Computer Simulation

Module 6: Generating Uniform Random Numbers

Dave Goldsman, Ph.D.
Professor
Stewart School of Industrial and Systems Engineering

Choosing a Good Generator – Some Theory

Lesson Overview

Last Time: Gave a couple of generators with extremely long cycle times.

This Time: We'll discuss some PRN generator properties from a theory point of view.

I'll present an amalgamation of typical results that I won't really hold you responsible for.

Here are some miscellaneous results due to Knuth and others that are helpful in determining the quality of a PRN generator.

Theorem: The generator $X_i = aX_{i-1} \bmod 2^n$ $(n > 3)$ can have cycle length of at most 2^{n-2}. This is achieved when X_0 is odd and $a = 8k + 3$ or $a = 8k + 5$ for some k.

Example (BCNN): $X_i = 13X_{i-1} \bmod (64)$.

X_0	X_1	X_2	X_3	X_4	$\cdots$	X_8	$\cdots$	X_{16}
1	13	41	21	17	$\cdots$	33	$\cdots$	**1**
2	26	18	42	34	$\cdots$	**2**		
3	39	56	63	51	$\cdots$	35	$\cdots$	**3**
4	52	36	20	**4**				

Really short periods! ☹

Lots of these types of cycle length results.

Theorem: $X_i = (aX_{i-1} + c) \bmod m$ $(c > 0)$ has full cycle if (i) c and m are relatively prime; (ii) $a - 1$ is a multiple of every prime which divides m; and (iii) $a - 1$ is a multiple of 4 if 4 divides m.

Corollary: $X_i = (aX_{i-1} + c) \bmod 2^n$ $(c, n > 1)$ has full cycle if c is odd and $a = 4k + 1$ for some k.

Theorem: The *multiplicative* generator $X_i = aX_{i-1} \bmod m$, with prime m has full period $(m - 1)$ if and only if (i) m divides $a^{m-1} - 1$; and (ii) for all integers $i < m - 1$, m does not divide $a^i - 1$.

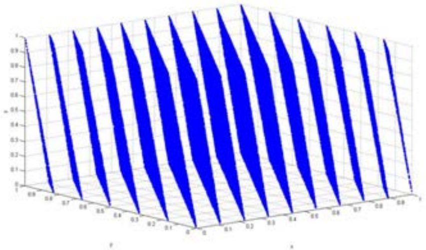
Remark: For $m = 2^{31} - 1$, it can be shown that 534,600,000 multipliers yield full period, the "best" of which is $a = 950{,}706{,}376$ (Fishman and Moore 1986).

Geometric Considerations

Theorem: The k-tuples $(R_i, \ldots, R_{i+k-1})$, $i \geq 1$, from multiplicative generators lie on parallel hyperplanes in $[0,1]^k$.

The following geometric quantities are of interest.

- Minimum number of hyperplanes (in all directions). Find the multiplier that maximizes this number.
- Maximum distance between parallel hyperplanes. Find the multiplier that minimizes this number.
- Minimum Euclidean distance between adjacent k-tuples. Find the multiplier that maximizes this number.



Remark: The RANDU generator is particularly bad since it lies on only 15 hyperplanes.

Can also look at one-step serial correlation.

Serial Correlation of LCGs (Greenberger 1961):

$$\mathrm{Corr}(R_1, R_2) \;\leq\; \frac{1}{a}\left(1 - \frac{6c}{m} + 6\left(\frac{c}{m}\right)^2\right) + \frac{a+6}{m}$$

This upper bound is very small for m in the range of 2 billion and, say, $a = 16807$.

Lots of other theory considerations that can be used to evaluate the performance of a particular PRN generator.

Summary

This Time: We saw a mishmash of PRN generator theoretical properties – just to give you a flavor (not to hold you responsible, necessarily).

Next Time: We'll go over some statistical considerations when choosing a good generator. These may be a bit more intuitive and relevant.

Computer Simulation

Module 6: Generating Uniform Random Numbers

Dave Goldsman, Ph.D.
Professor
Stewart School of Industrial and Systems Engineering

Choosing a Good Generator – Statistical Tests, Intro

Lesson Overview

Last Time: Plowed thru some miscellaneous theoretical properties of PRNs.

This Time: We'll give an overview on statistical tests for goodness-of-fit and independence.

The chi-squared test will really give you fits!

Statistical Tests Intro

We’ll look at two classes of tests:

Goodness-of-fit tests — are the PRNs approximately Unif(0,1)?

Independence tests — are the PRNs approximately independent?

If a generator passes both types of tests (in addition to others I won’t tell you about), we’ll be happy to use the PRNs it generates.

Intro (cont'd)

All tests are of the form H_0 (our null hypothesis) vs. H_1 (the alternative hypothesis).

We regard H_0 as the status quo, so we'll only reject H_0 if we have "ample" evidence against it. (Innocent until proven guilty.)

Usually, we really want to avoid incorrect rejections of H_0.

Intro (cont'd)

When we design the test, we set the level of significance

$\alpha = P(\text{Reject } H_0 \mid H_0 \text{ true})$.

Typically, $\alpha = 0.05$ or 0.1, and is the probability of Type I error.

We can also specify the probability of Type II error,

$\beta = P(\text{Accept } H_0 \mid H_0 \text{ false})$,

but we won't worry about that just now.

Summary

This Time: Presented an introduction to hypothesis testing in the context of selecting a PRN generator.

Next Time: We'll discuss the chi-squared goodness-of-fit test to check whether or not the PRNs are actually uniform.

Computer Simulation

Module 6: Generating Uniform Random Numbers

Dave Goldsman, Ph.D.

Professor

Stewart School of Industrial and Systems Engineering

Choosing a Good Generator – Goodness-of-Fit Tests

GTx

Lesson Overview

Last Time: Quick intro to hypothesis testing. Interested in testing PRNs for uniformity and independence.

This Time: We'll discuss the chi-squared goodness-of-fit test to check whether or not the PRNs are actually uniform.

There are many g-o-f tests, but this is the most tried-and-true.

χ^2 Goodness-of-Fit Test

Test $H_0 : R_1, R_2, \ldots R_n \sim$ Unif(0,1).

Divide the unit interval into k cells (subintervals). If you choose equi-probable cells $[0, \frac{1}{k}), [\frac{1}{k}, \frac{2}{k}), \ldots, [\frac{k-1}{k}, 1]$, then a particular observation R_j will fall in a particular cell with prob $1/k$.

Tally how many of the n observations fall into the k cells. If $O_i \equiv$ # of R_j's in cell i, then (since the R_j's are i.i.d.), we can easily see that $O_i \sim \text{Bin}(n, \frac{1}{k})$, $i = 1, 2, \ldots, k$.

Thus, the expected number of R_j's to fall in cell i will be $E_i \equiv \mathrm{E}[O_i] = n/k$, $i = 1, 2, \ldots, k$.

χ^2 Goodness-of-Fit Test

We reject the null hypothesis H_0 if the O_i's don't match the E_i's well.

The χ^2 goodness-of-fit statistic is

$$\chi_0^2 \equiv \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i}.$$

A large value of this statistic indicates a bad fit.

χ^2 Goodness-of-Fit Test

In fact, we *reject* the null hypothesis H_0 (that the observations are uniform) if $\chi^2_0 > \chi^2_{\alpha,k-1}$, where $\chi^2_{\alpha,k-1}$ is the appropriate $(1-\alpha)$ quantile from a χ^2 table, i.e., $P(\chi^2_{k-1} < \chi^2_{\alpha,k-1}) = 1-\alpha$.

If $\chi^2_0 \le \chi^2_{\alpha,k-1}$, we *fail to reject* H_0.

Usual recommendation from baby stats class: For the χ^2 g-o-f test to work, pick k, n such that $E_i \ge 5$ and n at least 30. But…

Unlike what you learned in baby stats class, when we test PRN generators, we usually have a *huge* number of observations n (at least millions) with a large number of cells k. When k is large, we can use the approximation

$$\chi^2_{\alpha,k-1} \approx (k-1)\left[1 - \frac{2}{9(k-1)} + z_\alpha\sqrt{\frac{2}{9(k-1)}}\right]^3,$$

where z_α is the appropriate standard normal quantile.

Remarks: (1) 16807 PRN generator usually passes the g-o-f test just fine. (2) We'll show how to do g-o-f tests for other distributions later on — just doing uniform PRNs for now. (3) Other g-o-f tests: Kolmogorov–Smirnov test, Anderson–Darling test, etc.

Illustrative Example: $n = 1000$ observations, $k = 5$ intervals.

interval	[0,0.2]	(0.2,0.4]	(0.4,0.6]	(0.6,0.8]	(0.8,1.0]
E_i	200	200	200	200	200
O_i	179	208	222	199	192

$$\chi_0^2 \equiv \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i} = 5.27. \qquad \chi^2_{\alpha,k-1} = \chi^2_{0.05,4} = 9.49.$$

Since $\chi_0^2 < \chi^2_{\alpha,k-1}$, we fail to reject H_0, and so we'll assume that the observations are approximately uniform. $\square$

Summary

This Time: Showed how to do a chi-squared g-o-f test for uniformity of PRNs. It’s fun! It’s nutritious!

Next Time: Independence Day!

Computer Simulation

Module 6: Generating Uniform Random Numbers

Dave Goldsman, Ph.D.

Professor

Stewart School of Industrial and Systems Engineering

Choosing a Good Generator – Independence Tests, I

Lesson Overview

Last Time: Discussed the chi-squared g-o-f test for uniformity of PRNs. It gave us the fits!

This Time: We'll look at so-called "runs" tests for *independence* of the PRNs.



Czech it out!

(Next time, we'll look at autocorrelation tests for independence.)

Independence – Runs Tests

Now consider the hypothesis $H_0 : R_1, R_2, \ldots, R_n$ are independent.

Let's look at Three Little Bears examples of coin tossing:

A. H, T, H, T, H, T, H, T, H, T,. . .   (negative correlation)

B. H, H, H, H, H, T, T, T, T, T,. . .   (positive correlation)

C. H, H, H, T, T, H, T, T, H, T,. . .   ("just right")

Definition: A *run* is a series of similar observations.

In A above, the runs are: “H”, “T”, “H”, “T”,. . . . (many runs)

In B, the runs are: “HHHHH”, “TTTTT”, ... (very few runs)

In C: “HHH”, “TT”, “H”, “TT”,. . . . (medium number of runs)

A *runs test* will reject the null hypothesis of independence if there are “too many” or “too few” runs, whatever that means. There are various types of runs tests; we’ll discuss two of them.

Runs Test "Up and Down". Consider the following PRNs.

$$.41 \quad .68 \quad .89 \quad .84 \quad .74 \quad .91 \quad .55 \quad .71 \quad .36 \quad .30 \quad .09\ldots$$

If the uniform increases, put a $+$; if it decreases, put a $-$ (like H's and T's). Get the sequence

$$+ + - - + - + - - - \ldots$$

Here are the associated runs:

$$++,\ --,\ +,\ -,\ +,\ - - -,\ \ldots$$

So do we have too many or two few runs?

Let A denote the total number of runs "up and down" out of n observations. ($A = 6$ in the above example.)

Amazing Fact: If n is large (say, ≥ 20) and the R_j's are actually independent, then

$$A \approx \mathrm{Nor}\left(\frac{2n-1}{3}, \frac{16n-29}{90}\right).$$

We'll reject H_0 if A is too big or small. The test statistic is

$$Z_0 = \frac{A - \mathrm{E}[A]}{\sqrt{\mathrm{Var}(A)}},$$

and we reject H_0 if $|Z_0| > z_{\alpha/2}$.

Up and Down Example

Suppose that $n = 100$ and $A = 55$.

Then A is approximately

$$\mathrm{Nor}(66.33,\ 17.46).$$

So $Z_0 = -2.71$.

If $\alpha = 0.05$, then $z_{\alpha/2} = 1.96$, and we reject H_0 (i.e., reject independence).

Runs Test "Above and Below the Mean". Again consider

$$.41 \quad .68 \quad .89 \quad .84 \quad .74 \quad .91 \quad .55 \quad .71 \quad .36 \quad .30 \quad .09\ldots$$

If $R_i \geq 0.5$, put a $+$; if $R_i < 0.5$, put a $-$. Get the sequence

$$- + + + + + + + - - - \ldots$$

Here are the associated runs, of which there are $B = 3$:

$$-, \quad + + + + + + +, \quad - - -$$

Fact: If n is large and the R_j's are actually independent, then

$$B \;\approx\; \text{Nor}\left(\frac{2n_1n_2}{n}+\frac{1}{2},\,\frac{2n_1n_2(2n_1n_2-n)}{n^2(n-1)}\right),$$

where n_1 is the number of observations ≥ 0.5 and $n_2 = n - n_1$.

The test statistic is $Z_0 = (B - \mathrm{E}[B])/\sqrt{\mathrm{Var}(B)}$, and we reject H_0 if $|Z_0| > z_{\alpha/2}$.

Illustrative Example (from BCNN): Suppose that $n = 40$, with the following $+/-$ sequence.

$$
\begin{array}{c}
- + + + + + + + - - - + + - + - - - - - \\
- - + + - - - - + + - - + - + - - + + -
\end{array}
$$

Then $n_1 = 18$, $n_2 = 22$, and $B = 17$. This implies that $\mathrm{E}[B] \doteq 20.3$ and $\mathrm{Var}(B) \doteq 9.54$. And this yields $Z_0 = -1.07$.

Since $|Z_0| < z_{\alpha/2} = 1.96$, we *fail* to reject the test; so we can treat the observations as independent. $\square$

Lots of other tests available for independence: Other runs tests, correlation tests, gap test, poker test, birthday test, etc.

Summary

This Time: We ran off at the mouth with runs tests for independence of PRNs: “Up and Down” and “Above and Below the Mean”.

Next Time: A bonus “autocorrelation” test for independence!

Computer Simulation

Module 6: Generating Uniform Random Numbers

Dave Goldsman, Ph.D.
Professor
Stewart School of Industrial and Systems Engineering

Choosing a Good Generator – Independence Tests, II

Lesson Overview

Last Time: We looked at a couple of runs tests for independence of PRNs

This Time: Autocorrelation tests for independence.

This is sort of bonus material, but we'll be talking about autocorr throughout the course, so let's take it out for spin here.

Correlation Test. Assuming that the R_i's are all Unif(0,1), let's conduct a *correlation* test for H_0: R_i's independent.

We define the *lag-1 correlation* of the R_i's by $\rho \equiv \mathrm{Corr}(R_i, R_{i+1})$. Ideally, ρ should equal zero. A good estimator for ρ is given by

$$\hat{\rho} \equiv \left(\frac{12}{n-1} \sum_{k=1}^{n-1} R_k R_{1+k} \right) - 3.$$

$$\hat{\rho} \approx \mathrm{Nor}\left(0, \frac{13n-19}{(n-1)^2} \right) \text{ (under } H_0\text{).}$$

The test statistic $Z_0 = \hat{\rho}/\sqrt{\mathrm{Var}(\hat{\rho})}$, and we reject if $|Z_0| > z_{\alpha/2}$.

Illustrative Example: Consider the following $n = 30$ PRNs.

0.29	0.38	0.46	0.29	0.69	0.73	0.80	0.74	0.99	0.75
0.88	0.66	0.56	0.41	0.35	0.22	0.18	0.05	0.25	0.36
0.39	0.45	0.50	0.62	0.76	0.81	0.97	0.72	0.11	0.55

After a little algebra, we get

$$\hat{\rho} = 0.950 \quad \text{and} \quad \text{Var}(\hat{\rho}) = \frac{13n - 19}{(n-1)^2} = 0.441.$$

So $Z_0 = 0.950/\sqrt{0.441} = 1.43$.

Since $|Z_0| < z_{\alpha/2} = 1.96$, we *fail* to reject the test, meaning that we can treat the PRNs as independent. (Of course, $n = 30$ is sort of small, and perhaps this decision will change if we increase n.) $\Box$

Summary

This Time: Autocorrelation tests for independence of PRNs.

This completes Module 6 on PRNs.

Next Module: PRNs are too easy! When we return, we shall be promoted to **random variate** **generation**!

https://getyarn.io/yarn-clip/49a98d2d-6852-4c74-8e06-5a87dac9e915