

- [1] J. M. Charnes. Statistical analysis of output processes. In *Proceedings of the 25th Winter Simulation Conference*, pages 41-49. ACM Press, December 1993. [[bib](#) | [DOI](#) ]
- [2] D. Goldsman. Simulation output analysis. In *Proceedings of the 24th Winter Simulation Conference*, pages 97-103. ACM Press, December 1992. [[bib](#) | [DOI](#) ]
- [3] M. Matsumoto and T. Nishimura. Mersenne Twister: A 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Trans. Model. Comput. Simul.*, 8(1):3-30, 1998. [[bib](#) | [DOI](#) ]

A new algorithm called Mersenne Twister (MT) is proposed for generating uniform pseudorandom numbers. For a particular choice of parameters, the algorithm provides a super astronomical period of  $2^{19937} - 1$  and 623-dimensional equidistribution up to 32-bit accuracy, while using a working area of only 624 words. This is a new variant of the previously proposed generators, TGFSR, modified so as to admit a Mersenne-prime period. The characteristic polynomial has many terms. The distribution up to  $v$  bits accuracy for  $1 \leq v \leq 32$  is also shown to be good. An algorithm is also given that checks the primitivity of the characteristic polynomial of MT with computational complexity  $O(p^2)$  where  $p$  is the degree of the polynomial. We implemented this generator in portable C-code. It passed several stringent statistical tests, including diehard. Its speed is comparable to other modern generators. Its merits are due to the efficient algorithms that are unique to polynomial calculations over the two-element field.