Chapter 4

Pseudorandom generator

In this chapter, we discuss multipurpose pseudorandom generators. Those exclusively for the Monte Carlo integration have been discussed in § 2.5 and will be discussed further in Chapter 5.

4.1 Computationally secure pseudorandom generator

4.1.1 Definitions

Let us introduce the definition of computationally secure pseudorandom generator as well as related notions. Basic ideas can be seen in [2, 49]. For details, see [24, 36].

Definition 4.1

1. This chapter mainly deals with partial recursive functions $f : \{0,1\}^* \to \{0,1\}^*$ of the following form; for each $n \in \mathbb{N}^+$, $f_n := f|_{\{0,1\}^{r(n)}} : \{0,1\}^{r(n)} \to \{0,1\}^{s(n)}$. We then write $f = \{f_n\}_n$. Let M be a Turing machine which computes f. The *time complexity* $T_f(n)$ of f is defined as the maximum number of steps that M needs to compute $f_n(x)$ where x runs over $\{0,1\}^{r(n)}$. This definition applies to functions of several variables as well.

2. A sequence of integers $\{\ell(n)\}_n$ is called a *polynomial parameter* if there exists a constant $c > 0$ such that $\ell(n) = O(n^c)$.

3. $f = \{f_n\}_n$ with $f_n : \{0,1\}^{r(n)} \to \{0,1\}^{s(n)}$ is called a *polynomial time function* if $r(n)$, $s(n)$ and $T_f(n)$ are polynomial parameters. This definition applies to functions of several variables as well.

4. When a random variable Y is distributed uniformly in a finite set B, we write $Y \in_U B$. We assume that Y is independent of all other random variables in the context. The probability measure that governs Y is often written as $\Pr_Y$.

5. $A = \{A_n\}_n$ is called a *random function* if A is of the form $A_n : \{0,1\}^{r(n)} \times \{0,1\}^{s(n)} \to \{0,1\}^{t(n)}$ with inputs $x \in \{0,1\}^{r(n)}$ and $Y \in_U \{0,1\}^{s(n)}$. We often omit the random variable in the notation and say simply "random function $A_n : \{0,1\}^{r(n)} \to \{0,1\}^{t(n)}$". But the time complexity of A is the one for two variable function $A_n(x,y)$. These definitions and notions apply to functions of several variables as well.