

QUASI- VERSUS PSEUDO-RANDOM GENERATORS: DISCREPANCY, COMPLEXITY AND INTEGRATION-ERROR BASED COMPARISON

SYAMAL KUMAR SEN, TATHAGATA SAMANTA AND ANDREA REESE

Department of Mathematical Sciences
Florida Institute of Technology
Melbourne, FL, 32901, USA
{sksen, tsamanta, areese}@fit.edu

Received May 2005; revised July 2005

ABSTRACT. *Presented here are several quasi- and pseudo-random number generators along with their numerical discrepancy, i.e., nonuniformity measure and computational/time complexity. These generators have been compared and ranked based on discrepancy, complexity, and error in multiple Monte Carlo integrations. We believe that such a statistical comparison/ranking will be useful for solving real world problems where one needs to scan an s -dimensional region for an optimal solution of a mathematical program or multiple integrations.*

Keywords: Complexity, Error, Low discrepancy sequence, Monte Carlo integration, Pseudo-random number, Quasi-random number

1. Introduction. *Non-existence of true random numbers in nature and artifact.* The dictionary meaning of the word “random” is “made or done by chance without plan”. By this meaning it implies that no one will be able to predict the outcome out of several possible outcomes of any process. In nature, the outcome of any process cannot be strictly random since there is a relationship between the outcome and the inputs of the process through the process which obeys all the laws of nature perfectly and exactly. This observance of all the concerned laws of nature by any activity/process/method/algorithm is a hypothesis which has never been disproved. There is no question of breaking any law of the material universe under any circumstances at any time. Of course due to our limitations such as the lack of complete and/or perfect knowledge of the system and of all the laws governing the system, we, the human beings, are not able to explain or predict many phenomena/outcomes. If there is no process, then there is no outcome and hence no random numbers (RNs). Similarly, artificially too, we are not able to generate true RNs. Thus *RN generation does exist neither in nature nor in digital computers (artifacts). Nature never produces any situation associated with a number that is random nor does it ever create chaos*¹. What we produce/generate in computers are thus called pseudo- (implying false) RNs (PRNs) and/or quasi- (implying sub-) RNs (QRNs).

Why quasi- over pseudo-random sequence. In many evolutionary approaches we need the explicit construction of point sets which fills out the s -dimensional (s -D) unit cube

¹The dictionary meaning of the word “chaos” is complete disorder or confusion. Chaos in science and engineering refers to an apparent lack of order in a system that nevertheless obeys certain laws and rules. This understanding of chaos is the same as that of dynamical instability.