
CONTENTS

| | |
|--|----|
| SERIES FOREWORD | ix |
| PREFACE | xi |
| 1 INTRODUCTION | 1 |
| 2 PRELIMINARIES FROM NUMBER THEORY | 7 |
| 2.1 Modular Arithmetic | 7 |
| 2.1.1 Integer Arithmetic | 8 |
| 2.1.2 Polynomial Arithmetic | 14 |
| 2.2 Geometry of Numbers | 24 |
| 2.2.1 Lattice | 24 |
| 2.2.2 Basis Reduction Algorithms | 34 |
| 2.3 Uniform Distribution of Sequences | 42 |
| 2.3.1 Weyl's Criterion | 42 |
| 2.3.2 Irregularities of Distribution | 49 |
| 3 LINEAR CONGRUENTIAL GENERATORS | 57 |
| 3.1 Lattice Structure | 61 |
| 3.2 Spectral Test | 65 |
| 3.3 Implementing Long-Period LCGs | 71 |
| 3.3.1 LCGs with Large Prime Moduli | 71 |
| 3.3.2 LCGs with Large Composite Moduli | 79 |
| 4 BEYOND LINEAR CONGRUENTIAL GENERATORS | 83 |

| | | |
|----------|---|------------|
| 4.1 | LCGs Using Polynomial Arithmetic | 83 |
| 4.1.1 | Lattice Structure of $LS(2)$ Sequences | 90 |
| 4.1.2 | Combined $LS(2)$ Sequences | 98 |
| 4.1.3 | Resolution-wise Lattice Structure | 110 |
| 4.1.4 | Further Analysis via Dyadic Boxes | 120 |
| 4.2 | LCGs Using Multiplicative Inversion | 129 |
| 4.2.1 | Generators Modulo 2^w | 129 |
| 4.2.2 | Generators Modulo a Prime | 131 |
| 4.3 | Random Sequences in Cryptography | 135 |
| 4.3.1 | Cryptographically Secure Sequences | 135 |
| 4.3.2 | Linear Complexity Profile | 138 |
| 5 | STATISTICAL TESTS | 143 |
| 5.1 | Description of Test Procedures | 144 |
| 5.1.1 | Tests for Goodness of Fit | 145 |
| 5.1.2 | Specific Tests | 146 |
| 5.1.3 | Multi-Level Tests | 151 |
| 5.2 | Tests Using Non-Uniform Random Variate Generation | 152 |
| 5.2.1 | Box-Muller Method and Neave Effect | 152 |
| 5.2.2 | Box-Muller Method with $LS(2)$ -Sequences | 156 |
| 6 | DERANDOMIZATION | 161 |
| 6.1 | Low-Discrepancy Sequences | 161 |
| 6.1.1 | (t, k) -Sequences and (t, m, k) -Nets | 162 |
| 6.1.2 | Generalized Niederreiter Sequences | 164 |
| 6.1.3 | Discrepancy and Numerical Integration | 180 |
| 6.1.4 | Dispersion and Global Optimization | 182 |
| 6.2 | K -wise Independent Random Variables | 186 |
| 6.2.1 | Definitions and Construction Methods | 186 |
| 6.2.2 | Almost K -wise Independence | 188 |
| A | SAMPLE C ROUTINES | 193 |
| | REFERENCES | 197 |
| | INDEX | 207 |