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-72

Макоїд Ігор, Оліферук Артур

Перевірили:

Чорний О.

Савчук М. М.

Завадська Л. О.

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.

Вариант 10

P1(X)= X20+X18+X11+X10+X8+X7+X6+X5+1

P2(X)= X24 + X17 + X14 + X13 + X12+ X9 + X6 + 1

Періоди

P1(X):

T = 1048575

P2(X):

T = 64897

Обчислені розподіли k-грам

2-gram	
0 0	131042
0 1	131113
1 0	131090
1 1	131042

2-gram	
0 0	8051
0 1	8139
1 0	8219
1 1	8039

3-gram	
0 0 0	43733
0 0 1	43648
0 1 0	43648
0 1 1	43904
1 0 0	43648
1 0 1	43904
1 1 0	43392
1 1 1	43648

3-gram	
0 0 0	2715
0 0 1	2706
0 1 0	2679
0 1 1	2660
1 0 0	2732
1 0 1	2693
1 1 0	2728
1 1 1	2719

4-gram	
0 0 0 0	16228
0 0 0 1	16582
0 0 1 0	16405
0 0 1 1	16415
0 1 0 0	16465
0 1 0 1	16200
0 1 1 0	16308
0 1 1 1	16426
1 0 0 0	16406
1 0 0 1	16476
1 0 1 0	16336
1 0 1 1	16398
1 1 0 0	16312
1 1 0 1	16456
1 1 1 0	16425
1 1 1 1	16305

4-gram	
0 0 0 0	976
0 0 0 1	1003
0 0 1 0	1024
0 0 1 1	975
0 1 0 0	1016
0 1 0 1	1016
0 1 1 0	1053
0 1 1 1	995
1 0 0 0	1038
1 0 0 1	1036
1 0 1 0	1043
1 0 1 1	945
1 1 0 0	1043
1 1 0 1	1004
1 1 1 0	1037
1 1 1 1	1020

5-gram	
0 0 0 0 0	6515
0 0 0 0 1	6592
0 0 0 1 0	6592
0 0 0 1 1	6592
0 0 1 0 0	6528
0 0 1 0 1	6400
0 0 1 1 0	6528
0 0 1 1 1	6528
0 1 0 0 0	6592
0 1 0 0 1	6592
0 1 0 1 0	6592
0 1 0 1 1	6464
0 1 1 0 0	6528
0 1 1 0 1	6528
0 1 1 1 0	6656
0 1 1 1 1	6528
1 0 0 0 0	6592
1 0 0 0 1	6464
1 0 0 1 0	6464
1 0 0 1 1	6464
1 0 1 0 0	6656
1 0 1 0 1	6528
1 0 1 1 0	6656
1 0 1 1 1	6656
1 1 0 0 0	6592
1 1 0 0 1	6592
1 1 0 1 0	6592
1 1 0 1 1	6464
1 1 1 0 0	6528
1 1 1 0 1	6528
1 1 1 1 0	6656
1 1 1 1 1	6528

5-gram	
0 0 0 0 0	393
0 0 0 0 1	412
0 0 0 1 0	393
0 0 0 1 1	404
0 0 1 0 0	422
0 0 1 0 1	381
0 0 1 1 0	386
0 0 1 1 1	390
0 1 0 0 0	438
0 1 0 0 1	407
0 1 0 1 0	428
0 1 0 1 1	438
0 1 1 0 0	431
0 1 1 0 1	406
0 1 1 1 0	441
0 1 1 1 1	380
1 0 0 0 0	394
1 0 0 0 1	405
1 0 0 1 0	394
1 0 0 1 1	410
1 0 1 0 0	401
1 0 1 0 1	406
1 0 1 1 0	441
1 0 1 1 1	382
1 1 0 0 0	381
1 1 0 0 1	391
1 1 0 1 0	386
1 1 0 1 1	390
1 1 1 0 0	393
1 1 1 0 1	406
1 1 1 1 0	442
1 1 1 1 1	407

Автокореляція	
d	**Значення**
0	0
1	524288
2	524288
3	524288
4	524288
5	524288
6	524288
7	524288
8	524288
9	524288
10	524288

Автокореляція	
d	**Значення**
0	0
1	32452
2	32460
3	32448
4	32440
5	32452
6	32440
7	32444
8	32440
9	32448
10	32448

За отриманими результатами було встановлено задані поліноми мають такі :

P1(X) - примітивний

P2(X) - не примітивний, але може бути незвідним

Код:

```
#include <fstream>
 #include <iostream>
 #include <cstring>
 #include <math.h>
 using namespace std;
 int main()
{
   int var24[24]={1,0,0,0,0,0,1,0,0,1,0,0,1,1,1,0,0,1,0,0,0,0,0,0};
   int def24[24]={0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1};
   int dif24[24]={0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1};
   int var[20]={1,0,0,0,0,1,1,1,1,0,1,1,0,0,0,0,0,0,1,0};
   int def[20]={0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1};
   int dif[20]={0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1};
   cout<<"========================Polinom st=20========================="<<endl;
   int T=0;
   bool mas[1048575];
   do{
            //suma
            int suma = 0;
            for(int i=0;i<20;i++){
                     suma+=(var[i]*def[i]);
            }
            //sdvig
            mas[T]=def[0];
            for(int i=0;i<19;i++){
```

```
                    def[i]=def[i+1];
            }
            def[19]=suma%2;
            T++;
 }
 while(!equal(def,def+20,dif));
 cout<<"T = "<<T<<endl;
  //2-gram
 cout<<"============2-gram============ "<<endl;
 for(int a=0;a<=1;a++){
            for(int b=0;b<=1;b++){
                    bool n[2];
                    n[0]=a;n[1]=b;
                    cout<<n[0]<<" "<<n[1]<<"  ";
                    unsigned int counter=0;
                    for(int i=0;i<T-T%2;i+=2){
                        bool m[2];
                        m[0]=mas[i];m[1]=mas[i+1];
                        if(equal(n,n+2,m))
                        counter++;
                                                }
                    cout<<"counter = "<<counter<<endl;

   }
}
//3-gram
cout<<"============3-gram============ "<<endl;
  for(int a=0;a<=1;a++){
            for(int b=0;b<=1;b++){
              for(int c=0;c<=1;c++){
                    bool n[3];
                    n[0]=a;n[1]=b;n[2]=c;
                    cout<<n[0]<<" "<<n[1]<<" "<<n[2]<<"  ";
                    unsigned int counter=0;
                    for(int i=0;i<T-T%3;i+=3){
                        bool m[3];
                        m[0]=mas[i];m[1]=mas[i+1];m[2]=mas[i+2];
                        if(equal(n,n+3,m))
                        counter++;
                                                }
                    cout<<"counter = "<<counter<<endl;
     }
   }
}
//4-gram
cout<<"============4-gram============ "<<endl;
for(int a=0;a<=1;a++){
            for(int b=0;b<=1;b++){
              for(int c=0;c<=1;c++){
        for(int d=0;d<=1;d++){
                    bool n[5];
                    n[0]=a;n[1]=b;n[2]=c;n[3]=d;
                    cout<<n[0]<<" "<<n[1]<<" "<<n[2]<<" "<<n[3]<<"  ";
                    unsigned int counter=0;
                    for(int i=0;i<T-T%4;i+=4){
```

```
                        bool m[4];
                        m[0]=mas[i];m[1]=mas[i+1];m[2]=mas[i+2];m[3]=mas[i+3];
                        if(equal(n,n+4,m))
                        counter++;
                                                }
                cout<<"counter = "<<counter<<endl;          }
    }
  }
}
 //5-gram
 cout<<"============5-gram============ "<<endl;
for(int a=0;a<=1;a++){
            for(int b=0;b<=1;b++){
              for(int c=0;c<=1;c++){
      for(int d=0;d<=1;d++){
        for(int e=0;e<=1;e++){
                bool n[5];
                n[0]=a;n[1]=b;n[2]=c;n[3]=d;n[4]=e;
                cout<<n[0]<<" "<<n[1]<<" "<<n[2]<<" "<<n[3]<<" "<<n[4]<<"  ";
                unsigned int counter=0;
                for(int i=0;i<T-T%5;i+=5){
                        bool m[5];
                        m[0]=mas[i];m[1]=mas[i+1];m[2]=mas[i+2];m[3]=mas[i+3];m[4]=mas[i+4];
                        if(equal(n,n+5,m))
                        counter++;
                                                }
                cout<<"counter = "<<counter<<endl;
        }
       }
    }
  }
}
cout<<"=========Autocorrelation========="<<endl;
for(int d=0;d<=10;d++){
int s,k=0;
for(int i=0;i<1048575;i++)
{
  s=(mas[i]+mas[(i+d)%1048575])%2;
  k+=s;
}
 cout<<"d = "<<d<<". Corel = "<<k<<endl;
}
cout<<"========================Polinom st=24========================="<<endl;
T=0;
bool mas24[64897];
do{
            //suma
            int suma = 0;
            for(int i=0;i<24;i++){
                        suma+=(var24[i]*def24[i]);
            }
            //sdvig
            mas24[T]=def24[0];
            for(int i=0;i<23;i++){
                        def24[i]=def24[i+1];
```

```
            }
            def24[23]=suma%2;
            T++;
 }
 while(!equal(def24,def24+24,dif24));
 cout<<"T = "<<T<<endl;
 //2-gram
 cout<<"============2-gram============ "<<endl;
 for(int a=0;a<=1;a++){
             for(int b=0;b<=1;b++){
                    bool n[2];
                    n[0]=a;n[1]=b;
                    cout<<n[0]<<" "<<n[1]<<"  ";
                    short unsigned int counter=0;
                    for(int i=0;i<T-T%2;i+=2){
                          bool m[2];
                          m[0]=mas24[i];m[1]=mas24[i+1];
                          if(equal(n,n+2,m))
                          counter++;
                                                }
                    cout<<"counter = "<<counter<<endl;
   }
}
//3-gram
cout<<"============3-gram============ "<<endl;
  for(int a=0;a<=1;a++){
             for(int b=0;b<=1;b++){
               for(int c=0;c<=1;c++){
                    bool n[3];
                    n[0]=a;n[1]=b;n[2]=c;
                    cout<<n[0]<<" "<<n[1]<<" "<<n[2]<<"  ";
                    short unsigned int counter=0;
                    for(int i=0;i<T-T%3;i+=3){
                          bool m[3];
                          m[0]=mas24[i];m[1]=mas24[i+1];m[2]=mas24[i+2];
                          if(equal(n,n+3,m))
                          counter++;
                                                }
                    cout<<"counter = "<<counter<<endl;
     }
   }
}
//4-gram
cout<<"============4-gram============ "<<endl;
for(int a=0;a<=1;a++){
             for(int b=0;b<=1;b++){
               for(int c=0;c<=1;c++){
        for(int d=0;d<=1;d++){
                    bool n[5];
                    n[0]=a;n[1]=b;n[2]=c;n[3]=d;
                    cout<<n[0]<<" "<<n[1]<<" "<<n[2]<<" "<<n[3]<<"  ";
                    short unsigned int counter=0;
                    for(int i=0;i<T-T%4;i+=4){
                          bool m[4];
                          m[0]=mas24[i];m[1]=mas24[i+1];m[2]=mas24[i+2];m[3]=mas24[i+3];
```

```
                        if(equal(n,n+4,m))
                        counter++;
                                                }
                    cout<<"counter = "<<counter<<endl;
        }
      }
    }
  }
  //5-gram
  cout<<"============5-gram============ "<<endl;
 for(int a=0;a<=1;a++){
              for(int b=0;b<=1;b++){
                for(int c=0;c<=1;c++){
        for(int d=0;d<=1;d++){
          for(int e=0;e<=1;e++){
                    bool n[5];
                    n[0]=a;n[1]=b;n[2]=c;n[3]=d;n[4]=e;
                    cout<<n[0]<<" "<<n[1]<<" "<<n[2]<<" "<<n[3]<<" "<<n[4]<<"  ";
                    short unsigned int counter=0;
                    for(int i=0;i<T-T%5;i+=5){
                        bool m[5];
                        m[0]=mas24[i];m[1]=mas24[i+1];m[2]=mas24[i+2];m[3]=mas24[i+3];m[4]=mas24[i+4];
                        if(equal(n,n+5,m))
                        counter++;
                                                }
                    cout<<"counter = "<<counter<<endl;
          }
        }
      }
    }
  }
  cout<<"=========Autocorrelation========="<<endl;
  for(int d=0;d<=10;d++){
  int s,k=0;
  for(int i=0;i<64897;i++)
  {
    s=(mas24[i]+mas24[(i+d)%64897])%2;
    k+=s;
  }
   cout<<"d = "<<d<<". Corel = "<<k<<endl;
  }
}
```

Висновок: по ходу виконання практикуму ми ознайомились з принципами побудови регістрів зсуву з лінійним зворотним зв’язком; освоєння їх програмну реалізацію; дослідили властивості лінійних рекурентних послідовностей та їх залежності від властивостей характеристичного полінома регістра.