Parallel Pseudorandom Number Generation

Suming Fang

August 30, 1997

On the Wednesday, August 27, 1997 Dr. Michael Mascagni, who is professor in the School of Mathematical Sciences of University of Southern Mississippi, gave us talk of "Recent Developments in Parallel Pseudorandom Number Generation".

Dr. Michael Mascagni is a researcher in vast area of parallel computing. First, he said, ensuring that pseudorandom number generators have good randomness properties is more complicated in a multiprocessor implementation than in the uniprocessor case. We discuss simple extensions of uniprocessor testing for SIMD parallel streams, and develop in detail a repeatability test for the SPMD paradigm. Also, examples of the application of these tests to an additive lagged-Fibonacci generator are given.

He said that three Single Processor Properties must be hold by parallel pseudorandom number generation (PRNGs). We start by defining properties of PRNGs in the most constrained case of parallel processing, which is the uniprocessor case, then relax the constraints successively to yield the SIMD, SPMD and MIMD paradigms, and at each level define the characteristics to be tested.

These are three basic properties that any PRNG should satisfy. The first of these is of course “randomness”: the stream of numbers produced should be similar to a truly random stream.

The second property is repeatability: the same sequence of pseudorandom numbers is returned when the initializing inputs to the generator are the same. It would be difficult to unknowingly design a generator without this property on a single processor, and testing is trivial.

The third property is portability: given the same initial conditions the stream should be the same on a variety of platforms. Portability is easily tested by running the generator on different machines and comparing the results.