Project Report

IMPLEMENTATION OF TEST CASES IN NIST RANDOMNESS TEST

Presented By :

Mohd Danish Kaleem, 510815062
Naman Mehta, 510815067
Chandan Sharma, 510815076

Overview

*What are Random Numbers?

*Significance of Random Numbers

*What is NIST(National Institute of Standards and Technology) Test Suite?

Frequency Test

Test Purpose :

1. The focus of the test is the proportion of zeroes and ones for the entire sequence

2. This test makes use of that approximation to assess the closeness of the fraction of 1's to 1/2.

3. All subsequent tests are conditioned on having passed this first basic test

Frequency Test Within a Block

Test Purpose :

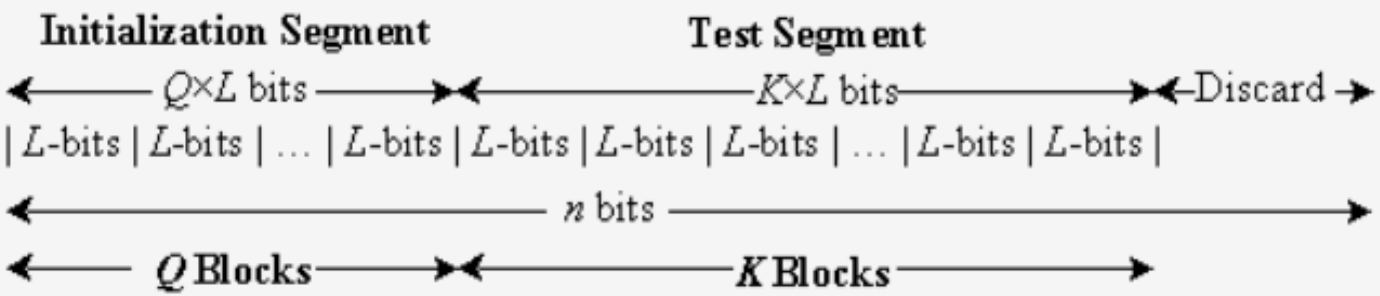
1. The focus of the test is the proportion of ones within M-bit blocks
2. Decomposing the test sequence into a number of nonoverlapping subsequences
3. For each substring, the proportion of ones is computed.
4. A chi-square statistic compares these substring proportions to the ideal
5. Small P-values indicate large deviations from the equal proportion of ones and zeros

$$X^2(obs) = 4M \sum_{i=1}^{N} \left[\pi_i - \frac{1}{2} \right]^2$$

Maurer's "Universal Statistical" Test

1. The focus of this test is the number of bits between matching patterns (a measure that is related to the length of a compressed sequence).
2. "the correct quality measure for a secret-key source in a cryptographic application."-Maurer
3. "related to the running time of [an] enemy's optimal key-search strategy,"
4. The purpose of the test is to detect whether or not the sequence can be significantly compressed without loss of information.
5. A significantly compressible sequence is considered to be non-random.
6. The sum of the log 2 distances between matching L-bit templates

Maurer's "Universal Statistical" Test



For example, if ε = 01011010011101010111, then n = 20. If L = 2 and Q = 4, then K = floor(n/L) -Q = floor(20/2) - 4 = 6 . The initialization segment is 01011010; the test segment is 011101010111.

Maurer's "Universal Statistical" Test

Block	Type	Contents
1	Initialization Segment	01
2		01
3		10
4		10
5	Test Segment	01
6		11
7		01
8		01
9		01
10		11

	Possible L-bit Value			
	00 (saved in T_0)	01 (saved in T_1)	10 (saved in T_2)	11 (saved in T_3)
Initialization	0	2	4	0

for eg-For block 5 (the 1 st test block): 5 is placed in the "01" row of the table (i.e., T 1), and sum=log 2 (5-2) = 1.584962501

Binary Matrix Rank Test

Test Purpose:

- To check for linear dependence among fixed-length substrings of the original sequence.
- sequence: construct matrices of successive zeroes and ones from the sequence, and check for linear dependence among the rows or columns of the constructed matrices.
- matrices. The deviation of the rank -or rank deficiency -of the matrices from a theoretically expected value gives the statistic of interest

Non Overlapping Template Matching test

Test Purpose:

*This test rejects sequences exhibiting too many or too few occurrences of a given aperiodic pattern.

*We consider a test based on patterns for fixed length m. A table of selected aperiodic words out of such patterns for m = 2, …, 8 is provided to us beforehand.

Overlapping Template Matching test

Test Purpose:

*This test rejects sequences which show too many or too few occurrences of m-runs of ones, but can be easily modified to detect irregular occurrences of any periodic pattern B..

*We consider a test based on patterns for fixed length m. A table of selected aperiodic words out of such patterns for m = 2, …, 8 is provided to us beforehand.

Runs test

Test Purpose:

*This test calculates the total number of runs in a sequence.

*It determines whether the oscillation between the ones and zeroes are too slow or too fast

Longest runs in a block test

Test Purpose:

*This test is designed to calculate the longest run of ones within M-bit blocks.

* The purpose of this test is to determine whether the length of the longest run of ones within the tested sequence is consistent with the length of the longest run of ones that would be expected in a random sequence

Cumulative Sum test

Test Purpose:

* This test is designed to determine whether the cumulative sum of the partial sequences occurring in the tested sequence is too large or too small relative to the expected behaviour of that cumulative sum for random sequences.

* It is recommended that each sequence to be tested consist of a minimum of 100 bits (i.e., $n >= 100$)