Technical Report: Dynamic Creator of 64-bit Mersenne Twister

Mutsuo Saito Makoto Matsumoto

2019-8-3

Abstract

On this report, we describe a dynamic creation program for 64-bit Mersenne Twister.

Improvement

Dynamic Creation of Pserudorandom Number Generators (DC) [2] was proposed by Matsumoto and Nishimura and a program for 32-bit Mersenne Twister (MT) [1] written in C is published on web page `http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/DC/dc.html` and Git Hub `https://github.com/MersenneTwister-Lab/dcmt`. 64-bit Mersenne Twister (MT64) [3] was proposed by Nishimura, but dynamic creation program for MT64 has not been supported.

There was a difficulty in calculating tempering parameter of MT64. Two tempering parameter sizes of MT are 25 and 17 bits, on the other hand, those of MT64 are 47 and 27 bits. Increased sizes of tempering parameters made dynamic creation very slow and impractical. To solve this difficulty, now, we adopt "Partial Bit Pattern" algorithm, which is the algorithm used in Mersenne Twister of Graphic Processors (MTGP) [4]. The algorithm separates tempering parameters some bit blocks and selects a bit pattern which gives the best $k(v)$ in the blocks. (Note: we talk about the algorithm of searching tempering paramaeters. The tempering algorithm itself of MT64 is not changed.)

Results of the Dynamic Creation

We made C++ program dcmt64(`https://github.com/MersenneTwister-Lab/dcmt64`). We executed the program on Super Computer of The Institute of Statistical Mathematics(ISM) in Japan.

Execution Environment:

CPU	Intel Xeon Gold 6154 (18 core, 3.0GHz)
Memory	384GB
OS	Red Hat Linux Enterprise Server 7
Compiler	g++

Execution Results:

used time	10h	used process	36
specified mexp	19937	parameters found	1161

Dimension defect(DD)[1, §1.2] is a simple evaluation index of $F2$-linear random number generators. The less DD is the better. The minimum DD of found parameters is 5023 and the maximum one is 25258. 95 percent parameters have DD less than 7000.

References

[1] M. Matsumoto and T. Nishimura. Mersenne twister: A 623-dimensionally equidistributed uniform pseudorandom number generator. *ACM Trans. on Modeling and Computer Simulation*, 8(1):3–30, January 1998. `http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/emt.html`.

[2] M. Matsumoto and T. Nishimura. Dynamic creation of pseudorandom number generator. In *Monte Carlo and Quasi-Monte Carlo Methods 1998*, pages 56–69. Springer-Verlag, 2000. `http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/DC/dc.html`.

[3] T. Nishimura. Tables of 64-bit mersenne twisters. *ACM Trans. on Modeling and Computer Simulation*, 10(4):348–357, October 2000.

[4] Mutsuo Saito and Makoto Matsumoto. Variants of mersenne twister suitable for graphic processors. *ACM Transactions on Modeling and Computer Simulation*, 39, February 2013. `doi:10.1145/1570256.1570353`.