Contents

Preface **vi**

Interdependence of Chapters and Sections xiii

Notations and symbols xiv

1 Coin tossing process **1**

1.1 Borel's model of coin tossing process 1

1.2 Construction of random variables from coin tossing process 2

1.3 Simulatable random variable 4

1.3.1 Stopping time and simulatable random variable 4

1.3.2 $\mathbb{T}^1$-valued uniform i.i.d. sequence as random source 6

2 Mathematical formulation of Monte Carlo method **9**

2.1 Overview 9

2.2 Monte Carlo method as gambling 11

2.2.1 Player's aim 11

2.2.2 An exercise 12

2.3 Problem of random number 13

2.4 Pseudorandom generator 14

2.4.1 Definition and role 14

2.4.2 Security 14

2.4.3 Computationally secure pseudorandom generator 15

2.5 Monte Carlo integration 16

2.5.1 i.i.d.-sampling 16

2.5.2 Random Weyl sampling 17

2.6 From viewpoint of mathematical statistics 20

2.6.1 Random sampling 20

2.6.2 Test for pseudorandom generator 20

3 Random number **23**

3.1 Partial recursive function 23

3.1.1 Primitive recursive function and partial recursive function 24

3.1.2 Kleene's normal form 25

3.1.3 Canonical order 26

3.1.4 Enumeration theorem and halting problem 27

3.2 Kolmogorov complexity and random number 30

3.3 Test and Martin-Löf's theorem 33

3.3.1 Formulation of test and universal test 34
3.3.2 Martin-Löf's theorem 36
3.4 Kolmogorov complexity and entropy 37
3.5 Infinite random sequence 39
3.6 Random number and probability theory 40

4 Pseudorandom generator 43

4.1 Computationally secure pseudorandom generator 43
4.1.1 Definitions 43
4.1.2 Computational security and Monte Carlo method 44
4.1.3 Existence problem 45
4.1.4 Next-bit-unpredictability 46
4.2 Pseudorandom generator by means of Weyl transformation 49
4.2.1 Definitions 49
4.2.2 Hardness of next-bit-prediction 50
4.2.3 Formula of finite dimensional distributions and disappearance of dependence 52
4.2.4 A priori estimate of finite dimensional distributions 54
4.3 Proofs of theorems 57
4.3.1 Proof of Lemma 4.12 57
4.3.2 Proof of Theorem 4.13 59
4.3.3 Proof of Theorem 4.15 65
4.3.4 Proof of Theorem 4.11 72
4.3.5 Precise estimate of exponential decay of two-term correlation . . 80

5 Monte Carlo integration 85

5.1 L^2-robustness 85
5.2 Random Weyl sampling (Part 2) 88
5.2.1 Degeneration of CLT-scaling limit 88
5.2.2 RWS in case $m \gg 1$ 91
5.2.3 Another example of pairwise independent random variables . . . 95
5.3 i.i.d.-sampling for simulatable random variables 96
5.4 Dynamic random Weyl sampling 98
5.4.1 Definition and Theorem 98
5.4.2 Proof of Theorem 5.13 99
5.4.3 Algorithm 101
5.4.4 Comparison between i.i.d.-sampling and DRWS 102
5.4.5 Limit theorem for convergence of DRWS 103

6 Implementation 113

6.1 Implementation of RWS 113
6.1.1 Implementation of Example 2.9 113
6.1.2 Implementation of Example 5.9 114
6.2 C language library : *random_sampler* 115
6.2.1 Source code 116
6.2.2 Specification of constant and function 120

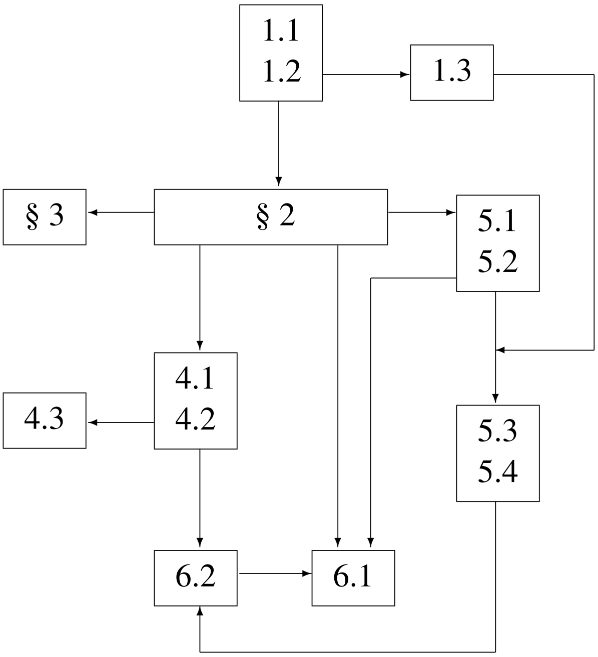
6.2.3 Sample codes 122
6.2.4 Restrictions of use 124

Closing remarks **125**

Bibliography **127**

Index **131**

Interdependence of Chapters and Sections


1.1
1.2
1.3
§ 3
§ 2
5.1
5.2
4.1
4.2
4.3
5.3
5.4
6.2
6.1