Generalized Mersenne Prime Number and Its Application to Random Number Generation

Lih-Yuan Deng
Department of Mathematical Sciences, The University of Memphis
LIHDENG@MEMPHIS.EDU

Abstract

A Mersenne prime number is a prime number of the form $2^k - 1$. In this talk, we consider a Generalized Mersenne Prime (GMP) which is of the form $R(k, p) = (p^k - 1)/(p - 1)$, where k, p and $R(k, p)$ are prime numbers. For such a GMP, we then propose a much more efficient search algorithm for a special form of Multiple Recursive Generator (MRG) with the property of an extremely large period length and a high dimension of equidistribution. In particular, we find that $(p^k - 1)/(p - 1)$ is a GMP, for a very large k and p. We then find a special form of MRG with order k and its period length breaking the current world record set by MT19937. Many other efficient and portable generators with various k are found and listed. Finally, for such a GMP and generator, we propose a simple and quick method of generating maximum period MRGs with the same order k. We will discuss its application to parallel random number generation.