Filip Kwiatkowski 283437 – BBS random number generator

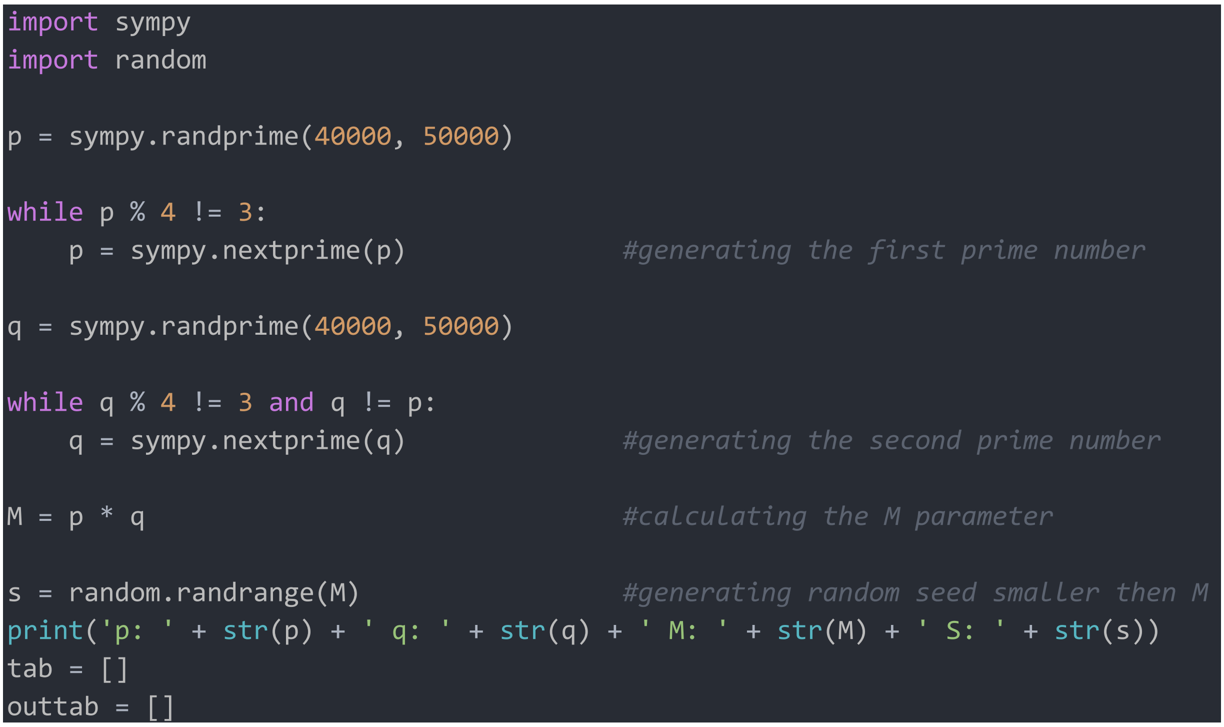
1. Algorithm definition

The BBS generator (Blum Blum Shub) was proposed in the 1986. It was derived from the O. Rabin's one way function. It takes o from: $x_{n+1} = x_n^2(mod\ M)$ where $M = p * q$

Both p and q are large (the larger the better) prime numbers, that has to satisfy the equation: $(p, q) \ \equiv 3(mod\ 4)$. This function will provide the sequence of numbers smaller than M and bigger than 0. From this sequence we can extract the least significant bit, most significant bit or the parity flag of each of the generated numbers. By doing that we receive a pseudorandom binary sequence. The security and performance of the generator highly depends on the chosen prime numbers. The higher the primes, the harder it is to find a loop in the generated sequence. While testing the algorithm (generating the sequence of 10000000 32bit decimal numbers) it has been observed that when choosing very small primes (0-50) the sequence looped after at most several hundred numbers, while choosing high primes (40000 – 50000) the loop was much rarer, but it could still occur even once each 10000 numbers, and when the primes were increased even more (400000 – 500000) the loop was present after 6 000 000 numbers, hence the higher primes are used, the safer and more "random" the generator is.

2. Python code

DISCLAIMER! : The code uses 2 additional modules to provide the ability of generating random prime numbers and random seed for each test. These modules are: random and sympy.



```
import sympy
import random

p = sympy.randprime(40000, 50000)

while p % 4 != 3:
    p = sympy.nextprime(p)              #generating the first prime number

q = sympy.randprime(40000, 50000)

while q % 4 != 3 and q != p:
    q = sympy.nextprime(q)              #generating the second prime number

M = p * q                               #calculating the M parameter

s = random.randrange(M)                 #generating random seed smaller then M
print('p: ' + str(p) + ' q: ' + str(q) + ' M: ' + str(M) + ' S: ' + str(s))
tab = []
outtab = []
```

```
outdec = 0
seqdec = []
size = 320
x0 = (s * s) % M

count = 0
while(count != size):                    #generating given quantity of numbers
via the BBS algorithm
    x = (x0 * x0) % M
    tab.append(x0 & 1)                   #extracting the least significant bit
form the generated number
    x0 = x
    count = count + 1

count = 1
power = 32
for i in tab:
    count = count + 1
    power = power - 1                    #spliting the sequence of bits into 32
bit decimal numbers
    outdec = outdec + (i * (2 ** power))
    if count % 32 == 0:
        power = 32
        seqdec.append(outdec)
        outdec = 0
        outbin = 0

for i in seqdec:
    print(i)
```

3. Tests

The sequence was tested using all of the dieharder tests. The sequence consisted of 10 000 000 32bit decimal numbers generated using following constants:

Prime number P : 419423

Prime number Q : 454303

Product of primes M : 190545127169

Seed S : 118610173460

The result of following tests are as follows:

```
#===================================================================
==========#
#            dieharder version 3.31.1 Copyright 2003 Robert G. Brown
#
#===================================================================
==========#
   rng_name    |           filename             |rands/second|
     file_input|                          bbs.txt|  4.81e+06  |
#===================================================================
==========#
        test_name   |ntup| tsamples |psamples|  p-value |Assessment
#===================================================================
==========#
# The file file_input was rewound 1 times
   diehard_birthdays|   0|       100|     100|0.05102298|  PASSED
# The file file_input was rewound 11 times
      diehard_operm5|   0|   1000000|     100|0.00164010|   WEAK
# The file file_input was rewound 24 times
  diehard_rank_32x32|   0|     40000|     100|0.29741905|  PASSED
# The file file_input was rewound 30 times
    diehard_rank_6x8|   0|    100000|     100|0.57831277|  PASSED
# The file file_input was rewound 32 times
   diehard_bitstream|   0|   2097152|     100|0.04063608|  PASSED
# The file file_input was rewound 53 times
        diehard_opso|   0|   2097152|     100|0.06007314|  PASSED
# The file file_input was rewound 67 times
        diehard_oqso|   0|   2097152|     100|0.00000000|  FAILED
# The file file_input was rewound 74 times
         diehard_dna|   0|   2097152|     100|0.00017532|   WEAK
# The file file_input was rewound 74 times
diehard_count_1s_str|   0|    256000|     100|0.13908737|  PASSED
```

```
# The file file_input was rewound 87 times
diehard_count_1s_byt|   0|    256000|     100|0.66339150|  PASSED
# The file file_input was rewound 87 times
 diehard_parking_lot|   0|     12000|     100|0.37143226|  PASSED
# The file file_input was rewound 88 times
    diehard_2dsphere|   2|      8000|     100|0.76189996|  PASSED
# The file file_input was rewound 88 times
    diehard_3dsphere|   3|      4000|     100|0.65649848|  PASSED
# The file file_input was rewound 111 times
     diehard_squeeze|   0|    100000|     100|0.00007748|   WEAK
# The file file_input was rewound 111 times
        diehard_sums|   0|       100|     100|0.00129522|   WEAK
# The file file_input was rewound 112 times
        diehard_runs|   0|    100000|     100|0.77837481|  PASSED
        diehard_runs|   0|    100000|     100|0.42390260|  PASSED
# The file file_input was rewound 125 times
       diehard_craps|   0|    200000|     100|0.00000164|   WEAK
       diehard_craps|   0|    200000|     100|0.14668879|  PASSED
# The file file_input was rewound 325 times
 marsaglia_tsang_gcd|   0|  10000000|     100|0.00000000|  FAILED
 marsaglia_tsang_gcd|   0|  10000000|     100|0.00000000|  FAILED
# The file file_input was rewound 326 times
         sts_monobit|   1|    100000|     100|0.07151460|  PASSED
# The file file_input was rewound 327 times
            sts_runs|   2|    100000|     100|0.00000211|   WEAK
# The file file_input was rewound 328 times
          sts_serial|   1|    100000|     100|0.07151460|  PASSED
          sts_serial|   2|    100000|     100|0.00007665|   WEAK
          sts_serial|   3|    100000|     100|0.33759885|  PASSED
          sts_serial|   3|    100000|     100|0.00059247|   WEAK
          sts_serial|   4|    100000|     100|0.23545071|  PASSED
          sts_serial|   4|    100000|     100|0.76361652|  PASSED
          sts_serial|   5|    100000|     100|0.04996869|  PASSED
          sts_serial|   5|    100000|     100|0.08324114|  PASSED
          sts_serial|   6|    100000|     100|0.08363405|  PASSED
          sts_serial|   6|    100000|     100|0.00136746|   WEAK
          sts_serial|   7|    100000|     100|0.22513796|  PASSED
          sts_serial|   7|    100000|     100|0.28925593|  PASSED
          sts_serial|   8|    100000|     100|0.41509649|  PASSED
          sts_serial|   8|    100000|     100|0.56309546|  PASSED
          sts_serial|   9|    100000|     100|0.00004142|   WEAK
          sts_serial|   9|    100000|     100|0.00000011|  FAILED
          sts_serial|  10|    100000|     100|0.36264365|  PASSED
          sts_serial|  10|    100000|     100|0.00023565|   WEAK
          sts_serial|  11|    100000|     100|0.27346295|  PASSED
          sts_serial|  11|    100000|     100|0.00230649|   WEAK
          sts_serial|  12|    100000|     100|0.06995814|  PASSED
          sts_serial|  12|    100000|     100|0.00000979|   WEAK
          sts_serial|  13|    100000|     100|0.00128432|   WEAK
          sts_serial|  13|    100000|     100|0.00014703|   WEAK
          sts_serial|  14|    100000|     100|0.00000108|   WEAK
          sts_serial|  14|    100000|     100|0.00077755|   WEAK
          sts_serial|  15|    100000|     100|0.00000220|   WEAK
          sts_serial|  15|    100000|     100|0.13738405|  PASSED
          sts_serial|  16|    100000|     100|0.00016482|   WEAK
          sts_serial|  16|    100000|     100|0.90003508|  PASSED
# The file file_input was rewound 330 times
         rgb_bitdist|   1|    100000|     100|0.32324409|  PASSED
# The file file_input was rewound 334 times
         rgb_bitdist|   2|    100000|     100|0.63401855|  PASSED
```

```
# The file file_input was rewound 340 times
         rgb_bitdist|   3|    100000|     100|0.75577896|  PASSED
# The file file_input was rewound 348 times
         rgb_bitdist|   4|    100000|     100|0.63978559|  PASSED
# The file file_input was rewound 358 times
         rgb_bitdist|   5|    100000|     100|0.77583277|  PASSED
# The file file_input was rewound 370 times
         rgb_bitdist|   6|    100000|     100|0.10544069|  PASSED
# The file file_input was rewound 384 times
         rgb_bitdist|   7|    100000|     100|0.00434192|   WEAK
# The file file_input was rewound 400 times
         rgb_bitdist|   8|    100000|     100|0.40415009|  PASSED
# The file file_input was rewound 418 times
         rgb_bitdist|   9|    100000|     100|0.00000014|  FAILED
# The file file_input was rewound 438 times
         rgb_bitdist|  10|    100000|     100|0.91398549|  PASSED
# The file file_input was rewound 460 times
         rgb_bitdist|  11|    100000|     100|0.97479937|  PASSED
# The file file_input was rewound 484 times
         rgb_bitdist|  12|    100000|     100|0.00000002|  FAILED
# The file file_input was rewound 486 times
rgb_minimum_distance|   2|     10000|    1000|0.19754263|  PASSED
# The file file_input was rewound 489 times
rgb_minimum_distance|   3|     10000|    1000|0.08064181|  PASSED
# The file file_input was rewound 493 times
rgb_minimum_distance|   4|     10000|    1000|0.00722590|  PASSED
# The file file_input was rewound 498 times
rgb_minimum_distance|   5|     10000|    1000|0.02712119|  PASSED
# The file file_input was rewound 500 times
    rgb_permutations|   2|    100000|     100|0.02077223|  PASSED
```

```
# The file file_input was rewound 503 times
    rgb_permutations|   3|    100000|     100|0.21739999|  PASSED
# The file file_input was rewound 507 times
    rgb_permutations|   4|    100000|     100|0.32300108|  PASSED
# The file file_input was rewound 512 times
    rgb_permutations|   5|    100000|     100|0.00001543|   WEAK
# The file file_input was rewound 522 times
      rgb_lagged_sum|   0|   1000000|     100|0.00434716|   WEAK
# The file file_input was rewound 542 times
      rgb_lagged_sum|   1|   1000000|     100|0.00000038|  FAILED
# The file file_input was rewound 572 times
      rgb_lagged_sum|   2|   1000000|     100|0.07942435|  PASSED
# The file file_input was rewound 612 times
      rgb_lagged_sum|   3|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 662 times
      rgb_lagged_sum|   4|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 722 times
      rgb_lagged_sum|   5|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 792 times
      rgb_lagged_sum|   6|   1000000|     100|0.11075046|  PASSED
# The file file_input was rewound 872 times
      rgb_lagged_sum|   7|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 962 times
      rgb_lagged_sum|   8|   1000000|     100|0.00002795|   WEAK
# The file file_input was rewound 1062 times
      rgb_lagged_sum|   9|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 1172 times
      rgb_lagged_sum|  10|   1000000|     100|0.00017643|   WEAK
# The file file_input was rewound 1292 times
      rgb_lagged_sum|  11|   1000000|     100|0.00000000|  FAILED
```

```
# The file file_input was rewound 1422 times
      rgb_lagged_sum|  12|   1000000|     100|0.01522051|  PASSED
# The file file_input was rewound 1562 times
      rgb_lagged_sum|  13|   1000000|     100|0.00001320|   WEAK
# The file file_input was rewound 1712 times
      rgb_lagged_sum|  14|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 1872 times
      rgb_lagged_sum|  15|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 2042 times
      rgb_lagged_sum|  16|   1000000|     100|0.03572794|  PASSED
# The file file_input was rewound 2222 times
      rgb_lagged_sum|  17|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 2412 times
      rgb_lagged_sum|  18|   1000000|     100|0.01535916|  PASSED
# The file file_input was rewound 2612 times
      rgb_lagged_sum|  19|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 2822 times
      rgb_lagged_sum|  20|   1000000|     100|0.00035754|   WEAK
# The file file_input was rewound 3042 times
      rgb_lagged_sum|  21|   1000000|     100|0.00000001|  FAILED
# The file file_input was rewound 3272 times
      rgb_lagged_sum|  22|   1000000|     100|0.00000126|   WEAK
# The file file_input was rewound 3512 times
      rgb_lagged_sum|  23|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 3762 times
      rgb_lagged_sum|  24|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 4022 times
      rgb_lagged_sum|  25|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 4292 times
      rgb_lagged_sum|  26|   1000000|     100|0.00657022|  PASSED
```

```
# The file file_input was rewound 4572 times
      rgb_lagged_sum|  27|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 4862 times
      rgb_lagged_sum|  28|   1000000|     100|0.01028510|  PASSED
# The file file_input was rewound 5162 times
      rgb_lagged_sum|  29|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 5472 times
      rgb_lagged_sum|  30|   1000000|     100|0.01482990|  PASSED
# The file file_input was rewound 5792 times
      rgb_lagged_sum|  31|   1000000|     100|0.00000000|  FAILED
# The file file_input was rewound 6122 times
      rgb_lagged_sum|  32|   1000000|     100|0.01890999|  PASSED
# The file file_input was rewound 6123 times
     rgb_kstest_test|   0|     10000|    1000|0.92189955|  PASSED
# The file file_input was rewound 6139 times
     dab_bytedistrib|   0|  51200000|       1|0.00000000|  FAILED
# The file file_input was rewound 6140 times
             dab_dct| 256|     50000|       1|0.00024846|   WEAK
Preparing to run test 207.  ntuple = 0
# The file file_input was rewound 6151 times
        dab_filltree|  32|  15000000|       1|0.00004321|   WEAK
        dab_filltree|  32|  15000000|       1|0.00000342|   WEAK
Preparing to run test 208.  ntuple = 0
# The file file_input was rewound 6154 times
       dab_filltree2|   0|   5000000|       1|0.00000000|  FAILED
       dab_filltree2|   1|   5000000|       1|0.00000000|  FAILED
Preparing to run test 209.  ntuple = 0
# The file file_input was rewound 6161 times
        dab_monobit2|  12|  65000000|       1|1.00000000|  FAILED
```