Framework for testing random numbers in parallel calculations

I. Vattulainen
Department of Chemistry, Building 207, Technical University of Denmark, DK-2800 Lyngby, Denmark
and Helsinki Institute of Physics, P.O. Box 9, FIN-00014 University of Helsinki, Helsinki, Finland
(Received 4 November 1998; revised manuscript received 8 February 1999)

We propose a framework for testing the quality of random numbers in parallel calculations. The key idea is to study cross-correlations between distinct sequences of random numbers via correlations between various diffusing random walkers, each of which is governed by a distinct random number sequence. The asymptotic power-law behavior of the corresponding correlation functions yields exponents, which can be compared with exact theoretical results. Correlations prior to the asymptotic regime can be further investigated by other complementary methods. We demonstrate this approach by three efficient tests, which find correlations in various commonly used pseudorandom number generators. Finally, we discuss some ideas for applying this framework in other contexts. [S1063-651X(99)05106-5]

PACS number(s): 02.70.Lq, 05.40.−a, 82.20.Wt

I. INTRODUCTION

Random numbers are used in various simulation techniques such as the Monte Carlo method, simulated annealing, and Langevin dynamics [1]. The purpose of random numbers is to introduce the stochastic dynamics in these methods, thus they all depend crucially on the quality of random numbers, which for practical reasons are usually produced by deterministic pseudorandom number generator algorithms [2]. Due to advances in developing better algorithms [2–4] and test methods [2–7], the problem raised by the deterministic nature of pseudorandom numbers is not as serious as one might suspect. However, no matter how weak the correlations in random number sequences are, they are still inevitable and can lead to erroneous results in some applications. This is particularly true in high-precision Monte Carlo work, where the high accuracy required and special simulation algorithms used have led to a situation where some well-known and commonly used pseudorandom number generators have failed in recent simulations of physical model systems [7–13]. These observations have given rise to a new *application specific* testing approach, where the models themselves act as a testing ground for pseudorandom numbers [7]. This approach has turned out to be very useful in revealing situations where the subtle, underlying correlations in pseudorandom number sequences interfere constructively with the simulation algorithm. A related problem concerns the use of pseudorandom numbers in parallel calculations, which is the usual approach when large-scale computations are carried out. In this respect, it is surprising to note that virtually all tests in present use have been designed to focus on correlations *within a single* pseudorandom number sequence $\{r_i\}$, while in parallel calculations it is the *cross-correlations* between *distinct* pseudorandom number sequences $\{r_i\}^{(1)}, \ldots, \{r_i\}^{(m)}$ that are at least equally important. This emphasizes the importance of developing novel test methods that mimic the use of random numbers in *parallel calculations*, and the need to test the quality of pseudorandom number sequences in this context.

In this work, our purpose is to introduce a framework for testing the quality of random numbers in parallel applications. The key idea is to study cross-correlations between non-overlapping sequences of random numbers in terms of random walks, which are relevant to a wide variety of disciplines, including physics, chemistry, biology, and economics [14]. For practical purposes, we demonstrate this approach by three tests. To optimize their efficiency in finding correlations, the tests are designed to be as simple as possible. Nevertheless they have a close connection with various commonly studied problems, namely, they focus on the asymptotic behavior of random walks governed by the corresponding universal exponents, which therefore allows a comparison with exact theoretical results. Correlations prior to the asymptotic regime are further investigated by other methods. The first two tests measure cross-correlations between two distinct random number sequences, considering their height correlations and intersection probabilities. The third test, which is based on calculating the number of sites visited by the random walkers, can be used to study cross-correlations between any number of distinct random number sequences. Although the emphasis here is on presenting the general framework, we also test a number of commonly used pseudorandom number generators and find the tests to be very efficient in probing short- and intermediate-range correlations. Ideas for applying this framework in other contexts are further discussed.

II. FRAMEWORK FOR TESTING RANDOM NUMBERS

Let us first briefly discuss the use of random numbers in parallel calculations and then justify our approach. In parallel simulations, the task is decomposed into several (about) equally sized subtasks, whose number equals the number of central processing units (CPU's) m. Within a given time period, each subtask $k=1, \ldots, m$ requires a distinct sequence of random numbers $\{r_i\}^{(k)}$, $i=1, \ldots, \Omega_k$, to update the system, after which the CPU's exchange information. This process is repeated a desired number of times. The correlations in pseudorandom numbers may now affect the dynamics in two ways. The first case regarding correlations *within* $\{r_i\}^{(k)}$ is well established, since it is characteristic for doing stochastic simulations in a ''traditional'' way in single work

stations. The second possibility concerns *cross-correlations* between *distinct* [15] random number sequences $\{r_i\}^{(1)}, \ldots, \{r_i\}^{(m)}$ used by processors one through m. In practical numerical work, this problem is faced, for example, in Langevin molecular dynamics simulations of fluids or in Monte Carlo simulations of diffusion on a lattice with *particle decomposition*, in which one divides particles over the CPU's. For simplicity, we now imagine each particle group k to be characterized by some pseudoparticle whose stochastic dynamics is governed by $\{r_i\}^{(k)}$. This pseudoparticle is immersed in a sea of other pseudoparticles, whose dynamics are governed by other sequences $\{r_i\}^{(l)}$, $l \neq k$. This gives rise to the leading idea in the present work. We consider diffusing random walkers, each of which is governed by a distinct random number sequence, and study their mutual correlations. Although this approach does not account for all microscopic degrees of freedom subject to stochastic dynamics in real model systems, it still grasps the point of interest in a simple and efficient manner.

We now propose three tests that are based on the idea above. They study both types of correlations, that is, correlations within a single random number sequence $\{r_i\}^{(k)}$ *and* correlations between *distinct* [15] random number sequences $\{r_i\}^{(1)}, \ldots, \{r_i\}^{(m)}$. Here we consider the case where the sizes Ω_k of sequences $\{r_i\}^{(k)}$ are equal for all k. Random numbers r_i are uniformly distributed between zero and one.

In the *height correlation test*, we consider the position x_i of a one-dimensional (1D) random walker vs the number of jumps made, i. The position $x_t = \Sigma_{i=1}^{t} \delta x_i$ is a sum of displacements δx_i, which are random variables

$$\delta x_i = \begin{cases} +1, & \text{if } r_i \leqslant 1/3 \\ 0, & \text{if } 1/3 < r_i \leqslant 2/3 \\ -1, & \text{otherwise.} \end{cases} \tag{1}$$

In this fashion, we construct the paths $x_i^{(1)}$ and $x_i^{(2)}$ from the sequences $\{r_i\}^{(1)}$ and $\{r_i\}^{(2)}$, respectively. The height between the two random walkers is then defined as $h_t = x_t^{(1)} - x_t^{(2)}$, whose correlation function $H_t \equiv \langle |h_t - h_0| \rangle \sim t^{\phi}$ is known to decay asymptotically as a power law with an exponent $\phi = 1/2$ [16]. Deviations from $\phi = 1/2$ are expected, if H_t does not correspond to a random process.

The *intersection test* deals with two random walks on a square lattice. Starting from the origin, the random walkers carry out jumps to the four possible directions with an equal probability. In this way, one obtains paths $(x_i^{(1)}, y_i^{(1)})$ and $(x_i^{(2)}, y_i^{(2)})$ of the two random walkers for all $i = 1,2, \ldots, \Omega$. We now consider the probability I_t that the two random walks after t jumps have *no* intersection other than their common starting point. We stress that the two random walks need not meet at the same site at the same time, but any common point in their paths is regarded as an intersection. For a random process, I_t behaves asymptotically like a power law $I_t \sim t^{-\alpha}$ with an exponent $\alpha = 5/8$ [17–19].

The previous tests focused on correlations between the paths of two random walks. The S_N *test* described next is more general in the sense that it can be applied to study any number of random walks. In *one dimension*, N random walkers move simultaneously without any interaction such that, at any jump attempt, they can make a jump to the left or to the right with equal probability. After $t \gg 1$ jumps by all random walkers, the mean number of sites visited, $S_{N,t}$, has an asymptotic form $S_{N,t} \sim f(N) t^{\gamma}$, where the scaling function $f(N) = (\ln N)^{1/2}$ and $\gamma = 1/2$ [20]. The value of γ observed serves as a measure of correlations.

In this work, the height correlation function H_t was investigated up to $\Omega = 2000$ with $M = 10^7$ independent runs, while in the intersection test the relevant parameters were $M = 10^8$ and $\Omega = 4000$. To allow a comparison of the efficiency of the three tests, the S_N test was also carried out with two random walkers ($N = 2$). In this case, the test utilized $M = 10^8$ samples with $\Omega = 2000$. To assure that these choices for the length of a single random walk Ω were large enough to find the true asymptotic behavior of the correlation functions, we considered the ''running exponent'' [21]

$$\epsilon_t \equiv \frac{\ln(C_{t+\delta t}/C_t)}{\ln[(t+\delta t)/t]} \tag{2}$$

of the corresponding correlation function C_t, which can be any of the functions H_t, I_t, or $S_{N,t}$. The time window δt used in this work was typically 200. As is shown below, the running exponent of the ''best'' pseudorandom number generators converges to the theoretically expected value well before Ω.

III. RESULTS FOR SOME PSEUDORANDOM NUMBER GENERATORS

The three tests were subjected to a number of commonly used pseudorandom number generators. The generators tested in this work include generalized feedback shift-register (GFSR) algorithms [22] R250 and R89, which are of the form $r_n = r_{n-250} \oplus r_{n-103}$ and $r_n = r_{n-89} \oplus r_{n-38}$, respectively, where $\oplus$ is the bitwise exclusive OR operator. A variation of the previous generators is ZIFF9689 [4], which is a GFSR generator with four taps, $r_n = r_{n-9689} \oplus r_{n-471} \oplus r_{n-314} \oplus r_{n-157}$. Other generators include combination generators RANMAR [23,24] and MZRAN [25], and a generator RANLUX [26], which is based on ideas of deterministic chaos. In RANLUX, one generates $b \geqslant 24$ random numbers, delivers 24 of them, and throws the remaining $b - 24$ numbers away. The value of b defines a ''luxury level'' ranging from zero ($b = 24$) to four ($b = 389$), for which we use notations RANLUX0 and RANLUX4, respectively. Other versions partially considered in this work are RANLUX1 ($b = 48$), RANLUX2 ($b = 97$), and RANLUX3 ($b = 223$). For further details of the generators, see the references above.

To determine the exponents ϕ, α, and γ, we considered their running counterparts via Eq. (2). Demonstrative results for the S_N test and the height correlation test are shown in Figs. 1(a) and 1(b), respectively. Aside from the initial regime which will be discussed separately below, all generators express similar behavior in the sense that the running exponents converge to some limiting value at large t. This regime was therefore used to determine the exponents [27].

The results for the exponents ϕ, α, and γ are given in Table I. Results for the GFSR generators R89 and R250 are not surprising, since they have recently failed in various random walk tests [4,7,11,28]. Exponents given by ZIFF9689, which is basically a three-decimation of $r_n = r_{n-9689}$

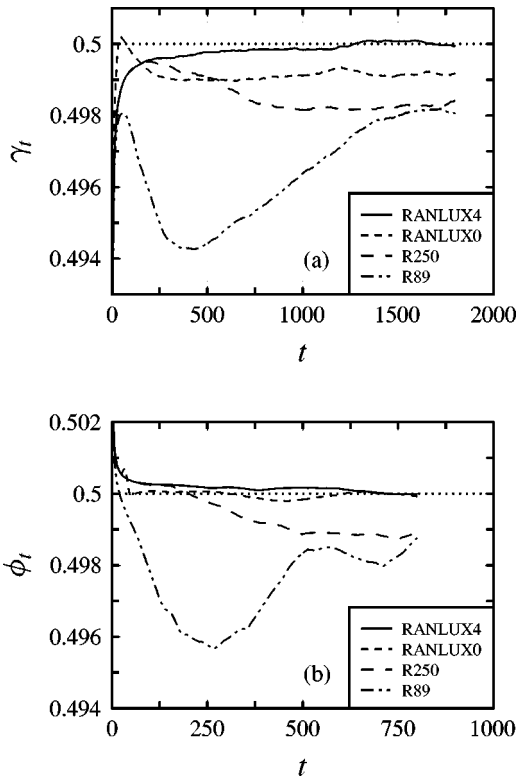

FIG. 1. (a) A demonstration of the temporal correlations in the S_N test. Shown here is the running exponent γ_t which converges to the asymptotic value γ (see Table I) at large t. The asymptotic, theoretically expected value $\gamma=1/2$ is illustrated with a dotted line. To clarify the presentation, results of RANMAR, MZRAN, and ZIFF9689 are not shown here. (b) Similar results for the running exponent ϕ_t in the height correlation test. In both figures, we used a time window $\delta t=200$. The variable t is given in units of jumps made in a random walk.

$\oplus r_{n-471}$ [4], are in agreement with exact values. This is mainly due to the long lag in this generator, which suppresses the dominating correlations out of reach. Of the other generators, the performance of RANLUX0 is rather weak. This finding is in agreement with recent studies, where one also observed pronounced short-range correlations [26,29,30]. The improved versions RANLUX1–RANLUX4 together with the combination generators MZRAN and RANMAR, on the other hand, perform very well.

As far as the efficiency of the tests is concerned, the results indicate that the S_N test is somewhat more efficient in finding correlations than the other two tests. This suggests that a close spatial coupling of the diffusing random walkers improves the efficiency of a test, and should be accounted for in further test development.

It is worth pointing out that the exponents extracted from the data characterize only the asymptotic behavior of the correlation functions. Correlations in pseudorandom number sequences are playing a role also at shorter scales. This is very evident from Fig. 1. Asymptotically γ_t and ϕ_t tend towards γ and ϕ given in Table I, while prior to this regime, for some generators, the running exponents do not level off monotonously but have a very complex behavior. To improve the efficiency of the tests, we next study how the correlations in correlation functions C_t^{RNG} are accumulated over

TABLE I. Results for the exponents of the three tests. The notation 0.4984(2) means 0.4984 ± 0.0002. The exponents were extracted from the asymptotic tail of the corresponding correlation functions, and the exponents that deviate from the exact value by more than two error bars are shown in bold face. The generators RANLUX1 – RANLUX3 have been studied only by the S_N test, which seems to be the most efficient one of the present tests; thus ''NA'' stands for not available. In the case of cumulative correlations described by ξ, the generator is considered to fail the test if $\xi>1$. Such cases are also clarified by presenting them in bold face.

RNG	Height correlation test		Intersection test		S_N test	
	ϕ	ξ	α	ξ	γ	ξ
RANLUX4	0.5001(1)		0.6257(5)		0.5000(1)	
RANLUX3	NA	NA	NA	NA	0.4999(1)	0.5
RANLUX2	NA	NA	NA	NA	0.5000(1)	0.2
RANLUX1	NA	NA	NA	NA	0.4999(1)	**1.1**
RANLUX0	0.4999(1)	0.7	**0.6240(4)**	0.2	**0.4991(1)**	**894.7**
RANMAR	0.5000(1)	**2.1**	0.6250(4)	0.9	0.5001(1)	**11.0**
MZRAN	0.5000(1)	0.2	0.6244(6)	0.8	0.5000(1)	0.1
ZIFF9689	0.5000(1)	0.3	0.6237(7)	0.4	0.5000(1)	0.1
R250	**0.4989(2)**	**5.5**	**0.6265(5)**	**19.7**	**0.4984(1)**	**23.8**
R89	**0.4984(2)**	**277.9**	**0.6205(5)**	**279.0**	**0.4981(1)**	**3940.6**
Exact	1/2		5/8		1/2	

all scales. Here C_t^{RNG} is any of the correlation functions H_t, I_t, $S_{N,t}$ as determined by some random number generator (RNG). Since the exact form of H_t, I_t, and $S_{N,t}$ for all t is not known, we compare the generators with respect to RANLUX4, whose overall performance here and also in other tests [26,30] has been remarkably good. We have chosen to consider the cumulative effect of squared displacements

$$d^{\mathrm{RNG}}=\sum_{t=1}^{\Omega}\frac{(C_t^{\mathrm{RANLUX4}}-C_t^{\mathrm{RNG}})^2}{C_t^{\mathrm{RANLUX4}}}, \tag{3}$$

which mimics the χ^2 test [31] and yields a test statistic $\xi^{\mathrm{RNG}}=d^{\mathrm{RNG}}/\sigma$, where σ is a measure of true fluctuations as determined from RANLUX4 [32]. Consistent results are found, if we replace RANLUX4 with either MZRAN or ZIFF9689 as a reference generator. This basically implies that the statistical quality of these three generators in the present tests is equally good.

As one can observe from Table I, ξ is a very strong measure of correlations in pseudorandom number sequences. Besides being consistent with the asymptotic results, ξ reveals that correlations in some generators are prominent also prior to the asymptotic regime. In this regard, results of R89, R250, and RANLUX0 are not surprising, although the extent of correlations is striking. More advanced versions of RANLUX, namely, RANLUX2 and RANLUX3, perform essentially better, while RANLUX1 seems to be a borderline case whose results in the S_N test are manifested by slight correlations. Nevertheless, one should pay attention to the results of RANMAR, which has recently performed well in various test schemes [7,10,23,24,29,33] and which has also been suggested as a good candidate when one aims towards a ''universal genera-

tor'' [24]. Despite the correct asymptotic behavior, results for ξ indicate that the pseudorandom number sequences produced by RANMAR contain correlations which are very weak but still observable when accumulated over a wide range of walk lengths. By studying Eq. (3) with varying Ω, we found that the correlation effects appear after about 120 jumps. This is comparable to the longer lag of 97 in the lagged Fibonacci part in RANMAR [23,24], thus providing a simple reason for this observation. Anyhow, we feel that one should not be surprised by any results presented here. Every pseudorandom number generator is a possible source of error in stochastic simulations, and it is only a question of time when the underlying correlations turn out to be relevant for the application under study. In other words, there are no universal pseudorandom number generators.

IV. SUMMARY AND DISCUSSION

In this work, we have presented a framework for testing the quality of pseudorandom number generators in parallel applications. The approach is based on studying mutual correlations between various random walks taking place simultaneously and has a close connection with many commonly studied problems. For practical purposes, we have demonstrated this approach by three tests, which find correlations in various commonly used pseudorandom number generators studied in this work. However, we stress that the three tests presented here serve mainly as a demonstration for further development. That could make use of polymer diffusion, where each polymer segment in a single chain is governed by a distinct pseudorandom number sequence, or of mutual correlations between self-avoiding random walks [34], for example. In a more general context, one can also study real model systems by starting two different runs from an identical initial state but with distinct pseudorandom number sequences, and consider how rapidly the two systems lose coherence. Therefore the only requirement is to study the *correlation* between some species governed by distinct sequences of random numbers. We finally close this work by addressing the importance of theoretical work [35]. Namely, although the present test methods are very useful in detecting correlations, they do not reveal how large the contribution arising *directly* from cross-correlations is. A theoretical basis for analyzing the pseudorandom number sequences is therefore crucial in understanding how cross-correlations come into play in stochastic simulation studies.

ACKNOWLEDGMENTS

P. L'Écuyer is thanked for his hospitality and discussions during the author's visit to the Université de Montréal where this work basically started. The author also thanks T. Ala-Nissila and R. M. Ziff for discussions, and the Helsinki Institute of Physics at the University of Helsinki, as well as Technical University of Denmark for computing resources. This work has, in part, been supported by a grant from the European Union.

[1] K. Binder and D.W. Heermann, *Monte Carlo Simulation in Statistical Physics* (Springer-Verlag, Berlin, 1988); M. P. Allen and D. J. Tildesley, *Computer Simulation of Liquids* (Oxford, New York, 1993); D. Frenkel and B. Smit, *Understanding Molecular Simulation: From Algorithms to Applications* (Academic Press, San Diego, 1996).

[2] P. L'Écuyer, Ann. Oper. Res. **53**, 77 (1994).

[3] P. Hellekalek, Math. Comput. Simul. **46**, 485 (1998).

[4] R.M. Ziff, Comput. Phys. **12**, 385 (1998); Phys. Rev. Lett. **69**, 2670 (1992).

[5] G. Marsaglia, in *Computer Science and Statistics: The Interface*, edited by L. Billard (Elsevier, Amsterdam, 1985), p. 3.

[6] A. Compagner, Phys. Rev. E **52**, 5634 (1995).

[7] I. Vattulainen, T. Ala-Nissila, and K. Kankaala, Phys. Rev. Lett. **73**, 2513 (1994); Phys. Rev. E **52**, 3205 (1995).

[8] A.M. Ferrenberg, D.P. Landau, and Y.J. Wong, Phys. Rev. Lett. **69**, 3382 (1992).

[9] W. Selke, A.L. Talapov, and L.N. Shchur, Pis'ma Zh. Éksp. Teor. Fiz. **85**, 1144 (1983) [JETP Lett. **58**, 665 (1993)].

[10] P.D. Coddington, Int. J. Mod. Phys. C **5**, 547 (1994); **7**, 295 (1996).

[11] P. Grassberger, J. Phys. A **26**, 2769 (1993); Phys. Lett. A **181**, 43 (1993).

[12] R.M. D'Souza, Y. Bar-Yam, and M. Kardar, Phys. Rev. E **57**, 5044 (1998).

[13] F.J. Resende and B.V. Costa, Phys. Rev. E **58**, 5183 (1998).

[14] J. Stat. Phys. **30**, 2 (1983), special issue, edited by G.W. Weiss and R.J. Rubin; E.W. Montroll and M.F. Shlesinger, in *Nonequilibrium Phenomena II: From Stochastics to Hydrodynamics*, edited by J.L. Lebowitz and E.W. Montroll (Elsevier, Amsterdam, 1984).

[15] There are many ways to construct the sequences $\{r_i\}^{(1)}, \ldots, \{r_i\}^{(m)}$ for the processors one through *m*. We used random numbers $\{r_i\}=r_1, \ldots, r_\Omega, r_{\Omega+1}, \ldots, r_{2\Omega}, \ldots$ generated by a single pseudorandom number generator to make nonoverlapping sequences $\{r_i\}^{(1)}=r_1, \ldots, r_\Omega$, $\{r_i\}^{(2)}=r_{\Omega+1}, \ldots, r_{2\Omega}$, and so forth. Other possibilities for constructing the sequences are given in, e.g., S. L. Anderson, SIAM Rev. **32**, 221 (1990).

[16] J. Krug, Adv. Phys. **46**, 139 (1997).

[17] B. Duplantier and K.-H. Kwon, Phys. Rev. Lett. **61**, 2514 (1988).

[18] K. Burdzy and G.F. Lawler, Ann. Prob. **18**, 981 (1990); G. Slade, Am. Sci. **84**, 146 (1996).

[19] Use of the intersection test to study more than two random walkers is also possible, although rigorous mathematical bounds for α in this case are not available (see Refs. [17,18]).

[20] H. Larralde, P. Trunfio, S. Havlin, H.E. Stanley, and G.H. Weiss, Phys. Rev. A **45**, 7128 (1992).

[21] Equation (2) is just one rational approach to consider the convergence of an exponent which characterizes power-law behavior. Another possibility given in Ref. [17] was found to yield consistent results in the asymptotic limit.

[22] T.G. Lewis and W.H. Payne, J. Assoc. Comput. Mach. **20**, 456 (1973).

[23] F. James, Comput. Phys. Commun. **60**, 329 (1990).
[24] G. Marsaglia, A. Zaman, and W.-W. Tsang, Stat. Prob. Lett. **9**, 35 (1990).
[25] G. Marsaglia and A. Zaman, Comput. Phys. **8**, 117 (1994).
[26] M. Lüscher, Comput. Phys. Commun. **79**, 100 (1994); F. James, *ibid.* **79**, 111 (1994).
[27] To determine the exponent, there are various ways which yield essentially identical results. Estimation of the error bars is a different matter. Use of linear regression is one possibility, but this approach provides an error estimate that is unreasonably small. To obtain a more realistic estimate, we determined the error bars (given in Table I) on the basis of fluctuations in the running exponents.
[28] L.N. Shchur, J.R. Heringa, and H.W.J. Blöte, Physica A **241**, 579 (1997).
[29] I. Vattulainen, K. Kankaala, J. Saarinen, and T. Ala-Nissila, Comput. Phys. Commun. **86**, 209 (1995).
[30] L.N. Shchur and P. Butera, Int. J. Mod. Phys. C **9**, 607 (1998).
[31] D.E. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 2nd ed. (Addison-Wesley, Reading, MA, 1981).
[32] To determine σ, we calculated a given correlation function C_t of RANLUX4 ten times with $M/10$ samples each up to $t=\Omega$. For each of these, we calculated $d^{LUX,i}$, $i=1,\ldots,10$, with respect to (an independent calculation of) C_t of RANLUX4 with M samples. Then σ is simply the mean of $\{d^{LUX,i}\}$. The same procedure was carried out for all correlation functions H_t, I_t, and $S_{N,t}$.
[33] K.G. Hamilton, Comput. Phys. Commun. **81**, 237 (1994).
[34] N. Madras and G. Slade, *The Self-Avoiding Walk* (Birkhäuser, Boston, 1993).
[35] For theoretical work on parallel random number generation, see K. Entacher, ACM Trans. Model. Comput. Simul. **8**, 61 (1998), and references therein.