

# Index

## Symbols

|  |     |   |     |
|--|-----|---|-----|
| #                                      | xiv | $E^{(m)}(k_0, \dots, k_{l-1}; \alpha)$      | 58  |
| $(u)_i$                                | 27  | <b>E</b>                                    | xiv |
| $:=$                                   | xiv | $\exists$                                   | xiv |
| $\ll, \gg$                             | 9   | $F^{(m)}(k_0, \dots, k_{l-1}; \alpha)$      | 51  |
| $\langle t \rangle$                    | 52  | $G^n(x_1, x_2, \dots, x_n)$                 | 27  |
| $\langle x_1, x_2, \dots, x_n \rangle$ | 27  | $K(y)$                                      | 31  |
| $\approx$                              | 12  | $K_A(x   y)$                                | 30  |
| $\in_U$                                | 43  | $L(p)$                                      | 30  |
| $\lceil t \rceil$                      | xiv | $\iff$                                      | xiv |
| $\lceil t \rceil_m$                    | 2   | $\implies$                                  | xiv |
| $\lfloor t \rfloor_m$                  | 2   | $m(x)$                                      | 35  |
| $\lfloor t \rfloor$                    | xiv | $m_U(x)$                                    | 34  |
| $\{0, 1\}^*$                           | 26  | mod   | xiv |
| $\emptyset$                            | xiv | $\mu_{z < t}(q(p, y, z))$                   | 33  |
| $\emptyset$                            | xiv | $\mu_y(p(x_1, \dots, x_n, y))$              | 24  |
| $\mathbf{1}_B(x)$                      | xiv | $\mathcal{N}(m, \sigma^2)$                  | xiv |
| $2^B$                                  | xiv | $\mathbb{N}^+$                              | xiv |
| $A(\alpha^{(m),s})$                    | 59  | $\mathbb{N}$                                | xiv |
| $\forall$                              | xiv | <b>NP</b>                                   | 45  |
| $\alpha_j^{(m)L}$                      | 52  | $O(f(n))$                                   | xiv |
| $\alpha_j^{(m)U}$                      | 52  | $\mathbb{P}$                                | 1   |
| $\alpha^{(m),s}$                       | 53  | $P_{(m)}$                                   | 2   |
| $B(\alpha^{(m),s})$                    | 53  | $P_m$                                       | 1   |
| $\mathcal{B}$                          | 1   | $\mathbb{P}^k$                              | 1   |
| $\mathcal{B}^m$                        | 104 | <b>P</b>                                    | 45  |
| $\mathcal{B}^r$                        | 104 | Pr  | xiv |
| $\mathcal{B}_m$                        | 2   | Pr <sub>Y</sub>                             | 43  |
| $\mathcal{B}_r$                        | 4   | $r_i(x)$                                    | 57  |
| $\beta$                                | 73  | $\mathbb{R}$                                | xiv |
| $\beta_j^{(m)}$                        | 52  | $S_{f,A}(n)$                                | 44  |
| $\square$                              | xiv | $\widetilde{S}_{f,\bar{A}}(n)$              | 46  |
| $\mathbb{C}$                           | xiv | $s_1, s_2$                                  | 53  |
| $D$                                    | 53  | $\sigma(m, j)$                              | 52  |
| $d_i$                                  | 1   | $T_f(n)$                                    | 43  |
| $\delta_{f,A}(n)$                      | 44  | $T_f(x, y, \alpha, \epsilon_1, \epsilon_2)$ | 73  |
| $\delta_{f,\bar{A}}(n)$                | 46  | $\mathbb{T}^1$                              | 1   |
| $D_m$                                  | 2   | $\mathbb{T}^k$                              | 1   |
|  |     | <b>V</b>                                    | xiv |

- $X_n^{(m)}(x; \alpha)$  ..... 57  
 $Y_n^{(m)}(x; \alpha)$  ..... 49  
 $\mathbb{Z}$  ..... xiv
- Figures**  
 Figure 2.1 ..... 10  
 Figure 3.1 ..... 25  
 Figure 3.2 ..... 26  
 Figure 4.1 ..... 66  
 Figure 4.2 ..... 67  
 Figure 5.1 ..... 92  
 Figure 5.2 ..... 93  
 Figure 5.3 ..... 93  
 Figure 5.4 ..... 104
- Tables**  
 Table 4.1 ..... 56  
 Table 5.1 ..... 91  
 Table 5.2 ..... 102  
 Table 5.3 ..... 103
- Theorems etc.**  
 Lemma 4.12' ..... 57  
 Theorem 4.13' ..... 59  
 Theorem 4.11' ..... 72
- Terms**  
 algorithm ..... 30  
 B-B-S generator ..... 48  
 canonical order ..... 26  
 Chebyshev's inequality ..... 12  
 coin tossing process ..... 1  
 complexity ..... 45  
   Kolmogorov — ..... 31  
   space — ..... 15  
   time — ..... 15, 43  
 critical sample number ..... 56, 124  
 distribution function ..... 45  
 DRWS ..... 99  
 dyadic expansion mapping ..... 2  
 empty word ..... 26  
 entropy ..... 37  
 enumerating function ..... 28  
 enumeration theorem ..... 28  
 ergodicity ..... 77, 78, 95  
 Gödel  
   — function ..... 27  
   — number ..... 28  
 gambling ..... 9, 11  
 generic value ..... 9, 11  
 halting problem ..... 29  
 i.i.d. .... 3  
   — sampling ..... 16, 96  
 Kleene's normal form ..... 25  
 Kolmogorov complexity ..... 31  
 $L^2$ -robust ..... 87  
 Lebesgue probability space ..... 1  
 mean square error ..... 99  
 Monte Carlo  
   — integration ..... 11, 16  
   — method ..... 11  
   quasi — method ..... 87  
 pairwise independent ..... 18, 20, 85, 88,  
   99, 102, 105  
**P  $\neq$  NP** conjecture ..... 45  
 polynomial  
   — parameter ..... 43  
   — time function ..... 43  
 pseudorandom generator ..... 10, 14, 44  
   B-B-S generator ..... 48  
   computationally secure — ..... 15, 44  
   cryptographically secure — ..... 15, 45  
   initialization of — ..... 14  
   next-bit-unpredictable — ..... 46  
   — secure against  $A$  ..... 10, 15  
   seed of — ..... 44  
   — by means of Weyl transformation  
     50  
 pseudorandom number ..... 14  
   seed of — ..... 10, 14, 45  
 quasi Monte Carlo method ..... 87  
 Rademacher functions ..... 57, 73, 94  
 random function ..... 43  
 random number ..... 10, 13, 31  
   random sequence ..... 39  
 recursive  
   —ly enumerable set ..... 27  
   maximal — null set ..... 39  
   partial — function ..... 23  
   primitive — function ..... 24  
   total — function ..... 25  
 rejection method ..... 6, 97, 106  
 RWS ..... 17, 88  
 sampling ..... 9  
   dynamic random Weyl — ..... 99  
   fundamental inequality about ..... 85

- i.i.d.— ..... 16, 96
- random Weyl — ..... 17, 88
- SD..... 91
- secure
  - against  $A$ ..... 10, 15
  - computationally — ..... 15, 44
  - cryptographically — ..... 15, 45
- significance level ..... 34, 40
- simulatable ..... 4
- stopping time ..... 4
  - measurable with respect to — ..... 4
- test ..... 20, 34
  - sequential — ..... 40
  - universal — ..... 34
  - universal sequential — ..... 40
- torus..... 1
- universal
  - sequential test..... 40
  - algorithm ..... 30
  - function ..... 28
  - test ..... 34
  - Turing machine ..... 28
- van der Corput sequence ..... 87
- Weyl
  - dynamic random — sampling ..... 99
  - pseudorandom generator by means of
    - transformation ..... 50
  - random — sampling..... 17, 88
  - transformation ..... 50