TECHNICKÁ UNIVERZITA KOŠICE

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

KATEDRA ELEKTRONIKY A MULTIMEDIÁLNYCH TELEKOMUNIKÁCIÍ

ZADANIE Z PREDMETU APLIKOVANÁ KRYPTOGRAFIA

Vypracovali:
Vladimír BÁLINT
Szabolcs CSERNOK
2000/2001

Úvod

Nech s = s0; s1; s2; ... ; sn-1 je binárna postupnosť dĺžky n. Existujú testy na určenie toho, či daná postupnosť je náhodná. Štatistické testy zvyčajne určujú, či binárna postupnosť má nejaké charakteristické vlastnosti, či je skutočne náhodná postupnosť. Musíme však zdôrazniť, že aj keď postupnosť bol vytvorený nenáhodným bitovým generátorom, test môže ukazovať, že postupnosť je náhodná. Ak postupnosť prejde všetky základné testy (monobit test, sériový test, poker test, run test a autokorelačný test), tak je už pravdepodobnosť väčšia, že je to náhodná postupnosť, ale istotu nebudeme mať.

Sériový test:

Účelom tohoto testu je určiť počet prípadov výskytu 00,01,10,a 11 v S. Očakávame, že sú približne tie isté. Nech n0,n1 popisujú počet 0 a 1 v S, a nech n00,n01,n10,n11 popisujú počet výskytov 00,01,10,11, jednotlivo. Všimnime si, že $n_{00}+n_{01}+n_{10}+n_{11}=n-1$. Pre štatistické vyjadrenie sa používa tento vzťah:

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

ktorý približne sleduje rozdeľovanie $\chi 2$ so stupňom voľnosti 2 pre $n \geq 21$.

Prahová hodnota je 5,9915.

Autokorelačný test

Účelom tohto testu je overenie korelácie medzi S a necyklicky posunutými verziami S. Nech d je pevná premenná , $1 \leq d \leq [n/2]$. Počet bitov v S nie je rovný s posunutiami d. Potom

$$A(d) = \sum_{i=0}^{n-d-1} s_i \oplus s_{i+d} ,$$

kde $\oplus$ vyjadruje operáciu XOR. Pre štatistické vyjadrenie sa používa tento vzťah

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

ktorý približne sleduje N(0,1) rozdeľovanie ak n-d≥10.

Keďže malé hodnoty A(d) sú podobne neočakávané ako výskyt veľkých hodnôt A(d). Postupnosť vyhovuje testu, ak $|X_5| < 1.96$.

Program v jazyku C

```
#include <stdio.h>
#include <math.h>
#include <stdlib.h>
#include <conio.h>
const MAX = 160.;
const D   =  8.;
void main()
{
char s[MAX];
float x2,x5;
int n0=0,n1=0,n00=0,n01=0,n10=0,n11=0;
int add=0,i;
double pom;

randomize();
for(i=0;i<MAX;i++)          //vygenerovanie postupnosti
        {
        s[i]=random(2);
        }

for(i=0;i<MAX;i++)          //pocet 0
        if (s[i]==0) n0++;
for(i=0;i<MAX;i++)          //pocet 1
```

```
            if (s[i]==1) n1++;

        for(i=0;i<MAX-1;i++)          //pocet 00
            if (s[i]==0&&s[i+1]==0) n00++;
        for(i=0;i<MAX-1;i++)                  //pocet 01
            if (s[i]==0&&s[i+1]==1) n01++;
        for(i=0;i<MAX-1;i++)          //pocet 10
            if (s[i]==1&&s[i+1]==0) n10++;
        for(i=0;i<MAX-1;i++)          //pocet 11
            if (s[i]==1&&s[i+1]==1) n11++;

            //vypocet statistickej hodnoty serioveho testu
        x2=( (4./(MAX-1) ) * ( n00*n00 + n01*n01 + n10*n10 + n11*n11 ) ) - ( (2./MAX)* ( n0*n0 + n1*n1 ) ) + 1.;

        for(i=0;i<MAX-D-1;i++)                //vypocet A(d)
            {
            if (s[i]^s[i+D]) add++;
            }
            //vypocet statistickej hodnoty autokorelacneho testu
        x5=(2.* (add - ( (MAX-D)/2.) ) ) / sqrt(MAX-D);

        printf("               s  =\n");//vypis postupnosti na obr.
        for(i=0;i<MAX;i++){
            if(i%20==0) printf("\n");
            printf("%d ",s[i]);
            }
                                    //vypis vysledkov
        printf("\n\n\n   Seriovy test:\n\n   n0    n1    n00   n01   n10   n11");
        printf("\n  %3d   %3d   %3d   %3d   %3d   %3d\n",n0,n1,n00,n01,n10,n11);
        printf("\n   x2 = %f     %s podmienke ",x2,(x2<5.9915)?"vyhovuje":"nevyhovuje");
        printf("\n\n\n   Autokorelacny test:");
        printf("\n\n          d   =   %d\n          A(d)   =   %d\n          x5   =   %f          %s podmienke\n",D,add,x5,(abs(x5)<1.96)?"vyhovuje":"nevyhovuje");
```

```
getchar();
}
```

Výpis programu

```
        s =

0 0 1 0 0 0 1 1 0 0 1 0 1 1 1 1 1 1 0 1
1 0 0 1 1 0 1 1 0 1 0 0 0 0 1 1 0 0 1 0
0 1 0 0 0 1 0 0 0 1 1 0 1 0 1 0 0 0 1 0
1 0 1 0 0 0 1 1 1 0 1 1 0 0 1 1 0 0 0 1
1 1 1 1 0 0 1 0 1 1 0 1 0 1 0 1 0 1 0 1
0 0 0 1 0 0 1 0 1 1 0 1 1 1 0 1 0 0 0 1
1 1 0 0 0 0 1 0 0 1 0 0 1 1 0 1 0 1 0 0
0 1 1 0 0 1 1 0 1 0 0 0 1 0 0 0 1 0 1 1
```

```
  Seriovy test:

  n0    n1    n00   n01   n10   n11
  85    75     39    46    45    29

  x2 = 3.972484      vyhovuje podmienke


  Autokorelacny test:
  d = 8
  A(d) = 70
  x5 = -0.973329     vyhovuje podmienke
```