Closing remarks

Looking back over the stream of mathematical formulations of randomness, we notice two guiding principles.

One is "*Grasp randomness only quantitatively*". People often discuss randomness philosophically. But since it is impossible to discuss the meaning of randomness in the completely formal mathematical logic, this guiding principle is a natural idea. It was proposed by Shannon in his information theory, and it led Kolmogorov complexity and the notion of computational security of pseudorandom generator.

The other one is "*Describe situations involving randomness — so paradoxically — in* deterministic *ways*". The axioms of probability theory, the notion of randomness, and the notion of pseudorandom generator were all led by this guiding principle. Therefore we may well say that our deterministic formulation of the Monte Carlo method, i.e., the idea that sampling of random variables should be done by the player's will, is quite natural (§ 2.2).[†1] In game theory as well as in cryptography, sampling of random variables is usually done by executors' will. Namely, in game theory, the choice of strategy is done by players' will, and in cryptography, the choice of password is done by users' will. But this is a new idea in the Monte Carlo method. As we mentioned in the text of this monograph, by this idea, the formulation of the Monte Carlo method can have compatibility with the notion of random number and that of pseudorandom generator, and as a result, the essential problem of sampling was made clear, which has been solved in the case of the Monte Carlo integration.

More than ten years ago, I happened to know references of pseudorandom generator used in cryptography via the internet. I was so surprised to know that the aim of pseudorandom generator is not to make randomness. However, it is only one of the many excellent ideas in computer science. Today, almost all important problems in computer science involve probability. Problems that can be solved by deterministic methods have all been solved. One of the main streams in computer science is the application of random sampling to difficult problems for which deterministic methods get nowhere. In this context, the Monte Carlo method is surely a subject of computer science.

Of course, probability theory is used very often in computer science. In particular, many algebraic or combinatorial facts are applied with probabilistic interpretations. But, for numerical calculus, algebraic methods do not always work so well. Indeed, the pseudorandom generator $\tilde{g}$ introduced in § 5.2.3 is not useful in practice, because the multiplication of $\mathrm{GF}(2^m)$ is too complicated. RWS, an analogy of $\tilde{g}$ obtained by discretizing

[†1] The private note of my lectures given at Kobe university (2000) mentioned in Preface did not include this idea. I think that I myself was not satisfied unconsciously with the lack of this idea. A sprout of this idea is seen in [42], which is fully developed in this monograph.

an analytic theorem (Theorem 5.5), is much more useful in practice. In general, algebraic devices give mathematically simple, beautiful and optimal solutions, but they lack continuity, i.e., they would be useless if a parameter changes even slightly. On the other hand, in analysis, since we do not pay attention to individuality of each number, such as being prime, we may fail in getting optimal solutions. Instead, we look at continuously changing phenomena in accordance with moving parameters. I expect that there are many problems in computer science for which analytic, in particular, probabilistic methods are useful.

Throughout this monograph, it is Weyl transformation that technically realizes the various ideas. Indeed, RWS, the pseudorandom generator introduced in § 4.2, and DRWS are all applications of it. Weyl transformation is random in the sense that it is ergodic, but it is almost deterministic in the sense that it is of entropy 0. This duality makes it possible to generate long diverse pseudorandom numbers from short seeds. I am thankful that such a simple dynamical system has very nice properties for the Monte Carlo method.