Utjecaj entropije na točnost računa u impulsnom računalu

Batelić, Mateja

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:167082

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-09-02**

Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET
FIZIČKI ODSJEK

Mateja Batelić

UTJECAJ ENTROPIJE NA TOČNOST RAČUNA U IMPULSNOM RAČUNALU

Diplomski rad

Zagreb, 2022.

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET
FIZIČKI ODSJEK

INTEGRIRANI PREDDIPLOMSKI I DIPLOMSKI SVEUČILIŠNI STUDIJ
FIZIKA

Mateja Batelić

Diplomski rad

Utjecaj entropije na točnost računa u impulsnom računalu

Voditelj diplomskog rada: dr. sc. Mario Stipčević

Ocjena diplomskog rada: _____

Povjerenstvo: 1. _____

2. _____

3. _____

Datum polaganja: _____

Zagreb, 2022.

Zahvaljujem se mentoru dr. sc. Mariu Stipčeviću na mentorstvu i višegodišnjoj suradnji te pomoći, strpljenju i savjetima prilikom izrade ovog rada.
Posebno se želim od srca zahvaliti svojoj majci i svom zaručniku, bez čije potpore, ljubavi i vjere u mene cijelo ovo studijsko putovanje bilo bi neizmjerno teže. Njihova podrška i ohrabrivanja su mi predstavljala motivaciju da uspješno prebrodim sve prepreke. Stoga im posvećujem ovaj rad.
Na kraju, velika hvala mojim prijateljima na podršci i razumijevanju te svim kolegama na pomoći i zajedničkom učenju tijekom studija.

Sažetak

Impulsno neuronsko računanje predstavlja treću računalnu paradigmu zajedno sa digitalnim i kvantnim računalima, a zasniva se na biološki inspiriranom načinu procesuiranja informacija, odnosno na samim neuronima, živčanim stanicama živih bića. U ovom radu prezentirano je impulsno računanje sa svim dosad poznatim sklopovima za osnovne matematičke operacije – redom množenje, zbrajanje, dijeljenje i oduzimanje. Nadalje, objašnjene su različite formulacije entropije, pri čemu je stavljen naglasak na pojam entropijskog budžeta kao pouzdane motivacije za pronalaženje kvalitetnog determinističkog sklopa za zbrajanje i demonstraciju numeričke preciznosti u računima. U rezultatima su prezentirani poboljšani deterministički i nedeterministički sklopovi za zbrajanje, a pritom su provjeravani rezultati same operacije zbrajanja i vrijednosti relativne entropije. Povrh toga, proučavano je ponašanje najbolje ocjenjenih sklopova za zbrajanje u sklopu rješavanja kvadratne funkcije kombinirajući odabrane sklopove za zbrajanje sa sklopom za množenje, koji predstavlja najjednostavniji i najtočniji sklop u impulsnom računanju. Time je demonstrirana primjena sklopova u impulsnom računalu uz postizanje veće točnosti nakon provođenja matematičkih operacija kroz kombinaciju naizgled konceptualno jednostavnih sklopova.

Ključne riječi: impulsno računanje, entropijski budžet, relativna entropija

The influence of entropy on the accuracy of calculations in pulse computer

Abstract

Neuronal pulse computing represents third paradigm along with digital and quantum computing, being based on biologically-inspired way of processing information, i.e., on neurons, which are neural cells in the body of living beings. In this work, pulse computing is presented together with all known circuits so far, for basic mathematical operations – respectively multiplication, addition, division, and subtraction. Furthermore, different formulations of entropy are explained, whereby emphasis is being placed on the concept of entropy budget as an underlying motivation for finding a high-quality deterministic circuit for addition and for demonstration of numerical precisions in calculations. In the results section, we present improved deterministic and nondeterministic addition circuits. In particular, the results of the addition operation itself and relative entropy values were checked. On top of that, the behaviour of the best rated addition circuits was studied to solve quadratic function by combining the selected circuits with the multiplication circuit, which represents the simplest and the most accurate circuit in pulse computing. This demonstrated the application of circuits in pulse computing, together with achieving higher precision, after conducting mathematical operations through seemingly conceptually simple circuits.

Keywords: pulse computing, entropy budget, relative entropy

Sadržaj

1 Uvod ... 1
2 Teorijska pozadina ... 3
2.1 Entropija ... 4
2.1.1 Shannonova entropija ... 4
2.1.2 Kolmogorov-Sinai entropija ... 6
2.1.3 Relativna entropija ... 7
2.1.4 Kriterij entropijskog budžeta (EBC) ... 7
2.2 Binomni proces ... 8
2.3 Slučajni flip-flop (RFF) ... 9
3 Eksperimentalni postav i metoda ... 13
3.1 Generiranje niza slučajnih impulsa ... 14
3.1.1 Detektori fotona ... 14
3.1.2 Linear feedback shift register (LFSR) ... 15
3.1.3 Generiranje frekvencije slučajnog niza impulsa ... 16
3.2 DE0-Nano programabilna pločica s FPGA čipom ... 18
3.2.1 Struktura i funkcija FPGA čipa ... 18
3.2.1 Programiranje FPGA čipa ... 19
3.3 Kontrolna elektronička oprema ... 20
4 Matematičke operacije u impulsnom računanju ... 21
4.1 Sklop za množenje ... 21
4.2 Sklopovi za zbrajanje ... 22
4.2.1 Zbrajanje s logičkim OR vratima ... 22
4.2.2 Zbrajanje s MUX-om ... 23
4.3 Sklop za dijeljenje ... 24
4.4 Sklop za oduzimanje ... 25
5 Utjecaj entropije na primjeru zbrajanja ... 27
5.1 Analiza sklopova za zbrajanje ... 28
5.1.1 Sklop za zbrajanje s MUX-om ... 28
5.1.2 Deterministički sklop za zbrajanje s MUX-om ... 31
5.1.3 Ekvivalentna verzija determinističkog sklopa s MUX-om ... 33
5.1.4 Prvo determinističko poboljšanje ... 33
5.1.5 Drugo determinističko poboljšanje ... 35

5.1.6 Nedeterminističko poboljšanje 37
5.2 Primjena zbrajanja kod kvadratne funkcije 39
5.1.5 Deterministički sklop 40
5.1.6 Nedeterministički sklop 42
6 Diskusija i zaključak 45

Dodaci 46
A Eksponencijalna distribucija 46
B Boolova algebra 48
C Flip-flopovi 53
D Dokaz EBC-a za zbrajanje 55

Literatura 57

1. Uvod

Pojam entropije prvi je uveo njemački teorijski fizičar Rudolf Julius Emanuel Clausius 1865. godine [1]. Postoji nekoliko definicija entropije od kojih su najpoznatije termodinamička i statistička definicija, no ovaj rad bazira se na entropiji u teoriji informacija zvanoj Kolmogorov-Sinaj entropija, prema ruskim matematičarima Andreju Nikolajeviču Kolmogorovu i Jakovu Grigorjeviču Sinaju. U tom kontekstu, entropija informatičkog sustava uistinu odgovara entropiji realnog sustava, predstavljenog sa logičkim sklopovima, tj. Boolovom algebrom, koja je ujedno i temelj današnjih digitalnih računala. Osim digitalnih računala, danas poznajemo još dvije računalne paradigme – kvantno računanje i impulsno (neuronsko) računanje. Upravo je ova posljednja paradigma od interesa u ovom radu.

Impulsno računanje prvi je uveo John von Neumann 1956. godine [2]. Razlika impulsnog računanja u odnosu na ostale paradigme je što digitalno računalo kao najmanji tip podataka koristi bit, dok kvantno računalo koristi qubit. Kod impulsnog računanja je situacija drugačija i korišteni tip podatka je slučajan niz impulsa. U tom slučajnom nizu, impulsi se pojavljuju u slučajnim trenucima u vremenu zbog čega sliče živčanim impulsima živih bića. Jedini parametar slučajnog niza impulsa je stopa impulsa, točnije vjerojatnost, koja je realan broj u ovoj paradigmi. U ovom radu korištena je unipolarna reprezentacija jer kod te reprezentacije slučajni impulsi najsličnije prikazuju impulse u sinapsama živčanih stanica sisavaca. Preostale dvije reprezentacije su polarna i bipolarna reprezentacija.

Ova paradigma uvedena 1956. godine bila je popularna sve do 70-tih godina prošlog stoljeća, kada je preuzelo kvantno računanje. Ponovni interes se pojavio u drugom desetljeću ovog stoljeća [2-4]. Ovakva računalna paradigma naziva se i stohastičko računanje [5-7]. Danas, stohastičkim računanjem se rješavaju problemi koji su zahtjevni za digitalna računala u smislu vremena izvršavanja, količine hardvera ili utroška energije, a oni uključuju duboko učenje koje imitira rad ljudskog mozga, obradu fotografija (detekcija rubova ili smanjenje šuma) i slično.

Jedna od glavnih motivacija uvođenja ovakvog načina računanja je obrađivanje podataka u neprekidnom nizu[1], čime se postiže maksimalna brzina dobivanja rezultata bez prethodnog akumuliranja ulaznih podataka kao što je to slučaj kod digitalnih računala.

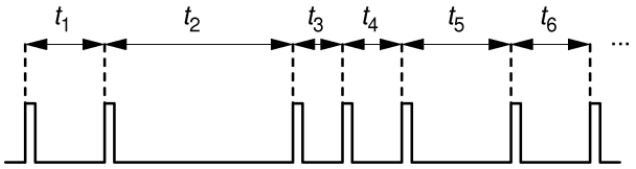
[1] Streamline computing (eng.)

Naravno, maksimalna brzina ovisi o maksimalnoj brzini hardware-a pa s poboljšanjem računala, dobivaju se sve precizniji rezultati bez potrebe za unapređivanjem same metode. Nadalje, zbog stohastičke prirode signala, glavni dio informacije dolazi prvi, a nakon njega slijede popravke, i to puno kasnije jer greška naglo opada s korijenom vremena brojenja izlaznih impulsa. Zbog toga je ovo još jedan dodatan i čvrst razlog zašto je RPC toliko efikasan i koristan.

U nastavku ovog rada opisani su koncepti entropije u poglavlju *Teorijska pozadina*, dok je u poglavlju *Eksperimentalni postav i metoda* detaljno prezentiran način provođenja eksperimenta uz uvođenje određenih eksperimentalnih pojmova. Nadalje, u poglavlju *Matematičke operacije u impulsnom* računanju opisani su dosad poznati sklopovi za osnovne računske operacije. Glavni dio rada je poglavlje *Utjecaj entropije na primjeru zbrajanja* u kojima su različiti sklopovi vrednovani na osnovu relativnih entropija, da bi u posljednjem poglavlju *Diskusija i zaključak* bili doneseni najvažniji zaključci sa primjerenim argumentima.

2. Teorijska pozadina

Impulsno neuronsko računanje koristi nizove slučajnih impulsa (RPT[2]), pri čemu je svaki impuls konstantne duljine trajanja i amplitude te obično kvadratnog oblika [8]. Primjer niza detekcija na vremenskoj osi prikazan je na Slici 1.1.



Slika 1.1: Niz slučajnih impulsa s različitim vremenima čekanja t_i, $i \in \mathbb{N}$, između dva susjedna događaja. Slika je preuzeta iz [8].

RPT je niz kvadratnih električnih impulsa konstantne širine i visine koji se pojavljuju slučajno u vremenu. Svaki impuls označava jedan Poissonov događaj koji nastaje kao posljedica kvantnog procesa prilikom emitiranja fotona iz LED[3] diode. Kvantni proces koji se pritom događa objašnjava se teorijom vezanja[4]. Unutar LED diode nalaze se dva sloja poluvodiča. Vodljivost poluvodiča može se povećati dopiranjem, čime se uspostavljaju p-tip i n-tip poluvodiča, ovisno o broju valentnih elektrona koje nečistoće sadrže. Nosioci naboja u p-spoju su šupljine, a u n-spoju elektroni. Zajedno čine p-n spoj kod kojeg se šupljine iz p-tipa miješaju sa elektronima iz n-tipa, čime nastaje područje osiromašenja. Naboj ne može prolaziti kroz područje osiromašenja osim ako je p-n spoj spojen na dovoljno veliku razliku potencijala te ako je p-tip spojen na pozitivni kraj baterije, a n-tip na negativni. Suprotno spajanje polova baterije ne bi moglo omogućiti prolazak naboja kroz područje osiromašenja, tj. struju. Upravo to čini definiciju LED diode. Prilikom sparivanja elektrona iz vodljive vrpce sa šupljinama iz valentne vrpce dolazi do emitiranja fotona. Jedan par elektron-šupljina proizvodi točno jedan foton. Time se dobiva slučajnost potrebna za daljnju izvedbu eksperimenta, a emitiranje i detekcija fotona u vremenu opisuje eksponencijalnu distribuciju, čiji izvod je detaljnije razrađen u Dodatku A. Točnije, kvantni efekt koji se događa prilikom detekcije fotona je fotoelektrični efekt u kojem svjetlost konstantnog

[2] Random Pulse Train (eng.)

[3] Light Emmiting Diode (eng.)

[4] Band theory (eng.)

makroskopskog intenziteta upada na SPAD[5] diodu, što je detaljnije opisano u poglavlju *Eksperimentalni postav*. Ovakav način dobivanja signala iz slučajnog izvora izabran je zbog toga što eksponencijalna distribucija ima maksimalnu entropiju, što je glavna tema ovog rada.

Impulsno neuronsko računalo koristi povezane osnovne sklopove Boolove algebre (AND, OR, NOT, …). S obzirom da je cilj da impulsi budu konstantne visine i širine, a signali na izlazu iz detektora su nejednolikog trajanja, ovaj problem je riješen diskretizacijom vremena. Točnije, vremensku os podijelimo na jednake intervale trajanja $\Delta t = 1\ \mu s$, kao što je prikazano na Slici 1b. U slučaju kada se impuls pojavi u jednom intervalu, tada tom intervalu pridijelimo logičku jedinicu. U suprotnom slučaju kada u danom intervalu nema signala, pridjeljujemo logičku nulu. Time dobivamo niz logičkih jedinica i nula koji predstavljaju ulazne vrijednosti za dane operacije Boolove algebre. Zbog toga je niz slučajnih impulsa karakteriziran s konstantnom vjerojatnosti p, koja označava vjerojatnost pojavljivanja impulsa $p \in [0,1]$ u sljedećem kratkom vremenskom intervalu. Detaljniji opis nastanka RPT-a opisan je u poglavlju *Eksperimentalni postav*. Diskretizacija vremenske osi omogućava da su impulsi uredno poredani u vremenu, čime se dobiva sličnost s električnim impulsima sisavaca, prikazanim na Slici 1c.

2.1 Entropija

2.1.1 Shannonova entropija

S obzirom da je vjerojatnost pojavljivanja impulsa u danom vremenskom intervalu upravo jednaka aritmetičkoj sredini

$$p = \frac{1}{N}\sum_{i=0}^{N-1} x_i, \tag{2.1}$$

Možemo definirati Shannonovu entropiju kao

$$H_1(x) = -p(x)\log_2 p(x) - \big(1-p(x)\big)\log_2\big(1-p(x)\big). \tag{2.2}$$

[5] Signle-Photon Avalanche Diode

Shannonova entropija odnosi se na nizove duljine 1, dakle pojedinačne bitove u našem slučaju pa zbog toga oznaka H ima uza sebe indeks 1. Entropija nam govori o tome koliko je promatrani niz slučajan. Što je entropija veća, to je niz slučajniji. Izraz za Shannonovu entropiju zapravo zbraja dva člana koji redom predstavljaju vjerojatnost da se pojavi logička jedinica $-p(x)\log_2 p(x)$ i vjerojatnost da se pojavi logička nula $\big(1-p(x)\big)\log_2\big(1-p(x)\big)$. Baza 2 odnosi se na broj različitih bitova, što je upravo 0 i 1 kao jedine dvije logičke mogućnosti.

S obzirom da postoji Shannonova entropija definirana za nizove duljine 1, također postoji i generalizirana Shannonova entropija za nizove duljine $n > 1$, koji se nazivaju n-grami:

$$H_n(x) = -\sum_{i=0}^{2^n-1} p_i \log_2 p_i\,, \tag{2.3}$$

gdje je p_i vjerojatnost pojavljivanja i-tog od 2^n mogućih n-grama koja počinje na poziciji bilo kojeg bita u RPT-u. Interpretacija ove relacije je da nam govori koliko je informacije sadržano u jednom n-gramu, odnosno relacija predstavlja količinu informacije koja je potrebna da bismo predvidjeli vjerojatnost pojavljivanja podniza duljine n. Prednost generalizirane Shannonove entropije je u tome što nizovi poput '101010101010…' računani pomoću relacije (2.2) imaju maksimalnu entropiju $H_1 = 1$, jer je vjerojatnost pojavljivanja nule i jedinice jednaka i iznosi $p(x) = 1/2$, a jasno je vidljivo da takav niz uopće nije slučajan. No, računajući H_2 prema relaciji (2.3), također je dobivena vrijednost entropije $H_2 = 1$, jer se ovdje radi o entropiji niza duljine dva, što se smatra jednim simbolom. S obzirom da kombinacija dva bita daje četiri kombinacije (00, 01, 10 i 11), u promatranom nizu zastupljene su samo dvije, a to su 01 i 10 jer n-gram može početi na bilo kojem mjestu u nizu. Stoga je njihova vjerojatnost jednaka 0.5, a preostale dvije kombinacije (00 i 11) se u promatranom nizu uopće ne pojavljuju pa je njihova vjerojatnost nula. Tako je dobivena entropija $H_2 = 1$. No, ono što je nama u ovom radu bitno je Shannonova entropija po bitu, koja se računa dijeljenjem relacije (2.3) sa brojem promatranih bitova n. Time se dobiva da Shannonova entropija po bitu iznosi $H_2 = 1/2$ po bitu, iz čega vidimo da niz nije potpuno slučajan. Zbog toga je relacija (2.3) relevantnija za procjenu slučajnosti niza jer obuhvaća nizove dulje od jedan i time nam daje uvid u moguće ponavljajuće uzorke [9].

2.1.2 Kolmogorov-Sinai entropija

Ono što je u ovom radu od interesa nije Shannonova entropija već Kolmogorov-Sinai (KS) entropija [9], koja je definirana kao

$$h(x) = \lim_{n\to\infty} h_n(x), \tag{2.4}$$

gdje je $h_n(x) = H_n(x) - H_{n-1}(x)$ za $n \geq 2$ i $h_1(x) \equiv H_1(x)$. Pritom se također pretpostavlja da broj bitova niza ide u beskonačnost pa zbog toga i smijemo promatrati limes. U suprotnom, limes ne bi imao smisla za n-grame dulje od ukupne duljine niza. Zbog toga entropija $h(x)$ predstavlja prosječnu količinu informacije potrebnu da se predvidi sljedeći bit [10]. Nadalje, $h_n(x)$ je monotono padajući niz zato što je $H_n(x)$ monotono padajući niz koji s vremenom pada sve sporije. Razlog sve sporijem padu je zato, što je vjerojatnost pronalaska n-grama u podnizu duljine n sve manja, točnije, vjerojatnost da ćemo predvidjeti n-ti bit ako znamo prethondih $n-1$ bitova je sve manja. Drugim riječima, informacije koje imamo o prethodna npr. tri bita da bismo mogli pretpostaviti vjerojatnost pojavljivanja četvrtog ne može biti manja od informacija koje bismo imali sa pojavljena četiri bita da bismo mogli pretpostaviti vjerojatnost pojavljivanja petog. S obzirom da je $h_n(x)$ monotono padajući niz za koji vrijedi $h_{n+1}(x) \leq h_n(x)$, slijedi da $h(x)$ možemo također zapisati i kao aritmetičku sredinu svih $h_n(x)$ u limesu kada $n \to \infty$, pa vrijedi

$$h(x) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n} h_i(x). \tag{2.5}$$

Sumiranjem svih $h_i(x)$ dobivamo da se svi $H_n(x)$ poništе osim $H_n(x)$ i H_0, pri čemu je $H_0 = 0$, iz čega slijedi:

$$h(x) = \lim_{n\to\infty} \frac{H_n(x)}{n}. \tag{2.6}$$

Ovaj izraz nam govori da je KS entropija jednaka normaliziranoj Shannonovoj entropiji u limesu velikih n-grama [9].

2.1.3 Relativna entropija

Sada, možemo definirati relativnu KS entropiju[6], koja nam govori koliko je velika entropija slučajnog niza u odnosu na maksimalnu entropiju koju niz može poprimiti za danu vjerojatnost [9], a definirana je kao:

$$h_{rel}(x) = \frac{h(x)}{h_1(x)}. \tag{2.7}$$

U stvarnost, slučajan niz impulsa ne mora nužno imati maksimalnu entropiju za danu vjerojatnost, a razlog tomu su autokorelacije koje nastaju prilikom izvršavanja Boolove algebre pa je onda ovo dobra mjera za ocjenu slučajnosti izlaznog niza i ispravnosti rada određenog sklopa. Vrijednost ovog izraza nalazi se unutar intervala [0,1], gdje $h_{rel} = 1$ označava impulse generirane binomnim procesom, koji je detaljno opisan u sljedećem potpoglavlju *Binomni proces*, pa slijedi da je $h(x) = h_1(x)$, pri čemu je $h_1(x) = H_1(x) - H_0(x) = H_1(x)$ jer je $H_0(x) = 0$. stoga se za binomni proces KS entropija svodi upravo na Shannonovu entropiju. S druge strane, $h_{rel}(x) = 0$ označava da je proces generacije bitova na izlazu iz pojedinog sklopa deterministički, odnosno vjerojatnost pojavljivanja bitova je unaprijed predodređena.

2.1.4 Kriterij entropijskog budžeta

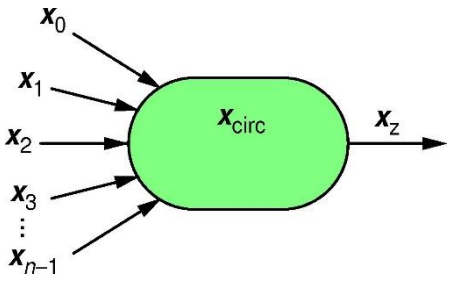
Kriterij entropijskog budžeta [9] tvrdi da entropija svih ulaznih nizova i unutarnja entropija sklopa mora biti veća ili jednaka entropiji izlaznog RPT-a:

$$\mathcal{H}(p(\boldsymbol{x}_z)) \leq h(\boldsymbol{x}_{\text{circ}}) + \sum_{i=0}^{n-1} h(\boldsymbol{x}_i), \tag{2.8}$$

gdje je $\boldsymbol{x}_z$ izlazni niz, $\boldsymbol{x}_{\text{circ}}$[7] unutarnji izvor entropije, a $\boldsymbol{x}_i, i = 0, n-1$ su ulazni nizovi, kao što je prikazano na Slici 2.1, preuzetoj iz [9].

[6] Postoji i drugo značenje pojma relativna entropija, koji se odnosi na Kulback-Leiberovu entropiju. Ona mjeri kolika je entropija jednog niza ako je drugi niz poznat. U slučaju kada su dva niza potpuno jednaka, tada je relativna entropija ta dva niza nula jer drugi niz ne sadrži nove informacije i nema nikakve nove neodređenosti.

[7] Circuit (eng. Sklop)



Slika 2.1: Mogući izvori entropije RPC sklopa dostupni za generiranje izlaznog RPT niza $\boldsymbol{x}_z$ su ulazni nizovi $\boldsymbol{x}_0, \dots, \boldsymbol{x}_{n-1}$ i unutarnji izvor entropije $\boldsymbol{x}_{\mathrm{circ}}$. Slika je preuzeta iz [9].

Unutarnji izvor entropije je u našem slučaju slučajni flip-flop jer on koristi dodatni RPT za generiranje vjerojatnosti impulsa na svome izlazu.

S obzirom na unutarnji izvor entropije samog sklopa, sklopove dijelimo na determinističke i nedeterminističke. Deterministički sklopovi su sklopovi koji ne sadrže dodatan izvor entropije osim entropije ulaznih nizova pa je tada $h(\boldsymbol{x}_{\mathrm{circ}}) = 0$. Suprotno, nedeterministički sklopovi sadrže dodatne izvore entropije pa za njih vrijedi nejednakost (2.8).

2.2 Binomni proces

S obzirom da je intenzitet iluminacije detektora konstantan, proces generiranja detekcija je stacionaran te, posljedično, vremena između susjednih impulsa slijede eksponencijalnu distribuciju [9]. Eksponencijalna distribucija je izabrana zbog maksimalne entropije koju sadrži, a detaljni izvod koji potvrđuje da se doista radi o eksponencijalnoj distribuciji prikazan je u Dodatku A. Iako je sama detekcija fotona Poissonov proces, slučajni impulsi nastaju binomnim procesom. Naime, nakon detekcije fotona, električni signali ulaze u sklop koji radi na principu bacanja novčića, a naziva se DRFS[8] (detaljni opis u poglavlju *Eksperimentalni postav*). Po izlazu iz DRFS-a dobivamo impuls s točno određeno postavljenom vjerojatnosti pojavljivanja impulsa u danom vremenskom intervalu. Time binomni proces postaje temeljni proces za ovaj eksperiment. Ovakav proces detekcije fotona te proizvodnje električnog signala je analogan primjeru s bacanjem novčića. Svaki

[8] Digital random frequency synthesis

put kad bacimo novčić dobivamo pismo ili glavu. U ovom eksperimentu se događa isto. Unutar svakog vremenskog intervala imamo mogućnost ili detektirati foton ili ne.

Prednost binomne raspodjele u odnosu na eksponencijalnu je u izvedbenoj realizaciji koja omogućava pojavu impulsa točno na početku vremenskog intervala pa ne dolazi do nezgodnih slučajeva u kojima jedan impuls počinje u jednom vremenskom intervalu, a završava u sljedećem. Laički rečeno, ili se impuls nalazi u danom vremenskom intervalu ili ne, a međuslučajeva nema. Time se postiže jednako trajanje svih proizvedenih impulsa i omogućava jednaki razmak između uzastopnih signala, što je bitno prilikom obrade i izvršavanja eksperimenta.

2.3 Slučajni flip-flop (RFF)

Posljednja kockica za razumijevanje teorijske pozadine je slučajni flip-flop (RFF) kao dodatni izvor slučajnosti. No, prije opisa rada samog RFF-a, krenimo od početka. RFF se kao i ostali sklopovi baziraju na Boolovoj logici, čije osnovne ideje i sklopovi (AND, OR, NOT,…) su opisane u Dodatku B radi potpunosti te kao podsjetnik čitatelju. Ti osnovni sklopovi Boolove logike predstavljaju gradivne elemente za RFF, kao i za sve ostale sklopove prikazane u ovom radu.

Slučajni flip-flop je nastao iz običnog flip-flopa. Razlikujemo četiri osnovne vrste flip-flopa, a to su SR flip-flop, JK flip-flop,, T[9] flip-flop (TFF) i D[10] flip-flop (DFF) [11]. Ovdje ćemo opisati TFF i DFF jer su na njegovim principima razvijeni T slučajni flip-flop (TRFF[11]) i D slučajni flip-flop (DRFF)[12], dok su ostale vrste flip-flopa objašnjenje u *Dodatku C*.

TFF je prikazan na Slici 2.2.a, a pripadni simbol na Slici 2.2.b. Rad TFF-a se bazira na taktnom signalu (CLK[13]). Ukoliko je stanje na ulazu T nisko (nula) i stanje na CLK se

[9] Toggle (eng.)

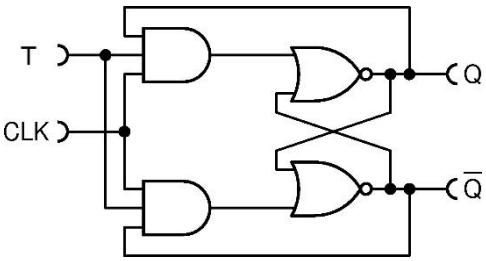
[10] Data (eng.)

[11] Toggle random flip-flop (eng.)

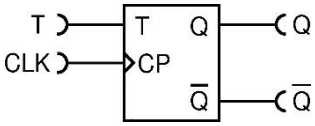
[12] Data random flip-flop (eng.)

[13] Clock (eng.)

mijenja iz niskog (nula) u visoko (jedan), tada stanje na izlazu Q ostaje nepromijenjeno. U suprotnom, ako je stanje na ulazu T visoko (jedan) i stanje na CLK se također mijenja iz niskog u visoko, tada se izlazno stanje Q mijenja iz niskog u visoko ili obrnuto, ovisno o tome kakvo je stanje bilo u prethodnom koraku, što je vidljivo u pripadnoj tablici istinitosti na Slici 2.2.c, gdje je pretpostavljeno da se kod svih kombinacija Q i T, stanje CLK-a mijenja iz niskog u visoko. Prilikom promjene stanja CLK-a iz visokog u nisko, ne događa se nikakva promjena izlaznog stanja Q. Zbog tih promjena stanja iz niskog u visoko prilikom svake promjene taktnog signala iz niskog u visoko i obrnuto je TFF dobio svoj naziv.



(a) Shema T flip-flopa.



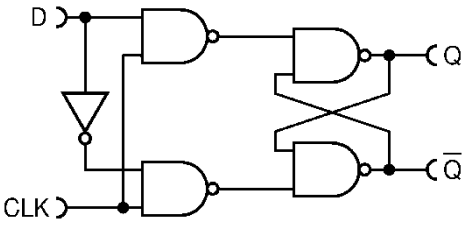
(b) Simbol T flip-flopa.

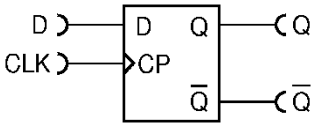
(c)Tablica istinitosti TFF-a.

Q	T	Q'
0	0	0
0	1	1
1	0	1
1	1	0

Slika 2.2: Grafički prikaz T flip-flopa (TFF). T predstavlja ulazno stanje, CLK je taktni signal, a Q i $\overline{Q}$ su izlazna stanja, pri čemu je $\overline{Q}$ obrnuto od Q. Kod tablice istinitosti je pretpostavljeno da za sve kombinacije Q i T, CLK mijenja stanje iz niskog u visoko. Prilikom promjene stanja CLK-a iz visokog u nisko ne događa se nikakva promjena izlaznog stanja Q. Q' označava sljedeći bit na izlazu.

DFF se sastoji od četiri NAND vrata povezanih međusobno i jednih NOT vrata te taktnog (CLK) signala, na čijem principu se rad ovog flip-flopa zasniva. Naziv je dobio prema tome što predstavlja memoriju, točnije pamti prethodnu vrijednost. Zbog toga se na izlazu uvijek pojavljuje prethodno pohranjena vrijednost stanja, a pohranjuje se trenutna kako bi se ona iskoristila u sljedećem trenutku. Na Slici 2.3.a prikazan je DFF, a njegov simbol na Slici 2.3.b.





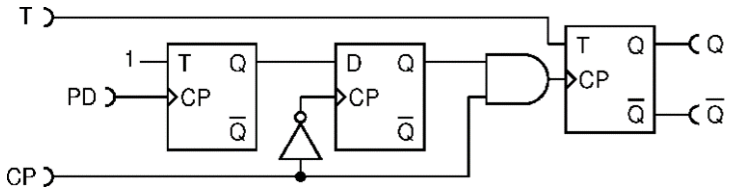
Q	D	Q'
0	0	0
0	1	1
1	0	0
1	1	1

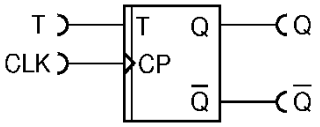
(a) Shema D flip-flopa. (b) Simbol D flip-flopa. c) Tablica istinitosti DFF-a.

Slika 2.3: Grafički prikaz D flip-flopa. D predstavlja ulaz, CLK je taktni signal, a Q i $\overline{Q}$ predstavljaju izlaze, pri čemu je $\overline{Q}$ obrnuto od Q. Kod tablice istinitosti je pretpostavljeno da za sve kombinacije Q i T, CLK mijenja stanje iz niskog u visoko. Prilikom promjene stanja CLK-a iz visokog u nisko ne događa se nikakva promjena izlaznog stanja Q. Q' označava sljedeći bit na izlazu.

Pretpostavimo li da je stanje na ulazu D visoko, a stanja na izlazu Q i $\overline{Q}$ redom visoko pa nisko te taktni signal prelazi iz niskog u visoko stanje, slijedi da su vrijednosti stanja na izlazima Q i $\overline{Q}$ nepromijenjena.

Sada kad smo upoznati sa TFF-om i DFF-om, možemo objasniti rad i izvedbu TRFF-a i DRFF-a, koji su slučajne verzije TFF-a i DFF-a [8]. TRFF i pripadni simbol prikazani su na Slici 2.4, dok su DRFF i njegov simbol prikazani na Slici 2.5.

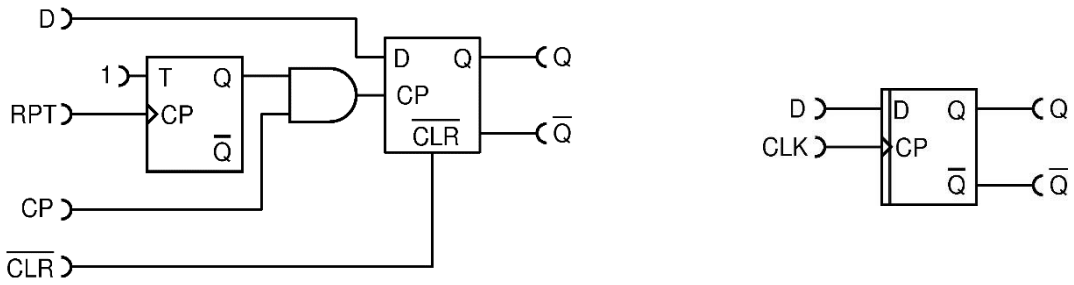




a) Shema TRFF-a. b) Simbol TRFF-a.

Slika 2.4: Grafički prikaz T slučajnog flip-flopa (TRFF) sa pripadnim simbolom TRFF-a. T i CP su ulazi, a Q i $\overline{Q}$ izlazi. PD je interni ulaz, koji nije prikazan na shemi simbola, a prima oko 16 Mcps[14] slučajnih impulsa iz detektora fotona.

[14] Mega counts per second (eng.)



a) Shema DRFF-a. b) Simbol DRFF-a.

Slika 2.5: a) Grafički prikaz D slučajnog flip-flopa (DRFF), b) simbol DRFF-a. D, CP, RPT i $\overline{CLR}$ su ulazi, a Q i $\overline{Q}$ izlazi.

Iako TRFF i DRFF oboje sadrže i TFF i DFF, TRFF se zasniva na principu TFF-a, a DRFF na principu DFF-a. Kod oba sklopa, T i CP[15] su ulazi, dok su Q i $\overline{Q}$ izlazi, kod kojih je $\overline{Q}$ konjugiran izlazu Q pa su signali točno obrnuti. Oni se nazivaju slučajnima jer je vjerojatnost da se ulazni impuls pojavi na ulazu T ili D i na izlazu Q 50%. Kod TRFF-a, ako se ulaz T konstantno drži na visokom stanju, tada pri svakom nailasku impulsa na ulaz CP kada on mijenja stanje iz niskog u visoko, izlaz Q mijenja stanje na slučajan način. Time se generiraju slučajni impulsi, odnosno bitovi pa TRFF u ovom eksperimentu služi kao dodatan izvor slučajnosti. Razlika između određenog tipa flip-flopa i istog tipa slučajnog flip-flopa je u tome što CP prihvaća ulazni impuls na slučajan način. Prema definiciji [8], vjerojatnost da će ulaz CP prihvatiti impuls je točno $1/2$, što vodi na maksimalnu neodređenost rada slučajnog flip-flopa.

[15] Clock pulse (eng.)

3 Eksperimentalni postav i metoda

Eksperimentalni postav sastojao se od računala i tri digitalne pločice, koje sadrže svu potrebnu elektroniku za izvođenje ovog eksperimenta, te osciloskopa i frekvenciometra kao kontrolnih uređaja. Elektronika se sastoji od tri pločice. Prva pločica sadrži kameru s dvadeset i tri piksela koju obasjava LED dioda konstantnog intenziteta u kontinuiranom načinu rada[16]. Dvadeset i tri piksela su zapravo dvadeset i tri SPAD diode u kojima se događa fotoelektrični efekt, koji uzrokuje kvantnu slučajnost. Ta pločica je spojena na DE0-Nano pločicu sa FPGA[17] čipom, koji čini samo srce ovog postava jer su sklopovi realizirani u njemu. Posljednja pločica sakuplja podatke s prethodnih i šalje ih u računalo. S obzirom da je DE0-Nano pločica središnji dio ove priče, u nastavku započinjemo sa određenim informacijama o njoj koje su potrebne za razumijevanje cijelog eksperimentalnog postava, dok je njezin detaljan opis prezentiran u potpoglavlju *DE0-Nano programabilna pločica sa FPGA čipom*, koje se nalazi u nastavku ovog poglavlja.

DE0-Nano pločica sadrži FPGA čip marke Intel-Altera, linije Cyclone IV sa 22 320 makro ćelija i četiri PLL-a[18], koji proizvode četiri sinkronizirana taktna (CLK) signala sa proizvoljnim fazama [9]. Faze koje smo izabrali su redom -90, 0, 45 i 90 stupnjeva. Glavni signal definira vremenske intervale i ima radni ciklus 50%, što znači da je 50% vremena na logičkoj jedinici, a 50% na logičkoj nuli, dok je trajanje impulsa (vrijeme provedeno na logičkoj jedinici) 500 ns. Frekvencija CLK-a koju smo odabrali je $f_{CLK} = 1\ MHz$, zbog čega je vremenski interval duljine $\Delta t = 1/f_{CLK} = 1\ \mu s$.

Vrijeme koherencije je vremensko trajanje tijekom kojeg se smatra da impulsni odziv kanala ne varira. Svjetlost je elektromagnetski val pa samim time za njega možemo definirati vrijeme koherencije, kao vrijeme tokom kojeg se propagirajući val smatra koherentnim, što znači da je njegova faza u prosjeku predvidljiva. Za izvor svjetlosti sa gausijanskim profilom, vrijeme koherencije dano je relacijom:

$$\tau_c = \frac{1}{c}\frac{\lambda_0^2}{\Delta\lambda}, \tag{3.1}$$

[16] Continous wave mode (eng.)

[17] Field Programmable Gate Array (eng.)

[18] Phase-Locked Loop (eng.)

gdje je c brzina svjetlosti, λ_0 valna duljina vrha[19], koja u našem slučaju LED diode iznosi $\lambda_0 = 670\,nm$, te $\Delta\lambda$ spektralna širina na pola maksimuma (FWHM[20]) koja iznosi $\Delta\lambda = 30\,nm$ [9,12]. Brzina svjetlosti aproksimativno iznosi $c = 3 \cdot 10^8\,m/s$ pa uvrštavajući spomenute iznose, dobivamo da je vrijeme koherencije $\tau_c = 50\,fs$. Iz toga slijedi da je frekvencija detekcije fotona $1/\tau_c \approx 20\,Tcps$[21]. Ovaj broj nam govori da dok god smo u režimu nižem od $1/\tau_c$, detekcije fotona su nekorelirane, točnije u tom režimu se ne pojavljuju vremenske korelacije. U ovom eksperimentu, korištena je frekvencija detekcija manja ili jednaka $16\,Mcps$, što je šest redova veličine niže od $1/\tau_c$.

3.1 Generiranje niza slučajnih impulsa

3.1.1 Detektori fotona

SPAD (Single photon avalanche diode, eng.) detektori su poluvodički uređaji bazirani na p-n spoju opisanom u uvodnom dijelu poglavlja *Teorijska pozadina* [13]. Svaki SPAD detektor od spomenuta dvadeset i tri ima dobro definiranu kvantnu efikasnost tj. vjerojatnost detekcije fotona, točnije vjerojatnost generiranja slobodnog nosioca naboja, koji je pojačavan mehanizmom lavine kako bi se dobila dovoljno jaka struja za generiranje digitalnog impulsa. Zbog toga su SPAD detektori pogodni za detektiranje signala niskog intenziteta, točnije pojedinačne fotone, što je upravo slučaj u ovom eksperimentu. Za razliku od lavinskih fotodioda, oni rade s obrnutim naponom u režimu daleko iznad napona proboja, što zovemo Geigerovim modom rada zbog sličnosti s Geiger-Millerovim brojačem, koji broji koliko je ionizirajućih čestica ili fotona prošlo kroz njega [14,15].

Nakon detekcije fotona, SPAD detektori proizvode električni signal kvadratnog oblika, što je upravo oblik koji je potreban za izvođenje ovog eksperimenta. Taj signal je duljine trajanja $6 - 14\,ns$, što je manje od kratkog trajanja mrtvog vremena od $25\,ns$, jer je bitno da je impuls kraći od mrtvog vremena detektora. Kratko mrtvo vrijeme je potrebno

[19] Peak wavelenght (eng.)

[20] Full width at half maximum

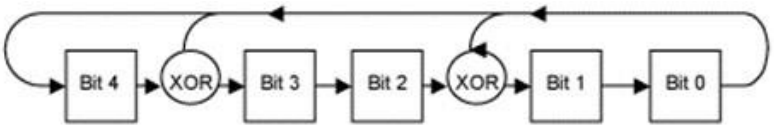
[21] Tera counts per second (eng.)

zbog malog stvaranja naknadnih impulsa[22], koji se smanjuju eksponencijalno, i visoke vjerojatnosti detekcije[23]. Time je osigurano da kada je proizveden električni impuls, da je on uzrokovan detekcijom samo jednog fotona. Tako generirani električni signali slijede eksponencijalnu distribuciju opisanu u *Dodatku A*, što je analogno detekciji gama zraka pomoću Geiger-Millerovog brojača [14].

3.1.2 Linear Feedback Shift Register (LFSR)

Iako su u ovom eksperimentalnom postavu sadržana dvadeset i tri detektora, od kojih svaki detektor predstavlja jedan bit, a deset bitova je određeno kao dovoljna točnost da predstavlja jedan niz slučajnih impulsa te su u ovom radu potrebna dva takva niza, znači da bi dvadeset detektora bilo dovoljno za izvođenje eksperimenta. No, s obzirom da se radi o istraživanju koje ima puno potencijala i čija tema tek probija svoje putove u popularizaciji, u ovom dijelu eksperimentalnog postava, prije samog generiranja niza slučajnih impulsa, signali iz detektora prolaze kroz sklop koji se naziva *Linear feedback shift register* (LFSR) i služi za proizvodnju 10x više slučajnih impulsa. Dakle, umjesto četrdeset SPAD detektora, moguće je pomoću ovog sklopa proizvesti slučajne signale sa samo četiri detektora kao da ih je četrdeset. Zbog toga ovaj dio nije neophodan za razumijevanje cijelog eksperimenta pa ga čitatelj može preskočiti.

LFSR pruža generiranje nesekvencijalnog niza bitova i kao takav služi za generiranje pseudoslučajnih brojeva, a jedino od čega se sastoji je operacija pomaka udesno i XOR logičkih vrata [9]. Pomak udesno ostvaruje se pomoću D flip-flopa. Slika 3.1 prikazuje pojednostavljenu shemu 5-bitnog LFSR-a.



Slika 3.1: Pojednostavljeni prikaz 5-bitnog LFSR-a (Linear Feedback Shift Register). Slika preuzeta iz [16].

[22] Afterpulsing (eng.)

[23] Detection rate (eng.)

Sa Slike 3.1 je vidljivo da LFSR čini jedan zatvoreni ciklus pa kao takav treba imati i početnu vrijednost koja se naziva sjeme. Rad registra je deterministički pa je tok vrijednosti koje proizvodi registar u potpunosti određen njegovim trenutnim ili prethodnim stanjem. Međutim, ono što utječe na generiranje pseudoslučajnih bitova je funkcija koja proizvodi nizove bitova, a to je upravno način na koji se bitovi pomiču udesno. Izlazni nizovi pseudoslučajnih bitova su oni bitovi generirani operacijom XOR nakon svakog pomicanja. Time se u ovom slučaju prikazanom na Slici 3.1 dobivaju dva niza pseudoslučajnih brojeva iz jednog detektora. Sa LFSR-om koji sadrži puno više bitova, moguće je na opisani način dobiti četrdeset pseudoslučajnih nizova od četiri ulazna slučajna niza sa četiri detektora.

3.1.3 Generiranje frekvencije slučajnog niza impulsa

Primijećeno je da nizovi impulsa koje generiraju ljudski senzorni neuroni koji se pojavljuju u ljudskom mozgu nalikuju RPT-u, što je dovelo do istraživanja biomimetričkih sustava temeljenih na obradi RPC-a. Budući da je jedina informacija koju nosi RPT njegova slučajna frekvencija, opravdano je pitanje kako ju točno generirati. Periodične signale, prikazane na Slici 3.2, je jednostavno generirati pomoću petlje za zaključavanje faze (PLL[24]). Upravo periodični signali stvaraju diskretiziranu vremensku os s obzirom da dijele vrijeme na odsječke jednake duljine. PLL radi tako što proizvodi frekvenciju oscilatora koja odgovara frekvenciji ulaznog signala.

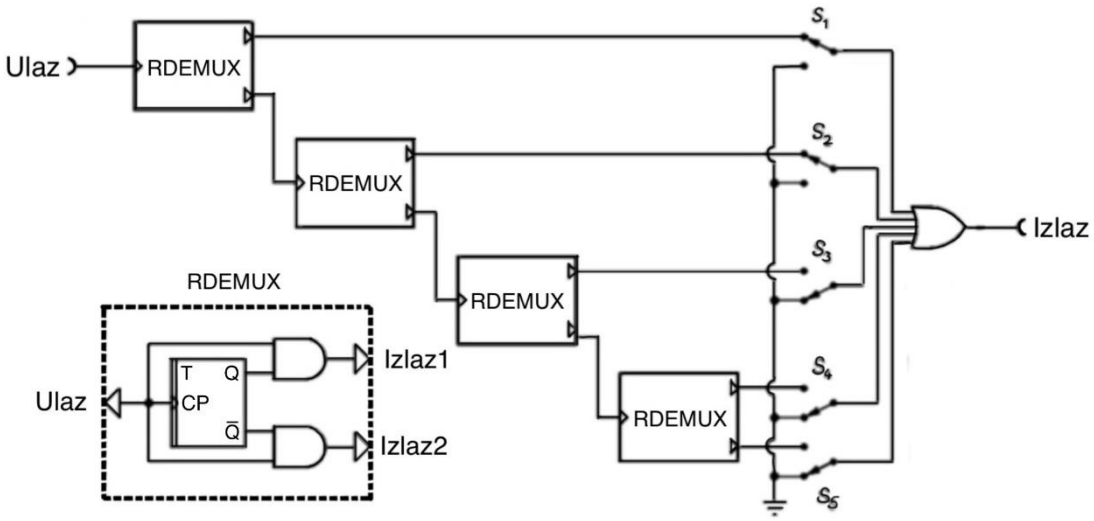
Slika 3.2: Kvadratni periodični signal koji proizvodi PLL (Phase-locked loop) nazvan taktni (CLK) signal.

Periodični signal je ključan, u nastavku, prilikom generiranja željene frekvencije RPT-a, a to se postiže pomoću digitalnog slučajnog frekvencijskog sintetizatora (DRFS[25]). DRFS radi na principu kaskade tako što proizvedeni električni impuls ulazi u sklop koji se naziva RDEMUX, a čija funkcija je kao raskrižje na kojem signal na slučajan način završava

[24] Phase-locked loop (eng.)

[25] Digital Random Frequency Synthesizer (eng.)

u jednom od dva moguća izlaza, kao što je prikazano na Slici 3.3. Više RDEMUX-a je povezano u niz tako da jedan od dva moguća izlaza prethodnog postaje ulaz u sljedeći. S obzirom da je vjerojatnost da će signal završiti na jednom izlazu 50%, odnosno 0.5, znači da je vjerojatnost da će signal završiti na jednom od izlaza drugog po redu RDEMUX-a je 25%, tj. 0.25 i tako redom. U našem slučaju je njihov broj 10 jer želimo toliku preciznost. Upravo zato je ranije spomenuto da je potrebno 10 detektora (deset pseudoslučajno generiranih impulsa) da bi se stvorio jedan niz slučajnih impulsa (RPT). Na kraju logička OR vrata služe da bismo sigurno na izlazu imali signal iz jednog od izlaza kaskade i to točno određene vjerojatnosti koja se dobiva zbrajanjem željenih izlaza koji predstavljaju ulaze u OR vrata. Na Slici 3.3 su to OR1 logička vrata [8].

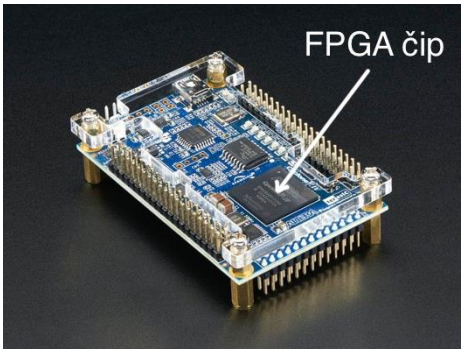


Slika 3.3: Grafički prikaz DRFS-a (digitalni slučajni frekvencijski sintetizator), koji se sastoji od više sklopova naziva RDEMUX, koji su pak povezani logičkim OR vratima kako bi se dobila željena frekvencija. Slika preuzeta iz [8].

Na ovaj način je dobiven RPT točno određene frekvencije koji predstavlja upravo ono što nam treba za izvođenje eksperimenta. Ovime je opis generiranja RPT-a završen, a u nastavku je opisan ostatak elektroničke opreme.

3.2 DE0-Nano programabilna pločica s FPGA čipom

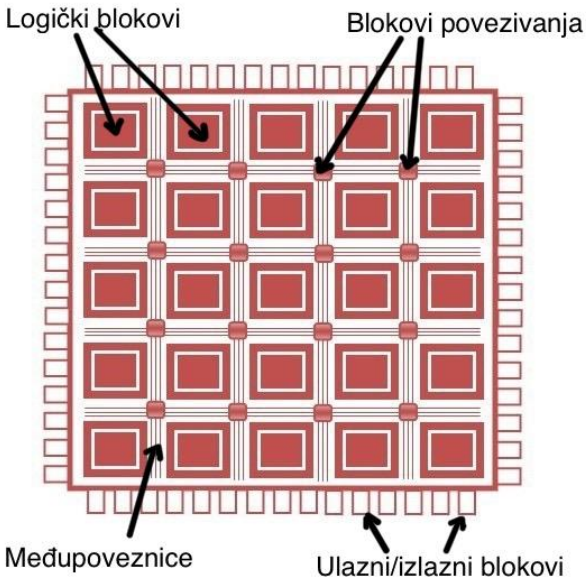
DE0-Nano programabilna pločica prikazana je na Slici 3.4. Kao što je već spomenuto, ona sadrži FPGA čip koji je uokviren crvenom bojom, a koji čini središte ovog eksperimenta pa će se daljnji tekst odnositi na njega, a opisivat će njegovu strukturu i funkciju te način na koji se programira [14].



Slika 3.4: DE0-Nano programabila pločica s FPGA čipom [14].

3.2.1 Struktura i funkcija FPGA čipa

Unutarnja struktura FPGA čipa prikazana je na Slici 3.5. Veliki crveni kvadratići predstavljaju konfigurabilne logičke blokove i služe za implementaciju logičkih funkcija. Svaki blok u sebi sadrži niz različitih logičkih vrata poput flip-flopova, multipleksera i ostalih logičkih vrata. Između tih logičkih blokova nalaze se crte koje se nazivaju međupoveznice, a omogućavaju interakciju između logičkih blokova. Na njihovim sjecištima nalaze se mali crveni kvadratići koji predstavljaju blokove povezivanja kako bi se povezali točno određeni logički blokovi koje želimo povezati. Konačno, na rubovima ove sheme nalaze se prazni kvadratići koji označavaju ulazne/izlazne blokove, koji omogućavaju vezu s vanjskim signalima [3,17].



Slika 3.5: Unutarnja struktura FPGA čipa [14].

3.2.2 Programiranje FPGA čipa

FPGA čip može se programirati korištenjem JTAG[26] programiranja, koje omogućava prijenos podataka u trajnu internu memoriju uređaja. To nam je osiguralo da konfiguriramo čip korištenjem Quartus Prime softvera u kojem su sklopovi za matematičke operacije prikazani simbolima Boolove algebre radi preglednosti [18]. Sklopovi su se programirali pomoću specijaliziranih jezika za opis sklopovlja zvanih HDL[27]. Trenutno najkorišteniji i najpoznatiji jezici su Verilog i VHDL[28], a u ovom radu korišten je jezik Verilog [4,19]. Isprogramirani dizajn ostaje u FPGA čipu do ponovnog reprogramiranja ili nestanka struje, čime je omogućena automatizacija mjerenja niza kombinacija ulaznih vrijednosti.

[26] Joint Test Action Group (eng.)

[27] Hardware Description Language (eng.)

[28] Very High Speed Integrated Circuit (eng.)

3.3 Kontrolna elektronička oprema

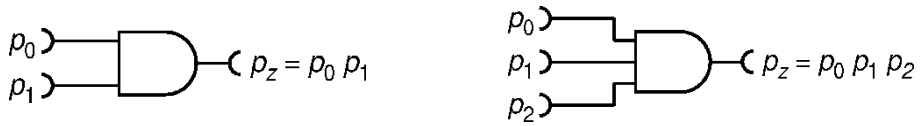
Osim glavnih uređaja dosad opisanih u poglavlju *Eksperimentalni postav*, u ovom eksperimentu korištena su dodatna dva uređaja za kontroliranje ispravnosti međukoraka između ulaznih i izlaznih vrijednosti prilikom provođenja ovog eksperimenta. Ti uređaji su osciloskop i frekvenciometar i njihova svrha je bila otklanjanje pogrešaka prilikom mjerenja koja su pokazivala neslaganja sa očekivanim rezultatima. Korišten je osciloskop marke Rigol, model MSO5204, a frekvenciometar marke Hameg, model HM8123 .

4 Matematičke operacije u impulsnom računanju

Osnovni RPC sklopovi izvode matematičke operacije zbrajanja, oduzimanja, množenja i dijeljenja, koji su potrebni za izradu univerzalnog RPC računala. U ovom poglavlju opisani su najprecizniji sklopovi dosad poznati u literaturi za sve četiri matematičke operacije. Redoslijed kojim su operacije opisane je specifičan jer polazimo od jednostavnijih operacija, a to su množenje i zbrajanje, prema kompleksnijima, a to su dijeljenje i oduzimanje. Ovakav poredak je kontra intuitivan jer je do sada poznato da su operacije zbrajanja i oduzimanja jednostavnije nego operacije množenja i dijeljenja. No, kako se RPC zasniva na modelu živčanog sustava, opis Boolove algebre nam sugerira da je povećanje broja impulsa jednostavnije od njihovog smanjenja. Zbog toga zbrajanje i množenje može biti izvedeno bez aproksimiranja, dok oduzimanje i dijeljenje koriste aproksimativne metode, koje rezultiraju kompleksnijim kalkulacijama.

4.1 Sklop za množenje

Sklop za množenje je najjednostavniji sklop u RPC-u [9,14]. Dobro je poznato da su za njegovu realizaciju potrebna samo jedna AND vrata, kao što je prikazano na Slici 4.1.a, pa je princip rada ovog sklopa jasan jer se impuls na izlazu pojavljuje samo u slučaju kad se oba impulsa istovremeno pojave na ulazima. Stoga je vjerojatnost na izlazu jednaka $p_z = p_0 \cdot p_1$. Time je vidljivo da je rezultat množenja egzaktan.



(a) Množenje dva broja. (b) Množenje tri broja.

Slika 4.1: Sklopovi za egzaktno množenje dva i tri decimalna broja u intervalu [0,1]. p_0, p_1 i p_2 su ulazi, CLK je taktni signal, a p_z je izlazni rezultat [9].

Množenje tri broja se također može ostvariti pomoću jednih logičkih AND vrata koja imaju tri ulaza, što je prikazano na Slici 4.1.b. Analogno, ovaj sklop se može napraviti i za istovremeno množenje n brojeva tako da se doda n ulaza u AND vrata. Zbog toga je ovaj primjer idealan za usporedbu RPC-a sa digitalnim računalima jer je njegova prednost ovdje lako uočljiva. Naime, kod digitalnih računala, množenje zahtijeva daleko veću

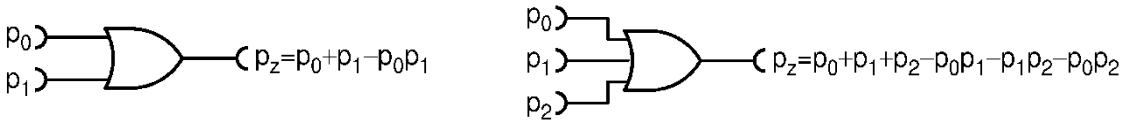
količinu logičkih logičkih vrata jer se n brojeva treba množiti sukcesivno $n-1$ puta, dok su ovdje dovoljna jedna logička vrata sa puno kraćim vremenom obrade podataka.

4.2 Sklopovi za zbrajanje

Druga matematička operacija po kompleksnosti je zbrajanje. S obzirom da je suma dvaju vjerojatnosti dana u intervalu $[0,2]$ umjesto $[0,1]$, tj. ne smije se prijeći 1 jer je i sama suma vjerojatnost, tada je jasno da potpuno zbrajanje nije moguće realizirati. Zbog toga su ovdje predstavljena dva sklopa za zbrajanje – jedno je aproksimativno zbrajanje, a drugo egzaktno poluzbrajanje.

4.2.1 Zbrajanje s logičkim OR vratima

Prvi sklop za zbrajanje sastoji se od jednih logičkih OR vrata, a radi na principu da se na izlazu pojavljuju impulsi kada se na barem jednom ulazu pojavi impuls [9,14]. Problem nastupa kada se na oba ulaza istovremeno pojavi impuls jer tada se na izlazu pojavljuje samo jedan impuls umjesto dva. Zbog toga je ovakvo zbrajanje aproksimativno jer se dio impulsa gubi, a vjerojatnost na izlazu iznosi $p_z = p_0 + p_1 - p_0 \cdot p_1$. Sklop je prikazan na Slici 4.2.a. U slučaju kada je umnožak vjerojatnosti ulaznih impulsa puno manji u odnosu na njihov zbroj, tada je zbrajanje točno, a to se događa za male vrijednosti ulaznih vjerojatnosti.



(a) Zbrajanje dva broja. (b) Zbrajanje tri broja.

Slika 4.2: Sklopovi za egzaktno zbrajanje dva i tri decimalna broja u intervalu $[0,1]$. p_0 i p_1 su ulazi, CLK je taktni signal, a p_z je izlazni rezultat [9].

Kao i kod sklopa za množenje, i ovaj sklop za zbrajanje može biti generaliziran na više ulaza. Na primjer, za tri ulazne vjerojatnosti, izlazna vjerojatnosti iznosi

$$p_z = p_0 + p_1 + p_2 - p_0 \cdot p_1 - p_1 \cdot p_2 - p_0 \cdot p_2. \tag{4.1}$$

Kao i u slučaju sa dva ulaza, ovaj sklop sa tri ulaza je također točan u limesu iščezavajuće malih ulaznih vjerojatnosti, a prikazan je na Slici 4.2.b.

Netko bi mogao pretpostaviti da u limesu velikih brojeva zbrajanje sa OR vratima ulazi u zasićenje, ali to ovdje nije slučaj. Iako je zbroj dviju vjerojatnosti u intervalu $[0,2]$, izlazna vjerojatnost ne može prijeći jedinicu zbog umnoška $p_0 \cdot p_1$. Ova tvrdnja je jasnije vidljivija ako izlaznu vjerojatnost zapišemo na malo drugačiji način:

$$\begin{aligned} p_z &= p_0 + p_1 - p_0 \cdot p_1 \\ &= 1 - (1 - p_0)(1 - p_1). \end{aligned} \tag{4.2}$$

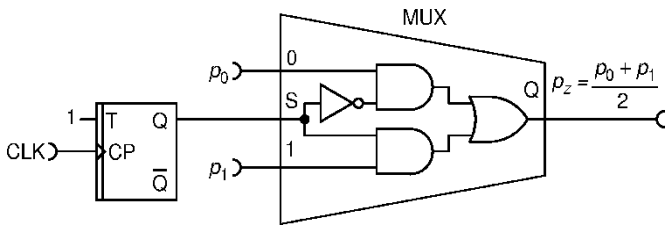
Iz ove jednakosti je vidljivo da su oba izraza u zagradama unutar intervala $[0,1]$ pa slijedi da je i njihov produkt unutar istog intervala. Oduzimanjem tog produkta od jedinice dobivamo da je rezultat također unutar intervala $[0,1]$, čime je prethodna tvrdnja potvrđena. To znači da ovaj sklop doista ne ulazi u zasićenje pa se u literaturi ponekad naziva i *saturirajuće zbrajalo* [9,17].

4.2.2 Zbrajanje s MUX-om

Drugi sklop za zbrajanje ostvaren je pomoću multipleksera (MUX[29]) i prikazan je na Slici 4.3 [9,14]. Ovdje se zapravo radi o poluzbrajalu jer je zbroj dviju vjerojatnosti podijeljen s dva. Naime, MUX radi na principu propuštanja ulaznih impulsa na slučajan način, a ono što uvjetuje slučajnost je slučajan flip-flop koji predstavlja selektiranje u MUX-u. Kada je slučajan flip-flop na jedinici (visoko stanje) propušta se impuls na jednom ulazu ukoliko ga ima, a kada je RFF na nuli (nisko stanje), onda se propušta impuls na drugom ulazu ako on postoji. Time je izlazna vjerojatnost u rasponu $[0,1]$ pa je na ovaj način riješen i problem zbrajanja brojeva čiji rezultat prelazi jedinicu. Dodatno, ulaz T u slučajnom flip-flopu postavljen je na visoko stanje, tj. jedinicu, kako bi TRFF doista generirao slučajan bit u sinkronizaciji sa svakim ulaznim impulsom. Prednost ovog sklopa za zbrajanje u odnosu

[29] Multiplexer (eng.)

na sklop za zbrajanje pomoću OR vrata je u tome što ovaj sklop daje egzaktan rezultat pa se stoga on danas isključivo i koristi.



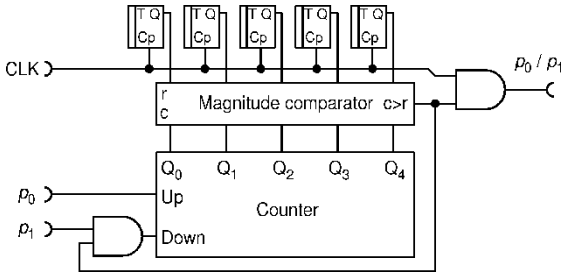
Slika 4.3: Shema sklopa za egzaktno zbrajanje dva broja u intervalu [0,1] pomoću multipleksera (MUX) i T slučajnog flip-flopa (TRFF). p_0 i p_1 su ulazi, CLK je taktni signal, a p_z je izlazni rezultat. Slika je preuzeta iz [9].

4.3 Sklop za dijeljenje

Sklopovi za dijeljenje i oduzimanje su jednako kompleksni, no dosad najtočnije poznati sklop za oduzimanje se zasniva na metodi sklopa za dijeljenje pa stoga prvo opisujemo sklop za dijeljenje.

Sklop za dijeljenje prikazan je na Slici 4.4, a sastoji se od brojača, komparatora, slučajnih flip-flopova i dvaju AND vrata. Ovaj sklop radi na principu negativne povratne sprege, što znači da se signal na izlazu iz komparatora množi sa ulaznim signalom p_1, odnosno sa djeliteljem. Komparator radi tako što uspoređuje koji je od dva binarna broja veći – 5-bitni binarni broj dobiven od slučajnih TRFF-ova, od kojih svaki predstavlja jedan bit i spojen je na ulazno visoko stanje, ili 5-bitni binarni broj iz brojača[30], kod kojeg impulsi iz ulaza p_0 povećavaju brojač, a impulsi dobiveni umnoškom impulsa iz ulaza p_1 i izlaza iz komparatora smanjuju brojač. U slučaju kada je broj iz brojača c veći od broja dobivenog iz TRFF-ova r, tj. $c > r$, tada je stanje na izlazu komparatora visoko. Time brojač i komparator magnitude "namještaju" izlaznu vjerojatnost tako da je $p_z \cdot p_1 = p_0$, čime se dobiva da je $p_z = p_0/p_1$. Na kraju, rješenje se dobiva tako što se izlazno stanje iz komparatora množi sa taktnim (CLK) signalom pa se produciraju impulsi slučajno raspoređeni u zadanim vremenskim intervalima, što je i bio cilj [9].

[30] Counter (eng.)



Slika 4.4: Shema sklopa za dijeljenje dva broja u intervalu [0,1]. p_0 i p_1 su ulazi, CLK je taktni signal, a p_0/p_1 je izlazni rezultat. Komparator magnitude uspoređuje dva broja: c dobiven iz brojača i r dobiven pomoću pet slučajnih flip-flopova (TRFF). Slika je preuzeta iz [9].

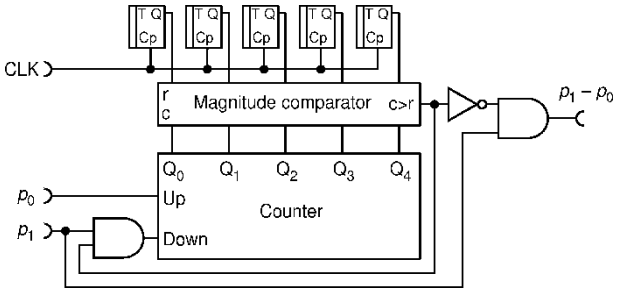
Jedini problem koji se može pojaviti kod ovakvog sklopa je situacija kada je $p_0 \approx p_1$ jer tada se može dogoditi da brojač prijeđe svoj maksimalni kapacitet ili odbroji ispod nule. Taj problem je riješen tako što je brojač maksimiziran na svoj najveći broj i minimiziran na nulu pa u slučaju prelaska tih granica, brojač zadržava postavljene vrijednosti. Zbog toga je brojač precizniji što ima više bitova. U našem slučaju je izabran 5-bitni brojač kao idealan omjer između preciznosti i utrošene količine logičkih elemenata kako bismo imali maksimalno jednostavan i efikasan sklop.

4.4. Sklop za oduzimanje

Kao što je spomenuto u prethodnom potpoglavlju *Sklop za dijeljenje*, poznate metode za oduzimanje zasnivaju se upravo na dijeljenju pa je time oduzimanje najkompleksnija matematička operacija prema RPC-u [9]. Dijeljenje se pojavljuje kod oduzimanja izlučimo li djeljenik iz izraza $p_1 - p_0$ čime dobivamo:

$$p_1 - p_0 = \left(1 - \frac{p_0}{p_1}\right) p_1. \tag{4.3}$$

Zbog toga je najefikasniji poznati sklop za oduzimanje koji se zasniva na principu dijeljenja prikazan na Slici 4.5, te se sastoji od istih elemenata kao i sklop za dijeljenje (komparator, brojač, pet TRFF-ova i dvoja AND vrata) uz jedini dodatak, a to su NOT vrata.



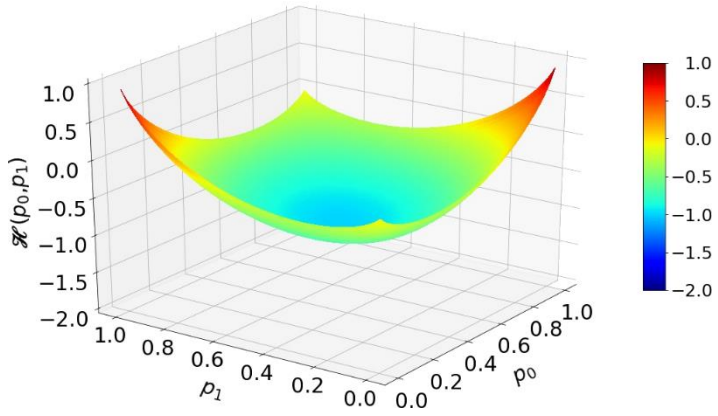
Slika 4.5: Shema sklopa za oduzimanje dva broja u intervalu $[0,1]$, s naslijeđenim karakteristikama sklopa za dijeljenje. p_0 i p_1 su ulazi, CLK je taktni signal, a p_0/p_1 je izlazni rezultat. Komparator magnitude uspoređuje dva broja: c dobiven iz brojača i r dobiven pomoću pet slučajnih flip-flopova (TRFF). Slika je preuzeta iz [9].

S obzirom da je ovaj sklop temeljen na principu dijeljenja, on je naslijedio princip negativne povratne sprege pa se signal na izlazu iz komparatora, nakon usporedbe binarnog broja iz brojača i slučajnog binarnog broja dobivenog pomoću pet TRFF-ova te potom množi sa djeljenikom tj. ulazom p_1. Rad komparatora, brojača i TRFF-ova opisan je u prethodnom potpoglavlju *Sklop za dijeljenje* jer upravo ti elementi služe za produkciju izraza p_1/p_0. Jedina razlika u odnosu na sklop za dijeljenje je što se izlaz iz komparatora ne množi sa taktnim signalom, već se stanje na izlazu iz komparatora invertira pomoću NOT vrata te potom množi sa djeljenikom p_1 [9].

Ovaj sklop za oduzimanje je specifičan jer obuhvaća tri matematičke operacije: dijeljenje, množenje pomoću logičkih AND vrata i oduzimanje, pa se na taj način može demonstrirati jednostavno RPC računalo.

5 Utjecaj entropije na primjeru zbrajanja

Prema EBC-u, egzaktan deterministički sklop za zbrajanje ne postoji [9]. Primjer sklopa opisanog u potpoglavlju *Sklopovi za zbrajanje* i prikazanog na Slici 4.2.a nam to i potvrđuje, jer takav sklop nema dovoljnu točnost. S obzirom da zbrajanje može rezultirati u vrijednostima većima od jedinice, shema entropijskog budžeta prikazana na Slici 5.1, preuzetoj iz [9], opisuje funkciju zbrajanje $p_z = (p_0 + p_1)/2$ pa je prikazana funkcija entropije $\mathcal{H}(p_0, p_1) = \mathcal{H}(p_z) - (\mathcal{H}(p_0) + \mathcal{H}(p_1))$.



Slika 5.1: Entropijski budžet sklopa za zbrajanje, čije ulazne vjerojatnosti su p_0 i p_1, za funkciju zbrajanja $p_z = (p_0 + p_1)/2$. Prikazana entropijska funkcija ima oblik $\mathcal{H}(p_0, p_1) = \mathcal{H}(p_z) - (\mathcal{H}(p_0) + \mathcal{H}(p_1))$. Slika je preuzeta iz [9].

Sa slike je vidljivo da se za određena područje ulaznih vrijednosti $p_0, p_1 \in [0,1]$ dobivaju crvene ili narančaste vrijednosti, što znači da je za ta područja entropija izlaznog niza p_z veća od entropije ulaznih nizova p_0 i p_1. Detaljnije, za ulazne vrijednosti $p_0 = 0$ i $p_1 = 1$ ili obrnuto, izlazna entropija bi trebala biti nula, no prema gornjoj slici, ona iznosi jedan. To znači da je entropija izlaznog niza doista veća ili jednaka zbroju entropija ulaznih nizova p_0 i p_1, a da bi se to ostvarilo, potrebno je da sklop sadrži dodatan izvor entropije. Zbog toga egzaktan deterministički sklop za funkciju $p_z = (p_0 + p_1)/2$ ne postoji. No, EBC se može zadovoljiti tako da podijelimo ulaze sa dva pomoću MUX sklopa i TRFF-a, koji predstavlja dodatan izvor entropije, kao što je prikazano na Slici 4.3. Tada vrijedi sljedeća nejednakost:

$$\mathcal{H}\left(\frac{p_0 + p_1}{2}\right) \leq \mathcal{H}\left(\frac{p_0}{2}\right) + \mathcal{H}\left(\frac{p_1}{2}\right), \tag{5.1}$$

a ona je i dokazana matematičkim putem u *Dodatku D*.

Iako egzaktan deterministički sklop ne postoj, ovdje je cilj pronaći što precizniji sklop sa maksimalno iskorištenom entropijom, koja bi idealno bila blizu maksimalne kako bi izlazni niz mogao predstavljati ulaz u sljedeći sklop. Stoga su uvjeti koje je potrebno zadovoljiti prilikom osmišljavanja ili poboljšavanja novog sklopa sljedeći:

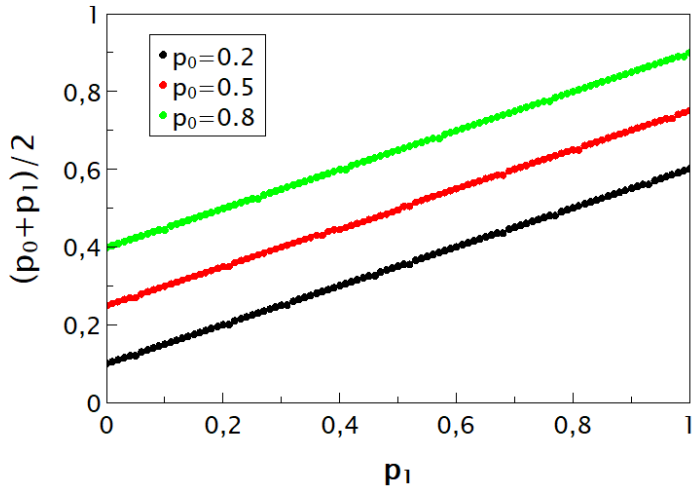
1. Minimizirati greške prilikom kalkulacija na cijelom prostoru stanja ulaznih parametara,
2. Minimizirati devijaciju na izlazu iz binomnog procesa,
3. Minimizirati količinu hardvera potrebnu za izradu sklopa.

U nastavku su prezentirani rezultati relativnih entropija i preciznosti postojećih ili poboljšanih sklopova za zbrajanje te potom primjena najkvalitetnije ocjenjenih sklopova za zbrajanje u kombinaciji sa množenjem u svrhu rješavanja zadane kvadratne jednadžbe. Promatrana entropija je relativna entropija kako bismo mogli ocijeniti slučajnost izlaznog niza.

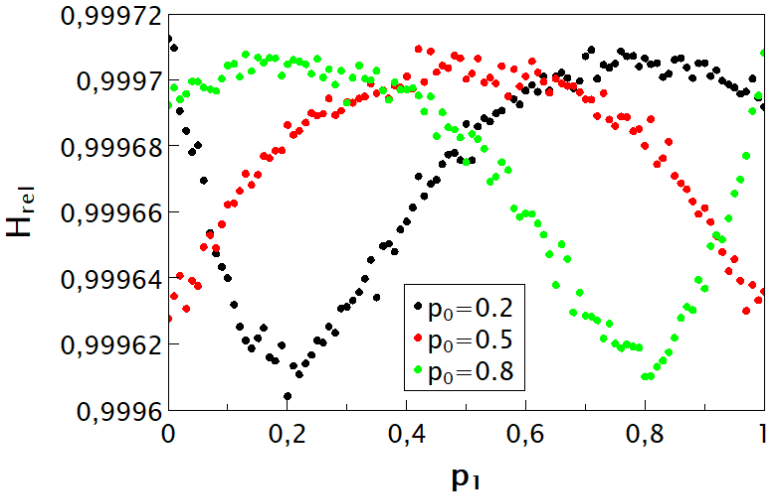
5.1 Analiza sklopova za zbrajanje

5.1.1 Sklop za zbrajanje s MUX-om

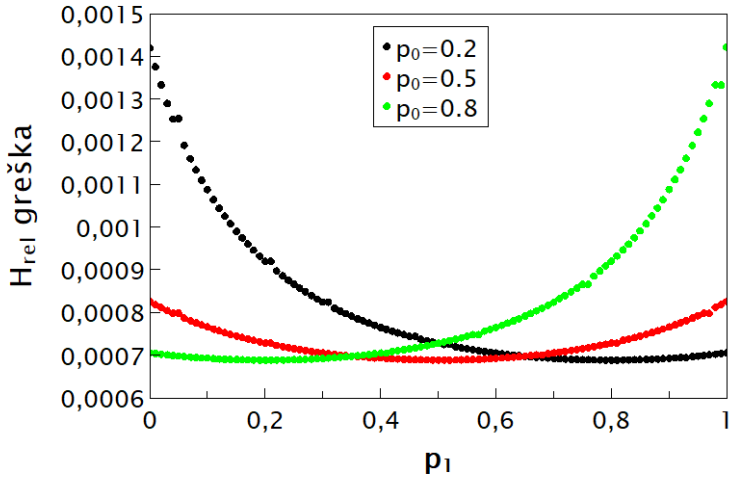
Nedeterministički MUX sklop je prvi sklop za zbrajanje koji daje točne rezultate i najpoznatiji je takav sklop u literaturi, a prethodno je opisan u potpoglavlju *4.2 Sklopovi za zbrajanje*. Stoga je vrijedno proučiti njegove entropijske vrijednosti. Rezultati mjerenja operacije zbrajanja prikazani su na Slici 5.2, gdje su točkice izmjerene vrijednosti za koje vidimo da lijepo prate linearnu ovisnost, kao što je i očekivano. Statističke pogreške su kod svih vrijednosti jednake i iznose 0.000158. Nadalje, na Slici 5.3.a prikazane su vrijednosti relativne entropije H_{rel} za iste kombinacije p_0 i p_1, dok su na Slici 5.3.b prikazane pripadne statističke pogreške za dobivene vrijednosti relativnih entropija.



Slika 5.2: Rezultati mjerenja operacije zbrajanja za sklop MUX, za tri fiksne vrijednosti $p_0 = 0.2, 0.5, 0.8$ te različite vrijednosti p_1.



a) Entropijske vrijednosti za tri fiksne vrijednosti $p_0 = 0.2, 0.5, 0.8$ te različite vrijednosti p_1.



b) Statističke pogreške za entropijske vrijednosti za tri fiksne vrijednosti $p_0 = 0.2, 0.5, 0.8$ te različite vrijednosti p_1.

Slika 5.3: Entropijske vrijednosti i pripadne statističke pogreške za sklop MUX.

Sa prikazanih slika je vidljivo da ovaj sklop daje ispravne rezultate zbrajanja te da su izlazni RPT-ovi najslučajniji kada je rezultat zbrajanja $(p_0 + p_1)/2$ oko vrijednosti 0.5, što je očekivano jer je za tu vrijednost entropija najviša. Zbog toga se za fiksne vrijednosti ulazne vrijednosti p_0 stvaraju maksimumi na Slici 5.3.a upravo oko vrijednosti 0.5 za ovu operaciju zbrajanja. Analogno tome, za te se maksimume stvaraju minimumi na Slici 5.3.b jer su tada pripadne statističke pogreške naravno najmanje.

Iako su sve vrijednosti relativnih entropija blizu jedinice, bitno je primijetiti da svejedno postoji određena ovisnost, koju ova funkcija entropije prati. Takva ovisnost ne bi trebala postojati kod ovog sklopa zbog potpune slučajnosti, te bi vrijednosti trebale fluktuirati sa većim ili manjim pomacima od maksimalne entropije na slučajan način. Stoga je ovdje moguće pretpostaviti da je ovakva ovisnost značajna unutar granica statističke pogreške. Jedan od razloga postojanja ove ovisnosti je mogućnost da je funkcijska ovisnost posljedica same numeričke metode korištenih programa za izračun relativne entropije. Drugi razlog obuhvaća mogućnost postojanja određenih varijacija u relativnoj entropiji ulaznih nizova zbog rezidualnih[31] autokorelacija samih ulaza p_0 i p_1, te selektnog ulaza na MUX, koje mogu nastati zbog nesavršenosti mjerne aparature. Dodatni efekt mogu biti i međusobne

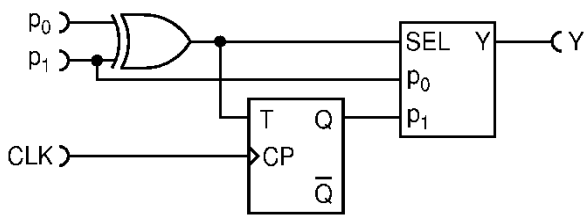
[31] Riječ *rezidualno* se odnosi samo na ulazne nizove.

korelacije[32], koje opisuju korelacije između dva nezavisna niza, npr. p_0 i p_1, no njihov utjecaj je vrlo mali pa one predstavljaju tek drugi red popravaka. Stoga, sve ove pretpostavke mogu biti predmet budućih istraživanja u ovoj tematici.

5.1.2 Deterministički sklop za zbrajanje s MUX-om

U referenci [19] opisan je deterministički sklop za zbrajanje čiju točnost smo provjerili, a entropijski budžet po prvi puta ispitivali. Sklop je prikazan na Slici 5.4, te je osmišljen kao poboljšana verzija sklopa MUX opisanog u potpoglavlju *4.2 Sklopovi za zbrajanje*, čiji rezultati su prezentirani u prethodnom potpoglavlju. Poboljšanje je napravljeno u smislu veće slučajnosti izlaznog niza, odnosno veće entropije, a na način da ne koristi dodatne izvore entropije osim entropije ulaznih RPT-ova. Time bi se postojeća količina entropije maksimalno iskoristila, a sklop bi trošio manje resursa, čime bi se ispunio treći uvjet prilikom kreiranja poboljšanih sklopova u uvodnom dijelu ovog poglavlja.

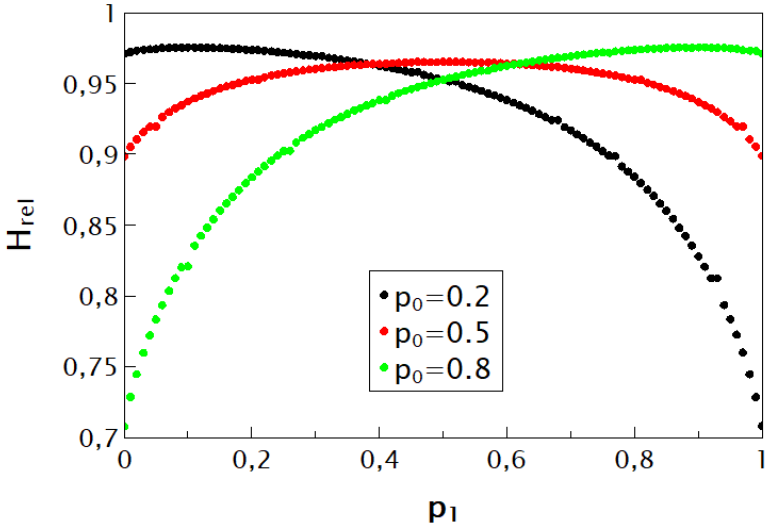
Sklop radi na principu toga što ulazne vrijednosti za MUX sklop više nisu slučajni RPT-ovi sa vjerojatnostima p_0 i p_1, već su one modificirane na način da je prvi ulaz RPT sa vjerojatnosti p_1, dok je drugi ulaz zapravo izlaz iz TFF-a čiji ulazi su taktni (CLK) signal i rezultat XOR-a između ulaznih RPT-ova sa vjerojatnostima p_0 i p_1. Taj rezultat XOR-iranja je ujedno i selektni signal MUX-a. Kada bi prvi ulaz na MUX bio RPT sa vjerojatnosti p_0, tada ovaj sklop ne bi davao ispravne rezultate jer su ulazi na MUX-u uvjetovani selektnim signalom.



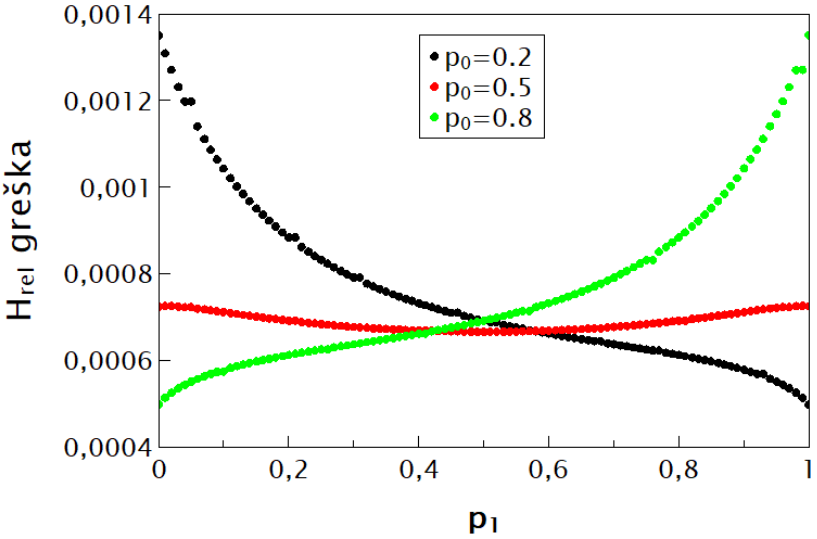
Slika 5.4: Shema sklopa za zbrajanje iz [19]. p_0 i p_1 su ulazne vrijednosti, a Y je rezultat zbrajanja ulaznih vrijednosti.

[32] Cross correlations (eng.)

Rezultati mjerenja su zadržali svoju preciznost pa stoga oni nisu uključeni u ovom dijelu, a vrijednosti relativnih entropija i pripadne statističke pogreške prikazane su na Slici 5.5. Iz dobivenih rezultata vidimo da je funkcijska ovisnost relativne entropije o ulaznoj vrijednosti p_1 izražena. Sa Slike 5.1 znamo da egzaktan deterministički sklop sa potpuno slučajnim impulsima ne postoji pa nam relativna entropija ukazuje na određene korelacije u izlaznom nizu. Svejedno, ovo je vrijedan sklop u impulsnom računanju jer ne koristi dodatan izvor entropije, a daje točne rezultate.



a) Entropijske vrijednosti za tri fiksne vrijednosti $p_0 = 0.2, 0.5, 0.8$ te različite vrijednosti p_1.

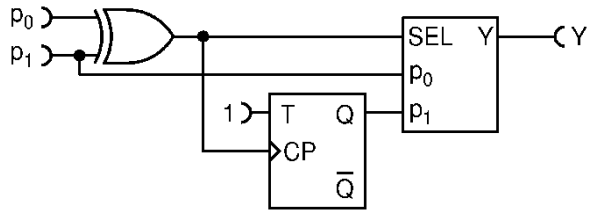


b) Statističke pogreške za entropijske vrijednosti za tri fiksne vrijednosti $p_0 = 0.2, 0.5, 0.8$ te različite vrijednosti p_1.

Slika 5.5: Entropijske vrijednosti i pripadne statističke pogreške za sklop na Slici 5.4.

5.1.3 Ekvivalentna verzija determinističkog sklopa s MUX-om

U RPC-u ne postoji jedinstveni sklop koji daje točno određene rezultate, već naizgled malo drugačiji sklop može davati jednake vrijednosti, a obavljati potpuno istu funkciju. Takav sklop je prikazan na Slici 5.6, a predstavlja ekvivalent prethodno opisanog sklopa za zbrajanje. Naime, jedina razlika je u ulaznim vrijednostima kod TFF-a jer je sada umjesto rezultata XOR-a na ulaz T stavljena jedinica, a rezultat XOR-a je stavljen na ulaz CP, gdje je prije bio taktni (CLK) signal.

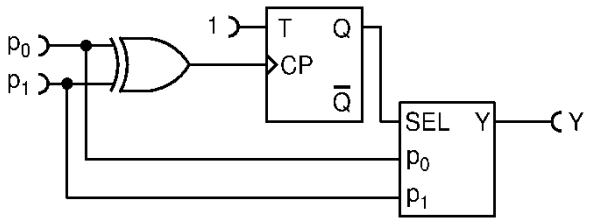


Slika 5.6: Ekvivalentna shema za sklop iz [19]. Jedina promjena su ulazne vrijednosti za T flip-flop.

Budući da je ova shema ekvivalentna shemi prvog sklopa za zbrajanje, rezultati su očekivano jednaki, odnosno apsolutno jednaki prethodnom sklopu, pa stoga nisu ponovo prezentirani ovdje. Ovo je bitan primjer raznovrsnosti RPC-a i mogućnosti koje otvara pomnim kombiniranjem logičkih vrata te njihovih ulaza i izlaza.

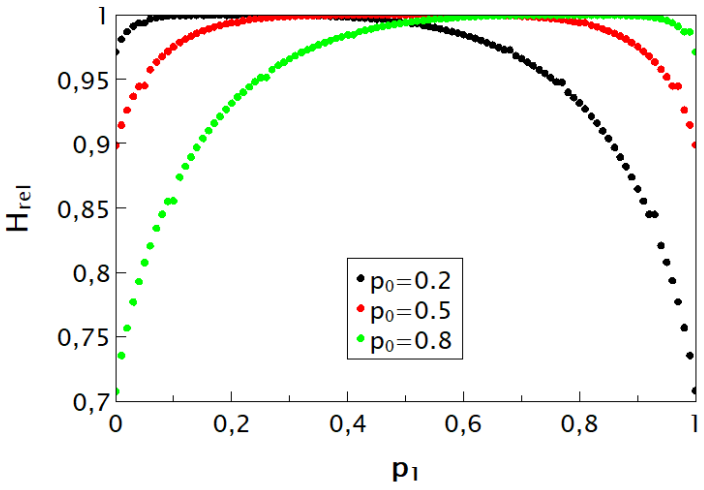
5.1.4 Prvo deterministično poboljšanje

S obzirom da deterministički sklop za zbrajanje daje točne rezultate zbrajanja i relativna entropija daje posljedično očekivane rezultate koji ukazuju na određene korelacije izlaznog signala, pokušali smo kreirati sklop koji će zadržati dobivenu računsku preciznost, a generirati slučajniji izlazni niz kako bi vrijednosti relativne entropije bile što bliže jedinici. Traženi sklop prikazan je na Slici 5.7. On je zapravo modificirana verzija ekvivalenta determinističkog sklopa s MUX-om, a razlika se krije u tome što su ulazi na MUX-u promijenjeni. Prije je p_1 bio spojen na prvi ulaz u MUX-u, a rezultat TFF-a na drugi, dok je XOR određivao selektno stanje. Sada su oba ulaza p_0 i p_1 spojena na ulaze MUX-a, dok je selektno stanje određeno stanjem na izlazu TFF-a.

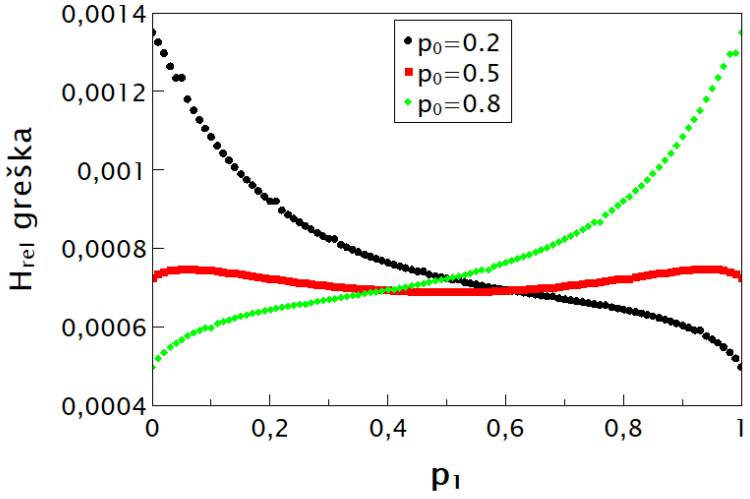


Slika 5.7: Shema deterministički poboljšanog sklopa s MUX-om.

Ovime je postignuta jednaka točnost, a entropijske vrijednosti su prikazane na Slici 5.8. Vrijednosti relativnih entropija su jednake jedinici u otprilike 50% kombinacija ulaznih vrijednosti p_0 i p_1, dok prethodno opisani sklop u potpoglavlju *5.1.2 Deterministički sklop za zbrajanje s MUX-om* ne doseže vrijednost jedan niti u jednom slučaju. Zbog toga je ovaj sklop prihvatljiviji kao izbor za povezivanje različitih operacija radi rješavanja neke složenije funkcije.



a) Entropijske vrijednosti za tri fiksne vrijednosti $p_0 = 0.2, 0.5, 0.8$ te različite vrijednosti p_1.



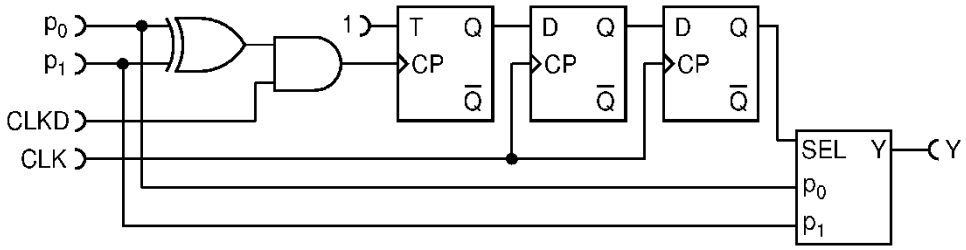
b) Statističke pogreške za entropijske vrijednosti za tri fiksne vrijednosti $p_0 = 0.2, 0.5, 0.8$ te različite vrijednosti p_1.

Slika 5.8: Entropijske vrijednosti i pripadne statističke pogreške za sklop na Slici 5.7.

5.1.5 Drugo deterministično poboljšanje

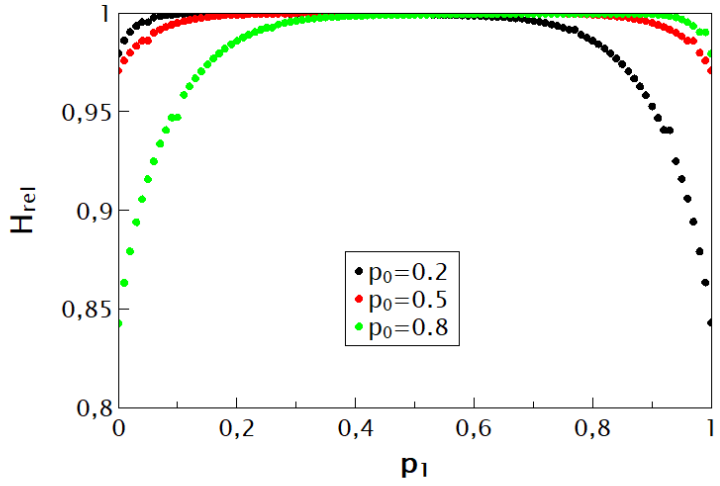
Iako prethodno opisani sklop daje točne rezultate i visoke vrijednosti relativne entropije, sada se pitamo mogu li se vrijednosti relativne entropije još više približiti jedinici za sve kombinacije za koje to nije bilo ispunjeno. Zbog toga je uvedeno poboljšanje u smislu veće slučajnosti odabira izlaznih impulsa u MUX-u, a ono je postignuto pomoću zakašnjavanja izlaza iz XOR-a za dva perioda. Sklop je prikazan na Slici 5.9. Prvo je izlazni signal iz XOR-a pomnožen sa taktnim signalom zakašnjelim za $1/4$ perioda, potom taj pomnoženi signal predstavlja taktni ulaz u TFF, čiji ulaz T je postavljen na jedinicu. Tako je izlazni signal iz TFF-a zakašnjen za $1/4$ perioda pa ga je potrebno zakasniti još za jedan cijeli period i $3/4$. Ta kašnjenja su postignuta pomoću dva DFF-a. D flip-flopovi inače služe za zakašnjavanje signala, a rade samo ako ulaz D nije na prijelazu stanja jer tada se može dogoditi da se dobro ne očita stanje. Naime, da bi se stanje ustabililo potrebno je određeno kratko, ali konačno vrijeme pa da bismo to izbjegli, odmah smo zakasnili signal iz XOR-a za $1/4$, čime smo dobili duplo kraće pulseve, ali sa trenucima promjene stanja usred stabilnosti impulsa na ulazu u D. Posebno je bitno napomenuti da su svi sklopovi namješteni da rade samo na promjeni stanja iz niskog u visoko. Zbog toga smo signal zakasnili, a ne uranili za $1/4$. DFF zakasni signal za proizvoljan dio perioda, ovisno o ulaznom signalu na

ulazu D, pa je tako nakon prvog DFF-a, signal iz TFF-a zakašnjen sveukupno za cijeli period, a nakon drugog DFF-a za dva puna perioda zato što je izlaz iz prvog DFF-a već poravnat sa taktnim signalom pa ga drugi DFF može zakasniti samo za puni period. Točnije, prvi DFF je signal iz TFF-a zakasnio za $3/4$ perioda, a drugi za još jedan cijeli period pa je ukupno kašnjenje na izlazu iz drugog DFF-a u odnosu na izlaz iz XOR-a puna dva perioda.

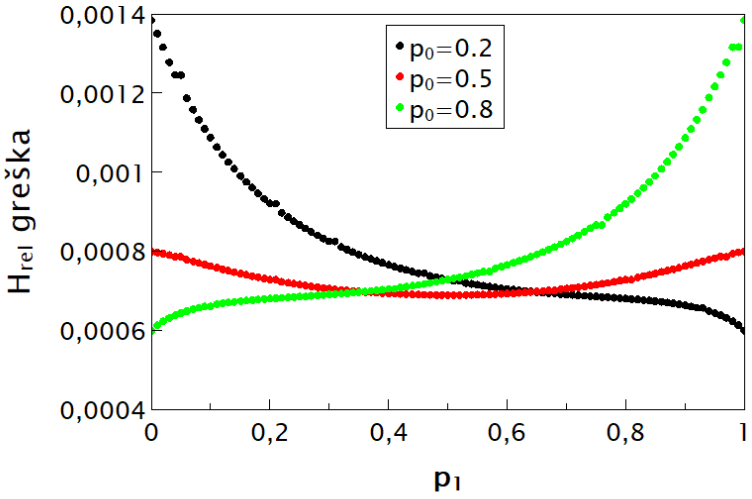


Slika 5.9: Shema poboljšanog sklopa za zbrajanje u odnosu na drugi sklop sa Slike 5.6.

Preciznost rezultata operacije zbrajanja je zadržala svoju točnost, ali entropijske vrijednosti su se promijenili te su prikazane na Slici 5.10. Sa slika vidimo da su se vrijednosti relativnih entropija još više približile jedinici, čime smo postigli maksimalno slučajan izlazni RPT s najmanjim utroškom resursa uz zadržanu preciznost računa i minimalne statističke pogreške. Naravno, za ovakav sklop smo i očekivali najslučajniji izlazni RPT jer odabirom selektnog ulaza na MUX-u, koji je dobiven operacijom XOR-a prethodnih impulsa, dobivamo slučajnije rezultate od selektnog ulaza koji je dobiven kao XOR trenutnih ulaznih impulsa, što je bio slučaj u prethodno opisanom sklopu. Time je ovaj sklop najbolji deterministički sklop za zbrajanje.



a) Entropijske vrijednosti za tri fiksne vrijednosti $p_0 = 0.2, 0.5, 0.8$ te različite vrijednosti p_1.

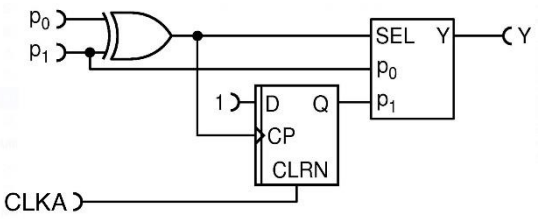


b) Statističke pogreške za entropijske vrijednosti za tri fiksne vrijednosti $p_0 = 0.2, 0.5, 0.8$ te različite vrijednosti p_1.

Slika 5.10: Entropijske vrijednosti i pripadne statističke pogreške za sklop na Slici 5.9.

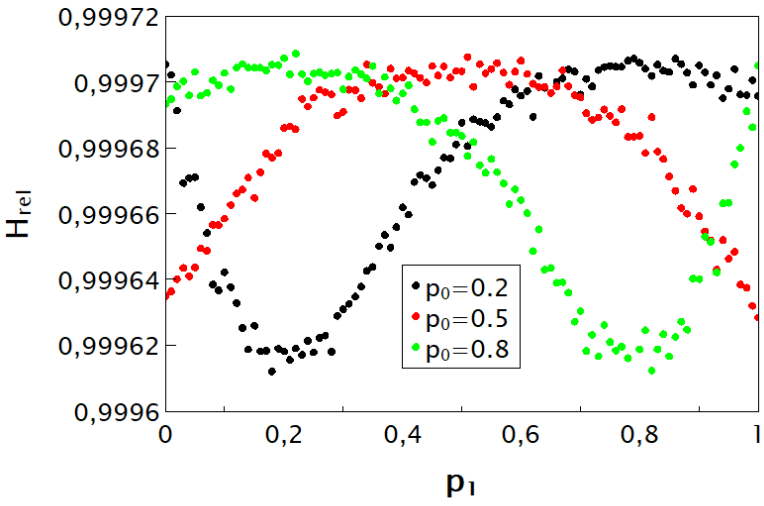
5.1.6 Nedeterminističko poboljšanje

Deterministički sklop za zbrajanje daje zadovoljavajuće vrijednosti na oba područja – rezultati zbrajanja i entropijske vrijednosti. No, postavlja se pitanje da li se te vrijednosti mogu dodatno unaprijediti uvođenjem dodatne entropije u sami sklop. Poboljšana nedeterministička verzija prikazana je na Slici 5.11.

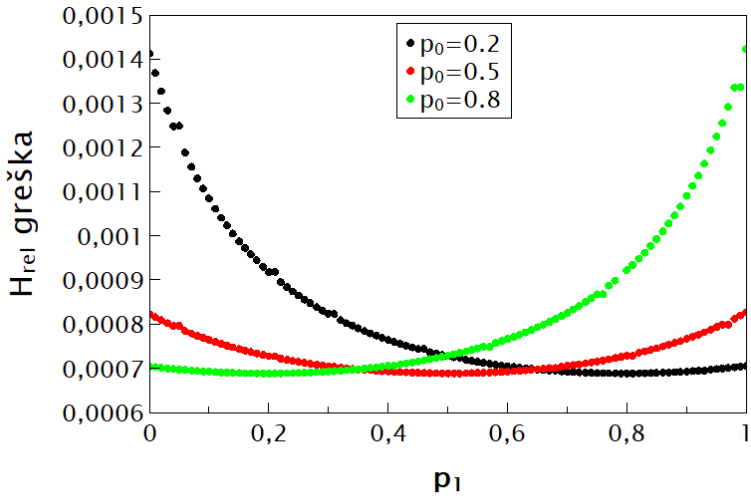


Slika 5.11. Shema nedeterministički poboljšanog sklopa s MUX-om.

Ovaj sklop je naslijedio preciznost i točnost originalne verzije, a entropijske vrijednosti su pokazale zadovoljavajuću slučajnost te su prikazane na Slici 5.12. Rezultati su očekivano najbliži jedinici za sve kombinacije ulaznih vrijednosti p_0 i p_1 s obzirom da je uvedena dodatna entropija. Upravo zbog korištenja te dodatne entropije, rezultati opisuju isti trend kao i kod samog sklopa za zbrajanje s MUX-om. Prednost ovog sklopa u odnosu na sami sklop za zbrajanje s MUX-om je u tome što ovdje imamo uštedu entropije, zbog toga što iskorištavamo entropije ulaznih nizova p_0 i p_1 kroz XOR vrata, koja predstavljaju selektni ulaz MUX_a. Zbog entropije, ovaj sklop otvara novu perspektivu u shvaćanju impulsnog računanja.



a) Entropijske vrijednosti za tri fiksne vrijednosti $p_0 = 0.2, 0.5, 0.8$ te različite vrijednosti p_1.



b) Statističke pogreške za entropijske vrijednosti za tri fiksne vrijednosti $p_0 = 0.2, 0.5, 0.8$ te različite vrijednosti p_1.

Slika 5.12: Entropijske vrijednosti i pripadne statističke pogreške za sklop na Slici 5.11.

5.2 Primjena zbrajanja kod kvadratne funkcije

Sveukupan cilj pronalaska sklopova koji daju najmanje korelirane izlazne nizove sa najvećom mogućom entropijom uz precizne računske rezultate je mogućnost kombiniranja sklopova za različite računske operacije u svrhu rješavanja kompliciranih funkcija poput polinoma [20]. Zbog toga je u ovom poglavlju opisana i objašnjena primjena najbolje ocijenjenih sklopova iz prethodnog potpoglavlja na primjeru rješavanja kvadratne funkcije sljedećeg oblika:

$$f(p) = \frac{p^2 + p}{2}, \tag{5.4}$$

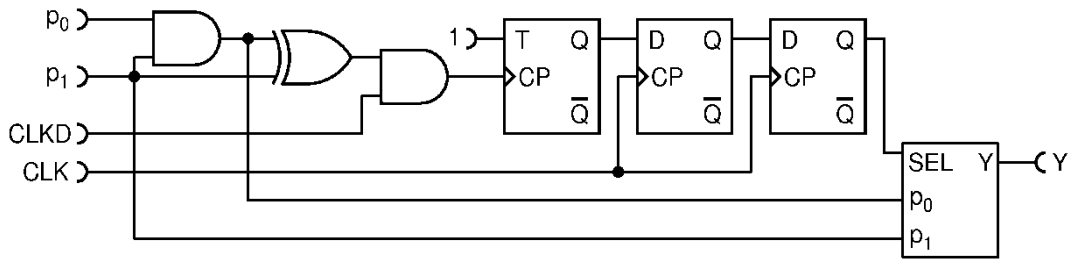
pri čemu je $p \in [0,,1]$ vjerojatnost pojavljivanja impulsa. Ova funkcija je izabrana jer mora sadržavati zbrajanje s obzirom da je to operacija koju proučavamo te množenje kao najjednostavniji i najpouzdaniji sklop za računske operacije.

U nastavku su prikazani rezultati za posljednja dva sklopa iz prethodnog potpoglavlja, a to su sklop iz drugog determinističkog poboljšanja i sklop iz nedeterminističkog poboljšanja. Netko se može pitati zašto baš sklop iz nedeterminističkog

poboljšanja s obzirom da on daje jednake autokorelacijske koeficijente kao i sam sklop MUX. Razlog tomu je što je kompliciraniji sklop sa više logičkih vrata skloniji autokorelacijama pa je stoga bitno proučiti ponašanje takvog sklopa u kombinaciji s drugima kako bi se spoznale njegove granice jer za sami MUX sigurno znamo da u kombinaciji s drugim logičkim vratima daje ispravne rezultate, što i taj sam sklop potvrđuje.

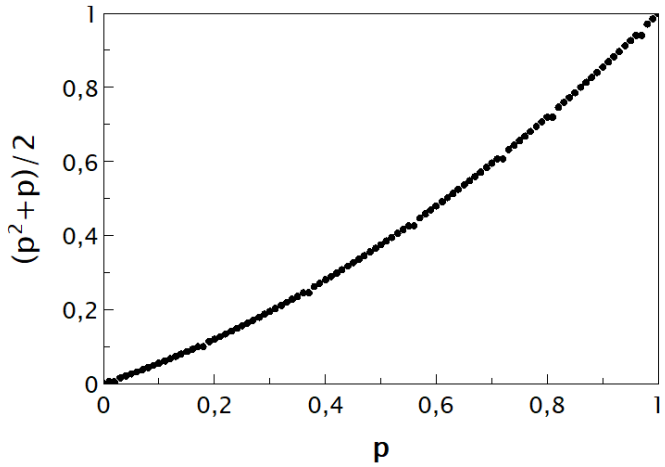
5.2.1 Deterministički sklop

Sklop za računanje odabrane kvadratne funkcije, koji sadrži deterministički sklop, prikazan je na Slici 5.13.

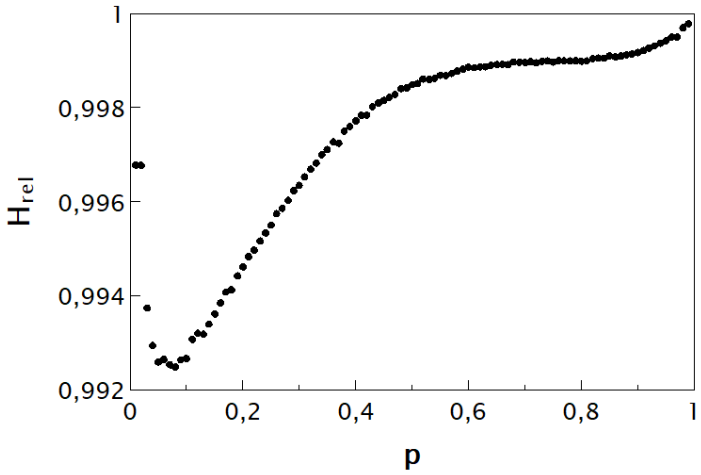


Slika 5.13: Shema sklopa za računanje kvadratne funkcije $f(p) = (p^2 + p)/2$ korištenjem determinističkog sklopa za zbrajanje opisanog u potpoglavlju *4.2.5 Drugo deterministično poboljšanje.*

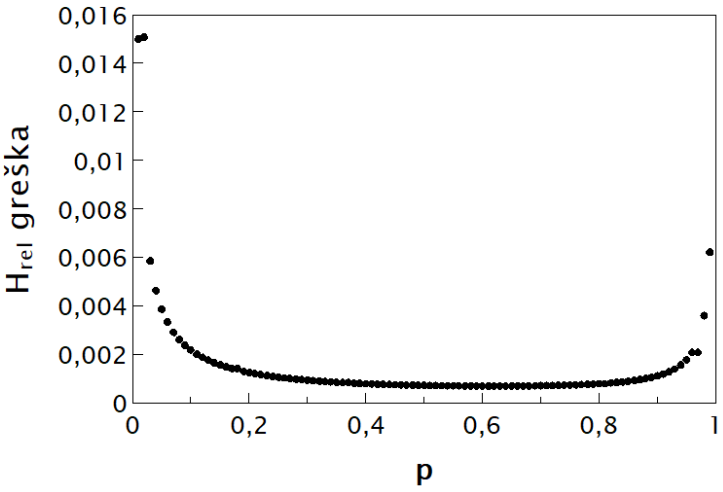
Rezultati kvadratne funkcije korištenjem determinističkog sklopa opisanog u potpoglavlju *4.2.5 Drugo deterministično poboljšanje* prikazani su na Slici 5.14, dok su entropijske vrijednosti izlaznog niza i pripadne statističke pogreške prikazane redom na Slikama 5.15.a i 5.15.b. Sa Slike 5.13 je jasno vidljivo da rezultati pokazuju kvadratnu krivulju, što je i bio cilj. Zanimljivo je primijetiti kako entropijska krivlja neprestano raste nakon što se prijeđe vrijednost $p = 0.1$. Razlog tome je što jedan ulazni RPT u sklop za zbrajanje više nema maksimalnu entropiju nego mu se ona smanjila nakon prolaska kroz logička AND vrata, koja označavaju množenje. Zbog toga je izuzetno bitno maksimizirati entropiju izlaznih nizova kako bi oni predstavljali što vjerodostojnije ulaze u druge sklopove. U suprotnom se dio informacije gubi.



Slika 5.14: Rezultati rješavanja kvadratne funkcije $f(p) = (p^2 + p)/2$ za različite vrijednosti vjerojatnosti p korištenjem determinističkog sklopa opisanog u potpoglavlju *4.2.5 Drugo deterministično poboljšanje*.



a) Entropijske vrijednosti.

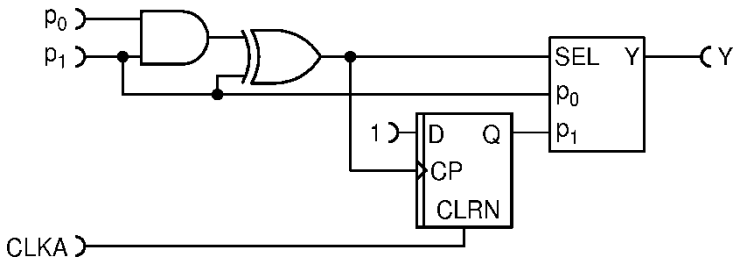


b) Statističke pogreške za entropijskih vrijednosti.

Slika 5.15: Entropijske vrijednosti i pripadne statističke pogreške nakon rješavanja kvadratne funkcije $f(p) = (p^2 + p)/2$ za različite vrijednosti vjerojatnosti p korištenjem deterministčkog sklopa opisanog u potpoglavlju *4.2.5 Drugo determinističko poboljšanje*.

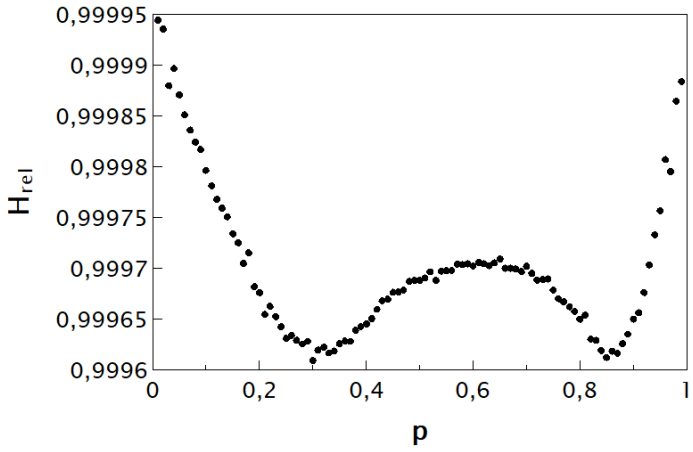
5.2.2 Nedeterministički sklop

Sklop za kvadratnu funkciju dobivenu korištenjem nedeterminističkog sklopa opisanog u potpoglavlju *4.2.6 Nedeterminističko poboljšanje* i logičkih AND vrata prikazan je na Slici 5.16.

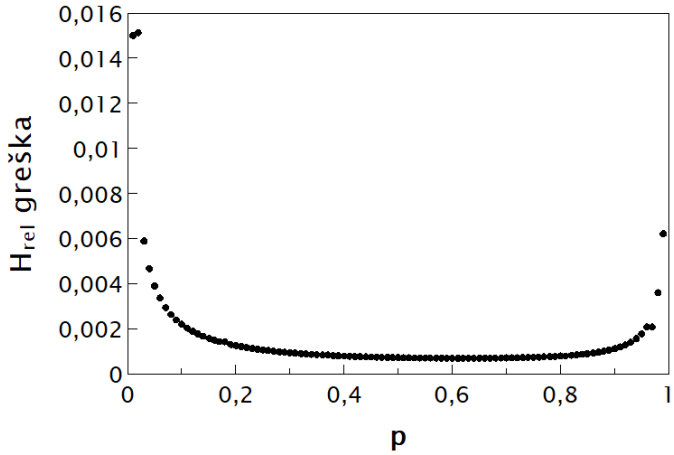


Slika 5.16: Shema sklopa za računanje kvadratne funkcije $f(p) = (p^2 + p)/2$ korištenjem deterministčkog sklopa za zbrajanje opisanog u potpoglavlju *4.2.6 Nedeterminističko poboljšanje*.

Rezultati su pokazali potpuno isto ponašanje kao i rezultati kvadratne funkcije determinističkog sklopa. Stoga rješenja kvadratne funkcije nisu ovdje ponovo prikazivane. Kako i kod samih sklopova za zbrajanje, ono što čini razliku su vrijednosti relativnih entropija. Na Slici 5.17 prikazane su entropijske vrijednosti i pripadne statističke pogreške.



a) Entropijske vrijednosti.



b) Statističke pogreške za entropijske vrijednosti.

Slika 5.17: Entropijske vrijednosti i pripadne statističke pogreške nakon rješavanja kvadratne funkcije $f(p) = (p^2 + p)/2$ za različite vrijednosti vjerojatnosti p korištenjem nedeterminističkog sklopa opisanog u potpoglavlju *4.2.6 Nedeterminističko poboljšanje*.

Sa Slike 5.17.a je vidljivo da postoji određeni trend kojega prikazane vrijednosti prate. Usporedbom sa prethodnim sklopom vidimo da su entropijske vrijednosti bliže jedinici u ovom slučaju. Iz toga zaključujemo da je nedeterministički sklop ipak pogodniji

za korištenje u RPC-u jer, iako koristi dodatnu entropiju, najvažniji je dobiveni rezultat i mogućnost daljnje upotrebe radi stvaranja univerzalnog RPC računala.

6 Diskusija i zaključak

Elektronički sklopovi za matematičke operacije u impulsnom računanju predmet su istraživanja radi izgradnje univerzalnog RPC računala, koje radi na principu živčanog sustava živih bića jer se električni impulsi u mozgu propagiraju na način veoma sličan logičkim impulsima. U ovom radu proučavali smo relativne entropije deterministčkih i nedeterminističkih elektroničkih sklopova za zbrajanje, te uporabu najkvalitetnije ocijenjenih sklopova u impulsnom računanju kroz kombiniranje sa sklopovima drugih matematičkih operacija, konkretno množenjem.

Relativna entropija je novi koncept koji opisuje omjer između Kolmogorov-Sinai entropije i Shannonove entropije definirane za niz duljine jedan, a služi za karakterizaciju slučajnosti izlaznog niza nakon obavljanja određene matematičke operacije. Što veća slučajnost je potrebna kako bi se dane matematičke operacije mogle povezati u cjelinu radi rješavanja kompleksnijih problema poput polinoma. Dobiveno je da su vrijednosti relativnih entropija najbliže jedinici u slučaju drugog deterministčkog poboljšanja i nedeterminističkog poboljšanja. Nedeterminističko poboljšanje daje svakako vrijednosti bliže jedinici od deterministčkog poboljšanja s obzirom da koristi izvor dodatne entropije, a to je D slučajni flip-flop. Samo korištenje entropije ulaznih nizova nije dostatno za zadovoljavanje kriterija entropijskog budžeta, kao što je i prikazano u ovom radu. Nadalje, ti sklopovi su ukomponirani sa sklopom za zbrajanje radi rješavanja zadanog polinoma i dobiveno je da je svakako veća izlazna slučajnost niza nedeterminističkog sklopa, kao što je očekivano. Nadasve je bitno spomenuti da dobivene funkcijske ovisnosti relativne entropije nedeterminističkih sklopova o ulaznom nizu nisu statistički značajne, što nije slučaj kod deterministčkih sklopova. To je dodatan razlog koji ukazuje da je nedeterministički sklop kvalitetnija opcija za izgradnju univerzalnog RPC računala.

Za kraj, potrebno je istaknuti da statističke pogreške relativnih entropija kod većine sklopova također prate određeni trend, neovisno o tome da li je sklop deterministički ili nedeterministički. Taj trend može predstavljati uvid u moguća daljnja poboljšanja sklopova radi postizanja veće slučajnosti izlaznih nizova, te napredniju konstrukciju dosad poznatih sklopova, kako bi se različite matematičke operacije mogle povezati za preciznije rješavanje raznih problema. Time bi se stvorila prednost pred ostalim računalnim paradigmama, a primjene takve paradigme sezale bi od umjetne inteligencije jakih karakteristika do boljeg razumijevanja neurona i načina rada ljudskog mozga [7].

Dodaci

Dodatak A: Eksponencijalna distribucija

Eksponencijalna distribucija [14] je posljedica slučajnosti i međusobne neovisnosti fotokonverzija uzrokovanih konstantnom jačinom svjetlosti koja pada na detektore fotona. Osnovne pretpostavke koje opisuju izvor slučajnih događaja su sljedeće:

I. Vjerojatnost da će se slučajni događaj dogoditi u sljedećih Δt vremena jednaka je $\lambda \Delta t$ u granici $\Delta t \rightarrow 0$, neovisno o trenutku promatranja.

II. Veličina λ je konstantna u vremenu.

III. Slučajni događaji su međusobno nezavisni.

Slučajni događaji koji sačinjavaju niz slučajnih impulsa predstavljaju samu jezgru ovog rada, a u realizaciji su to detekcije fotona. Zbog toga želimo pronaći funkciju gustoće vjerojatnosti duljine intervala između susjednih događaja $F(t)$. Za početak pretpostavimo da se jedan slučajni događaj dogodio u trenutku $t = 0$. Pitamo se kolika je vjerojatnost da se sljedeći događaj dogodi nakon vremena t. Prema uvjetu III, zbog međusobne neovisnosti događaja, vjerojatnost pojavljivanja slučajnog događaja nakon vremena t jednaka je umnošku vjerojatnosti da se taj događaj dogodio neposredno *nakon* vremena t i vjerojatnosti da se niti jedan događaj *nije* dogodio do trenutka t. Da bismo to izračunali, prvo trebamo podijeliti promatrano vrijeme t na N kratkih vremenskih intervala $\Delta t = t/N$, pri čemu je N proizvoljan veliki prirodan broj. Posljedično, vjerojatnost da se događaj dogodio u kratkom vremenskom intervalu iznosi $\lambda \Delta t$, dok je vjerojatnost da se događaj nije dogodio u tom istom vremenskom intervalu jednaka $1 - \lambda \Delta t$. S obzirom da tih kratkih vremenskih intervala ima N, tada je ukupna vjerojatnost da se niti jedan događaj nije dogodio tokom cijelog trajanja vremena jednaka $(1 - \lambda \Delta t)^N$. Konačno, ukupna vjerojatnost pojavljivanja dva susjedna događaja udaljena za vremenski interval t jednaka je

$$p = (1 - \lambda \Delta t)^N \lambda \Delta t, \tag{A.1}$$

gdje p predstavlja vjerojatnost da se događaj dogodi u intervalu (0,t), što se može zapisati kao umnožak tražene funkcije gustoće vjerojatnosti $F(t)$ i kratkog vremenskog intervala Δt. Uzimajući u obzir da je $\Delta t = t/N$, slijedi da je

$$F(t)\Delta t = \left(1 - \lambda\frac{t}{N}\right)^{N} \lambda\Delta t. \tag{A.2}$$

U granici kada $N \to \infty$, dobivamo

$$F(t) = \lambda \lim_{N\to\infty} \left(1 - \lambda\frac{t}{N}\right)^{N}. \tag{A.3}$$

Svodeći prethodni izraz na relaciju pogodnu za korištenje Eulerove formule, uvodimo supstituciju $n = -N/\lambda t$, čime prethodni izraz prelazi u

$$F(t) = \lambda \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^{-\lambda t n}. \tag{A.4}$$

Korištenjem Eulerove formule dobivamo

$$F(t) = \lambda e^{-\lambda t}. \tag{A.5}$$

Dobivena funkcija gustoće vjerojatnosti je eksponencijalna i opisuje slučajno distribuirane događaje u vremenu pa je proces koji generira ovakve događaje upravo Poissonov proces.

Dodatak B: Boolova logika

Boolova logika opisuje jednostavne sklopove koji predstavljaju logičke operacije Boolove algebre. U osnovne sklopove spadaju AND, OR i NOT, a u ostale jednostavne sklopove još ulaze NAND, NOR, XOR i XNOR. U nastavku su osnovni logički sklopovi AND i OR opisani detaljno u digitalno logici (DRL[33]), logički NOT sklop u RTL[34] logici, a ostali jednostavni sklopovi su samo prikazani simbolički s pripadnim tablicama istinitosti. Iako je danas uglavnom u uporabi CMOS[35] logika, DRL logika koristi diode i otpornike kojima je jednostavnije ilustrirati rad osnovnih sklopova u odnosu na CMOS tranzistore koje koristi CMOS logika. U daljnjim shemama DRL logike, R označava otpor iznosa $R \simeq 5\ k\Omega$, R_s je unutarnji otpor iznosa $R_s \simeq 100\ k\Omega$, $D1$ i $D2$ predstavljaju diode, a naponi su označeni slovom V. Visoki napon predstavlja logičku jedinicu i obično iznosi $V(1) = 5\ V$, a niski logičku nulu s naponom od $V(0) = 0\ V$. Pritom se pretpostavlja idealna I-R karakteristika diode [11].

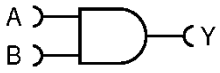
B.1 AND (I) logička vrata (konjukcija)

Logička AND (I) vrata prikazana su na Slici B.1.a i predstavljaju operaciju konjukcije u Boolovoj algebri. Ta operacija nam govori da je stanje na izlazu visoko (jedan) samo ako su oba ulaza na visokom stanju (jedan), kao što je vidljivo u pripadnoj tablici istinitosti na Slici B.1.b. Izvedbena shema prikazana je na Slici B.1.c, s koje vidimo da, ako je na barem jednom od ulaza A i B napon $V(0)$, tada je i napon na izlazu Y jednak $V(0)$. Jedino u slučaju kada je napon na oba ulaza A i B jednak $V(1)$, tada je i napon na izlazu $V(1)$. U tom slučaju se naponi na ulazima A i B jedino mogu razlikovati u šumu pa je, posljedično, napon na izlazu Y tada jednak nižem naponu od ta dva. Zaključno, napon na izlazu Y uvijek je jednak najmanjem naponu danom na ulazima A i B [11].

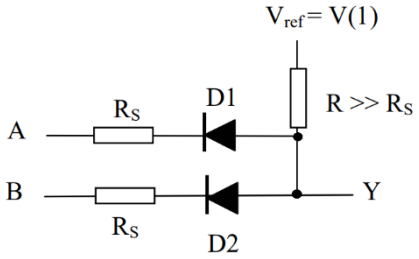
[33] Diode resistor logic (eng.)

[34] Resistor transistor logic (eng.)

[35] Complementary Metal Oxide Semiconductor (eng.)



A	B	Y
0	0	0
0	1	0
1	0	0
1	1	1



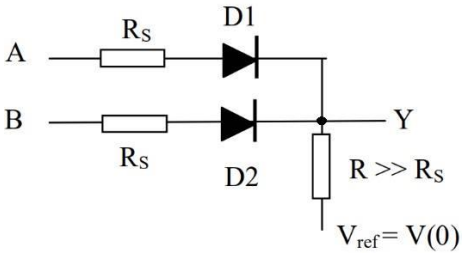
(a) Oznaka za konjukciju. (b) Tablica istinitosti za konjukciju. (c) Izvedbena shema konjukcije.

Slika B.1: Grafički prikaz logičkih AND (I) vrata sa pripadnom tablicom istinitosti i izvedbenom shemom u DRL logici. A i B predstavljaju ulaze, a Y predstavlja izlaz.

B.2 OR (ILI) logička vrata (disjunkcija)

Logička OR (ILI) vrata prikazana na Slici B.2.a predstavljaju operaciju disjunkcije u Boolovoj algebri, koja nam govori da je stanje na izlazu visoko ukoliko je barem jedno od ulaznih stanja visoko, tj. na logičkoj jedinici. Pripadna tablica istinitosti prikazana je na Slici B.2.b, dok je izvedbena shema disjunkcije u DRL logici prikazana na Slici B.2.c. S izvedbene sheme jasno vidimo kada je napon na barem jednom od ulaza A i B jednak $V(1)$, tada je izlazni napon $V(1)$. U jedinom slučaju, kada su oba ulazna napona $V(0)$, izlazni napon je nizak tj. na logičkoj nuli, što je lijepo sažeto u tablici istinitosti. Suprotno od konjukcije, u izvedbi disjunkcije je izlazni napon uvijek jednak najvišem ulaznom naponu [11].

A	B	Y
0	0	0
0	1	1
1	0	1
1	1	0

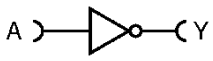


(a) Oznaka za disjunkciju. (b) Tablica istinitosti za disjunkciju. (c) Izvedbena shema disjunkcije.

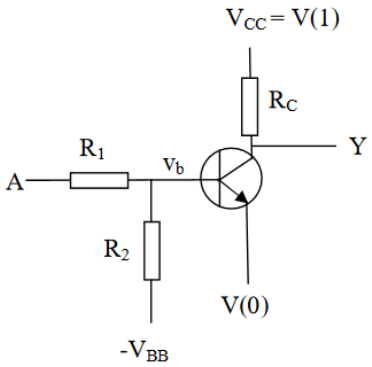
Slika B.2: Grafički prikaz logičkih OR (ILI) vrata sa pripadnom tablicom istinitosti i izvedbenom shemom u DRL logici. A i B predstavljaju ulaze, a Y predstavlja izlaz.

B.3 NOT (NE) logička vrata (negacija)

Logička NOT (NE) vrata su prikazana na Slici B.3.a, a predstavljaju operaciju negacije u Boolovoj algebri, koja okreće ulazne vrijednosti. Dakle, visoko stanje se mijenja u nisko i obrnuto, što je prikazano u tablici istinitosti na Slici B.3.b. Izvedbena shema negacije u RTL logici prikazana je na Slici B.3.c, a ostvarena je pomoću BJT[36] tranzistora, koji koristi i elektrone i šupljine kao nosioce naboja za kontroliranje struje i napona koji prolaze [11].



A	Y
0	1
1	0



(a) Oznaka za negaciju. (b) Tablica istinitosti za negaciju. (c) Izvedbena shema negacije.

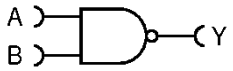
Slika B.3: Grafički prikaz logičkih NOT (NE) vrata sa pripadnom tablicom istinitosti i izvedbenom shemom u RTL logici. A predstavlja ulaz, a Y predstavlja izlaz.

B.4 Ostali jednostavni logički sklopovi

Logička NAND, NOR, XOR i XNOR vrata spadaju u jednostavne logičke sklopove, a nastala su kao spoj osnovnih logičkih sklopova. Zbog toga za njih ne ćemo prikazivati izvedbenu logiku već samo njihove simbole i pripadne tablice istinitosti.

NAND vrata su spoj logičkih AND vrata i logičkih NOT vrata, dok su NOR vrata kombinacija logičkih OR i logičkih NOT vrata. Zbog toga su njihove tablice istinitosti obrnute od AND i OR vrata, a oznake i pripadne tablice istinitosti prikazane su na Slikama B.4 i B.5.

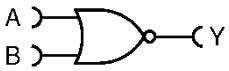
[36] Bipolar junction transistor (eng.)



A	B	Y
0	0	1
0	1	1
1	0	1
1	1	0

(a) Oznaka logičkih NAND vrata. (b) Tablica istinitosti logičkih NAND vrata.

Slika B.4: Grafički prikaz logičkih NAND vrata sa pripadnom tablicom istinitosti. A i B predstavljaju ulaze, a Y predstavlja izlaz.



A	B	Y
0	0	1
0	1	0
1	0	0
1	1	0

(a) Oznaka logičkih NOR vrata. (b) Tablica istinitosti logičkih NOR vrata.

Slika B.5: Grafički prikaz logičkih NOR vrata sa pripadnom tablicom istinitosti. A i B predstavljaju ulaze, a Y predstavlja izlaz.

XOR (isključiv[37] OR) vrata se ponašaju slično kao i logička OR vrata, uz jednu razliku, a to je da je na izlazu logička jedinica jedino kada je samo jedno od ulaznih stanja visoko, tj. na logičkoj jedinici. U slučaju kada su oba ulazna stanja jednaka, tada je izlazno stanje nisko, tj. na logičkoj nuli. Nadalje, XNOR vrata su tada samo kombinacija logičkih XOR i NOT vrata pa je pripadna tablica istinitosti XNOR vrata obrnuta od tablice istinitosti XOR vrata. Na Slikama B.6 i B.7 prikazane su oznake za logička XOR i XNOR vrata zajedno sa opisanim tablicama istinitosti.

[37] Exclusive (eng.)

A	B	Y
0	0	0
0	1	1
1	0	1
1	1	0

(a) Oznaka logičkih XOR vrata. (b) Tablica istinitosti logičkih XOR vrata.

Slika B.6. Grafički prikaz logičkih XOR vrata sa pripadnom tablicom istinitosti. A i B predstavljaju ulaz, a Y predstavlja izlaz.

A	B	Y
0	0	1
0	1	0
1	0	0
1	1	1

(a) Oznaka logičkih XNOR vrata. (b) Tablica istinitosti logičkih XNOR vrata..

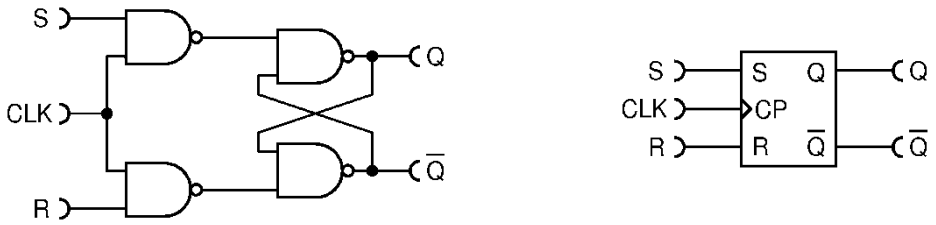
Slika B.7. Grafički prikaz logičkih XNOR vrata sa pripadnom tablicom istinitosti. A i B predstavljaju ulaz, a Y predstavlja izlaz.

Dodatak C: Flip-flopovi

Flip-flop je je jedan od osnovnih sklopova sekvencijalne logike koji ima dva stabilna stanja i može se koristiti za pohranu informacija. Postoje četiri osnovne vrste flip-flopova: SR flip-flop, JK flip-flop, D flip-flop i T flip-flop. U poglavlju *Slučajni flip-flop* opisani su T flip-flop i D flip-flop pa su ovdje opisana preostala dva tipa. Za sve flip-flopove treba postaviti inicijalne uvjete i na ulazima i na izlazima.

C.1 SR flip-flop

SR (Set-Reset) flip-flop se sastoji od četiriju NAND vrata povezanih međusobno i ulaznog taktnog (CLK) signala, kao što je prikazano na Slici C.1.a, dok je njegov simbol prikazan na Slici C.1.b. Pretpostavimo li da je na ulazu S visoko stanje, a na ulazu R nisko te da je taktni signal također na logičkoj jedinici, kao i početno stanje na izlazu Q, dok je stanje na izlazu $\overline{Q}$ nisko, slijedi da je stanje na izlazu Q visoko, a stanje na izlazu $\overline{Q}$ nisko. Daljnjom promjenom ulaznih vrijednosti S i R, mijenjaju se stanja na izlazima Q i $\overline{Q}$.



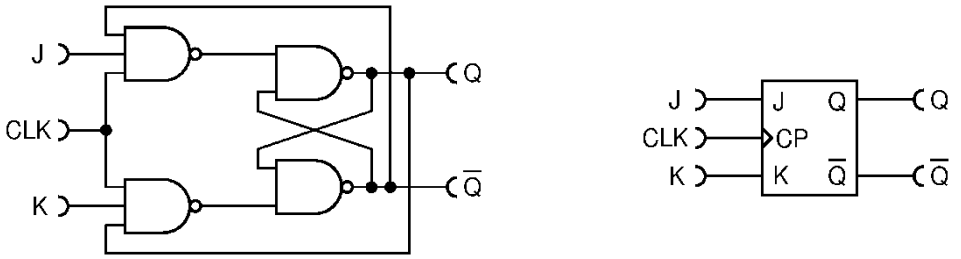
(a) Shema SR flip-flopa. (b) Simbol SR flip-flopa.

Slika C.1: Grafički prikaz SR flip-flopa. S (set) i R (reset) predstavljaju ulaze, CLK je taktni signal, a Q i $\overline{Q}$ predstavljaju izlaze.

C.2 JK flip-flop

JK flip-flop se kao i SR flip-flop sastoji od četiriju NAND vrata koja su međusobno povezana na jednak način kao i kod SR flip-flopa. Jedina je razlika što su ulazna NAND vrata dodatno povezana sa izlazima Q i $\overline{Q}$. Zbog toga JK flip-flop funkcionira na isti način kao i JK flip-flop. Možemo reći da je JK flip-flop naslijedio ponašanje SR flip-flopa. Dakle, ako pretpostavimo da su izlazna stanja Q i $\overline{Q}$ redom npr. 1 i 0, te ulazna

stanja J i K redom npr. 1 i 0, a CLK je na visokom stanju, tada izlazna stanja Q i $\overline{Q}$ ostaju nepromijenjena. Na Slici C.2.a prikazan je shematski JK flip-flop, a njegov simbol na Slici C.2.b.



(a) Shema JK flip-flopa. (b) Simbol JK flip-flopa.

Slika C.2: Grafički prikaz JK flip-flopa. J i K predstavljaju ulaze, CLK je taktni signal, a Q i $\overline{Q}$ predstavljaju izlaze.

C.3 Univerzalni flip-flop

Lako je vidljivo da sve četiri vrste flip-flopova imaju zajedničke elemente pa nije iznenađujuće što univerzalan flip-flop postoji. Posebno je zanimljivo što je univerzalan flip-flop upravo JK flip-flop. Da bismo JK flip-flop postavili kao SR flip-flop, potrebno je uvjet J = K = 1 interpretirati kao naredbu za prebacivanje flip-flopa, točnije za promjenu njegovog izlaza u logički komplement. U tom slučaju je kombinacija J = 1 i K = 0 naredba za postavljanje flip-flopa (set), a kombinacija J = 0 i K = 1 naredba za resetiranje flip-flopa (reset). Posljednja kombinacija J = K = 0 samo održava postojeće stanje flip-flopa na izlazu. Nadalje, da bismo JK upotrijebili kao D flip-flop, potrebno je samo ulaz K postaviti da bude jednak komplementu ulaza J. Konačno, da bismo iz JK flip-flopa dobili T flip-flop, potrebno je postavili ulaz K jednak ulazu J. Time je vidljivo da je JK flip-flop doista univerzalan i da se može konfigurirati da radi kao bilo koji tip flip-flopa.

Dodatak D: Dokaz EBC-a za zbrajanje

***Teorem*:** Neka je zadana funkcija $\mathcal{H}(p) = -p\log_2 p - (1-p)\log_2(1-p)$ za $p \in [0,1]$ uz uvjete $\mathcal{H}(0) = \mathcal{H}(1) = 1$ i neka je $a, b \in [0, 0.5]$. Tada vrijedi:

$$\mathcal{H}(a+b) \leq \mathcal{H}(a) + \mathcal{H}(b)\,. \qquad (D.1)$$

Prvo se postavljaju i dokazuju dvije leme [9].

***Lema* 1.** Za $a, b \in (0, 0.5)$ vrijedi sljedeća nejednakost:

$$-(a+b)\log_2(a+b) \leq -a\log_2(a) - b\log_2(b)\,. \qquad (D.2)$$

Dokaz. Prvo se dokazuje sljedeća nejednakost:

$$-a\log_2(a+b) \leq -a\log_2(a)\,. \qquad (D.3)$$

Vrijedi:

$$a + b \geq a\,. \qquad (D.4)$$

Budući da je $\log_2(t)$ monotono rastuća funkcija na intervalu $(0, 0.5)$, slijedi da je

$$\log_2(a+b) \geq \log_2(a). \qquad (D.5)$$

Množeći gornju nejednakost sa $-a \leq 0$ dobiva se:

$$-a\log_2(a+b) \leq -a\log_2(a)\,, \qquad (D.6)$$

Čime je dokazana relacija (D.3).

Analogno vrijedi i za relaciju

$$-b\log_2(a+b) \leq -b\log_2(b). \qquad (D.7)$$

Konačno, sumirajući relacije (D.3) i (D.7) dobiva se nejednakost (D.2), Q.E.D.

***Lema* 2.** Za $a, b \in (0, 0.5)$ vrijedi sljedeća nejednakost:

$$-(1-(a+b))\log_2(1-(a+b)) \leq -(1-a)\log_2(1-a) - (1-b)\log_2(1-b)\,. \qquad (D.8)$$

Dokaz. Kako bi se dokazala zadana nejednakost (D.8), prvo je potrebno dokazati postojanje maksimuma sljedeće nejednakosti:

$$f(a,b) = -\big(1-(a+b)\big)\log_2\big(1-(a+b)\big) + (1-a)\log_2(1-a) + (1-b)\log_2(1-b) \tag{D.9}$$

Ekstrem ove funkcije dobiva se računanjem derivacije obje varijable a i b te izjednačavanjem s nulom.

$$\frac{df(a,b)}{da} = \frac{\ln\big(1-(a+b)\big) - \ln(1-a)}{\ln(2)} = 0 \;\Rightarrow b = 0 \tag{D.10}$$

$$\frac{df(a,b)}{db} = \frac{\ln\big(1-(a+b)\big) - \ln(1-b)}{\ln(2)} = 0 \;\Rightarrow a = 0 \tag{D.11}$$

Iz izračunatoga se vidi da je barem jedna varijabla jednaka nuli pa tada funkcija $f(a,b)$ poprima vrijednosti nula, što je upravo njezina ekstremna vrijednost. Stoga je $f(0,b) = f(a,0) = f(0,0) = 0$. Sada jedino još preostaje pitanje da li je taj ekstrem minimum ili maksimum funkcije. S obzirom da je $-\log_2(t)$ monotono padajuća funkcija na intervalu $(0, 0.5)$, funkcija $f(a,b)$ se može zapisati kao

$$f(a,b) = -\log_2\left(\frac{\big(1-(a+b)\big)^{1-(a+b)}}{(1-a)^{1-a}(1-b)^{1-b}}\right). \tag{D.12}$$

Iz ovoga je jasno vidljivo da je dobivena ekstremna vrijednost upravo maksimum funkcije. To vodi na to da je $f(a,b) \leq 0$ pa slijedi:

$$-\big(1-(a+b)\big)\log_2\big(1-(a+b)\big) + (1-a)\log_2(1-a) + (1-b)\log_2(1-b) \leq 0\,, \tag{D.13}$$

$$-\big(1-(a+b)\big)\log_2\big(1-(a+b)\big) \leq -(1-a)\log_2(1-a) - (1-b)\log_2(1-b)\,. \tag{D.14}$$

Q.E.D.

Dokaz teorema. Zbrajanjem dviju lema slijedi jednadžba (D.1) za $a, b \in (0, 0.5)$. Analitičkim proširenjem i korištenjem zadanih definicija ovog teorema, ovaj teorem vrijedi na punom intervalu $a, b \in [0, 0.5]$.

Literatura

[1] (16) Hrvatska enciklopedija, mrežno izdanje (2021.), Leksikografski zavod Miroslav Krleža, http://www.enciklopedija.hr/Natuknica.aspx?ID=18042, 22.6.2022.

[2] (15) von Neumann, J. Probabilistic logics and synthesis of reliable organisms from unreliable components. // Automata studies. Vol. 34 (1956.), str. 43-98.

[3] Ribeiro, S. T. Random pulse machine. // IEEE Transactions on Electronic Computers, Vol. EC-16 (1967.), str. 261-276.

[4] Gaines, B. R. Stochastic Computing Systems. // Advances in information systems science, Springer (1969.), str. 37-172.

[5] Lawlor, R. C. Computer utilizing random pulse trains. // U.S. Patent 3,612,845, (1971.)

[6] Alaghi, A.; Hayes, J. P. Survey of stochastic computing. // ACM Transactions on Embedded computing systems (TECS), Vol. 12, 2s (2013.), str. 1-19.

[7] Alaghi, A.; Qian, W.; Hayes, J. P. The promise and challenge of stochastic computing. // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 37, 8 (2017.), str. 1515-1531.

[8] Stipčević, M. Quantum random flip-flop and its applications in random frequency synthesis and true random number generator. // Review of Scientific Instruments, Vol. 87, 3 (2016.), str. 035113.

[9] Stipčević, M.; Batelić, M. Entropy considerations in improved circuits for a biologically-inspired random pulse computer. // Scientific reports, Vol. 12, 1 (2022.), str. 1-17.

[10] Seuer, R.; Molgedey, L.; Ebeling, W.; Jiménez-Montaño, M. A. Entropy and optimal partition for dana analysis. // The European Physical Journal B-Condensed Matter and Complex Systems, Vol. 19, 2 (2001.), str. 265-269.

[11] Paunović, S. Digitalna elektronika, 2. izdanje, Zagreb, Školska knjiga, 1999.

[12] Koch, C.; Bernander, Ö.; Douglas, R. J. Do neurons have a voltage or a current threshold for action potential initiation? // Journal of computational neuroscience, Vol. 2, 1 (1995.), str. 63-82.

[13] Veerappan, C.; Charbon. E. A low dark count pin diode based SPAD in CMOS technology. // IEEE transactions on electron devices, Vol. 63, 1 (2015.), str. 65-71.

[14] Batelić, M. Impulsno neuronsko računanje. Rad za Rektorovu nagradu. Zagreb : Prirodoslovno-matematički fakultet, 2019.

[15] Jennewein, T.; Achleitner, U.; Weihs, G.; Weinfurter H.; Zeilinger, A. A fast and compact quantum random number generator. // Review of Scientific Instruments, Vol. 71, 4 (2000.), str. 1675-1680.

[16] Linear feedback shift register, (2022.), Course Hero, https://images.app.goo.gl/xTnpTu2f4AnqJPUa8, 4.7.2022.

[17] Amano, H. Principles and Structures of FPGAs, Singapore, Springer, 2018.

[18] Serrano, J. Introduction to FPGA design. // CERN Accelerator School, 2008.

[19] Lee, V. T.; Alaghi, A.; Hayes, J. P., Sathe, V.; Ceze, L. Energy-efficient hybrid stochastic-binary neural networks for near-sensor computing. // Design, Automation & Test in Europe Conference and Exibition (DATE), IEEE, (2017.), str. 13-18.

[20] Liu, Y.; Parhi, K. K. Computing polynomials using unipolar stochastic logic. // ACM Journal on Emerging Technologies in Computing Systems (JETC), Vol. 13, 3 (2017.), str. 1-30.