1^0. Ковэю мен Макферсон кездейсоқтығы аясындағы Лехмердің сызықтық конгруэнтті тізбегі.

Лехмердің сызықтық конгруэнтті тізбегі 1948 жылы түзудің $y = ax + c$ теңдеуінен, $1,2,\dots,N$ сандар тізбегін

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

рекурренттік формуласы бойынша орынауыстыру арқылы жасалған.

1965 жылы Ковэю және Макферсон ұсынған кездейсоқтық тұжырымдамасы Лехмер тізбегіндегі N санына тәуелді a мен с сандарын осы тізбектің Фурье ақырлы тригонометриялық жіктелуіндегі нөлге ең жақын орналасқан нөлден өзгеше Фурье коэффициентінің координатасы мүмкіндігінше нөлден алыс болатындай таңдаудан тұрады. Осыған байланысты бұл әдіс «спектралдық критерий» деп аталады.

Мүмкін, осы есептің бүкіл құндылығы математикада ең бастапқы іргелі қойылымға сүйенетін тұжырымның өзі де іргелі болып саналатындығында шығар.

Кремний алқабының астанасы Стэнфордта Дональд Кнут жұмыс істейді.

Дональд Кнут (Лекс Фридман, ғылыми журналист, 2025 жыл): *Дональд Кнут — компьютерлік ғылымдар мен математика саласындағы ең ұлы әрі ең ықпалды ғалымдардың бірі. Ол есептеу техникасы әлеміндегі Нобель сыйлығы деп аталатын Тьюринг сыйлығының 1974 жылғы лауреаты.* «Бағдарламалау өнері» *атты көптомдық magnum opus фундаменталді еңбектің авторы.*

Дональд Кнут алгоритмдердің есептеу күрделілігінің қатаң анализі саласына бірқатар шешуші үлес қосты, оның ішінде баршамыз жақсы көріп, кеңінен қолданатын асимптотикалық Үлкен О нотациясын кеңінен таратуы бар. Сондай-ақ ол компьютерлік ғылымдар саласының мамандары, физиктер, математиктер, жалпы алғанда ғалымдар мен инженерлер ғылыми мақалалар жазу және оларға көркем, жоғары сапалы пішін беру үшін кеңінен қолданады ***мәтінге*** *терім жасауға мүмкіндік беретін Latex жүйесін жасады.*

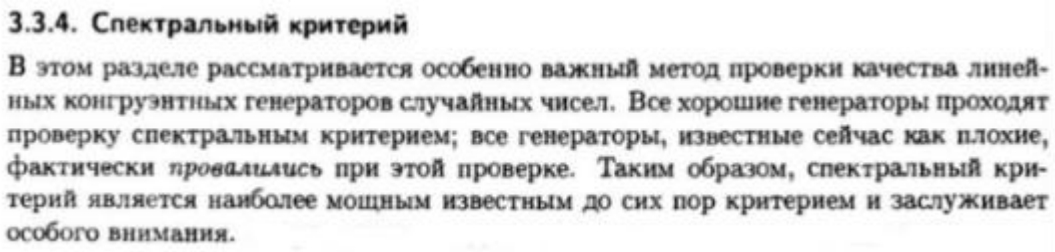
“Бағдарламалау өнері” (The Art of Computer Programming) атты Д.Э. Кнуттың монографиясының Компьютерлік ғылымдар әлеміндегі рөлі бүкіл Адамзат деңгейіне дейін көтерілген:

American Scientist журналы « » еңбегін Paul Diracтың кванттық механика бойынша еңбектері, Albert Einsteinнің салыстырмалылық теориясы жөніндегі жұмыстары және басқа да санаулы іргелі зерттеулермен қатар XX ғасырдың физика-математика саласындағы 12 үздік монографиясының қатарына енгізді.

Кітаптың бірінші томының үшінші басылымының мұқабасында Bill Gatestың «*Егер сіз өзіңізді шынымен мықты бағдарламашымын деп санасаңыз…, „Бағдарламалау өнері“ (Кнуттың) оқып шығыңыз…, … Егер сіз*

бұл еңбекті толық оқып шыға алсаңыз, онда міндетті түрде маған түйіндемеңізді жіберіңіз» деген.

Енді монографияның өзіне жүгінейік:



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 *проваливались* при этой проверке. Таким образом, спектральный критерий является наиболее мощным известным до сих пор критерием и заслуживает особого внимания.

Өзінің монографиясының үш басылымының әрқайсысында Дональд Кнут осы тақырыптың сол кезеңдегі жағдайын сипаттап отырған, шыққан соңғы нұсқасында қосымша мәліметтермен бірге шамамен мазмұндау 50 бет мәтінді құрайды.

Мәтіннің шамамен төрттен бір бөлігінде 50 жыл бойы мыңдаған және он мыңдаған ғылыми жарияланымдарда (ең жоғары наукометриялық көрсеткіштерге қарамастан) толық әрі түпкілікті шешімін таппаған мәселелер баяндалған. Ал

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

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

жұмысында 10 жолда есептің қойылымы, 10 жолда толық шешімі және де небәрі 1 жолда практикалық ұсынымға арналған толық шешім беру Математиканың құдіреті, сұлулығы мен тылсым сыры көрсетеді.

1948 жылы анықталған *Лехмердің кездейсоқ сандар генераторы* немесе максимал периодты *сызықтық конгруэнттік тізбек* анықтамасы бойынша $x_{n+1} = (ax_n + c) mod\ N, n \geq 0$ теріс емес бүтін сандардан тұратын $\langle x_n \rangle$ рекурренттік тізбек болып табылады, мұндағы $a > 1, N > a, \mathrm{c} > 0$ бүтін сандары c мен N өзара жай, $a - 1$ саны N санының жай бөлгіштерінің еселігі және N саны 4 санына еселі болған жағдайда *4* санына еселі.

Сонымен қатар, $s(s \geq 2)$-өлшемді $y_1 = (x_1, \ldots, y_s)$, $y_2 = (x_2, \ldots, x_{s+1}), \ldots, y_{N-s+1} = (x_{N-s+1}, \ldots, x_N)$ тізбектері үшін

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

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

орындалады**.**

Сонда мәселе берілген $s \geq 2, \tau \geq 2, \lambda \geq 1$ мәндері үшін N және a жұптарын $(a-1)^{\tau} \equiv 0(mod\ N), (a-1)^{\tau-1} \not\equiv 0(mod\ N), \lambda N = (a-1)^{\tau}$ орындалатындай және $\nu_s(a,N)$ шамасы белгілі $\nu_s(a,N) \leq \gamma(s)N^{\frac{1}{s}}$ жоғарғы бағалау шарты жағдайында барынша үлкен болатындай етіліп таңдалуы қажет.

«Сиқырлы» *a* және *N* сандары жағдайында «SC-спектралдық критерий» мәселесінің толық шешімі төмендегідей тұжырымдалады:

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

мұндағы $(-b_{\mathrm{m}})$ саны $(a-1)^{\,m}$ өрнегінің a дәрежелері бойынша жіктегендегі модулі бойынша ең үлкен теріс биномиалді коэффициенті: $b_2 = 2, b_3 = 3, b_4 = 4, b_5 = 10, b_6 = 20, b_7 = 35, b_8 = 56, b_9 = 126, b_{10} = 252, b_{11} = 462, b_{12} = 792, b_{13} = 1716, b_{14} = 3432, b_{15} = 6435$, ... және т.б.

1^0-3^0-пунктерінде бұрын белгілі болған жоғарғы бағалау, ары қарай жақсартылмайтын, «күшейтілген» реттік асимптотика түрінде дәлелденсе, 4^0-пунктте қолданылмайтын жағдайды сипаттау арқылы толық көрініс аяқтайды.

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

Барлық мүмкін болатын x_0, a, c, N сандарының Үлкен деректер жиынынан «сиқырлы» *a* және *N* сандарын тек *эксперименттік* жолмен бөліп көрсету екіталайлығы «ML-AI ғылымды толық алмастыра ала ма?» деген сұраққа берілетін ықтимал жауаптардың тағы бірі.