

NIST 测试使用手册

运行环境：ubuntu(windows 系统请安装 VMware 虚拟机并下载 ubuntu 系统)

步骤一：打开 Matlab，修改本目录下的 NIST.m 脚本内容，将脚本内示例混沌加密算法替换为所需待测的加密算法并运行，生成 NIST.txt 文件。

步骤二：打开虚拟机运行 ubuntu 系统，打开终端，将 NIST.txt 与 sts-2_1_2.zip 文件拷贝至虚拟机中，在拷贝的目录下进行后续操作。

步骤三：对包进行解压缩，解压在拷贝目录下。

```
rrior@zhangziruideMBP sts-2.1.2 % ./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
```

进入到解压缩的该目录下（输入命令 cd 文件名），输入 make 进行编译 makefile 文件，得到 assess 文件（编译成功后该目录下会有 assess 文件）在该目录下输入 ./assess data-length，data-length 为测试的数据长度，此处 data-length 输入值为 1000000（注：NIST 一次测量的最大数据长度为 1000000bits，而我们的文件大小为 100000000bits,在后续的 bitstreamsnum 中输入 100，bitstreamsnum*data-length=总文件大小）

步骤四：运行 NIST 程序后，会进入以下界面：

```
sts-2.1.2 — assess 100000000 — 80x24
/usr/bin/gcc -o obj/utilities.o -c -Wall ./src/utilities.c
/usr/bin/gcc -o obj/generators.o -c -Wall ./src/generators.c
/usr/bin/gcc -o obj/genutils.o -c -Wall ./src/genutils.c
/usr/bin/gcc -o assess ./obj/assess.o ./obj/frequency.o ./obj/blockFrequency.o .
./obj/cusum.o ./obj/runs.o ./obj/longestRunOfOnes.o ./obj/serial.o ./obj/rank.o .
./obj/discreteFourierTransform.o ./obj/nonOverlappingTemplateMatchings.o ./obj/ov
erlappingTemplateMatchings.o ./obj/universal.o ./obj/approximateEntropy.o ./obj/
randomExcursions.o ./obj/randomExcursionsVariant.o ./obj/linearComplexity.o ./ob
j/dfft.o ./obj/cephes.o ./obj/matrix.o ./obj/utilities.o ./obj/generators.o ./ob
j/genutils.o -lm
rrior@zhangziruideMBP sts-2.1.2 % ./assess 100000000
  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: NIST.txt
```

根据生成器提示选择 0 输入文件，输入 NIST.txt，之后则是选择测试类型，即下面的 15 种测试类型：

```
sts-2.1.2 — assess 100000000 — 80x24

[8] Micali-Schnorr          [9] G Using SHA-1

Enter Choice: 0

User Prescribed Input File: NIST.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
```

它有一个提示可以测试上述 15 种测试，即 Enter Choice 输入 1。输入 1 后会弹出以下界面，数值不需要修改填写 0 继续即可：

```
sts-2.1.2 — assess 100000000 — 80x24

[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

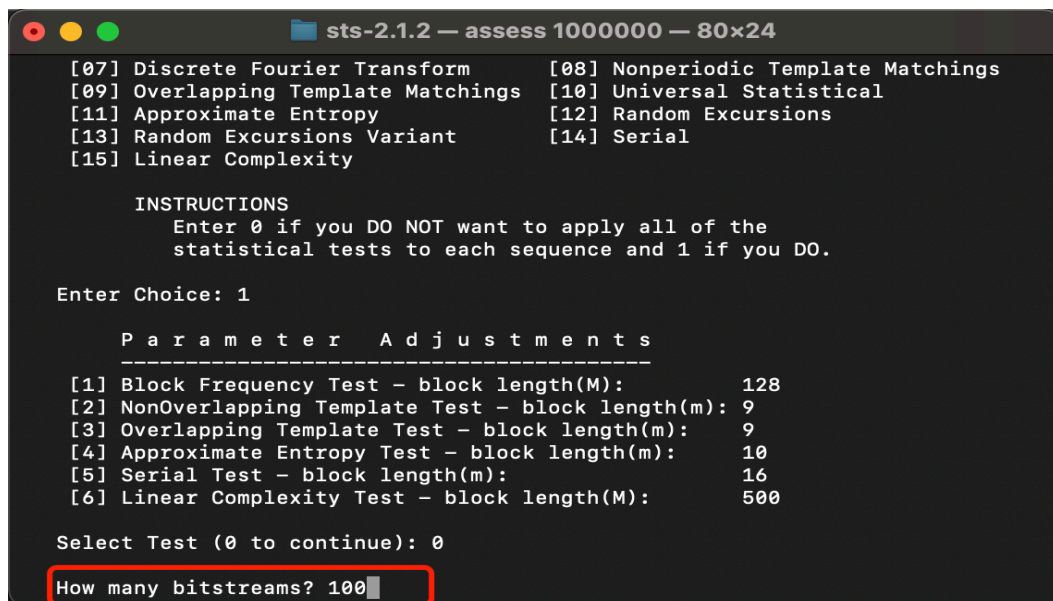
P a r a m e t e r   A d j u s t m e n t s
-----

[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
```

确认后需要继续填写 bitstreamsnum, 这里填写 100

($\text{bitstreamsnum} \times \text{datalength} = \text{总文件大小}$) :



```
sts-2.1.2 — assess 1000000 — 80x24

[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.

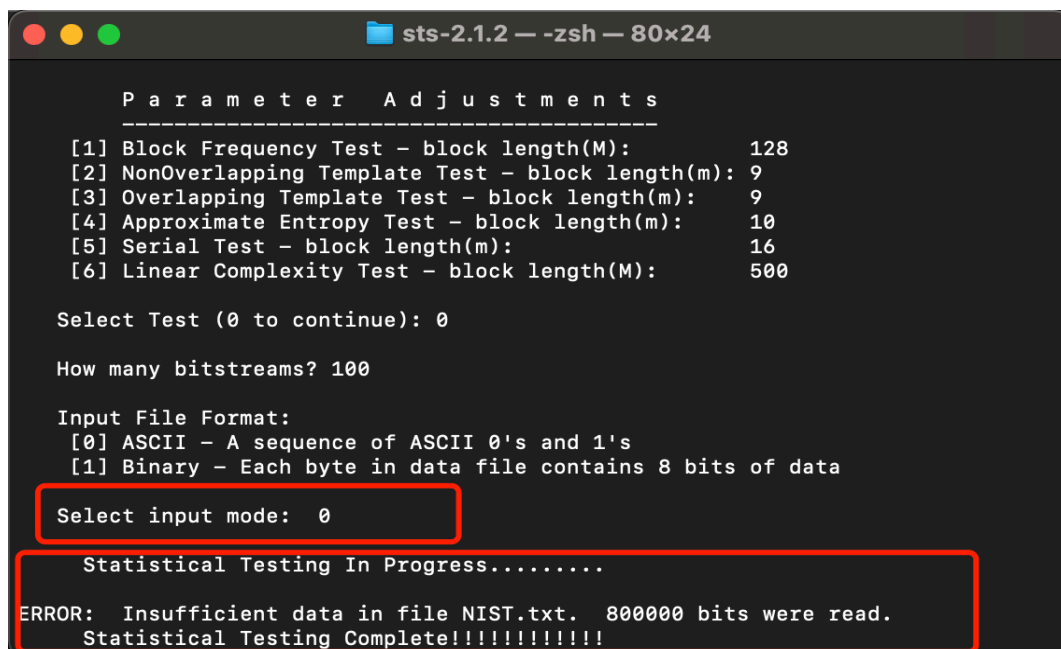
Enter Choice: 1

  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? 100
```

最后一项会问输入文件的形式是 ASCII 类型的数据构成的序列 (ASCII 中的 0 和 1) 还是 8 位的二进制数据, 此处选 0, 测试开始运行, 程序运行时间较长, 大概需要 5-10 分钟左右:



```
sts-2.1.2 — -zsh — 80x24

  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? 100

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.....
ERROR: Insufficient data in file NIST.txt. 800000 bits were read.
Statistical Testing Complete!!!!!!!!!!!!
```

当数据测试完成后, 会在测试包所在目录的 experiments->AlgorithmTesting 目录下生成两个测试报告文件, 他们分别是 finalAnalysisReport.txt 和 freq.txt。

finalAnalysisReport.txt												
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES												
generator is <NIST.txt>												
C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
15	10	6	7	14	7	8	14	14	5	0.137282	96/100	Frequency
8	9	15	11	12	6	8	13	9	9	0.678686	100/100	BlockFrequency
15	10	12	10	6	11	5	12	9	10	0.574903	98/100	CumulativeSums
16	11	8	9	11	14	5	10	5	11	0.275709	96/100	CumulativeSums
7	10	10	17	9	12	4	12	12	7	0.236810	100/100	Runs
12	13	5	8	14	6	10	16	6	10	0.181557	99/100	LongestRun
8	8	10	9	12	9	10	13	8	13	0.935716	99/100	Rank
12	6	12	11	13	9	12	11	7	7	0.759756	100/100	FFT
6	13	10	7	8	11	8	11	11	15	0.637119	100/100	NonOverlappingTemplate
12	10	15	13	8	5	8	10	11	8	0.574903	98/100	NonOverlappingTemplate
15	9	6	9	5	11	7	13	9	16	0.191687	99/100	NonOverlappingTemplate
12	10	12	10	10	9	9	11	10	7	0.991468	100/100	NonOverlappingTemplate
9	8	7	7	11	14	9	11	13	11	0.816537	100/100	NonOverlappingTemplate
9	12	7	9	10	11	10	8	10	14	0.935716	99/100	NonOverlappingTemplate
10	9	14	8	12	13	6	5	16	7	0.213309	100/100	NonOverlappingTemplate
10	9	9	13	11	10	13	8	7	10	0.946308	99/100	NonOverlappingTemplate
13	6	15	12	10	13	6	8	8	9	0.455937	97/100	NonOverlappingTemplate

freq.txt												
FILE = NIST.txt ALPHA = 0.0100												
BITSREAD = 1000000 0s = 500108 1s = 499892												
BITSREAD = 1000000 0s = 499715 1s = 500285												
BITSREAD = 1000000 0s = 500105 1s = 499895												
BITSREAD = 1000000 0s = 500840 1s = 499160												
BITSREAD = 1000000 0s = 500435 1s = 499565												
BITSREAD = 1000000 0s = 500939 1s = 499061												
BITSREAD = 1000000 0s = 500038 1s = 499962												
BITSREAD = 1000000 0s = 500128 1s = 499872												
BITSREAD = 1000000 0s = 498671 1s = 501329												
BITSREAD = 1000000 0s = 500070 1s = 499930												
BITSREAD = 1000000 0s = 499621 1s = 500379												
BITSREAD = 1000000 0s = 500355 1s = 499645												
BITSREAD = 1000000 0s = 499659 1s = 500341												
BITSREAD = 1000000 0s = 499637 1s = 500363												
BITSREAD = 1000000 0s = 500169 1s = 499831												
BITSREAD = 1000000 0s = 500123 1s = 499877												
BITSREAD = 1000000 0s = 501171 1s = 498829												
BITSREAD = 1000000 0s = 499630 1s = 500370												
BITSREAD = 1000000 0s = 500797 1s = 499203												
BITSREAD = 1000000 0s = 499253 1s = 500747												
BITSREAD = 1000000 0s = 499812 1s = 500188												
BITSREAD = 1000000 0s = 500175 1s = 499825												
BITSREAD = 1000000 0s = 500441 1s = 499559												
BITSREAD = 1000000 0s = 500211 1s = 499789												
BITSREAD = 1000000 0s = 500582 1s = 499418												

以上测试结果以 P 值为准，在 ALPHA = 0.0100 条件下（默认值），当 P 值大于 0.01 时，表示随机性良好，且值越大性能越好。