Looking at the Uniform Distribution

Richard Schwartz

Carson City, Nevada

richard1941@gmail.com



- What is it?
- How can a data set be displayed?
- How can we tell is something is wrong with it?
- Moments
- Histograms
- The chi square statistic (simplified)
- Some Limitations on Testing
- The Probability Integral Transformation
- Application to RNG Testing
- Some Interesting Results

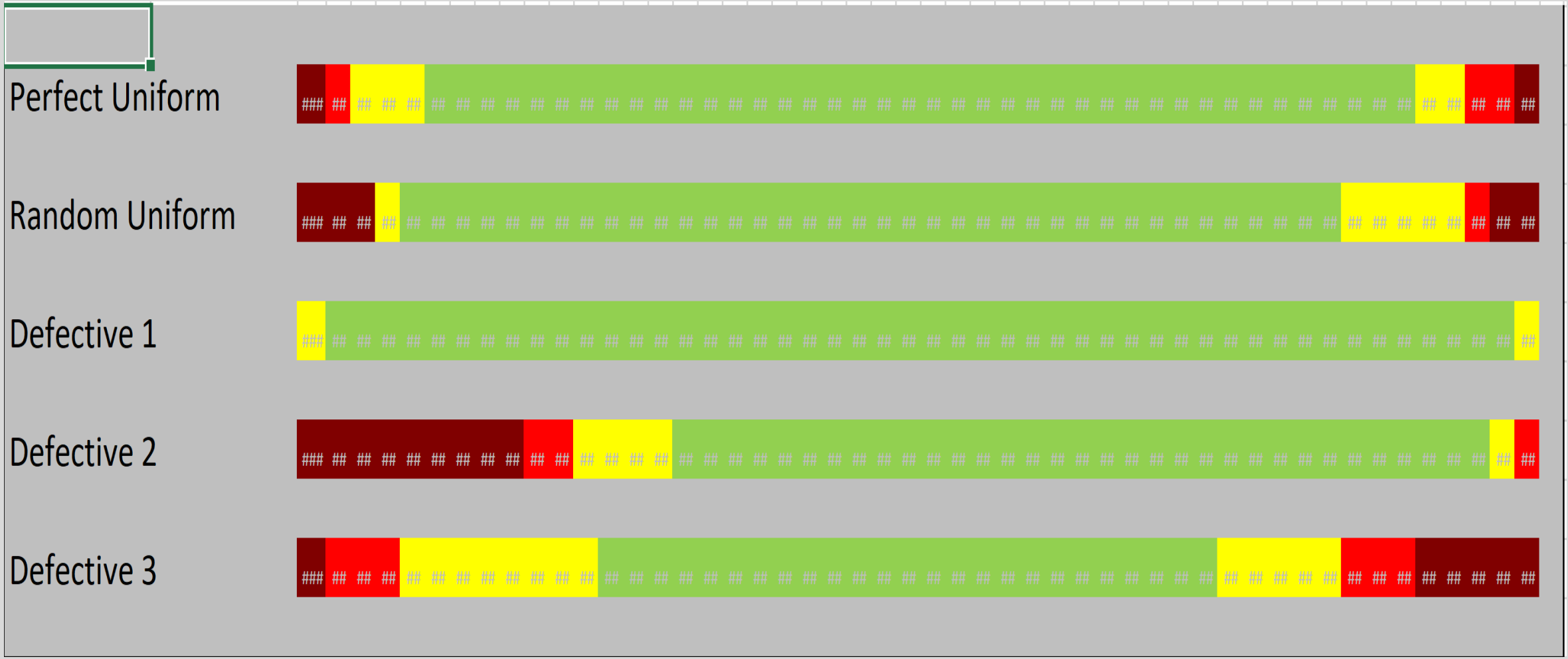
Uniform Distribution

- A number between 0 and 1 is generated
- The probability that the random number is less than x is…. x
- The probatility density function is 1 in the unit interfal, 0 elsewhere
- The mean is 0.5
- The variance is 1/12
- When we have a list of such random numbers from a source interesting observations can be made

Visualization of Data

- It is useful to sort the data.
- Data in certain ranges can be colored.
- Or the sorted data can be plotted
- See the following for a sample of 50 numbers from various distributions…

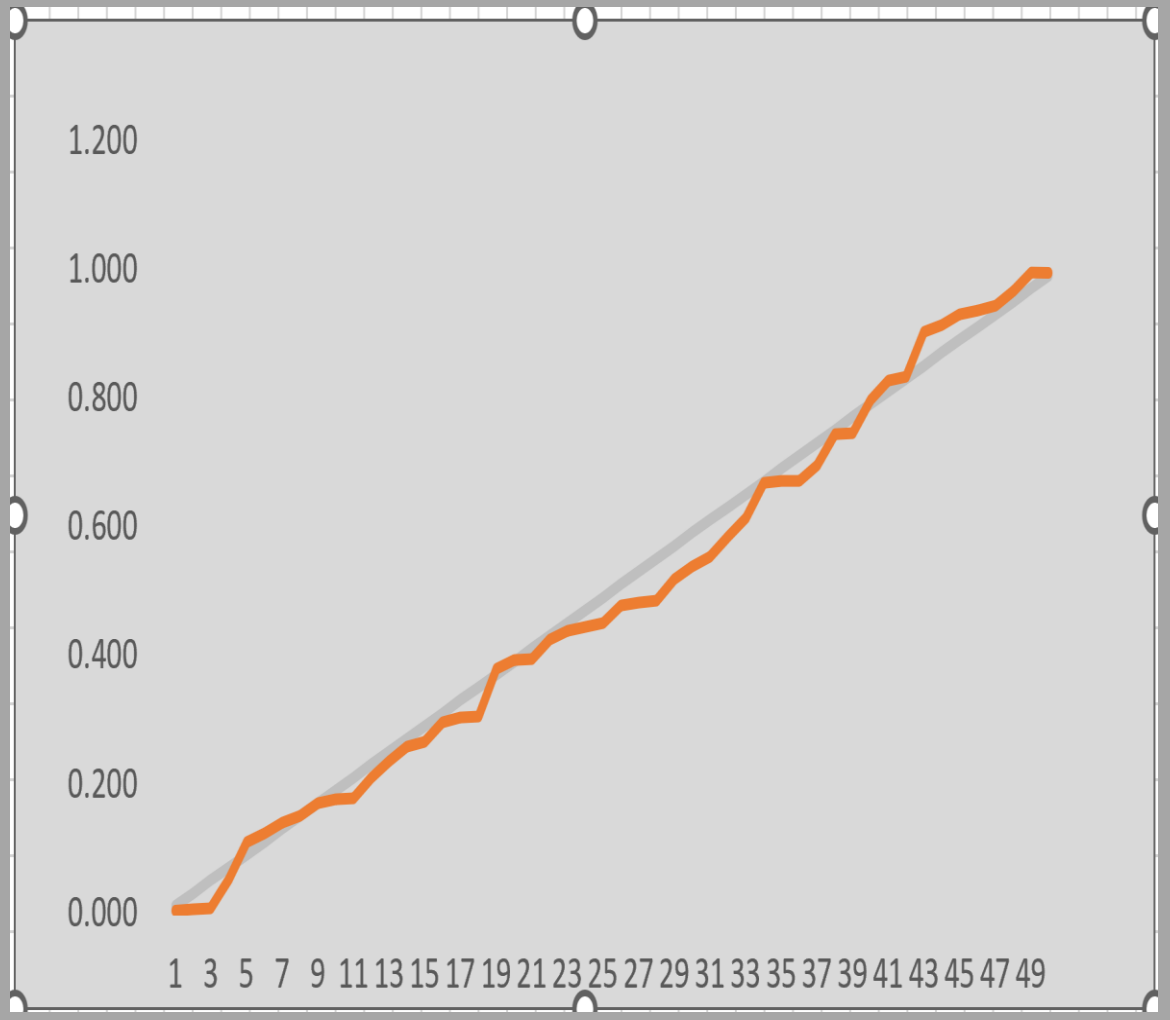
50 Random Numbers (sorted)



Defective Detective… just look!

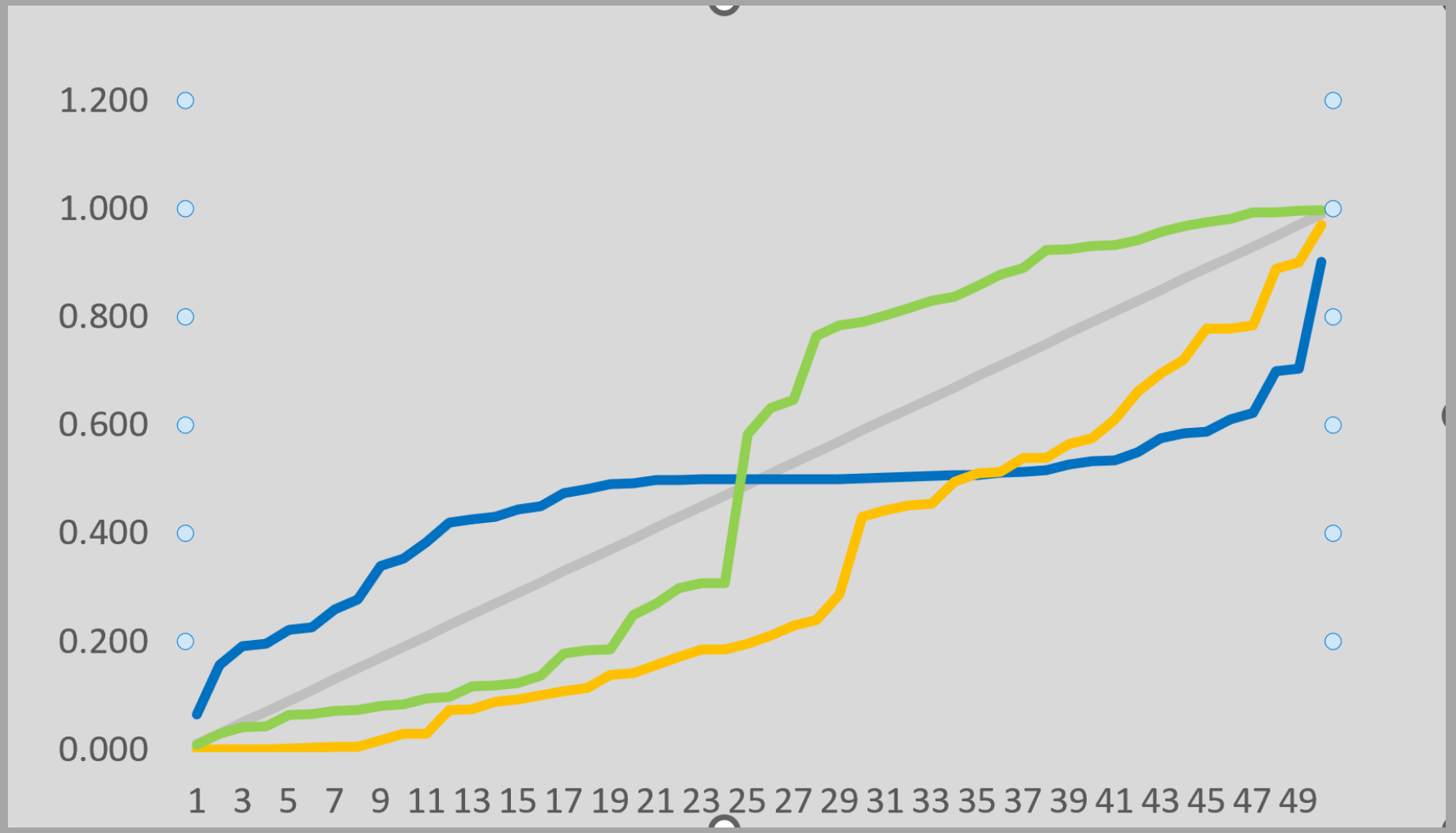
- Defective 1: Too much green, not enough in the tails .
- Defective 2: Asymmetric
- Defective 3: Tailheavy

50 Random Numbers (sorted) from U(0,1)



Note: the maximum deviation of the random curve from the straight line is the Kolmogorov-Smirnov statistic. Refer to Namir Shamas for more details .

When the Distribution is NOT Uniform…



Random Number Generator Testing

- We can test a batch of random numbers
  - A single batch might pass all tests
  - Why it might NOT pass all tests?
    - Unlucky
    - Defective Generator
  - To discover which, we must test numerous batches

Some Remarks on Random Number Generation and Testing

Our machines have limits: number of digits, memory, time, and sample limitations..

Digit Count

- HP-67 had 12 digit arithmetic (according to my emulator)
  - Floating point only, no integers
  - 9.99999 EEX 12 ↑ ↑ 1 - - yields a 1.
  - 1.001 EEX 13 ↑ ↑ 1 - - yields a 0.
  - The last two digits were undisplayed “guard digits”
- WP-34s has 16 digit arithmetic
  - 9.99999 EEX 15 FILL 1 - - yields 1
  - 1.001 EEX 16 FILL 1 - - yields 0
- Digits in x * y at most sum of number of digits in x and in y
  - Example, 997 * 999999 = 996,999,003 (3+6=9)
  - RNG intermediate results must not exceed the maximum digit count
- We work in floating point and must live with these limits

Memory Limits

In RNG testing we need to store histogram counts.

- Storing 2 bins in each memory provides 172 bins.
- Max bin count could be 99,999,999 without overflow
- The above leaves 14 registers for the actual RNG and supporting functions.
- Alternative: 3 bins per register for a total of 258 bins with max count of about 215000.

Time Limits

RNGs fail for large sample sizes. But testing the best RNG's to the breaking point may not be possible before the sun goes out and we have other worries.

Sample Size LImitations

- The chi square test requires a minimum count of 5 in cach bin, and our edge histogram consumes an average of f100 random numbers for each bin count.
- With 120 bins of equal probability, we need an average of about 16 counts per bin to assure that each bin gets at least 5. A permutation bin is calculated from five random numbers.
- That is a 120x16x5 = 9600 random numbers, a significant fraction of the 50,000 period of classic 997X, The 172 bin uniformity tests are even worse!

What If a Sample Repeats?

- Short period RNG's like 997X6 may repeat a set of random numbers
- All counts in the histogram are doubled.
- The variance in the chi square formula increases by factor of 4
- The expected value increases by a factor of 2
- Net result: chi square statistic doubles.

Example: 997X6, 10 Bins

- 500 Samples
  - Chi Square = 11.280
  - Probability = 0.743
- 500 Samples (twice)
  - Chi Square = 22.56
  - Probability= 0.993

Beware Repeating Random Numbers!

Subsamples

If there is a uniform distribution over a set of bins, the distribution will be uniform over any subset of those bins.

Example: we want to test distribution of pairs of random numbers in a 20x20 array. That is 400 bins.

Solution: just look at the first 172 of these.

Downside: much time will be wasted generating samples that are not examined. For a 100x100 array of bins, the test will go very v e r y s l o w . . .

Implementing the Chi Square Test

What I did, and why...

Test Result Depends on…

- Starting seed
- Starting point in RNG cycle
- Bin Count
- Sample size

Starting Seed

997X is a multiplicative congruential RNG. The random numbers are the powers of 997 (or some other multiplier) mudulo 1,000,000. These form a cyclic group with identity 1.

The size of that group is established by Knuth theorem D at 50,000.

Use 1 as the starting seed (represented as 0.000001, for example), the identity element of the group.

Since the period is 50,000, the inverse of 997 is 997^49999 (mod 1000000).. Calculation is easy on the WP-34s with the ^mod function.

more on theStarting Seed

Some RNG's use more than one memory to store the seed. If they are interrupted, they can jump to a different orbit that may have much shorter period.

To randomize seed without RNG interruption, use the following at the beginning of the test:

LBL A XEQ 99 KEY? L BACK 002 STOP, where LBL 99 is the RNG

User presses A, and thousands of random numbers are generated before A is pressed again. The RNG is NOT interrupted.

Sample Size

- Some statistical tests require large samples.
- Small sample size results in bins with fewer than 5 sample, invalidating the chi square test.
- Avoid nearly empty bins of low probability by arranging for all to have equal probability
- Very large samples become non-random. Increasing cycle length is key to improving an RNG.

Some Actual Test Data

- The following tests show the distribution of 50 chi square probabilities. In a truly random RNG, these should be uniformly distributed.
- Visualizing test data allows us to see that something is wrong, even when every test yields an acceptable result!
- Since the test data is from U(0, 1), analyze it by same method as the original uniform… subject to the much smaller sample size. For example, look at mean, variance, and other moments…

Effect of Bin Count:

more bins make test harder to pass

997X6	1260	0.032	0.096	0.108	0.116	0.127	0.154	0.157	0.205	0.209	0.220	0.226	0.243	0.256	0.258	0.260	0.274	0.334	0.353	0.362	0.388	0.403	0.416	0.416	0.435	0.441	0.441	0.471	0.486	0.503	0.509	0.511	0.542	0.544	0.548	0.554	0.592	0.602	0.604	0.653	0.664	0.673	0.700	0.731	0.811	0.837	0.841	0.860	0.861	0.884	0.981
20 bins	1600	0.094	0.108	0.118	0.120	0.136	0.196	0.222	0.239	0.251	0.318	0.321	0.321	0.334	0.341	0.354	0.366	0.370	0.381	0.397	0.408	0.419	0.419	0.422	0.425	0.454	0.459	0.466	0.484	0.498	0.499	0.511	0.537	0.554	0.613	0.617	0.617	0.620	0.635	0.684	0.695	0.802	0.811	0.858	0.858	0.874	0.927	0.947	0.952	0.970	0.976
	2000	0.055	0.055	0.055	0.105	0.114	0.154	0.168	0.177	0.191	0.219	0.226	0.228	0.232	0.233	0.245	0.247	0.274	0.378	0.380	0.409	0.425	0.427	0.428	0.429	0.447	0.480	0.482	0.499	0.513	0.513	0.521	0.526	0.528	0.538	0.543	0.544	0.546	0.581	0.621	0.682	0.685	0.690	0.730	0.739	0.739	0.744	0.806	0.824	0.831	0.872
	2500	0.039	0.053	0.066	0.091	0.127	0.134	0.155	0.178	0.211	0.246	0.257	0.280	0.292	0.301	0.315	0.327	0.328	0.351	0.352	0.366	0.389	0.419	0.420	0.433	0.441	0.444	0.451	0.452	0.489	0.519	0.525	0.545	0.553	0.627	0.642	0.662	0.665	0.703	0.732	0.732	0.741	0.749	0.754	0.755	0.771	0.822	0.826	0.830	0.872	0.878
	3200	0.044	0.149	0.151	0.153	0.154	0.163	0.176	0.192	0.194	0.209	0.220	0.226	0.236	0.246	0.246	0.270	0.285	0.287	0.312	0.321	0.332	0.339	0.354	0.375	0.395	0.401	0.410	0.435	0.456	0.493	0.505	0.511	0.526	0.553	0.555	0.561	0.570	0.589	0.605	0.612	0.648	0.664	0.668	0.679	0.701	0.712	0.760	0.773	0.795	0.943
	4000	0.015	0.097	0.116	0.120	0.197	0.216	0.219	0.225	0.243	0.250	0.253	0.266	0.282	0.288	0.301	0.304	0.308	0.308	0.312	0.320	0.353	0.353	0.358	0.363	0.368	0.376	0.382	0.388	0.391	0.393	0.399	0.408	0.410	0.417	0.438	0.450	0.457	0.475	0.488	0.488	0.490	0.520	0.537	0.537	0.544	0.593	0.622	0.626	0.671	0.724
	5000	0.111	0.155	0.194	0.198	0.209	0.210	0.219	0.251	0.262	0.269	0.274	0.287	0.287	0.296	0.298	0.302	0.310	0.314	0.317	0.320	0.320	0.324	0.324	0.334	0.370	0.371	0.373	0.374	0.375	0.379	0.385	0.389	0.392	0.400	0.412	0.424	0.436	0.452	0.505	0.533	0.581	0.581	0.593	0.604	0.612	0.662	0.681	0.735	0.754	0.783
	6300	0.050	0.057	0.133	0.139	0.146	0.209	0.218	0.218	0.242	0.245	0.249	0.250	0.263	0.264	0.276	0.283	0.285	0.320	0.334	0.341	0.382	0.387	0.388	0.391	0.399	0.401	0.417	0.431	0.431	0.444	0.455	0.456	0.481	0.496	0.498	0.526	0.540	0.543	0.548	0.565	0.569	0.574	0.590	0.596	0.625	0.631	0.633	0.673	0.706	0.757
	8000	0.035	0.036	0.078	0.083	0.120	0.120	0.158	0.168	0.239	0.266	0.400	0.402	0.409	0.435	0.441	0.460	0.465	0.470	0.471	0.472	0.477	0.477	0.481	0.486	0.488	0.507	0.509	0.526	0.531	0.546	0.547	0.565	0.566	0.585	0.596	0.600	0.607	0.609	0.612	0.613	0.635	0.637	0.644	0.647	0.648	0.650	0.703	0.725	0.736	0.772
	10000	0.064	0.071	0.080	0.080	0.094	0.097	0.101	0.109	0.127	0.135	0.135	0.135	0.135	0.143	0.154	0.171	0.171	0.198	0.213	0.326	0.360	0.385	0.402	0.416	0.422	0.427	0.452	0.461	0.512	0.523	0.536	0.547	0.555	0.557	0.583	0.621	0.623	0.647	0.666	0.669	0.683	0.692	0.716	0.717	0.739	0.766	0.768	0.777	0.821	0.834
	12500	0.043	0.044	0.065	0.092	0.100	0.126	0.126	0.129	0.132	0.140	0.156	0.159	0.194	0.204	0.209	0.216	0.244	0.265	0.266	0.266	0.274	0.304	0.312	0.313	0.314	0.317	0.321	0.336	0.345	0.348	0.354	0.360	0.364	0.379	0.391	0.403	0.410	0.568	0.663	0.704	0.705	0.705	0.719	0.744	0.748	0.757	0.788	0.790	0.792	0.825
	16000	0.178	0.200	0.201	0.201	0.205	0.211	0.212	0.219	0.224	0.226	0.227	0.237	0.238	0.240	0.243	0.255	0.271	0.273	0.278	0.279	0.283	0.289	0.292	0.300	0.321	0.325	0.326	0.379	0.382	0.388	0.392	0.392	0.393	0.396	0.399	0.399	0.416	0.422	0.434	0.439	0.453	0.465	0.470	0.478	0.503	0.530	0.531	0.564	0.591	0.656
	20000	0.030	0.047	0.057	0.057	0.062	0.066	0.067	0.080	0.123	0.150	0.152	0.168	0.170	0.183	0.191	0.193	0.205	0.214	0.217	0.233	0.236	0.237	0.240	0.244	0.245	0.252	0.262	0.273	0.275	0.288	0.292	0.310	0.322	0.333	0.376	0.378	0.408	0.427	0.434	0.446	0.446	0.469	0.471	0.493	0.503	0.536	0.560	0.562	0.580	0.584
	25000	0.016	0.019	0.034	0.040	0.045	0.053	0.053	0.053	0.053	0.054	0.056	0.059	0.066	0.070	0.072	0.072	0.081	0.083	0.084	0.091	0.091	0.099	0.118	0.121	0.125	0.158	0.172	0.187	0.200	0.200	0.213	0.219	0.233	0.239	0.241	0.245	0.251	0.257	0.267	0.282	0.318	0.325	0.337	0.338	0.380	0.405	0.426	0.451	0.456	0.473

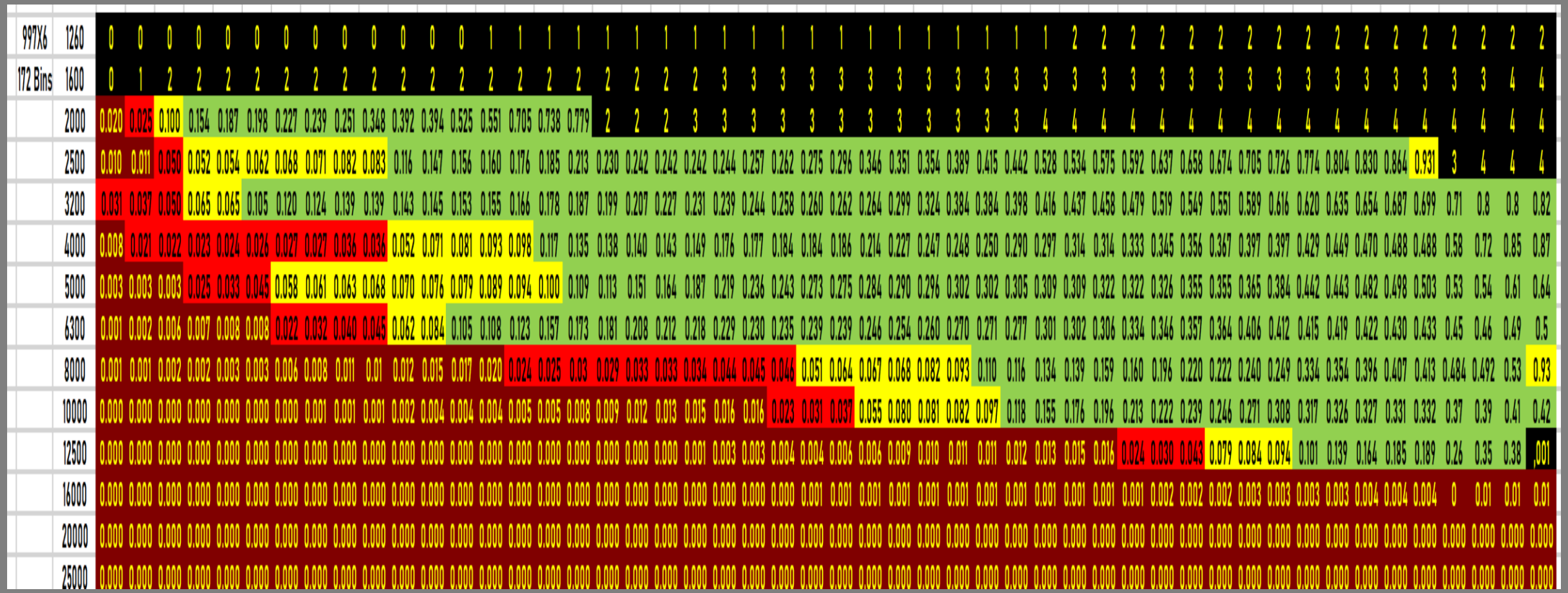
997X6	1260	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
172 Bins	1600	0	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	4	4
	2000	0.020	0.025	0.100	0.154	0.187	0.198	0.227	0.239	0.251	0.348	0.392	0.394	0.525	0.551	0.705	0.738	0.779	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	2500	0.010	0.011	0.050	0.052	0.054	0.062	0.068	0.071	0.082	0.083	0.116	0.147	0.156	0.160	0.176	0.185	0.213	0.230	0.242	0.242	0.242	0.244	0.257	0.262	0.275	0.296	0.346	0.351	0.354	0.389	0.415	0.442	0.528	0.534	0.575	0.592	0.637	0.658	0.674	0.705	0.726	0.774	0.804	0.830	0.864	0.931	3	4	4	4
	3200	0.031	0.037	0.050	0.065	0.065	0.105	0.120	0.124	0.139	0.139	0.143	0.145	0.153	0.155	0.166	0.178	0.187	0.199	0.207	0.227	0.231	0.239	0.244	0.258	0.260	0.262	0.264	0.299	0.324	0.384	0.384	0.398	0.416	0.437	0.458	0.479	0.519	0.549	0.551	0.589	0.616	0.620	0.635	0.654	0.687	0.699	0.71	0.8	0.8	0.82
	4000	0.008	0.021	0.022	0.023	0.024	0.026	0.027	0.027	0.036	0.036	0.052	0.071	0.081	0.093	0.098	0.117	0.135	0.138	0.140	0.143	0.149	0.176	0.177	0.184	0.184	0.186	0.214	0.227	0.247	0.248	0.250	0.290	0.297	0.314	0.314	0.333	0.345	0.356	0.367	0.397	0.397	0.429	0.449	0.470	0.488	0.488	0.58	0.72	0.85	0.87
	5000	0.003	0.003	0.003	0.025	0.033	0.045	0.058	0.061	0.063	0.068	0.070	0.076	0.079	0.089	0.094	0.100	0.109	0.113	0.151	0.164	0.187	0.219	0.236	0.243	0.273	0.275	0.284	0.290	0.296	0.302	0.302	0.305	0.309	0.309	0.322	0.322	0.326	0.355	0.355	0.365	0.384	0.442	0.443	0.482	0.498	0.503	0.53	0.54	0.61	0.64
	6300	0.001	0.002	0.006	0.007	0.008	0.008	0.022	0.032	0.040	0.045	0.062	0.084	0.105	0.108	0.123	0.157	0.173	0.181	0.208	0.212	0.218	0.229	0.230	0.235	0.239	0.239	0.246	0.254	0.260	0.270	0.271	0.277	0.301	0.302	0.306	0.334	0.346	0.357	0.364	0.406	0.412	0.415	0.419	0.422	0.430	0.433	0.45	0.46	0.49	0.5
	8000	0.001	0.001	0.002	0.002	0.003	0.003	0.006	0.008	0.011	0.01	0.012	0.015	0.017	0.020	0.024	0.025	0.03	0.029	0.033	0.033	0.034	0.044	0.045	0.046	0.051	0.064	0.067	0.068	0.082	0.093	0.110	0.116	0.134	0.139	0.159	0.160	0.196	0.220	0.222	0.240	0.249	0.334	0.354	0.396	0.407	0.413	0.484	0.492	0.53	0.93
	10000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.001	0.001	0.001	0.002	0.004	0.004	0.004	0.005	0.005	0.008	0.009	0.012	0.013	0.015	0.016	0.016	0.023	0.031	0.037	0.055	0.080	0.081	0.082	0.097	0.118	0.155	0.176	0.196	0.213	0.222	0.239	0.246	0.271	0.308	0.317	0.326	0.327	0.331	0.332	0.37	0.39	0.41	0.42
	12500	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.001	0.003	0.003	0.004	0.004	0.006	0.006	0.009	0.010	0.011	0.011	0.012	0.013	0.015	0.016	0.024	0.030	0.043	0.079	0.084	0.094	0.101	0.139	0.164	0.185	0.189	0.26	0.35	0.38	,001
	16000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.001	0.001	0.001	0.001	0.001	0.001	0.001	0.001	0.001	0.001	0.001	0.001	0.002	0.002	0.002	0.003	0.003	0.003	0.003	0.004	0.004	0.004	0	0.01	0.01	0.01
	20000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	25000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

Effect of Sample Size

- For small samples, there are not enough random numbers to assure a minimum of 5 in each bin, which is required for validity of the chisquare test. ***
- For large samples, forced uniformity creates a set of random numbers that behaves in a non-random way.

*** The teachings of Ismaili Shimi are that a few bins with a count of four are OK.

Effect of Sample Size



Best Row of the 997X6 Tests



Some Primitive Statistics

Expected from Perfect RNG

- Mean:
  0.5000 ± 0.0408
- Standard Deviation
  0.2875 ± 0.0187
- $E(x^2)$
  0.333 ± 0.042

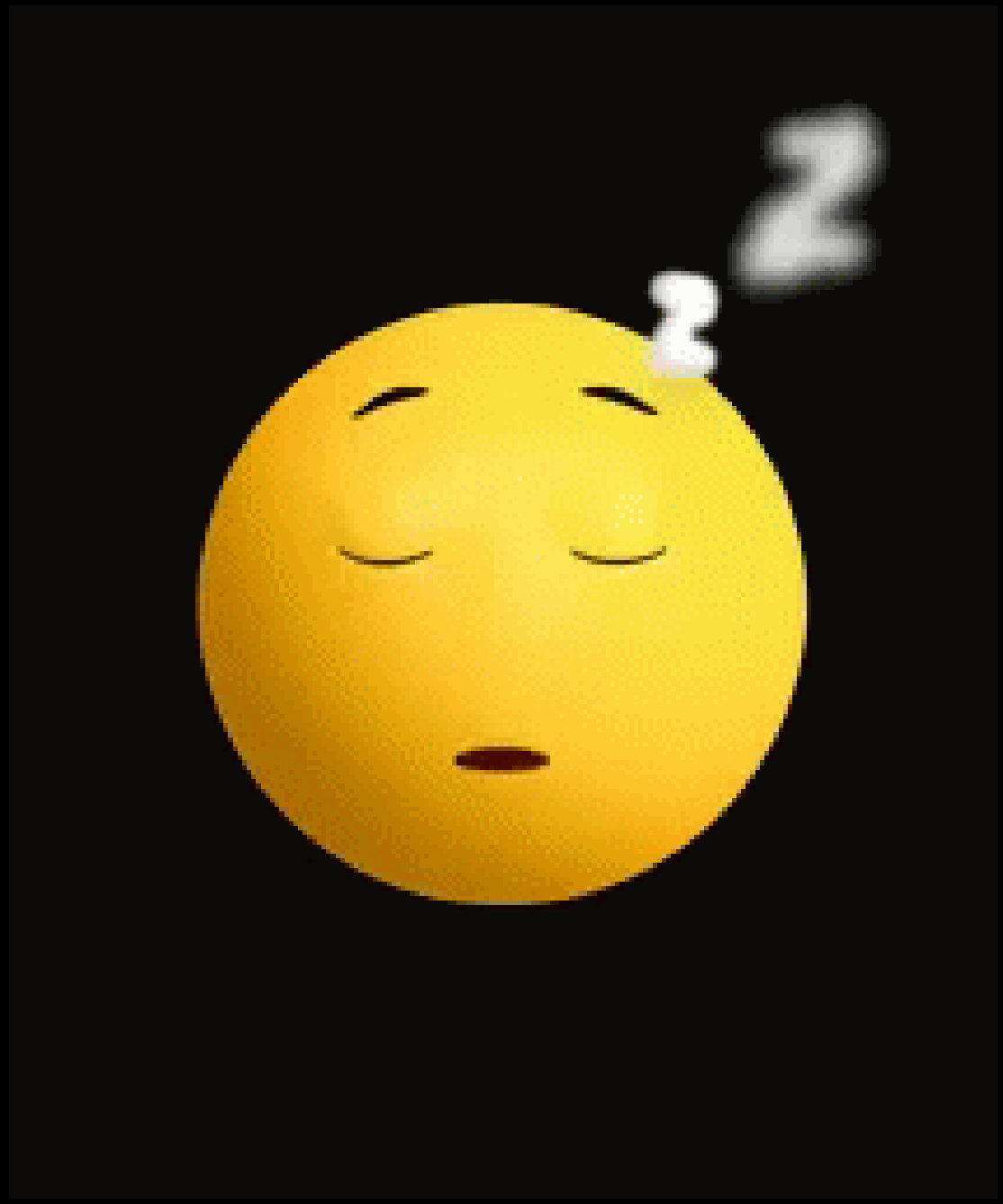
997X6, 50 tests

- Mean
  0.344 (-3.8σ)
- Standard Deviation
  0.2303 (-3.0σ)
- $E(x^2)$
  0.171 (-3.8σ)

Finding:

Although individual batches of 6300 random numbers are acceptably uniform per the chi square test, the PROCESS THAT GENERATES THEM is hopelessly defective. You never know if you will be lucky to get a good batch.

Do not despair! Things can be made better (but not perfect).



HHC2026