APL Quantum

RESEARCH ARTICLE | SEPTEMBER 20 2024

Comparing pseudo- and quantum-random number generators with Monte Carlo simulations

David Cirauqui ; Miguel Ángel García-March ; Guillem Guigó Corominas; Tobias Graß ; Przemysław R. Grzybowski ; Gorka Muñoz-Gil ; J. R. M. Saavedra ; Maciej Lewenstein

Check for updates

APL Quantum 1, 036125 (2024)
https://doi.org/10.1063/5.0199568

View Online
Export Citation

Articles You May Be Interested In

A high speed, postprocessing free, quantum random number generator
Appl. Phys. Lett. (July 2008)

Fully passive quantum random number generation with untrusted light

Metalens array for quantum random number
Appl. Phys. Rev. (September 2024)

04 December 2025 19:44:04

APL Quantum
Special Topics
Open for Submissions
Submit Today!
AIP Publishing

AIP Publishing

APL Quantum ARTICLE pubs.aip.org/aip/apq

Comparing pseudo- and quantum-random number generators with Monte Carlo simulations

Cite as: APL Quantum 1, 036125 (2024); doi: 10.1063/5.0199568
Submitted: 23 January 2024 • Accepted: 26 August 2024 •
Published Online: 20 September 2024

View Online Export Citation CrossMark

David Cirauqui,[1,2,a)] Miguel Ángel García-March,[2,3] Guillem Guigó Corominas,[2] Tobias Graß,[2] Przemysław R. Grzybowski,[2,4] Gorka Muñoz-Gil,[2,5] J. R. M. Saavedra,[1] and Maciej Lewenstein[2,6]

AFFILIATIONS

[1] Quside Technologies SL, Mediterranean Technology Park, 08860 Castelldefels, Barcelona, Spain
[2] ICFO - Institut de Ciencies Fotòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain
[3] Instituto Universitario de Matemática Pura y Aplicada, Universitat Politècnica de València, 46022 València, Spain
[4] Institute of Spintronics and Quantum Information, Faculty of Physics, Adam Mickiewicz University in Poznań, Umultowska 85, 61-614 Poznań, Poland
[5] Institute for Theoretical Physics, University of Innsbruck, Technikerstr. 21a, A-6020 Innsbruck, Austria
[6] ICREA, Pg. Lluís Companys 23, 08010 Barcelona, Spain

[a)] **Author to whom correspondence should be addressed:** dcirauqui@quside.com

ABSTRACT

We study how the Monte Carlo simulations of the critical dynamics of two-dimensional Ising lattices are affected by the quality (as compared to true randomness) of the pseudo-randomness used in them by computing an observable known to be sensitive to it: the dynamic critical exponent z. To this end, we first present a review of the literature and then perform the same simulations with different pseudo-randomness sources. We control the quality of the random streams by physically reseeding the generators and observe that while the mean value of the measured observable is slightly affected by the correlations within them, its variance does get a severe impact. By studying this affectation and how such pseudo-random streams perform under standard randomness tests based on statistical analysis, we conclude that the new protocol is able to detect other types of correlations and can thus be used as an additional test. On the other hand, we present the first (to the best of our knowledge) computation of the dynamic critical exponent with a perfectly random quantum random number generator (QRNG) and hypothesize that the presented strategy may point toward a route to establish quantum advantage based on the quality of results as complementary to those strategies based on the speed of the computational task.

© 2024 Author(s). All article content, except where otherwise noted, is licensed under a Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/). https://doi.org/10.1063/5.0199568

I. INTRODUCTION

Monte Carlo (MC) methods are a collection of algorithms that use the probabilistic sampling of certain purely deterministic functions in order to speed up (or simply even make possible) a given computation and are commonly used in a broad range of applications. To this end, MC algorithms perform a random number-assisted search of the solution space, and therefore, the quality of the obtained results can be affected by that of the random numbers (RN) used, thus relying on them being *good enough*. For instance, a MC algorithm using RN presenting unknown correlations on timescales different than the simulation time will in many cases perform a rather bad exploration of the solution space, thus yielding poor results. Modern computations in which MC algorithms are used usually demand vast amounts of RN, which only makes this problem more notorious. Furthermore, current MC simulations are typically executed in parallel and distributed architecture, with each of the simulation threads typically running its own random number generator (RNG). Deviations from an ideal RNG (for example, by having a short repetition period) may introduce correlations between the

04 December 2025 19:44:04

different threads executing the simulation. This results in a breach of one of the most relevant theoretical assumptions of the MC method, that is, each of the samples is independent from the others. Furthermore, this breach is not only a theoretical concern: its effects may be noticeable in any simulation that is sensitive to the correlations between random numbers.[1,2]

Concretely, it has been observed that the simulation of complex physical systems can make some hidden correlations within "good quality" pseudo-random sequences arise and affect their results.[1,2] A paradigmatic example of this phenomenon is the computation of the dynamic critical exponent z, a characteristic constant appearing when studying the dynamics of spin lattices near a phase transition. Phase transitions are characterized by presenting time and space correlations on all possible scales, and therefore, even the usually undetectable long-range correlations present within the RN streams arise and can have a dramatic impact on the value obtained.[2]

The problem then arises from the long-known difficulty of computers to generate such an RN: strictly speaking, all algorithm-based random number generators (RNGs) are pseudo-random, in the sense that they are completely deterministic, and, thus, present correlation. There mainly exist two different strategies to generate pseudo-random numbers in a computer: via algorithmic procedures and via the extraction of entropy from physical processes within the machine. Typically, there is a trade-off between the statistical correlations (their "quality," as compared to true RN) within PRN and their generation rate. On the one hand, RNGs using iterative non-linear maps may be very fast but have typically relatively short correlation lengths. On the other hand, RNGs based on measuring physical or natural processes do not show correlations besides those given by the fact that one measures them within finite streams but are slower and less efficient. As an alternative, quantum random number generators (QRNGs) have been proposed as the ultimate and only possible way to obtain truly unpredictable and uncorrelated randomness. Furthermore, these devices have been already commercialized in the last decade and are expected to soon be able to generate random bits at fast enough speeds for them to be useful additions for computing and cryptographic purposes. In this regard, QRNGs are clearly one of the most advanced quantum technologies.

Either classical or quantum, a significant challenge for randomness technologies consists of assuring non-predictability of RNG outputs, which is usually done with statistical tests.[3–5] The National Institute of Standards and Technologies (NIST) has collected and defined a set of tests to measure the quality of PRNGs,[6] which, however, have serious drawbacks. For instance, future and more complex PRNGs may present new types of correlations that such tests were not designed to detect, or, as we shall see later, some long studied calculations, such as the MC simulations of certain systems, may be affected by the correlations within PRN streams passing them. In this paper, we propose to use the simulation of such classical statistical physics systems at criticality as an unbiased test of RNGs on equal footing, concretely focusing on the calculation of the dynamic critical exponent characterizing the relaxation dynamics of the 2D Ising system. We start by reviewing some background concepts related to the generation of pseudo-random numbers and the studied physical problem. To begin with this paper's contributions, we first review, in Sec. III A, the many estimations of this exponent found in the literature, obtained via theoretical, experimental, and numerical strategies, and extract a reference value to which we compare the results of Secs. III B–III D. In Sec. III B, we compute it by means of MC simulations performed with a pool of PRNGs ranging from bad to good quality ones and compare and discuss the results. We find that the variance of the results exponentially grows when the simulations require more RN than the period of repetition of the generators (and thus the sequences start to repeat) and explore how such a variance explosion can be avoided via reseeding. Later, in Sec. III C, we compute this exponent with a QRNG, finding that it is close to the defined reference value. We finally compare, in Sec. III D, all the used generators with standard statistical tests and discuss their similarities and differences, supporting the complementarity of additional tests based on physical simulations, such as the one proposed here.

II. METHODS

A. PRNGs

Pseudo-random numbers are nothing but outputs of a given algorithmic process and, being thus obtained by means of deterministic functions, are completely predictable if the state of the function at a given time is known. In its most general form, a pseudo-random number generator is a function of the form

$$\vec{x}_n = f(\vec{x}_{n-1}), \tag{1}$$

where the vector $\vec{x}_n$ is called the state of the PRNG at stage n. Afterward, a post-processing of the internal state x_n transforms it into the output random number, $r_n = g(\vec{x}_n)$. Ideally, the function $g(f(\vec{x}_{n-1}))$ will seem to output uncorrelated numbers on the short run (where, in reality, short refers to "as long as possible"), while emulating a certain probability distribution, typically uniform, on the long one.

1. Reseeding

Note that taking into account that we want to be able to code such functions so that they can be used in computer simulations, the state must be comprised of (at least at the bit level) discrete values. In addition, any realistic implementation of a probability distribution will inevitably be bound to a certain range of outputs as those values whose probability of appearance is lower than the machine's precision will be assigned a real probability of exactly zero. Jointly, these two properties that any imaginable PRNG will have effectively lead to a very undesired conclusion: a PRNG will always have a period of repetition as well since the function outputting the numbers will eventually repeat a given input. This means that once a certain amount of pseudo-random numbers is output by the function, the stream will reach the same initial state and, thus, will exactly repeat itself (or a smaller cycle within the whole sequence if the first repeated output does not coincide with the very initial seed) over again.

This repetition of sequences can be nonetheless avoided by *reseeding* the generator. The reseeding operation consists of, at a given frequency (ideally corresponding to a period shorter than the PRNG's period of repetition), externally changing the state with a new random seed (or single bits of the current state). If the seed is truly random, i.e., obtained from a true random number generator, then the PRNG will have an infinite period of repetition.[2] Contrarily, if the seed is output by a second PRNG, the first one will

04 December 2025 19:44:04

© Author(s) 2024

then have an enlarged period of repetition, but it will not be infinite and the sequences will repeat themselves over again once the second PRNG reaches its own maximum amount of different output pseudo-random numbers.

2. LCGs

A Linear Congruential Generator (LCG)[7,8] is a pseudo-random engine algorithm that, given a previous state x_n, produces a new state x_{n+1} such that

$$x_{n+1} = (ax_n + c) \mod m, \tag{2}$$

finally outputting a pseudo-random number with the application of the identity function on the new state, $r_n = x_n$. The parameters defining the LCG a, c, and m are strictly positive integer constants called multiplier, increment, and modulus, respectively (except for the increment, which can be 0 and in which case the LCG is usually referred to as Lehmer RNG).

Due to the modulo operation, the output pseudo-random numbers may be within the range

$$0 \le x_n < m, \tag{3}$$

and therefore, they have a potential period of repetition of at most m as, by construction, once a number is repeated, the sequence starts over again from that number. Their easy general formula makes them fast and efficient to implement in computing devices and, thus, are widely used in computer simulations. Furthermore, as their state is comprised of a single mod m number, the memory required for its storage is relatively low; this is helpful especially when multiple independent pseudo-random streams are needed. On the other hand, their pseudo-randomness quality is seen to be extremely sensitive to their defining parameters, and thus, their selection requires much more care. For instance, a bad choice of parameters can yield an LCG with a period of repetition shorter than its modulus.

B. QRNGs

Based on both theoretical principles and a huge body of striking experimental evidence, quantum mechanical processes are believed to be inherently random. Therefore, in contra-position to the classical devices generating random numbers by extracting and manipulating entropy from physical processes, such as thermal noise (whose apparent randomness comes from the lack of knowledge of the internal state of a certain physical system rather than true unpredictability) and algorithmic PRNGs, QRNGs offer the only known way to produce truly unpredictable random numbers. Their randomness can be certified by means of a Bell test[9] and has so far thoroughly passed all the most stringent ones, with device-independent quantum information processing (DIQIP) generators even achieving loophole-free certification.[10]

Several methods to harness such quantum randomness have been proposed and realized into actual QRNGs. The so-called "certified randomness"[10] can be obtained by means of device-independent quantum information processing (DIQIP) randomness protocols, which employ Bell-inequality violation on systems of photons,[11,12] ions,[13] nitrogen-vacancy centers,[14] neutral atoms,[15] and superconducting qubits.[16] Nevertheless, DIQIP approaches are not particularly efficient in terms of bit-rate generation as they often rely on measuring the properties of few-particle systems.[17] For practical reasons, then it is useful to measure signals from quantum processes and subsequently extract their randomness with classical devices. These involve devices to observe the timing of nuclear decay,[18] electron shot noise in semiconductors, splitting of photons on beam-splitters, timing of photon arrivals, vacuum fluctuations, laser phase diffusion, amplified spontaneous emission, Raman scattering, atomic spin diffusion, and others. For a review on the topic, see Ref. 17.

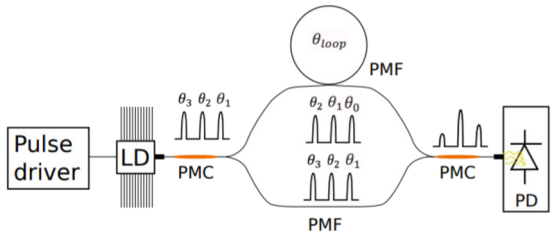

FIG. 1. Scheme of Quside's PD-QRNG used in this work. A laser is modulated above and below threshold, each time generating a pulse with a random phase θ_i. By means of an unbalanced Mach–Zehnder interferometer, each pulse is interfered with a later generated random phase pulse, turning phase fluctuations into intensity fluctuations, which are further converted into random numbers by using conventional photodetectors and electronics. Reproduced with permission from Abellán *et al.*, Opt. Express **22**, 1645 (2014). Copyright 2014 Optica.[19]

The fastest quantum random number generators available today make use of macroscopic traces of processes of a quantum origin, such as laser phase diffusion (PD) QRNGs,[19–22] whose behavior is understood solely from a quantum-mechanical perspective.[23] Such fast QRNGs have reached record generation speeds on the order of a 100 Gbps[24,25] at the time of writing.

It is not the intention of the present paper to discuss the advantages and disadvantages of each type of QRNG, so for an in-depth discussion, the interested reader is referred to Ref. 17 and the references to each example. On the contrary, our main purpose is to see and compare the effects that the potentially hidden correlations within random or pseudo-random streams can have in some physical MC simulations, and thus, by assuming that all types of QRNGs are indeed random, their output streams should be indistinguishable under this paper's perspective. Due to time constraints, we will restrict our analysis to that of a fast PD-based QRNG, whose functioning is sketched in Fig. 1.

C. The dynamic critical exponent

Consider a system comprised by a set of N Ising spins $\sigma_i = \pm 1$ arranged on a two-dimensional square lattice of linear side L, such that $N = L^2$. Spins are coupled by means of the coupling coefficient J_{ij}. We consider only the coupling to nearest neighbors and $J_{ij} = J$ constant for all pairs of spins. The Hamiltonian that describes the statics and thermodynamics of this system is therefore

$$H = -\sum_{i,j} J_{ij}\sigma_i\sigma_j = -J\sum_{\langle i,j\rangle} \sigma_i\sigma_j, \tag{4}$$

where the sum of the term on the right is restricted to the nearest neighbors and $1 \le i,j \le L$. This model is commonly used to study the behavior of ferromagnetic materials; for this purpose, periodic

04 December 2025 19:44:04

© Author(s) 2024

boundary conditions are typically used, simulating a square unit cell of size L within the periodic system under study.

The model describes the transition between the two phases of a simple ferromagnetic material: at low temperatures, most of the spins are aligned in the same direction, resulting in non-zero magnetization and ferromagnetic behavior of the material at macroscopic scales; on the contrary, at high temperatures, the fluctuations of the spins associated with thermal effects exceed the ferromagnetic order induced by the Hamiltonian; in this scenario, the spins act independently, generating zero average magnetization and thus making the material paramagnetic. The phase transition occurs when the system reaches the so-called critical temperature T_c; at this temperature, the domains of high magnetization in one direction are gradually destroyed by the effect of thermodynamic fluctuations and converted into zones of high magnetization in the opposite direction. Then, macroscopically, the system is magnetized, but the orientation of the magnetic field changes in time. This behavior is illustrated in Fig. 2. The time-delayed correlation of the order parameter (magnetization) is

$$\chi(t) = \langle M(t)M(0)\rangle = \sum_k a_k e^{-t/\tau_k}, \tag{5}$$

where the sum over k runs over the system's excited modes,[26] M is the system's magnetization, $\tau_k = 1/\lambda_k$ is the relaxation time for the kth excited mode, which has eigenvalue λ_k, and a_k are t-independent constants. The probability of finding the system at configuration σ at time t for some initial configuration being σ_0 can be solved to be $P(\sigma, t|\sigma_0) = \sum_{k=0}^{\infty} c_k(\sigma_0)e^{-\lambda_k t}\phi_k(\sigma)$, with $\phi_k(\sigma)$ being the eigenmode with eigenvalue λ_k with standard methods (see Ref. 26 for one dimension and via the master equation and more general methods in Refs. 27 and 28).

If the system is truly infinite, at the temperature approaching the critical temperature T_c, the relaxation times τ_k diverge, leading to the "critical slowing down" effect. The dynamic critical scaling hypothesis[27–32] predicts that diverging τ_k have a power-law dependence on the diverging static correlation length ξ, which scales as $\xi \propto |T - T_c|^{-\nu}$. We define then the dynamic exponent z as

$$\tau_k \propto \xi^z. \tag{6}$$

Since all τ_k diverge, the relaxation process is dominated by the first excited mode with τ_1. This one effectively determines the relaxation time of the system $\tau = \tau_1$ of the whole system so that

$$\chi(t) = \langle M(t)M(0)\rangle \propto e^{-t/\tau}. \tag{7}$$

In practice, we deal with finite systems of size $L^2 \propto M^2 = N$. This means that at T_c, the static correlation ξ grows, achieving the longest wavelength $\lambda_{\max} \simeq L$. The relaxation time of the system is then expected to have a power-law relation with $\lambda_{\max}$, i.e., for finite size scaling (FSS),

$$\tau_{\mathrm{FSS}}(L) \propto L^z. \tag{8}$$

Combining the above equations, one can determine the relaxation times and exponent z of finite Ising lattices from Monte Carlo simulations of kinetic models, as first suggested by Hohenberg and Halperin.[30]

D. Measuring z in MC simulations

In order to measure the dynamic critical exponent, we perform MC simulations of the Hamiltonian [Eq. (4)] and compute its magnetization after each MC step. We run the simulations for different lattice sizes L and for a total of 1300τ time steps (where we approximate $\tau \approx L^2$) to ensure a proper decay of the correlation function that enables us to extract the relaxation time of the system. We then determine τ by fitting the obtained results for each lattice size with a decaying exponential within the time interval $t \in (0.3\tau_{FSS}, 1.1\tau_{FSS})$, again using $\tau_{FSS} = L^2$. This strategy allows us to avoid both the initial high non-linearities and the fluctuations in the tail of the exponential, as discussed in Ref. 2. Finally, we plot the obtained $\tau(L)$ in a logarithmic scale as a function of the lattice size to obtain the dynamic exponent z by means of a linear fit.

In order to obtain statistically relevant results, we compute the mean value and the variance of the dynamic critical exponent from a total of N_{it} iterations for each lattice size, which are initialized with different random seeds.

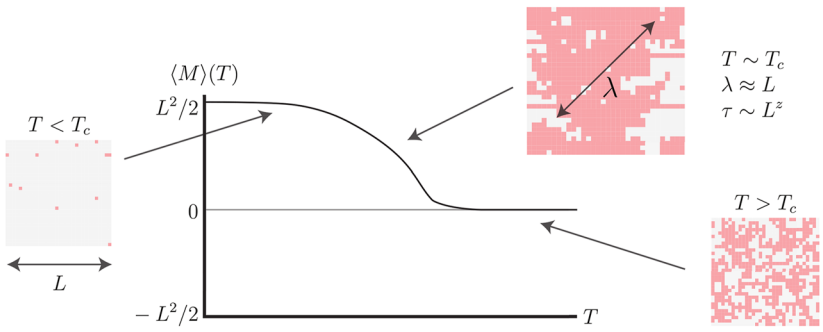

FIG. 2. 2D Ising model dynamics. For temperatures below the critical temperature, T_c, the system is in an ordered state and, thus, shows ferromagnetic behavior; for temperatures larger than T_c, the system is in a disordered state and, thus, does not show any spontaneous magnetization. At T_c, the system shows a phase transition (see main text for details).

04 December 2025 19:44:04

© Author(s) 2024

III. RESULTS

A. The dynamic critical exponent in the literature

We start this section by presenting a review and discussion of previous studies. Over the years, many attempts to give an appropriate value for the dynamic critical exponent z have been carried on from theoretical,[33–44] experimental,[45–49] and computational[50–72] approaches. Here, with the aim of illustrating how vastly the obtained results vary, we present a long, yet possibly non-exhaustive collection of values found in the literature for both two- and three-dimensional lattices. Some of the references presented here give various values corresponding to different types of lattices in an attempt to show the postulated universality of z across models. We plot in the top panel of Fig. 3 the obtained exponents as a function of the year of its calculation. Surprisingly, even with the expected improvement of the used methods, there is no clear tendency, neither in two-, three-dimension, theoretical, or MC calculations, and even the various results obtained in recent years show a wide spreading. The data are gathered in Tables VI and VII from Appendix C. We plot in the bottom panel of Fig. 3(a) histogram grouping the theoretical predictions and the MC ones. While the values obtained by means of theoretical methods do not show any apparent distribution, the ones obtained with MC calculations can be fitted to a Gaussian distribution with mean $\langle z_{\mathrm{MC}} \rangle = 2.1664$.

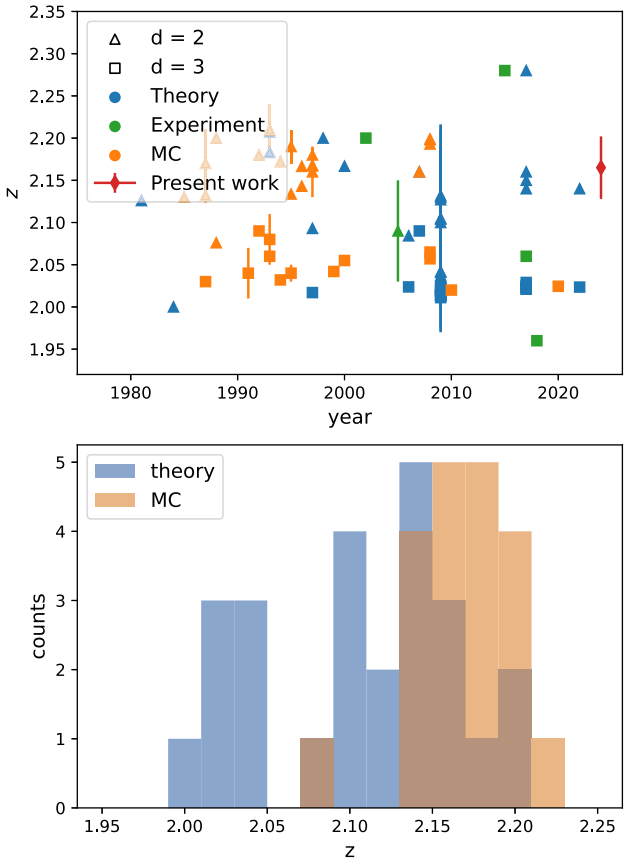

FIG. 3. Dynamic critical exponents given in the literature. Top: Different z calculated over the years in two and three dimensions. Triangles and squares label two- and three-dimensional lattices, while colors blue, green, and orange mark whether these values were obtained theoretically, experimentally, or via MC simulations, respectively. The value obtained in Sec. III C of the present work by MC methods using a QRNG is marked with a red diamond. Bottom: Histogram showing the z predictions theoretically and with MC in two dimensions.

B. Detecting correlations in PRNGs

We begin this paper's contributions by exploring how does the dynamic critical exponent vary when computing it with a collection of different LCGs, all of them presumably showing low correlations.[7] The modulus, parameter, and increment used for each LCG are resumed in Table I.

Following the procedure discussed in Sec. II D, we run the simulations for the following lattice sizes: $L = \{4, 8, 16, 32, 64, 128, 256, 512\}$. Since we use $1300L^{\tau}$ MC time steps and approximate $\tau \approx 2$, the computation times increase as $t \propto L^2$, and we thus restrict our number of iterations to $N_{it} = 1000$ for sizes ranging from $L = 4$ to $L = 64$, $N_{it} = 500$ for $L = 128$ and $L = 256$, and $N_{it} = 10$ for $L = 512$.

As a final remark, we run these simulations in a graphics processing unit (GPU). This fact, besides shorter simulation times, effectively further lowers the correlations that the PRNGs show. This is done by means of a kernel that, given L^2 different states x_n, yields L^2 new states X_{n+1} such that each spin within the lattice works with its own PRNG (all of them implementing the same LCG and initialized with different random seeds).

1. Fundamental tests

The procedure explained above is applied to the discussed Hamiltonian [Eq. (4)] for each of the PRNGs in Table I. We then compare them with the theoretical estimate of z obtained by studying the stochastic matrices governing the physics of our system in the classical Ref. 39, that is, $z = 2.1667 \pm 0.0005$, since it is also the most

TABLE I. Parameters of each of the linear congruential generators used in the PRNG simulations.

	Modulus	Multiplier	Increment
PRNG0	$2^{32}-1$	16 807	0
PRNG1	$2^{25}-39$	12 836 191	0
PRNG2	$2^{23}-15$	422 527	0
PRNG3	$2^{17}-1$	43 165	0

TABLE II. Dynamic exponents z and relative errors with respect to theoretical estimate ϵ_r, obtained for each PRNG.

	z	ϵ_r
PRNG0	2.1087	0.0268
PRNG1	2.1159	0.0234
PRNG2	2.1047	0.0286
PRNG3	2.1162	0.0233

04 December 2025 19:44:04

© Author(s) 2024

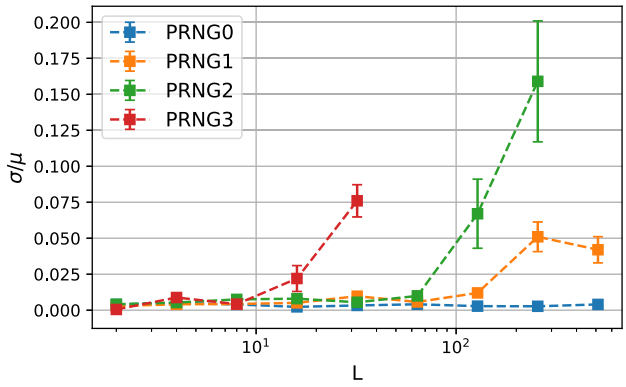

FIG. 4. Statistical variance of the dynamic exponent z, normalized to its mean value, as a function of lattice size for different PRNGs. The reduced variance drastically increases when the simulations demand an amount of random numbers greater than the PRNG's period of repetition.

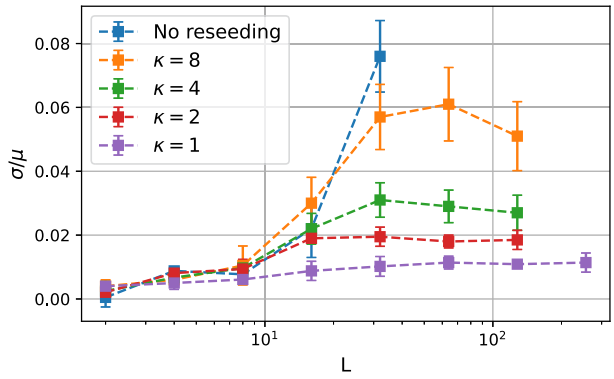

FIG. 5. Normalized variance for PRNG3 as a function of lattice size, with reseeding. Physical reseeding of the generator every $(m-1)$, $2(m-1)$, $4(m-1)$, and $8(m-1)$ random numbers. PRNG3 without reseeding is shown for comparison. The variance explosion is avoided in all cases, reaching a value that depends on the frequency of the reseeding.

similar one to the mean value found with MC approaches in the literature, as seen in Sec. III A. We summarize our results in Table II, in which we show the obtained dynamic exponents z, as well as their respective errors relative to the theoretical estimate, ϵ_r (we take as reference $z_{\text{ref}} = 2.1667$ and approximate ϵ_r to the fourth decimal).

All tested PRNGs yield a reasonable approximation of the dynamic exponent, as can be seen in Table II, but they differ in their predicted value in the second significant decimal.

Importantly, the statistical variance of the results poses a considerable caveat that must be taken into account when interpreting them. For any given PRNG, once the amount of random numbers consumed by the algorithm exceeds its period of repetition (modulus in Table I), the sequence repeats itself, introducing a large amount of correlation at large time scales. We observe that these extra correlations affect the obtained dynamic exponent by exponentially enlarging the variance between iterations of the same simulation while keeping its mean value constant. To quantify these correlations, we define the normalized variance as σ^2/μ^2, where σ is the variance of the results and μ is their mean value. For this case, the normalized variance stays more or less constant (around a value of $\frac{\sigma^2}{\mu^2} \approx 0.01$) until the lattice reaches a size large enough so that its simulation requires more random numbers than the generator's period of repetition. Beyond this point, the variance starts to increase exponentially with lattice size, as shown in Fig. 4. In this figure showing the normalized variance (and in the following ones in which we plot this parameter), the error bars are computed as the fourth moment of the N_{it} values of each dynamic critical exponent.

Furthermore, as we keep increasing L far beyond the variance's explosion point, the obtained magnetization auto-correlation function $\chi(t)$ no longer resembles an exponential decay but instead starts showing a noisy behavior. Therefore, one cannot strictly speak of, nor extract, a reliable value for the dynamic exponent.

2. Effects of reseeding

After observing that repeating random sequences greatly affects the results obtained with PRNGs, we explore the effects that the reseeding operation discussed above has on them. In our case, when we reseed our generators, we replace the whole input x_{i-1} with a new true random number obtained from the computer's physical entropy source. Besides the reseeding, the parameters and procedures of all the simulations remain unchanged.

We first take a look at the normalized variance obtained by PRNG3, since it is the one with the shortest period of repetition. We reseed it every $\kappa(m-1)$ pseudo-random numbers, where m is the modulus parameter of the LCG, and we first consider $\kappa = \{1, 2, 4, 8\}$. As shown in Fig. 5, we find that for all cases, the variance explosion observed before is avoided. In this case, the normalized variance does not grow monotonically but instead reaches a plateau whose value appears to be proportional to the number of repetitions introduced in the pseudo-random sequences before the reseeding is carried out (i.e., the amount of extra correlations introduced in our algorithm, compared to the infinite-period PRNG).

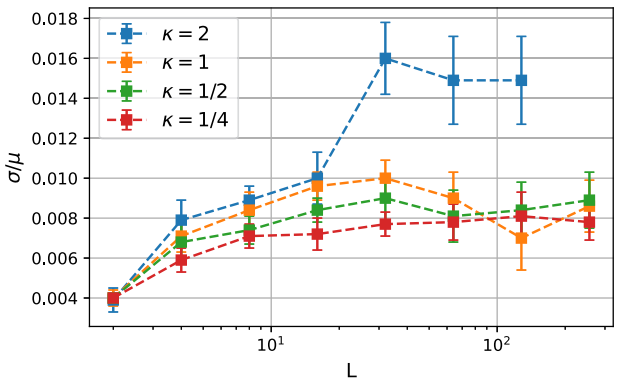

FIG. 6. Normalized variance for PRNG3 as a function of lattice size, with high frequency reseeding. Physical reseeding of the generator every $2(m-1)$, $(m-1)$, $\frac{(m-1)}{2}$, and $\frac{(m-1)}{4}$ random numbers. Beyond that point, the error bars do not allow us to distinguish the results for higher reseeding frequencies. The value of the variance's plateaus is further reduced at high frequencies.

04 December 2025 19:44:04

© Author(s) 2024

As shown in Fig. 5, the case $\kappa = 1$, i.e., an example of an infinite-period pseudo-random number generator, exhibits the lowest normalized variance of all presented cases. Interestingly, by allowing $\kappa < 1$ (and thus paying the computational cost associated with a high-frequency reseeding), we observe that we can still lower this value further down (see Fig. 6). This scenario minimizes the correlations appearing in the pseudo-random sequences, approaching a true RNG (TRNG) as κ gets smaller. Therefore, this fact allows us to conclude that *the use of PRNGs, even those showing low correlations and having a theoretically infinite period, can indeed affect the quality of our results in terms of variance* for the problem at hand. Moreover, as we show here, once κ is fixed, the variance of the obtained z converges to a plateau and barely changes with L. Hence, performing longer simulations will not improve the approximation.

Next, we extract the values of the reduced variance plateaus and plot them as a function of the reseeding period κ. Interestingly, as shown in Fig. 7, both quantities show a linear relation. By means of a linear fitting, we then can extrapolate the reduced variance for $\kappa = 0$, that is, the case of a TRNG. We obtain a value of $\frac{\sigma^2}{\mu^2}(\kappa = 0) = 0.0044 \pm 0.0027$ (corresponding to a 95% confidence level). Note that this value coincides with the initial points of the curves of Figs. 5 and 6, corresponding to simulations of very small latices, where correlations between pseudo-random numbers are still non-detectable.

On top of the presented effect on the variance of the estimation of the dynamic exponent z, we also analyze its mean value for different κ. We observe that the reseeding of the generators yields a more accurate result for the mean value of the dynamic exponent (see Table III). We note that for every case with reseeding and for every frequency κ implemented, the relative error to the theoretical reference value is reduced to about half the one obtained with the different PRNGs used in Table II, which were not reseeded. Nevertheless, we cannot reduce this error further. We emphasize that reducing κ reduces the variance, bringing the result closer to those of a TRNG, but at a larger computational cost for smaller and smaller κ. The results here point out that in the limit of very small κ, one should obtain results close to those obtained with a TRNG. Nonetheless, there is no practical way of testing this due to the large computational cost of reseeding from the system's entropy source.

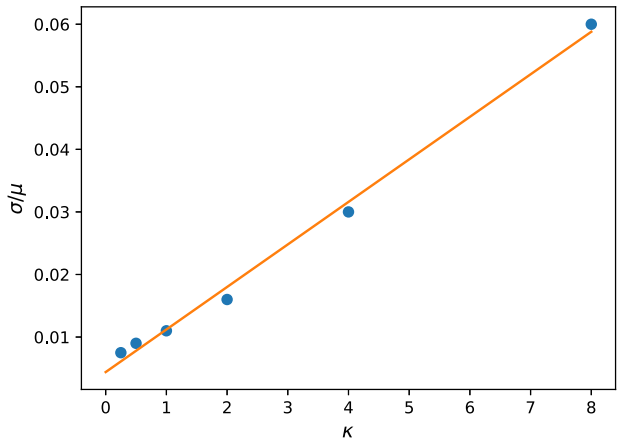

FIG. 7. Reduced variance for different values of the reseeding period κ of PRNG3 (dots) and linear fit (line). The extrapolated value for a TRNG is $\frac{\sigma^2}{\mu^2}(\kappa = 0) = 0.0044 \pm 0.0027$.

TABLE III. Dynamic exponents z and relative errors with respect to theoretical estimate ϵ_r for different reseeding frequencies of PRNG3.

	z	ϵ_r
$\kappa = 2$	2.1815	0.0068
$\kappa = 1$	2.1477	0.0088
$\kappa = \frac{1}{2}$	2.1482	0.0085
$\kappa = \frac{1}{4}$	2.1441	0.0104

3. Reseeded PRNGs against NIST tests

We tested the PRNGs using the NIST statistical test suite[73] and observed that while those having repeated sequences do not pass it, we are able to decrease the number of failed tests within the suite, until eventually making it pass all of them for sufficiently high reseeding frequencies. PRNG0 already passed the tests without reseeding, while PRNG1 and PRNG2 only needed reseeding with $\kappa = 1$. On the other hand, PRNG3 needed $\kappa = \frac{1}{16}$ as it was usually failing, out of more than 200 different tests within the suite, only one of them after being reseeded with $\kappa = 1$ (the FFT test).

One should therefore note two facts. On the one hand, all PRNGs are able to pass NIST tests, and on the other one, we can still see improvement in the variance of the results when further reducing κ. These two observations lead to the conclusion that this protocol is able to distinguish between pseudo-random sequences containing different amounts of randomness amplification, that is, that have used more or less extensively the PRNG's algorithm (so that their next outcome can be predicted with a higher or lower probability) and to therefore identify which one is closer to a true RNG. In addition, this should be more noticeable as larger lattices are employed.

The variance in the obtained results in this kind of physical simulation can therefore be used as an additional randomness test since it is affected by some correlations that NIST tests are not able to detect.

C. Calculation of the dynamic critical exponent z with a QRNG

In this section, we present the results of the calculation of the dynamic critical exponent using a Field-Programmable Gate Array (FPGA) and, most importantly, a Quantum Random Number Generator (QRNG). As in Sec. III B, we performed simulations for different lattice sizes. In Fig. 8, we show the time-delayed correlation of the order parameter (magnetization), $\chi(t)$, as a function of time. We see the expected exponential decay described by Eq. (7). By fitting the previous equation, we extract the average value of the exponent τ for each L. We performed 100 simulations for L up to 256 and 15 simulations for $L = 512$ due to the large computational cost in this last case (see discussion below). It is very apparent from the last panel in Fig. 8 that the results for $L = 512$ are more noisy than those obtained for smaller lattice sizes, a fact that we associate with the smaller number of simulations.

04 December 2025 19:44:04

© Author(s) 2024

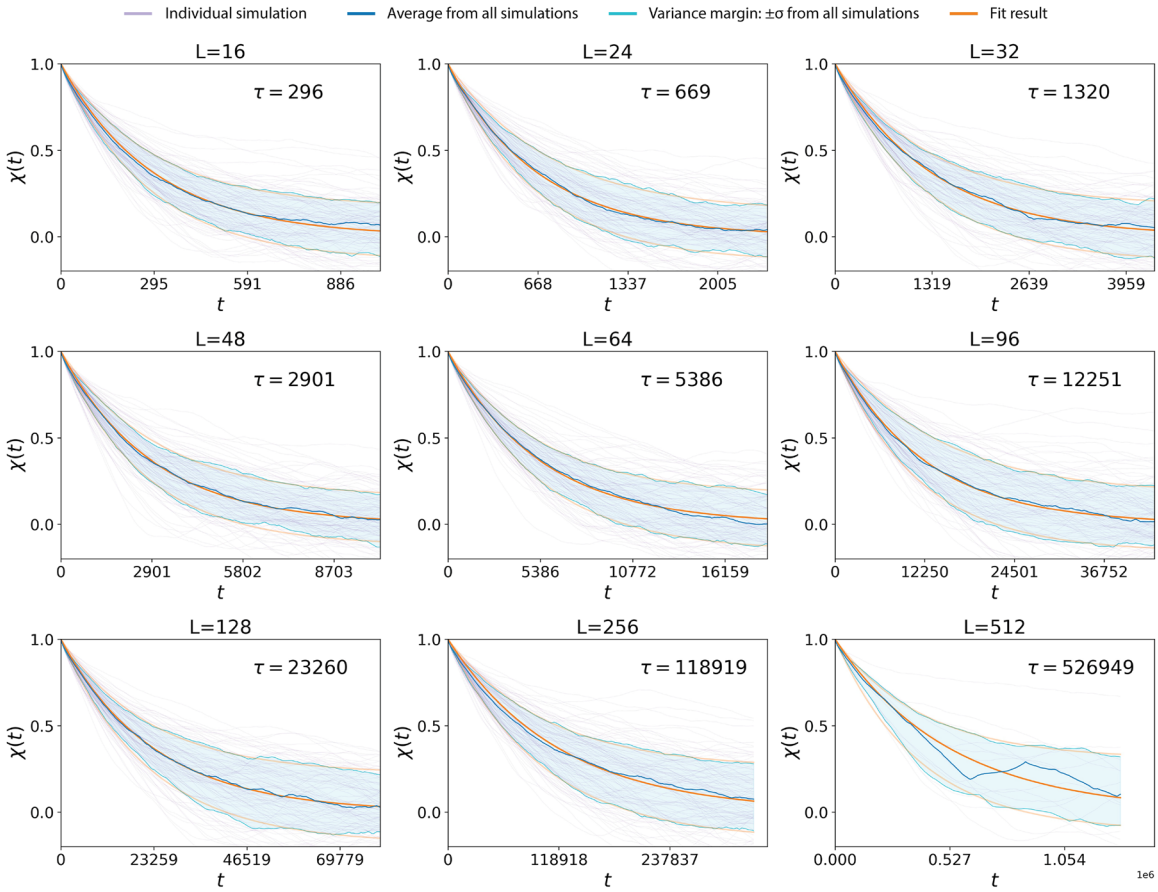

FIG. 8. Determination of the relaxation time as a function of lattice size. Inset τ values are the decay times associated with the orange curves, which correspond to the averages obtained by the fitting of the multiple repetitions simulated at each side length. The individual simulations (purple) as well as the variance interval for all of them (cyan) are also shown in the graphs.

In Fig. 9, we represent the average correlation time $\tau(L)$ obtained from these results. Performing a linear fitting of the obtained curve, we find a value of the critical exponent $z = 2.165 \pm 0.039$. We emphasize that, from here, there is a clear strategy to improve this value: performing multiple simulations for bigger lattices would add more points to the fit, resulting in a better approximation of this coefficient. However, unlike the case of pseudo-generators, obtaining correlation times for larger cell sizes is limited by the vast need for random numbers required by the simulation. Note that for each step of the simulation, $N \propto L^2$ random numbers are required. As the simulations are run for $1300\tau_k = 1300L^z$ steps, we require on the order of $1300L^{z+2}$ random numbers. Assuming that each of these numbers has 32-bit precision, we face a massive consumption of about $41\,600 \cdot L^{z+2}$ randomly distributed bits. For small cell sizes, these requirements are innocuous; however, the $\sim L^4$ exponential growth in demand for random numbers is prohibitive.

In order to avoid this computational bottleneck and to speed-up the simulations, we used an amplification of the QRNG's random numbers in the $L = 512$ case. This amplification consists of the implementation of a PRNG on the FPGA, which is reseeded as fast as

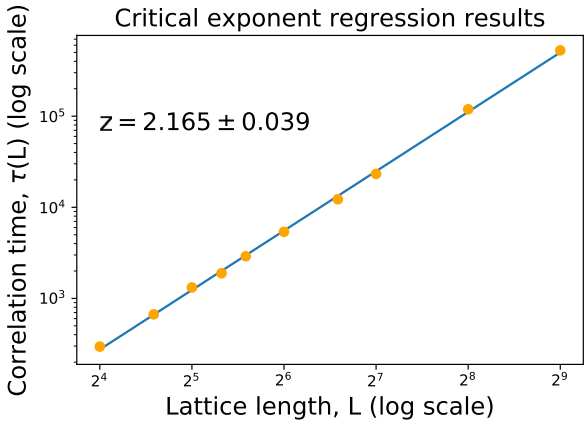

FIG. 9. Critical exponent calculation with a quantum random number source. Orange: estimated relaxation times (in log 10 scale) as a function of the lattice size (in log 2 scale); blue: the linear fitting $\log_2(\tau) = z \cdot \log_2(L) + b$ associated. The slope of the fitting $z = 2.165 \pm 0.039$ corresponds to the critical exponent, in agreement with theoretical results.

04 December 2025 19:44:04

© Author(s) 2024

the QRNG provides new seeds. This decision introduces some correlations that are not present for smaller lattices. This fact, along with the very low number of repetitions, could potentially be the reason of the more noisy behavior observed in the last panel of Fig. 8, as discussed in Sec. II A. Nevertheless, due to the small size of the statistical sample at hand, we cannot conclude which one of them is the predominant reason without additional simulations.

D. Comparison with other standard randomness tests

Finally, we compare the results obtained by all the considered (pseudo-) random number generators used throughout this work in the standard randomness NIST SP800-22 statistical tests.[73]

In Fig. 10 we show the violin plots of the NIST tests' results obtained with all the considered PRNGs with high frequency reseeding (with seeds obtained from the hardware's physical entropy and using $\kappa = 1$), together with the QRNG, to illustrate how these are distributed. The ordinate axis labels the percentage of passed tests, while a wider figure indicates that a bigger proportion of tests obtain results within that ordinate value when using that particular generator. We observe that PRNG0 and PRNG3 obtain clearly worse results than the other ones as their violin plots' tails extend all the way below the expected failure rate $\alpha = 0.01$. In contrast, PRNG1 and PRNG2 show a distribution that is localized around the expected failure rate. Moreover, this distribution strikingly resembles that of the QRNG. The bad results obtained by PRNG3 are easily explained by the fact that even with a high frequency reseeding, its period of repetition is short enough for the NIST tests to catch the inner correlations. Contrarily, the explanation for the bad results of PRNG0, which has the longest period of repetition among all of them, is more subtle and can indicate that its inner correlations are more apparent to the NIST tests than those present in other generators. While those inner correlations are not seen to affect the computation of the dynamic exponent as those present in PRNG1, PRNG2, and PRNG3 (see Fig. 4), the correlation shown by these first two, which indeed affect the variance in z, seem to pass unseen under the NIST SP800-22 tests. We thus conclude that there are certain types of correlations that can be detected with standard methods but not with the present one, and vice versa, so that both strategies can be jointly considered in order to improve the set of randomness tests. Furthermore, it is important to stress on the fact that the computation of the dynamic exponent is affected by the correlations present in some generators that are, from the NIST SP800-22 STS perspective, indistinguishable from a QRNG.

IV. CONCLUSIONS AND OUTLOOK

In this work, we have computed the dynamic critical exponent z of the two-dimensional Ising lattice with Monte Carlo simulations using a pool of different pseudo-random number generators. These range from poor ones showing lots of correlations to ones using high-frequency reseeding that are thus similar in quality to a true physical RNG and even a QRNG whose output streams are completely uncorrelated.

We also review the literature and observe that there is a huge spread within the values obtained by different techniques, not showing any convergence with different theoretical approaches. Since the MC studies do show some convergence to a value that seems close to the one obtained by one of such theoretical approaches (studying the stochastic matrices that govern the physics of the considered system), we take this value as a reference. We then show how its value obtained via MC simulations is affected by the quality of the random number streams used in it (that is, as compared to a set of truly uncorrelated ones). On the one hand, its mean value appears to be slightly affected by the RNG used, and better ones yield a value closer to the one we take as a reference. On the other hand, the impact of the quality of the RNGs on the variance of the results does appear to be dramatically noticeable. We extrapolate the variance that a TRNG would yield and, since the applied standard randomness tests are not able to distinguish some of the PRNGs used, hypothesize that this limiting value of the variance could be used in the future as an additional randomness test. Faster QRNGs are still needed to test this hypothesis, which could potentially yield an advantage of these quantum randomness technologies over classical ones, not on speed but on quality of the obtained results in the large lattice limit $L \to \infty$.

Given the fact that the value of the dynamic critical exponent is affected by the quality of the randomness source used, another

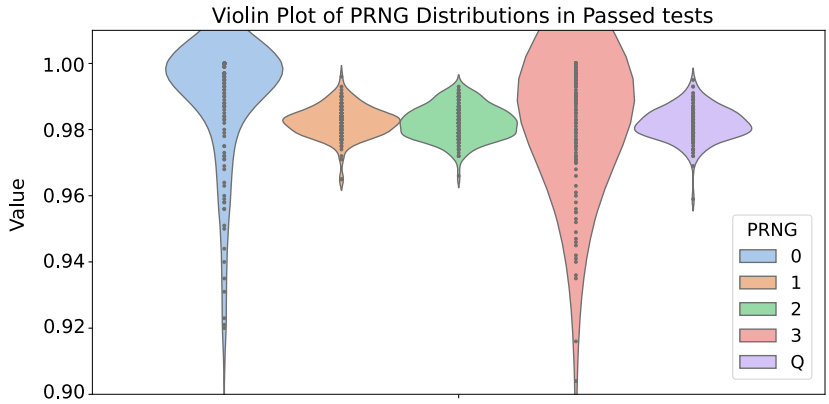

FIG. 10. Violin plots of the randomness tests passed by all the PRNGs and the QRNG. While PRNG0 and PRNG3 obtain clearly worse results than the other ones, PRNG1 and PRNG2 are indistinguishable from the QRNG.

04 December 2025 19:44:04

© Author(s) 2024

important output of this work is the fact that it constitutes, to the best of our knowledge, the first computation of it using a QRNG. The value obtained is actually close to the reference value considered in the reviewing of Sec. III A. While only one QRNG has been tested (a phase diffusion based QRNG), under the assumption of these kinds of randomness technologies producing true random numbers, the results of the present work should not be affected by the actual technology used to produce them (nuclear decay, splitting of photons in beam-splitters, etc.). Still, once such other technologies are able to reach fast enough output speeds, it would anyway be interesting to test this.

ACKNOWLEDGMENTS

We dedicate this work to the memory of Roy J. Glauber and Fritz Haake, once the Masters of Kinetic Ising Models.

We acknowledge Joana Fraxanet, Lluis Torner, Sergi Ferrando, Pau Gómez, Felix Tebbenjohanns, and Carlos Abellán. We also acknowledge discussions with Josep Maria Martorell, Mervi Mantsinen, Xavier Saez, Vassil Alexandrov, Francisco Castejón, and Shinsuke Satake in the early stage of this project. We acknowledge ERC AdG NOQIA; MCIN/AEI (PGC2018-0910.13039/501100011033, CEX2019-000910-S/10.13039/501100011033, Plan National FIDEUA PID2019-106901GB-I00, Plan National STAMEENA PID2022-139099NB, I00, project funded by MCIN/AEI/10.13039/501100011033 and by the "European Union NextGenerationEU/PRTR" (PRTR-C17.I1), FPI); QUANTERA MAQS PCI2019-111828-2; QUANTERA DYNAMITE PCI2022-132919, QuantERA II Program co-funded by European Union's Horizon 2020 program under Grant Agreement No. 101017733; Ministry for Digital Transformation and of Civil Service of the Spanish Government through the QUANTUM ENIA project call - Quantum Spain project, and by the European Union through the Recovery, Transformation and Resilience Plan - NextGenerationEU within the framework of the Digital Spain 2026 Agenda; Fundació Cellex; Fundació Mir-Puig; Generalitat de Catalunya (European Social Fund FEDER and CERCA program, AGAUR Grant No. 2021 SGR 01452, QuantumCAT U16-011424, co-funded by ERDF Operational Program of Catalonia 2014-2020); Barcelona Supercomputing Center MareNostrum (FI-2023-3-0024), funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union, European Commission, European Climate, Infrastructure and Environment Executive Agency (CINEA), or any other granting authority. Neither the European Union nor any granting authority can be held responsible for them (HORIZON-CL4-2022-QUANTUM-02-SGA PASQuanS2.1, 101113690, EU Horizon 2020 FET-OPEN OPTOlogic, Grant No 899794), EU Horizon Europe Program (This project has received funding from the European Union's Horizon Europe research and innovation program under Grant Agreement No. 101080086 NeQST Grant Agreement No. 101080086—NeQST); ICFO Internal "QuantumGaudi" project; European Union's Horizon 2020 program under the Marie Skłodowska-Curie Grant Agreement No. 847648; "La Caixa" Junior Leaders fellowships, La Caixa" Foundation (ID 100010434): CF/BQ/PR23/11980043. D.C.G. acknowledges funding from Generalitat de Catalunya (AGAUR Doctorats Industrials 2019, 2n termini). MAGM acknowledges funding from the Spanish Ministry of Education and Professional Training (MEFP) through the Beatriz Galindo program 2018 (BEAGAL18/00203). G.M.-G. acknowledges funding from the European Union.

AUTHOR DECLARATIONS

Conflict of Interest

The authors have no conflicts to disclose.

Author Contributions

David Cirauqui: Investigation (equal); Software (equal); Writing – original draft (equal); Writing – review & editing (equal). **Miguel Ángel García-March**: Conceptualization (equal); Investigation (supporting); Writing – original draft (equal); Writing – review & editing (equal). **Guillem Guigó Corominas**: Writing – original draft (supporting); Writing – review & editing (supporting). **Tobias Graß**: Investigation (supporting); Visualization (supporting). **Przemysław R. Grzybowski**: Investigation (supporting); Supervision (equal); Writing – review & editing (equal). **Gorka Muñoz-Gil**: Investigation (supporting); Writing – review & editing (supporting). **J. R. M. Saavedra**: Conceptualization (equal); Funding acquisition (equal); Investigation (supporting); Software (equal); Supervision (equal); Writing – review & editing (equal). **Maciej Lewenstein**: Conceptualization (equal); Funding acquisition (equal); Investigation (lead); Supervision (equal); Writing – original draft (supporting); Writing – review & editing (supporting).

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

APPENDIX A: PARALLELIZATION USING FPGAs/GPUs: RANDOMNESS CONSUMPTION

Note that our code runs over every single spin at any time step. This updating process differs from other possible implementations of the Metropolis algorithm that rely on sequential updates such as sampling and updating L^2 (with L the lattice size) spins for each iteration, with the spins selected at random. Such a sequential implementation does not guarantee that all of the spins will be given the chance of being updated, nor that all of them will be updated only once in each Monte Carlo sweep (even if it does satisfy ergodicity in the long run). This fact does not make a difference in the obtained results[74] but yields a considerable improvement in performance when using the parallel Metropolis version. Not only it allows the spins to be updated in a parallel manner but also it reduces the entropy consumption of the algorithm since the it does not require such L^2 random numbers at every time step that chooses the spins to be updated. On the other hand, our implementation assumes that every single spin might be asked to flip with a certain probability following the Metropolis algorithm, thus consuming again L^2 random numbers, while a CPU-based code would only need a fraction $\alpha \leq 1$ of them, corresponding to these spins that are not flipped

04 December 2025 19:44:04

© Author(s) 2024

TABLE IV. Estimated randomness consumption.

L	MC updates/ simulation	N_{it}	Random bits/ update	Total bits required (GB)
16	533 192	100	512	3.2
24	1 285 292	100	1152	17.2
32	2 399 489	100	2048	57.2
48	5 784 114	100	4608	310.3
64	10 798 263	100	8192	1029.8
96	26 029 866	100	18 432	5585.4
128	48 594 709	100	32 768	18 537.4
256	218 687 559	100	131 072	333 690.7
512	984 145 175	10	524 288	600 674.5
			TOTAL	959 905.8

directly after computing its energy difference between both initial and proposed states.

Taking everything into account, a sequential algorithm consumes $n_{\text{seq}} = L^2(1+\alpha)$ random numbers at every time step, while the parallel one only demands $n_{\text{par}} = L^2$, which equals the best lower bound achievable with a sequential device. In this direction, our code could be further optimized in order to avoid the discard of the $L^2(1-\alpha)$ numbers that are not used in the previous iteration, replacing these ones consumed and therefore yielding a much lower demand of $n_{\text{par}} = L^2\alpha$.

In Table IV, we estimate the amount of randomness consumed by each simulation assuming $N_{\text{it}} = 100$.

When implementing the code in a GPU, we note that, given the availability of GPU resources, the possible optimization of the PRN generation introduced in previous paragraph would not yield any improvement. It is also worth noting that such optimization would introduce even more correlations in the results: by possibly discarding some random numbers, we indeed lower the correlation between the probabilities used by a given spin to be updated at two different times.

TABLE V. Results obtained for $\log(\tau_0)$ by using different RNGs. These values correspond to the fittings yielding the dynamic exponents shown in Secs. III B and III C.

	$\log(\tau_0)$
QRNG	−0.362
PRNG3 $k = \frac{1}{2}$	−0.1701
PRNG3 $k = 2$	−0.2454
PRNG2	−0.0906
PRNG0	−0.1007
PRNG1	−0.1183

TABLE VI. All calculated exponents from the literature in two dimensions, to the best of our knowledge. The TP and hc signs indicate that the results are obtained for triangular and honeycomb lattices, respectively, while square lattices are used if nothing is explicitly stated.

Year	References	Method	z
1981	Bausch	Theory	2.126
1984	Domany	Theory	2
1985	Williams	MC	2.13 (3)
1987	Ito	MC	2.132 ± 0.008
1987	Tang	MC	2.17 ± 0.04
1988	Ito	MC	2.2
1988	Mori	MC	2.076 ± 0.005
1992	Stauffer	MC	2.18
1993	Dammann	Theory	2.183 ± 0.005
1993	Wang	Theory	2.207 ± 0.008
1993	Muenkel	MC	2.21 ± 0.03
1994	Grassberger	MC	2.172 ± 0.006
1995	Gropengiesser	MC	2.18 ± 0.02
1995	Li	MC	2.1337 (41)
1996	Li	MC	2.143 (5)
1996	Nightingale	MC	2.1665 (12)
1997	Soares	MC	2.16 ± 0.03
1997	Wang	MC	2.168 ± 0.005
1997	Wang	MC	2.180 ± 0.009, TP
1997	Wang	MC	2.167 ± 0.008, hc
1997	Prudnikov	Theory	2.093
1998	Wang	Theory	2.2
2000	Nightingale	Theory	2.1667 ± 0.0005
2005	Dunlavy	Experiment	2.09 ± 0.06
2006	Krinitsyin	Theory	2.0842 ± 0.0039
2007	Canet	Theory	2.16 (1)
2007	Lei	MC	2.16
2008	Murase	MC	2.193 (5)
2008	Murase	MC	2.198 (4), hc
2008	Murase	MC	2.199 (3), TP
2009	Nalimov	Theory	2.020 ± 0.045
2009	Nalimov	Theory	2.023 ± 0.053
2009	Nalimov	Theory	2.026 ± 0.055
2009	Nalimov	Theory	2.100 ± 0.089
2009	Nalimov	Theory	2.105 ± 0.084
2009	Nalimov	Theory	2.104 ± 0.080
2009	Nalimov	Theory	2.127 ± 0.089
2009	Nalimov	Theory	2.132 ± 0.084
2009	Nalimov	Theory	2.130 ± 0.080
2009	Nalimov	Theory	$2.037^{+0.033}_{-0.0}$
2009	Nalimov	Theory	$2.041^{+0.040}_{-0.0}$
2009	Nalimov	Theory	$2.042^{+0.041}_{-0.0}$
2017	Duclut	Theory	2.28
2017	Duclut	Theory	2.16
2017	Duclut	Theory	2.15
2017	Duclut	Theory	2.14
2022	Adzhemyan	Theory	2.14 (2)

04 December 2025 19:44:04

© Author(s) 2024

TABLE VII. All calculated exponents from the literature in three dimensions, to the best of our knowledge. The bcc and fcc signs indicate that the results are obtained for body and face centered cubic lattices, respectively, while regular cubic lattices are used if nothing is explicitly stated.

Year	References	Method	z
1987	Wansleben	MC	2.03 ± 0.04
1991	Wansleben	MC	2.04 ± 0.03
1992	Stauffer	MC	2.09
1993	Ito	MC	2.06 (2)
1993	Muenkel	MC	2.08 ± 0.03
1994	Grassberger	MC	2.032 ± 0.004
1995	Gropengiesser	MC	2.04 ± 0.01
1997	Prudnikov	Theory	2.017
1999	Jaster	MC	2.042 (6)
2000	Ito	MC	2.055 (10)
2002	Livet	Experiment	2.2
2006	Krinitsyin	Theory	2.0237 ± 0.0055
2007	Canet	Theory	2.09 (4)
2008	Murase	MC	2.065 (25), bcc
2008	Murase	MC	2.057 (25), fcc
2009	Nalimov	Theory	2.011 ± 0.012
2009	Nalimov	Theory	2.013 ± 0.012
2009	Nalimov	Theory	2.014 ± 0.011
2009	Nalimov	Theory	2.021 ± 0.006
2009	Nalimov	Theory	2.022 ± 0.005
2009	Nalimov	Theory	2.022 ± 0.005
2009	Nalimov	Theory	2.023 ± 0.006
2009	Nalimov	Theory	2.024 ± 0.005
2009	Nalimov	Theory	2.024 ± 0.005
2009	Nalimov	Theory	$2.013^{+0.011}_{-0.0}$
2009	Nalimov	Theory	$2.014^{+0.011}_{-0.0}$
2009	Nalimov	Theory	$2.014^{+0.011}_{-0.0}$
2010	Collura	MC	2.020 (8)
2015	Livet	Experiment	2.28
2017	Niermann	Experiment	2.06
2017	Duclut	Theory	2.029
2017	Duclut	Theory	2.024
2017	Duclut	Theory	2.023
2017	Duclut	Theory	2.025
2017	Duclut	Theory	2.021
2017	Duclut	Theory	2.021
2018	Livet	Experiment	1.96 (11)
2020	Hasenbusch	MC	2.0245 (15)
2022	Adzheyman	Theory	2.0235 (8)

APPENDIX B: LINEAR FIT OF THE DYNAMIC EXPONENT

As discussed in Sec. II C, the relaxation time of the system is expected to have a power-law relation with the lattice size L. In order to obtain the dynamic exponent z, one can take logarithms to both sides of Eq. (8) by naively reducing it to an equality $\tau = L^z$ and then make a linear fit $\log(\tau) = z\log(L)$. Instead, we strictly consider the proportional sign in Eq. (8) by stating that $\tau = \tau_0 L^z$, therefore allowing the linear fit to have an offset, $\log(\tau) = z\log(L) + \log(\tau_0)$.

We summarize our findings in Table V, in which we compare the offset obtained by the fitting of the QRNG data against those obtained by the PRNG data. There are two main things worth noting about the obtained results. First, we observe that all of them yield a non-zero, negative offset. Second, we note that those PRNGs using reseeding (thus having an infinite period, and therefore being closer to a TRNG) yield values closer to the one obtained by the QRNG. This fact hints that this parameter could potentially serve in the purpose of discerning good from bad randomness too.

APPENDIX C: SUMMARY OF ALL CALCULATED DYNAMIC CRITICAL EXPONENTS FOR TWO AND THREE DIMENSION

In Tables VI and VII, we gather all calculated exponents from the literature in two and three dimensions, to the best of our knowledge, for theoretical, MC, as well as experimental approaches. These are the data plotted in Fig. 3.

REFERENCES

[1] T. H. Click, A. Liu, and G. A. Kaminski, "Quality of random number generators significantly affects results of monte carlo simulations for organic and biological systems," J. Comput. Chem. **32**, 513 (2011).
[2] Y. Lin and F. Wang, "Linear relaxation in large two-dimensional Ising models," Phys. Rev. E **93**, 022113 (2016).
[3] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," (unpublished).
[4] G. Marsaglia, W. W. Tsang *et al.*, "Some difficult-to-pass tests of randomness," J. Stat. Software **7**, 1 (2002).
[5] D. Eddelbuettel and R. G. Brown, "RDieHarder: An R interface to the dieharder suite of random number generator tests," Initial version as of May 2007.
[6] N. I. of Standards and Technology, Security Requirements for Cryptographic Modules, Technical Report Federal Information Processing Standards Publications (FIPS PUBS) 140-2, Change Notice 2 December 03, 2002, U.S. Department of Commerce, Washington, D.C., 2001.
[7] P. L'ecuyer, "Tables of linear congruential generators of different sizes and good lattice structure," Math. Comput. **68**, 249 (1999).
[8] E. Faure, E. Fedorov, I. Myronets, and S. Sysoienko, "Method for generating pseudorandom sequence of permutations based on linear congruential generator," in *CMIS* (CEUR, 2022).
[9] M. Rowe, D. Kielpinski, V. Meyer *et al.*, "Experimental violation of a Bell's inequality with efficient detection," Nature **409**, 791–794 (2001).
[10] A. Acín and L. Masanes, "Certified randomness in quantum physics," Nature **540**, 213–219 (2016).
[11] L. K. Shalm, E. Meyer-Scott *et al.*, "Strong loophole-free test of local realism," Phys. Rev. Lett. **115**, 250402 (2015).
[12] M. Giustina, M. A. M. Versteegh *et al.*, "Significant-loophole-free test of Bell's theorem with entangled photons," Phys. Rev. Lett. **115**, 250401 (2015).
[13] S. Pironio, A. Acín, S. Massar *et al.*, "Random numbers certified by Bell's theorem," Nature **464**, 1021–1024 (2010).
[14] B. Hensen, H. Bernien, A. Dréau *et al.*, "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres," Nature **526**, 682–686 (2015).
[15] W. Rosenfeld, M. Weber, J. Volz, F. Henkel, M. Krug, A. Cabello, M. Zukowski, and H. Weinfurter, "Towards a loophole-free test of Bell's inequality with entangled pairs of neutral atoms," Adv. Sci. Lett. **2**, 469 (2009).
[16] M. Jerger, Y. Reshitnyk, M. Oppliger *et al.*, "Contextuality without nonlocality in a superconducting quantum system," Nat. Commun. **7**, 12930 (2016).
[17] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**, 015004 (2017).

04 December 2025 19:44:04

© Author(s) 2024

[18]M. Isida and H. Ikeda, "Random number generator," Ann. Inst. Stat. Math. **8**, 119 (1956).
[19]C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," Opt. Express **22**, 1645 (2014).
[20]F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," Opt. Express **20**, 12366 (2012).
[21]M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, "True random numbers from amplified quantum vacuum," Opt. Express **19**, 20665 (2011).
[22]Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, "Robust random number generation using steady-state emission of gain-switched laser diodes," Appl. Phys. Lett. **104**, 261112 (2014).
[23]A. Schawlow and C. Townes, "Infrared and optical masers," Phys. Rev. **112**, 1940 (1958).
[24]J. Liu, J. Yang, Z. Li, Q. Su, W. Huang, B. Xu, and H. Guo, "117 Gbits/s quantum random number generation with simple structure," IEEE Photonics Technol. Lett. **29**, 283 (2017).
[25]C. Bruynsteen, T. Gehring, C. Lupo, J. Bauwelinck, and X. Yin, "100-Gbit/s integrated quantum random number generator based on vacuum fluctuations," PRX Quantum **4**, 010330 (2023).
[26]R. Glauber, "Time-dependent statistics of the Ising model," J. Math. Phys. **4**, 294 (1963).
[27]S.-K. Ma, *Modern Theory of Critical Phenomena* (Routledge, 2018).
[28]J. Zinn-Justin, *Quantum Field Theory and Critical Phenomena* (Clarendon Press, 1996).
[29]B. Halperin and P. Hohenberg, "Scaling laws for dynamic critical phenomena," Phys. Rev. **177**, 952 (1969).
[30]P. C. Hohenberg and B. I. Halperin, "Theory of dynamic critical phenomena," Rev. Mod. Phys. **49**, 435 (1977).
[31]M. Suzuki, "Static and dynamic finite-size scaling theory based on the renormalization group approach," Prog. Theor. Phys. **58**, 1142 (1977).
[32]G. Ódor, "Universality classes in nonequilibrium lattice systems," Rev. Mod. Phys. **76**, 663 (2004).
[33]R. Bausch, V. Dohm, H. K. Janssen, and R. Zia, "Critical dynamics of an interface in 1 + ε dimensions," Phys. Rev. Lett. **47**, 1837 (1981).
[34]E. Domany, "Exact results for two- and three-dimensional Ising and Potts models," Phys. Rev. Lett. **52**, 871 (1984).
[35]J. Wang, "Critical slowing down of the two-dimensional kinetic Ising model with Glauber dynamics," Phys. Rev. B **47**, 869 (1993).
[36]B. Dammann and J. Reger, "Dynamical critical exponent of the two-dimensional Ising model," Europhys. Lett. **21**, 157 (1993).
[37]J. Wang and C. Gan, "Nonequilibrium relaxation of the two-dimensional Ising model: Series-expansion and Monte Carlo studies," Phys. Rev. E **57**, 6548 (1998).
[38]V. Prudnikov, S. Belim, E. Osintsev, and A. Fedorenko, "Critical dynamics of disordered magnets in the three-loop approximation," Phys. Solid State **40**, 1383 (1998).
[39]M. P. Nightingale and H. W. J. Blöte, "Monte Carlo computation of correlation times of independent relaxation modes at criticality," Phys. Rev. B **62**, 1089 (2000).
[40]A. Krinitsyn, V. Prudnikov, and P. Prudnikov, "Calculations of the dynamical critical exponent using the asymptotic series summation method," Theor. Math. Phys. **147**, 561–575 (2006).
[41]L. Canet and H. Chaté, "A non-perturbative approach to critical dynamics," J. Phys. A: Math. Theor. **40**, 1937 (2007).
[42]M. Nalimov, V. Sergeev, and L. Sladkoff, "Borel resummation of the ε-expansion of the dynamical exponent z in model a of the $\phi^4(O(n))$ theory," Theor. Math. Phys. **159**, 499 (2009).
[43]C. Duclut and B. Delamotte, "Frequency regulators for the nonperturbative renormalization group: A general study and the model a as a benchmark," Phys. Rev. E **96**, 012149 (2017).
[44]L. Adzhemyan, D. Evdokimov, M. Hnatic, E. Ivanova, M. Kompaniets, A. Kudlis, and D. Zakharov, "The dynamic critical exponent z for 2d and 3d ising models from five-loop expansion," Phys. Lett. A **425**, 127870 (2022).
[45]F. Livet, F. Bley, J. Simon, R. Caudron, J. Mainville, M. Sutton, and D. Lebolloch, "Statics and kinetics of the ordering transition in the AuAgZn 2 alloy," Phys. Rev. B **66**, 134108 (2002).
[46]M. Dunlavy and D. Venus, "Critical slowing down in the two-dimensional Ising model measured using ferromagnetic ultrathin films," Phys. Rev. B **71**, 144406 (2005).
[47]F. Livet, M. Fèvre, G. Beutier, and M. Sutton, "Ordering fluctuation dynamics in $AuAgZn_2$," Phys. Rev. B **92**, 094102 (2015).
[48]D. Niermann, C. Grams, P. Becker, L. Bohatý, H. Schenck, and J. Hemberger, "Critical slowing down near the multiferroic phase transition in $MnWO_4$," Phys. Rev. Lett. **114**, 037204 (2015).
[49]F. Livet, M. Fèvre, G. Beutier, F. Zontone, Y. Chushkin, and M. Sutton, "Measuring the dynamical critical exponent of an ordering alloy using x-ray photon correlation spectroscopy," Phys. Rev. B **98**, 014202 (2018).
[50]J. K. Williams, "Monte Carlo estimate of the dynamical critical exponent of the 2d kinetic Ising model," J. Phys. A: Math. Gen. **18**, 1781 (1985).
[51]S. Tang and D. Landau, "Monte Carlo study of dynamic universality in two-dimensional Potts models," Phys. Rev. B **36**, 567 (1987).
[52]N. Ito, M. Taiji, and M. Suzuki, "Accurate estimation of the dynamical critical exponent of the two-dimensional kinetic Ising model based on the Ising machine *m*-TIS," J. Phys. Soc. Jpn. **56**, 4218 (1987).
[53]S. Wansleben and D. Landau, "Dynamical critical exponent of the 3d Ising model," J. Appl. Phys. **61**, 3968 (1987).
[54]N. Ito, M. Taiji, and M. Suzuki, "Critical dynamics of the Ising model with Ising machine," J. Phys. Colloq. **49**, C1397 (1988).
[55]M. Mori and Y. Tsuda, "Vectorized Monte Carlo simulation of large Ising models near the critical point," Phys. Rev. B **37**, 5444 (1988).
[56]S. Wansleben and D. Landau, "Monte Carlo investigation of critical dynamics in the three-dimensional Ising model," Phys. Rev. B **43**, 6006 (1991).
[57]D. Stauffer, "Simulation of time exponent in 2d Glauber kinetic Ising model," Physica A **184**, 201–204 (1992).
[58]C. Münkel, D. Heermann, J. Adler, M. Gofman, and D. Stauffer, "The dynamical critical exponent of the two-, three- and five-dimensional kinetic Ising model," Physica A **193**, 540–552 (1993).
[59]N. Ito, "Non-equilibrium relaxation and interface energy of the Ising model," Physica A **196**, 591–614 (1993).
[60]Z. Li, L. Schülke, and B. Zheng, "Dynamic Monte Carlo measurement of critical exponents," Phys. Rev. Lett. **74**, 3396 (1995).
[61]P. Grassberger, "Damage spreading and critical exponents for 'model A' Ising dynamics," Physica A **214**, 547–559 (1995).
[62]U. Gropengiesser, "Damage spreading and critical exponents for 'model A' Ising dynamics," Physica A **215**, 308–310 (1995).
[63]Z. Li, L. Schülke, and B. Zheng, "Finite-size scaling and critical exponents in critical relaxation," Phys. Rev. E **53**, 2940 (1996).
[64]M. Nightingale and H. Blöte, "Dynamic exponent of the two-dimensional ising model and monte carlo computation of the subdominant eigenvalue of the stochastic matrix," Phys. Rev. Lett. **76**, 4548 (1996).
[65]F. Wang and C. Hu, "Universality in dynamic critical phenomena," Phys. Rev. E **56**, 2310 (1997).
[66]M. S. Soares, J. Kamphorst Leal da Silva, and F. SáBarreto, "Numerical method to evaluate the dynamical critical exponent," Phys. Rev. B **55**, 1021 (1997).
[67]A. Jaster, "Computer simulations of the two-dimensional melting transition using hard disks," Phys. Rev. E **59**, 2594 (1999).
[68]N. Ito, K. Hukushima, K. Ogawa, and Y. Ozeki, "Nonequilibrium relaxation of fluctuations of physical quantities," J. Phys. Soc. Jpn. **69**, 1931 (2000).
[69]X. Lei, J. Zheng, and X. Zhao, "Monte Carlo simulations for two-dimensional Ising system far from equilibrium," Chin. Sci. Bull. **52**, 307 (2007).

04 December 2025 19:44:04

© Author(s) 2024

[70] Y. Murase and N. Ito, "Dynamic critical exponents of three-dimensional Ising models and two-dimensional three-states Potts models," J. Phys. Soc. Jpn. **77**, 014002 (2008).
[71] M. Collura, "Off-equilibrium relaxational dynamics with an improved Ising Hamiltonian," J. Stat. Mech.: Theory Exp. **2010**, P12036.
[72] M. Hasenbusch, "Monte Carlo study of a generalized icosahedral model on the simple cubic lattice," Phys. Rev. B **102**, 024406 (2020).
[73] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," in *Special Publication (NIST SP) - 800-22 Rev 1a* (National Institute of Standards and Technology, Gaithersburg, MD, 2010).
[74] M. Weigel, "Performance potential for simulating spin models on GPU," J. Comput. Phys. **231**, 3064 (2012).

04 December 2025 19:44:04

© Author(s) 2024