Linear congruential generator

From Wikipedia, the free encyclopedia

A **linear congruential generator** (**LCG**) is an algorithm that yields a sequence of randomized numbers calculated with a linear equation. The method represents one of the oldest and best-known pseudorandom number generator algorithms.[1] The theory behind them is easy to understand, and they are easily implemented and fast, especially on computer hardware which can provide modulo arithmetic by storage-bit truncation.

The generator is defined by the recurrence relation:

$$X_{n+1} = (aX_n + c) \mod m$$

where X is the sequence of pseudorandom values, and

$m,\ 0 < m$ – the "modulus"
$a,\ 0 < a < m$ – the "multiplier"
$c,\ 0 \leq c < m$ – the "increment"
$X_0,\ 0 \leq X_0 < m$ – the "seed" or "start value"

are integer constants that specify the generator. If $c = 0$, the generator is often called a **multiplicative congruential generator** (MCG), or Lehmer RNG. If $c \neq 0$, the method is called a *mixed congruential generator*.[2]

Contents

Period length

The period of a general LCG is at most *m*, and for some choices of factor *a* much less than that. Provided that the offset *c* is nonzero, the LCG will have a full period for all seed values if and only if:[2]

1. c and m are relatively prime,
2. $a - 1$ is divisible by all prime factors of m,
3. $a - 1$ is a multiple of 4 if m is a multiple of 4.

These three requirements are referred to as the Hull-Dobell Theorem.[3] While LCGs are capable of producing pseudorandom numbers which can pass formal tests for randomness, this is extremely sensitive to the choice of the parameters *c*, *m*, and *a*.

Historically, poor choices had led to ineffective implementations of LCGs. A particularly illustrative example of this is RANDU, which was widely used in the early 1970s and led to many results which are currently being questioned because of the use of this poor LCG.[4]

Parameters in common use

The most efficient LCGs have an *m* equal to a power of 2, most often $m = 2^{32}$ or $m = 2^{64}$, because this allows the modulus operation to be computed by merely truncating all but the rightmost 32 or 64 bits. The following table lists the parameters of LCGs in common use, including built-in *rand()* functions in runtime libraries of various compilers.

Source	*m*	(multiplier) *a*	(increment) *c*	output bits of seed in *rand()* / *Random(L)*
Numerical Recipes	2^{32}	1664525	1013904223	
Borland C/C++	2^{32}	22695477	1	bits 30..16 in *rand()*, 30..0 in *lrand()*
glibc (used by GCC)[5]	2^{31}	1103515245	12345	bits 30..0
ANSI C: Watcom, Digital Mars, CodeWarrior, IBM VisualAge C/C++ [6]	2^{31}	1103515245	12345	bits 30..16
Borland Delphi, Virtual Pascal	2^{32}	134775813	1	bits 63..32 of *(seed * L)*
Microsoft Visual/Quick C/C++	2^{32}	214013 ($343FD_{16}$)	2531011 ($269EC3_{16}$)	bits 30..16
Microsoft Visual Basic (6 and earlier)[7]	2^{24}	1140671485 ($43FD43FD_{16}$)	12820163 ($C39EC3_{16}$)	
RtlUniform from Native API[8]	$2^{31}-1$	2147483629 ($7FFFFFED_{16}$)	2147483587 ($7FFFFFC3_{16}$)	
Apple CarbonLib, C++11's `minstd_rand0`[9]	$2^{31}-1$	16807	0	see MINSTD
C++11's `minstd_rand`[9]	$2^{31}-1$	48271	0	see MINSTD
MMIX by Donald Knuth	2^{64}	6364136223846793005	1442695040888963407	
Newlib	2^{64}	6364136223846793005	1	bits 63...32
VAX's **MTH$RANDOM**,[10] old versions of glibc	2^{32}	69069	1	
Java's java.util.Random, glibc	2^{48}	25214903917	11	bits 47...16

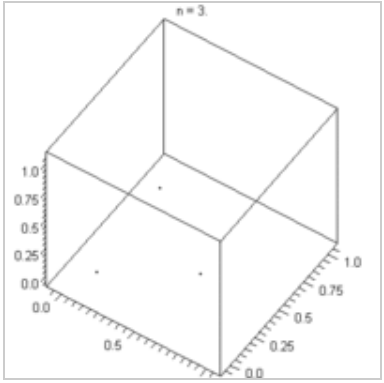
[ld]rand48[_r]()				
Formerly common:				
RANDU [4]	2^{31}	65539	0	

As shown above, LCGs do not always use all of the bits in the values they produce. For example, the Java implementation operates with 48-bit values at each iteration but returns only their 32 most significant bits. This is because the higher-order bits have longer periods than the lower-order bits (see below). LCGs that use this truncation technique produce statistically better values than those that do not.

Advantages and disadvantages of LCGs

LCGs are fast and require minimal memory (typically 32 or 64 bits) to retain state. This makes them valuable for simulating multiple independent streams.

LCGs should not be used for applications where high-quality randomness is critical. For example, it is not suitable for a Monte Carlo simulation because of the serial correlation (among other things). They should also not be used for cryptographic applications; see cryptographically secure pseudo-random number generator for more suitable generators. If a linear congruential generator is seeded with a character and then iterated once, the result is a simple classical cipher called an affine cipher; this cipher is easily broken by standard frequency analysis.



Hyperplanes of a linear congruential generator in three dimensions

LCGs tend to exhibit some severe defects. For instance, if an LCG is used to choose points in an n-dimensional space, the points will lie on, at most, $m^{1/n}$ hyperplanes (Marsaglia's Theorem, developed by George Marsaglia). This is due to serial correlation between successive values of the sequence X_n. The spectral test, which is a simple test of an LCG's quality, is based on this fact.

A further problem of LCGs is that the lower-order bits of the generated sequence have a far shorter period than the sequence as a whole if m is set to a power of 2. In general, the nth least significant digit in the base b representation of the output sequence, where $b^k = m$ for some integer k, repeats with at most period b^n.

Nevertheless, LCGs may be a good option. For instance, in an embedded system, the amount of memory available is often severely limited. Similarly, in an environment such as a video game console taking a small number of high-order bits of an LCG may well suffice. The low-order bits of LCGs when m is a power of 2 should never be relied on for any degree of randomness whatsoever. Indeed, simply substituting 2^n for the modulus

term reveals that the low order bits go through very short cycles. In particular, any full-cycle LCG when m is a power of 2 will produce alternately odd and even results.

Comparison with other PRNGs

If higher-quality random numbers are needed, and sufficient memory is available (~ 2 kilobytes), then the Mersenne twister algorithm provides a vastly longer period ($2^{19937} - 1$) and variate uniformity.[11] The Mersenne twister generates higher-quality deviates than almost any LCG. A common Mersenne twister implementation, interestingly enough, uses an LCG to generate seed data.

A Linear Feedback Shift Register PRNG can be implemented with essentially the same amount of memory and produces a stream of pseudorandom numbers with better randomness qualities when considering streams of bits, albeit with a bit more computation.

The linear feedback shift register has a strong relationship to linear congruential generators.[12] Given a few values in the sequence, some techniques can predict the following values in the sequence for not only linear congruent generators but any other polynomial congruent generator.[12]

See also

- Full cycle
- Inversive congruential generator
- Multiply-with-carry
- Lehmer RNG (sometimes called the Park-Miller RNG)
- Combined Linear Congruential Generator

Notes

1. ^ "Linear Congruential Generators (http://demonstrations.wolfram.com/LinearCongruentialGenerators/)" by Joe Bolte, Wolfram Demonstrations Project.
2. ^ ***a*** ***b*** Knuth 1997, Sec. 3.2.1
3. ^ Severance, Frank (2001). *System Modeling and Simulation*. John Wiley & Sons, Ltd. p. 86. ISBN 0-471-49694-4.
4. ^ ***a*** ***b*** Press, William H., et al. (1992). *Numerical Recipes in Fortran 77: The Art of Scientific Computing* (2nd ed.). ISBN 0-521-43064-X.

5. ^ The GNU C library's *rand()* in stdlib.h uses a simple (single state) linear congruential generator only in case that the state is declared as 8 bytes. If the state is larger (an array), the generator becomes an additive feedback generator and the period increases. See the simplified code (http://www.mscs.dal.ca/~selinger/random/) that reproduces the random sequence from this library.
6. ^ "A collection of selected pseudorandom number generators with linear structures, K. Entacher, 1997" (http://citeseer.ist.psu.edu/viewdoc/download?doi=10.1.1.53.3686&rep=rep1&type=pdf). Retrieved 16 June 2012.
7. ^ "How Visual Basic Generates Pseudo-Random Numbers for the RND Function" (http://support.microsoft.com/kb/231847). *Microsoft Support*. Microsoft. Retrieved 17 June 2011.
8. ^ In spite of documentation on MSDN (http://msdn.microsoft.com/en-us/library/bb432429(VS.85).aspx), RtlUniform uses LCG, and not Lehmer's algorithm, implementations before Windows Vista are flawed, because the result of multiplication is cut to 32 bits, before modulo is applied
9. ^ ***a*** ***b*** "ISO/IEC 14882:2011" (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50372). ISO. 2 September 2011. Retrieved 3 September 2011.
10. ^ GNU Scientific Library: Other random number generators (http://www.gnu.org/software/gsl/manual/html_node/Other-random-number-generators.html)
11. ^ Matsumoto, Makoto, and Takuji Nishimura (1998) ACM Transactions on Modeling and Computer Simulation 8
12. ^ ***a*** ***b*** RFC 4086 section 6.1.3 "Traditional Pseudo-random Sequences"

References

- S.K. Park and K.W. Miller (1988). "Random Number Generators: Good Ones Are Hard To Find" (http://portal.acm.org/citation.cfm?id=63042). *Communications of the ACM* **31** (10): 1192–1201. doi:10.1145/63039.63042 (http://dx.doi.org/10.1145%2F63039.63042).
- D. E. Knuth. *The Art of Computer Programming*, Volume 2: *Seminumerical Algorithms*, Third Edition. Addison-Wesley, 1997. ISBN 0-201-89684-2. Section 3.2.1: The Linear Congruential Method, pp. 10–26.
- P. L'Ecuyer (1999). "Tables of Linear Congruential Generators of Different Sizes and Good Lattice Structure" (http://citeseer.ist.psu.edu/132363.html). *Mathematics of Computation* **68** (225): 249–260. doi:10.1090/S0025-5718-99-00996-5 (http://dx.doi.org/10.1090%2FS0025-5718-99-00996-5).
- Press, WH; Teukolsky, SA; Vetterling, WT; Flannery, BP (2007), "Section 7.1.1. Some History" (http://apps.nrbook.com/empanel/index.html#pg=343), *Numerical Recipes:*

The Art of Scientific Computing (3rd ed.), New York: Cambridge University Press, ISBN 978-0-521-88068-8
- Gentle, James E., (2003). *Random Number Generation and Monte Carlo Methods*, 2nd edition, Springer, ISBN 0-387-00178-6.
- Joan Boyar (1989). "Inferring sequences produced by pseudo-random number generators" (http://portal.acm.org/citation.cfm?id=59305&dl=ACM&coll=portal). *Journal of the ACM* **36** (1): 129–141. doi:10.1145/58562.59305 (http://dx.doi.org/10.1145%2F58562.59305). (in this paper, efficient algorithms are given for inferring sequences produced by certain pseudo-random number generators).

External links

- The simulation Linear Congruential Generator (http://www.vias.org/simulations/simusoft_lincong.html) visualizes the correlations between the pseudo-random numbers when manipulating the parameters.
- Security of Random Number Generation: An Annotated Bibliography (http://www.cs.virginia.edu/~rjg7v/annotated.html)
- Linear Congruential Generators post to sci.math (http://www.math.niu.edu/~rusin/known-math/99/LCG)
- The "Death of Art" computer art project at Goldstein Technologies LLC, uses an LCG to generate 33,554,432 images (http://www.goldsteintech.com/art.php)
- P. L'Ecuyer and R. Simard, "TestU01: A C Library for Empirical Testing of Random Number Generators" (http://www.iro.umontreal.ca/~lecuyer/myftp/papers/testu01.pdf), May 2006, revised November 2006, *ACM Transactions on Mathematical Software*, 33, 4, Article 22, August 2007.