擬似乱数生成の評価
長周期連性テスト
PANAMA(MULTI-S01) 編

平成 13 年 1 月 21 日

1 取得条件

FIPS 140 と同様に 20000 bits をサンプリングして，その中で同一 bits (gaps, blocks) の長さを評価する．このテストでは，長さを 1,2,3,4,5,6,... と可能な限り分解する．出力系列が真の乱数系列とみなせるならば，0 または 1 が数十 bits も連続することはまずない．FIPS 140 を合格する条件は全てのサンプルに対して，長さ 34 以上の gaps または blocks が発生しないことである．

鍵は，別冊「PANAMA の評価に利用した鍵の種類」にある組み合わせ (秘密鍵を 999 通り，乱数列番号を 100 通り) を対象とし，各々の出力の先頭 20000bits を対象に評価を行った．

つまり，このテストでは計約 10 万件のテストを行ったことになる．

2 テスト結果

テスト結果を示す.

2.1 gaps の分布

左から順に gaps の長さ，度数である．

```
00001  249750334
00002  124879133
00003  62430058
00004  31222492
00005  15608059
00006  7801718
00007  3906730
00008  1952368
00009  975026
00010  487174
00011  243902
00012  121662
00013  61150
```

```
00014  30813
00015  14862
00016  7423
00017  3910
00018  1884
00019  979
00020  471
00021  231
00022  110
00023  64
00024  40
00025  12
00026  7
00027  9
00028  3
00029  0
00030  0
00031  0
00032  0
00033  1
00034  0
00035  0
```
(以下全て 0)

2.2 blocks の分布

左から順に blocks の長さ，度数である．

```
00001  249747126
00002  124887636
00003  62436648
00004  31211226
00005  15607354
00006  7801247
00007  3904971
00008  1951483
00009  976600
00010  487658
00011  244355
00012  121597
00013  60892
00014  30750
00015  15390
00016  7651
```

```
00017  3858
00018  1950
00019  991
00020  521
00021  243
00022  139
00023  61
00024  39
00025  15
00026  9
00027  3
00028  2
00029  0
00030  0
00031  0
00032  1
00033  0
00034  0
00035  0
```

付録に度数分布を示す．度数分布をみる限り，理想的な分布に見える．

3 評価

10 万件の検査の結果は FIPS 140 の試験を合格したと判断する下記に，最大 gaps/blocks が発生した際の gaps/blocks の値を示す.

3.1 最大 gaps と 最大 blocks

最大 gaps が発生したのは 秘密鍵 ca550 乱数列番号 da030 のときで，次のようになる.

```
#  da030ca550.pnm
01, 2457, 2488
02, 1228, 1228
03, 604, 617
04, 330, 311
05, 173, 141
06, 87, 90
07, 34, 41
08, 18, 22
09, 10, 7
10, 4, 4
11, 2, 3
12, 3, 2
```

```
13, 1, 1
14, 0, 0
15, 0, 0
16, 2, 0
17, 0, 0
18, 0, 0
19, 0, 0
20, 0, 0
21, 0, 0
22, 0, 0
23, 0, 0
24, 0, 0
25, 0, 0
26, 0, 0
27, 0, 0
28, 0, 0
29, 0, 0
30, 0, 0
31, 0, 0
32, 0, 0
33, 1, 0
```

最大 blocks が発生したのは 秘密鍵 cs0ef 乱数列番号 da051 のときで，次のようになる．

```
01, 2474, 2450
02, 1237, 1244
03, 644, 635
04, 292, 307
05, 166, 175
06, 69, 77
07, 47, 34
08, 22, 20
09, 10, 16
10, 1, 5
11, 1, 1
12, 2, 1
13, 1, 0
14, 0, 0
15, 0, 0
16, 0, 0
17, 0, 0
18, 0, 0
19, 0, 0
20, 0, 0
21, 0, 0
```

```
22, 0, 0
23, 0, 0
24, 0, 0
25, 0, 0
26, 0, 0
27, 0, 0
28, 0, 0
29, 0, 0
30, 0, 0
31, 0, 0
32, 0, 1
```

度数分布

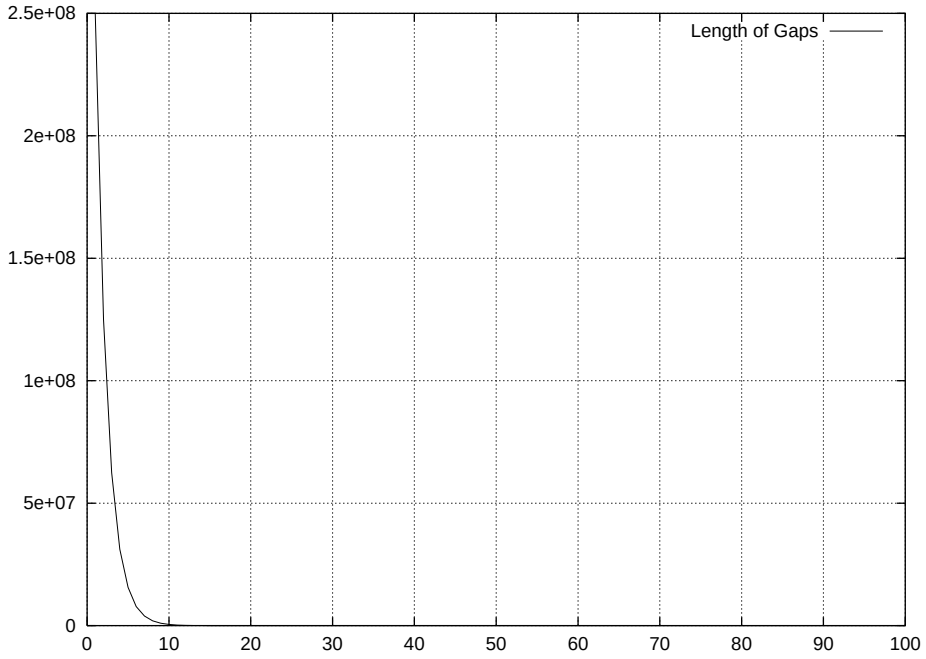

図 1: gaps(OFF bit(=0)) の長さの分布

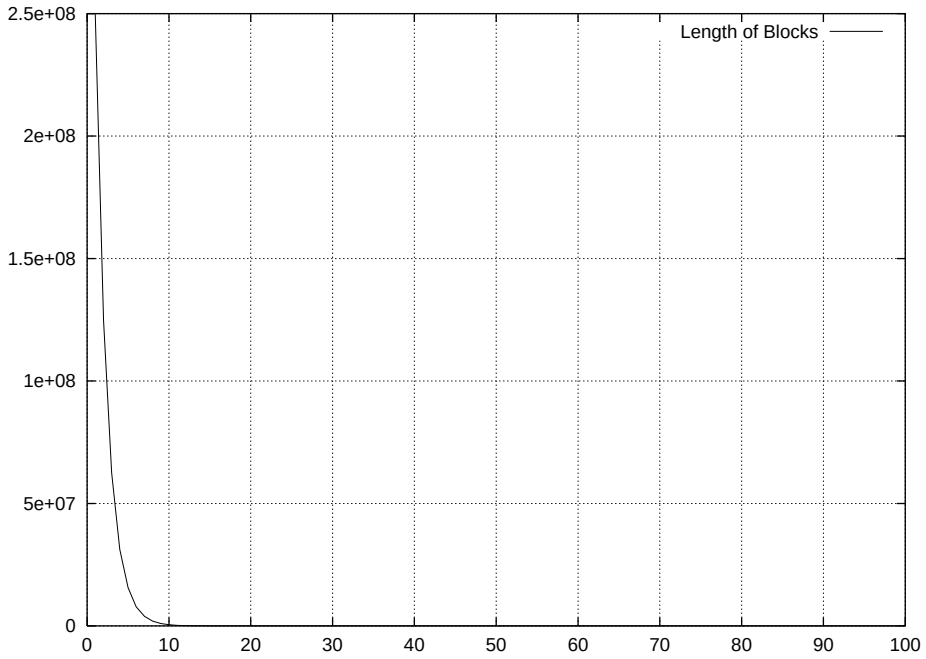

図 2: blocks(ON bit(=1) の長さの分布