Quality pseudo-random number generator

Jerzy Tarasiuk

A pseudo-random number generator was written to match needs of nuclear and high-energy physics computations which in some cases require very long and independent random number sequences to be obtained by many people who work simultaneously using computers. Its period about 10^36 should be sufficient for all computers in the world.

The generator is a computer procedure producing numbers looking like random, capable to repeat entire sequence when desired, but also with ability to warrant no repeats (of the sequence, of course, individual numbers repeat many times). I was able to write the generator due to few articles I was informed about by Jouke R. Heringa via e-mail. (Thanks, Jouke!). Its source code is available by anonymous FTP or e-mail.

Basic properties of the generator :

- period (2^89-1)*(2^31-1) - about 10^36.
- result is integer number of required number of bits. For every bit position used in result, in entire period counts of zeros and ones differ by one (period length is odd number).
- small correlations, expected about 2^-31; no typical for many generators correlations like "sum of low order bits of numbers N, N+38 and N+89 is always even" - I looked at several public domain generators and I found almost all relatively good ones available in source have this kind of correlations. Instead, a probability the sum is odd is 2^30/(2^31-1), not 1/2.
- initialization can specify any starting position in the entire period, and fast algorithm is built in initialization to compute the generator state for any position without the skipping a number of results used in other generators like V113 in CERNLIB, unacceptable for starting position like 2^60=10^18 - it would take years. This generator starts in a fraction of second.
- its construction warrants sequences obtained for different starting positions to be different, due to the method using one sequence; no typical for multi-sequence generators danger of a possibility to get the same numbers when specify different sequences and different starting positions - their algorithm warrants it must occur at least for the least significant bit and it isn't known at what position difference it occurs.
- identical results on PC, Sun4 and VAX machines (tested).
- standard C and standard Fortran versions.

One can have many independent copies of the generator in a single program (need allocate space for data used by each copy; 512 bytes of data on 32-bit machines).

Full text of the article and source code of the generator are available by: anonymous FTP at zfja-gate.fuw.edu.pl (you need command "cd rand" after login) or e-mail containing line "GET RAND/JT-RAND.ZIP" to listserv@zfja-gate.fuw.edu.pl.

References

[1]. Jouke R. Heringa, H.W.J. Bloete and A. Compagner, International Journal of Modern Physics C3,561 (1992).

[2]. M. Zivkovic, Mathematics of Computation 62,385 (1994).