ТРЕХМЕРНОЕ ОБОБЩЕНИЕ ГЕНЕРАТОРА LFSR СЛУЧАЙНЫХ ТОЧЕК

Калугин А.Н.
Самарский государственный аэрокосмический университет

Аннотация

В работе рассматривается новый метод генерации псевдо-случайных последовательностей точек, являющийся обобщением генератора Таусворта. Блоки последовательности, сгенерированной на первом этапе базовой схемы интерпретируются как цифры представления элемента кольца алгебраических целых в кубическом расширении поля рациональных чисел с использованием канонических системах счисления. Приводятся сравнительные результаты использования генератора для интегрирования методом Монте-Карло.

Введение

История разработки генераторов псевдослучайных последовательностей насчитывает несколько десятилетий. Разработано множество генераторов, реализующих различные алгоритмы и идеи. Однако большинство из созданных генераторов являются одномерными [1]: выходная последовательность такого генератора состоит из точек определенного промежутка числовой прямой, чаще всего (0.1]. Генерация последовательности с заданным законом распределения обычно осуществляется путем преобразования равномерно распределенной последовательности [2].

Развитие многопроцессорных систем, создание параллельных алгоритмов специфика реальных задач обуславливают необходимость разработки параллеллельных генераторов, генераторов, производящих многомерные последовательности [2] (последовательности точек в пространстве $\mathbb{R}^n$ [3]).

Исследованы [3, 4, 5] методы генерации таких последовательностей основанные на разбиении одномерной псевдо-случайной последовательности, использовании нескольких одномерных генераторов различных типов или одного типа с различными параметрами.

В данной работе рассматривается принципиально иная процедура генерации трехмерной псевдослучайной последовательности точек. Предлагаемая процедура основана на обобщении одномерного генератора Таусворта [7] (Tausworthe generator, linear feedback shift register generator, LFSR). Состояние (битовый вектор) генератора интерпретируется как цифры представления элементов кольца целых чисел в кубическом расширении поля рациональных чисел $\mathbb{Z}[\theta]$ в канонической системе счисления (canonical number system, CNS [10]).

Предложенный метод был использован для вычисления многомерных интегралов методом Монте-Карло. Результаты численного эксперимента и сравнение с предложенной схемы с другими генераторами приведены в разделе 4.2.

1. Генератор Таусворта

Процедура генерации Таусворта [7, 8] основана на использовании последовательности, заданной линейным рекуррентным соотношением в конечном поле из двух элементов $\mathbf{GF}(2)$. Блоки элементов этой последовательности (битовые блоки) рассматриваются как цифры записи дробной части некоторого числа в двоичной системе счисления.

Определим процедуру генерации Таусворта более формально. Пусть $\mathbf{GF}(2)$ – конечное поле из двух элементов. Далее рассмотрим многочлен

$$P(z) = z^m - a_1 z^{m-1} - \ldots - a_m,\ a_j \in \mathbf{GF}(2), \qquad (1)$$

характеристический многочлен рекуррентного соотношения (2)

$$x_n = a_1 x_{n-1} + a_2 x_{n-2} + \ldots + a_k x_{n-m} \pmod 2. \qquad (2)$$

Пусть s_i – состояние генератора (вектор бит)

$$s_i = (x_i, x_{i+1}, \ldots, x_{i+m-1}) \in \{0,1\}^m. \qquad (3)$$

Будем полагать, что задано начальное состояние $s_0 = (x_0, x_1, \ldots, x_{m-1}) \in \{0,1\}^m$.

Рассмотрим рациональное число u_n, представление которого в двоичной системе счисления имеет вид:

$$u_n = \sum_{i=1}^{L} x_{nq+i-1} \cdot 2^{-i}, \qquad (4)$$

где q и L натуральные. Если многочлен (1) не приводим, $s_0 \neq 0$ и $\text{НОК}(q, 2^m - 1) = 1$, тогда периоды последовательностей x_n и u_n равны $\rho(x_n) = \rho(u_n) = 2^m - 1$ [8] (в этом случае, x_n и u_n - последовательности максимального периода, x_n называется m-последовательностью [9]).

Свойства генератора Таусворта изучены, существуют методы супер-быстрого вычисления элементов последовательности (3), если характеристический многочлен (1) является трехчленом особого вида [8].

2. Канонические системы счисления

Предлагаемый метод генерации основывается на использовании канонических систем счисления (canonical number systems), введенных в [10] и исследованных многими авторами в [11], [12] и др.

Приведем формальное определение канонической системы счисления. Назовем *решеткой* (lattice) Λ в $\mathbb{R}^k$ множество всех линейных комбинаций с целыми коэффициентами k линейно независимых векторов .

Рассмотрим решетку Λ, групповой эндоморфизм $M : \Lambda \to \Lambda$, $\det(M) \neq 0$, и множество D, конечное подмножество Λ, $0 \in D$.

Тройка объектов (Λ, M, D) называется *системой счисления* (или, иначе, тройка (Λ, M, D) обладает свойством *единственности представления*), если для любого элемента $n \in \Lambda$ существует единственное представление вида (5):

$$n = \sum_{i=0}^{l} M^i a_i \,, \tag{5}$$

где $a_i \in D$ и $l \geq 0, l \in \mathbb{Z}$.

В этом случае, эндоморфизм M называется *основанием системы счисления,* а D – *множеством цифр*.

Система счисления $(\mathbb{Z}^k, M, D)$ называется *канонической*, если D образует полную систему вычетов по модулю M и

$$D = \{ve_1, v = 0,1,...,\left|\det M\right| - 1\}, \tag{6}$$

где $e_1 \cong (1,0...0)$.

Рассмотрим канонические системы счисления, генерируемые многочленами с целыми коэффициентам. Рассмотрим многочлен

$$\begin{aligned} &f(x) = c_k x^k + c_{k-1} x^{k-1} + ... + c_0 = \\ &= (x - \theta_1)...(x - \theta_k), c_k = 1. \end{aligned} \tag{7}$$

Обозначим Λ_f кольцо классов вычетов $\mathbb{Z}[x]/(f)$.

Пусть, далее $\beta = x + (f)$ - образ x в Λ_f. Нетрудно заметить, что множество $I_\beta = \{\beta\sigma, \sigma \in \Lambda_f\}$ представляет собой идеал, порождающий факторкольцо Λ_f / I_β.

Выбирая по одному элементу из каждого класса эквивалентности в Λ_f / I_β, можно сформировать множество цифр (6)

$D_\beta = \{a_0 = 0, a_1, ...a_{t-1}\}$.

Введя в кольце Λ_f эндоморфизм $M_\beta(\alpha) = \beta\alpha$, можно показать [12], что для определенных многочленов (7), тройка $(\Lambda_f, M_\beta, D_\beta)$ обладает свойством единственности представления.

Многочлены, генерирующие канонические системы счисления (CNS-полиномы), могут быть найдены с помощью алгоритма CNS-Sieve, предложенного в [12]. В этой работе также вычислены многочлены (7) степени до 8, порождающие бинарные канонические системы счисления, $D = \{0,1\}$.

Необходимо отметить, что, так как CNS-многочлены не приводимы, то соответствующие фактор-кольца $\mathbb{Z}[x]/(f_j)$ изоморфны алгебраическим расширениям $\mathbb{Z}[\theta]$, порожденным корнями $f_j(x)$.

Далее в данной работе будут использованы бинарные канонические системы счисления в $\mathbb{Z}[\theta]$, порожденные многочленами (8).

$$\begin{aligned} &f_1 = 2 + x^3, \\ &f_2 = 2 - x + x^3, \\ &f_3 = 2 + x + x^2 + x^3, \\ &f_4 = 2 + 2x + 2x^2 + x^3. \end{aligned} \tag{8}$$

3. Трехмерное обобщение генератора Таусворта. Генератор LFSR-CNS

На втором этапе схемы генерации Таусворта последовательности бит (2) интерпретируется как цифры записи дробной части некоторого числа в двоичной системе счисления (3).

По аналогии, рассмотрим последовательность (2) как последовательность цифр представления разложения (5), представления элементов Λ_f в бинарной канонической системе счисления, порожденной одним из многочленов (8).

Конкретизируя схему генерации, положим, $q = 1; L = m$, тогда выражение (4) примет вид:

$$\tilde{u}_n = \sum_{i=1}^{m-1} M^i x_{n+i} \,, \tag{9}$$

где $x_i \in \{0,1\} \cong D_f$.

Таким образом, каждому вектору состояния (3) s_i генератора (2) поставлен в соответствие элемент $\tilde{u}_n \in \Lambda_f$.

Для $f \in \{f_1, ..., f_4\}$ можно показать, что, $\Lambda_f \cong \mathbb{Z}[\theta] \cong \mathbb{Z}^3$. Таким образом, каждому вектору s_i поставлен в соответствие элемент «трехмерного пространства».

Заметим, что вследствие уникальности представления (5), различным векторам s_i соответствуют различные элементы $n \in \Lambda_f$, а, следовательно, и точки $\mathbb{Z}^3$.

Множество $\tilde{U}$ точек $\mathbb{Z}^3$, соответствующих всем возможным векторам s_i, представляет собой область сложной (фрактальной) формы. Это множество можно считать аналогом фундаментальной области $[0,1)$ для одномерного случая [13]. На рис. 1–3 приведены примеры областей для рекуррентных соотношений (2) порядка $3t$ с периодом $\rho = 2^{3t} - 1$.

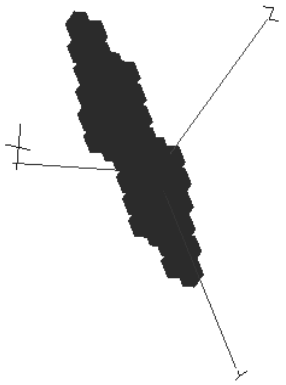

Рис. 1. $\tilde{U}$, соответствующее f_2 и $t = 3$

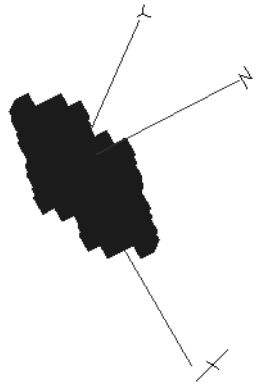

Рис. 2. $\tilde{U}$, соответствующее f_3 и $t = 3$

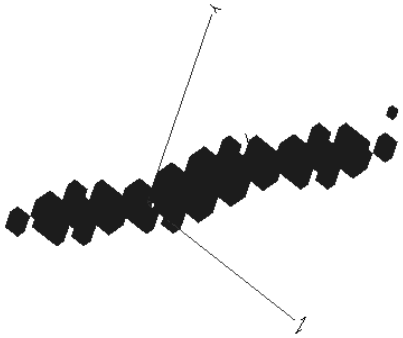

Рис. 3. $\tilde{U}$, соответствующее f_4 и $t = 3$

Определим в пространстве $\mathbb{Z}^3$ куб

$$C = \{z : z \in \mathbb{Z}^3, 0 \le z_i < 2^t, i = 0,1,2\}. \quad (10)$$

Рассмотрим точки $\tilde{u}_n \in \tilde{U}$ и $\hat{u}_n \in C$. Определим взаимно однозначное соответствие:

1. $\hat{u}_n = \tilde{u}_n$, если $\tilde{u}_n \in C$.

2. если $\tilde{u}_n \notin C$, то вместо $\tilde{u}_n$ будем брать точку $\hat{u}_n \in C$, полученную параллельным переносом $\tilde{u}_n$ с шагами (a,b,c), лежащую в другой в другой «чешуйке» из $\widehat{U}$.

Таким образом, каждому вектору состояния s_i взаимнооднозначно ставится в соответствие элемент куба (10) или, после масштабирования, куба $[0,1)^3$.

4. Свойства LFSR–CNS генератора

Генератор LFSR-CNS – трехмерный генератор псевдо–случайных последовательностей. Так как генератор получен путем альтернативной интерпретации второго этапа генератора Таусворта, он наследует как «плохие», так и «хорошие» свойства базового генератора. Однако данный генератор обладает также и новыми свойствами.

4.1 Спектральные свойства

При использовании рекуррентных соотношений, соответствующих m-последовательностям максимального периода $\rho = 2^{3t} - 1$, на выходе генератора появятся все $2^{3t} - 1$ точки сетки (с шагом 2^{-t}) трехмерного единичного куба (кроме точки $(0,0,0)$).

В отличие от классических схем распараллеливания одномерных генераторов, осуществляемых методом leapfrog [6], рассмотренный алгоритм обладает лучшими характеристиками в смысле спектрального критерия предложенного в [2] в трехмерном пространстве.

4.2 Интегрирование по методу Монте-Карло

Для экспериментальной оценки свойств генератора могут быть использованы различные методы [14], в частности вычисление многомерных интегралов по методу Монте-Карло.

Было произведено вычисление интеграла

$$I_j = \iiint\limits_{z \in [0,1)^3} y_j(z)dz, \quad (11)$$

некоторых классов функций путем вычисления сумм

$$\bar{I}_j = \frac{1}{N}\sum_{i=0}^{N-1} y_j(u_i). \quad (12)$$

Последовательности $u_i^{(k)}$ в суммах (12) сгенерированы с использованием LFSR-CNS генератор и других генераторов MC1-MC4 использованных Н.М. Коробовом [15].

В качестве подынтегральных функций были использованы

$$y_1(z) = 8z_0z_1z_2;\ y_2(z) = \frac{2}{3}(z_0 + 3z_1 - z_2);\quad (13,14)$$

$$y_3(z) = \frac{2}{11-4e} z_0^3 z_1^2 z_2 e^{z_0 z_1 z_2}; \quad (15)$$

$$y_4(z) = \frac{8m^{3/2}}{\pi^{3/2}} \prod_{j=0}^{2} (1-z_j)^{-2} e^{-(mz_j^2)/(1-z_j)^2}; \quad (16)$$

$m = 1,10,30,60$.

Точное значение интеграла (11) для функций (13)-(16) равно 1. Количество точек сетки $N \approx 4 \cdot 10^3$. Был использован LFSR-CNS генератор, соответствующий f_1 и $t = 7$. Результаты эксперимента представлены в таблице 1.

Результаты, полученные с помощью методов MC1–MC4, заимствованы из [15].

Заключение

Предложенный метод генерации псевдо-случайных последовательностей, благодаря «естественной трехмерности», может быть широко использован при решении различных 3D задач (например для работы с 3D Ising models [16]). Существование CNS-полиномов более высоких степеней обуславливает возможность увеличения «естественной размерности».

Следует, заметить, что статистические, корреляционные свойства рассматриваемого генератора, возможность его распараллеливания для задач более высокой размерности не изучены подробно.

Таблица 1. Вычисление трехмерного интеграла методом Монте-Карло при использовании различных генераторов случайных чисел

Подынтегральные функции	Метод неравномерных сеток	Методы Монте-Карло				
		1	2	3	4	Предлагаемый метод
y_1	0,39	0,78	1,05	1,02	1,01	0,997
y_2	0,73	0,94	0,997	1,008	1,008	0,998
y_3	0,81	0,75	1,07	1,04	0,98	0,987
y_4 (m=1)	1,03	1,23	1,02	0,92	0,98	1,01
y_4 (m=10)	1,38	1,67	1,32	0,84	0,79	0,914
y_4 (m=30)	3,22	2,49	0,88	0,92	0,94	0,971
y_4 (m=30)	7,49	3,87	0,54	0,53	1,15	1,037

Большое влияние на свойства данного генератора оказывает тип использованной рекуррентной последовательности. При дальнейшем развитии теории генераторов Таусворта (LFSR-генераторов) полученные результаты могут быть легко обобщены на случай рассматриваемого LFSR-CNS генератора.

Благодарности

Данная работа была выполнена при финансовой поддержке Министерства образования и науки РФ, Администрации Самарской области, Фонда гражданских исследований и развития США (CRDF Project SA-014-02) в рамках совместной Российско-Американской программы «Фундаментальные исследования и высшее образование» (BHRE), а также Российского фонда фундаментальных исследований (гранты №№ 05-01-96501, 03-01-00736).

Литература

1. L'Ecuyer P., Uniform Random Number Generation, Annals of Operations Research, 53, 1994, pp. 77-120.
2. Knuth D. E., The Art of Computer Programming. Vol 2. Seminumerical Algorithms. Second Edition. Addison-Wesley. Reading. Massachusetts, 1981.
3. Coddington P., Random Number Generators for Parallel Computers, NHSE Review, Second Issue, Northeast Parallel Architectures Center, 1996, http://nhse.cs.rice.edu/NHSEreview /RNG/ .
4. Entacher K., Parallel Streams of Linear Random Numbers in the Spectral Test, ACM Transactions on Modeling and Computer Simulation 9, 1999, no. 1, 31-44.
5. Entacher K., Uhl A., Wegenkittl S. Parallel Random Number Generation: Long- range Correlations Among Multiple Processors. In P. Zinterhof, M. Vajteršic, and A. Uhl, editors, Parallel Computation, volume 1557 of Lecture Notes in Computer Science, 107-116 (Springer, New York, 1999).
6. Shirinvasan A., Ceperley D., Mascagni M. Random Number Generators for Parallel Applications; in Monte Carlo Methods in Chemical Physics, D. Ferguson, J. I. Siepmann, and D. G. Truhlar, Eds. Advances in Chemical Physics, vol. 105, , 13-36. (John Wiley and Sons, Inc., New York, NY).
7. Tausworthe R. C., Random Numbers Generated by Linear Recurrence Modulo Two, Mathematics of Computation, 19, 1965, 201-209.
8. L'Ecuyer P., Maximally equidistributed combined Tausworthe generators. Mathematics of Computation, 65, 213 (1996), 203-213.
9. Lidl R., Niederreiter H., Finite Fields (Addison-Wesley, Reading, Massachussets, 1983).
10. Kátai I., Kovács B., Canonical number systems in imaginary quadratic fields, Acta Mathematica Academiae Scientarium Hungaricae. 37 (1-3), 1981, 159-164.
11. Thuswardner J., Elementary properties of canonical number systems in quadratic fields, G.E.Bergum et al. (eds.), Applications of Fibonacci Numbers, Volume 7, 405-415.
12. Kovács A., Generalized binary number systems, Annales Univ. Sci. Budapest, Sect. Comp. 20, 2001, 195-206.
13. Chernov V.M., Fast uniform distribution of sequences for fractal sets. Proceedings of International Conference on Computer Vision and Graphics, 2004, September 22-24, 2004, Warsaw, Poland, Computational IMAGING AND VISION SERIES, Kluwer Academic Press (accepted for publication)
14. Coddington P., Analysis of Random Number Generators Using Monte-Carlo Simulation, Int. J. Mod. Phys. C 5, 1994, 547.
15. Коробов Н.М., Теоретико-числовые методы в приближенном анализе. М.:МЦНМО, 2004 – 288 с.
16. Coddington P., Tests of random number generators using Ising model simulations, Int. J. of Mod. Phys., "C" 7(3), 1996, 295- 303.