Міністерство освіти і науки України Національний
технічний університет України «Київський політехнічний
інститут імені Ігоря Сікорського» Фізико-технічний
інститут

ЛАБОРАТОРНА РОБОТА №4

з **дисципліни**

«Криптографія»

на тему:
«Побудова регістрів зсуву з лінійним зворотним зв'язком та дослідження їх властивостей»

Виконали:
студенти 3 курсу ФТІ
групи ФБ-71
Романюк Д.О. Семичастний В.С
Перевірили:
Чорний О.
Савчук М. М.
Завадська Л. О.

Київ 2019

Мета роботи :
Ознайомлення з принципами побудови регістрів зсуву з лінійним зворотним зв'язком; практичне освоєння їх програмної реалізації; дослідження властивостей лінійних рекурентних послідовностей та їх залежності від властивостей характеристичного полінома регістра.

Порядок виконання роботи:

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Вибрати свій варіант завдання згідно зі списком. Варіанти завдань містяться у файлі Crypto_CP4 LFSR_Var.
2. За даними характеристичними многочленами p1(x), p2(x) скласти лінійні рекурентні співвідношення для ЛРЗ, що задаються цими характеристичними многочленами.
3. Написати програми роботи кожного з ЛРЗ L1 , L2 . 4. За допомогою цих програм згенерувати імпульсні функції для кожного з ЛРЗ і підрахувати їх періоди.
5. За отриманими результатами зробити висновки щодо влавстивостей кожного з характеристичних многочленів p1(x), p2(x): многочлен примітивний над F2 ; не примітивний, але може бути незвідним; звідний.
6. Для кожної з двох імпульсних функцій обчислити розподіл k-грам на періоді, k≤ni, де ni - степінь полінома fi(x), i=1,2 а також значення функції автокореляції A(d) для 0≤ d ≤ 10. За результатами зробити висновки.

Рекурентні співвідношення:

14	$P_1(X)= X^{24} + X^{22} + X^{21} + X^{19} + X^{17} + X^{15} + X^{11} + X^{10} + X^8 + X^2 + 1$ $P_2(X)= X^{20} + X^{19} + X^{18} + X^{14} + X^{12} + X^{10} + X^9 + X^7 + 1$

Результати:
Поліном p1 = [1,1,0,0,0,0,0,1,0,1,1,0,0,0,1,0,1,0,1,0,1,1,0]
Період: 8126433
Значення автокереляції
Avtoker1: 4063216 Avtoker2: 4063216 Avtoker3: 4063216 Avtoker4: 4063216 Avtoker5: 4063216 Avtoker6: 4063216 Avtoker7: 4063216 Avtoker8: 4063216 Avtoker9: 4063216 Avtoker10: 4063216
H – грами:

Биграммы:
00 1016193
10 1015298
11 1016192
01 1015533
Триграммы:
000 338559
010 338772
111 338643
100 338516
001 338644
011 338516
101 338516
110 338644
Четыреграммы:
0000 127410
0010 126901
1111 127070
0001 127324
0111 126987
0100 126767
1001 127002
1101 127356
0101 126735
0011 126790
1100 126925
1110 126807
1000 126666
1010 127054
0110 126627
1011 127187
Пятиграмы:
00000 50900
00101 51006
11100 50926
01011 51042
11111 50880
00100 50715
10000 50771
10100 50790
11101 50715
00001 50527
01001 50667
10011 50178
10101 50683
11010 50746
01000 50938
01110 50806
11001 51067
01010 51091
10111 50613
11011 50677
11000 50862
01100 50986
00011 50578
10001 51023
00110 50940
10110 50390
11110 51072
10010 50468

00111 50923
01111 50833
00010 50651
01101 50822

Поліном p2 = [1,0,0,0,0,0,1,0,1,1,0,1,0,1,0,0,0,1,1]
Період: 1048575
Значення автокереляції
Avtoker1: 524288 Avtoker2: 524288 Avtoker3: 524288 Avtoker4: 524288 Avtoker5: 524288 Avtoker6: 524288
Avtoker7: 524288 Avtoker8: 524288 Avtoker9: 524288 Avtoker10: 524288
H – грами:

Биграммы:
00 131071
11 131072
01 131072
10 131072
Триграммы:
000 43602
110 43760
010 43609
111 43676
001 43961
011 43627
100 43663
101 43626
Четыреграммы:
0000 16340
0011 16594
0110 16351
0101 16440
1100 16338
1011 16308
1110 16560
1000 16273
1001 16380
1101 16297
1111 16289
0100 16389
0010 16420
1010 16390
0001 16377
0111 16397
Пятиграммы:
00000 6575
00011 6609
01100 6456
10111 6603
00101 6617
10011 6516
11100 6679
00010 6612
00100 6550
00111 6604
10100 6534
01111 6609
11011 6571
10101 6672
01010 6405
01000 6591
10001 6533
11001 6549
10110 6579
01001 6579
01101 6533
10000 6552
01011 6595
11110 6465
01110 6475
00001 6501
10010 6509
11000 6532
11111 6533
00110 6572
11101 6514
11010 6490

Код програми:

```
from collections import Counter

p1 =
[1,1,0,0,0,0,0,1,0,1,1,0,0,0,1,0,1,0,1,0,1
,1,0]
a1 =
[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,1]
p2 =
[1,0,0,0,0,0,1,0,1,1,0,1,0,1,0,0,0,1,1]
a2 =
[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1]
a0 =
[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,1]
maxperiod1 = 2 ** (len(p1) + 1)
maxperiod2 = 2 ** (len(p2) + 1)

def hz(p1, p2, a0, a1, a2, maxperiod1,
maxperiod2):
    l1 = []
    l2 = []
    bigrams = ''
    threegrams = ''
    fourgrams = ''
    fivegrams = ''
    bigrams2 = ''
    threegrams2 = ''
    fourgrams2 = ''
    fivegrams2 = ''
    twgams = dict()
    trgams = dict()
    frgams = dict()
    fvgams = dict()
    twgams2 = dict()
    trgams2 = dict()
    frgams2 = dict()
    fvgams2 = dict()
    avtoker1 = 0
    avtoker2 = 0
```

```
        avtoker3 = 0
        avtoker4 = 0
        avtoker5 = 0
        avtoker6 = 0
        avtoker7 = 0
        avtoker8 = 0
        avtoker9 = 0
        avtoker10 = 0
        avtoker11 = 0
        avtoker12 = 0
        avtoker13 = 0
        avtoker14 = 0
        avtoker15 = 0
        avtoker16 = 0
        avtoker17 = 0
        avtoker18 = 0
        avtoker19 = 0
        avtoker20 = 0

        for i in range(1, maxperiod1):
                hz = 0
                for j in
range(len(p1)):
                        hz += (p1[j]
* a1[j])
                        hz %= 2
                l1.append(a1[0])
                for k in range(len(p1)
- 1):
                        a1[k] = a1[k
+ 1]
                a1[22] = hz
                if a1 == a0:
                        break
        print(i)
        for i in l1:
                if len(bigrams) < 2:
                        bigrams +=
str(i)
                else:
                        if
twgams.get(bigrams):

        twgams[bigrams] += 1
                        else:

        twgams[bigrams] = 1
                        bigrams =
str(i)
        g = Counter(twgams)
        for key in g.keys():
                print('Bigramsp1',
key , g[key])

        for i in l1:
                if len(threegrams) <
3:
                        threegrams
+= str(i)
                else:
                        if
trgams.get(threegrams):

        trgams[threegrams] += 1
                        else:

        trgams[threegrams] = 1
                        threegrams =
str(i)
        g = Counter(trgams)
        for key in g.keys():
                print('Threegramsp1',
key , g[key])

        for i in l1:
                if len(fourgrams) < 4:
                        fourgrams
+= str(i)
                else:
                        if
frgams.get(fourgrams):

        frgams[fourgrams] += 1
                        else:

        frgams[fourgrams] = 1
                        fourgrams =
str(i)
        g = Counter(frgams)
        for key in g.keys():
                print('Fourgramsp1',
key , g[key])

        for i in l1:
                if len(fivegrams) < 5:
                        fivegrams
+= str(i)
                else:
                        if
fvgams.get(fivegrams):

        fvgams[fivegrams] += 1
```

```
                else:

        fvgams[fivegrams] = 1
                fivegrams =
str(i)
        g = Counter(fvgams)
        for key in g.keys():
                print('Fivegramsp1',
key , g[key])

        for i in range(len(l1)):
                avtoker1 += (l1[i] +
l1[(i + 1)%len(l1)]) % 2
        for i in range(len(l1)):
                avtoker2 += (l1[i] +
l1[(i + 1)%len(l1)]) % 2
        for i in range(len(l1)):
                avtoker3 += (l1[i] +
l1[(i + 1)%len(l1)]) % 2
        for i in range(len(l1)):
                avtoker4 += (l1[i] +
l1[(i + 1)%len(l1)]) % 2
        for i in range(len(l1)):
                avtoker5 += (l1[i] +
l1[(i + 1)%len(l1)]) % 2
        for i in range(len(l1)):
                avtoker6 += (l1[i] +
l1[(i + 1)%len(l1)]) % 2
        for i in range(len(l1)):
                avtoker7 += (l1[i] +
l1[(i + 1)%len(l1)]) % 2
        for i in range(len(l1)):
                avtoker8 += (l1[i] +
l1[(i + 1)%len(l1)]) % 2
        for i in range(len(l1)):
                avtoker9 += (l1[i] +
l1[(i + 1)%len(l1)]) % 2
        for i in range(len(l1)):
                avtoker10 += (l1[i] +
l1[(i + 1)%len(l1)]) % 2
        print("Avtoker1:",avtoker1,"
Avtoker2:",avtoker2,"
Avtoker3:",avtoker3,"
Avtoker4:",avtoker4,"
Avtoker5:",avtoker5,"
Avtoker6:",avtoker6,"
Avtoker7:",avtoker7,"
Avtoker8:",avtoker8,"
Avtoker9:",avtoker9,"
Avtoker10:",avtoker10)

        print("//////////////////////////////////
//////////P2////////////////////////////////")

        for i in range(1, maxperiod2):
                hz = 0
                for j in
range(len(p2)):
                        hz += (p2[j]
* a2[j])
                        hz %= 2
                l2.append(a2[0])
                for k in range(len(p2)
- 1):
                        a2[k] = a2[k
+ 1]
                a2[18] = hz
                if a2 == a0:
                        break
        print(i)
        for i in l2:
                if len(bigrams2) < 2:
                        bigrams2 +=
str(i)
                else:
                        if
twgams2.get(bigrams2):

        twgams2[bigrams2] += 1
                        else:

        twgams2[bigrams2] = 1
                        bigrams2 =
str(i)
        g = Counter(twgams2)
        for key in g.keys():
                print('Bigramsp2',
key , g[key])

        for i in l2:
                if len(threegrams2) <
3:
                        threegrams2
+= str(i)
                else:
                        if
trgams2.get(threegrams2):

        trgams2[threegrams2] += 1
                        else:

        trgams2[threegrams2] = 1
```

```
                        threegrams2
= str(i)
        g = Counter(trgams2)
        for key in g.keys():
                print('Threegramsp2',
key , g[key])

        for i in l2:
                if len(fourgrams2) <
4:
                        fourgrams2
+= str(i)
                else:
                        if
frgams2.get(fourgrams2):

        frgams2[fourgrams2] += 1
                        else:

        frgams2[fourgrams2] = 1
                        fourgrams2
= str(i)
        g = Counter(frgams2)
        for key in g.keys():
                print('Fourgramsp2',
key , g[key])

        for i in l2:
                if len(fivegrams2) <
5:
                        fivegrams2
+= str(i)
                else:
                        if
fvgams2.get(fivegrams2):

        fvgams2[fivegrams2] += 1
                        else:

        fvgams2[fivegrams2] = 1
                        fivegrams2
= str(i)
        g = Counter(fvgams2)
        for key in g.keys():
                print('Fivegramsp2',
key , g[key])

        for i in range(len(l2)):
                avtoker11 += (l2[i] +
l2[(i + 1)%len(l2)]) % 2
        for i in range(len(l2)):
                avtoker12 += (l2[i] +
l2[(i + 1)%len(l2)]) % 2
        for i in range(len(l2)):
                avtoker13 += (l2[i] +
l2[(i + 1)%len(l2)]) % 2
        for i in range(len(l2)):
                avtoker14 += (l2[i] +
l2[(i + 1)%len(l2)]) % 2
        for i in range(len(l2)):
                avtoker15 += (l2[i] +
l2[(i + 1)%len(l2)]) % 2
        for i in range(len(l2)):
                avtoker16 += (l2[i] +
l2[(i + 1)%len(l2)]) % 2
        for i in range(len(l2)):
                avtoker17 += (l2[i] +
l2[(i + 1)%len(l2)]) % 2
        for i in range(len(l2)):
                avtoker18 += (l2[i] +
l2[(i + 1)%len(l2)]) % 2
        for i in range(len(l2)):
                avtoker19 += (l2[i] +
l2[(i + 1)%len(l2)]) % 2
        for i in range(len(l2)):
                avtoker20 += (l2[i] +
l2[(i + 1)%len(l2)]) % 2
        print("Avtoker1:",avtoker11,"
Avtoker2:",avtoker12,"
Avtoker3:",avtoker13,"
Avtoker4:",avtoker14,"
Avtoker5:",avtoker15,"
Avtoker6:",avtoker16,"
Avtoker7:",avtoker17,"
Avtoker8:",avtoker18,"
Avtoker9:",avtoker19,"
Avtoker10:",avtoker20)
hz(p1, p2, a0, a1, a2, maxperiod1,
maxperiod2)
```