How Bad are Irrational Rotations for Generating Pseudo-Random Numbers?

Monte Carlo simulation involves the estimation of probabilities or means based on the corresponding statistics of randomly generated scenarios. Rather than generating truly random numbers, most computer systems use pseudo-random numbers, which appear random but in fact come from a formula.

The randomness of a random number generator can be assessed by statistical tests, from numerical verification of theoretical results (such as Khintchine's iterated logarithm law) or tests such as Marsaglia's 'diehard' suite designed specifically to detect known flaws in simple generators. A good random number generator, such as the Mersenne Twister algorithm, triggers a large number of Type II errors, that is, the null hypothesis of randomness is not rejected even though it is a false.

One of the simplest random number generators, known as irrational rotation, involves taking an irrational number, such as a = sqrt(2), then defining the nth random number as the fractional part of an. That generator fails many of the standard tests, but has the advantage of simplicity and ease of implementation and therefore can be useful in teaching and for research where reproducibility of results is of importance. Hardy and Littlewood proved results on the sums of irrational rotations. The equi-distribution of irrational rotations is an immediate consequence of Weyl's criterion.

This project is to investigate the behaviour of pseudo-random walks, whose increments are generated from a desired distribution from irrational rotations using the inverse CDF transform method. Numerical experiments suggest that the extreme points of such walks occur at time points related to solutions of Pell's equation, and that the growth of the extrema is slower than suggested by the iterated logarithm law. The purpose of the project is to develop hypotheses based on numerical investigations and then to prove them using methods from number theory and/or Fourier analysis.

References

Paul Glasserman (2003) Monte Carlo Methods in Financial Engineering. Springer.

Hardy, Godfrey H., and John E. Littlewood (1922). Some problems of Diophantine approximation: The lattice-points of a right-angled triangle. Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg. Vol. 1. No. 1.

Matsumoto, M.; Nishimura, T. (1998). Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. ACM Transactions on Modeling and Computer Simulation. 8 (1): 3–30. CiteSeerX 10.1.1.215.1141. doi:10.1145/272991.272995. S2CID 3332028.

Marsaglia (1995) The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness". Florida State University. 1995.

Weyl, H. (1916) Über die Gleichverteilung von Zahlen mod. Eins. Math. Ann. 77, 313-352, 1916. Reprinted in Gesammelte Abhandlungen, Band I. Berlin: Springer-Verlag, pp. 563-599, 1968. Also reprinted in Selecta Hermann Weyl. Basel, Switzerland: Birkhäuser, pp. 111-147, 1956.