A new matrix test for randomness

Otokar Grošek, Slovak University of Technology, Bratislava
Joint work with Milan Vojvoda and Robert Krchňavý

It is well known that there is no way deterministically to make a decision whether an observed finite sequence is a part of an output from pseudo/true-random number generator (PRNG) or not. Even more there are still some problems to define the mathematical/cryptologycal primitive PRNG. From practical point of view there is a straightforward way to use a test suite for testing various properties of such (finite) sequences. Among many we recall [1, 2, 3, 4, 5]. Some of them also contain the Binary Matrix Rank Test (BMRT). The purpose of this test is to check for linear dependence among fixed length substrings of the original sequence. This test is based on the fact whether the number of $n \times n$ matrices generated from the sequence, and having ranks $n, n-1$, and $n-2$ respectively statistically coincide with the expected number of such matrices (approximately 29%, 58% and 13%). When $n \geq 10$ the rest of matrices represent less than 0.5%.

As an Example when this test fails, i.e. it does not recognize a sequence generated by LFSR and primitive polynomials, we present two trinomials over $GF(2)$:

(1) $x^{97} + x^6 + 1$ - here 75% of NIST test suite accepted this sequence, including BMRT;

(2) $x^{646} + x^{249} + 1$ - here 15% of NIST test suite accepted this sequence, including BMRT.

We present a new test based on a multiplicative semigroup of matrices over two algebraic structures, namely $n \times n$ boolean matrices, and $n \times n$ matrices over the field $GF(q), q = 2$ and 4. Concretely we use distribution of matrices according to so called Euler-Fermat Theorem for Finite Semigroups,[6].

Let S be a finite semigroup. Then for any element $x \in S$, in the sequence $x, x^2, \ldots$, for some $1 \leq s < t$ must hold $x^s = x^t$. Let $k(x) = k$, and $d(x) = d$ be the least exponent for which $x^k = x^{k+d}$. It is well known, and easy to prove that

$$\{x^k, \ldots, x^{k+d-1}\} \tag{1}$$

forms a cyclic group of order d, and this group is determined by the (unique) idempotent $e = x^r,\ k \leq r \leq k + d - 1$ belonging to this group.

Definition. *Let S be a finite semigroup and define numbers K, D and R as follows:*

$$\begin{aligned} K &= \max\{k(x) \,|\, x \in S\} \\ D &= \mathrm{lcm}(d(x) \,|\, x \in S), \end{aligned}$$

and R is uniquely determined integer such that $K \leq R < K + D$ and $D|R$.

Theorem (Euler-Fermat Theorem for Finite Semigroups,[6])**.** *For any $x \in S$ and K, D, R defined as above holds*

$$x^{K+D} = x^K,$$

and x^R is an idempotent. Moreover, K, D and R are the least positive integers having this property.

There is a limited number of semigroups for which the "universal exponents" K, D and R are known. In the cases under our consideration the results are known.

Another theorem distributes matrices over $GF(q)$ by rank

Theorem (Euler-Fermat Theorem for Semigroup of matrices,[7])**.** *Let*

$$\lambda(\ell, q) = p^t \mathrm{lcm}(q^\ell - 1, q^{\ell-1} - 1, \ldots, q - 1)$$

where t is the least integer for which $p^t \geq 1$. For any $n \times n$ matrix A over $GF(q)$, with $1 \leq \mathrm{rank}(A) \leq h \leq n - 1$ we have

$$A^{h+1} = A^{h+1+\lambda(h,q)},$$

and this result is the best possible.

Getting these characteristics k, d, h together we can divide the semigorup of matrices to disjoint parts and form a new χ^2- test. We have used this tests in some practical situations, and in some cases, like the above mentioned LFSR, it works better than BMRT.

Acknowledgment: This work is supported by Grant VEGA 1/3115/06.

References

[1] E. Dawson: QUT Crypt-x Software. Information Security Institute. `http://www.isi.qut.edu.au/`
[2] B. Heyber: Cryptometry - statistical tests for crypto-primitives. 6th IEEE, Japan-Benelux Workshop, Essen 1996, p. 8.1 - 8.3, ISBN 90-74249-09-4.
[3] G. Marsaglia: `http://stat.fsu.edu/~geo/diehard.html`, 1997.
[4] NIST: A Statistical test suite for random and pseudorandom number generators for cryptographic applications. Special publication 800-22, 2001. `http://csrc.nict.gov/encryption/aes/`
[5] NESSIE. M. Dichtl: Document NES/DOS/SAG/WP2/023/2. Description of General NESSIE Test Tools. , SIEMENS AG, Munich, Germany. `http://www.cryptonessie.org`
[6] Š. Schwarz: *On the Semigroup of Binary Relations on a Finite Set.* Czech. Math. J. **20**(95) 1970, 632–679.
[7] Š. Schwarz: *Fermat's theorem for matrices revisited.* Math. Slovaca **4**(95) 1985, 343–347.