Preface

The Monte Carlo method is a numerical method to solve mathematical problems by computer-aided sampling of random variables. It has started when von Neumann, Ulam and others applied it to the simulation of nuclear fissions[†1] by newly invented computers in 1940's, i.e., in the midst of World War II ([16]). Since then, along with the development of computer, the Monte Carlo method has been used in all fields of science and technology, and has produced remarkable results. The development of the Monte Carlo method will surely continue.

In this monograph, however, we do not deal with such brilliant applications of the method, but we mainly discuss its mathematical foundation, in particular, the justifiability of computer-aided sampling methods. That is, there is a fundamental difficulty that computers cannot generate random numbers, so that we use pseudorandom numbers instead of them in Monte Carlo methods. Here, a number of researchers have had a serious suspicion;

> *Monte Carlo methods using pseudorandom numbers can never have any mathematical justification.*

As a matter of fact, this suspicion is merely a misunderstanding due to the prejudice caused by intuitive interpretations of the Monte Carlo method, random number and pseudorandom number.[†2] Namely, learning the notions of random number and pseudorandom number correctly, and formulating the Monte Carlo method properly, we see that there is the possibility to remove this suspicion, and in fact, that we can actually remove it in many cases. In this monograph, we give detailed explanations about this. At the same time, the reader will find that such a proper mathematical formulation of the Monte Carlo method leads to the development of the most reliable computer-aided sampling methods.

How to execute sampling of random variables by computer has been an important issue since the Monte Carlo method came into the world. In 1960's, Kolmogorov and others defined the notion of random number by using a function which is called "the Kolmogorov complexity" today ([5, 18, 19, 20, 26]). It was an epoch-making work that was done by making free use of the theory of computation, which theory was initiated in 1930's. About 20 years after their works, in 1980's, Blum and others defined the notion of pseudorandom number in the context of cryptography ([2, 3, 49]). It was based on the

[†1] In order to make atomic bombs.

[†2] Many references about the Monte Carlo method do not distinguish random number and pseudorandom number. For instance, although the chapter title of [17] is "Random numbers", it actually deals with pseudorandom number. In this monograph, they are strictly distinguished.

theory of computational complexity, which discusses realistic possibility of computation. But unfortunately, researchers of the Monte Carlo method have not paid attention to those notions of random number and pseudorandom number. This is because the former is hard to understand and does not provide any practical solution, and the latter has been thought to be useful only in cryptography but useless in the Monte Carlo method.

This is nothing but a misunderstanding; they have not been able to evaluate those notions of random number and pseudorandom number properly, because their way of thinking about the Monte Carlo method has been too vague. In this monograph, we introduce a definite formulation of the Monte Carlo method which is based on and compatible with those notions of random number and pseudorandom number. As a result, we see that

> *Monte Carlo methods using pseudorandom numbers may have mathematical justification. As a matter of fact, for the purpose of the Monte Carlo integration,*[†3] *there exist pseudorandom numbers which can serve as complete substitutes for random numbers.*

Let us take a general view of this monograph.

In Chapter 1, the fair coin tossing process is introduced as the model process of random number and pseudorandom number. In the first half of the chapter, it is observed that an arbitrary random variable — or more generally, an arbitrary sequence of independent random variables — can be theoretically constructed from the fair coin tossing process. The second half of the chapter deals with *simulatable* random variables, i.e., those which can be constructed in practice from the fair coin tossing process by computer programs.

In Chapter 2, a proper mathematical formulation of the Monte Carlo method as well as rough definitions of random number and pseudorandom number is introduced. The aim of the Monte Carlo method and how it ought to be are prescribed, and random number and pseudorandom number are definitely placed in the formulation. The reader should read this chapter very carefully, because the way of looking at things in this monograph is quite different from the current explanations of the Monte Carlo method (cf. [16, 17, 34]). Chapter 2 is the backbone of the whole monograph, and hence it would be sufficiently profitable for the reader to understand this single chapter.

In Chapter 3, partial recursive function, a fundamental notion in the theory of computation, is first introduced with its basic properties (cf. [6, 32]). Then the Kolmogorov complexity being introduced, the notion of random number is defined (cf. [5, 18, 19, 20, 21, 23, 26, 54]). Although the Kolmogorov complexity can be defined for all finite $\{0,1\}$-sequences, it is not computable. It is made clear that this fact is closely related to an important result "the uncomputability of halting problem" in the theory of computation. The second half of Chapter 3, Martin-Löf's theorem ([26]) is proved. This theorem explains the relation between random numbers and statistical tests for randomness. It is often said that Kolmogorov's probability theory avoids asking the most basic question "What is randomness?" But as we see here, he did give an excellent answer to this difficult question. In the last section § 3.6, it is observed that realizing the notion of random number brings a deep understanding of not only the Monte Carlo method but also probability theory itself.

[†3] A numerical integration method making use of the law of large numbers.

In the first half § 4.1 of Chapter 4 deals with basic items of computationally secure pseudorandom generator (cf. [24, 36]). In particular, it is made clear that the computational security is also a desirable property for pseudorandom generator in the Monte Carlo method. It is observed that this property is closely related to the **P** ≠ **NP** conjecture, which clearly shows the essential difficulty of pseudorandom generation. In the second half § 4.2 of the chapter, a pseudorandom generator ([37]) discovered by the author is introduced. It approaches to computationally secure pseudorandom generation from probability theory. In § 4.3, full proofs of the theorems exhibited in § 4.2 are given.

Chapter 5 deals with the random Weyl sampling (abbreviated as RWS, [38, 44]) in detail, which plays a role of secure pseudorandom generator in the Monte Carlo integration. In particular, it is shown that the central limit theorem scaling of the sample mean of RWS converges to 0 in probability as the sample size tends to infinity. This means that with high probability, RWS has less error than i.i.d.-sampling, and hence it is more advantageous in the Monte Carlo integration (cf. [40]). In § 5.4, the dynamic random Weyl sampling (abbreviated as DRWS, [39]) is introduced as an extension of RWS for the numerical integration of any simulatable random variables. A numerical example proves DRWS to be the most reliable sampling method for the Monte Carlo integration.

Chapter 6 deals with the implementations by C language of the pseudorandom generator introduced in § 4.2, RWS in § 2.5.2 and DRWS in § 5.4 (cf. [43]). The C language library in § 6.2 can be used for all purposes of the Monte Carlo method.

This monograph includes almost all materials which the author thinks important. But the research is going on. Some important open problems are mentioned here and there. Although they are not easy at all, any challenges to them are welcome.

—— ◇ —— ◇ ——

This monograph originates in a private note of my lectures given at Kobe University, May 2000. At that time, K.Fukuyama recommended me to write a complete lecture note to be published by Department of Mathematics, Kobe University. Although given a lot of advice by him, I could not write a manuscript that satisfied myself. I regret that I put him to a great deal of trouble. But thanks to this experience, I could study the Monte Carlo method so intensively, and my understanding of it became much deeper. As a result, I could write a monograph that satisfies myself this time. I would like to apologize to Fukuyama and to thank him so much. I used old versions of this monograph for lectures and seminars in Department of Mathematics, Osaka University. Each time a student found a mistake in an old version, I revised it. I am grateful to my diligent students. I am also grateful to Professors M.Yor, H.Niederreiter, K.Handa, A.Fujiwara, and the anonymous reviewer for giving me valuable advice. Finally, I must say that some of important contents of this monograph could not have been obtained without S.Takanobu's strong collaboration.

April 2011.

Hiroshi SUGITA