2. The Lehmer Linear Congruential Sequence in the Coveyou–MacPherson Randomness Framework.

The Lehmer linear congruential sequence was introduced in 1948 from the equation of a straight line $y = ax + c$ in the form of a permutation of the sequence $1,2, \dots, N$ according to the recurrence formula

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

The randomness proposed by Covey and MacPherson in 1965 consists in finding a and c depending on N in such a way that, in the expansion into a finite trigonometric Fourier sum of a fixed number of consecutive elements of this sequence, the coordinate of the nonzero Fourier coefficient closest to zero is as far as possible from that same zero—hence the name "spectral criterion".

And in this, perhaps, lies the entire value of this problem: in mathematics there are many examples where a formulation based on the most elementary foundations is itself fundamental.

There is Stanford, the capital of Silicon Valley, and there is Donald Knuth.

Donald Knuth (Lex Fridman, science journalist, 2025): *Donald Knuth is one of the greatest and most influential scientists in the history of Computer Science and Mathematics. He is the recipient of the 1974 Turing Award, often referred to as the Nobel Prize of computing. He is the author of the multi-volume work The Art of Computer Programming, his magnum opus.*

He made several key contributions to the rigorous analysis of the computational complexity of algorithms, including the popularization of asymptotic notation, which we all fondly know as Big O notation. He also created the TeX typesetting system, which is used by most computer scientists, physicists, mathematicians, and, more broadly, scientists and engineers to write scientific papers and give them a beautiful appearance.

The role of D. E. Knuth's monograph *The Art of Computer Programming* in the world of Computer Science is elevated to the level of all humankind:

The journal American Scientist included The Art of Computer Programming in the list of the 12 greatest physical and mathematical monographs of the twentieth century, alongside the works of Dirac on quantum mechanics, Einstein on the theory of relativity, and a small number of others.

The cover of the third edition of the first volume of the book contains a quotation by Bill Gates: *"If you think you're a really good programmer…, read The Art of Computer Programming (by Knuth)… If you can read the whole thing, you should definitely send me your résumé."*

Let us turn to the monograph itself:

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.

In each of the three editions of his monograph, Donald Knuth described the state of the subject at the time of its preparation; in the latest known presentation, together with the accompanying material, it amounts to approximately 50 pages of text.

About a quarter of these pages are devoted to problems that, over the course of 50 years, have not found a complete and final solution in thousands and tens of thousands of publications with the highest scientometric indicators. And herein lies the power, beauty, and mystery of Mathematics: for 10 lines of problem formulation, there are 10 lines of a complete solution, followed by a practical recommendation expressed in just one line.

Temirgaliev N. Elementarnoe postroenie lineinoi kongruentnoi posledovatel'nosti Lekhmera s toi stepen'yu sluchainosti, s kakoi trebovaniyam sluchainosti otvechaet spektral'nyi test Koveiu i Makfersona[Elementary construction of the linear congruent Lehmer sequence with the degree of randomness that is required by the spectral test of Coveyou and MacPherson], Vestnik Evraziiskogo natsional'nogo universiteta imeni L.N. Gumileva. Seriya Matematika. Informatika. Mekhanika [Bulletin of L.N. Gumilyov Eurasian National University. Mathematics, Computer Science, Mechanics Series]. 2018. Vol. 123. No. 2. Pp. 8–55.

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

`*The Lehmer random number generator*, or the *linear congruential sequence* of maximal period introduced in 1948, is, by definition, a recurrent sequence $\langle x_n \rangle$ of nonnegative integers

$$X_{n+1} = (aX_n + c) mod\, N, n \geq 0$$

where integer numbers $a > 1, N > a$, c > 0 such that c and N mutually prime, $a - 1$ *divisible by each prime divisor* N *and divisible by* 4, if N *divisible by* 4. Also, for s -dimensional $(s \geq 2)$ sequence $y_1 = (x_1, \dots, y_s)$, $y_2 = (x_2, \dots, x_{s+1}), \dots, y_{N-s+1} = (x_{N-s+1}, \dots, x_N)$ let define

$$\nu_s(a, N) = inf\left\{\sqrt{m_1^2 + \cdots + m_s^2} : m = (m_1, \dots, m_s) \in Z^s, m \neq 0, \sum_{j=1}^{s} m_j a^{j-1} \equiv 0 (mod\, N)\right\}.$$

Then the problem consists, for given $s \geq 2, \tau \geq 2, \lambda \geq 1$ in choosing pairs N and a such that $(a-1)^{\tau} \equiv 0(mod\ N), (a-1)^{\tau-1} \not\equiv 0(mod\ N), \lambda N = (a-1)^{\tau}$ and so that the quantity $\nu_s(a, N)$ is as large as possible, given a known upper bound of $\nu_s(a, N) \leq \gamma(s) N^{\frac{1}{s}}$.

A complete solution to the "SC-spectral criterion" problem for the "*magic*" numbers *a* and *N* is as follows:

1^0.SC-2: $\nu_2^2(a, N; (a-1)^2 = N) = (a-1)^2 \left(1 - 2\frac{a-2}{(a-1)^2}\right) = N\left(1 - 2\frac{\sqrt{N}-1}{N}\right)$,

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

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

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

where $(-b_{\mathrm{m}})$ is the binomial coefficient with the largest absolute value and negative sign in the expansion of $(a-1)^{m}$ in powers of a: $b_2 = 2, b_3 = 3, b_4 = 4, b_5 = 10$, $b_6 = 20,\ b_7 = 35,\ b_8 = 56,\ b_9 = 126,\ b_{10} = 252,\ b_{11} = 462, b_{12} = 792,\ b_{13} = 1716, b_{14} = 3432, b_{15} = 6435, \ldots$ and so on.

We note that in Sections 1^0-3^0, a "strengthened" asymptotic estimate of the previously known upper bound is established, and hence it is unimprovable, whereas Section 4^0 completes the full picture as the case of non-applicability.

Practical choice of $\boldsymbol{a}$ and $\boldsymbol{N}$:

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

Apparently, it is hardly possible to experimentally identify the "magical" ≡ "enchanted" numbers *a* and *N* from all possible Big Data x_0, a, c, N, which provides yet another possible answer to the question: "Can ML-AI completely replace Science?"