1992.

[70] Abellán C et al, *Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode*, OE 22, 1645–1654, 2014.

[71] Bucci M et al., *A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC*, IEEE Trans. Com., 52(4): 403-409, 2003.

[72] Sunar B, *True random number generators for cryptography*, Cryptographic Engineering, Springer, pp. 55–73, 2009.

[73] Sunar B et al., *A provably secure true random number generator with built-in tolerance to active attacks*, IEEE Tran. Com. 56(1), 109–119, 2007.

[74] Uchida A et al., *Fast physical random bit generation with chaotic semiconductor lasers*, Natur. Phot. 2, 728–732, 2008.

[75] Knuth E, *High speed single photon detection in the near infrared*, The Art of Comp. Programm., vol. 2, Addison Wesley, 1997.

[76] Kinniment D & Chester E, *Design of an on-chip random number generator using metastability*, ESSCIRC, 4(6): 595–598, 2002.

[77] Institut Ruder Bošković, *QRBG 121, 2012*, http://qrbg.irb.hr.

[78] Reidler I et al., *Ultra high-speed random number generation based on a chaotic semiconductor laser*, PRL 103(2), 024102, 2009.

[79] Goldberg I & Wagner D, *Randomness in the Netscape browser*, Dobb's Journal, 2003.

[80] Grabher P et al., *Non-deterministic processors: FPGA-based analysis of area, performance and security*, In: Serpanos D, Wolf W (eds), ACM, Grenoble, pp 1-10, 2009.

[81] Guo H et al., *Truly random number generation based on measurement of phase noise of a laser*, PRE 81, 051137, 2010.

[82] Yang L & Wang X, *Design of pseudo-random bit generator based on chaotic maps*, Int. JMPB 26(32): 1250208, 2012.

[83] Yuan L et al., Shields, *High speed single photon detection in the near infrared*, APL 91, 041114, 2007.

[84] Li X et al., *Scalable parallel physical random number generator based on a superluminescent LED*, OL 36, 1020–1022, 2011.

[85] Wang X-& Qin X, *A new pseudo-random number generator based on CML and chaotic iteration*, ND 70(2): 1589–1592, 2012.

[86] Bagini V & Bucci M., *A design of reliable true random number generator for cryptographic applications*, CHES, Springer, Berlin, pp 204–218, 2002.

[87] Tkacik E, *A hardware random number generator, in Cryptographic*, CHES, Springer, Berlin, pp. 450–453, 2002.

[88] T. McNichol, *Totally random.* Wired 11(8), 2003, http://www.wired.com/wired/archive/11.08/random.html.

[89] Jennewein T et al., *A fast and compact quantum random number generator*, RSI 71, 1675–1680, 2000.

[90] Stipčević M, *Apparatus and method for generating true random bits based on time integration of an electronic noise source*, Pat. Numb. WO03040854, 2001.

[91] Stipčević M, *Fast nondeterministic random bit generator based on weakly correlated physical events*, RSI 75, 4442–4449, 2004.

[92] Stipčević M, *Quantum random bit generator*, Pat. Num. WO2005106645 (A2), 2004.

[93] Wahl M et al., *An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements.* APL 98, 171105, 2011.

[94] Wayne A et al., *Photon arrival time quantum random number generation.* JMO 56, 516–522, 2009.

[95] Kwon O, *Quantum random number generator using photon-number path entanglement.* AO 48, 1774–1778, 2009.

[96] Chevalier P et al., *Random number generator.* U.S. Pat. Num. 3,790,768, 1974.

[97] Narendra P et al., *A random bit generator using chaotic maps.* IJNS 10(1): 32–38, 2010.

[98] Wayne A & Kwiat G, *Low-bias high-speed quantum random number generator via shaped optical pulses.* OE 18, 9351–9357, 2010.

[99] Miszczak A, *Generating and using truly random quantum states in Mathematica*, ArXiv: 1102.4598v2, 2011.

[100] Kanter I et al., *An optical ultrafast random bit generator.* N. Phot. 4(1), 58–61, 2010.

[101] Vallone G et al., *Self-calibrating quantum random number generator based on the uncertainty principle*, ArXiv: 1401.7917, 2014.

[102] Peres Y, *Iterating von Neumann's procedure for extracting random bits*, AS 20, 590–597, 1992.

[103] Akaike H, *On optimum character of von Neumann's Monte Carlo model*, AISM, 7(1):183-193, 1956.

[104] Clarke Ryan, *Comparison of digital bit streams using modified parity.* US4530095 A, 1983.

[105] Davies B, *Exclusive OR (XOR) and Hardware Random Number Generators*, 2002, http://www.robertnz.net/pdf/xor2.pdf.

[106] Knuth DE, *Art of computer programming*, vol 2: Seminum. Algorithm, Inc., Boston, 1997.

[107] J. von Neumann, *Various techniques for use in connection with random digits*, Collections 5, 768–770, 1963.

[108] Ruhkin A et al., *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications.* NIST Spec. Publ. 800-22 rev1a, 2010.

[109] NIST *Security Requirements for Cryptographic Modules. FIPS PUB 140-1,* 1994.

[110] Ruhkin A, *Statistical testing of randomness: Old and new procedures*, World Scientific, Singapore, 2011.

[111] Zelinka I et al., *Do evolutionary algorithms indeed require random numbers*?, Advan. in intellig. Syst. and comp., vol 210, Springer, pp 61–75, 2013.

[112] Maurer M, *A universal statistical test for random bit generators.* Jour. of Cryp. 5(2), 89 – 105, 1992.

[113] Sprott C, *Chaos and time-series analysis*, Oxford University Press, NY, 2003.

[114] Easter J & French C, *Annex C: approved random number generators for FIPS PUB 140-2*, NIST, 2012.

[115] Persohn J & Povinelli J, *Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation.* CSF 45(3):238–245, 2012.

[116] Vattulainen I et al., *Physical tests for random numbers in simulations.* PRL 73, 2513–2516, 1994.

[117] http://www.itl.nist.gov/fipspubs/fip140-1.htm

[118] Marsaglia G, *DIEHARD Battery of Stringent Randomness Tests*, 1995, http://stat.fsu.edu/~geo/diehard.html.

[119] Blanchard P et al., *Markov chains or the game of structure and chance*, EPJCT, 184(1): 1-82, 2010.

[120] P. Jonsson, *Boom in Internet gambling ahead?* US policy reversal clears the way, http://tinyurl.com/86b9aaz, 26 December 2011

[121] Polulyakh NS, A. V. Sapiga VA, *Use of random numbers in computer simulation of magnetic resonance signals.* Technical Physics, 51(4):431-435, 2006.

[122] WIPL-D, *High Frequency Electromagnetic Modelling and Simulation Software*, www.wipl-d.com

[123] Click T et al., *Quality of random number generators significantly affects results of Monte Carlo simulations for organic and biological systems.* J. Com. Ch. 32, 513–524, 2011.

[124] Kim T et al., *Complete physical simulation of the entangling-probe attack on the Bennett-Brassard 1984 protocol.* PRA 75, 042327, 2007.

[125] Schmid F & Wilding B, *Errors in Monte Carlo simulations using shift register random number generators*. IJMP 6, 781–787, 1995.

[126] Zhao QP, *Data acquisition and simulation of natural phenomena.* Science China Informat. Sciences, 54(4): 683-716, 2011.

[127] W. Diffie, M.E. Hellman, *New directions in cryptography.* IEEE Trans. Inf. Theory 22, 644–654, 1976.

[128] F. Rodriguez-Henriquez, N.A. Saqib, A. Diaz-Perez, Ç.K. Koç, *Cryptographic Algorithms on Reconfigurable Hardware*, Springer, Berlin, 2007.

[129] D.J. Bernstein, J. Buchmann, E. Dahmen, *(eds.), Post-Quantum Cryptography*, Springer, Heidelberg, 2009.

[130] Diffie, W, *The national security establishment and the development of public-key cryptography.* Designs, Codes and Cryptography, 7(1-2), 9-12, 1996.

[131] C.H. Bennett, G. Brassard, *Quantum cryptography: public key distribution and coin tossing*, in Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, 10–12, pp. 175–179, Dec 1984.

[132] Allan W. Scott, *Understanding Microwaves*, John Wiley and Sons, 2005.

[133] E. Wolff, R. Kaul, *Microwave Engineering and System Applications*, John Wiley & Sons, Inc., 1988.

[134] C. A. Balanis, *Advanced Engineering Electromagnetics*, John Wiley & Sons, Inc., New York, 1989.

[135] M. Khader, W. Barnes, *Telecommunications Systems and Technology*, Prentice Hall, 2000.

[136] R. Collin, *Foundations for Microwave Engineering*, *Microwave Components, Devices and Active Circuits*, McGraw-Hill.Kogakusha, Great Britain, 1966.

[137] P. F. Combes, *Microwave Transmission for Telecommunications*, John Wiley and Sons, 1988.

[138] M. Golio, *The RF and Microwave Handbook*, CRC Press, 2001.

[139] J.Surutka, *Elektromagnetika*, Gradjevinska knjiga, Beograd, 1965.

[140] D. M. Pozar, *Microwave Engineering*, John Wiley & Sons, Inc, USA, 1998.

Prilog

Izvorni kod MiBiS&XOR algoritma u C# programskom jeziku

```
using System;
using System.Collections;
using System.Collections.Generic;
using System.Diagnostics;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.IO;
namespace BitMixerConsole
{
   class Program
   {
   private static BitArray _bitArrayInput = new BitArray(1048577);
      private static int _bitNumber = 1048577;
      private static List<int> _inputList = new List<int>(1048577);
      private static List<int> _stepList = new List<int>(1048577);
      private static List<int> _lastStepList = new List<int>();
      private static int _lastLeftMid;
      private static int _lastMidCalc;
      private static double _steps;
      public static List<bool> _allBytes;
      private static int _lastStepPointer;
      private static int _lastMiddlePointer;
      private static int _refMiddle;
      private static bool _hasToIncrease;
      private static Stopwatch _stopWatch;
      static void Main(string[] args)
      {
         _stopWatch = new Stopwatch();
         byte[] file = File.ReadAllBytes(@"C:\g9.wav");
         byte[] fileReal = new byte[(_bitNumber/8)+1];
         Array.Copy(file, fileReal, fileReal.Length);
         BitArray arr = new BitArray(fileReal);
         _bitArrayInput = new BitArray(arr);
        Console.WriteLine("Mixer input : " + _bitNumber + " bits");
         _bitNumber = arr.Length;
         _stopWatch.Start();
         for (int i = 1; i <= _bitNumber; i++)
         {
```

```
            _inputList.Add(i);
        }
        CalculateSteps();
        for (int i = 0; i <= _steps; i++)
        {
            DoStep(i);
        }
        PlaceBits(ref arr);
        XorBits(ref arr);
        _stopWatch.Stop();
        Console.WriteLine("Completed in : " + _stopWatch.Elapsed.Milliseconds + "
miliseconds");
        Console.ReadLine();
    }
    private static void PlaceBits(ref BitArray array)
    {
        for (int i = 0; i < _stepList.Count; i++)
        {
            array[i] = _bitArrayInput[_stepList[i] - 1];
        }
    }
    private static void XorBits(ref BitArray array)
    {
        BitArray newB = new BitArray((array.Length) / 2);
        BitArray newA = new BitArray((array.Length) / 2);
        BitArray finalArray = new BitArray(2);
        if (array.Length / 2 != (int)array.Length / 2)
            finalArray = new BitArray((array.Length / 2) + 1);
        else
            finalArray = new BitArray((array.Length / 2));
        List<bool> arrB = new List<bool>(newB.Length);
        List<bool> arrA = new List<bool>(newA.Length);
        for (int i = 0; i < newB.Length; i += 2)
        {
            if (i <= newB.Length)
            {
                arrB.Add(array[i]);
            }
        }
        for (int i = 1; i < newA.Length; i += 2)
        {
            if (i <= newA.Length)
```

```
        {
            arrA.Add(array[i]);
        }
    }
    newA = new BitArray(arrA.Count);
    newB = new BitArray(arrB.Count);
    for (int i = 0; i < arrA.Count; i++)
    {
        newB[i] = arrB[i];
        newA[i] = arrA[i];
    }
    finalArray = newB.Xor(newA);
    if (array.Length / 2 != (int)array.Length / 2)
    finalArray[finalArray.Length - 1] = array[array.Length - 1];
    array = finalArray;
}
private static void CalculateSteps()
{
    _steps = Math.Log(_bitNumber - 1, 2) + 1;
    if (_steps != (int)_steps)
    {
        _hasToIncrease = true;
        _steps++;
        _steps = (int)_steps;
    }
    Console.WriteLine("Total amount of steps : " + _steps);
}
private static void DoStep(int step)
{
    if (step < 4)
    {
        FillArray(5);
        _refMiddle = _inputList[2];
        _stepList[0] = _inputList[0];
        _stepList[1] = _inputList[3];
        _stepList[2] = _inputList[2];
        _stepList[3] = _inputList[4];
        _stepList[4] = _inputList[1];
        _lastStepList = _stepList;
        _lastLeftMid = _stepList[1];
        _lastStepPointer = 2;
        _lastMiddlePointer = 2;
```

```
}
if (step >= 4)
{
   if (!_hasToIncrease)
   {
      if (step >= 4)
      {
         int newBits = (int)Math.Pow(2, step - 2);
         int bitsInNew = _lastStepList.Count + newBits;
         int middle = (int)((bitsInNew / 2f));
         int splitSides = (int)(bitsInNew / 2f);
         FillArray(bitsInNew);
         _stepList[middle] = _refMiddle;
         _stepList[middle - 1] = _lastLeftMid * 2;
         _stepList[middle + 1] = _lastLeftMid * 2 + 1;
         _lastMidCalc = _lastLeftMid * 2;
         SortLeftSide(bitsInNew, middle);
         _lastStepPointer = _lastMiddlePointer;
   SortRightSide(bitsInNew, middle, _lastLeftMid * 2 + 1);
         _lastStepList = _stepList;
         _lastMiddlePointer = middle;
         _lastStepPointer = middle;
         _lastLeftMid = _lastLeftMid * 2;
         _lastMidCalc = _lastLeftMid * 2;
      }
   }
   else
   {
      if (step >= 4 && step != _steps)
      {
         int newBits = (int)Math.Pow(2, step - 2);
         int bitsInNew = _lastStepList.Count + newBits;
         int middle = (int)((bitsInNew / 2f));
         int splitSides = (int)(bitsInNew / 2f);
         FillArray(bitsInNew);
         _stepList[middle] = _refMiddle;
         _stepList[middle - 1] = _lastLeftMid * 2;
         _stepList[middle + 1] = _lastLeftMid * 2 + 1;
         _lastMidCalc = _lastLeftMid * 2;
         SortLeftSide(bitsInNew, middle);
         _lastStepPointer = _lastMiddlePointer;
   SortRightSide(bitsInNew, middle, _lastLeftMid * 2 + 1);
```

```
                _lastStepList = _stepList;
                _lastMiddlePointer = middle;
                _lastStepPointer = middle;
                _lastLeftMid = _lastLeftMid * 2;
                _lastMidCalc = _lastLeftMid * 2;
            }
            else
            {
                int newBits = (int)Math.Pow(2, (step - 1) - 1) + 1;
                int bitsInNew = _bitNumber - newBits;
                int totalBits = newBits + bitsInNew;
                int middle = (int)((totalBits / 2f));
                _stepList = _lastStepList;
                FillRemaining(bitsInNew, newBits);
            }
        }
    }
}
private static void SortLeftSide(int bitsInNew, int middle)
{
    for (int i = 1; i < (int)(bitsInNew / 2f); i++)
    {
        if (i / 2f == (int)(i / 2f))
        {
            _stepList[(middle - 1) - i] = _lastMidCalc - 2;
            _lastMidCalc = _lastMidCalc - 2;
        }
        else
        {
_stepList[(middle - 1) - i] = _lastStepList[_lastStepPointer - 1];
            _lastStepPointer--;
        }
    }
}
private static void SortRightSide(int bitsInNew, int middle, int rightOfMiddle)
{
    _lastMidCalc = rightOfMiddle;
    for (int i = 1; i < (int)(bitsInNew / 2f); i++)
    {
        if (i / 2f == (int)(i / 2f))
        {
            if ((_lastMidCalc - 2) < _bitNumber)
```

```
                {
                    _stepList[(middle + 1) + i] = _lastMidCalc - 2;
                    _lastMidCalc = _lastMidCalc - 2;
                }
                else
                    break;
            }
            else
            {
    _stepList[(middle + 1) + i] = _lastStepList[_lastStepPointer + 1];
                _lastStepPointer++;
            }
        }
    }
    private static void FillArray(int count)
    {
        _stepList = new List<int>(count);
        for (int i = 0; i < count; i++)
        {
            _stepList.Add(i);
        }
    }
    private static void FillRemaining(int remaining, int lastBit)
    {
        for (int i = 1; i <= remaining; i++)
        {
            int grabInt = _inputList[(lastBit + i) - 1];
            if (i / 2f == (int)(i / 2))
            {
                _stepList.Insert(_stepList.Count - i + 1, grabInt);
            }
            else
            {
                _stepList.Insert(i, grabInt);
            }
        }
    }
  }
}
```