Metryki losowości, testy FIPS 140-2 generatorów liczb pseudolosowych

Mikołaj Koszowski 274392
Hubert Nowakowski 274415

Zadanie na poziom 5

1) Test FIPS dla /dev/random

Po przeanalizowaniu ciągu losowego wygenerowanego z systemowego generatora liczb losowych otrzymaliśmy skuteczność 99.9% dla 320000000 bitów.

```
In [5]: N = int(320000000/8)

In [6]: !head -c$N /dev/random | rngtest
        rngtest 5
        Copyright (c) 2004 by Henrique de Moraes Holschuh
        This is free software; see the source for copying conditions.  There is NO warranty; not even for MERCHANTABILITY
        or FITNESS FOR A PARTICULAR PURPOSE.

        rngtest: starting FIPS tests...
        rngtest: entropy source drained
        rngtest: bits received from input: 320000000
        rngtest: FIPS 140-2 successes: 15989
        rngtest: FIPS 140-2 failures: 10
        rngtest: FIPS 140-2(2001-10-10) Monobit: 0
        rngtest: FIPS 140-2(2001-10-10) Poker: 1
        rngtest: FIPS 140-2(2001-10-10) Runs: 3
        rngtest: FIPS 140-2(2001-10-10) Long run: 6
        rngtest: FIPS 140-2(2001-10-10) Continuous run: 0
        rngtest: input channel speed: (min=1.279; avg=6.815; max=19073.486)Mibits/s
        rngtest: FIPS tests speed: (min=10.620; avg=43.355; max=91.699)Mibits/s
        rngtest: Program run time: 51827062 microseconds
```

Rysunek 1: Wynik testu FIPS dla generatora systemowego.

2) Liniowy generator kongruentny

Generator LCG oblicza kolejne liczby pseudolosowe x_1 z zakresu wartości <0, m-1> na podstawie wzoru:

$$x_i = (a \cdot x_{i-1} + 1)\ mod\ m\ ,$$

gdzie x_1 jest wartością inicjującą generator (seed). Jakość takiego generatora mocno zależy od doboru jego parametrów. Parametr *m* powinien być duży, aby zapewnić długi cykl.

Generator ze źle dobranymi parametrami (*a=19, c=1, x=0, m=381*) test FIPS zwrócił skuteczność 0%. Dla większego parametru m ($m=2^{32}$) uzyskano skuteczność 0.5%. Dla parametrów używanych w kompilatorze Borland C/C++ uzyskano skuteczność 99.9%, czyli wynik na poziomie systemowego generatora liczb losowych.

3) Usprawnienie generatora LCG

W celu usprawnienia losowości generatora LCG generowane bajty są mieszane funkcją XOR z bajtami czytanymi ze skompresowanego pliku (gzip). Funkcja XOR może tylko dodać entropii, więc spodziewamy się, że tak wygenerowany ciąg liczb będzie uzyskiwał większą skuteczność dla testu FIPS.

```
%%time
acc_FIPS(get_improved(10**7))
```

```
/home/fisher/projects/repo/master/mosesdecoder/scripts/tests/cs-en-sample/lm.en.gz 237898
/home/fisher/projects/repo/dev/cmake_update/cmake-3.16.4.tar.gz 9113021
/home/fisher/projects/wykop/mongo_dump/dump/wykop/post.bson.gz 918184403
rngtest 5
Copyright (c) 2004 by Henrique de Moraes Holschuh
This is free software; see the source for copying conditions.  There is NO warranty; not even for ME
RCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

rngtest: starting FIPS tests...
rngtest: entropy source drained
rngtest: bits received from input: 320000000
rngtest: FIPS 140-2 successes: 11590
rngtest: FIPS 140-2 failures: 4409
rngtest: FIPS 140-2(2001-10-10) Monobit: 2965
rngtest: FIPS 140-2(2001-10-10) Poker: 2822
rngtest: FIPS 140-2(2001-10-10) Runs: 2801
rngtest: FIPS 140-2(2001-10-10) Long run: 7
rngtest: FIPS 140-2(2001-10-10) Continuous run: 6
rngtest: input channel speed: (min=2222222222.222; avg=15206729398.346; max=0.000)bits/s
rngtest: FIPS tests speed: (min=34.060; avg=90.531; max=98.317)Mibits/s
rngtest: Program run time: 16988209 microseconds

CPU times: user 13.3 s, sys: 488 ms, total: 13.8 s
Wall time: 17 s
0.7244202762672667
```

Rysunek 2: Wynik testu FIPS dla usprawnionego LCG ze źle dobranymi parametrami.

Dla generatora z małym parametrem m=381 skuteczność wzrosła do 72.4%. Jest to znacznie lepszy wynik, lecz nadal nie jest to dostatecznie dobry generator, by można go uznać za bezpieczny. Dla większego parametru $m=2^{32}$ uzyskaliśmy skuteczność na poziomie równym systemowemu generatorowi (99.9%).

Generator	**Początkowa skuteczność**	**Skuteczność po usprawnieniu**
/dev/random	99.9 %	–
LCG z parametrami jak w Borland C/C++	99.9 %	–
LCG: m=381	0.0 %	72.4 %
LCG: $m=2^{32}$	0.5 %	99.9 %

Kod dostępny pod:
https://github.com/Fisher16/KiBD

Źródła:

http://www.algorytm.org/liczby-pseudolosowe/generator-lcg-liniowy-generator-kongruentny.html
https://rosettacode.org/wiki/Linear_congruential_generator