NIST Statistical Test Suite: An Introduction

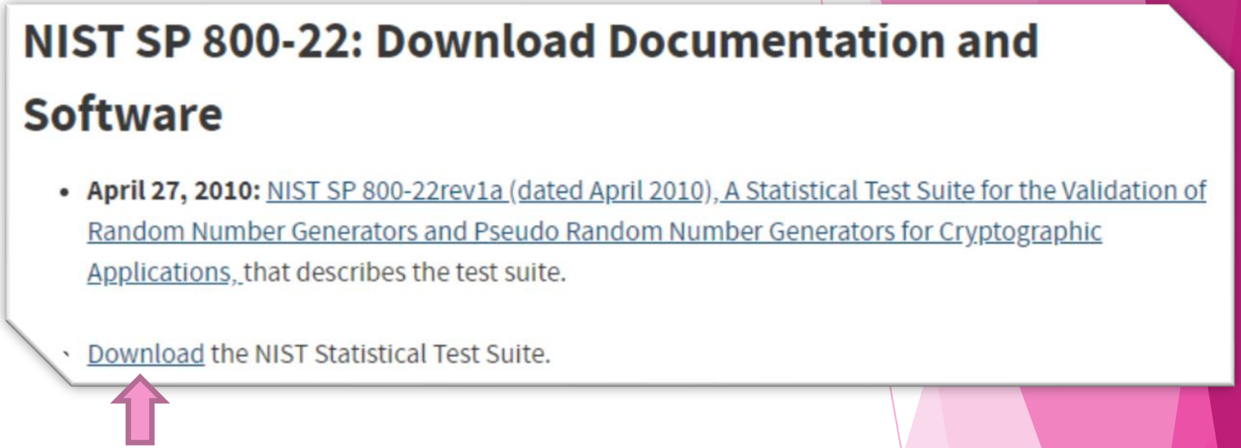
By Farah Ferdaus and Tauhidur Rahman

What is NIST STS?

- NIST Statistical Test Suite is an important testing suite for randomness analysis often used for formal certifications or approvals.
- For More detail visit:
  - https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final (Manual guide by NIST)
  - https://crocs.fi.muni.cz/lib/exe/fetch.php?media=public:research:romjist_v11_for_publish.pdf (A short explanation of 15 NIST tests)

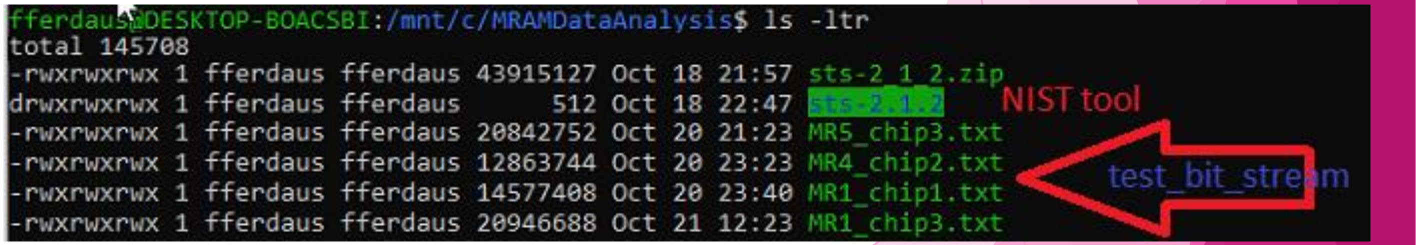
Download the NIST STS tool

- To download NIST STS tool visit:
  - https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software
- Linux machine required
  - Tips: Use “Windows Subsystem for Linux” for windows 10 operating system (https://docs.microsoft.com/en-us/windows/wsl/install-win10)
- NOTE: Keep the unzipped version of the tool on the same folder (directory) where the test_bit_stream files are located.



NIST SP 800-22: Download Documentation and Software

- **April 27, 2010:** NIST SP 800-22rev1a (dated April 2010), A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, that describes the test suite.
- Download the NIST Statistical Test Suite.

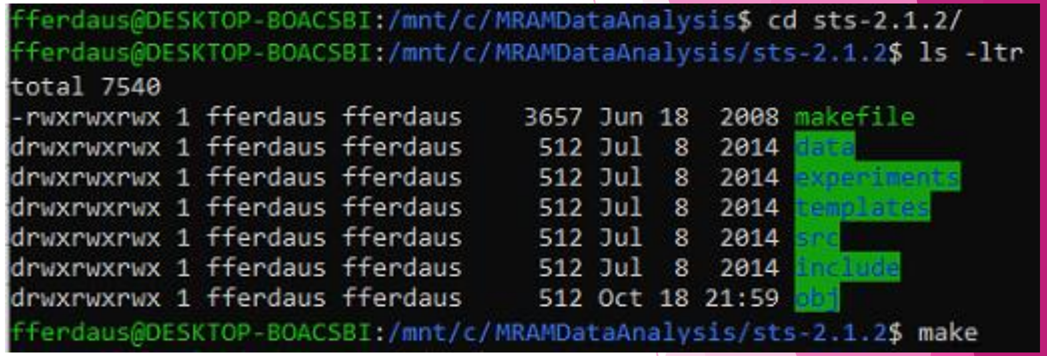


```
fferdaus@DESKTOP-BOACSBI:/mnt/c/MRAMDataAnalysis$ ls -ltr
total 145708
-rwxrwxrwx 1 fferdaus fferdaus 43915127 Oct 18 21:57 sts-2 1 2.zip
drwxrwxrwx 1 fferdaus fferdaus      512 Oct 18 22:47 sts-2.1.2
-rwxrwxrwx 1 fferdaus fferdaus 20842752 Oct 20 21:23 MR5_chip3.txt
-rwxrwxrwx 1 fferdaus fferdaus 12863744 Oct 20 23:23 MR4_chip2.txt
-rwxrwxrwx 1 fferdaus fferdaus 14577408 Oct 20 23:40 MR1_chip1.txt
-rwxrwxrwx 1 fferdaus fferdaus 20946688 Oct 21 12:23 MR1_chip3.txt
```

Install the NIST STS tool

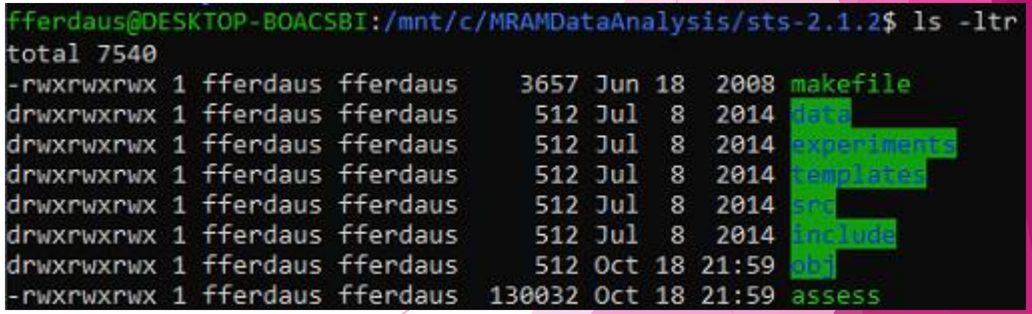
- To install NIST STS tool go to the <sts-2.1.2> directory and type “***make***” to execute the ***makefile***.
  - *Might require to install make package:*

    ```
    sudo apt install make
    ```



```
fferdaus@DESKTOP-BOACSBI:/mnt/c/MRAMDataAnalysis$ cd sts-2.1.2/
fferdaus@DESKTOP-BOACSBI:/mnt/c/MRAMDataAnalysis/sts-2.1.2$ ls -ltr
total 7540
-rwxrwxrwx 1 fferdaus fferdaus   3657 Jun 18  2008 makefile
drwxrwxrwx 1 fferdaus fferdaus    512 Jul  8  2014 data
drwxrwxrwx 1 fferdaus fferdaus    512 Jul  8  2014 experiments
drwxrwxrwx 1 fferdaus fferdaus    512 Jul  8  2014 templates
drwxrwxrwx 1 fferdaus fferdaus    512 Jul  8  2014 src
drwxrwxrwx 1 fferdaus fferdaus    512 Jul  8  2014 include
drwxrwxrwx 1 fferdaus fferdaus    512 Oct 18 21:59 obj
fferdaus@DESKTOP-BOACSBI:/mnt/c/MRAMDataAnalysis/sts-2.1.2$ make
```

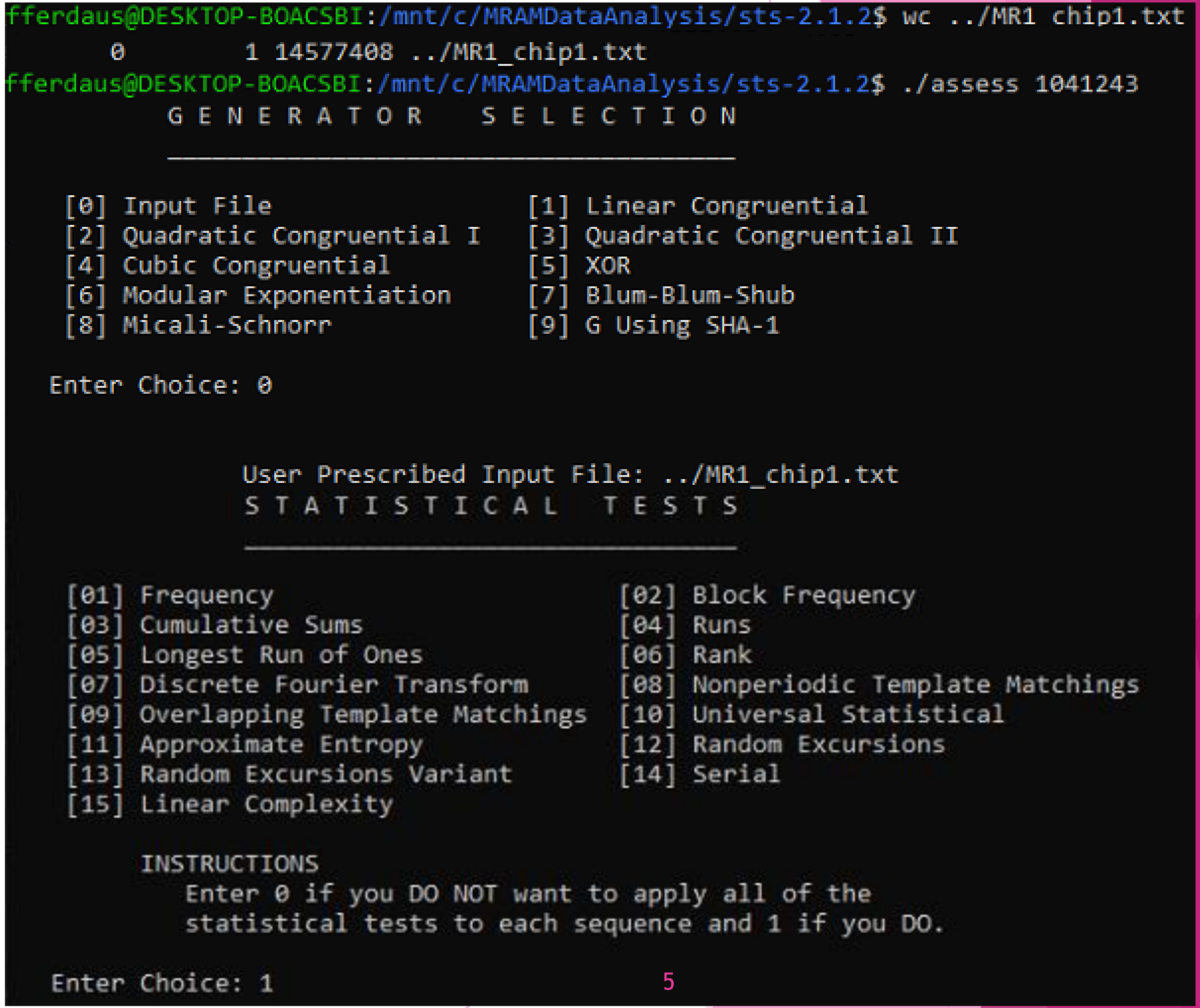
- After successful installation, An executable file named ***assess*** should appear in the project directory.



```
fferdaus@DESKTOP-BOACSBI:/mnt/c/MRAMDataAnalysis/sts-2.1.2$ ls -ltr
total 7540
-rwxrwxrwx 1 fferdaus fferdaus   3657 Jun 18  2008 makefile
drwxrwxrwx 1 fferdaus fferdaus    512 Jul  8  2014 data
drwxrwxrwx 1 fferdaus fferdaus    512 Jul  8  2014 experiments
drwxrwxrwx 1 fferdaus fferdaus    512 Jul  8  2014 templates
drwxrwxrwx 1 fferdaus fferdaus    512 Jul  8  2014 src
drwxrwxrwx 1 fferdaus fferdaus    512 Jul  8  2014 include
drwxrwxrwx 1 fferdaus fferdaus    512 Oct 18 21:59 obj
-rwxrwxrwx 1 fferdaus fferdaus 130032 Oct 18 21:59 assess
```

Run the Test Code

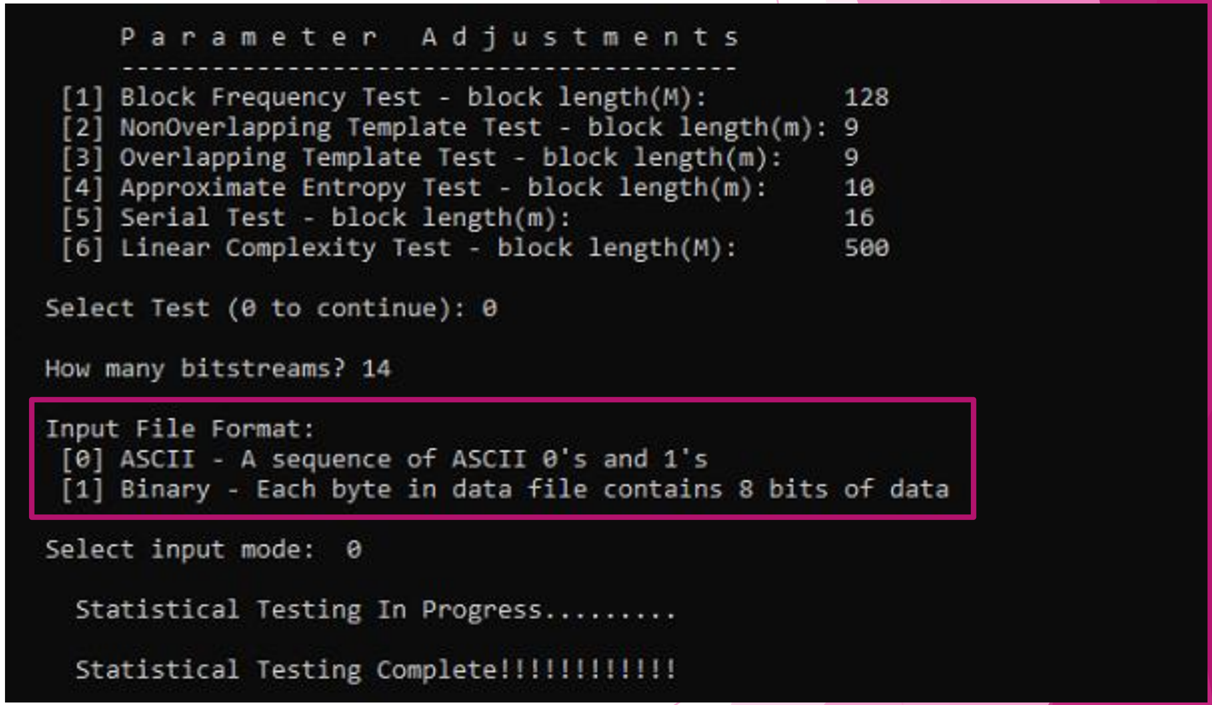
- To invoke the NIST STS, type the following:
  - `./assess <sequenceLength>`
  - Min bit stream length (sequenceLength) should be 10^6.
- A series of menu prompts will be displayed in order to select the data to be analyzed and the statistical tests to be applied.



```
fferdaus@DESKTOP-BOACSBI:/mnt/c/MRAMDataAnalysis/sts-2.1.2$ wc ../MR1 chip1.txt
       0        1 14577408 ../MR1_chip1.txt
fferdaus@DESKTOP-BOACSBI:/mnt/c/MRAMDataAnalysis/sts-2.1.2$ ./assess 1041243
           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: ../MR1_chip1.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
```

Run the Test Code

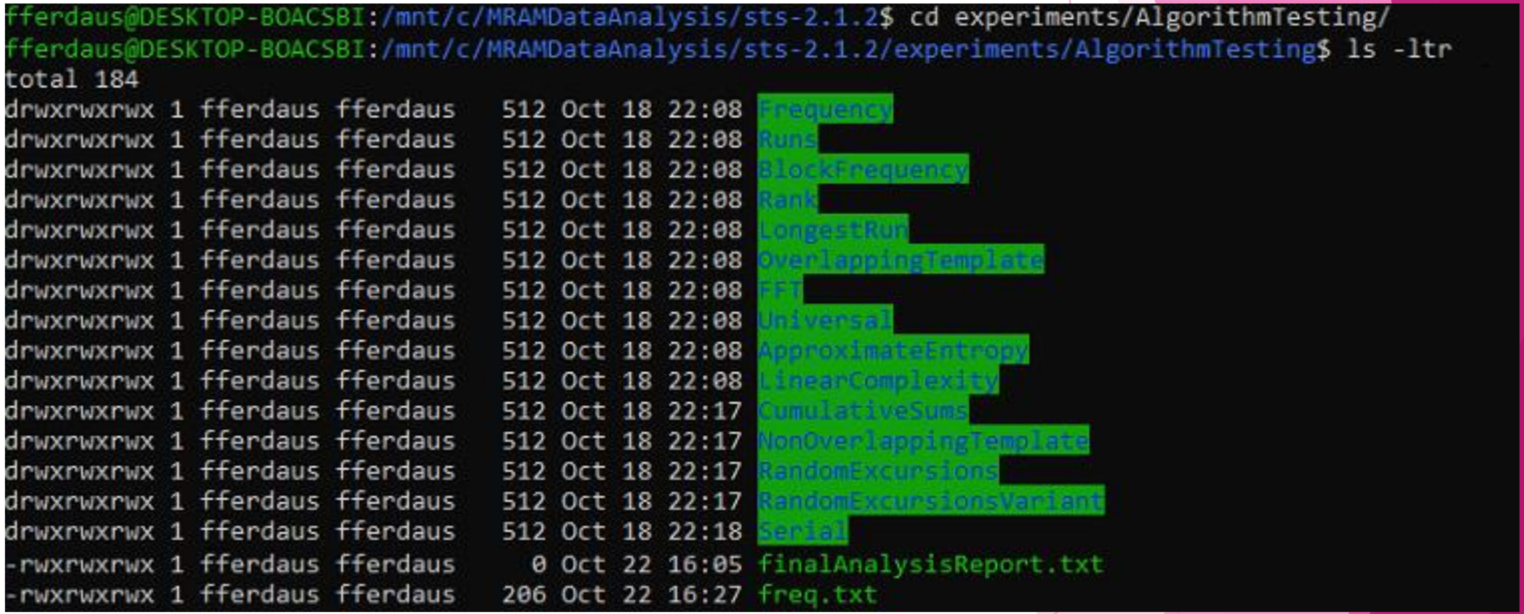
- Min number of bitstream sequence should be 10 to evaluate all tests.
  - Number of bits in the file must be ≥ (#bitstream × `sequenceLength`)
- The user must specify whether the file consists of bits stored in ASCII format (containing 0’s and 1’s) or binary format (packing 8-bit data in a single byte).



```
        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? 14

   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!!!!!!!!!!!!
```

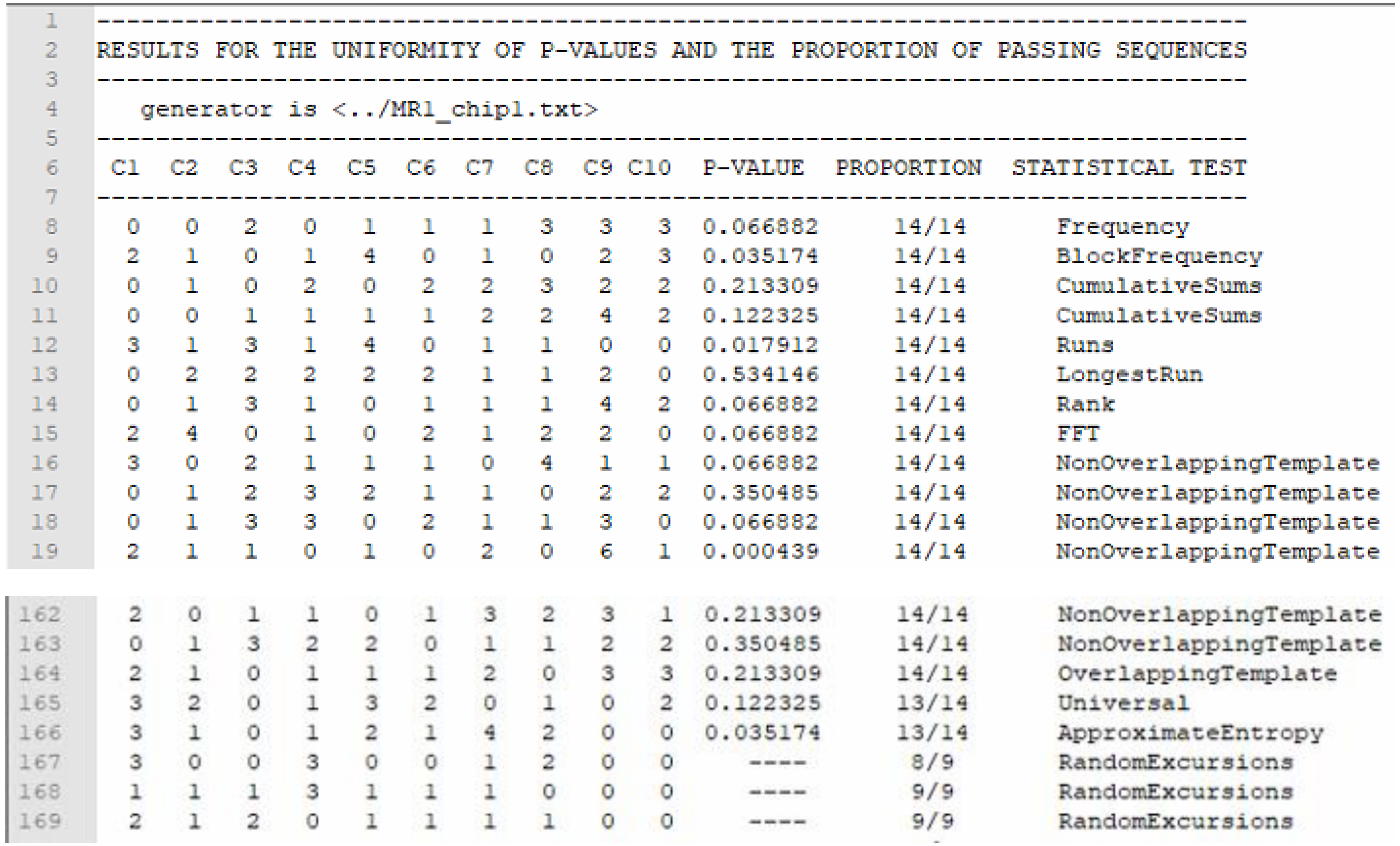
Empirical results Location

- Once the testing process is complete, the empirical results can be found in the ***experiments/*** subdirectory.
- A file ***finalAnalysisReport.txt*** (summary report) will be generated when statistical testing is complete which is located at ***experiments/AlgorithmTesting/*** subdirectory.



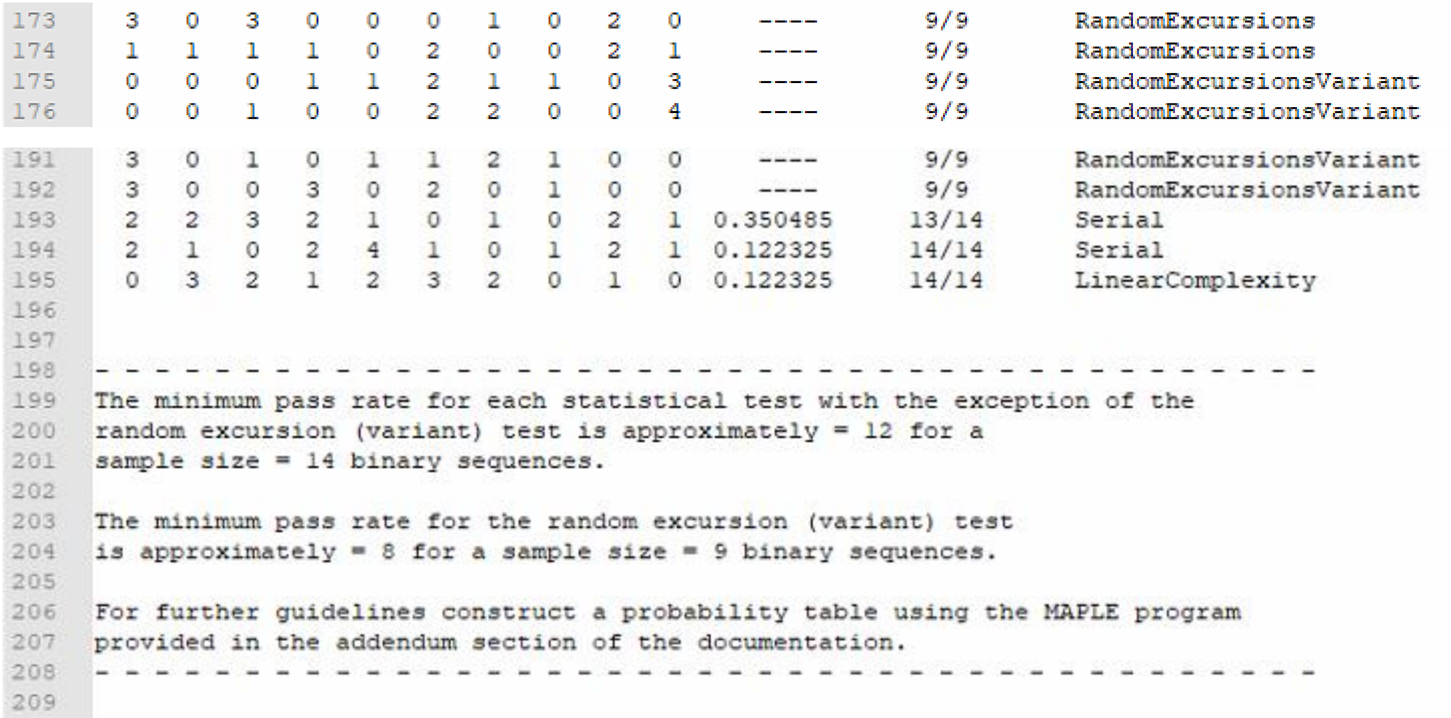
```
fferdaus@DESKTOP-BOACSBI:/mnt/c/MRAMDataAnalysis/sts-2.1.2$ cd experiments/AlgorithmTesting/
fferdaus@DESKTOP-BOACSBI:/mnt/c/MRAMDataAnalysis/sts-2.1.2/experiments/AlgorithmTesting$ ls -ltr
total 184
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:08 Frequency
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:08 Runs
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:08 BlockFrequency
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:08 Rank
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:08 LongestRun
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:08 OverlappingTemplate
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:08 FFT
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:08 Universal
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:08 ApproximateEntropy
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:08 LinearComplexity
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:17 CumulativeSums
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:17 NonOverlappingTemplate
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:17 RandomExcursions
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:17 RandomExcursionsVariant
drwxrwxrwx 1 fferdaus fferdaus   512 Oct 18 22:18 Serial
-rwxrwxrwx 1 fferdaus fferdaus     0 Oct 22 16:05 finalAnalysisReport.txt
-rwxrwxrwx 1 fferdaus fferdaus   206 Oct 22 16:27 freq.txt
```

Depiction of the Final Analysis Report



```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <../MR1_chip1.txt>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
  0   0   2   0   1   1   1   3   3   3  0.066882     14/14      Frequency
  2   1   0   1   4   0   1   0   2   3  0.035174     14/14      BlockFrequency
  0   1   0   2   0   2   2   3   2   2  0.213309     14/14      CumulativeSums
  0   0   1   1   1   1   2   2   4   2  0.122325     14/14      CumulativeSums
  3   1   3   1   4   0   1   1   0   0  0.017912     14/14      Runs
  0   2   2   2   2   2   1   1   2   0  0.534146     14/14      LongestRun
  0   1   3   1   0   1   1   1   4   2  0.066882     14/14      Rank
  2   4   0   1   0   2   1   2   2   0  0.066882     14/14      FFT
  3   0   2   1   1   1   0   4   1   1  0.066882     14/14      NonOverlappingTemplate
  0   1   2   3   2   1   1   0   2   2  0.350485     14/14      NonOverlappingTemplate
  0   1   3   3   0   2   1   1   3   0  0.066882     14/14      NonOverlappingTemplate
  2   1   1   0   1   0   2   0   6   1  0.000439     14/14      NonOverlappingTemplate

  2   0   1   1   0   1   3   2   3   1  0.213309     14/14      NonOverlappingTemplate
  0   1   3   2   2   0   1   1   2   2  0.350485     14/14      NonOverlappingTemplate
  2   1   0   1   1   1   2   0   3   3  0.213309     14/14      OverlappingTemplate
  3   2   0   1   3   2   0   1   0   2  0.122325     13/14      Universal
  3   1   0   1   2   1   4   2   0   0  0.035174     13/14      ApproximateEntropy
  3   0   0   3   0   0   1   2   0   0    ----        8/9       RandomExcursions
  1   1   1   3   1   1   1   0   0   0    ----        9/9       RandomExcursions
  2   1   2   0   1   1   1   1   0   0    ----        9/9       RandomExcursions
```

Depiction of the Final Analysis Report



```
 3   0   3   0   0   0   1   0   2   0      ----       9/9       RandomExcursions
 1   1   1   1   0   2   0   0   2   1      ----       9/9       RandomExcursions
 0   0   0   1   1   2   1   1   0   3      ----       9/9       RandomExcursionsVariant
 0   0   1   0   0   2   2   0   0   4      ----       9/9       RandomExcursionsVariant

 3   0   1   0   1   1   2   1   0   0      ----       9/9       RandomExcursionsVariant
 3   0   0   3   0   2   0   1   0   0      ----       9/9       RandomExcursionsVariant
 2   2   3   2   1   0   1   0   2   1   0.350485     13/14      Serial
 2   1   0   2   4   1   0   1   2   1   0.122325     14/14      Serial
 0   3   2   1   2   3   2   0   1   0   0.122325     14/14      LinearComplexity


- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 12 for a
sample size = 14 binary sequences.

The minimum pass rate for the random excursion (variant) test
is approximately = 8 for a sample size = 9 binary sequences.

For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

```