NAG Fortran Library Chapter Introduction

G05 – Random Number Generators

Contents

1 Scope of the Chapter

This chapter is concerned with the generation of sequences of independent pseudo-random and quasi-random numbers from various distributions, and the generation of pseudo-random time series from specified time-series models.

2 Background to the Problems

2.1 Pseudo-random Numbers

A sequence of pseudo-random numbers is a sequence of numbers generated in some systematic way such that its statistical properties are as close as possible to those of true random numbers: for example, negligible correlation between consecutive numbers. The most common methods are based on the **multiplicative congruential** algorithm, see Knuth (1981). The basic algorithm is defined as:

$$n_i = (a \times n_{i-1}) \bmod m \tag{1}$$

The integers n_i are then divided by m to give uniformly distributed pseudo-random numbers lying in the interval $(0, 1)$.

Alternatively there is a variant known as the Wichmann–Hill algorithm, see Maclaren (1989), defined as:

$$\begin{aligned} n_{1,i} &= \left(a_1 \times n_{1,i-1}\right) \bmod m_1 \\ n_{2,i} &= \left(a_2 \times n_{2,i-1}\right) \bmod m_2 \\ n_{3,i} &= \left(a_3, \times, n_{3,i-1}\right) \bmod m_3 \\ n_{4,i} &= \left(a_4, \times, n_{4,i-1}\right) \bmod m_4 \\ U_i &= \left(\frac{n_{1,i}}{m_1} + \frac{n_{2,i}}{m_2} + \frac{n_{3,i}}{m_3} + \frac{n_{4,i}}{m_4}\right) \bmod 1.0 \end{aligned} \tag{2}$$

This generates pseudo-random numbers U_i, uniformly distributed in the interval $(0, 1)$.

Either of these algorithms can be selected to generate uniformly distributed pseudo-random numbers. If the basic algorithm (1) is selected then the NAG generator uses the values $a = 13^{13}$ and $m = 2^{59}$ in (1). This generator gives a **cycle length** (i.e., the number of random numbers before the sequence starts repeating itself) of 2^{57}. A good rule of thumb is never to use more numbers than the square root of the cycle length in any one experiment as the statistical properties are impaired. For closely related reasons, breaking numbers down into their bit patterns and using individual bits may cause trouble.

If the Wichmann–Hill algorithm is selected then one or more of 273 independent generators are available. Each of these is defined by the set of constants a_j and m_j for $j = 1, \ldots, 4$. The constants a_j are in the range 112 to 127 and the constants m_j are prime numbers in the range 16718909 to 16776971, which are close to $2^{24} = 16777216$. These constants have been chosen so that they give good results with the spectral test, see Knuth (1981) and Maclaren (1989). The period of each Wichmann–Hill generator would be at least 2^{92} if it were not for common factors between $(m_1 - 1)$, $(m_2 - 1)$, $(m_3 - 1)$ and $(m_4 - 1)$. However, each generator should still have a period of at least 2^{80}. Further discussion of the properties of these generators is given in Maclaren (1989) where it was shown that the generated pseudo-random sequences are essentially independent of one another according to the spectral test.

The sequence given in (1) needs an initial value n_0, known as the **seed**, while the sequence given in (2) needs four such seeds. The use of the same seed will lead to the same sequence of numbers when these are computed serially. One method of obtaining a seed is to use the real-time clock; this will give a non-repeatable sequence. It is important to note that the statistical properties of the random numbers are only guaranteed within sequences and not between sequences. Repeated initialization will thus render the numbers obtained less rather than more independent. Similarly the statistical properties of the random numbers are not guaranteed between two sequences generated using the two algorithms.

2.2 Quasi-Random Numbers

Quasi-random numbers are intended primarily for use in Monte Carlo integration. Like pseudo-random numbers they are uniformly distributed but they are not statistically independent, rather they are designed to give a more even distribution in multidimensional space (uniformity). Therefore, they are often more efficient than pseudo-random numbers in multidimensional Monte Carlo methods. There are several quasi-

random generators, three of which are available in this chapter, they are the Sobol, Faure and Neiderreiter generators.

2.3 Non-uniform Random Numbers

Random numbers from other distributions may be obtained from the uniform random numbers by the use of transformations and rejection techniques, and for discrete distributions, by table based methods.

(a) Transformation Methods

For a continuous random variable, if the cumulative distribution function (CDF) is $F(x)$ then for a uniform $(0, 1)$ random variate u, $y = F^{-1}(u)$ will have CDF $F(x)$. This method is only efficient in a few simple cases such as the exponential distribution with mean μ, in which case $F^{-1}(u) = -\mu \log u$. Other transformations are based on the joint distribution of several random variables. In the bivariate case, if v and w are random variates there may be a function g such that $y = g(v, w)$ has the required distribution; for example, the Student's t-distribution with n degrees of freedom in which v has a Normal distribution, w has a gamma distribution and $g(v, w) = v\sqrt{n/w}$.

(b) Rejection Methods

Rejection techniques are based on the ability to easily generate random numbers from a distribution (called the envelope) similar to the distribution required. The value from the envelope distribution is then accepted as a random number from the required distribution with a certain probability; otherwise, it is rejected and a new number is generated from the envelope distribution.

(c) Table Search Methods

For discrete distributions, if the cumulative probabilities, $P_i = \text{Prob}(x \leq i)$, are stored in a table then, given u from a uniform $(0, 1)$ distribution, the table is searched for i such that $P_{i-1} < u \leq P_i$. The returned value i will have the required distribution. The table searching can be made faster by means of an index, see Ripley (1987). The effort required to set up the table and its index may be considerable, but the methods are very efficient when many values are needed from the same distribution.

2.4 Copulas and Other Random Structures

A copula is a function that links the univariate marginal distributions with their multivariate distribution. Sklar's theorem Sklar (1973) states that if f is an m-dimensional distribution function with continuous margins $f_1, f_2, \cdots, f_m$, then f has a unique copula representation, c, such that

$$f(x_1, x_2, \cdots, x_m) = c(f_1(x_1), f_2(x_2), \cdots, f_m(x_m))$$

The copula, c, is a multivariate uniform distribution whose dependence structure is defined by the dependence structure of the multivariate distribution f, with

$$c(u_1, u_2, \cdots, u_m) = f\big(f_1^{-1}(u_1), f_2^{-1}(u_2), \cdots, f_m^{-1}(u_m)\big)$$

where $u_i \in [0, 1]$. This relationship can be used to simulate variates from distributions defined by the dependence structure of one distribution and each of the marginal distributions given by another. For additional information see Nelsen (1998) or Boye (Unpublished manuscript) and the references therein.

In addition to random numbers from various distributions, random compound structures can be generated. These include random time series, random matrices and random samples.

The efficiency of a simulation exercise may often be increased by the use of variance reduction methods (see Morgan (1984)). It is also worth considering whether a simulation is the best approach to solving the problem. For example, low-dimensional integrals are usually more efficiently calculated by routines in Chapter D01 rather than by Monte Carlo integration.

3 Recommendations on Choice and Use of Available Routines

Note: please refer to the Users' Note for your implementation to check that a routine is available.

3.1 Design of the Chapter

All the generation routines call an internal generator (selected to be either the basic generator (1) or a Wichmann–Hill generator (2)), which generates random numbers from a uniform distribution over $(0, 1)$.

3.1.1 Initialization

Prior to generating any variates the internal generator must be initializd. Two utility routines are provided for this, G05KBF and G05KCF, both of which allow either the basic generator or one of the 273 Wichmann–Hill generators to be chosen as the internal generator.

G05KBF selects and initializes a generator to a repeatable (when executed serially) state: two calls of G05KBF with the same parameter-values will result in the same subsequent sequences of random numbers (when both are generated serially). The basic generator or one of 273 Wichmann–Hill generators can be selected as the base generator.

G05KCF selects and initializes a generator to a non-repeatable state, in such a way that different calls of G05KCF, either in the same run or different runs of the program, will almost certainly result in different subsequent sequences of random numbers.

Routines to save and restore generator states are not required since the ISEED parameter contains the current state and can have its values copied and stored at any time.

3.1.2 Repeated intialisation

As mentioned in Section 2, it is important to note that the statistical properties of pseudo-random numbers are only guaranteed within sequences and not between sequences produced by the same generator. Repeated initialization will thus render the numbers obtained less rather than more independent. In a simple case there should be only one call to G05KBF or G05KCF and this call should be before any call to an actual generation routine.

3.1.3 Copulas

After calling G05RAF or G05RBF the G01F routines in Chapter G01 can be used to convert the uniform marginal distributors into a different form as required.

3.2 Programming Advice

Take care when programming calls to those routines in this chapter which are functions. The reason is that different calls with the same parameters are intended to give different results.

For example, if you wish to assign to Z the difference between two successive random numbers generated by G05KAF, beware of writing

```
Z = G05KAF(IGEN,ISEED) - G05KAF(IGEN,ISEED)
```

It is quite legitimate for a Fortran compiler to compile zero, one or two calls to G05KAF; if two calls, they may be in either order (if zero or one calls are compiled, Z would be set to zero). A safe method to program this would be

```
X = G05KAF(IGEN,ISEED)
Y = G05KAF(IGEN,ISEED)
Z = X-Y
```

4 Index

5 Routines Withdrawn or Scheduled for Withdrawal

Withdrawn Routine	Mark of Withdrawal	Replacement Routine(s)
G05AAF	7	G05KAF
G05ABF	7	G05LGF
G05ACF	7	G05LJF
G05ADF	7	G05LAF
G05AEF	7	G05LAF
G05AFF	7	G05LKF
G05AGF	7	G05LLF
G05AHF	7	G05LFF
G05AJF	7	G05LFF
G05AKF	7	G05LFF
G05ALF	7	G05LEF
G05AMF	7	G05LEF
G05ANF	7	G05LCF
G05APF	7	G05LBF
G05AQF	7	G05LDF
G05ARF	7	G05MZF
G05ASF	7	G05MJF
G05ATF	7	G05MAF
G05AUF	7	G05MLF
G05AVF	7	G05MKF
G05AWF	7	G05MZF
G05AZF	7	G05MZF
G05BAF	7	G05KBF
G05BBF	7	G05KCF
G05CAF	22	G05KAF
G05CBF	22	G05KBF
G05CCF	22	G05KCF
G05CFF	22	F06DFF
G05CGF	22	F06DFF
G05DAF	22	G05LGF
G05DBF	22	G05LJF
G05DCF	22	G05LNF
G05DDF	22	G05LAF
G05DEF	22	G05LKF
G05DFF	22	G05LLF
G05DGF	16	G05LFF
G05DHF	22	G05LCF
G05DJF	22	G05LBF
G05DKF	22	G05LDF
G05DLF	16	G05LEF
G05DMF	16	G05LEF
G05DPF	22	G05LMF
G05DRF	22	G05MEF
G05DYF	22	G05MAF
G05DZF	22	G05KEF
G05EAF	22	G05LZF
G05EBF	22	G05MAF

G05ECF	22	G05MKF
G05EDF	22	G05MJF
G05EEF	22	G05MCF
G05EFF	22	G05MLF
G05EGF	22	G05PAF
G05EHF	22	G05NAF
G05EJF	22	G05NBF
G05EWF	22	G05PAF
G05EXF	22	G05MZF
G05EYF	22	G05MZF
G05EZF	22	G05LZF
G05FAF	22	G05LGF
G05FBF	22	G05LJF
G05FDF	22	G05LAF
G05FEF	22	G05LEF
G05FFF	22	G05LFF
G05FSF	22	G05LPF
G05GAF	22	G05QAF
G05GBF	22	G05QBF
G05HDF	22	G05PCF
G05YAF	23	G05YCF, G05YDF, G05YEF, G05YFF, G05YGF, G05YHF, G05YJF and G05YKF
G05YBF	23	G05YCF, G05YDF, G05YEF, G05YFF, G05YGF, G05YHF, G05YJF and G05YKF
G05ZAF	22	No replacement document required

6 References

Boye E (Unpublished manuscript) Copulas for Finance: A reading guide and some applications Financial Econometrics Research Centre, City University Business School, London

Knuth D E (1981) *The Art of Computer Programming (Volume 2)* (2nd Edition) Addison–Wesley

Maclaren N M (1989) The generation of multiple independent sequences of pseudorandom numbers *Appl. Statist.* **38** 351–359

Morgan B J T (1984) *Elements of Simulation* Chapman and Hall

Nelsen R B (1998) *An Introduction to Copulas. Lecture Notes in Statistics 139* Springer

Ripley B D (1987) *Stochastic Simulation* Wiley

Sklar A (1973) Random Variables: Joint Distribution Functions and Copulas *Kybernetika* **9** 499–460