Testing Randomness : Physical Generators and Statistical Procedures

Andrew Rukhin
Statistical Engineering Division, ITL, NIST

March 16, 2017
Random Numbers

Communications
Banking Industry

Monte Carlo Simulations

Medical Statistics

Randomized Clinical Trials
Tpppett (1927)
Testing Randomness
Kendall, Babbington Smith

Knuth Vol 2
classical tests
Marsaglia, Diehard
demands long sequences

TestU01, L’Ecuyer, Simard
Other commercial packages
NIST
A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,
NIST Special Publication 800-22, Department of Commerce
last revision 2012
Currently 15 tests

Provide a user with a characteristic of source randomness

Each test produces a P-value

Uniform in $(0,1)$

Have to choose an alternative hypothesis
Tests based on the properties of a random walk

Discrete Fourier transform (spectral) test

Non-overlapping and overlapping template matchings

Tests based on patterns
Tests of randomness based on the number of missing words or of words with a given frequency

Complexity based tests
Strong Loophole-Free Test of Local Realism
Physical Review Letters, 2015
L. K. Shalem + 34 co-authors

Realism: any system has preexisting values for all possible measurements

Local realism: preexisting values depend only on events in the past light cone
Bell’s inequalities allow to test local realism as a statistical hypothesis.

Bell’s test: source generates particles and sends them to two parties $A$ and $B$. $A$ and $B$ randomly and independently choose properties to measure.
Later compare their measurement results

Local realism constrains the joint probability distribution

Bell’s inequalities obeyed by local realistic probability distributions

Can be violated by entangled quantum particles

The local realism can be (and was) tested experimentally
Bell’s inequalities violated by pairs of polarization-entangled photons
Independence of $A$ and $B$ actions

Have to choose measurement settings based on fast random events that occur in the short time before a signal traveling at the speed of light from the entangled-photon creation would be able to reach $A$ and $B$
$A$ and $B$ must be free to make random measurement choices physically independent one from another and of any properties of the particles.

Tests of randomness come handy!

Bell’s test: series of trials
- $A$ chooses between $a$ and $a'$
- $B$ chooses between $b$ and $b'$
- record $\pm$ or 0
Local realism implies

\[ P(++) \leq P(+0|ab') + P(0+|a'b) + P(++) |a'b') \]

\( P(++) |ab) \): probability \( A \) and \( B \) choose settings \( ab \), both record +
entangled quantum particles can (do) violate this inequality

Null hypothesis: probability distribution constrained by local realism
Test statistic: take all measured data $T_k, k = 1, \ldots, N$ (both settings and measurement results)

$N_S$ number of successes (trials such that $T_k = + + ab$)

$$P(\text{at least } N_S \text{ successes}) \leq P(\text{Bin}(N, 1/2) \geq N_S)$$

(tight) upper bound on P-values

P-value the maximum value under local realism that $N_S$ is at least as large as the observed value

Gill (2003) no assumptions about the distribution of events

Does not require iid data
### Experimental results

| $N(++)|ab$ | Total trials       | $P$ – value   |
|----------|-------------------|---------------|
| 1257     | 175,654,992       | $2.510^{-3}$  |
| 3800     | 175,744,824       | $2.410^{-6}$  |
| 6378     | 177,358,351       | $5.910^{-9}$  |
| 8820     | 177,797,650       | $2.010^{-7}$  |

rows: number of aggregate laser pulses (1, 3, 5 or 7)
The reported experiment
commissioning run of the Bell test machine to certify randomness
The goal to incorporate as an additional source of real-time randomness
NIST public random number beacon

https://beacon.nist.gov 512 bits every minute

Quantum Random Number Generator
unpredictable sampling
secure authentication mechanisms
secure multiparty computation
Photon Sampling RNG
Single-photon detection of optical states

By sampling the output of a detector one can set the detection probability at 0.5.
Depends on the amplitude of the attenuated optical state.
Allows to generate a random bit on demand.
Passes NIST Statistical Test Suite for Randomness at $\alpha = 0.01$. 
Quality control issue
The probability of detection can shift over time
Kalman filtering (autocorrelation present)
Intervene when

$$|\bar{p} - \frac{1}{2}| \geq 6.28\sqrt{\frac{\bar{p}(1 - \bar{p})}{n}}$$