The Spectral Test & Theoretical Tests

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

Example: We expect that if X_i is $U[0,1)$ 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 $\frac{1}{2} + v$, $v = (2(c \bmod d) - d)/2m$

$d = \gcd(a-1, m)$, so $|v| < \frac{d}{2m}$

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

The calculation: $S(X) = (aX + c) \bmod m$

thus we are reduced to count $\#\, x \ni S(x) < x$ over the full period.

Note: $\left\lceil \frac{X - S(X)}{m} \right\rceil = \begin{cases} 1 & S(X) < X \\ 0 & \text{otherwise} \quad (\text{never} =) \end{cases}$

We must compute

$$\sum_{0 \le x < m} \left\lceil \frac{X - S(X)}{m} \right\rceil = \textcircled{*}$$

$$(*) = \sum_{0 \le x < m} \left\lceil \frac{x}{m} - \frac{(ax+c) \bmod m}{m} \right\rceil$$

$$(ax+c) \bmod m = ax + c - \left\lfloor \frac{ax+c}{m} \right\rfloor \cdot m$$

$$= \sum_{0 \le x < m} \left\lceil \frac{x}{m} - \frac{ax+c}{m} + \left\lfloor \frac{ax+c}{m} \right\rfloor \right\rceil = \sum_{0 \le x < m} \left\lceil -\frac{(a-1)x+c}{m} \right\rceil$$

$$+ \sum_{0 \le x < m} \left\lfloor \frac{ax+c}{m} \right\rfloor$$

call $b = a-1$

$\lceil -y \rceil = -\lfloor y \rfloor$

$$= \sum_{0 \le x < m} \left(\left\lfloor \frac{ax+c}{m} \right\rfloor - \left\lfloor \frac{bx+c}{m} \right\rfloor \right)$$

Recall (from COT 5507 or general knowledge)

$$\sum_{0 \le j < k} \left\lfloor \frac{hj+c}{k} \right\rfloor = \frac{(h-1)(k-1)}{2} + \frac{g-1}{2} + g \lfloor c/g \rfloor$$

$g = \gcd(h,k)$

now we assume $\gcd(a,m) = 1$ for maximal period reasons, so $g = 1$

$$\sum_{0 \le x < m} \left\lfloor \frac{ax+c}{m} \right\rfloor = \frac{(a-1)(m-1)}{2} + c = \frac{b(m-1)}{2} + c$$

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

$$c = \left\lfloor \frac{c}{d} \right\rfloor d + c \pmod d$$

$$\left\lfloor \frac{c}{d} \right\rfloor d = c - c \pmod d \quad \text{and so}$$

$$\sum_{0 \le x < m} \left\lfloor \frac{bx+c}{m} \right\rfloor = \frac{(b-1)(m-1)}{2} + \frac{d-1}{2} + c + (c \bmod d)$$

$$* = \frac{b(m-1)}{2} + c - \frac{(b-1)(m-1)}{2} - \frac{d-1}{2} - c + (c \bmod d)$$

$$= \frac{m-1}{2} - \frac{d-1}{2} + (c \bmod d) \quad \text{divid by } m$$

$$= \frac{1}{2} - \frac{1}{2m} - \frac{d}{2m} + \frac{1}{2m} + \frac{(c \bmod d)}{m}$$

$$= \frac{1}{2} + \frac{(2(c \bmod d) - d)}{2m} \quad \text{— } r$$

This shows how simple RNGs and simple, often full-period properties, can lead to exact tests.

The Spectral Test: Theoretical test that still requires computer interpretation, like an empirical test. To date, all good generators pass this test, while all known bad generators fail it!

$\{(U_n, U_{n+1}, \ldots, U_{n+t-1}) \mid 0 \le n < m\}$ created by an LCG

(X_0, a, c, m), $s(x) = (ax+c) \bmod m$

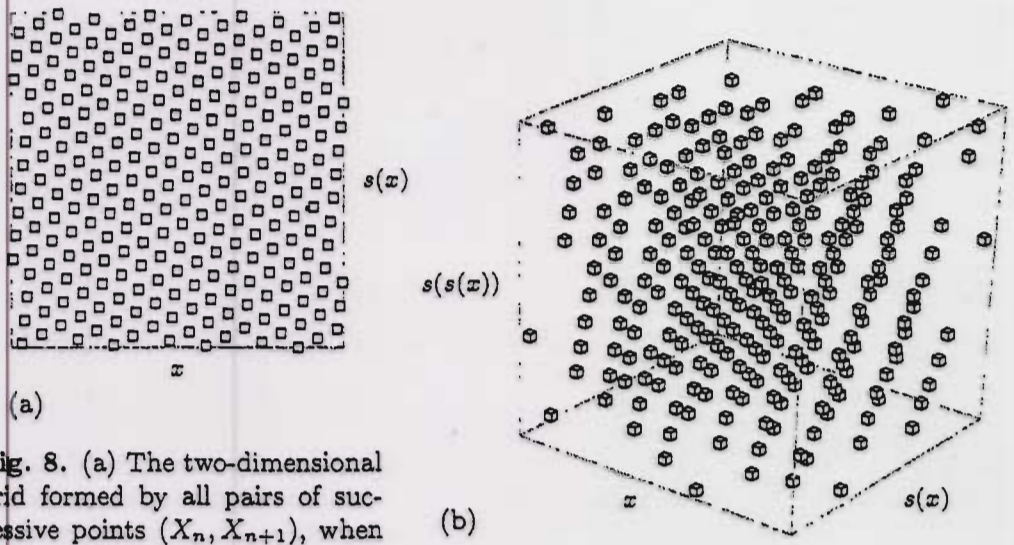

Fig. 8. (a) The two-dimensional grid formed by all pairs of successive points (X_n, X_{n+1}), when $X_{n+1} = (137X_n + 187) \bmod 256$. (b) The three-dimensional grid of triplets (X_n, X_{n+1}, X_{n+2}).

$\{\frac{1}{m}(x, s(x), s^2(x), \ldots, s^{t-1}(x)) \mid 0 \le x < m\}$. Above is easily covered by a small family of planes.

ν_2: 2D accuracy

ν_2^{-1}: maximum distance between lines that cover $\{(\frac{x}{m}, \frac{s(x)}{m})\}$

ν_3^{-1}: maximum distance between planes that cover $\{(\frac{x}{m}, \frac{s(x)}{m}, \frac{s(s(x))}{m}\}$

Note: A truly random sequence truncated to a given accuracy has the same accuracy in all dimension. But a periodic sequence w/per = m will have less accuracy as dimension increases no more than $m^{1/t}$ in t-dims. -4-

The spectral test tries to find r_t, $2 \le t \le 6$, perhaps up to $t = 10$. For $t > 10$ seems rather unimportant.

Theory of the Spectral Test:

$$m^{-1} s^i(x) = \left(\frac{a^i x + (1 + a + \cdots + a^{i-1})c}{m} \right) \bmod 1$$

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

$$L = \left\{ \left(\frac{x}{m} + h_1, \frac{s(x)}{m} + h_2, \ldots, \frac{s^{t-1}(x)}{m} + h_t \right) \mid x, h_i \in \mathbb{Z} \right\}$$

$$= \left\{ V_0 + \left(\frac{x}{m} + h_1, \frac{ax}{m} + h_2, \ldots, \frac{a^{t-1}x}{m} + h_t \right) \mid x, h_i \in \mathbb{Z} \right\}$$

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

Note: The "free" integers $(x, h_1, h_2, \ldots, h_t)$ can be changed to $(x + h_1 m, 0, h_2 - a h_1, \ldots, h_t - a^{t-1} h_1)$ without loss of generality, this is similar to the transformation done in the "Mainly in the Planes" paper of Marsaglia:

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

$$\left.\begin{aligned} V_1 &= \tfrac{1}{m}(1, a, a^2, \ldots, a^{t-1}) \\ V_i &= e_i, \quad i = 2, \ldots, t \end{aligned}\right\} \text{ basis for a } t\text{-dim lattice}$$

Note: V_0 is not multiplied by an arbitrary integer and is constant. In terms of hyperplane spacing it makes no difference & can be dropped.

Remark: Since $V_0 = \frac{c}{m}(0, 1, 1+a, 1+a+a^2, \ldots, 1+a+\cdots+a^{t-2})$ it is the only place where "c" appears. Thus w.r.t. the spectral test $x_n = ax_{n-1} + c$ & $x_n = ax_{n-1}$ will have identical results. Thus we need only consider this lattice

$$L_0 = \{y_1 V_1 + \cdots + y_t V_t \mid y's \in \mathbb{Z}\}$$

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

$$\{(x_1, \ldots, x_t) \mid x_1 u_1 + \cdots + x_t u_t = g \in R\}$$

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/ $g = 1$:

$$\min_{x_1, \ldots, x_t} \{\sqrt{x_1^2 + \cdots + x_t^2} \mid x_1 u_1 + \cdots x_t u_t = 1\}$$

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

So the min occurs when $x_i = u_i \cdot (\sum u_i^2)$ & the distance between neighboring hyperplanes is

$$(\sum u_i^2)^{-1/2} = \text{length}(U)^{-1} = v_t^{-1}$$

$$v_t = \min\{\text{length}(U) \mid X \cdot U = g \text{ has all of } L_0\}$$

Properties of U

- $U = (u_1, \cdots, u_t) \neq (0, \cdots, 0)$
- $V \cdot U \in \mathbb{Z} \Leftrightarrow V \in L_0$

  this means $V \in L_0^*$
- Since $e_1, \cdots, e_t \in L_0$, $u_i \in \mathbb{Z}$ $i = 1, \cdots, t$
- $U \cdot V_1 \in \mathbb{Z} \Leftrightarrow \frac{1}{m}(u_1 + au_2 + \cdots + a^{t-1}u_t) \in \mathbb{Z}$

  $u_1 + au_2 + \cdots + a^{t-1}u_t \equiv 0 \pmod{m}$
- Any $U \in \mathbb{Z}^t \neq 0$ satisfying ⑤ defines a family of hyperplanes as desired

$$\gamma_t^2 = \min_{U \in \mathbb{Z}^t \neq 0} \{ U \cdot U \mid u_1 + au_2 + \cdots + a^{t-1}u_t \equiv 0 \pmod{m} \}$$

⊛

$$= \min_{x \in \mathbb{Z}^t \neq 0} \left((m_1 x_1 - a x_2 - \cdots - a^{t-1} x_t)^2 + x_2^2 + x_3^2 + \cdots + x_t^2 \right)$$

A Computational Method: Have reduced to minimizing ⊛, cannot exhaust. Consider

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

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

$= [U_1, \cdots, U_t]$

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

$$= |x_1 U_1 + \cdots + x_t U_t|^2$$

Since V is nonsingular we can find $V_1, \ldots, V_t \Rightarrow$

$$U_i \cdot V_j = \delta_{ij} \quad 1 \le i, j \le t$$

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

For ⊛ + the spectral test, the quadratic form looks like

$$U_1 = (m, 0 \cdots, 0) \qquad V_1 = \frac{1}{m}(1, a, a^2, \ldots, a^{t-1})$$
$$U_2 = (-a, 1, 0 \cdots, 0)$$
$$U_3 = (-a^2, 0, 1, \ldots, 0) \qquad V_i = e_i \quad i = 2, \ldots, t$$
$$\vdots$$
$$U_t = (-a^{t-1}, 0, 0, \ldots, 1)$$

The 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.

ν_t^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

Line	a	m	ν_2^2	ν_3^2	ν_4^2	ν_5^2	ν_6^2
1	23	10^8+1	530	530	530	530	447
2	2^7+1	2^{35}	16642	16642	16642	15602	252
3	$2^{18}+1$	2^{36}	34359738368	6	4	4	4
4	3141592653	2^{35}	2997222016	1026050	27822	1118	1118
5	137	256	274	30	14	6	4
6	3141592621	10^{10}	4577114792	1034718	62454	1776	542
7	3141592221	10^{10}	4293881050	276266	97450	3366	2382
8	4219755981	10^{10}	10721093248	2595578	49362	5868	820
9	4160984121	10^{10}	9183801602	4615650	16686	6840	1344
10	$2^{24}+2^{13}+5$	2^{35}	8364058	8364058	21476	16712	1496
11	5^{13}	2^{35}	33161885770	2925242	113374	13070	2256
12	$2^{16}+3$	2^{29}	536936458	118	116	116	116
13	1812433253	2^{32}	4326934538	1462856	15082	4866	906
14	1566083941	2^{32}	4659748970	2079590	44902	4652	662
15	69069	2^{32}	4243209856	2072544	52804	6990	242
16	1664525	2^{32}	4938916874	2322494	63712	4092	1038
17	314159269	$2^{31}-1$	1432232969	899290	36985	3427	1144
18	62089911	$2^{31}-1$	1977289717	1662317	48191	6101	1462
19	16807	$2^{31}-1$	282475250	408197	21682	4439	895
20	48271	$2^{31}-1$	1990735345	1433881	47418	4404	1402
21	40692	$2^{31}-249$	1655838865	1403422	42475	6507	1438
22	44485709377909	2^{46}	5.6×10^{13}	1180915002	1882426	279928	26230
23	31167285	2^{48}	3.2×10^{14}	4111841446	17341510	306326	59278
24	see (38)		2.4×10^{18}	4.7×10^{11}	1.9×10^{9}	3194548	1611610
25	see (39)		$(2^{31}-1)^2$	1.4×10^{12}	643578623	12930027	837632
26	see the text	2^{64}	8.8×10^{18}	6.4×10^{12}	4.1×10^{9}	45662836	1846368
27	see the text	$\approx 2^{78}$	$2^{62}+1$	4281084902	2.2×10^{9}	1.8×10^{9}	1862407
28	$2^{-24.389}$	$\approx 2^{576}$	1.8×10^{173}	3.5×10^{115}	4.4×10^{86}	2×10^{69}	5×10^{57}
29	$(2^{32}-5)^{-400}$	$\approx 2^{1376}$	1.6×10^{414}	8.6×10^{275}	1×10^{207}	2×10^{165}	8×10^{137}

$\lg\nu_2$	$\lg\nu_3$	$\lg\nu_4$	$\lg\nu_5$	$\lg\nu_6$	μ_2	μ_3	μ_4	μ_5	μ_6	Line
4.5	4.5	4.5	4.5	4.4	$2\epsilon^5$	$5\epsilon^4$	0.01	0.34	4.62	1
7.0	7.0	7.0	7.0	4.0	$2\epsilon^6$	$3\epsilon^4$	0.04	4.66	$2\epsilon^3$	2
17.5	1.3	1.0	1.0	1.0	3.14	$2\epsilon^9$	$2\epsilon^9$	$5\epsilon^9$	ϵ^8	3
15.7	10.0	7.4	5.1	5.1	0.27	0.13	0.11	0.01	0.21	4
4.0	2.5	1.9	1.3	1.0	3.36	2.69	3.78	1.81	1.29	5
16.0	10.0	8.0	5.4	4.5	1.44	0.44	1.92	0.07	0.08	6
16.0	9.0	8.3	5.9	5.6	1.35	0.06	4.69	0.35	6.98	7
16.7	10.7	7.8	6.3	4.8	3.37	1.75	1.20	1.39	0.28	8
16.5	11.1	7.0	6.4	5.2	2.89	4.15	0.14	2.04	1.25	9
11.5	11.5	7.2	7.0	5.3	$8\epsilon^4$	2.95	0.07	5.53	0.50	10
17.5	10.7	8.4	6.8	5.6	3.03	0.61	1.85	2.99	1.73	11
14.5	3.4	3.4	3.4	3.4	3.14	ϵ^5	ϵ^4	ϵ^3	0.02	12
16.0	10.2	6.9	6.1	4.9	3.16	1.73	0.26	2.02	0.89	13
16.1	10.5	7.7	6.1	4.7	3.41	2.92	2.32	1.81	0.35	14
16.0	10.5	7.8	6.4	4.0	3.10	2.91	3.20	5.01	0.02	15
16.1	10.6	8.0	6.0	5.0	3.61	3.45	4.66	1.31	1.35	16
15.2	9.9	7.6	5.9	5.1	2.10	1.66	3.14	1.69	3.60	17
15.4	10.3	7.8	6.3	5.3	2.89	4.18	5.34	7.13	7.52	18
14.0	9.3	7.2	6.1	4.9	0.41	0.51	1.08	3.22	1.73	19
15.4	10.2	7.8	6.1	5.2	2.91	3.35	5.17	3.15	6.63	20
15.3	10.2	7.7	6.3	5.2	2.42	3.24	4.15	8.37	7.16	21
22.8	15.1	10.4	9.0	7.3	2.48	2.42	0.25	3.10	1.33	22
24.1	16.0	12.0	9.1	7.9	3.60	3.92	5.27	0.97	3.82	23
30.5	19.4	15.4	10.8	10.3	1.65	0.29	3.88	0.02	4.69	24
31.0	20.2	15.6	11.8	9.8	3.14	1.49	0.44	0.69	0.66	25
31.5	21.3	16.0	12.7	10.4	1.50	3.68	4.52	4.02	1.76	26
31.0	16.0	15.5	15.4	10.4	$5\epsilon^5$	$4\epsilon^9$	$8\epsilon^5$	2.56	ϵ^4	27
288.	192.	144.	115.	95.9	2.27	3.46	3.92	2.49	2.98	28
688.	458.	344.	275.	229.	3.10	2.04	2.85	1.15	1.33	29

Understanding The Table

Lines 1 & 2: multiplier too small
Line 3: good r_2 but bad afterwards
Line 4: "random" multiplier
Line 5: the gen. of the pictures
Lines 6 & 7: notice 0 mult. effect
Lines 8, 9, 10: mults. chosen r_2, r_2, r_3
Line 11: Very good, but 2^{25} faded
Line 12: RANDU replaced 11!
Lines 13 & 14: Bench - Nied coprimes
Lines 16 & 23: Seach-based choices
Line 22: Cray X-MP library (2^{47})
Line 26: "Modern modulus" choice
Line 15: Nominated by GM to be "best"
Line 17: Random primitive root
Line 18: Seach
Line 19: $m = 2^{31}-1$, $a = 75$: Lewis, Goodman, Miller
Line 20: Seach for $a^2 < 2^{31}-1$
Line 21: Smaller modulus, similar results
Line 24: Combined 20 + 21 (subtracted)
Line 25: 2nd order $m = 2^{31}-1$
Lines 27-29: AWC / SWB, 28: RANLUX