Statistical Testing of Random Number Generators

Juan Soto

soto@nist.gov

301/975-4641

Outline

- Statistical Hypotheses Testing
- The NIST Statistical Test Suite
- Repeated Trial Assessment
- Current Work Items
- Summary

Statistical Test Suites

Author	***Source***
Knuth	The Art of Computer Programming Volume 2
Marsaglia	DIEHARD
Gustafson, et. al.	Crypt-X
Menezes, et. al.	Handbook of Applied Cryptography
Rukhin, et. al.	NIST Statistical Test Suite (STS)

Statistical Hypotheses Testing:
Evaluation Approaches

- Threshold Values
  - A binary sequence fails a test if the test statistic falls below a pre-specified threshold value.
  - *e.g., Sequence Complexity Test (Crypt-XS)*
- Probability Values (P-values)
  - A binary sequence fails a test if the test statistic falls below a preset significance level.
  - *e.g., Each statistical test in the NIST STS*

The NIST Statistical Test Suite

- NIST Framework
  - Given a finite length binary sequence, S, compute a test statistic and its corresponding P-value.
- Application of the Statistical Tests
  - 50-60 P-values per binary sequence.
  - Very small P-values indicate failure of a test.

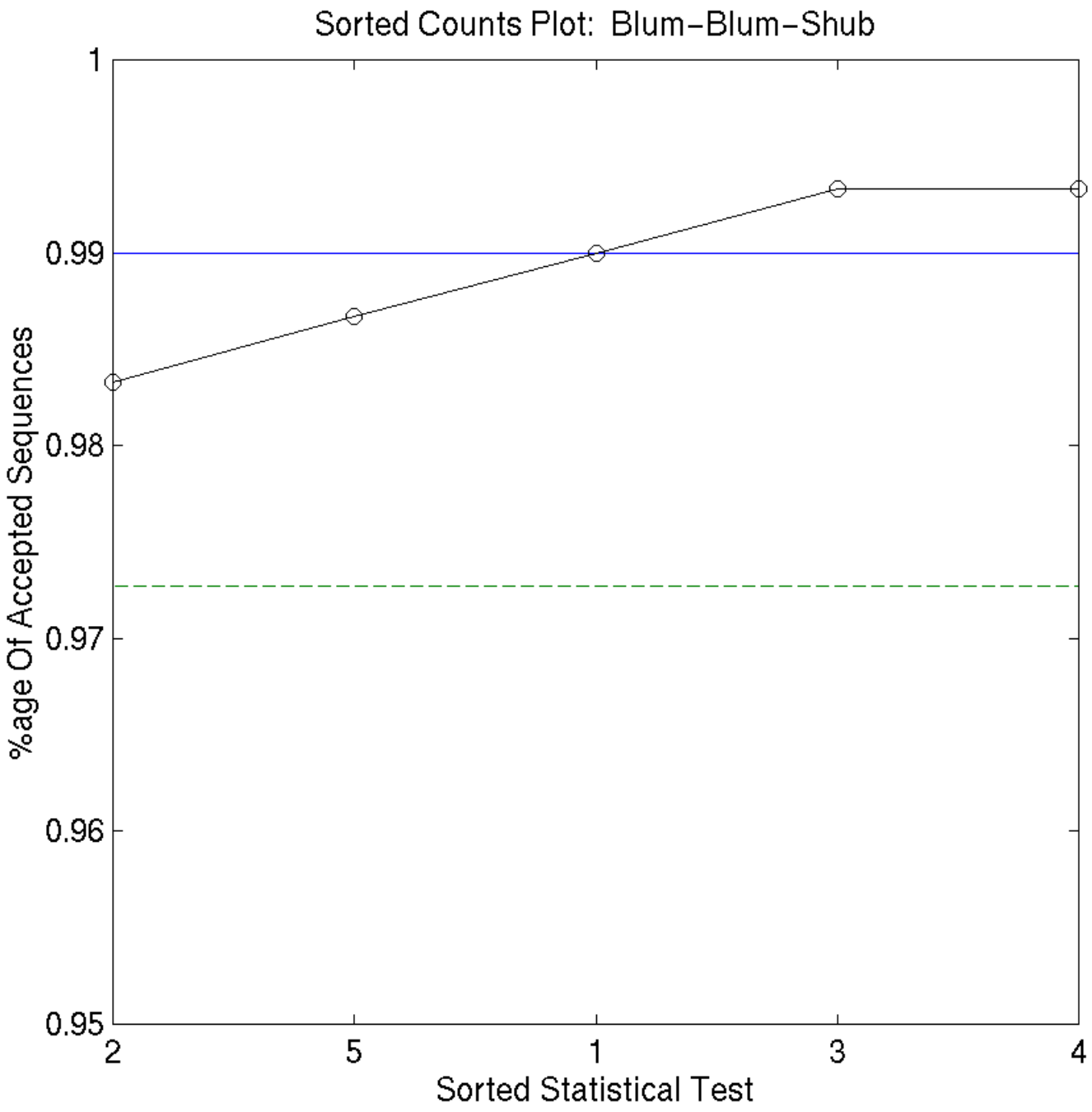
The NIST Statistical Test Suite

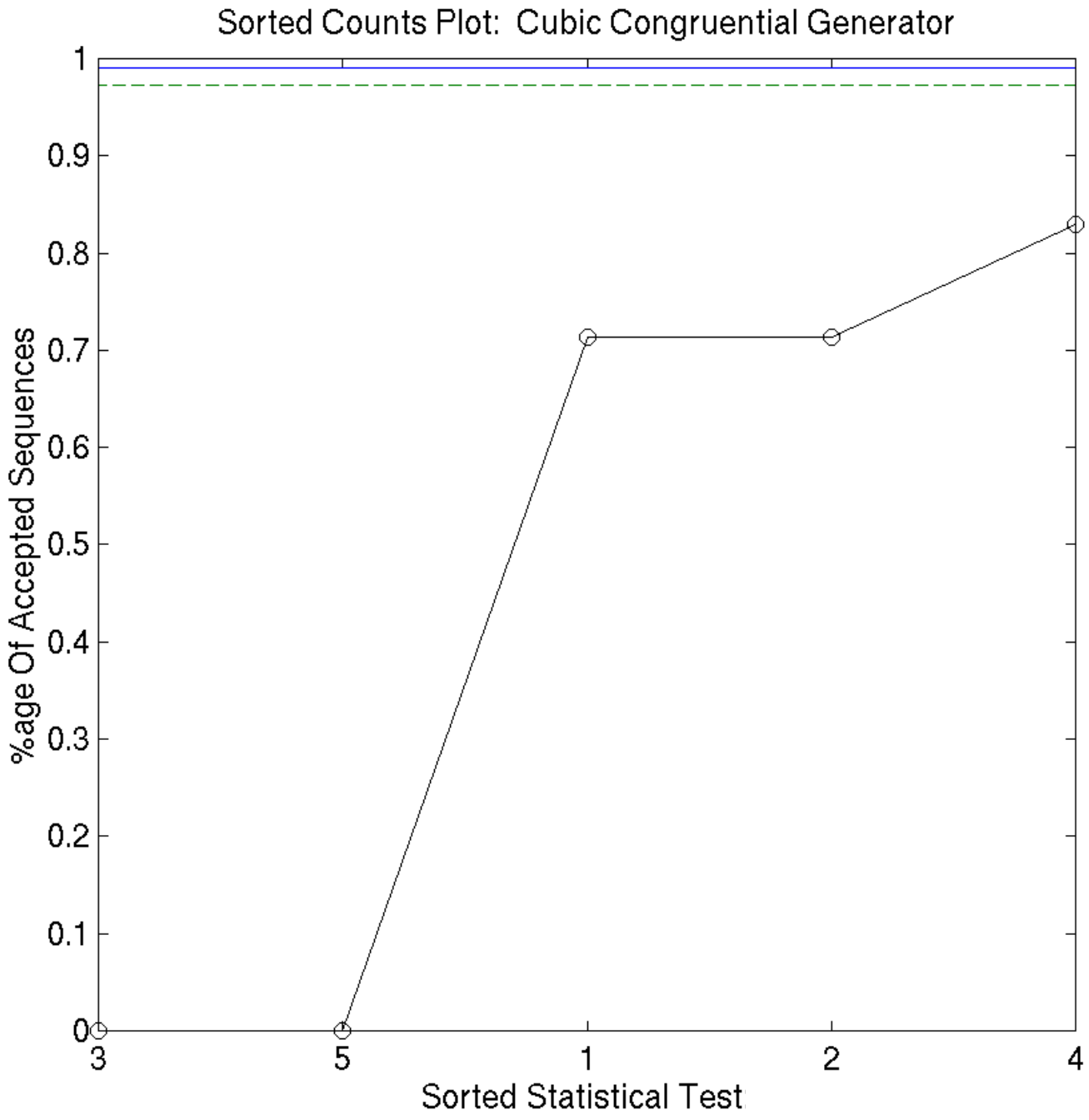
Strings Viewed As Random Walks	Look for Patterns		**Complexity/ Compression**
Frequency	Runs	Long Runs	**Rank**
Block Frequency	Aperiodic Templates	Universal Statistical	**Spectral**
Cumulative Sum	Periodic Templates	Serial	**Lempel-Ziv Complexity**
Random Excursions (Variant)	Approximate Entropy		**Linear Complexity**

Repeated Trial Assessment

- Numerical Experiments
  - Samples of 300 binary sequences (10^6 bits/sequence).
  - Apply 5 statistical tests
    - 1 = Frequency, 2 = Cusum, 3 = Runs, 4 = Spectral, 5 = ApEn.
- Analysis of Empirical Results
  - 1500 P-values per sample.
  - In theory, P-values should be uniformly distributed.
  - % of Passing Sequences:

$$0.99 - 3\sqrt{\frac{0.01*0.99}{300}} \approx 0.9727$$


Sorted Counts Plot: Blum–Blum–Shub
1
0.99
0.98
0.97
0.96
0.95
%age Of Accepted Sequences
2
5
1
3
4
Sorted Statistical Test


Sorted Counts Plot: Cubic Congruential Generator
%age Of Accepted Sequences
Sorted Statistical Test
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
3
5
1
2
4

Alternate Decision Rule

$$\pi = \binom{n}{x} p^x q^{n-x}$$

$\alpha = 0.01$

$n = 300$

$p = 0.99$

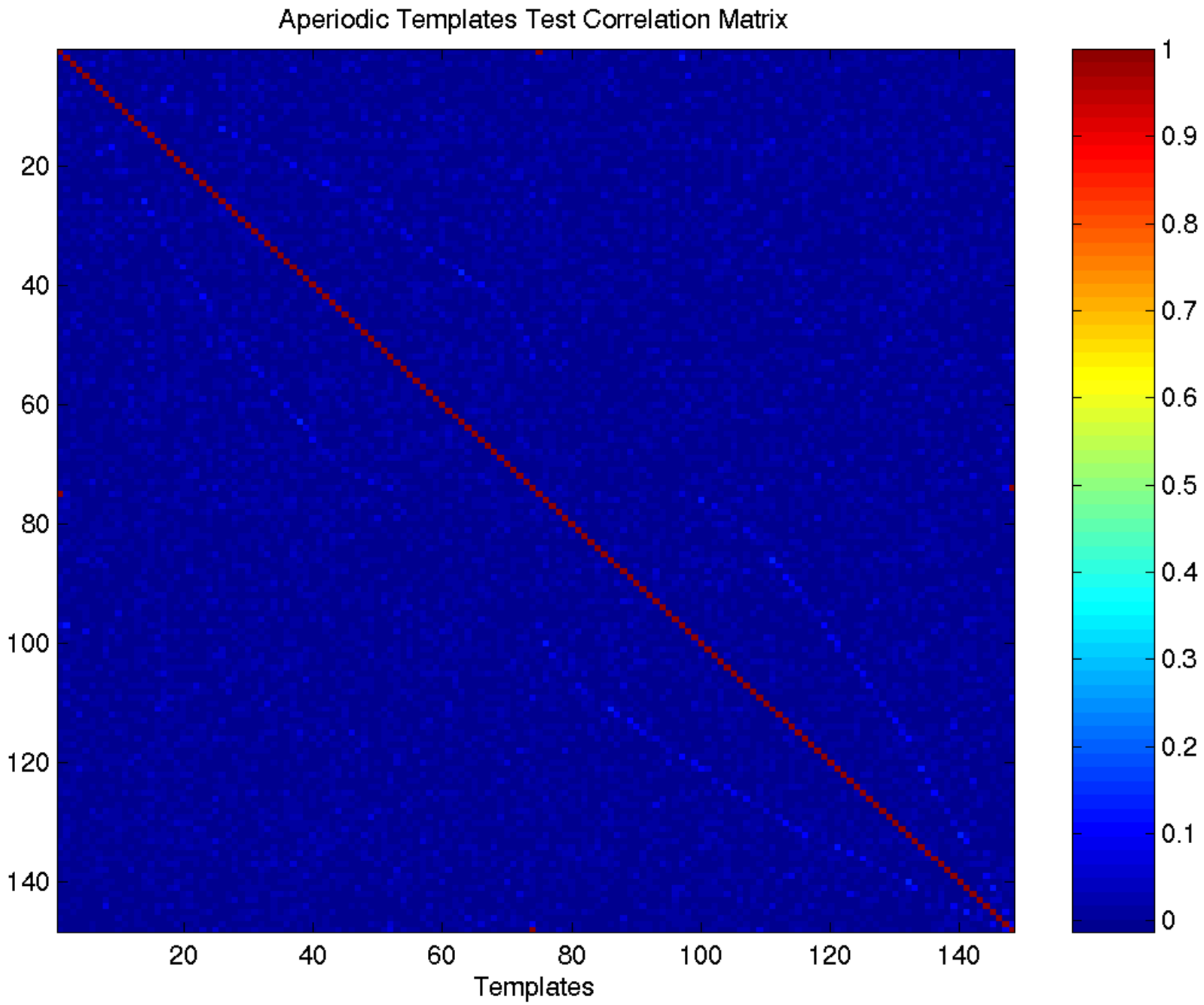
$q = 0.01$

$x \in [0,300]$

S	F	Proportion	π	Σ π
300	0	1.0000	0.049041	0.049041
299	1	0.9967	0.148609	0.197650
298	2	0.9933	0.224414	0.422064
297	**3**	**0.9900**	**0.225170**	0.647234
296	4	0.9867	0.168877	0.816111
295	5	0.9833	0.100985	0.917096
294	6	0.9800	0.050153	0.967249
293	7	0.9767	0.021277	0.988526
292	**8**	**0.9733**	**0.007871**	0.996397
291	**9**	**0.9700**	**0.002580**	0.998977
290	10	0.9667	0.000758	0.999735

Current Work Items

- Peer review process is underway
- Independence of the statistical tests
- Development of new statistical tests
  - Long Sequences - Ising Model Based Tests
  - Modification for Short Sequences


Aperiodic Templates Test Correlation Matrix
20
40
60
80
100
120
140
Templates
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0

Summary

- New metrics to investigate the randomness of cryptographic RNGs.
- Illustrated numerical experiments conducted utilizing the NIST STS.
- Addressed the analysis of empirical results.

Questions? Comments?