О предельном поведении некоторых линейных конгруэнтных генераторов псевдослучайных чисел

Самахова Мария Александровна, группа 522

Санкт-Петербургский Государственный Университет
Математико-механический факультет
Кафедра статистического моделирования

Научный руководитель — к.ф.-м.н. Некруткин В.В.
Рецензент — к.ф.-м.н. Голяндина Н.Э.

Стохастическая модель ЛКГ: определение

Линейный конгруэнтный генератор : последовательность вида

$$a_{n+1} = \frac{(\lambda a_n + r) \,(\mathrm{mod}\, m)}{m} = \{\lambda a_n + c\}, \quad n \geqslant 0,$$

$a_0 = k/m$ — начальное значение, $c = r/m$.

Рассматриваем случай $m = 2^p$, r — нечетное число, $\lambda = 1 \,(\mathrm{mod}\, 4)$.

Тогда $T = 2^p$ — максимальный период и $a_n \in H = \{0, 1/2^p, \ldots, 1 - 1/2^p\}$.

Стохастическая модель ЛКГ :

$$\alpha_{n+1}^{(p)} = \{\lambda \alpha_n^{(p)} + c\}, \quad n \geqslant 0,$$

где $\lambda = \lambda(p)$ и $\alpha_0^{(p)}$ — случайная величина, р. р. на $H = \{0, 1/2^p, \ldots, 1 - 1/2^p\}$.

Стохастическая модель ЛКГ: слабая сходимость

Общая проблема:

- Условия на $\lambda(p)$, при которых $\mathcal{P}_d^{(p)} = \mathcal{L}(\alpha_0^{(p)}, \ldots, \alpha_{d-1}^{(p)}) \Rightarrow \mathrm{U}_d$ при $p \to \infty$ (асимптотическая допустимость).
- Условия, при которых эта сходимость максимально быстрая.

Что известно (общие результаты):

- (Некруткин, 1981) Асимптотическая допустимость эквивалентна сходимости $\omega_d^{(p)} = \min\left\{\|\ell\| : \ell \in \mathbb{Z}^d,\ \ell \neq \mathbf{0},\ \sum_{j=0}^{d-1} l_j \lambda^j = 0 \,(\mathrm{mod}\, 2^p)\right\} \to \infty$.

  ($1/\omega_d^{(p)}$ — это спектральное расстояние между $\mathcal{P}_d^{(p)}$ и U_d).
- $\omega_d^{(p)} \leqslant \gamma_d 2^{p/d}$ (Классический результат, γ_d — константы Эрмита).

Отсюда определение: последовательность $\lambda(p)$ асимптотически оптимальна в размерности d с константой c_d, если $\limsup_{p\to\infty} \omega_p^{(d)} 2^{-p/d} = c_d > 0$.

Стохастическая модель ЛКГ: известные результаты

Что известно (теоретические примеры, Некруткин 1981):

- Существует последовательность $\lambda(p)$, допустимая при любом d. (Но: очень медленная сходимость.)
- Существует последовательность $\lambda(p)$, оптимальная при фиксированном d. (Но: только при этом d.)

Что известно (численные эксперименты):

- Предположение: мультипликаторы вида

$$\lambda(p) = 2^{\lceil p/q_1 \rceil} + \ldots + 2^{\lceil p/q_n \rceil} + k \tag{1}$$

являются оптимальными $\Leftrightarrow d = q_j$.

Что известно (Герловина и Некруткин, 2005):

- Теорема. *Если* $n = 2$ *и* q_1, q_2 *взаимно просты, то мультипликаторы* (1) *допустимы* $\Leftrightarrow d \leqslant \max(q_1, q_2)$.

Результаты: допустимость

Мультипликаторы вида

$$\lambda(p) = 2^{\lceil r_1 p/q_1 \rceil} + \ldots + 2^{\lceil r_n p/q_n \rceil} + k \tag{2}$$

Теорема 1. *Пусть* $1 > r_1/q_1 > \ldots > r_n/q_n$ *и* $k = 1 \pmod 4$. *Тогда при* $d \leqslant d_0 = \lceil q_n/r_n \rceil$ *последовательность мультипликаторов* (2) *допустима в размерности* d.

То есть: в размерностях $d \leqslant d_0$ есть слабая сходимость к равномерному распределению.

Замечание. *Мультипликаторы вида* (2) *при* $k = k(p) \to +\infty$ *и* $\log_2 k(p) = o(p)$ *допустимы во всех размерностях* d.

То есть: слабая сходимость к равномерному распределению есть во всех размерностях d.

Результаты: предельная последовательность

Мультипликаторы вида $\lambda(p) = 2^{\lceil r_1 p/q_1 \rceil} + \ldots + 2^{\lceil r_n p/q_n \rceil} + k$, $k = \text{const}$

Вопрос: что при $d > d_0 = \lceil r_n/q_n \rceil$?

Оказывается, что сходимости к равномерному распределению нет.

А что есть?

Теорема 2. *Пусть последовательность случайных величин* $\beta_0, \beta_1, \ldots$ *такая, что*

- $\mathcal{L}(\beta_0, \ldots, \beta_{d_0-1}) = \mathrm{U}_{d_0}$,
- $\beta_m = \left\{ \sum\limits_{j=0}^{d_0-1} (-k)^{d_0-j+1} \mathrm{C}_{d_0}^{j} \, \beta_{m-d_0+j} \right\}, \quad m \geqslant d_0.$

Тогда при $p \to \infty$ *и любом* d

$$\mathcal{P}_d^{(p)} = \mathcal{L}(\alpha_0^{(p)}, \ldots, \alpha_{d-1}^{(p)}) \Rightarrow \mathcal{L}(\beta_0, \ldots, \beta_{d-1}).$$

Результаты: оптимальность

Мультипликаторы вида

$$\lambda(p) = 2^{\lceil p/q_1 \rceil} + \ldots + 2^{\lceil p/q_n \rceil} + k \tag{3}$$

Гипотеза: оптимальность при $d = q_j$ для всех j и отсутствие оптимальности при других $d < q_n$.

Теорема 3. *Пусть* $1 > q_1 > \ldots > q_n$, $k = 1 \pmod 4$.

Тогда последовательность мультипликаторов (3) *асимптотически оптимальна в минимальной и максимальной размерностях* q_1, q_n.