Bibliography

[1] P. Billingsley, *Probability and measure*, 3rd edition, John Wiley & Sons, (1995).

[2] L. Blum, M. Blum and M. Shub, A simple unpredictable pseudorandom number generator, *SIAM J. Comput.*, **15-2** (1986), 364–383.

[3] M. Blum and S. Macali, How to generate cryptographically strong sequences of pseudorandom bits, *SIAM J. on Computing*, vol. **13**, (1984) 850–864. A preliminary version appears in *Proceedings of the IEEE Foundations of Comput. Sci.* (1982), 112–117.

[4] E. Borel, Les probabilités dénombrables et leurs applications arithmétiques, *Rend. Circ. Mat. Palermo*, **27** (1909), 247–271.

[5] G.J. Chaitin, Algorithmic information theory, *IBM J. Res. Develop.*, **21** (1977), 350–359.

[6] M. Davis, *Computability and Unsolvability*, McGraw-Hill, (1958).

[7] R. Durrett, *Probability: theory and examples*, Second edition. Duxbury Press, Belmont, CA, 1996.

[8] K. Fukuyama, The central limit theorem for Rademacher system, *Proc. Japan Acad.*, **70**, Ser. A, No.7 (1994), 243–246.

[9] K. Fukuyama, Riesz-Raikov sums and Weyl transform, *Monte Carlo Methods and Applications*, VSP, **2-4** (1996), 271–293.

[10] S. Heinrich, E. Novak, and H. Pfeiffer, How many random bits do we need for Monte Carlo integration? *Monte Carlo and quasi-Monte Carlo methods 2002*, Springer, Berlin (2004), 27–49.

[11] K. Itô, K.P. McKean, Jr., *Diffusion processes and their samples paths*, Die Grundlehren der mathematischen Wissenschaftem in Einzeldarstellungen Band 125, Second Printing, Springer-Verlag, (1974).

[12] S. Janson, Some pairwise independent sequences for which the central limit theorem fails, *Stochastics* **23-4** (1988), 439–448.

[13] A. Joffe, On a sequence of almost deterministic pairwise independent random variables, *Proc. Amer. Math. Soc.* **29** (1971), 381–382.

[14] A. Joffe, On a set of almost deterministic k-independent random variables *Ann. Probability* **2-1** (1974), 161–162.

[15] M. Kac, On the distribution of values of sums of type $\sum f(2^k t)$, *Ann. Math.*, **47** (1946), 33–49.

[16] M.H. Kalos and P.A. Whitlock, *Monte Carlo methods*, Vol.I Basics. John Wiley & Sons, Inc., New York, (1986).

[17] D.E. Knuth, *The Art of Computer Programming*, 3rd ed., Volume 2, Chapter 3, *Random numbers*, Addison-Wesley, (1997).

[18] A.N. Kolmogorov, On tables of random numbers, *Sankhyā, Indian J. Statist. Ser. A* 25 (1963) 369–376.

[19] A.N. Kolmogorov, Three approaches to the definition of the concept "quantity of information". (Russian) *Problemy Peredači Informacii* 1 (1965) vyp. 1, 3–11.

[20] A.N. Kolmogorov, Logical basis for information theory and probability theory, *IEEE Trans. on Inform. Theo.*, vol.IT-**14-5**, Sept. (1968), 662–664.

[21] A.N. Kolmogorov, *Selected works of A. N. Kolmogorov. Vol. III. Information theory and the theory of algorithms*, Edited by A. N. Shiryayev [A. N. Shiryaev]. Translated from the 1987 Russian original by A. B. Sossinsky. Mathematics and its Applications (Soviet Series), 27. Kluwer Academic Publishers Group, Dordrecht, (1993) xxvi+275 pp.

[22] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Interscience, (1974).

[23] M. Li and P. Vitányi, *An introduction to Kolmogorov complexity and its applications*, 2nd ed. Graduate Texts in Computer Science. Springer-Verlag, New York, (1997).

[24] M. Luby, *Pseudorandomness and cryptographic applications*, Princeton Computer Science Notes, Princeton University Press, (1996).

[25] G. Maruyama, On an asymptotic property of a gap sequence, *Kôdai Math. Sem. Rep.* **1950** (1950), 31–32.

[26] P. Martin-Löf, The definition of random sequences, *Inform. Control*, **7** (1966), 602–619.

[27] M. Matsumoto and T. Nishimura, Mersenne twister: a 623-dimensionally equidistributed uniform pseudorandom number generator, *ACM. Trans. Model. Comput. Simul.*, **8-1**, (1998), 3–30.

[28] J. von Neumann, Various techniques used in connection with random digits, *U.S. Natl. Bur. Stand. Appl. Math. Ser.*, **12** (1951), 36–38.

[29] H. Niederreiter, Quasi-Monte Carlo methods and pseudorandom numbers, *Bull. Amer. Math. Soc.*, **84** (1978), 957–1041.

[30] K.R. Parthasarathy, *Probability measure on metric spaces*, Academic Press, (1967).

[31] H. Pfeiffer, *Monte Carlo methods with few random bits*, Dissertation zur Erlangung des akademischen Grades doctor rerum naturalium (Dr. rer. nat.), vorgelegt dem Rat der Fakultät für Mathematik und Informatik der Friedrich-Schiller-Universität Jena, 2005.

[32] J.R. Shoenfield, *Mathematical Logic*, Addison-Wesley, (1967).

[33] Ya.G. Sinai, *Probability Theory — An Introductory Course*, Springer Textbook, 1992.

[34] I.M. Sobol', *A Primer for the Monte Carlo Method*, CRC Press, (1994).

[35] H. Steinhaus, Sur la probabilité de la convergence de séries, *Studia Math.*, **2** (1930), 21–39.

[36] D.R. Stinson, *Cryptography (Theory and practice)*, CRC Press, (1995).

[37] H. Sugita, Pseudo-random number generator by means of irrational rotation, *Monte Carlo Methods and Applications*, VSP, **1-1** (1995), 35–57.

[38] H. Sugita, Robust numerical integration and pairwise independent random variables, *Jour. Comput. Appl. Math.*, **139** (2002), 1–8.

[39] H. Sugita, Dynamic random Weyl sampling for drastic reduction of randomness in Monte Carlo integration, *Math. Comput. Simulation*, **62** (2003), 529–537.

[40] H. Sugita, Numerical integration of complicated functions and random sampling (in Japanese), "Sugaku", 56-1, Iwanami-shoten (2004), 1–17.(English translation, *SUGAKU EXPOSITIONS*, 19-2, AMS, December 2006, 153–169.)

[41] H. Sugita, An analytic approach to secure pseudorandom generation, *Proceedings of 2003 Ritsumeikan Symposium on Stochastic Processes and its Applications to Mathematical Finance*, World Scientific, (2004), 355–368.

[42] H. Sugita, Security of Pseudo-random Generator and Monte Carlo Method, *Monte Carlo Methods and Appl.*, **10-3**, VSP, (2004), 609–615.

[43] H. Sugita, The Random Sampler, available at;
http://homepage.mac.com/hiroshi_sugita/mathematics.html.

[44] H. Sugita and S. Takanobu, Random Weyl sampling for robust numerical integration of complicated functions, *Monte Carlo Methods and Appl.*, **6-1**, VSP, (1999), 27–48.

[45] M. Takahashi, *Theory of computation (Computability and λ-calculus)*, Kindai-Kagaku sha, (*Japanese*)(1991).

[46] S. Takanobu, On the strong-mixing property of skew product of binary transformation on 2-dimensional torus by irrational rotation, *Tokyo J. Math.* **25-1** (2002), 1–15.

[47] S. Tezuka, *Uniform Random Numbers: Theory and Practice*, Kluwer Academic Publ., (1995).

[48] A. Turing, On Computable Numbers, With an Application to the Entscheidungsproblem, *Proceedings of the London Mathematical Society, Series 2*, Volume 42 (1936). Eprint. Reprinted in The Undecidable pp.115–154. http://www.abelard.org/turpap2/tp2-ie.asp

[49] A. Yao, Theory and applications of trapdoor functions, *Proceedings of the IEEE Foundations of Comput. Sci.*, (1982), 80–91.

[50] K. Yasutomi, A limit theorem for sequences generated by Weyl transformation: Disappearance of dependence, *Probab. Theory Relat. Fields* **124** (2002), no. 2, 178–188.

[51] K. Yasutomi, A direct proof of dependence vanishing theorem for sequences generated by Weyl transformation, *J. Math. Kyoto Univ.* **43** (2003), no. 3, 599–607.

[52] K. Yasutomi, A dependence vanishing theorem for sequences generated by Weyl transformation, *J. Math. Kyoto Univ.* **44** (2004), no. 2, 365–380.

[53] K. Yasutomi, Private communication.

[54] A.K. Zvonkin and L.A. Levin, The complexity of finite objects and the basing of the concepts of information and randomness on the theory of algorithms, (Russian), *Uspehi Mat. Nauk* 25 (1970), no. 6(156), 85–127, (English translation by S.M. Rudolfer) *Russian Math. Surveys* **25-6** (1970), 83–124.