NSP 800 随机数质量测试步骤

ymgongcn@gmail.com

2014 年 4 月 26 日

随机数样本的说明：

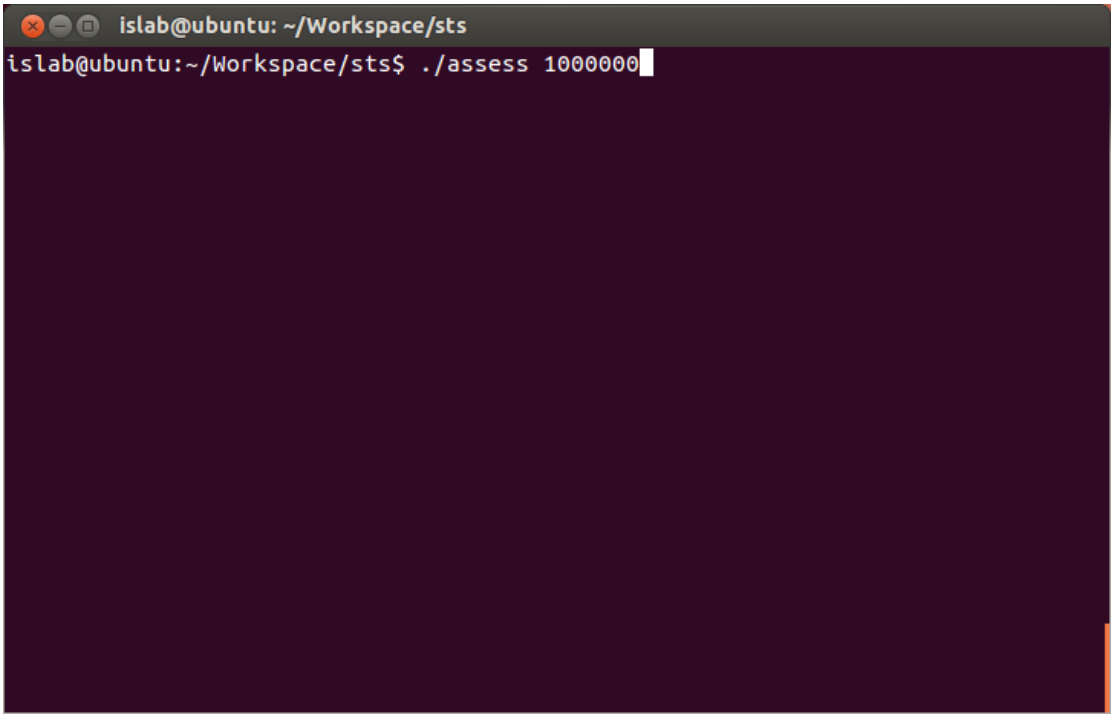
推荐的测试样本为 1G（1G=1024M=1024*1024K=1024*1024*1024）个随机数，随机数形式为 0 和 1 的组合。如果以 ASCII 码序列存放随机数，即每一 Byte 代表一个随机的 0 或 1，那么样本的大小为 1G Bytes，即 1024 MB。如果以二进制文件存放随机数，即每一位就是一个随机数，那么样本的大小为 1G/8 Bytes，即 1024/8 MB，即 128 MB。

测试软件的说明：

使用 NIST 的 sts 随机数质量测试软件，在 Linux（这里使用 Ubuntu 12.04 LTS）下使用 make 命令编译，生成 access 可执行文件。

测试步骤：

1. 把随机数样本 rand.txt 放到 sts/data 目录下（也可以放到其他目录），这里使用的样本随机数是以 ASCII 码序列的形式存储。
2. 进入 sts 目录，运行 assess，后面的参数表示每组中随机数的个数。在测试中，为了把 1G 个随机数分成 1024 组，那么每组就会有 1024*1024 个随机数，这里为了简单起见，把随机数分为 1000 组，每组中 1000,000 个随机数（总随机数的个数会小于 1G 个）。



3. 该步骤中，在“Enter Choice: ”后输入“0”，表示选择“[0] Input File”，指定随机数的文件。

```
islab@ubuntu: ~/Workspace/sts
islab@ubuntu:~/Workspace/sts$ ./assess 1000000
          G E N E R A T O R    S E L E C T I O N
          ----------------------------------------

    [0] Input File                  [1] Linear Congruential
    [2] Quadratic Congruential I    [3] Quadratic Congruential II
    [4] Cubic Congruential          [5] XOR
    [6] Modular Exponentiation      [7] Blum-Blum-Shub
    [8] Micali-Schnorr              [9] G Using SHA-1

   Enter Choice: 0
```

4. 输入随机数文件位置，这里是“./data/rand.txt”。

```
islab@ubuntu: ~/Workspace/sts
islab@ubuntu:~/Workspace/sts$ ./assess 1000000
          G E N E R A T O R    S E L E C T I O N
          ----------------------------------------

    [0] Input File                  [1] Linear Congruential
    [2] Quadratic Congruential I    [3] Quadratic Congruential II
    [4] Cubic Congruential          [5] XOR
    [6] Modular Exponentiation      [7] Blum-Blum-Shub
    [8] Micali-Schnorr              [9] G Using SHA-1

   Enter Choice: 0


                User Prescribed Input File: ./data/rand.txt
```

5. 该步骤列出了 15 中随机数测试标准，如果只想测试某一种，那么输入“0”，然后在对应的标准上设置“0”或“1”。如果要测试所有标准，那么在该步骤中输入“1”。这里需要全部测试这些标准。

```
islab@ubuntu: ~/Workspace/sts
 [8] Micali-Schnorr            [9] G Using SHA-1

Enter Choice: 0


            User Prescribed Input File: ./data/rand.txt

            S T A T I S T I C A L   T E S T S
            _________________________________

 [01] Frequency                       [02] Block Frequency
 [03] Cumulative Sums                 [04] Runs
 [05] Longest Run of Ones             [06] Rank
 [07] Discrete Fourier Transform      [08] Nonperiodic Template Matchings
 [09] Overlapping Template Matchings  [10] Universal Statistical
 [11] Approximate Entropy             [12] Random Excursions
 [13] Random Excursions Variant       [14] Serial
 [15] Linear Complexity

      INSTRUCTIONS
         Enter 0 if you DO NOT want to apply all of the
         statistical tests to each sequence and 1 if you DO.

Enter Choice: 1
```

6. 该步骤中可以进行参数调整，一般使用默认的参数，输入“0”，进入下一步。

```
islab@ubuntu: ~/Workspace/sts
 [03] Cumulative Sums                 [04] Runs
 [05] Longest Run of Ones             [06] Rank
 [07] Discrete Fourier Transform      [08] Nonperiodic Template Matchings
 [09] Overlapping Template Matchings  [10] Universal Statistical
 [11] Approximate Entropy             [12] Random Excursions
 [13] Random Excursions Variant       [14] Serial
 [15] Linear Complexity

      INSTRUCTIONS
         Enter 0 if you DO NOT want to apply all of the
         statistical tests to each sequence and 1 if you DO.

Enter Choice: 1

     P a r a m e t e r   A d j u s t m e n t s
     -----------------------------------------
 [1] Block Frequency Test - block length(M):         128
 [2] NonOverlapping Template Test - block length(m): 9
 [3] Overlapping Template Test - block length(m):    9
 [4] Approximate Entropy Test - block length(m):     10
 [5] Serial Test - block length(m):                  16
 [6] Linear Complexity Test - block length(M):       500

Select Test (0 to continue): 0
```

7. 指定随机数的组数，在步骤 2 中已经说明，这里把随机数分为 1000 组。

```
islab@ubuntu: ~/Workspace/sts
 [07] Discrete Fourier Transform      [08] Nonperiodic Template Matchings
 [09] Overlapping Template Matchings  [10] Universal Statistical
 [11] Approximate Entropy             [12] Random Excursions
 [13] Random Excursions Variant       [14] Serial
 [15] Linear Complexity

      INSTRUCTIONS
         Enter 0 if you DO NOT want to apply all of the
         statistical tests to each sequence and 1 if you DO.

Enter Choice: 1

     P a r a m e t e r   A d j u s t m e n t s
     -----------------------------------------
 [1] Block Frequency Test - block length(M):         128
 [2] NonOverlapping Template Test - block length(m): 9
 [3] Overlapping Template Test - block length(m):    9
 [4] Approximate Entropy Test - block length(m):     10
 [5] Serial Test - block length(m):                  16
 [6] Linear Complexity Test - block length(M):       500

Select Test (0 to continue): 0

How many bitstreams? 1000
```

8. 选择随机数文件的格式，因为该测试中随机数是以 ASCII 码的“0”和“1”形式存储的，因此这里选择“0”。

```
islab@ubuntu: ~/Workspace/sts
      INSTRUCTIONS
         Enter 0 if you DO NOT want to apply all of the
         statistical tests to each sequence and 1 if you DO.

Enter Choice: 1

     P a r a m e t e r   A d j u s t m e n t s
     -----------------------------------------
 [1] Block Frequency Test - block length(M):         128
 [2] NonOverlapping Template Test - block length(m): 9
 [3] Overlapping Template Test - block length(m):    9
 [4] Approximate Entropy Test - block length(m):     10
 [5] Serial Test - block length(m):                  16
 [6] Linear Complexity Test - block length(M):       500

Select Test (0 to continue): 0

How many bitstreams? 1000

Input File Format:
 [0] ASCII - A sequence of ASCII 0's and 1's
 [1] Binary - Each byte in data file contains 8 bits of data

Select input mode:  0
```

9. 全部设置完成，开始测试。

```
islab@ubuntu: ~/Workspace/sts
Enter Choice: 1

     P a r a m e t e r   A d j u s t m e n t s
     -----------------------------------------
 [1] Block Frequency Test - block length(M):         128
 [2] NonOverlapping Template Test - block length(m): 9
 [3] Overlapping Template Test - block length(m):    9
 [4] Approximate Entropy Test - block length(m):     10
 [5] Serial Test - block length(m):                  16
 [6] Linear Complexity Test - block length(M):       500

Select Test (0 to continue): 0

How many bitstreams? 1000

Input File Format:
 [0] ASCII - A sequence of ASCII 0's and 1's
 [1] Binary - Each byte in data file contains 8 bits of data

Select input mode:  0

  Statistical Testing In Progress.........
```

10. 当出现“Statistical Testing Complete!!!!!!!!!!!”后，测试完成。在 sts/experiments/AlgorithmTesting 目录下，会出现“finalAnalysisReport.txt”和“freq.txt”。该目录下与每种测试标准对应的文件夹中会有更详细地数据记录。

```
islab@ubuntu: ~/Workspace/sts
     P a r a m e t e r   A d j u s t m e n t s
     -----------------------------------------
 [1] Block Frequency Test - block length(M):         128
 [2] NonOverlapping Template Test - block length(m): 9
 [3] Overlapping Template Test - block length(m):    9
 [4] Approximate Entropy Test - block length(m):     10
 [5] Serial Test - block length(m):                  16
 [6] Linear Complexity Test - block length(M):       500

Select Test (0 to continue): 0

How many bitstreams? 1000

Input File Format:
 [0] ASCII - A sequence of ASCII 0's and 1's
 [1] Binary - Each byte in data file contains 8 bits of data

Select input mode:  0

  Statistical Testing In Progress.........

  Statistical Testing Complete!!!!!!!!!!!!

islab@ubuntu:~/Workspace/sts$
```

11. 测试结果说明。打开“finalAnalysisReport.txt”文件，从文件最后的说明部分可以看到，除“随机游动测试”和“随机游动状态频数测试”之外，每项测试至少要通过 980 组才能说明通过了该项测试。同样，“随机游动测试”和“随机游动状态频数测试”也要满足其指定的条件。“PROPORTION”列说明了总组数中通过的组数，如果某项测试的“P-VALUE”列或“PROPORTION”列标有“*”，则表明该项测试未通过。