The Spectral Test & Theoretical Tests

Theoretical tests are the application of a statistical property to a simple occurrence where, under certain circumstances, the EXACT VALUE can be computed.

Example: We expect that if $X_i \sim U(0,1)$ i.i.d. then $X_{n+1} < X_n$ with $p = 0.5$.

Let $X_{n+1} = aX_n + c \pmod{m}$, then the fraction of $X_{n+1} < X_n$ (averaged over the full period) is $\frac{1}{2} + \frac{1}{m} \frac{d}{gcd(a-1,m)}$, so $1 + \frac{1}{2m}$

Clearly, if $d = 1$, $r$ is minimized.

The calculation: $s(x) = (ax + c) \mod m$

thus we are reduced to count $\# x \geq s(x) \leq x$ over the full period.

Note: $\left\lfloor \frac{x - s(x)}{m} \right\rfloor = \begin{cases} 1 & s(x) \leq x \\ 0 & \text{otherwise (never =)} \end{cases}$

We must compute

$$\sum_{0 \leq x < m} \left\lfloor \frac{x - s(x)}{m} \right\rfloor = \_ \_$$
\[ \left( \frac{\Gamma \left( \frac{a}{2} \right)}{\Gamma \left( \frac{a}{2} \right)} \right) p + \frac{2}{1 - \eta} + \frac{2}{1 - \eta(1 - \eta)} = \left\lfloor \frac{m}{c} + \frac{2}{1 - \eta(1 - \eta)} \right\rfloor \]

Let \( c = c + \frac{2}{1 - \eta(1 - \eta)} \), then \( 1 = \frac{m}{c} \).

Now, assume \( \gcd(a, m) = 1 \).

Recall (from cot 5.507 or general knowledge)

\[ \left( \frac{m}{c + \frac{2}{1 - \eta(1 - \eta)}} \right) \]

\[ = \left\lfloor \frac{m}{c + \frac{2}{1 - \eta(1 - \eta)}} \right\rfloor \]

\[ = \left\lfloor \frac{m}{c} \right\rfloor \]

If \( y \) is \( \frac{m}{c} \) and \( a \equiv m \pmod{c} \).

\[ \left\lfloor \frac{m}{c} \right\rfloor = y \]

Then \( a \equiv m \pmod{c} \).

\[ \left\lfloor \frac{m}{c} \right\rfloor = y \]

\[ \frac{m}{c} = a \equiv m \pmod{c} \]

\[ \left\lfloor \frac{m}{c} \right\rfloor \]
\[ c = \lfloor \frac{d}{x} \rfloor + c \pmod{d} \]

\[ \lfloor \frac{d}{x} \rfloor = c - c \pmod{d} \quad \text{and so} \]

\[ \sum_{0 \leq x < m} \left\lfloor \frac{bx+c}{m} \right\rfloor = \frac{(b-1)(m-1)}{2} + \frac{d-1}{2} + c + c \pmod{d} \]

\[ x = \frac{b(m-1)+c}{2} - \frac{(b-1)(m-1)}{2} - \frac{d-1}{2} - c + c \pmod{d} \]

\[ = \frac{m-1}{2} - \frac{d-1}{2} + c \pmod{d} \quad \text{divid by } m \]

\[ = \frac{1}{2} - \frac{1}{2} \cdot \frac{d}{2} + \frac{1}{2} \cdot \frac{1}{2} + c \pmod{d} \]

\[ = \frac{1}{2} + \frac{(2(c \pmod{d}) - d)}{2m} \\

This shows how simple \textit{RN6s} and simple, often full-period properties, can lead to exact tests.

\underline{The Spectral Test}: Theoretical test that still requires computer experimentation, like an empirical test. To date, all good generators pass this test, while all known, bad generators fail it?

\[ \{ u_0, u_{n+1}, \ldots, u_{n+t-1} \} \quad 1 \leq n \leq m^3 \] created by an LCG
\( (x_0, a, c, m) \), \( s(x) = (ax + c) \mod m \)

Fig. 8. (a) The two-dimensional grid formed by all pairs of successive points \((X_n, X_{n+1})\), when \(X_{n+1} = (137X_n + 187) \mod 256\). (b) The three-dimensional grid of triplets \((X_n, X_{n+1}, X_{n+2})\).

\[ s^1(x), s^2(x), \ldots, s^{t-1}(x) \] \( x \in \{ 0, 1, 2, \ldots, m \} \). Above is easily covered by a small family of planes.

\( V_2 \): 2D accuracy

\( V_2^{-1} \): maximum distance between that cover \[ \{ \frac{x}{m}, \frac{s(x)}{m}, \frac{s^2(x)}{m}, \ldots, \frac{s^{t-1}(x)}{m} \} \]

\( V_3^{-1} \): maximum distance between planes that cover \[ \{ \frac{x}{m}, \frac{s(x)}{m}, \frac{s^2(x)}{m}, \ldots, \frac{s^{t-1}(x)}{m} \} \]

Note: A truly random sequence truncated to a given accuracy has the same accuracy in all dimension. But a periodic sequence \( \omega/p + k \equiv m \) will have less accuracy as dimension increases no more than \( m \sqrt{t} \) in \( t \)-dims.
The spectral test tries to find $\nu_t, 0 \leq t \leq 5$, perhaps up to $t = 10$. For $t > 10$ seems rather unimportant.

**Theory of the Spectral Test:**

$$m^{-1}S_t(x) = \left( \frac{\sin((1+\alpha + \ldots + \alpha^t)c)}{m} \right) \mod 1$$

If we periodically extend our definition of these pts. We remove the "mod 1" to get these points:

$$L = \{ (x, h_0, h_1, \ldots, h_t) \mid x, h_i \in \mathbb{Z} \}$$

$$= \{ V_0 + (x, h_0, \alpha h_0, \ldots, \alpha^t h_0) \mid x, h_i \in \mathbb{Z} \}$$

$V_0 = \frac{1}{m} (0, c, (1+\alpha)c, (1+\alpha^2)c, \ldots, (1+\alpha^t)c)$, a constant vector.

**Note:** The "free" integers $(x, h_0, h_1, \ldots, h_t)$ can be changed to $(x+h_0m, 0, h_0, \ldots, h_t)$ without loss of generality; this is similar to the transformation done in the "Mainly in the Plains" paper of Marsaglia:

$$L = \{ V_0 + y_1 V_1 + y_2 V_2 + \ldots + y_t V_t \mid y_i \in \mathbb{Z} \}$$

$$V_i = \frac{1}{m} (1, \alpha, \alpha^2, \ldots, \alpha^{i-1})$$ basis for a

$$V_i = c_i, i = 2, \ldots, t$$ $t$-dim lattice
Note: $V_0$ is not multiplied by an arbitrary integer and is constant. In terms of hyperplane spacing it makes no difference $a$ can be dropped.

**Remark:** Since $V_0 = \frac{a}{2} (0, \frac{1}{2}, 1 + a, 1 + 2a, \ldots, 1 + \cdots + a)$ it is the only place where $\frac{1}{2}$ appears. Thus w.r.t. the spectral form $x_i = a x_{i-1} + c$ we will have identical results. Thus we need only consider this lattice.

$L_0 = \{ y, V_1, \ldots, V_k | y \in \mathbb{Z} \}$

Recall: $U = (u_1, \ldots, u_k)$ defines a family of hyperplanes $\perp$ to $U$ as:

$$\{ (x_1, \ldots, x_k) | x_1 u_1 + \ldots + x_k u_k = g \in \mathbb{R} \}$$

In our case we can consider only $g \in \mathbb{Z}$, thus the distance between hyperplanes is the minimum distance from $(0,0,\ldots,0)$ to the hyperplane w/g = 1:

$$\min \{ \sqrt{x_1^2 + \ldots + x_k^2} | x_1 u_1 + \ldots + x_k u_k = 1 \}$$

(Cauchy: $(\Sigma x_i u_i)^2 \leq (\Sigma x_i^2) (\Sigma u_i^2)$)

So the min occurs when $x_i = u_i$. $(\Sigma u_i^2)^{-\frac{1}{2}}$ or the distance between neighboring hyperplanes is $(\Sigma u_i^2)^{-T_2} = \text{length}(U)^{-1} = V_c^{-1}$

$$V_c = \min \{ \text{length}(U) | x \cdot U = g \} \text{ has all of } L_0$$

- 6 -
Properties of $U$
- $U = (u_1, \ldots, u_t) \neq (0, \ldots, 0)$
- $V, U \in \mathbb{Z}^t, V \in \mathbb{L}_0$
  
  This means $V \in \mathbb{L}_0$.
- Since $c_1, \ldots, c_t \in \mathbb{L}_0$, $u_i \in \mathbb{Z}$ for $i = 1, \ldots, t$
  
  $u_i, c_1, \ldots, c_t \in \mathbb{L}_0 \Rightarrow \frac{1}{m} (u_1 + c_1 u_1 + \cdots + c_t u_t) \in \mathbb{Z}$
  
  $u_1, u + c_2 + \cdots + c_t u_t \equiv 0 \pmod{m}$
- Any $U \in \mathbb{Z}^t$ satisfying $\mathcal{S}$ defines a family of hyperplanes as desired

$$\tau_c = \min \|U \cdot U| u_i + c_2 + \cdots + c_t u_t \equiv 0 \pmod{m}\|$$

A Computational Method: Have reduced to minimizing $\ominus$, cannot exhaust. Consider

$$f(x_1, \ldots, x_t) = \sum_{j=1}^{t} \left( \sum_{i=1}^{n} u_{ij} x_i \right), \text{ minimize for } x \in \mathbb{Z}^t \neq 0$$

$U = (u_{ij})$ is a nonsingular matrix

$$f(x_1, \ldots, x_t) = (x, U_1 + \cdots + x_t U_t) \cdot (x, U_1 + \cdots + x_t U_t)$$

$$= (x, U_1 + \cdots + x_t U_t)^T$$
Since $V$ is nonsingular we can find $V_1, \ldots, V_6 \in \mathbb{R}^6$ such that $U_i \cdot V_j = \delta_{ij}$ for $1 \leq i, j \leq 6$.

The $[V_1, \ldots, V_6]$ is the inverse matrix.

For the spectral test, the quadratic form looks like:

- $U_1 = (m, 0, \ldots, 0)$
- $U_2 = (-a, b, 0, \ldots, 0)$
- $U_3 = (-a, 0, 1, \ldots, 0)$
- $U_4 = (a, 0, 0, \ldots, 1)$
- $U_5 = (-a, 0, 0, \ldots, 1)$

$V_1 = e_1$

$V_i = e_2$, $i = 2, \ldots, 6$

$V_i$'s are the basis for $L_0$, thus the $U_i$'s are a basis for $L_0^*$, the dual lattice.

Thus we now see the relationship between the spectral test and lattice reduction.

$\chi^2$ can be found by finding the shortest nonzero vector in the appropriate $t$-dimensional lattice.

**Ratings for Various Generators:**

We look at results from Knuth.
### SAMPLE RESULTS OF THE SPECTRAL TEST

<table>
<thead>
<tr>
<th>Line</th>
<th>$a \times 10^8$</th>
<th>$m$</th>
<th>$\nu_2^2$</th>
<th>$\nu_3^2$</th>
<th>$\nu_4^2$</th>
<th>$\nu_5^2$</th>
<th>$\nu_6^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>23</td>
<td>$2^{35}$</td>
<td>530</td>
<td>530</td>
<td>530</td>
<td>530</td>
<td>447</td>
</tr>
<tr>
<td>2</td>
<td>$27 + 1$</td>
<td>$2^{35}$</td>
<td>16642</td>
<td>16642</td>
<td>16642</td>
<td>15602</td>
<td>252</td>
</tr>
<tr>
<td>3</td>
<td>$2^{25} + 1$</td>
<td>$2^{36}$</td>
<td>34359738368</td>
<td>6</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>3141592653</td>
<td>$2^{35}$</td>
<td>29972202106</td>
<td>1026050</td>
<td>27822</td>
<td>1118</td>
<td>1118</td>
</tr>
<tr>
<td>5</td>
<td>137</td>
<td>$2^{56}$</td>
<td>274</td>
<td>30</td>
<td>14</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>3141592621</td>
<td>$10^{10}$</td>
<td>4577114792</td>
<td>1034718</td>
<td>62454</td>
<td>1776</td>
<td>542</td>
</tr>
<tr>
<td>7</td>
<td>3141592221</td>
<td>$2^{10}$</td>
<td>4293881050</td>
<td>278266</td>
<td>97450</td>
<td>3366</td>
<td>2382</td>
</tr>
<tr>
<td>8</td>
<td>4197559881</td>
<td>$10^{10}$</td>
<td>10721093248</td>
<td>23965578</td>
<td>49362</td>
<td>5868</td>
<td>820</td>
</tr>
<tr>
<td>9</td>
<td>4106984121</td>
<td>$10^{10}$</td>
<td>9183832062</td>
<td>4615650</td>
<td>16686</td>
<td>6840</td>
<td>1344</td>
</tr>
<tr>
<td>10</td>
<td>$2^{24} + 2^{13} + 5$</td>
<td>$2^{35}$</td>
<td>8364058</td>
<td>8364058</td>
<td>21476</td>
<td>16712</td>
<td>1496</td>
</tr>
<tr>
<td>11</td>
<td>$5^{13}$</td>
<td>$2^{35}$</td>
<td>33161885770</td>
<td>2925242</td>
<td>113374</td>
<td>13070</td>
<td>2256</td>
</tr>
<tr>
<td>12</td>
<td>$2^{26} + 3$</td>
<td>$2^{29}$</td>
<td>536936458</td>
<td>118</td>
<td>116</td>
<td>116</td>
<td>116</td>
</tr>
<tr>
<td>13</td>
<td>1812433253</td>
<td>$2^{32}$</td>
<td>4326934538</td>
<td>1462856</td>
<td>15082</td>
<td>4868</td>
<td>906</td>
</tr>
<tr>
<td>14</td>
<td>1566053941</td>
<td>$2^{32}$</td>
<td>4657948970</td>
<td>2079590</td>
<td>44902</td>
<td>4652</td>
<td>662</td>
</tr>
<tr>
<td>15</td>
<td>69069</td>
<td>$2^{32}$</td>
<td>4243200856</td>
<td>2072544</td>
<td>52804</td>
<td>6990</td>
<td>242</td>
</tr>
<tr>
<td>16</td>
<td>1664525</td>
<td>$2^{32}$</td>
<td>4938916774</td>
<td>2322494</td>
<td>63712</td>
<td>4092</td>
<td>1038</td>
</tr>
<tr>
<td>17</td>
<td>3141592698</td>
<td>$2^{31} - 1$</td>
<td>1432232969</td>
<td>892990</td>
<td>36985</td>
<td>3427</td>
<td>1144</td>
</tr>
<tr>
<td>18</td>
<td>620809111</td>
<td>$2^{31} - 1$</td>
<td>1977288717</td>
<td>1623137</td>
<td>48191</td>
<td>6101</td>
<td>1462</td>
</tr>
<tr>
<td>19</td>
<td>16807</td>
<td>$2^{31}$</td>
<td>282475250</td>
<td>408197</td>
<td>21682</td>
<td>4343</td>
<td>895</td>
</tr>
<tr>
<td>20</td>
<td>48271</td>
<td>$2^{31} - 1$</td>
<td>1990735345</td>
<td>1433881</td>
<td>47418</td>
<td>4404</td>
<td>1402</td>
</tr>
<tr>
<td>21</td>
<td>40092</td>
<td>$2^{31} - 249$</td>
<td>1658583865</td>
<td>1409422</td>
<td>42475</td>
<td>6507</td>
<td>1438</td>
</tr>
<tr>
<td>22</td>
<td>444857087377099</td>
<td>$2^{46}$</td>
<td>$5.6 \times 10^{43}$</td>
<td>$1160915002$</td>
<td>$1882426$</td>
<td>$279928$</td>
<td>$26230$</td>
</tr>
<tr>
<td>23</td>
<td>311672356</td>
<td>$2^{48}$</td>
<td>$3.2 \times 10^{44}$</td>
<td>$111814446$</td>
<td>$17341510$</td>
<td>$306926$</td>
<td>$59278$</td>
</tr>
<tr>
<td>24</td>
<td>see (38)</td>
<td>$2^{49}$</td>
<td>$2.4 \times 10^{48}$</td>
<td>$4.7 \times 10^{11}$</td>
<td>$1.9 \times 10^9$</td>
<td>$3194548$</td>
<td>$161610$</td>
</tr>
<tr>
<td>25</td>
<td>see (39)</td>
<td>$2^{49}$</td>
<td>$(2^{31} - 1)^2$</td>
<td>$1.4 \times 10^{12}$</td>
<td>$643578623$</td>
<td>$12930027$</td>
<td>$837632$</td>
</tr>
<tr>
<td>26</td>
<td>see the text</td>
<td>$2^{64}$</td>
<td>$8.8 \times 10^{48}$</td>
<td>$6.4 \times 10^{42}$</td>
<td>$4.1 \times 10^9$</td>
<td>$45662836$</td>
<td>$1846368$</td>
</tr>
<tr>
<td>27</td>
<td>see the text</td>
<td>$2^{64}$</td>
<td>$2^{24} + 1$</td>
<td>$281084902$</td>
<td>$2.2 \times 10^{10}$</td>
<td>$1.8 \times 10^9$</td>
<td>$1862407$</td>
</tr>
<tr>
<td>28</td>
<td>$2^{24} - 389$</td>
<td>$2^{576}$</td>
<td>$1.8 \times 10^{173}$</td>
<td>$3.5 \times 10^{115}$</td>
<td>$4.4 \times 10^{83}$</td>
<td>$2 \times 10^{90}$</td>
<td>$5 \times 10^{87}$</td>
</tr>
<tr>
<td>29</td>
<td>$(2^{32} - 5) - 400$</td>
<td>$2^{1376}$</td>
<td>$1.6 \times 10^{414}$</td>
<td>$8.6 \times 10^{275}$</td>
<td>$1 \times 10^{207}$</td>
<td>$2 \times 10^{165}$</td>
<td>$8 \times 10^{337}$</td>
</tr>
</tbody>
</table>
Understanding The Table

Lines 1-2: multiplier too small
Line 3: good v2 but bad afterwards
Line 4: "random" multiplier
Line 5: the gen. of the pictures
Line 6-7: notice a mm +1 effect
Lines 8, 10: mults chosen \( V_8, V_{10}, V_{15} \)
Line 11: Very good, but 2^{15} faded
Line 12: RANDU replaced 11!
Lines 13-14: Borosh-Niederreiter
Lines 15-23: Search-based choices
Line 22: Cray X-MP library (240)
Line 26: "Modern modulus" choice
Line 15: Nominated by G.M. to be "best"
Line 17: Random primitive root
Line 18: Search
Line 19: \( m > 2^{31} - 1 \), \( a = 75 \): Lewis, Goldigna, Miller
Line 20: Search for \( a^2 < 2^{31} - 1 \)
Line 21: Smaller modulus, similar results
Line 24: Combined 20+21 (subtracted)
Line 25: 2^nd order \( m = 2^{31} - 1 \)
Lines 27-29: AWC/SWB, 2P: RANCUX

-10-