5/30/2023

Numaratoare cu reatie liniara (LFSR)

Proiect PSN

NUME PRENUME: Tcaci Liviu

Grupa : 30211

Îndrumător: ing. DIana Pop

Contents

[1 Specificații 2](#_Toc130249632)

[2 Proiectare 3](#_Toc130249633)

[2.2.1 Schema Bloc 3](#_Toc130249634)  
[2.2.2 Unitatea de Control și Unitatea de Execuție 4…3](#_Toc130249635) [2.2.3 Determinarea resurselor (UE) 4](#_Toc130249637)  
[2.2.4 Reprezentarea UC prin diagrama de stări (organigrama) 8](#_Toc130249641)  
[2.2.5 Schema de detaliu a proiectului 12](#_Toc130249642)

[3 Manual de utilizare și întreținere](#_Toc130249643) 8

[4 Justificarea soluției alese](#_Toc130249644) 9

[5 Posibilități de dezvoltări ulterioare 1](#_Toc130249645)0

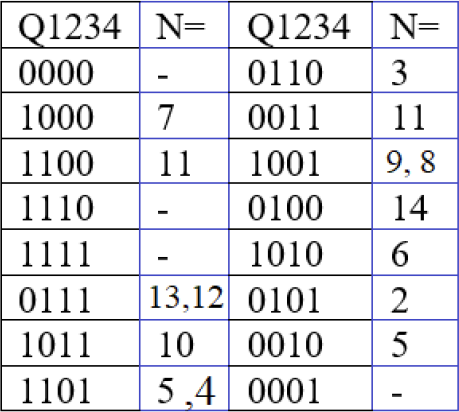
[6 Bibliografie 1](#_Toc130249646)1

Numaratoare cu reatie liniara (LFSR)

1 Specificații

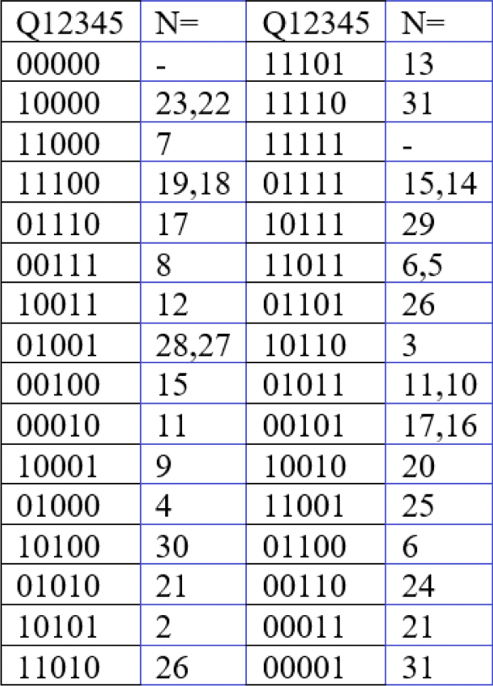
Această documentație prezintă o modalitate simplă și ușoară de a implementa un contor Linear Feedback Shift Register (LFSR) pe 4 și 5 biți. Sistemul proiectat primește intrări pentru lungimea buclei de numărare și selectarea variantei de contor: 4 biți sau 5 biți.

Contorul LFSR servește diverse aplicații în domeniul teoriei informațiilor, al teoriei codificării și al criptografiei, cum ar fi generarea de numere pseudoaleatoare, secvențe pseudo-zgomote, contoare digitale rapide și secvențe de albire.



Pentru un contor clasic de 4 biți, bucla fundamentală de feedback de la Q3 și Q4 exclude starea 1111. Se știe bine că, dacă cele două stări care au cei trei biți inferiori egali cu „1” sunt decodificate și feedback-ul pentru acele stări este inversat, atunci contorul LFSR pe 4 biți contorizează modulo 16 și nu are stare de blocare [2,3].

Următorul tabel arată decodificarea suplimentară a semnalului de feedback care este cerută de contoarele LFSR care au un ciclu mai scurt N.



În mod analog, în cazul unui LFSR de 5 biți, avem: pentru un ciclu de lungime 31, ieșirea Q5 va fi conectată la intrarea porții AND „B” și nu se va folosi poarta AND „C”; pentru orice valoare mai mica de 31 poarta SI „C” va fi programata conform Tabelului 2; pentru valorile 5, 10, 14, 16, 18, 22, 27, 31 iesirea Q5 va fi conectata la intrarea portii SI „B”; pentru orice alte valori ieșirea Q5 nu va fi conectată la intrarea porții AND „B” [2].

**2 Proiectare. Conceptul Black box**

# 

# 2.2.1. Maparea intrărilor/ieșirilor cutiei mari pe cele două componente UC și UE.

# Intrări

# MODE este introdus printr-un comutator și permite alegerea variantei de contor (pe 4 sau 5 biți), dacă comutatorul este pornit, atunci MODE este 1 logic și varianta pe 5 biți este setată, altfel când comutatorul este oprit, atunci MODE este 0 logic și varianta pe 4 biți este setată.

# lungimea N a buclei. N este un număr dat de un buton prin apăsarea creșterii cifrei până la 31, care este maxim, apoi se resetează; de la 2 la 31 pentru un contor de 5 biți și de la 2 la 15 pentru un contor de 4 biți.

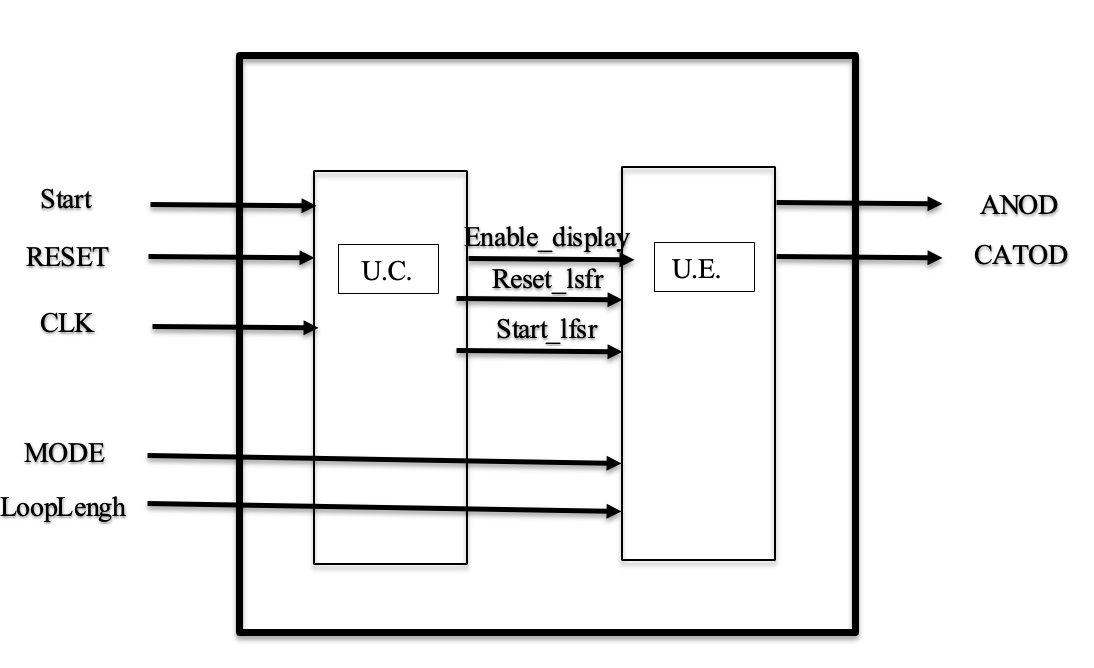
# START introdus de un buton pentru începerea numărării.

# Ieșiri:

# ANODE și CATOD pe 4 și, respectiv, 7 biți și vor fi folosite pentru a afișa numerele pe afișajul cu 7 segmente. Toate numerele de afișat sunt mai mici sau egale cu 31, așa că două afișaje sunt folosite pentru a le afișa și alte două sunt folosite pentru a introduce N.

## Unitatea de Control (UC) si Unitatea de Executie (UE)

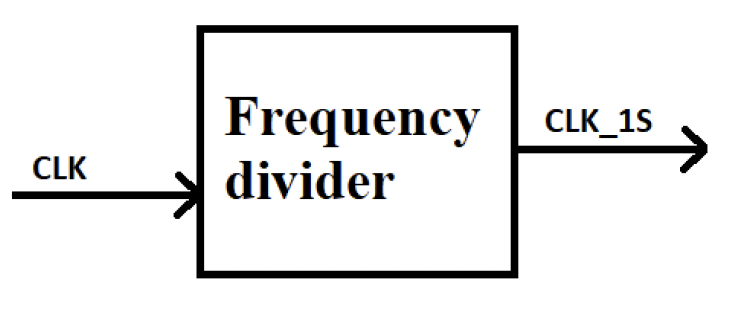
# Unitatea de execuție este realizată în principal din LFRS în sine, dar conține și o mulțime de componente periferice necesare pentru ieșirea și intrarea datelor. Toate aceste componente funcționează sincron ghidate de unitatea de control prin trei semnale: ENABLE, RESET și LOAD. Intrările unității de control sunt butonul START și semnalul STOP care este returnat de LFRS din UE când bucla este terminată.



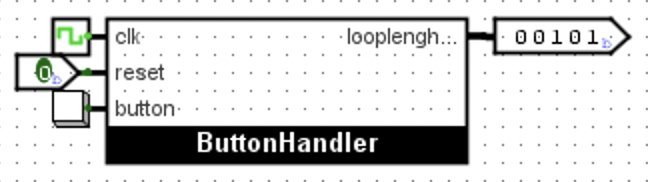
### UE va primi ca intrări aceste trei semnale și, în plus, modul de funcționare și lungimea buclei Looplength (N) prin butonul MODE și, respectiv, două comutatoare.

### Determinarea resurselor (UE)

a. Divizor de frecventa. Implementarea folosește o frecvență de ceas de 200 HZ necesară pentru ca ochiul uman să capteze lumina de pe afișajul cu șapte segmente.



b. DCD – Rolul său este de a citi lungimea buclei numerice și de a o transforma într-un număr binar pe 5 biți. De asemenea, trimite numărul pe afișajul cu 7 segmente pentru a fi afișat pe măsură ce este introdus. Se va realiza prin apăsarea x timp pe un buton pentru a obține x cifre.



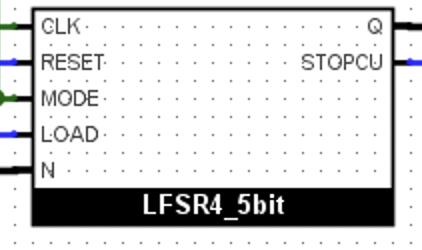
e. LFSR returnează forma binară a numerelor care urmează să fie afișate, la un interval de semnale de o secundă ale ceasului, pe ieșirea Q. Este un contor de feedback liniar care, în funcție de intrarea MODE, numără pe 4 sau 5 biți. (Este formată din cinci flip flops, cea mai semnificativă fiind dezactivată în funcție de valorile intrării MODE). Acesta primește de la SELECTIONS și C\_gate variabilele C, QX, D și returnează o serie de N numere în ordine relativ aleatorie pe 4 sau 5 biți după semnalele de o secundă ale ceasului. După finalizarea buclei, semnalul STOPCU este activat.

Are trei componente:

a) Un registru de 5 biți. Cel mai semnificativ bit Q4 va fi ignorat (va obține valoarea 0 în funcție de valoarea MODE). Registrul este încărcat atunci când unitatea de comandă activează semnalul LOAD și imediat după ce este dezactivat începe să se deplaseze spre dreapta. După finalizarea buclei modulo-N, END\_CICLE va reseta registrul activând semnalul STOPCU.

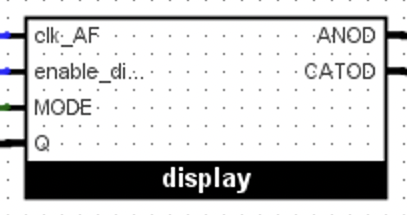
b) END\_CICLE este un numărător pe 8 biți care numără până la N. Când ajunge la acest număr activează STOPCU și oprește bucla LFRS.

c) SHIFT RIGHT - Calculează SR în funcție de valorile calculate de celelalte resurse și de MODE. (SR este o valoare de 0 sau 1, care este returnată de SHIFT RIGHT).



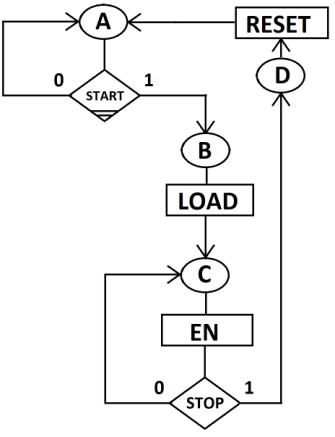
f. Componentă numită display care va prelua semnalul enable\_dislpay din Unitatea de control care va porni această componentă, semnal clk\_AF care va avea 200 hz, apoi va lua ieșirea Q a lfsr care este pe 5 biți și o va converti în consecință în tabelele în care coloana Q este ieșirea lfsr și N= este la care trebuie să facem conversia.

De exemplu, dacă Q e 00011 și luând în considerare că a funcționat cu logica MODE set 0, ceea ce înseamnă că pe 4 biți ar trebui să scoată cifra „2”, dacă ar fi să setăm pe logica MODUL 1, ar trebui să scoată „11”. În cazul „-”, acest simbol îl vom scoate prin aprinderea doar a afișajului cu 7 segmente a segmentului g. În cazul de exemplu 01011, unde are două valori 17 și 16, acestea vor fi afișate prin comutarea reciprocă în decurs de 1 secundă. De asemenea, țineți cont de faptul că, în cazul în care „-” sau o singură cifră, cum ar fi 1, 3, care pot fi reprezentate pe un singur afișaj cu 7 segmente, pentru un număr cu două cifre va trebui să le împărțim în zeci și unități care vor fi afișate pe două 7. afișaj segment. Și încă un convertor care va avea ca ieșire ANOD care este pe 2 biți (pentru că avem nevoie doar de două afișaje cu 7 segmente) și catod pe 7 biți care ne va ajuta să afișăm pe numere pe FPGA.

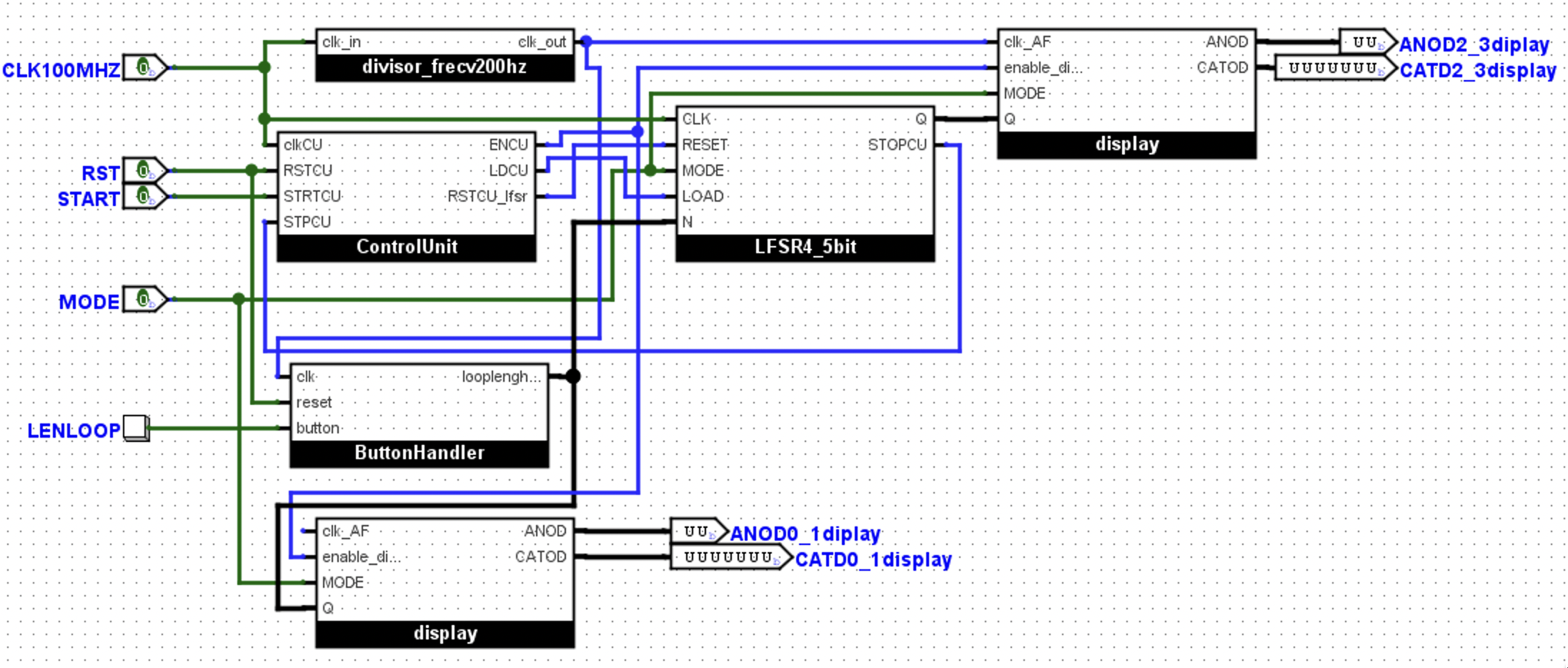


* + 1. Reprezentarea UC prin diagrama de stări (organigrama)

Următoarea diagramă arată cele 4 stări A-D prin care trece sistemul și descrie comportamentul acestuia. A este starea inițială care așteaptă datele de intrare (modul pe care îl alegem și lungimea N) până când butonul START este apăsat și sistemul trece la următoarea stare B. Apoi, prima comandă este trimisă la unitatea de execuție LOAD , care încarcă numerele din tabele în registru. În starea C, avem semnalul ENABLE (controlează un afișaj cu 7 segmente) care este activat până la oprirea buclei când semnalul STOP transformă 1 logic. Urmează starea D, care RESETează LFSR și îl pregătește pentru buclele următoare.



* + 1. Schema detaliata a proiectului



**3 Manual de utilizare si intretinere**

Acest manual de utilizare și întreținere oferă instrucțiuni detaliate și instrucțiuni pentru operarea și întreținerea sistemului de contor LFSR pe 4 și 5 biți implementat.

3.1 Prezentare generală a sistemului

Sistemul de contor LFSR pe 4 și 5 biți este proiectat pentru a genera numere pseudo-aliatoare utilizând registre de deplasare cu feedback linear (LFSR). Oferă flexibilitatea de a alege între variantele de contor pe 4 și 5 biți, în funcție de cerințele utilizatorului. Sistemul include o unitate de control (CU) și o unitate de execuție (UE) responsabile cu gestionarea funcționării și afișajului contorului.

3.2 Configurare hardware

* Asigurați-vă că sistemul este conectat la o sursă de alimentare stabilă.
* Conectați perifericele necesare, cum ar fi o unitate de afișare, la porturile desemnate de pe sistem.
* Verificați dacă toate conexiunile sunt sigure și așezate corect.

3.3 Funcționarea sistemului

* Porniți sistemul pornind sursa de alimentare.
* Sistemul se va inițializa și va afișa o stare implicită pe unitatea de afișare conectată.
* Pentru a porni contorul, apăsați butonul „Start” de pe unitatea de control.
* Contorul va începe să numere și să afișeze numerele generate pe unitatea de afișare conectată.
* Pentru a opri contorul, apăsați butonul „Stop” de pe unitatea de comandă.

3.4 Configurarea sistemului

* Sistemul oferă opțiunea de a selecta între variantele de contor pe 4 și 5 biți.
* Pentru a configura varianta de contor, localizați comutatoarele sau butoanele de configurare de pe sistem.

# Justificarea soluției alese

Soluția aleasă pentru implementarea unui sistem de contor LFSR pe 4 și 5 biți oferă mai multe avantaje și justificări:

Simplitate și ușurință în implementare: Soluția propusă oferă un design simplu și ușor de implementat pentru sistemul de contor LFSR. Prin utilizarea componentelor de bază, cum ar fi flip-flops, multiplexoare, comparatoare și decodoare, implementarea poate fi realizată fără complexitate semnificativă sau necesitatea de hardware specializat.

Flexibilitate și adaptabilitate: Designul permite flexibilitate în alegerea variantei de contor, fie pe 4 biți, fie pe 5 biți, în funcție de preferința utilizatorului. Această flexibilitate permite sistemului să răspundă diferitelor cerințe și aplicații.

Contorizare eficientă și fiabilă: Implementarea încorporează conexiuni de feedback adecvate bazate pe varianta de contor selectată și lungimea buclei. Prin decodificarea și inversarea feedback-ului pentru anumite stări, contorul LFSR realizează o numărare eficientă modulo durata ciclului dorită, asigurând o funcționare fiabilă fără stări de blocare.

Tranziție și control clar de stare: descompunerea unității de control (CU) și a unității de execuție (UE) a sistemului oferă un mecanism de tranziție de stare bine definit. CU gestionează intrări precum butonul de pornire și semnalul de oprire, în timp ce UE gestionează execuția contorului, inclusiv încărcarea numerelor, activarea afișajului și resetarea LFSR. Această împărțire clară a funcționalității îmbunătățește controlul și funcționarea sistemului.

Design modular și reutilizare: soluția folosește o abordare de proiectare modulară, cu diferite componente responsabile pentru sarcini specifice, cum ar fi diviziunea în frecvență, conversia numerelor, selecția conexiunilor, porțile și afișarea. Această structură modulară îmbunătățește reutilizarea componentelor individuale în alte modele și facilitează întreținerea și îmbunătățirile viitoare.

Optimizarea resurselor: Designul utilizează eficient resurse, cum ar fi multiplexoarele și ROM-urile, pentru a obține funcționalitatea dorită. Prin selectarea intrărilor și configurațiilor adecvate, sistemul minimizează utilizarea resurselor, menținând în același timp precizia și performanța.

În general, soluția aleasă atinge un echilibru între simplitate, flexibilitate, eficiență și modularitate. Oferă o abordare practică și eficientă pentru implementarea unui sistem de contor LFSR pe 4 și 5 biți, făcându-l potrivit pentru diverse aplicații în teoria informației, teoria codificării și criptografie.

# 5 Posibilități de dezvoltări ulterioare

Sistemul de contor LFSR oferă numeroase aplicații în diverse domenii, oferind beneficii semnificative utilizatorilor. Această secțiune explorează diversele aplicații și evidențiază avantajele utilizării sistemului.

3.1 Teoria informației:

În teoria informației, sistemul de contor LFSR își găsește utilitate în generarea de secvențe pseudo-aleatoare. Aceste secvențe servesc ca componente cheie pentru sarcini precum criptarea, detectarea erorilor și codarea canalului. Capacitatea sistemului de a genera secvențe lungi cu aleatorie statistică ridicată îl face un instrument esențial pentru asigurarea securității și integrității datelor.

Criptare: Sistemul de contor LFSR poate fi folosit în algoritmi criptografici în care sunt necesare secvențe pseudo-aleatorie pentru generarea cheilor sau operațiunile de criptare în flux. Prin generarea de secvențe imprevizibile, sistemul îmbunătățește securitatea datelor criptate, făcându-le mai rezistente la accesul neautorizat sau decriptare.

Detectarea erorilor: În sistemele de comunicație, sistemul de contorizare LFSR poate fi utilizat în scopuri de detectare a erorilor. Prin generarea de secvențe cu proprietăți dezirabile, cum ar fi perioade lungi și caracteristici bune de dispersie, sistemul permite tehnici eficiente de detectare și corectare a erorilor, cum ar fi verificările de redundanță ciclică (CRC) sau sumele de control.

3.2 Teoria codificării:

Teoria codificării utilizează pe scară largă sistemul de contor LFSR datorită capacității sale de a genera diverse secvențe cu proprietăți dezirabile. Aceste proprietăți se dovedesc benefice în proiectarea codurilor de corectare a erorilor pentru transmiterea fiabilă a datelor.

Coduri Linear Feedback Shift Register (LFSR): Sistemul de contor LFSR servește ca instrument fundamental pentru generarea codurilor LFSR. Aceste coduri prezintă capabilități excelente de corectare a erorilor și găsesc aplicații în telecomunicații, sisteme de stocare și comunicații prin satelit. Capacitatea sistemului de a genera secvențe cu perioade lungi și proprietăți bune de autocorelare contribuie la proiectarea și implementarea eficientă a acestor coduri.

Generarea secvenței: Capacitatea sistemului de contor LFSR de a genera secvențe pseudo-aleatoare este valoroasă în teoria codificării. Aceste secvențe pot fi utilizate în scopuri de codificare sau de răspândire, sporind robustețea și securitatea datelor codificate în timpul transmisiei.

3.3 Criptografia:

Sistemul de contor LFSR joacă un rol crucial în diverse aplicații criptografice, beneficiind de capacitatea sa de a genera secvențe pseudo-aleatorie.

Cifre de flux: Cifrele de flux se bazează pe generarea de secvențe lungi, imprevizibile. Sistemul de contor LFSR, cu caracterul său aleatoriu ridicat și perioadele lungi, oferă o resursă excelentă pentru design-uri de criptare în flux. Prin generarea unui flux de biți pseudo-aleatorii, sistemul facilitează procesele de criptare și decriptare, salvând informațiile sensibile.

Generarea cheilor criptografice: capacitatea sistemului de a genera secvențe pseudo-aleatoare poate fi folosită pentru generarea cheilor criptografice. Cheile puternice și imprevizibile sunt esențiale pentru operațiuni criptografice sigure. Sistemul de contor LFSR oferă o sursă fiabilă de pseudo-aleatorie, asigurând generarea de chei de criptare robuste.

În general, sistemul de contor LFSR găsește aplicații în teoria informației, teoria codificării și criptografie, oferind numeroase beneficii utilizatorilor. Capacitatea sa de a genera secvențe lungi, pseudo-aleatoare, cu proprietăți dorite, susține securitatea datelor, detectarea erorilor, corectareaerorilor și operațiuni criptografice, contribuind la fiabilitatea și integritatea diferitelor sisteme și aplicații.

# 6 Bibliografie

* „Proiectarea sistemelor numerice folosind tehnologia FPGA” de S. Nedevschi, Z. Baruch şi O. Creţ
* <https://www.fpga4student.com>
* https://inst.eecs.berkeley.edu/~cs150/sp03/handouts/15/LectureA/lec27-2up.pdf