Chin. Ann. Math. Ser. B
46(2), 2025, 241–260
DOI: 10.1007/s11401-025-0013-4

Chinese Annals of Mathematics, Series B

Monte Carlo Integration Using Elliptic Curves*

Chung Pang MOK[1] Huimin ZHENG[2]

Abstract The authors carry out numerical experiments with regard to the Monte Carlo integration method, using as input the pseudorandom vectors that are generated by the algorithm proposed in [Mok, C. P., Pseudorandom Vector Generation Using Elliptic Curves and Applications to Wiener Processes, *Finite Fields and Their Applications*, **85**, 2023, 102129], which is based on the arithmetic theory of elliptic curves over finite fields. They consider integration in the following two cases: The case of Lebesgue measure on the unit hypercube $[0,1]^d$, and as well as the case of Wiener measure. In the case of Wiener measure, the construction gives discrete time simulation of an independent sequence of standard Wiener processes, which is then used for the numerical evaluation of Feynman-Kac formulas.

Keywords Pseudorandom vectors, Elliptic curves, Finite fields, Monte Carlo integration, Feynman-Kac formulas
2020 MR Subject Classification 11K45, 65C10, 65C05, 65M75

1 Introduction

In numerical integration via the Monte Carlo method, and in the simulation of stochastic processes, an important role is played by the generation of pseudorandom numbers, and other more general pseudorandom variables. The most basic one is that of sequence of uniform pseudorandom numbers in unit interval $[0,1]$, that simulates a sample of a sequence of independent identically distributed random variables, with values in $[0,1]$ with uniform distribution. The linear congruential generator is an efficient algorithm to generate such a sequence of uniform pseudorandom numbers. Similarly in the higher dimensional case, namely the case of uniform pseudorandom vectors in the unit hypercube $[0,1]^d$, can be generated by using the matrix version of the linear congruential generator. The high dimensional case is particularly significant from the perspective of Monte Carlo methods, as these are essentially the only proven methods that could beat the curse of dimensionality. Nevertheless, it is well known that, in the higher dimensional case, the sequence of pseudorandom vectors produced by using the linear

Manuscript received June 22, 2022. Revised October 30, 2022.
[1]Shanghai Institute for Mathematics and Interdisciplinary Sciences, Shanghai 200438, China. E-mail: cpmok@simis.cn
[2]Department of Mathematics, Nanjing University, Nanjing 210093, China; Jiangsu National Center for Applied Mathematics, Nanjing 210023, China; College of Information and Network Engineering, Anhui Science and Technology University, Bengbu 233030, Anhui, China. E-mail: zhhm@smail.nju.edu.cn
*This work was supported by the National Natural Science Foundation of China (Nos. 11571163, 12231009), the Key Special Project on Key Scientific Issues of Transformational Technology (No. SQ2020YFA070208) and the Ministry of Science and Technology of Suzhou (No. ZXL2021458).

congruential generator (or its matrix version thereof) could exhibit lattice structures, which sometimes make them not suitable for use in Monte Carlo methods.

In [11], an algorithm is presented to construct sequence of uniform pseudorandom vectors in the unit hypercube $[0,1]^d$, using the arithmetic of elliptic curves over finite fields, with the aim of producing high dimensional pseudorandom vectors with good qualities of uniformity and randomness, and to achieve high accuracy in applications to Monte Carlo integration and simulation.

In this paper, we carry out numerical experiments with regard to Monte Carlo integration and simulation, using as input the high dimensional uniform pseudorandom vectors generated by the algorithm of loc. cit. The following cases are considered. First is the case of Monte Carlo integration of functions on the unit hypercube $[0,1]^d$ with respect to Lebesgue measure, which is the subject of Sections 2–4. Secondly, these uniform pseudorandom vectors are employed to construct discrete time simulation of an independent sequence of standard Wiener processes, which is then applied to numerically solving stochastic ordinary differential equations (driven by Wiener processes), and consequently used for the numerical evaluation of Feynman-Kac formulas in Sections 5–6. The numerical experiments in this paper demonstrate that the high dimensional pseudorandom vectors produced by the algorithm (cf. [11]) have good uniformity and randomness properties, making them suitable for application in Monte Carlo methods.

2 Uniform Pseudorandom Vectors in the Unit Hypercube

We first recall the algorithm from Section 2 of [11] for the generation of uniform pseudorandom vectors in $[0,1]^d$ with respect to Lebesgue measure (and using the notations there), referring to loc. cit. for its theoretical aspects.

Fix $a, r, s \in \mathbf{Z}_{\geq 1}$ with $d \leq 2rs$ (the fundamental case is $s = 1$). Put $m = ar$. Fix a prime p and a finite field F with characteristic p whose cardinality is equal to p^m. Denote by K the subfield of F with cardinality p^a. Fix a basis $\mathfrak{a}' = \{\kappa'_1, \cdots, \kappa'_a\}$ of the extension $K/\mathbf{F}_p$, and a basis $\mathfrak{b}' = \{\lambda'_1, \cdots, \lambda'_r\}$ of the extension F/K. In loc. cit, we fix a basis $\mathfrak{a}$ for $K/\mathbf{F}_p$ and a basis $\mathfrak{b}$ for F/K. Then $\mathfrak{a}'$ and $\mathfrak{b}'$ are dual to $\mathfrak{a}$ and $\mathfrak{b}$ with respect to the trace $\mathrm{Tr}_{K/\mathbf{F}_p}$ and $\mathrm{Tr}_{F/K}$, respectively. For any $z \in F$ and $1 \leq j \leq r$, define

$$\langle z \rangle_j = \mathrm{Tr}_{F/K}(z \cdot \lambda'_j) \in K.$$

We also define, for any $w \in K$,

$$\Phi(w) = \sum_{i=1}^{a} \frac{\mathrm{Tr}_{K/\mathbf{F}_p}(w \cdot \kappa'_i)}{p^i} \in [0,1),$$

where we regard the values of $\mathrm{Tr}_{K/\mathbf{F}_p}$ as elements of $\{0, 1, \cdots, p-1\} \subset \mathbf{Z}_{\geq 0}$. Thus the integer a is the number of digits in the base p expansion of the number $\Phi(w) \in [0,1)$.

Fix an elliptic curve E defined over F with identity element $\mathbf{O}$, whose affine Weierstrass coordinates are noted as x and y. We then have the finite abelian group $E(F)$ with identity

element $\mathbf{O}$. Fix a point $Q \in E(F)$ and also a nonzero integer e. The multiplication by e map on E is noted as $[e]$. Given an initial state $P_0 \in E(F)$, define $\{P_n\}_{n\geq 0} \subset E(F)$, by using the recursion

$$P_{n+1} = [e](P_n) + Q, \quad n \geq 0.$$

For $n \geq 0$, define $G(P_n) \in [0,1]^{2r}$ by the rule

$$G(P_n) = (\Phi(\langle x(P_n)\rangle_1), \cdots, \Phi(\langle x(P_n)\rangle_r), \Phi(\langle y(P_n)\rangle_1), \cdots, \Phi(\langle y(P_n)\rangle_r))$$

for $P_n \neq \mathbf{O}$ (thus in fact we have $G(P_n) \in [0,1)^{2r}$ in this case), and define $G(\mathbf{O}) = (1, \cdots, 1)$ (all coordinates are equal to 1).

For $n \geq 0$, define $\mathfrak{u}_n \in [0,1]^{2rs}$ by the rule

$$\mathfrak{u}_n = (G(P_{ns}), G(P_{ns+1}), \cdots, G(P_{ns+s-1}))$$

regarded as vectors in $[0,1]^{2rs}$.

Finally fix a set injection $\pi : \{1, \cdots, d\} \to \{1, \cdots, 2rs\}$, and define $u_n \in [0,1]^d$ for $n \geq 0$, by the rule that for $1 \leq i \leq d$, the i-th coordinate of u_n is equal to the $\pi(i)$-th coordinate of $\mathfrak{u}_n$. The sequence $\{u_n\}_{n\geq 0} \subset [0,1]^d$ is then, with respect to the choices made above, the sequence of uniform pseudorandom vectors in $[0,1]^d$ as defined by the algorithm of [11].

3 An Illustration for the Unit Square

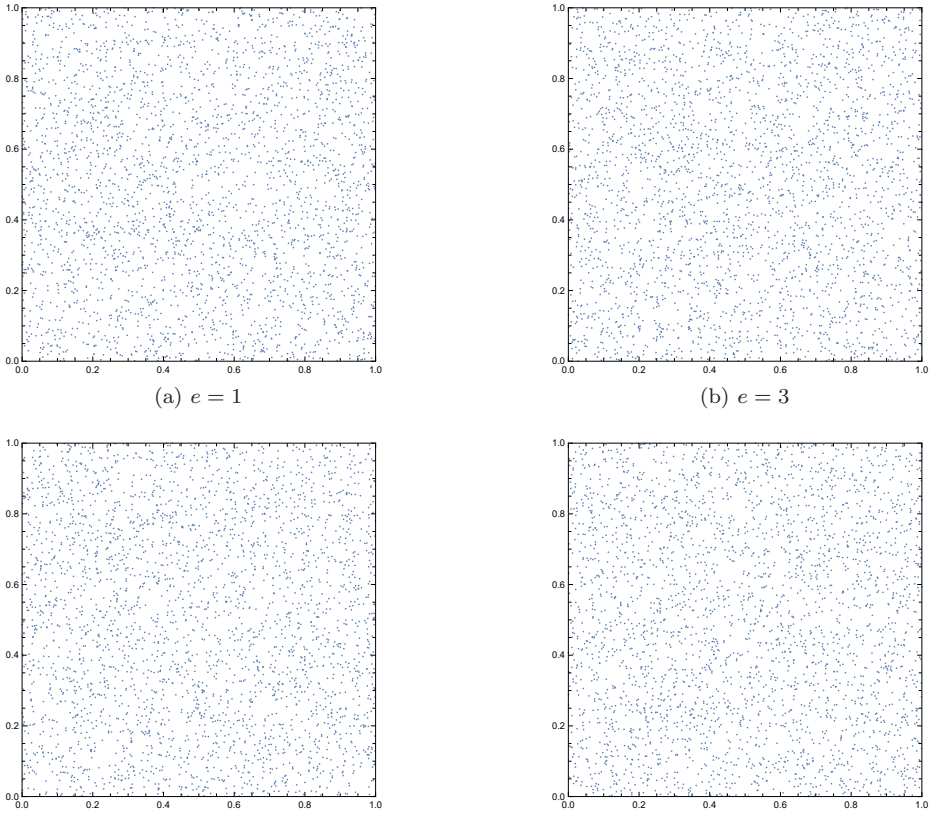
We take $a = 9, r = 5, s = 1$. The prime p is taken to be 17 and fix the finite field F with cardinality equal to 17^{45}. We fix a basis $\mathfrak{a}'$ for $K/\mathbf{F}_{17}$ and a basis $\mathfrak{b}'$ for F/K. The elliptic curve E over F is taken to be the one given by the affine Weierstrass equation $y^2 = x^3 + 1$ (which is a supersingular elliptic curve over F). In this case, $E(F)$ is in fact cyclic with order equal to $17^{45} + 1$. The point $Q \in E(F)$ is chosen to be a generator of $E(F)$, and we consider the cases $e = 1, 3, 5, 7$.

The initial value $P_0 \in E(F)$ is chosen arbitrarily, and we compute $\{G(P_n)\}_{n\geq 0} \subset [0,1]^{10}$ with respect to these choices (the explicit data for the choices of $\mathfrak{a}', \mathfrak{b}', Q, P_0$ is given in Section 9, Appendix II). For $n \geq 0$, we define the vector u_n in the unit square $[0,1]^2$, by taking the first and second coordinates of $G(P_n)$, namely $\Phi(\langle x(P_n)\rangle_1)$ and $\Phi(\langle x(P_n)\rangle_2)$, to be the first and second coordinates of u_n, respectively. In Figure 1, we plot the first 3000 values of u_n, when $e = 1, 3, 5, 7$, respectively. We cannot observe any obvious lattice structures or linear correlations in these point distributions.

To test for the uniformity and pseudorandomness of the two dimensional vectors $\{u_n\}_{n\geq 0} \subset [0,1]^2$, we consider the oscillatory function f defined on $[0,1]$ with range in $[0,1]$,

$$f(x) = \frac{1}{2}\Big(\sin\Big(\frac{1}{x}\Big) + 1\Big) \quad \text{for } x \neq 0, \quad f(0) = 0.$$

We interpret the Lebesgue integral $\int_0^1 f\,\mathrm{d}x$ as the area of the open region $M \subset [0,1]^2$ bounded by the graph of f, and the lines $y = 0, x = 0, x = 1$ (see Figure 2). Then in terms



(a) $e = 1$ (b) $e = 3$

(c) $e = 5$ (d) $e = 7$

Figure 1 The first 3000 values of u_n.

of Monte Carlo integration (which will be considered in more details in the next section), the Monte Carlo estimator of the area of M is given by (when the first N samples of $\{u_n\}_{n\geq 0}$ are used):

$$\frac{1}{N}\sum_{n=0}^{N-1}\delta_M(u_n),$$

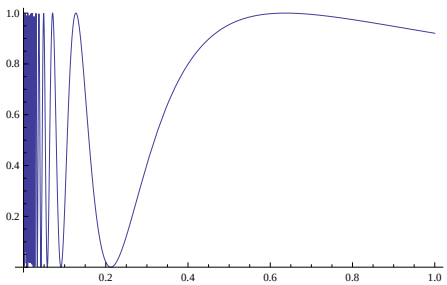


Figure 2

where $\delta_M : [0,1]^2 \to \{0,1\}$ is the characteristic function of the region M. Taking the parameter

e to be equal to 1 in the computations, the numerical results are tabulated in Table 1. Using the command NIntegrate of Mathematica, the numerical value of the integral $\int_0^1 f\,\mathrm{d}x$ is computed to be 0.752034, and we see an excellent agreement.

Table 1 Numerical results.

Methods	# points	Numerical results for $\int_0^1 f\,\mathrm{d}x$
NIntegrate	-	0.752034
MC	1000	0.752000
MC	5000	0.751000
MC	10000	0.752200
MC	15000	0.752467
MC	20000	0.751700

4 Monte Carlo Integration for $[0,1]^d$

Recall Kolmogorov's Strong Law of Large Numbers. Let (X,μ) be a probability space. Consider a sequence of independent and identically distributed X-valued random variables $\{U_n\}_{n\geq 0}$, defined on a probability space $(\Omega,\mathbf{P})$, with distribution law being equal to μ. Given $f\in L^1(X,\mu)$, we have almost surely for $\omega\in\Omega$:

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N-1}f(U_n(\omega))=\int_X f\,\mathrm{d}\mu. \tag{4.1}$$

The quantity $\frac{1}{N}\sum\limits_{n=0}^{N-1}f(U_n(\omega))$ is referred to as Monte Carlo estimator of the integral $\int_X f\,\mathrm{d}\mu$, when the first N elements $U_0(\omega),\cdots,U_{N-1}(\omega)$ of the sample sequence $\{U_n(\omega)\}_{n\geq 0}$ are used. In addition, if we have $f\in L^1(X,\mu)\cap L^2(X,\mu)$, then

$$\mathbf{E}\Big[\Big|\frac{1}{N}\sum_{n=0}^{N-1}f(U_n(\cdot))-\int_X f\,\mathrm{d}\mu\Big|^2\Big]=\frac{\text{variance}(f)}{N}, \tag{4.2}$$

where the expectation $\mathbf{E}$ is with respect to $\mathbf{P}$.

In this section, we consider the case where $X=[0,1]^d$ (for $d\in\mathbf{Z}_{\geq 1}$) with μ being equal to the Lebesgue measure. The case of Wiener measure will be considered in more details in Sections 5–6.

The uniform pseudorandom vectors of Section 2 act as simulation of sample sequences of sequence of independent and identically distributed random variables with values in $[0,1]^d$, with uniform distribution with respect to Lebesgue measure. We refer to [11] for theoretical justification. In this section, we consider examples of Monte Carlo integration of functions on $[0,1]^d$, using these uniform pseudorandom vectors. From (4.2), we have the well known fact about the advantage of Monte Carlo integration, namely that on average the error is, in terms of the number of samples used, independent of the dimension d.

For $d \in \mathbf{Z}_{\geq 1}$, we consider the function f defined on $[0,1]^d$, given by the formula

$$f(x_1, \cdots, x_d) = \prod_{i=1}^{d} \exp\Big(-\frac{x_i}{i}\Big). \tag{4.3}$$

By multivariable integration, we have

$$\int_{[0,1]^d} f(x_1, \cdots, x_d)\, \mathrm{d}x_1 \cdots \mathrm{d}x_d = \prod_{i=1}^{d} i \cdot \Big(1 - \exp\Big(-\frac{1}{i}\Big)\Big). \tag{4.4}$$

Similarly consider the function g defined on $[0,1]^d$, given by the formula

$$g(x_1, \cdots, x_d) = \prod_{i=1}^{d} \cos\Big(\frac{\pi x_i}{2i}\Big). \tag{4.5}$$

Again by multivariable integration, we have

$$\int_{[0,1]^d} g(x_1, \cdots, x_d)\, \mathrm{d}x_1 \cdots \mathrm{d}x_d = \prod_{i=1}^{d} \Big(\frac{2i}{\pi} \cdot \sin\Big(\frac{\pi}{2i}\Big)\Big). \tag{4.6}$$

We apply Monte Carlo integration to computing the numerical values of the integrals (4.4) and (4.6), for a number of values of the dimension d.

We choose the finite fields $K \subset F$ and the elliptic curve E over F as in Section 3. Thus again $a = 9, r = 5$. The choices of $\mathfrak{a}', \mathfrak{b}', Q, P_0$ are again as in Section 3. We take $e = 3$. The sequence of ten dimensional uniform pseudorandom vectors $\{G(P_n)\}_{n\geq 0} \subset [0,1]^{10}$ is then computed.

Below we consider $d = 2rs = 10s$, with $s = 1, 5, 10, 50, 100$, corresponding to the dimensions $d = 10, 50, 100, 500, 1000$, respectively. The sequence of uniform pseudorandom vectors $\{u_n\}_{n\geq 0} \subset [0,1]^d$ is then defined to be

$$u_n = (G(P_{ns}), G(P_{ns+1}), \cdots, G(P_{ns+s-1})), \quad n \geq 0,$$

regarded as vectors in $[0,1]^d$. The Monte Carlo estimators of the integrals (4.4) and (4.6) are then given by $\frac{1}{N}\sum_{n=0}^{N-1} f(u_n)$ and $\frac{1}{N}\sum_{n=0}^{N-1} g(u_n)$, respectively, when the first N samples of $\{u_n\}_{n\geq 0}$ are used. The number of samples N to be used for computations is taken to be 3000. The numerical results for the integrals (4.4), (4.6), and the corresponding Monte Carlo estimators are tabulated in Table 2 below.

Table 2 Numerical results for f and g.

d	$\int_{[0,1]^d} f$	MC for $\int_{[0,1]^d} f$	$\int_{[0,1]^d} g$	MC for $\int_{[0,1]^d} g$
10	0.246528	0.248362	0.506345	0.514815
50	0.112786	0.11315	0.490888	0.495361
100	0.0799835	0.0799167	0.488904	0.491036
500	0.0358531	0.0359526	0.487307	0.490386
1000	0.0253593	0.0252431	0.487107	0.484721

We also consider the following six integrals on $[0,1]^{10}$:

$$I_1 = \int_{[0,1]^{10}} \frac{\exp\Big(\sqrt{1+\prod\limits_{i=1}^{10} x_i}\Big)}{1+\sum\limits_{i=1}^{10} x_i^3}\,\mathrm{d}x_1\cdots\mathrm{d}x_{10},$$

$$I_2 = \int_{[0,1]^{10}} \frac{1+\sin\Big(\sum\limits_{i=1}^{10} x_i^2\Big)}{\sqrt{1+\sum\limits_{i=1}^{10} x_i^2}}\,\mathrm{d}x_1\cdots\mathrm{d}x_{10},$$

$$I_3 = \int_{[0,1]^{10}} \frac{\ln\Big(1+\sum\limits_{i=1}^{10} x_i^2\Big)}{\prod\limits_{i=1}^{10}\sqrt{1+x_i^2}}\,\mathrm{d}x_1\cdots\mathrm{d}x_{10},$$

$$I_4 = \int_{[0,1]^{10}} \frac{\sqrt{1+\sum\limits_{i=1}^{10} x_i^4}}{\ln\Big(2+\sum\limits_{i=1}^{10} x_i^2\Big)}\,\mathrm{d}x_1\cdots\mathrm{d}x_{10},$$

$$I_5 = \int_{[0,1]^{10}} \frac{\exp\Big(\sqrt{\sum\limits_{i=1}^{10} x_i^2}\Big)}{1+\sum\limits_{i=1}^{10} x_i^5}\,\mathrm{d}x_1\cdots\mathrm{d}x_{10},$$

$$I_6 = \int_{[0,1]^{10}} \frac{\ln\Big(2+\sum\limits_{i=1}^{10} x_i^3\Big)}{1+\exp\Big(\sqrt{\sum\limits_{i=1}^{10} x_i^4}\Big)}\,\mathrm{d}x_1\cdots\mathrm{d}x_{10}.$$

The Monte Carlo estimators of the integrals $I_1, I_2, I_3, I_4, I_5, I_6$ are computed by using the ten dimensional uniform pseudorandom vectors $\{G(P_n)\}_{n\geq 0} \subset [0,1]^{10}$ as above (i.e., taking $u_n = G(P_n)$ for $n \geq 0$), with the number of samples N being equal to 5000 in the computations. These are compared with the values computed by using the ten-fold iteration of the one dimensional Gauss-Legendre quadrature rule, with 5 sample points being used for each dimension . Thus the number of sample points needed for the ten-fold iteration is $5^{10} \approx 9.766$ million. Specifically, with $h(x_1, \cdots, x_{10})$ being any one of the integrands occurring in the above ten dimensional integrals, the Gauss-Legendre approximation of the integral is computed as

$$\frac{1}{2^{10}} \sum_{i_1=1}^{5} \cdots \sum_{i_{10}=1}^{5} w_{i_1} \cdots w_{i_{10}} \cdot h\Big(\frac{u_{i_1}+1}{2}, \cdots, \frac{u_{i_{10}}+1}{2}\Big),$$

where we have

$$u_1 = 0, \quad w_1 = \frac{128}{225},$$

$$u_2 = \frac{1}{3}\sqrt{5 - 2\sqrt{\frac{10}{7}}}, \quad w_2 = \frac{322 + 13\sqrt{70}}{900},$$
$$u_3 = -\frac{1}{3}\sqrt{5 - 2\sqrt{\frac{10}{7}}}, \quad w_3 = \frac{322 + 13\sqrt{70}}{900},$$
$$u_4 = \frac{1}{3}\sqrt{5 + 2\sqrt{\frac{10}{7}}}, \quad w_4 = \frac{322 - 13\sqrt{70}}{900},$$
$$u_5 = -\frac{1}{3}\sqrt{5 + 2\sqrt{\frac{10}{7}}}, \quad w_5 = \frac{322 - 13\sqrt{70}}{900}.$$

Finally, we also use the command NIntegrate of Mathematica (local adaptive method) to compute the numerical values of the integrals $I_1, I_2, I_3, I_4, I_5, I_6$. The results are tabulated in Table 3 below.

Table 3 Numerical results.

	NIntegrate	Gauss-Legendre	MC
I_1	0.660371	0.660371	0.663356
I_2	0.472556	0.472556	0.478301
I_3	0.386224	0.386224	0.386548
I_4	1.03125	1.03125	1.03032
I_5	7.2269	7.22908	7.30951
I_6	0.294796	0.294796	0.295298

These numerical results demonstrate that the pseudorandom vectors $\{u_n\}_{n\geq 0} \subset [0,1]^d$ have good uniformity and pseudorandomness properties for Monte Carlo integration of functions on $[0,1]^d$.

5 Simulation of Independent Sequence of Wiener Processes

We now consider the simulation of sample paths of an independent sequence of (one dimensional) standard Wiener processes. Let T be a positive real number, and put

$$C_0([0,T]) = \{c : [0,T] \to \mathbf{R}, \ \ c \text{ is continuous and } c(0) = 0\}.$$

A Wiener process (or Brownian motion) on the time interval $[0,T]$ can be thought of as a $C_0([0,T])$-valued random variable. More precisely let Ω be a probability space with probability measure $\mathbf{P}$. Then a map

$$b : \Omega \to C_0([0,T])$$

is a standard Wiener process on the time interval $[0,T]$, if it satisfies:

• For any $0 \leq t \leq T$, the map $b_t : \Omega \to \mathbf{R}$, given by $b_t(\omega) = (b(\omega))(t)$ for $\omega \in \Omega$, is a $\mathbf{R}$-valued random variable on Ω (thus b corresponds to the stochastic process $\{b_t\}_{t\in[0,T]}$).

• For any $0 \leq t_1 \leq t_2 \leq \cdots \leq t_{n-1} \leq t_n \leq T$, the $\mathbf{R}$-valued random variables $b_{t_2} - b_{t_1}, \cdots, b_{t_n} - b_{t_{n-1}}$ on Ω are independent.

• For any $0 \leq s < t \leq T$, the $\mathbf{R}$-valued random variable $b_t - b_s$ on Ω is normally distributed with mean zero and variance $t - s$.

• Thus, for any Borel measurable subset J of $\mathbf{R}$, the probability

$$\mathbf{P}(\{\omega \in \Omega,\, b_t(\omega) - b_s(\omega) \in J\}) \tag{5.1}$$

is given by

$$\frac{1}{\sqrt{2\pi(t-s)}} \int_J \exp\Big(-\frac{x^2}{2(t-s)}\Big)\, \mathrm{d}x. \tag{5.2}$$

The push-forward of the probability measure $\mathbf{P}$ on Ω to $C_0([0,T])$, via the map b, is the Wiener measure μ_W on $C_0([0,T])$. Thus, $C_0([0,T])$ equipped with the Wiener measure μ_W is a probability space.

A sequence of Wiener processes on the time interval $[0,T]$ is said to be independent, if it is independent as a sequence of $C_0([0,T])$-valued random variables.

Wiener process satisfies the scaling property: If $b : \Omega \to C_0([0,1])$ is a standard Wiener process on the time interval $[0,1]$, then $b^T : \Omega \to C_0([0,T])$ as given by

$$(b^T(\omega))(t) = T^{\frac{1}{2}} \cdot (b(\omega))\Big(\frac{t}{T}\Big), \quad \omega \in \Omega, t \in [0,T]$$

is a standard Wiener process on the time interval $[0,T]$. Hence without loss of generality, we assume $T = 1$ in what follows.

We follow Section 3 of [11] to simulate a sequence of independent standard Wiener processes on the time interval $[0,1]$, or more precisely, discrete time simulation of sample path sequence of a sequence of independent standard Wiener processes. We fix a large integer d which is used for the discretization of the time interval $[0,1]$, and let $\{u_n\}_{\geq 0} \subset [0,1]^d$ be a sequence of uniform pseudorandom vectors as in Section 2. Discard u_n if any one of the coordinates of u_n is equal to 0 or 1, and we may assume $\{u_n\}_{n\geq 0} \subset (0,1)^d$. By applying either the inverse transform method or the Box-Muller method (in the Box-Muller case we assume d is even), we transform $\{u_n\}_{n\geq 0}$ into a sequence $\{v_n\}_{n\geq 0} \subset \mathbf{R}^d$ of Gaussian pseudorandom vectors, with the distribution being equal to the standard normal distribution of $\mathbf{R}^d$ (i.e., the mean is the zero vector, and the variance is the identity matrix). We briefly recall the Box-Muller method: Assume that d is even: $d = 2g$. Put for $n \geq 0$ and $j = 1, \cdots, g$:

$$\begin{aligned} v_n^{(2j-1)} &= \sqrt{-2\ln(u_n^{(2j-1)})}\cos(2\pi u_n^{(2j)}), \\ v_n^{(2j)} &= \sqrt{-2\ln(u_n^{(2j-1)})}\sin(2\pi u_n^{(2j)}), \end{aligned}$$

where $u_n = (u_n^{(1)}, \cdots, u_n^{(d)})$. The sequence $\{v_n\}_{\geq 0}$, with $v_n = (v_n^{(1)}, \cdots, v_n^{(d)})$, is then a sequence of Gaussian pseudorandom vectors in $\mathbf{R}^d$, with standard normal distribution on $\mathbf{R}^d$.

Discard v_n if it is equal to the zero vector. Normalize the vector v_n by defining $w_n = \frac{v_n}{\|v_n\|}$. Then $\{w_n\}_{n\geq 0} \subset S^{d-1}$ is a sequence of pseudorandom vectors on the $d-1$ dimensional unit

hypersphere $S^{d-1} \subset \mathbf{R}^d$, with uniform distribution with respect to the rotationally invariant probability measure on S^{d-1}.

Define the cumulative sum construction

$$\Sigma_d : \mathbf{R}^d \to C_0([0,1]),$$

where if $w = (w^{(1)}, \cdots, w^{(d)}) \in \mathbf{R}^d$, then $\Sigma_d(w) \in C_0([0,1])$ is the piecewise linear function, defined by the conditions that the values of $\Sigma_d(w)$ at the discrete times $0, \frac{1}{d}, \cdots, \frac{d-1}{d}, 1$ are given by

$$(\Sigma_d(w))\Big(\frac{i}{d}\Big) = \sum_{k=1}^{i} w^{(k)}, \quad i = 0, 1, \cdots, d-1, d$$

and linearly interpolated in between the times $0, \frac{1}{d}, \cdots, \frac{d-1}{d}, 1$. Then with $\{w_n\}_{n\geq 0} \subset S^{d-1}$ as above, put $\mathcal{B}_n = \Sigma_d(w_n) \in C_0([0,1])$ for $n \geq 0$. In Section 3 of loc. cit. we have defined the sequence $\{\mathcal{B}_n\}_{n\geq 0} \subset C_0([0,1])$ as discrete time simulation of an independent sequence of standard Wiener processes, with uniform distribution with respect to the discrete time simulation of the Wiener measure (where as in loc. cit. the discrete time simulation of the Wiener measure, is the measure on $C_0([0,1])$ given by the push-forward of the rotationally invariant probability measure on S^{d-1}, via the map $\Sigma_d|_{S^{d-1}}$; it converges weakly to the Wiener measure μ_W as $d \to \infty$).

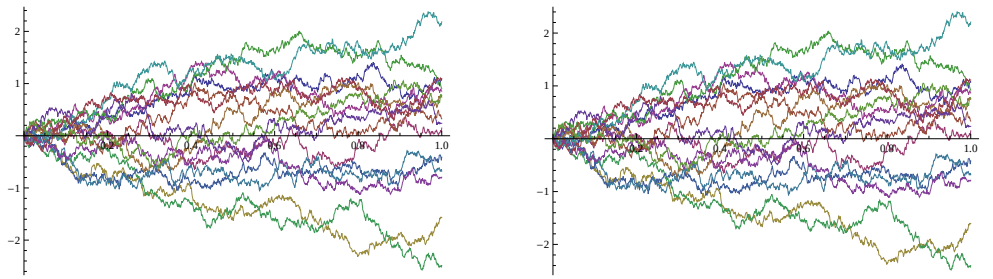
We can also perform the cumulative sum construction with the Gaussian pseudorandom vectors $\{v_n\}_{n\geq 0}$ multiplied by the factor $\frac{1}{\sqrt{d}}$ (this construction appears more commonly in the literature); to distinguish between these two constructions, we refer to the construction $\{\Sigma_d(w_n)\}_{n\geq 0}$ above as the one with time direction normalization (TDN for short), and the construction $\big\{\frac{1}{\sqrt{d}} \cdot \Sigma_d(v_n)\big\}_{n\geq 0}$ as the one without time direction normalization.

In the simulation below, we take $d = 1000$. The finite fields $K \subset F$ and the elliptic curve E over F are as in Sections 3–4. Thus again $a = 9, r = 5$. We take $s = 100$, and so $2rs = 1000 = d$. The choices of $\mathfrak{a}', \mathfrak{b}', Q, P_0$ are as before. We take $e = 1$, and the sequence of uniform pseudorandom vectors $\{u_n\}_{n\geq 0} \subset [0,1]^{1000}$ is given by

$$u_n = (G(P_{100n}), G(P_{100n+1}), \cdots, G(P_{100n+99})), \quad n \geq 0$$

(regarded as vectors in $[0,1]^{1000}$). Then with the Box-Muller method, the Gaussian pseudorandom vectors $\{v_n\}_{n\geq 0} \subset \mathbf{R}^{1000}$ and the pseudorandom vectors $\{w_n\}_{n\geq 0}$ on the unit hypersphere S^{999} are obtained. In Figure 3 below, we plot the first fifteen sample paths of the simulation, both in the case of construction with time direction normalization (Figure 3(a)) and in the case of construction without time direction normalization (Figure 3(b)).

Using the first 5000 sample paths of the simulation, we compute the Monte Carlo estimators of the quantity (5.1), for a number of choices of $0 \leq s < t \leq 1$ and $J \subset \mathbf{R}$ (chosen to be an interval). The results are tabulated in Table 4 below. Comparing with the theoretical value (5.2), we again see excellent agreement.



(a) (b)

Figure 3 Fifteen sample paths of the simulation of sequence of independent standard Wiener processes.

Table 4 Numerical results.

s	t	J	Theoretical	MC (with TDN)	MC (without TDN)
0.25	0.75	$(0,\infty)$	0.5	0.5054	0.5054
0.25	0.75	$(0,1.5)$	0.483053	0.4884	0.4888
0.4	0.5	$(-1.1,1.1)$	0.999496	0.9998	0.9998
0.2	0.56	$(-0.1,0.2)$	0.196742	0.2056	0.2066
0.1	0.35	$(-1,0.5)$	0.818595	0.8186	0.8176
0.32	0.4	$(0.7,1.85)$	0.00666416	0.006	0.006

6 Numerical Evaluation of Feynman-Kac Formulas

In this section, we use the discrete time simulation of sample path sequences of sequence of independent standard Wiener processes, to give numerical evaluation of Feynman-Kac formulas. We recall the following special case of the Feynman-Kac formula, as given by [9, Chapter 5, Theorem 7.6], which suffices for our purpose. Fix $T > 0$.

Let $\sigma(x)$ and $\mu(x)$ be (globally) Lipschitz continuous functions on $\mathbf{R}$. For each $x \in \mathbf{R}$, let $\{X_t^x\}_{t\in[0,T]}$ be a stochastic process on the time interval $[0,T]$, defined on a probability space $(\Omega^x, \mathbf{P}^x)$, that is a solution to the stochastic ordinary differential equation

$$\begin{aligned} \mathrm{d}X_t^x &= \mu\big(X_t^x\big)\mathrm{d}t + \sigma\big(X_t^x\big)\mathrm{d}b_t, \\ X_0^x &= x, \end{aligned} \tag{6.1}$$

where $b : \Omega^x \to C_0([0,T])$ is a standard Wiener process on the time interval $[0,T]$ (recall that b corresponds to the stochastic process $\{b_t\}_{t\in[0,T]}$).

Let $V(x)$ be a nonnegative continuous function on $\mathbf{R}$, and $f(x)$ be a continuous functions on $\mathbf{R}$ that is of (at most) polynomial growth. Then the unique solution $u(x,t)$ to the following Cauchy problem (6.2)–(6.3) that is of (at most) polynomial growth in the variable x (uniformly in the time variable t):

$$\frac{\partial}{\partial t}u(x,t) = \frac{\sigma(x)^2}{2}\frac{\partial^2}{\partial x^2}u(x,t) + \mu(x)\frac{\partial}{\partial x}u(x,t) - V(x)\cdot u(x,t), \quad x \in \mathbf{R},\ t \in [0,T], \tag{6.2}$$

$$u(x,0) = f(x), \quad x \in \mathbf{R} \tag{6.3}$$

is given by

$$u(x,t) = \mathbf{E}^x\Big[\exp\Big(-\int_0^t V(X_s^x(\cdot))\,\mathrm{d}s\Big) f(X_t^x(\cdot))\Big], \tag{6.4}$$

where the expectation $\mathbf{E}^x$ is defined with respect to $\mathbf{P}^x$.

The Feynman-Kac formula (6.4) can be evaluated numerically as a Monte Carlo estimator. For simplicity we take $T = 1$. Fix a large integer d, which is used for the discretization of the time interval $[0,1]$, and let $\{\mathcal{B}_n\}_{n\geq 0} \subset C_0([0,1])$ be discrete time simulation of sample path sequence of a sequence of independent standard Wiener processes, with uniform distribution with respect to discrete time simulation of Wiener measure, as given by the construction in Section 5 (specifically, the construction with time direction normalization).

For the first step, the stochastic ordinary differential equation (6.1) can be solved numerically, by using either the Euler-Maruyama scheme or the Milstein scheme (c.f. [5, Section 7.2]). We illustrate with the latter.

Assume that the function σ is differentiable with derivative σ'. For $x \in \mathbf{R}$ and $n \geq 0$, define $\mathcal{X}_n^x : [0,1] \to \mathbf{R}$ to be the continuous function on the time interval $[0,1]$, specified by the following conditions:

(i) $\mathcal{X}_n^x(0) = x$.

(ii) For $i = 0, 1, \cdots, d-1,$ we have

$$\begin{aligned}\mathcal{X}_n^x\Big(\Big(\frac{i+1}{d}\Big)\Big) &= \mathcal{X}_n^x\Big(\frac{i}{d}\Big) + \mu\Big(\mathcal{X}_n^x\Big(\frac{i}{d}\Big)\Big)\cdot\frac{1}{d} + \sigma\Big(\mathcal{X}_n^x\Big(\frac{i}{d}\Big)\Big)\cdot\Big(\mathcal{B}_n\Big(\Big(\frac{i+1}{d}\Big)\Big) - \mathcal{B}_n\Big(\frac{i}{d}\Big)\Big)\\ &\quad + \frac{1}{2}\sigma\Big(\mathcal{X}_n^x\Big(\frac{i}{d}\Big)\Big)\sigma'\Big(\mathcal{X}_n^x\Big(\frac{i}{d}\Big)\Big)\cdot\Big(\Big(\mathcal{B}_n\Big(\Big(\frac{i+1}{d}\Big)\Big) - \mathcal{B}_n\Big(\frac{i}{d}\Big)\Big)^2 - \frac{1}{d}\Big).\end{aligned}$$

(iii) For $i = 0, 1, \cdots, d-1,$ and $\dfrac{i}{d} \leq t \leq \dfrac{i+1}{d},$ we have

$$\begin{aligned}\mathcal{X}_n^x(t) &= \mathcal{X}_n^x\Big(\frac{i}{d}\Big) + \mu\Big(\mathcal{X}_n^x\Big(\frac{i}{d}\Big)\Big)\cdot\Big(t - \frac{i}{d}\Big) + \sigma\Big(\mathcal{X}_n^x\Big(\frac{i}{d}\Big)\Big)\cdot\Big(\mathcal{B}_n(t) - \mathcal{B}_n\Big(\frac{i}{d}\Big)\Big)\\ &\quad + \frac{1}{2}\sigma\Big(\mathcal{X}_n^x\Big(\frac{i}{d}\Big)\Big)\sigma'\Big(\mathcal{X}_n^x\Big(\frac{i}{d}\Big)\Big)\cdot\Big(\Big(\mathcal{B}_n(t) - \mathcal{B}_n\Big(\frac{i}{d}\Big)\Big)^2 - \Big(t - \frac{i}{d}\Big)\Big).\end{aligned}$$

Then $\{\mathcal{X}_n^x\}_{n\geq 0}$ is the sequence of numerical solutions to the stochastic ODE (6.1) (with respect to the sequence $\{\mathcal{B}_n\}_{n\geq 0}$), according to the Milstein scheme. Note that on each subinterval $\big[\frac{i}{d}, \big(\frac{i+1}{d}\big)\big]$ (here $i = 0, 1, \cdots, d-1$), the numerical solution $\mathcal{X}_n^x$ is either a line segment or a parabola segment.

The Monte Carlo estimator of (6.4) is then given by (when the first N sample paths are-used)

$$\frac{1}{N}\sum_{n=0}^{N-1} \exp\Big(-\int_0^t V(\mathcal{X}_n^x(s))\,\mathrm{d}s\Big) f(\mathcal{X}_n^x(t)). \tag{6.5}$$

In the examples below, we use the simulation of sample path sequence $\{\mathcal{B}_n\}_{n\geq 0}$ in Section 5. Thus $d = 1000$, and the number of sample paths N for computing the Monte Carlo estimator is equal to 5000.

Example 6.1 Take $\sigma(x) \equiv 1$, $\mu(x) \equiv 0$, $V(x) = \frac{1}{2}x^2$. By standard method of separation of variables, the solution to the Cauchy problem

$$\frac{\partial}{\partial t}u(x,t) = \frac{1}{2}\frac{\partial^2}{\partial x^2}u(x,t) - \frac{1}{2}x^2 \cdot u(x,t),$$
$$u(x,0) = x^2 \exp\Big(-\frac{x^2}{2}\Big)$$

is given by

$$u(x,t) = \Big(x^2 - \frac{1}{2}\Big)\exp\Big(-\frac{x^2}{2} - \frac{5}{2}t\Big) + \frac{1}{2}\exp\Big(-\frac{x^2}{2} - \frac{1}{2}t\Big).$$

The solution to the stochastic ODE (6.1) in the present setting is simply $X_t^x = x + b_t$ for $0 \le t \le 1$. And so for $n \ge 0$, we have $\mathcal{X}_n^x = x + \mathcal{B}_n$.

In Table 5, the numerical results for $u(x,t)$ and the Monte Carlo estimator, for a number of values of (x,t), are tabulated.

Table 5 Numerical results for Example 6.1.

x	t	$u(x,t)$	MC estimator
0.0	0.12	0.100473	0.100708
	0.55	0.253366	0.25373
	0.82	0.267458	0.269742
1.5	0.15	0.541075	0.540634
	0.89	0.16542	0.1604
	0.97	0.150212	0.146349
4.6	0.28	0.000271838	0.000271146
	0.42	0.000194077	0.000201864
	0.93	0.0000593357	0.0000574343

Example 6.2 Take $\sigma(x) \equiv 1$, $\mu(x) = -x$, $V(x) \equiv 0$. By standard method of separation of variables, the solution to the Cauchy problem

$$\frac{\partial}{\partial t}u(x,t) = \frac{1}{2}\frac{\partial^2}{\partial x^2}u(x,t) - x\frac{\partial}{\partial x}u(x,t),$$
$$u(x,0) = x^3$$

is given by

$$u(x,t) = \Big(x^3 - \frac{3}{2}x\Big)\exp(-3t) + \frac{3}{2}x\exp(-t).$$

The stochastic ODE (6.1) in the present setting

$$\mathrm{d}X_t^x = -X_t^x\mathrm{d}t + \mathrm{d}b_t, \quad X_0^x = x$$

is known as the equation for Ornstein-Uhlenbeck process.

In Figure 4, we plot the first few sample paths of $\{\mathcal{X}_n^x\}_{n\ge 0}$, where we take $x = 0.5$.

In Table 6, the numerical results for $u(x,t)$ and the Monte Carlo estimator, for a number of values of (x,t), are tabulated.

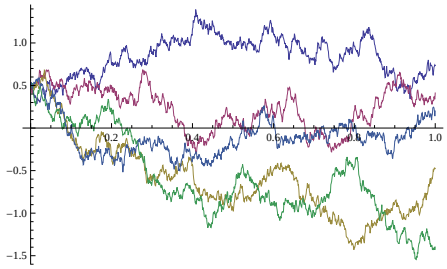


Figure 4 Ornstein-Uhlenbeck Process.

Table 6 Numerical results for Example 6.2.

x	t	$u(x,t)$	MC estimator
0.5	0.01	0.136009	0.138471
	0.12	0.229143	0.23619
	0.78	0.2836	0.283965
4.0	0.02	60.5035	60.6174
	0.25	32.0701	32.4253
	0.94	5.80091	5.88172
7.8	0.12	333.298	334.38
	0.45	127.45	128.387
	0.66	69.9528	70.3336

Example 6.3 Take $\sigma = \alpha \cdot x$, where $\alpha \in \mathbf{R}_{>0}$ is a positive constant, and $\mu(x) = \beta \cdot x$, $V(x) \equiv \beta$, where $\beta \in \mathbf{R}$ is a (nonnegative) constant. Then the equation

$$\frac{\partial}{\partial t}u(x,t) = \frac{1}{2}\alpha^2 x^2 \frac{\partial^2}{\partial x^2}u(x,t) + \beta x \frac{\partial}{\partial x}u(x,t) - \beta u(x,t) \tag{6.6}$$

(here we consider only the region $x > 0$) is the time-reversed Black-Scholes equation. Upon the change of variables transformation

$$z = \ln(x) + \Big(\beta - \frac{\alpha^2}{2}\Big)t,$$
$$v(z,t) = u(x,t) \cdot \exp(\beta t),$$

the time reversed Black-Scholes equation becomes the heat equation on $\mathbf{R}$:

$$\frac{\partial}{\partial t}v(z,t) = \frac{1}{2}\alpha^2 \frac{\partial^2}{\partial z^2}v(z,t),$$

which could be solved by standard method in terms of the heat kernel.

The stochastic ODE (6.1) in the present setting

$$\mathrm{d}X_t^x = \beta X_t^x \mathrm{d}t + \alpha X_t^x \mathrm{d}b_t, \quad X_0^x = x$$

is known as the equation for geometric Brownian motion. The exact solution is given by

$$X_t^x = x \exp\Big(\Big(\beta - \frac{\alpha^2}{2}\Big)t + \alpha b_t\Big).$$

Thus for $n \geq 0$, we take $\mathcal{X}_n^x$ as given by

$$\mathcal{X}_n^x(t) = x \exp\Big(\Big(\beta - \frac{\alpha^2}{2}\Big)t + \alpha \mathcal{B}_n(t)\Big)$$

for $0 \leq t \leq 1$.

Taking $\alpha = \beta = 1$, in Figure 5, we plot the first few sample paths of $\{\mathcal{X}_n^x\}_{n\geq 0}$, where we take $x = 0.2$.

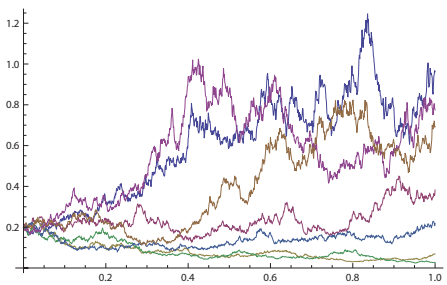


Figure 5 Geometric Brownian Motion.

Define $f(x) = \sin(\ln(x))$ for $x \geq 1$ and $f(x) = 0$ for $x \leq 1$. Consider the corresponding Cauchy problem with the PDE given by (6.6), with $\alpha = \beta = 1$. In terms of the change of variables transformation as above

$$\begin{aligned} z &= \ln(x) + \frac{1}{2}t, \\ v(z,t) &= u(x,t) \cdot \exp(t), \end{aligned}$$

the Cauchy problem becomes

$$\begin{aligned} &\frac{\partial}{\partial t} v(z,t) = \frac{1}{2}\frac{\partial^2}{\partial z^2} v(z,t), \\ &v(z,0) = g(z), \end{aligned}$$

where $g(z) = \sin(z)$ for $z \geq 0$ and $g(z) = 0$ for $z \leq 0$. The solution is given by

$$\begin{aligned} v(z,t) &= \frac{1}{\sqrt{2\pi t}} \int_{-\infty}^{\infty} g(y) \exp\Big(-\frac{(z-y)^2}{2t}\Big)\,\mathrm{d}y \\ &= \frac{1}{\sqrt{2\pi t}} \int_{0}^{\infty} \sin(y) \cdot \exp\Big(-\frac{(z-y)^2}{2t}\Big)\,\mathrm{d}y, \end{aligned}$$

and so

$$u(x,t) = \frac{\exp(-t)}{\sqrt{2\pi t}} \int_0^{\infty} \sin(y) \cdot \exp\Big(-\frac{\big(\ln(x) + \frac{t}{2} - y\big)^2}{2t}\Big)\,\mathrm{d}y.$$

In Table 7, the numerical results for $u(x,t)$ and the Monte Carlo estimator, for a number of values of (x,t), are tabulated.

Table 7 Numerical results for Example 6.3.

x	t	$u(x,t)$	MC estimator
0.2	0.36	0.00116327	0.00125004
	0.77	0.0134829	0.0138267
	0.98	0.0204211	0.0206518
2.5	0.56	0.411061	0.414545
	0.7	0.344585	0.345809
	0.94	0.251402	0.251611
5.2	0.7	0.319492	0.315669
	0.87	0.237883	0.232871
	0.95	0.206465	0.202842

Remark 6.1 The construction given in Section 5 of discrete time simulation of sample path sequences of sequence of independent standard Wiener processes, can be extended directly to the higher dimensional case (cf. [11, Remark 3.3]). These could be employed for the numerical evaluation of higher dimensional Feynman-Kac formulas. This is particularly significant from the point of view of Monte Carlo methods, in view of the phenomenon of the curse of dimensionality. We also refer to the papers [1, 3–4, 6–8] for the case of non-linear Feynman-Kac formulas.

7 Conclusion

The numerical experiments that we have carried out demonstrate that the algorithm of [11] is able to produce sequences of high dimensional pseudorandom vectors, with good uniformity and randomness properties, making them suitable for application in Monte Carlo integration, Monte Carlo simulation, stochastic optimization, sequential Monte Carlo, Markov chain Monte Carlo, multilevel Monte Carlo, etc (for reference on Monte Carlo methods see for example (cf. [2, 10, 13])). In the case of $[0,1]^d$, these sequences of pseudorandom vectors act as simulation of sample sequences of a sequence of independent and identically distributed random variables with values in $[0,1]^d$, with uniform distribution with respect to Lebesgue measure; in the case of $C_0([0,T])$, these act as simulation of sample path sequences of a sequence of independent standard Wiener processes, with uniform distribution with respect to (discrete time simulation of) Wiener measure. In the latter case, these simulations could be employed for the numerical evaluation of Feynman-Kac formulas.

For numerical integration, it is well known that, in moderate dimensions and for functions of moderate variation with sufficient smoothness, Quasi-Monte Carlo methods (cf. [12]), that are based on the use of quasi-random low discrepancy sequences, for example the Halton, Sobol, Faure or Niederreiter sequences, etc, give better rates of convergence as compared to Monte Carlo methods (with the latter being based on the use of sequences with strong randomness properties). An interesting problem is to develop hybrid algorithms combining the pseudoran-

dom sequence algorithm of [11] with Quasi-Monte Carlo methods (randomized Quasi-Monte Carlo for example); this will be the subject of future investigation.

8 Appendix I: An Illustration for the Unit Sphere

We give an illustration for the construction of pseudorandom vectors on the unit sphere S^2, with uniform distribution with respect to the rotationally invariant probability measure on S^2 (c.f. Section 5 and also [11, Section 3.1]). The sequence of uniform pseudorandom vectors $\{G(P_n)\}_{n\geq 0} \subset [0,1]^{10}$ is as in Section 3 with $e = 1$. Apply the Box-Muller method to $\{G(P_n)\}_{n\geq 0}$ and obtain sequence of Gaussian pseudorandom vectors $\{v_n\}_{n\geq 0} \subset \mathbf{R}^{10}$ (with standard normal distribution on $\mathbf{R}^{10}$). Define $\{\overline{v}_n\}_{n\geq 0} \subset \mathbf{R}^3$ with the coordinates of $\overline{v}_n$ being given by the first three coordinates of v_n. Then $\{\overline{v}_n\}_{n\geq 0}$ is a sequence of Gaussian pseudorandom vectors in $\mathbf{R}^3$ (with standard normal distribution on $\mathbf{R}^3$). Finally, define $w_n = \frac{\overline{v}_n}{\|\overline{v}_n\|} \in S^2$. Then $\{w_n\}_{n\geq 0} \subset S^2$ is a sequence of pseudorandom vectors on S^2, with uniform distribution with respect to the rotationally invariant probability measure on S^2. In Figures 6–7 below, we plot the first 3000 sample points of the Gaussian pseudorandom vectors $\{\overline{v}_n\}_{n\geq 0}$, and the uniform pseudorandom vectors $\{w_n\}_{n\geq 0}$ on S^2.

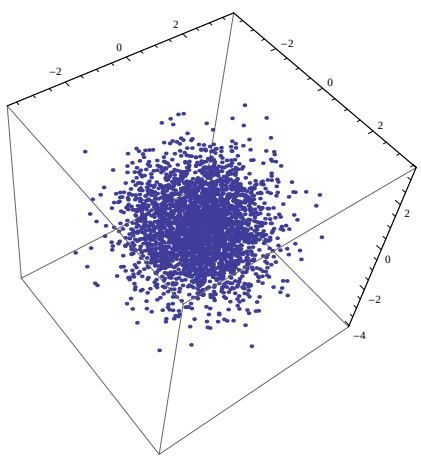


Figure 6 Gaussian pseudorandom vectors in $\mathbf{R}^3$.

9 Appendix II: Some Data

Throughout this paper, the computations of points of elliptic curves over finite fields are performed using the PARI/GP package. The rest of the computations are performed using Mathematica 9.0. Starting from Section 3, we have taken the finite field F to be of characteristic equal to 17, with cardinality equal to 17^{45}. We fix a primitive element f of the finite field F; in particular $\{1, f, f^2, \cdots, f^{44}\}$ is a basis of F over $\mathbf{F}_{17}$, and we express the elements of F in terms of this basis.

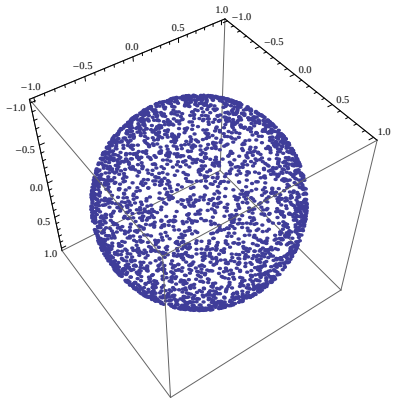


Figure 7 Uniform pseudorandom vectors on S^2.

The minimal polynomial of f over $\mathbf{F}_{17}$, which is thus a primitive polynomial over $\mathbf{F}_{17}$, is given by (the coefficients are taken as elements in $\mathbf{F}_{17}$)

$$x^{45}+14x^{44}+14x^{43}+6x^{42}+6x^{41}+16x^{40}+4x^{39}+10x^{38}+10x^{37}+15x^{36}+12x^{35}+16x^{34}+10x^{33}+16x^{31}+2x^{30}+x^{29}+13x^{28}+14x^{27}+5x^{26}+11x^{25}+10x^{23}+7x^{21}+2x^{20}+x^{19}+6x^{18}+6x^{17}+13x^{16}+15x^{14}+2x^{13}+6x^{12}+12x^{11}+12x^{10}+13x^9+14x^8+2x^7+x^6+5x^4+10x^3+6x^2+16.$$

With the elliptic curve E over F given by the affine Weierstrass equation $y^2=x^3+1$, the finite abelian group $E(F)$ is cyclic of order $17^{45}+1$, and we take the point Q to be a generator of $E(F)$, with affine Weierstrass coordinates given by

$$\begin{aligned}x(Q)=\ & f^{44}+13f^{43}+10f^{42}+9f^{41}+15f^{40}+16f^{39}+14f^{38}+14f^{37}+8f^{36}+f^{35}+14f^{34}\\ & +14f^{33}+6f^{32}+13f^{31}+f^{30}+12f^{29}+12f^{28}+16f^{27}+5f^{26}+12f^{25}+9f^{24}+9f^{23}\\ & +10f^{22}+9f^{21}+7f^{20}+8f^{19}+7f^{18}+13f^{17}+2f^{16}+5f^{15}+16f^{14}+10f^{13}+9f^{12}\\ & +5f^{11}+4f^{10}+2f^9+4f^8+5f^7+14f^6+12f^5+4f^4+15f^3+7f^2+14f+4,\\ y(Q)=\ & 3f^{44}+9f^{43}+3f^{42}+11f^{41}+6f^{40}+9f^{39}+13f^{38}+3f^{37}+13f^{36}+14f^{35}+14f^{34}\\ & +16f^{33}+3f^{32}+9f^{31}+3f^{30}+13f^{29}+3f^{28}+5f^{27}+15f^{26}+f^{25}+9f^{24}+12f^{23}+10f^{22}\\ & +8f^{21}+4f^{20}+f^{18}+2f^{17}+12f^{16}+9f^{15}+12f^{14}+12f^{13}+8f^{12}+13f^{11}+3f^{10}+6f^8\\ & +3f^7+8f^6+5f^5+16f^4+12f^3+14f+8.\end{aligned}$$

The affine Weierstrass coordinates of the point P_0 are given by

$$\begin{aligned}x(P_0)=\ & 9f^{44}+5f^{43}+12f^{41}+10f^{40}+4f^{39}+5f^{38}+4f^{37}+8f^{36}+7f^{35}+6f^{34}+14f^{33}+3f^{32}\\ & +10f^{31}+6f^{29}+14f^{28}+2f^{27}+4f^{26}+11f^{25}+5f^{23}+2f^{22}+4f^{21}+5f^{20}+9f^{19}+7f^{18}\\ & +4f^{17}+14f^{16}+8f^{15}+6f^{14}+13f^{13}+13f^{12}+9f^{11}+9f^{10}+16f^9+13f^8+14f^7+16f^6\\ & +9f^5+5f^4+11f^3+4f+3,\\ y(P_0)=\ & 8f^{44}+10f^{43}+13f^{42}+8f^{41}+6f^{40}+9f^{39}+16f^{38}+13f^{37}+15f^{36}+9f^{35}+3f^{34}\\ & +f^{33}+8f^{32}+13f^{31}+4f^{30}+14f^{29}+5f^{28}+8f^{27}+12f^{26}+13f^{25}+11f^{24}+11f^{23}+f^{22}\\ & +5f^{21}+14f^{20}+8f^{19}+2f^{18}+3f^{17}+2f^{16}+11f^{15}+8f^{14}+f^{13}+16f^{12}+3f^{11}+11f^{10}\\ & +6f^9+9f^8+8f^7+9f^6+6f^5+10f^4+14f^3+16f^2+13f+6.\end{aligned}$$

Finally, with K being equal to the unique subfield of F of cardinality equal to 17^9, the basis $\mathfrak{a}'$ for $K/\mathbf{F}_{17}$ is taken to be $\{\kappa'_1, \cdots, \kappa'_9\}$, with

$$\kappa'_1 = 1,$$

$$\begin{aligned}\kappa'_2 = {} & f^{43} + 6f^{41} + 14f^{40} + 8f^{39} + 16f^{38} + 4f^{37} + 5f^{36} + 4f^{35} + 9f^{34} + 12f^{33} + 4f^{32} + 16f^{31} \\ & + 4f^{30} + 10f^{29} + 8f^{28} + 12f^{27} + 14f^{26} + 3f^{25} + 14f^{24} + 11f^{23} + 11f^{22} + 16f^{21} + 8f^{19} + 14f^{17} \\ & + 9f^{16} + 10f^{15} + f^{14} + 8f^{13} + 7f^{12} + 4f^{11} + 13f^{10} + 4f^9 + 11f^8 + 4f^6 + 10f^5 + 13f^4 \\ & + 2f^3 + 14f^2 + f + 12,\end{aligned}$$

$$\begin{aligned}\kappa'_3 = {} & 15f^{44} + 3f^{43} + 10f^{42} + 9f^{40} + 9f^{39} + 11f^{38} + 3f^{37} + 4f^{36} + 6f^{35} + 2f^{33} + f^{32} + f^{31} + 13f^{30} \\ & + 10f^{29} + 15f^{28} + 15f^{27} + 14f^{26} + 16f^{25} + 6f^{24} + 8f^{23} + 11f^{22} + 9f^{21} + f^{20} + 2f^{19} + 7f^{18} \\ & + 8f^{17} + 8f^{16} + 11f^{14} + 14f^{13} + 15f^{12} + 16f^{11} + 12f^{10} + 6f^9 + 7f^8 + 11f^7 + 4f^6 + 10f^5 \\ & + 16f^3 + 15f^2 + 13f + 7,\end{aligned}$$

$$\begin{aligned}\kappa'_4 = {} & 4f^{43} + 7f^{42} + 7f^{41} + 13f^{40} + 2f^{39} + 15f^{38} + 12f^{36} + 3f^{35} + 14f^{34} + 11f^{33} + 11f^{32} \\ & + 4f^{31} + 5f^{30} + 3f^{28} + 2f^{27} + 10f^{26} + f^{25} + 14f^{24} + 7f^{23} + 7f^{22} + 9f^{21} + 3f^{20} + 3f^{19} \\ & + 12f^{18} + 16f^{17} + 6f^{15} + 6f^{14} + 11f^{12} + 10f^{11} + 9f^{10} + 14f^9 + 12f^8 + f^7 + 2f^5 \\ & + 4f^3 + 3f^2 + 14,\end{aligned}$$

$$\begin{aligned}\kappa'_5 = {} & 15f^{44} + 6f^{43} + 12f^{42} + 14f^{41} + 13f^{40} + 3f^{39} + 6f^{38} + 15f^{37} + 3f^{36} + 14f^{35} + 15f^{34} \\ & + 13f^{33} + 8f^{32} + 7f^{31} + 2f^{30} + 2f^{29} + 9f^{28} + 2f^{27} + 13f^{26} + 5f^{25} + 14f^{24} + 16f^{23} + 6f^{22} \\ & + f^{21} + 16f^{20} + 4f^{19} + 4f^{18} + 4f^{17} + 15f^{16} + 5f^{15} + f^{14} + 7f^{13} + 2f^{12} + 4f^{11} + 14f^{10} \\ & + 6f^9 + 15f^8 + 6f^7 + 11f^6 + 12f^5 + 16f^4 + 2f^3 + 2f^2 + 8f + 5,\end{aligned}$$

$$\begin{aligned}\kappa'_6 = {} & 6f^{44} + 11f^{43} + 11f^{42} + 10f^{41} + 16f^{40} + 11f^{39} + 16f^{38} + 13f^{37} + 10f^{36} + 16f^{35} + 6f^{33} \\ & + 6f^{32} + 8f^{31} + 11f^{30} + 3f^{29} + 6f^{28} + 12f^{27} + 13f^{26} + 8f^{25} + 3f^{24} + 11f^{23} + 16f^{22} + 5f^{21} \\ & + 4f^{20} + f^{19} + 4f^{18} + 12f^{17} + 14f^{16} + f^{15} + 2f^{14} + 5f^{13} + 2f^{12} + 7f^{11} + 5f^{10} + 4f^9 + 4f^8 \\ & 8f^7 + 10f^6 + 12f^5 + 5f^4 + 13f^3 + 14f^2 + 11f + 6,\end{aligned}$$

$$\begin{aligned}\kappa'_7 = {} & 12f^{44} + 4f^{43} + 5f^{41} + 8f^{40} + 2f^{38} + 6f^{37} + 16f^{36} + 9f^{35} + 10f^{34} + 9f^{33} + 7f^{32} + 3f^{31} \\ & + 9f^{30} + 14f^{29} + 5f^{27} + 5f^{26} + 6f^{25} + 12f^{24} + 14f^{23} + f^{22} + 8f^{20} + 8f^{19} + 3f^{17} + f^{16} + 3f^{15} \\ & + 14f^{14} + 3f^{13} + 12f^{12} + 13f^{11} + 7f^{10} + 7f^9 + 14f^8 + 4f^7 + 10f^6 + 11f^5 + 16f^4 + 6f^3 \\ & + 7f^2 + 9f + 14,\end{aligned}$$

$$\begin{aligned}\kappa'_8 = {} & 2f^{44} + 2f^{43} + 6f^{42} + 14f^{41} + 2f^{40} + 2f^{39} + 14f^{38} + 16f^{37} + 4f^{36} + 4f^{35} + 13f^{34} + 12f^{33} \\ & + 3f^{32} + 11f^{31} + 6f^{30} + 2f^{29} + 4f^{28} + 12f^{27} + 11f^{26} + 3f^{25} + 3f^{24} + 15f^{23} + 11f^{22} + 15f^{21} \\ & + 7f^{20} + 12f^{19} + 3f^{18} + 2f^{17} + f^{16} + 12f^{15} + 12f^{14} + 6f^{13} + 6f^{12} + 15f^{11} + 10f^{10} + 7f^9 \\ & + 3f^8 + 14f^7 + 5f^6 + 4f^5 + 13f^4 + 15f^3 + 8f^2 + 2f + 14,\end{aligned}$$

$$\begin{aligned}\kappa'_9 = {} & 6f^{44} + 7f^{43} + f^{42} + 6f^{41} + 2f^{40} + 2f^{39} + 5f^{38} + 6f^{37} + 3f^{36} + 16f^{35} + 11f^{34} + 12f^{33} \\ & + 14f^{32} + 15f^{31} + 9f^{30} + 10f^{29} + 15f^{28} + 13f^{27} + 6f^{26} + 4f^{25} + 11f^{24} + 4f^{23} + 13f^{22} \\ & + 3f^{21} + 6f^{20} + 7f^{19} + 12f^{18} + 6f^{17} + 15f^{16} + 8f^{15} + 4f^{14} + 12f^{13} + 14f^{12} + 10f^{11} + 11f^{10} \\ & + 16f^9 + 5f^8 + 13f^7 + 11f^6 + 16f^5 + 4f^4 + 11f^3 + 6f^2 + f + 13\end{aligned}$$

and the basis $\mathfrak{b}'$ for F/K is taken to be $\{1, f, f^2, f^3, f^4\}$.

Acknowledgments The authors would like to thank Professor Hourong Qin for encouragements. We acknowledge the support of the Jiangsu National Center for Applied Mathematics, where the research was conducted.

Declarations

Conflicts of interest The authors declare no conflicts of interest.

References

[1] Beck, C., Hutzenthaler, M. and Jentzen, A., On nonlinear Feynman-Kac formulas for viscosity solutions of semilinear parabolic partial differential equations, *Stochastics and Dynamics*, **21**(8), 2021, 2150048.

[2] Barbu, A. and Zhu, S.-C., Monte Carlo Methods, Springer-Verlag, Springer Nature Singapore Pte Ltd., 2020.

[3] E, W., Hutzenthaler, M., Jentzen, A. and Kruse, T., On multilevel Picard numerical approximations for high-dimensional nonlinear parabolic partial differential equations and high-dimensional nonlinear backward stochastic differential equations, *Journal of Scientific Computing*, **79**(3), 2019, 1534–1571.

[4] E, W., Hutzenthaler, M., Jentzen, A. and Kruse, T., Multilevel Picard iterations for solving smooth semilinear parabolic heat equations, *Partial Differential Equations and Applications*, **2**(80), 2021.

[5] Graham, C. and Talay, D., Stochastic Simulation and Monte Carlo Methods: Mathematical Foundations of Stochastic Simulation, Stochastic Modelling and Applied Probability, **68**, Springer-Verlag, Heidelberg, 2013.

[6] Hutzenthaler, M., Jentzen, A. and von Wurstemberger, P., Overcoming the curse of dimensionality in the approximative pricing of financial derivatives with default risks, *Electronic Journal of Probability*, **25**, 2020, 1–73.

[7] Hutzenthaler, M., Jentzen, A., Kruse, T., et al., Overcoming the curse of dimensionality in the numerical approximation of semilinear parabolic partial differential equations, *Proceedings of the Royal Society A*, **476**(2244), 2020, 20190630.

[8] Hutzenthaler, M. and Kruse, T., Multi-level Picard approximations of high dimensional semilinear parabolic differential equations with gradient-dependent nonlinearities, *SIAM Journal on Numerical Analysis*, **58**(2), 2020, 929–961.

[9] Karatzas, I. and Shreve, S., Brownian Motion and Stochastic Calculus, Graduate Texts in Mathematics, **113**, Springer-Verlag, New York, 1988.

[10] Kroese, D. P., Taimre, T. and Botev, A. I., Handbook of Monte Carlo Methods, Wiley Series in Probability and Statistics, John Wiley & Sons, Inc. Hoboken, NJ, 2011.

[11] Mok, C. P., Pseudorandom Vector Generation Using Elliptic Curves and Applications to Wiener Processes, *Finite Fields and Their Applications*, **85**, 2023, 102129.

[12] Niederreiter, H., Random Number Generation and Quasi-Monte Carlo Methods, CBMS-NSF Regional Conference Series in Applied Mathematics, **63**, 1992.

[13] Rubinstein, R. Y. and Kroese, D. P., Simulation and the Monte Carlo Method, 3rd ed., Wiley Series in Probability and Statistics, John Wiley & Sons, Inc. Hoboken, NJ, 2017.