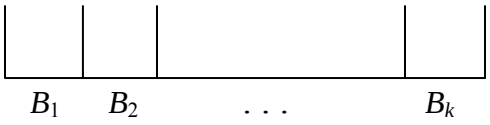
Random-Number Generators 2 (Chapter 7, Law)

- **Testing random number generators**
  - Since random number generators are completely deterministic, we need to test to see if they appear to be random and ***IID uniform*** on [0, 1].
  - There are two types of tests: *Empirical* and *theoretical*.
  - Empirical tests are statistical tests performed on the numbers produced by a generator.
  - Empirical tests, are, therefore, local as they depend on a specific sample of numbers used for testing.
  - Theoretical test are global. The parameters of a generator are used to assess the quality of the generator.

- **Elements of a statistical test**
  - Statistical tests are used to draw conclusions using data.
  - Statistical tests allow deciding between two alternatives:
    - H_0: The *null hypothesis*,
    - H_a: The *alternative hypothesis*.
  - H_0 represents the status-quo.
  - H_a is the hypothesis we want to provide evidence to justify.
  - We show that H_a is true by showing that H_0 is not true.

- The decision between "reject H_0" and "do not reject H_0" is made based on a *test statistic* (*TS*) which is computed based on available data.
- The decision is valid at a *risk level* α .
- The *rejection region (RR)* specifies the values of *TS* for which H_0 is rejected.
- Then, one can make a conclusion of the form:
  "At 100α% significance level there is (in)sufficient statistical evidence to favor H_a".

- **χ^2 (chi-squared) random variable**
  - Let $Z_1, Z_2, \ldots, Z_n$ be iid standard normal random variables, then $\chi^2_n = \sum_{i=1}^{n} Z_i^2$ has a χ^2 distribution with n "degrees of freedom" (df).
- **Pearson's Theorem**
  - Consider k boxes $B_1, B_2, \ldots, B_k$, as in the following figure:



  - Assume that we throw n balls into these boxes randomly independently of each other.
  - Let p_i be the probability that a ball is thrown in box i.
  - Let O_i be the number of observed balls in box i.
  - Then, O_i is binomially distributed with $E_i = E[O_i] = np_i$.

- Further, define the rv χ^2 as

$$\chi^2 = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i}.$$

- Pearson's Theorem states that for n large enough χ^2 has a χ^2 distribution with $k-1$ df.
- (The proof is based on the normal approximation to the Binomial distribution, the central limit theorem and noting that O_i are dependent and accounting for their correlation.)

- **χ^2 test for random number generators**
  - This test works on n generated pseudo random numbers, $u_1, u_2, \ldots, u_n$, where n is large.
  - It tests whether the u_is are uniformly distribute on (0,1).
  - One divides the (0,1) interval into k equal segments segment and measure the number of u_is in each segment, O_i .
  - Select k such that the expected number of observations $n/k \geq 5$ (see Law pp. 343-345) for further discussion.
  - The test is performed as follows.
    - H_0: u_is are $U(0,1)$
    - H_a: u_is are not $U(0,1)$
    - $TS: \ \chi^2 = \sum_{i=1}^{k} \frac{(O_i - n/k)^2}{(n/k)}$.
    - RR: Reject H_0 if $\chi^2 > \chi^2_{k-1,1-\alpha}$, where $\chi^2_{k-1,1-\alpha}$ is such that $P\{\chi^2_{k-1} < \chi^2_{k-1,1-\alpha}\} = 1-\alpha$ and χ^2_{k-1} is a χ^2 rv with $k-1$ df.

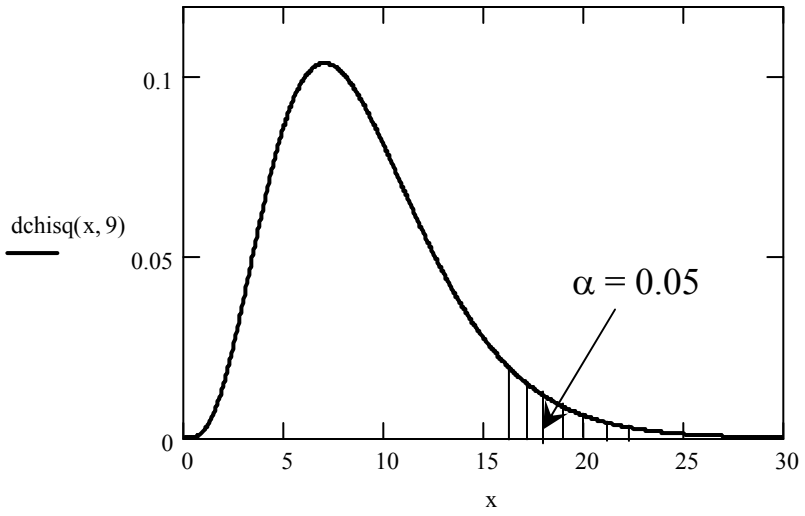
- **Example 1: χ^2 test**
  - The following 100 numbers were generated using Excel.

0.126	0.092	0.375	0.938	0.254	0.223	0.029	0.359	0.397	0.343
0.086	0.300	0.072	0.001	0.404	0.621	0.092	0.120	0.565	0.869
0.255	0.958	0.874	0.893	0.046	0.424	0.325	0.603	0.235	0.660
0.167	0.336	0.708	0.589	0.381	0.225	0.191	0.288	0.596	0.633
0.832	0.422	0.902	0.348	0.143	0.039	0.723	0.372	0.920	0.928
0.786	0.680	0.430	0.610	0.363	0.463	0.670	0.678	0.926	0.223
0.208	0.650	0.070	0.010	0.696	0.340	0.548	0.497	0.973	0.518
0.821	0.456	0.485	0.629	0.683	0.953	0.338	0.750	0.780	0.075
0.321	0.994	0.984	0.293	0.185	0.454	0.474	0.557	0.094	0.464
0.690	0.636	0.195	0.645	0.680	0.548	0.118	0.543	0.476	0.137

  - Use the χ^2 test to test if this data is uniformly distributed.
  - The TS is computed as follows.

i	Interval	O_i	E_i	$(O_i - E_i)^2 / E_i$
1	[0.0,0.1)	12	10	0.4
2	[0.1,0.2)	9	10	0.1
3	[0.2,0.3)	10	10	0
4	[0.3,0.4)	13	10	0.9
5	[0.4,0.5)	12	10	0.4
6	[0.5,0.6)	8	10	0.4
7	[0.6,0.7)	16	10	3.6
8	[0.7,0.8)	5	10	2.5
9	[0.8,0.9)	5	10	2.5
10	[0.9,1.0]	10	10	0
			χ^2	10.8

  - For $\alpha = 0.05$, the "critical value" for the test is $\chi^2_{9,0.95} = 16.919$ (see Table T.2, p. 717, Law).
  - Decision: Do not reject H_0.
  - Conclusion: At a 5% significance level there is insufficient statistical evidence that the data is not U(0,1).



- **What is α anyway?**
  - α is the probability of a "Type I error",

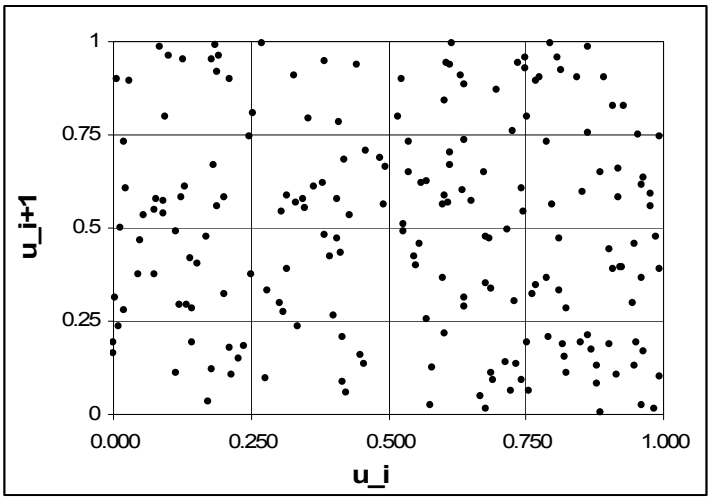
$$\alpha = P\{\text{Reject } H_0 | H_0 \text{ is true}\} .$$

  - In Example 1 we would reject H_0 if $\chi^2 > 16.919$ and conclude that the data is not U(0,1).
  - But this conclusion is false if the data is actually U(0,1).
  - This could happen, with probability

$$\alpha = P\{\chi^2 > 16.919\} = 0.05 .$$

- **Serial Test**
  - This is a generalization of the χ^2 test to higher dimensions.
  - Idea of the test: If the u_is are iid $U(0,1)$ rvs, then the d-tuples $\mathbf{u}_1 = (u_1, u_2, \ldots, u_d)$, $\mathbf{u}_2 = (u_{d+1}, u_{d+2}, \ldots, u_{2d})$, …., are iid random vectors uniformly distributed on $[0,1]^d$.

- For example, for $d = 2$, one arranges the generated random numbers into $\{(u_1, u_2), (u_3, u_4), \ldots, (u_{2n-1}, u_{2n})\}$ and divides $(0,1)^2$ into k^2 squares labeled (j_1,j_2), $j_1 = 1,\ldots, k$, $j_2 = 1,\ldots, k$.
- The serial test detects correlations (checks independence).



- For d =2, the test is performed as follows.
  - H_0: $\mathbf{u}_i$s are iid $U(0,1)\times U(0,1)$
  - H_a: u_is are not iid $U(0,1)\times U(0,1)$
  - $TS: \quad \chi^2 = \sum_{j_1=1}^{k}\sum_{j_2=1}^{k} \frac{[O_{j_1 j_2} - n/k^2]^2}{(n/k^2)}$, where $O_{j_1 j_2}$ is the number of $\mathbf{u}_i$ vectors falling in cell (j_1, j_2).
  - RR: Reject H_0 if $\chi^2 > \chi^2_{k^2-1,1-\alpha}$.

- **Runs tests**
  - These are tests of independence.
  - They should be used before tests of uniformity (such as χ^2).
  - They are based on the number of runs, where a run is sequence of successive increasing or decreasing numbers.

- There are many types of runs tests. E.g., some are based on counting the total number of runs and others are based on counting runs of different lengths (see Law p. 407).

- **Runs up and down test**
  - This test counts the total number of runs r in a series of generated numbers $u_1, u_2, \ldots, u_n$.
  - The logic is that a truly random (independent) series, the number of runs should not be too small, nor too large.
  - If n is large and the u_is are independent then it can be shown that the number of runs R is normally distributed with the following mean and variance

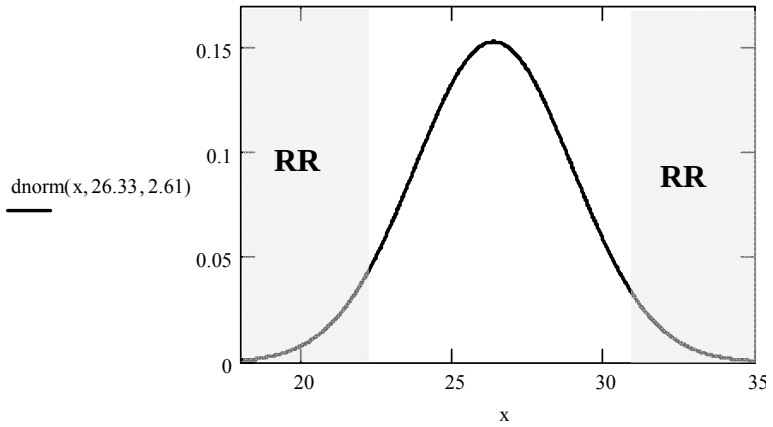
$$E[R] = \frac{2n-1}{3}, \quad \sigma_R^2 = \frac{16n-29}{90}.$$

  - The test is then performed as follows.
    - H_0: u_is are independent.
    - H_a: u_is are not independent.
    - $TS: \ z = \dfrac{r - E[R]}{\sigma_R}$.
    - RR: Reject H_0 if $z < -z_{1-\alpha/2}$ or $z > z_{1-\alpha/2}$.

- **Example 2: Runs test**
  - The following 40 numbers were generated from Excel.
  - Check independence using the runs test.

0.84	0.20	0.92	0.01	0.89	0.48	0.32	0.97	0.98	0.15
−	−	+	−	+	−	−	+	+	−
0.37	0.44	0.00	0.84	0.52	0.82	0.60	0.84	0.47	0.02
−	+	−	+	−	+	−	+	−	−
0.57	0.95	0.94	0.46	0.76	0.43	0.95	0.19	0.38	0.64
+	+	−	−	+	−	+	−	+	+
0.72	0.24	0.00	0.72	0.33	0.54	0.65	0.80	0.41	0.86
+	−	−	+	−	+	+	+	−	+

  - The number of runs here is $r = 28$.
  - With $n = 40$, $E[R] = \frac{2(40)-1}{3} = 26.33$, $\sigma_R = \sqrt{\frac{16(40)-29}{90}} = 2.61$.
  - $TS:\ z = \frac{r - E[R]}{\sigma_R} = \frac{28 - 26.33}{2.61} = 0.641$.
  - For $\alpha = 0.05$, the critical values is $z_{1-\alpha/2} = 1.96$.
  - Since $-z_{1-\alpha/2} < z < z_{1-\alpha/2}$, do not reject H_0.
  - Conclusion: At a 5% significance level there is insufficient statistical evidence that the u_is are not independent.

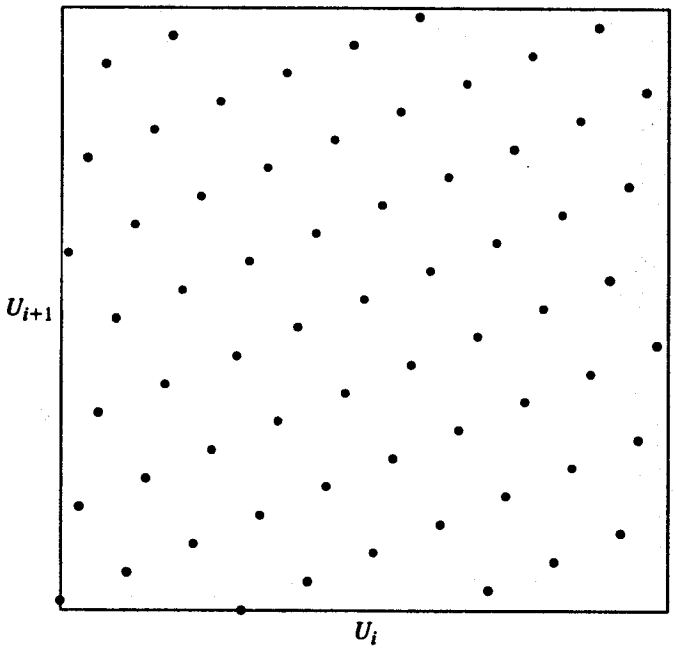


- **Theoretical tests**
  - As aforementioned, these tests do not use generated data.
  - They develop properties for a generator based on its parameters values.
  - For example, for a LCG it can be shown that the sample mean and variance of the generated u_is over a full cycle are $\bar{U} = \frac{1}{2} - \frac{1}{2m}$ and $s^2 = \frac{1}{12} - \frac{1}{12m^2}$.
  - This is a good indication for large period m since the exact values for "real" U(0,1) numbers are 1/2 and 1/12.
  - The best well-known theoretical tests are based on the observation of Marsaglia (1968) for LCGs:

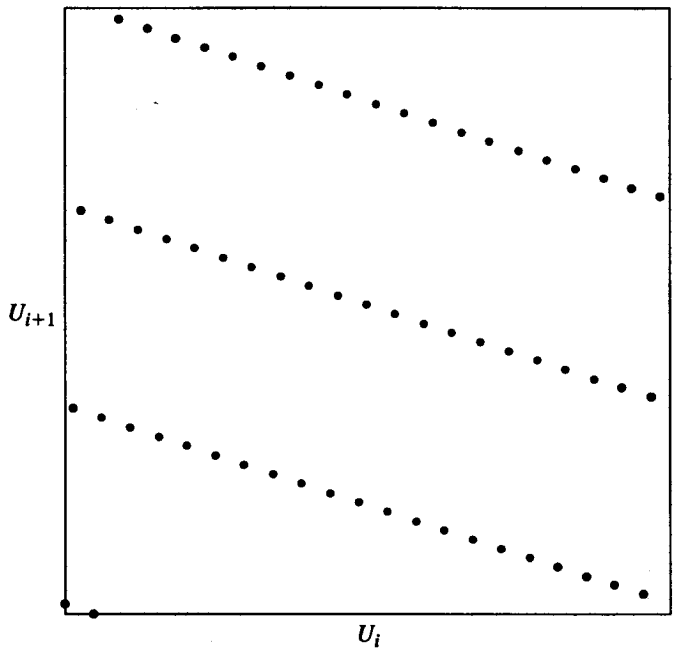
    "Random numbers fall mainly in the planes"
  - For example, when plotting a large number of pairs (u_i, u_{i+1}) generated by a LCG, the values cluster around parallel lines through the unit square in a *lattice* structure.
  - The following two pages present examples of this.
  - Many theoretical, *Spectral* and *lattice* tests, attempt to compute the distance between hyperplanes, where the numbers fall.
  - The smaller this distance the better.

Two-dimensional

$m = 64$, $a = 37$, $c = 1$:

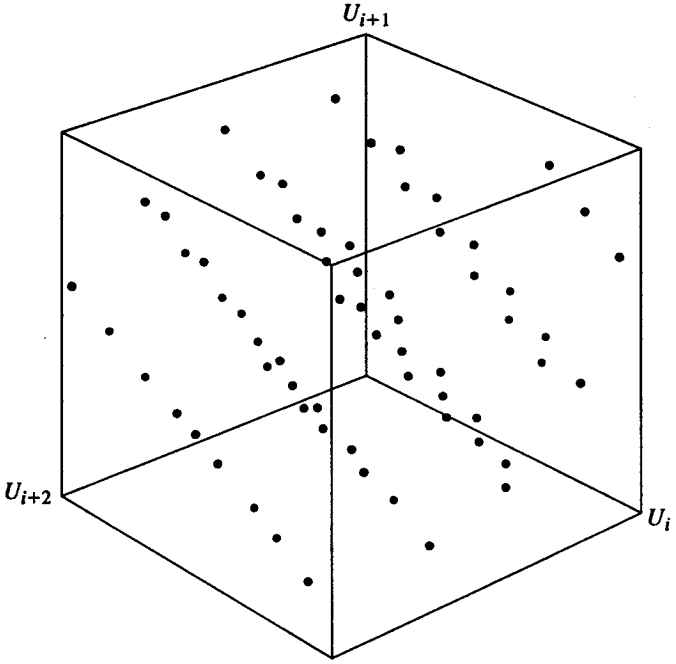


$m = 64$, $a = 21$, $c = 1$ (only change from above: $a = 21$ rather than 37):



Three-dimensional

$m = 64$, $a = 37$, $c = 1$:



$m = 2^{31} = 2{,}147{,}483{,}648$, $a = 2^{16} + 3 = 65{,}539$, $c = 0$ (RANDU):