FAST NORMAL RANDOM NUMBER GENERATORS FOR VECTOR PROCESSORS

RICHARD P. BRENT

Abstract

We consider pseudo-random number generators suitable for vector processors. In particular, we describe vectorised implementations of the Box-Muller and Polar methods, and show that they give good performance on the Fujitsu VP2200. We also consider some other popular methods, e.g. the Ratio method [4, 5] and the method of Von Neumann and Forsythe [1], and show why they are unlikely to be competitive with the Polar method on vector processors.

Comments

Only the Abstract is given here. The full report appeared as [3]. For related work on uniformly distributed random numbers, see [2].

References

1. R. P. Brent, "Algorithm 488: A Gaussian pseudo-random number generator (G5)", *Communications of the ACM* 17 (1974), 704–706. Zbl 292.65003. rpb023.
2. R. P. Brent, "Uniform random number generators for supercomputers" *Proc. Fifth Australian Supercomputer Conference*, Melbourne, December 1992, 95–104. rpb132.
3. R. P. Brent, *Fast Normal Random Number Generators for Vector Processors*, Technical Report TR-CS-93-04, Computer Sciences Laboratory, Australian National University, March 1993, 7 pp. rpb141.
4. A. J. Kinderman and J. F. Monahan, "Computer generation of random variables using the ratio of uniform deviates", *ACM Transactions on Mathematical Software* 3 (1977), 257–260.
5. J. L. Leva, "A fast normal random number generator", *ACM Transactions on Mathematical Software* 18 (1992), 449–453.

Computer Sciences Laboratory, Australian National University, Canberra, ACT 0200
E-mail address: rpb@cslab.anu.edu.au

1991 *Mathematics Subject Classification.* Primary 65C10; Secondary 65D20, 65Y05, 65Y10.
Key words and phrases. Random numbers, vector processor, normal distribution, Gaussian distribution, parallel computation, Box-Muller method, polar method, ratio method, Von Neumann and Forsythe method, pipelining, rational approximation, logarithm, square root.

rpb141a typeset using $\mathcal{AMS}$-LaTeX