

Kodas:

```
6 from Golomb import getTests, printCheck
7 import random
8
9
10 def linearReg(c):
11     X = []
12     for i in range(len(c)):
13         X.append(int(round(random.random(), 0)))
14
15     n = len(X)
16     m = pow(2, n) - 1
17     c = c[::-1]
18     string = ""
19
20     for i in range(m):
21         string += str(X[n-1])
22         temp = 0
23         for j in range(n):
24             temp += int(X[j])*int(c[j])
25
26         j = n-1
27         while j > 0:
28             X[j] = X[j-1]
29             j -= 1
30
31         X[0] = str((temp % 2))
32
33     return string
```

Išvedimas:

```
35 string = linearReg("1000001")
36 print (string)
37 printCheck(string, 0.05)
38
39 string = linearReg("1000111")
40 print (string)
41 printCheck(string, 0.05)
42
43 string = linearReg("1100101")
44 print (string)
45 printCheck(string, 0.05)
46
47 string = linearReg("10010101")
48 print (string)
49 printCheck(string, 0.05)
50
51 string = linearReg("10110001")
52 print (string)
53 printCheck(string, 0.05)
54
55 string = linearReg("11100001")
56 print (string)
57 printCheck(string, 0.05)
```

Išbandžiau algoritmą su 6 skirtingais C vektoriais, gautais iš 7 ir 8 laipsnio primityviųjų daugianarių ir patikrinau, kad jie tikrai išveda maksimalaus ilgio m bitų seką išvesdamas 10 daugiau simbolių nei m ir patikrindamas kad pirmi 10 simbolių sutampa tikrai su paskutiniais 10 simbolių.

## Rezultatai:

```
[Running] python -u "c:\Users\Warius\Desktop\7 semestras\informacinės saugos pagrindai\uzduotys\Golomb\SLD.py"
110110101101100100100011100001011111001010111001101000100111100010100001100000111111010101001100111010010100011011
{'T1': 0.007874015748031496, 'T2': 0.023872015997994822, 'T4': 0.501937984496124, 'T5': 0.25, 'T1check': 3.841458820694124, 'T2check': 5
T1 - Pass
T2 - Pass
T4 - Pass
T5 - Pass
10111000010011000001010101101001001001111001000110101000011111101110110111101000101001011111000100000110011011000111001110
{'T1': 0.007874015748031496, 'T2': 0.023872015997994822, 'T4': 0.001937984496124031, 'T5': 1.0, 'T1check': 3.841458820694124, 'T2check':
T1 - Pass
T2 - Pass
T4 - Pass
T5 - Pass
10100010111000111101101010111111010011000010100010101101100101011000100001001111100111001001000110011011110000001110
{'T1': 0.007874015748031496, 'T2': 0.023872015997994822, 'T4': 0.001937984496124031, 'T5': 0.75, 'T1check': 3.841458820694124, 'T2check'
T1 - Pass
T2 - Pass
T4 - Pass
T5 - Pass
00101001100110111101010101100011111110100100000011101100000010011010000011010111000010111100100011100010110010010011101011010011110
{'T1': 0.00392156862745098, 'T2': 0.011826462868611998, 'T4': 0.0012178606851300832, 'T5': 1.414213562373095, 'T1check': 3.8414588206941
T1 - Pass
T2 - Pass
T4 - Pass
T5 - Pass
0110000101001011110100111111101000011001111000011010011010001110111000111010000000111110001001000100010101010111001000110010010
{'T1': 0.00392156862745098, 'T2': 0.011826462868611998, 'T4': 0.0012178606851300832, 'T5': 0.7071067811865475, 'T1check': 3.841458820694
T1 - Pass
T2 - Pass
T4 - Pass
T5 - Pass
001010010101011111000101100100001010001001001010101001100101111010001110110111100001001111011011100001001110101100011110
{'T1': 0.00392156862745098, 'T2': 0.011826462868611998, 'T4': 0.0012178606851300832, 'T5': 0.8838834764831843, 'T1check': 3.841458820694
T1 - Pass
T2 - Pass
T4 - Pass
T5 - Pass
```

Paskaičiavau testines reikšmes  $T_i$  ir reikšmes pagal kurias reikia patikrinti ar seka praeina testą –  $T_{i\text{check}}$  ( $T_i$  turi būti mažiau už  $T_{i\text{check}}$ , skaičiuojant  $T_5$   $d = n/2$ ). Jei seka praeina testą išvedama „Pass“, jei ne išvedama „Fail“

Kai  $C = [1,0,0,0,1]$ :

Seka:

110110101101100100100011100001011111001010111001101000100111100010100001100000  
1000000111111101010100110011101110100101100011011

$T_1 = 0.007874015748031496$	$T_{1\text{check}} = 3.841458820694124$	Pass
$T_2 = 0.023872015997994822$	$T_{2\text{check}} = 5.991464547107979$	Pass
$T_4 = 0.501937984496124$	$T_{4\text{check}} = 9.487729036781154$	Pass
$T_5 = 0.25$	$T_{5\text{check}} = 1.959963984540054$	Pass

Kai C = [1,0,0,0,1,1,1]:

Seka:

10111000010011000001010101101001001010011110010001101010000111111011101101111  
0100010110010111110001000000110011011000111001110

Kai C = [1,1,0,0,1,0,1]:

Seka:

10100010111000111101110110101111110100110000110100001010010110110010101011000  
1000001001111100111001001000110011011110000001110

Kai C = [1,0,0,1,0,1,0,1]:

Seka:

00101001100110111101010101100011111110100100000001110110000001001101000001101  
011100001011110010001110001011001001001110101101101001111011011101000110110011  
10010110101001011101111011100110000110010101000101011111100111110000010100001  
000011110001100010001

Kai C = [1,0,1,1,0,0,0,1]:

Seka:

011000010100101111010011111111010100001110011110000110110011010001111011100011  
101000000011111000100101000100010110101011100100011001001001110000001000010011  
01111001100111011111001011001010110110100100000110001101011000101010100110000  
010111010111110110111

Kai C = [1,1,1,0,0,0,0,1]:

Seka:

001010010110101111100010110010000101000100100101010100110010111010001110110011  
111011010000001000001011110111011110000100111010110001111001101101111111101010  
111001110010011010100001101110000011000011100011001100010001101001111010010001  
010110110000000111111