

2. Линейная конгруэнтная последовательность Лехмера в случайности Ковэю и Макферсона

Линейная конгруэнтная последовательность Лехмера создана в 1948 году от уравнения прямой $y = ax + c$ в виде перестановки последовательности $1, 2, \dots, N$ по рекуррентной формуле

$$x_{n+1} = ax_n + c \pmod{N} \quad (n \geq 0).$$

Случайность Ковэю и Макферсона 1965 года предложения состоит в нахождении a и c в зависимости от N такими, чтобы в разложении в конечную тригонометрическую сумму Фурье фиксированного количества последовательных элементов этой последовательности координата наиболее близкого к нулю ненулевого коэффициента Фурье будет наиболее от того же нуля удалена, — отсюда и название «Спектральный критерий».

И в этом, наверное, вся ценность этой задачи — в Математике много примеров, когда опирающаяся на самое начальное фундаментальное постановка сама фундаментальна.

Есть Стэнфорд, столица Кремниевой долины, в нем Дональд Кнут.

Дональд Кнут (Лекс Фридман, научный журналист, 2025 год):
Дональд Кнут один из величайших и самых влиятельных учёных в области



Компьютерных наук и Математики за всю историю. Он лауреат премии Тьюринга за 1974 год, которую называют Нобелевской премией в мире вычислительной техники. Он автор многотомного труда своего Magnit opus искусство программирования.

Он внёс несколько ключевых вкладов в строгий анализ вычислительной сложности алгоритмов, включая популяризацию асимптотической нотации, которую мы все с любовью знаем как нотацию Большое О. Он также создал систему вёрстки текс, которую используют большинство специалистов в области компьютерных наук, физиков, математиков, да и в целом учёных и инженеров, чтобы писать научные статьи и придавать им прекрасный вид.

Роль монографии Д.Э. Кнута «Искусство программирования» (The Art of Computer Programing) в мире Компьютерных наук возводится на уровень всего Человечества:

Журнал American Scientist включил «Искусство программирования» в список 12 лучших физико-математических монографий XX-го столетия

вместе с работами Дирака по квантовой механике, Эйнштейна по теории относительности и немногочисленными другими.

Обложка третьего издания первого тома книги содержит цитату [Билла Гейтса](#): «Если вы считаете себя действительно хорошим программистом..., прочитайте „Искусство программирования“ (Кнута)... Если вы сможете прочесть весь этот труд, то вам определённо следует отправить мне резюме».

Обратимся к самой монографии:

3.3.4. Спектральный критерий

В этом разделе рассматривается особенно важный метод проверки качества линейных конгруэнтных генераторов случайных чисел. Все хорошие генераторы проходят проверку спектральным критерием; все генераторы, известные сейчас как плохие, фактически провалились при этой проверке. Таким образом, спектральный критерий является наиболее мощным известным до сих пор критерием и заслуживает особого внимания.

В каждом из трех изданий своей монографии Дональд Кнут описывал состояние этой темы на момент ее подготовки, в последнем известном изложении вместе с сопутствующими сведениями составляет порядка 50 страниц текста.

На четверти страницах текста выписано то, что в течение 50 лет не нашло полного и окончательного решения в тысячах и десятках тысяч публикаций со всеми высшими наукометрическими показателями, и в этом мощь, красота и таинство Математики – на 10 строк постановки задачи 10 строк полного решения с последующей практической рекомендацией равно в 1 строку:

Темиргалиев Н. Элементарное построение линейной конгруэнтной последовательности Лехмера с той степенью случайности, с какой требованиям случайности отвечает спектральный тест Ковзю и Макферсона // Вестник Евразийского национального университета имени Л.Н.Гумилева. Серия Математика. Информатика. Механика. 2018. Т. 123. № 2. С. 8-55.

Temirgaliyev N. Full spectral testing of linear congruent method with a maximum period // arXiv:1607.00950 [math.NA]

Генератор случайных чисел Лехмера или же Линейная конгруэнтная последовательность максимального периода 1948 года создания есть, по определению, рекуррентная последовательность $\langle x_n \rangle$ целых неотрицательных чисел $x_{n+1} = (ax_n + c) \bmod N, n \geq 0$, где целые числа $a > 1, N > a, c > 0$ таковы, что c и N взаимно просты, $a - 1$ кратно каждому простому делителю N и кратно 4, если N кратно 4. Также для s -мерной ($s \geq 2$) последовательности $y_1 = (x_1, \dots, x_s), y_2 = (x_2, \dots, x_{s+1}), \dots, y_{N-s+1} = (x_{N-s+1}, \dots, x_N)$ положим

$$v_s(a, N) = \inf \left\{ \sqrt{m_1^2 + \dots + m_s^2} : m = (m_1, \dots, m_s) \in Z^s, \right.$$

$$\left. m \neq 0, \sum_{j=1}^s m_j a^{j-1} \equiv 0 \pmod{N} \right\}.$$

И тогда задача заключается при заданных $s \geq 2, \tau \geq 2, \lambda \geq 1$ в выборе пар N и a такими, что $(a-1)^\tau \equiv 0 \pmod{N}, (a-1)^{\tau-1} \not\equiv 0 \pmod{N}, \lambda N = (a-1)^\tau$ и чтобы величина $v_s(a, N)$ была возможно большей при известной оценке сверху $v_s(a, N) \leq \gamma(s)N^{\frac{1}{s}}$.

Полное решение проблемы «SC-спектральный критерий» в «магических» $\equiv$ «волшебных» числах a и N заключается в следующем

$$1^0. \text{ SC-2: } v_2^2(a, N; (a-1)^2 = N) = (a-1)^2 \left(1 - 2 \frac{a-2}{(a-1)^2}\right) = N \left(1 - 2 \frac{\sqrt{N}-1}{N}\right),$$

$$2^0. \text{ SC } (2 \leq s = \tau): N^{\frac{2}{s}} \left(1 - (b_s - 1)N^{-\frac{1}{s}}\right)^2 = (a - b_s)^2 \leq v_s^2(a, N; (a-1)^s = N) \leq a^2 + 1 = N^{\frac{2}{s}} \left(1 + 2N^{-\frac{1}{s}} + 2N^{-\frac{2}{s}}\right).$$

$$3^0. \text{ SC } (2 \leq s < \tau, \lambda \geq 1): (N\lambda)^{\frac{2}{\tau}} \left(1 - (b_s - 1)(N\lambda)^{-\frac{1}{\tau}}\right)^2 = (a - b_\tau)^2 \leq v_s^2(a, N; (a-1)^\tau = N\lambda, 1 \leq \lambda \leq (a-1)^{\tau-s}) \leq a^2 + 1 = (N\lambda)^{\frac{2}{\tau}} \left(1 + 2(N\lambda)^{-\frac{1}{\tau}} + 2(N\lambda)^{-\frac{2}{\tau}}\right),$$

$$4^0. \text{ SC } (s > \tau \geq 2, \lambda \geq 1): v_s^2(a, N; (a-1)^\tau = N\lambda, \lambda \geq 1) \leq \sum_{k=0}^{\tau} \left(\binom{\tau}{k}\right)^2,$$

где $(-b_m)$ есть наибольший по модулю отрицательный биномиальный коэффициент в разложении $(a-1)^m$ по степеням a : $b_2 = 2, b_3 = 3, b_4 = 4, b_5 = 10, b_6 = 20, b_7 = 35, b_8 = 56, b_9 = 126, b_{10} = 252, b_{11} = 462, b_{12} = 792, b_{13} = 1716, b_{14} = 3432, b_{15} = 6435, \dots$ и т.д.

Отметим, что в пунктах 1^0 - 3^0 установлена, можно сказать, «усиленная» асимптотика порядка ранее известной оценки сверху, стало быть, неулучшаемая, тогда как пункт 4^0 завершает полную картину как случай неприменимости.

Практический выбор a и N : $a = 4^{r_0} p_1^{r_1} \dots p_t^{r_t} + 1, N = 4^{u_0} p_1^{u_1} \dots p_t^{u_t}, 2 \leq s \leq \tau = \max \left\{ \left\lceil \frac{u_1}{r_1} \right\rceil; \dots; \left\lceil \frac{u_t}{r_t} \right\rceil \right\}.$

По-видимому, вряд ли из всех возможных Больших данных x_0, a, s, N экспериментально можно выделить «магические» $\equiv$ «волшебные» числа a и N , что есть еще один возможный ответ на вопрос “Может ли ML-AI полностью заменить Науку?”