

## Тестирование генераторов псевдослучайных последовательностей с помощью трехмерной модели Изинга

# 09, сентябрь 2012

DOI: 10.7463/0912.0445380

Белим С. В., Шершик А. Ю.

УДК 681.3

Россия, Омский государственный университет им. Ф.М. Достоевского

[sbelim@mail.ru](mailto:sbelim@mail.ru)

### 1. Введение

Традиционный подход к тестированию псевдослучайных последовательностей связан с рассмотрением их как значений случайной величины [1]. Далее выдвигаются предположения о распределении случайной величины, которые проверяются методами математической статистики. Однако такой подход отличается некоторой абстрактностью, так как не делается никаких предположений о природе случайной величины.

На сегодняшний день разработан ряд математических моделей, описывающих процессы, изучаемые статистической физикой. Использование данных моделей позволяет выявить закономерности, лежащие в основе термодинамических явлений. Важной составляющей всех таких моделей является использование псевдослучайных последовательностей. Причем модели статистической физики достаточно чувствительны к качеству псевдослучайной последовательности.

Одной из широко используемых является модель Изинга [2], предназначенная для исследования фазовых переходов в ферромагнитных системах. Одним из применений модели Изинга является определение температуры фазового перехода и значений критических индексов, характеризующих степенное поведение термодинамических функций. Значительное отличие псевдослучайной последовательности от истинно случайной должно приводить к значениям критических индексов, существенно отличающимся от полученных в рамках реального эксперимента, либо другими теоретическими методами [3].

Целью данной статьи является тестирование линейного конгруэнтного генератора псевдослучайных последовательностей с помощью алгоритма Метрополиса [2] для модели Изинга.

## 2. Модель Изинга и алгоритм Метрополиса

Трехмерная модель Изинга является одной из самых распространенных при исследовании ферромагнитных материалов. Она достаточно хорошо исследована различными теоретическими методами вблизи точки фазового перехода второго рода [4], что делает ее наиболее подходящей для исследования адекватности компьютерных моделей.

Трехмерная модель Изинга представляет собой прямоугольную сетку в трехмерном пространстве, в узлах которой расположены спины  $S_i$ , принимающие одно из двух значений ( $1/2$  или  $-1/2$ ). О двух возможных значениях принято говорить как о двух противоположных ориентациях спина. Воздействие теплового движения, интенсивность которого определяется температурой, сводится к тому, что спины могут спонтанно переворачиваться в некоторые моменты времени и находиться в энергетически невыгодном положении. Общая же энергия определяется попарной суммой обменных взаимодействий между ближайшими спинами:

$$E = J \sum S_i S_j.$$

Здесь суммируются только пары ближайших соседей,  $J$  – константа обменного взаимодействия.

Описанная система может находиться в двух состояниях (фазах) – парамагнитном и ферромагнитном. Парамагнитная фаза соответствует неупорядоченной ориентации спинов, в результате чего суммарная намагниченность системы  $m = \sum S_i$  будет нулевой ( $m=0$ ). Данное состояние возможно только при наличии разупорядочивающего теплового движения. Причем тепловое разупорядочивание должно доминировать над упорядочивающим обменным взаимодействием. Парамагнитная фаза наблюдается при высоких температурах. Ферромагнитная фаза наблюдается при более низких температурах, вследствие чего намагниченность системы будет ненулевой ( $|m| > 0$ ). Температуру перехода из парамагнитной фазы в ферромагнитную ( $T_c$ ) принято называть критической. Вблизи критической температуры наблюдаются критические явления, состоящие в том, что основные термодинамические функции демонстрируют сингулярное поведение. Расходимости термодинамических функций системы принято аппроксимировать степенными функциями, показатели которых получили название критических индексов. Традиционно вводятся следующие критические индексы:

- 1) для намагниченности  $m \sim |T - T_c|^\beta$ ,
- 2) для теплоемкости  $C \sim |T - T_c|^\alpha$ ,
- 3) для восприимчивости  $\chi = \partial m / \partial h$ ,  $h$  - внешнее поле,  $\chi \sim |T - T_c|^\gamma$ ,
- 4) для радиуса корреляции  $R_c \sim |T - T_c|^\nu$ ,
- 5) для корреляционной функции  $G(K) \sim k^{-2+\eta}$ .

Критические индексы связаны между собой скейлинговыми соотношениями:

$$\alpha = 2 - \nu D, \quad \beta = 0.5 \nu (D - 2 + \eta), \quad \gamma = \nu (2 - \eta).$$

$D$  - размерность пространства. Таким образом, задача описания критического поведения системы сводится к определению любых двух из критических индексов.

Аналитические исследования с помощью теоретико-полевого подхода позволили получить значения [6]:

$$\alpha=0.104, \beta=0.325, \gamma=1.243, \nu=0.632, \eta=0.030.$$

Данные значения были получены для бесконечной модели Изинга. В рамках компьютерного эксперимента приходится иметь дело с системами конечного размера  $L$ , на которые накладываются циклические граничные условия. В этом случае критические индексы могут быть определены из теории конечноразмерного скейлинга [5], согласно которому для наблюдения за поведением теплоемкости и восприимчивости в зависимости от температуры могут быть использованы флуктуационные соотношения:

$$C=(NK^2)(\langle U^2 \rangle - \langle U \rangle^2), \chi=(NK)(\langle m^2 \rangle - \langle m \rangle^2),$$

где  $K=J/T$ ,  $N=L^3$  – число узлов,  $E$  - внутренняя энергия,  $m$  – намагниченность системы, угловые скобки означают термодинамическое усреднение.

Критическая температура перехода может быть определена с помощью кумулянтов Биндера четвертого порядка [7]:

$$U_L=1-\langle m^4 \rangle / (3\langle m^2 \rangle^2).$$

Для систем с разными размерами  $L$  кумулянты пересекаются в критической точке  $T_c$ . Восприимчивость и намагниченность удовлетворяют следующим соотношениям:

$$\chi \sim L^{\nu}, m \sim L^{-\beta}.$$

Для определения критического индекса радиуса корреляции было использовано соотношение:

$$V_3 \sim L^{1/\nu}, V_3=1/(3\langle m^2 \rangle^2)[\langle m^4 \rangle \langle U \rangle - 2(\langle m^4 \rangle \langle m^2 U \rangle) / (\langle m^2 \rangle^2) + \langle m^4 U \rangle].$$

Для моделирования поведения системы вблизи критической температуры нами был использован алгоритм Метрополиса [2]. Алгоритм Метрополиса начинается со случайно выбранной конфигурации спинов. Затем производится случайный выбор одного из спинов и вычисляется изменение энергии  $\Delta E$ . Если произошло уменьшение энергии ( $\Delta E < 0$ ), то новая конфигурация принимается. Если энергия увеличилась ( $\Delta E > 0$ ), то генерируется случайное число  $p$  из интервала  $[0,1]$  и вычисляется величина  $W = \exp(-\Delta E/T)$ . Если  $W > p$ , то новая конфигурация принимается, в противном случае отбрасывается. Описанные шаги повторяются заданное количество раз. Термодинамическое усреднение производится по полученным конфигурациям.

### 3. Линейный конгруэнтный генератор псевдослучайных последовательностей

Линейный конгруэнтный генератор (LCG) псевдослучайных чисел был впервые предложен в 1948 году Лехмером (D.H. Lehmer) [1] и является на сегодняшний день одним из самых популярных. Псевдослучайная последовательность целых чисел определяется начальным значением  $x_0$  и рекуррентным соотношением

$$x_{n+1} = ax_n + c \pmod{M},$$

где  $M > 0$  – модуль последовательности,  $a$  – множитель ( $0 < a < M$ ) и  $c$  – аддитивная константа.

Обычно  $M$  выбирается в виде степени 2 и записывается в виде  $M = 2^w$ , а  $w$  имеет длину машинного слова (тип WORD). В этом случае существует возможность достичь наибольшего периода последовательности, выбрав нечетное  $c$  и  $a = 1 \pmod{4}$ . Но эти условия не гарантируют генерацию последовательности псевдослучайных чисел с хорошими характеристиками. В качестве примера достаточно рассмотреть тривиальный случай  $a = c = 1$ . Если  $M$  представлено в виде степени 2, то младшие биты членов последовательности не ведут себя как псевдослучайные числа. Можно показать, что младшие  $k$  бит повторяются с периодом не превышающим  $2^k$ . Поэтому необходимо рассматривать старшие биты, надеясь, что они ведут себя как псевдослучайные числа.

#### 4. Компьютерный эксперимент

Для выяснения возможности использования модели Изинга в качестве теста псевдослучайных последовательностей был осуществлен компьютерный эксперимент по нахождению критических индексов. В каждом из экспериментов реализовывался алгоритм Метрополиса для трехмерной модели Изинга с использованием линейных конгруэнтных генераторов с различными мультипликативными константами. График зависимости критических индексов  $\alpha$ ,  $\beta$ ,  $\gamma$  и  $\nu$  от значения мультипликативной константы представлен на рисунке 1.

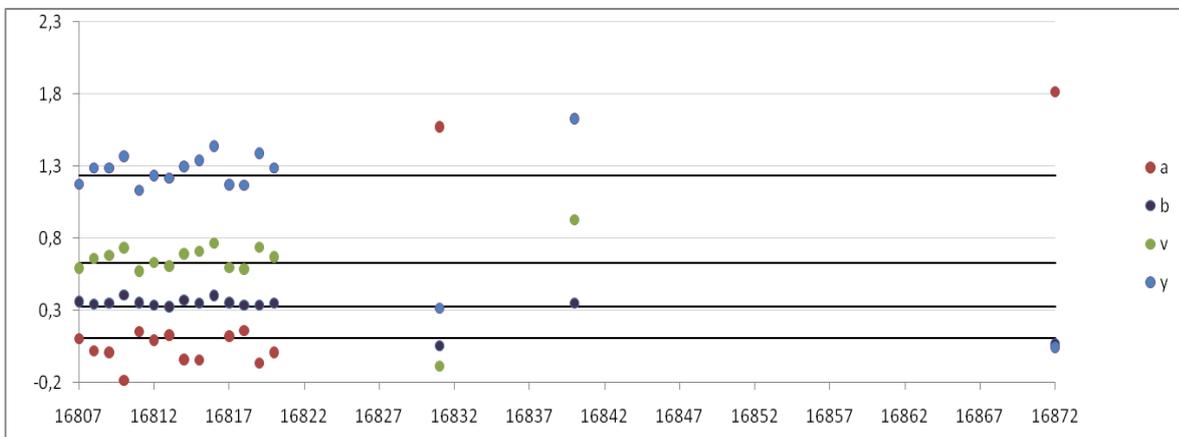


Рисунок 1. График зависимости критических индексов  $\alpha$ ,  $\beta$ ,  $\gamma$  и  $\nu$  от значения мультипликативной константы.

Как хорошо видно из графика существуют значения мультипликативной константы, которые приводят к неадекватным результатам. Так при  $a = 16872$  наблюдается anomalously большое значение индекса  $\alpha$  и anomalously низкое значение индекса  $\gamma$ . При  $a = 16810$  значение индекса  $\alpha$  становится отрицательным, что полностью противоречит наблюдаемому физическому поведению. Эти отклонения связаны с «плохим» качеством

псевдослучайной последовательности, а именно распределение чисел далеко от равномерного. С другой для мультипликативной константы  $a=16812$ , не удовлетворяющей условию  $a \equiv 1 \pmod{4}$ , результаты практически совпадают с критическими индексами, предсказываемыми теорией, то есть псевдослучайная последовательность достаточно близка к случайной.

Следует отметить, что результаты существенно зависят не только от равномерности распределения псевдослучайных чисел, но от длины псевдослучайной последовательности. На рисунке 2 представлен график зависимости среднеквадратичного отклонения значений критических индексов от предсказываемых теорией в зависимости от длины периода псевдослучайной последовательности. Для удобства длина периода представлена в виде  $M/K$ , где  $M$  – модуль из уравнения генератора, в нашем случае  $M=2^{31}-1$ , а  $K$  – длина периода псевдослучайной последовательности.

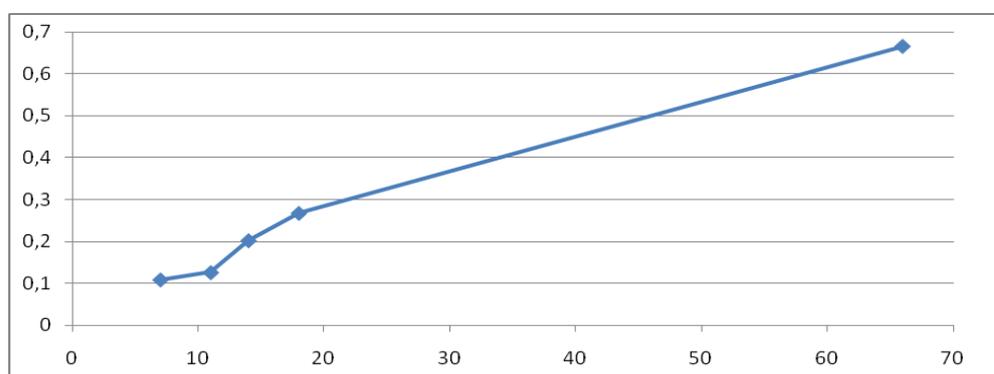


Рисунок 2. График зависимости среднеквадратичного отклонения значений критических индексов от предсказываемых теорией в зависимости от длины периода псевдослучайной последовательности

Если период псевдослучайной последовательности слишком мал, то становится невозможным само вычисление критических индексов, так как не может быть определена критическая температура. Для «коротких» последовательностей кумуляты Биндера перестают пересекаться в одной точке. На рисунках 3 и 4 представлены графики зависимости кумулянтов Биндера от температуры для системы с псевдослучайной последовательности с большим периодом ( $a=16807$ ) и маленьким периодом ( $a=16831$ ).

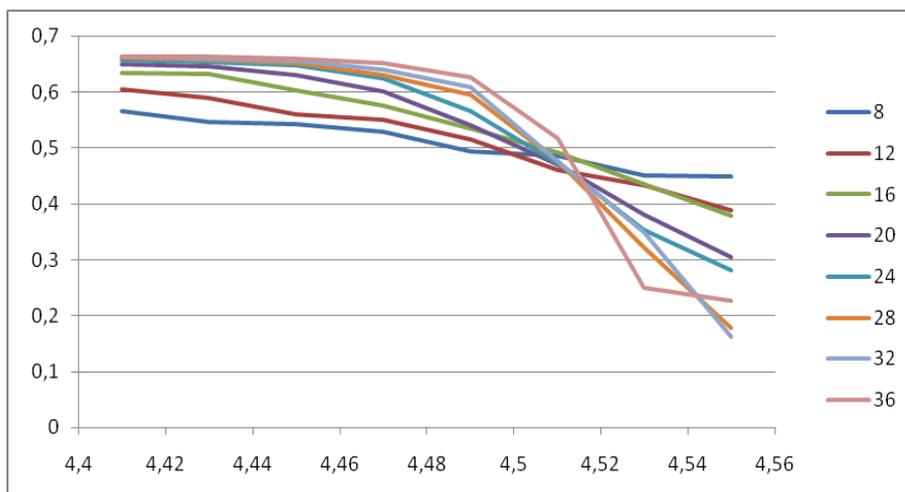


Рисунок 3. Кумулянты Биндера для последовательности с  $a=16807$ .

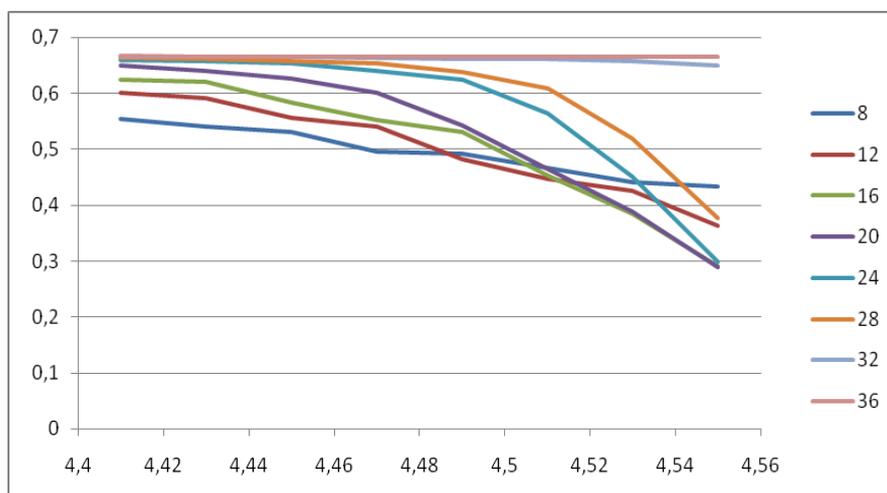


Рисунок 4. Кумулянты Биндера для последовательности с  $a=16831$ .

Легко понять, что требования к длине периода последовательности определяются линейными размерами исследуемой решетки. Так для  $a=16840$  отклонение от теоретических значений начинает проявляться при  $L>80$  ( $\ln(L)>4,4$ ), а для  $a=16831$  уже при  $L>20$  ( $\ln(L)>3$ ).

## 5. Результаты и выводы

Таким образом алгоритм Метрополиса для трехмерной модели Изинга может быть использован для тестирования качества псевдослучайной последовательности. При отклонении распределения от равномерного наблюдается отклонение критических индексов от предсказываемых теоретически. При недостаточно длинном периоде последовательности наблюдается расхождение кумулянтов Биндера, что не позволяет определить температуру перехода.

## Литература

1. Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы. - 3-е изд.- М.:«Вильямс», 2007. - 832 с.
2. Landau D.P., Binder K. A guide to Monte Carlo simulation in statistical physics. Cambridge University Press, 2005.- 427 p.
3. Coddington P.D. Tests of random number generators using Ising model simulations // Int. J. Modern Physics C.- 1996. –V. 7. - N 3.- P. 295-303.
4. Гинзбург С.Л. Определение фиксированной точки и критических индексов // ЖЭТФ (Журнал экспериментальной и теоретической физики).- 1975.- Т.68, N 1. - С.273-286.
5. Fisher M.E., Barber M.N. Scaling Theory for Finite-Size Effects in the Critical Region // Phys. Rev. Lett.- 1972.- V. 28. - P. 1516-1519.

## Testing generators of pseudorandom sequences using three-dimensional Ising model

# 09, September 2012

DOI: [10.7463/0912.0445380](https://doi.org/10.7463/0912.0445380)

Belim S., V., Shereshik A.Yu.

Russia, Omsk F.M. Dostoevsky State University  
[sbelim@mail.ru](mailto:sbelim@mail.ru)

The authors researched sensitivity of the Metropolis algorithm for the three-dimensional Ising model to the choice of a pseudorandom sequence generator. The authors show that shortcomings of pseudorandom sequence statistical properties result in the behavior of the Ising model that differs from the one predicted by methods of theoretical physics. It is shown that the Ising model can be used for testing pseudorandom sequence generators.

---

**Publications with keywords:** [pseudorandom binary sequences](#), [generators of pseudo random sequences](#), [Ising model](#)

**Publications with words:** [pseudorandom binary sequences](#), [generators of pseudo random sequences](#), [Ising model](#)

---

### References

1. Knuth D.E. *The Art of Computer Programming. V. 2. Seminumerical Algorithms*. Addison-Wesley, 1997. (Russ. ed.: Knut D. *Iskusstvo programmirovaniia. T. 2. Poluchislennye algoritmy*. Moscow, Vil'iams, 2007. 832 p.).
2. Landau D.P., Binder K. *A guide to Monte Carlo simulation in statistical physics*. Cambridge University Press, 2005. 427 p.
3. Coddington P.D. Tests of random number generators using Ising model simulations. *Int. J. Modern Physics C*, 1996, vol. 7, no. 3, pp. 295-303.
4. Ginzburg C.L. Opredelenie fiksirovannoi tochki i kriticheskikh indeksov [The definition of fixed point and critical indices]. *Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki* [Journal of Experimental and Theoretical Physics], 1975, vol. 68, no. 1, pp. 273-286.
5. Fisher M.E., Barber M.N. Scaling Theory for Finite-Size Effects in the Critical Region. *Phys. Rev. Lett.*, 1972, vol. 28, pp. 1516-1519.