

**Метод квази Монте-Карло на основе алгебраической теории чисел
(С.М. Воронин: “Дыхание настоящей математики - от проблемы Ферма до квадратурных формул”)**

Естественная задача приближенного интегрирования приобрела особую актуальность во время работ над атомной бомбой в США, и тогда американский математик фон Нейман создал метод, ныне широко известный как "Метод Монте-Карло". Позже советский математик Н.М.Коробов предложил новый, более экономичный для ЭВМ, теоретико-числовой подход к этой задаче, впоследствии интенсивные исследования по этой теме проводились в ФРГ (Э.Хлавка), в Китае (в их числе также работавшие над ядерным проектом своей страны вице-президент АН КНР Хуа Ло-Кен и академик АН КНР Вань Юань) и многими математиками из этих и других стран.

Однако, несмотря на все эти усилия международно известных научных школ, задача нахождения эффективного алгоритма построения равномерно распределенных сеток решена не была.

Одним из главных достижений Н.Темиргалиева (1989 год) является решение этой задачи, долго не поддававшейся усилиям математиков из разных стран и в американском журнале "Gontemporary Mathematics" ("Современная математика"), названной "центральной в численном интегрировании", что было обусловлено быстрым развитием компьютерной технологии:

Являющаяся искомой случайная многомерная последовательность

$$x_k = (x_k^{(1)}, \dots, x_k^{(s)}) \quad (k = 1, 2, \dots, N)$$

будет извлечена из метода Монте-Карло по правилу

$$x_k^{(1)} \equiv a_1 k \pmod{N}, \dots, x_k^{(s)} \equiv a_s k \pmod{N},$$

в котором для безгранично возрастающих целых положительных N по вполне определенному алгоритму вычисляются целые положительные числа $a_1, \dots, a_s$ такие, что соответствующая этим числам s -мерная последовательность $(\{\dots\})$ - дробная часть, $a = (a_1, \dots, a_s)$)

$$\xi_k(a) = \left(\left\{ \frac{a_1}{N} k \right\}, \dots, \left\{ \frac{a_s}{N} k \right\} \right) \equiv \left(\left\{ a \frac{k}{N} \right\} \right) \quad (k = 1, \dots, N) \quad (*)$$

является равномерно распределенной.

Пусть дано целое положительное число s . Конечное множество $\{\eta_k\}_{k=1}^N$ точек s -мерного единичного куба $[0, 1]^s$ называют сеткой, а η_k — ее узлами.

Дискрепансом (впервые как самостоятельное понятие «дисперсия интенсивности» изучалось в, введение самого термина относят к ван дер Корпу) сетки $\{\eta_k\}_{k=1}^N$ из $[0,1]^s$ называют число

$$D_s(\eta_1, \eta_2, \dots, \eta_N) = \sup \left\{ \left| \frac{G_J}{N} - \frac{|J|}{1} \right| = \left| \frac{1}{N} \sum_{k=1}^N \chi_J(\eta_k) - \prod_{j=1}^s (b_j - a_j) \right| : J = \prod_{j=1}^s [a_j, b_j] \subset [0,1]^s \right\},$$

где J – параллелепипед в $[0,1]^s$ со сторонами, параллельными осям, $|J|$ – его s -мерный объем, G_J – количество членов $\eta_1, \dots, \eta_N$, содержащихся в J , $\chi_B(x)$ – характеристическая функция множества B .

Дискрепанс есть количественная характеристика отклонения доли $\frac{G_J}{N}$ сетки $\eta_1, \dots, \eta_N$ в J от идеального распределения $\frac{|J|}{1}$, выраженного отношением меры J к мере всего единичного куба, и, тем самым, позволяет количественно отличить «хорошее» распределение от «плохого».

Последовательность сеток $\{\eta_k^{(N_t)}\}_{k=1}^{N_t}$ из $[0,1]^s$, где $\{N_t\}_{t=1}^\infty$ – достаточно плотная возрастающая (не быстрее степенной скорости) последовательность целых положительных чисел, называют равномерно распределенной на $[0,1]^s$, если для некоторых положительных величин $c(s)$ и $\beta(s)$ и всех $t \geq 1$ имеет место неравенство

$$D_s(\eta_1^{(N_t)}, \eta_2^{(N_t)}, \dots, \eta_{N_t}^{(N_t)}) \leq c(s) \frac{\ln^{\beta(s)} N_t}{N_t}.$$

Обратимся к построению сеток. В 1959 году Н.М.Коробов доказал, что для любого целого положительного N существуют взаимно простые с N целые числа $a_1, \dots, a_s$ такие, что соответствующая этим числам сетка (*) является равномерно распределенной. В дальнейшем сетки вида (*) из других соображений были переоткрыты в 1962 году Э. Хлавкой, применение теории дивизоров также приводит к таким же сеткам.

Теоретический и практический интерес к построению сеток вида (*) объясняется, в частности, следующим. В общем случае, для записи сетки объема N требуется sN действительных чисел. Достоинством сеток вида (*) является тот факт, что они полностью определяется, независимо от объема N , заданием $s+1$ целых чисел $(N, a_1(N), \dots, a_s(N)) \in \mathbb{Z}^{s+1}$ (и легко выписывается за $\asymp N$ элементарных арифметических операций), причем каждая координата каждого узла сетки есть обыкновенная дробь с малым, в данных условиях, знаменателем N .

Так, например, при размерности $s = 10$ и количестве узлов сетки $N = 10^6$ объем записи и хранения сетки в памяти ЭВМ составляет $sN = 10^7$ чисел, в то время как в случае сетки вида (*) запись и хранение обеспечивается $s+1 =$

11 целыми числами (причем, независимо от числа узлов N). Тем самым, в случае равномерно распределенных сеток (*), по указанию С.М.Никольского нами названного «Сетка Коробова», речь идет о *сверхсжатии* информации объема sN до $s + 1$ и, по тем же причинам, в *сверхэкономном* хранении в памяти ЭВМ.

Пусть $l \geq 3$ - простое число, $\theta = \cos \frac{2\pi}{l} + i \sin \frac{2\pi}{l} = e^{i \frac{2\pi}{l}}$ и пусть

$$N(m) = \prod_{k=1}^s (m_1 + m_2 \theta^k + \dots + m_s \theta^{(s-1)k}),$$

где

$$s = l - 1, \quad m = (m_1, \dots, m_s) \in Z^s.$$

Алгоритм построения равномерно распределенных сеток:

Теорема А (Е.А. Баилов, М.Б. Сихов, Н. Темиргалиев; Журнал вычислительной математики и математической физики, 2014, том 54, № 7, с. 1059-1077). Пусть даны $l = s + 1 \geq 3$ - простое число и $r > 1$. Пусть дано $R > 1$ и

$$E = \Gamma_R \equiv \{m = (m_1, \dots, m_s) \in Z^s : \bar{m}_1 \cdot \dots \cdot \bar{m}_s \leq R\}, \quad \bar{m}_j = \max\{1, |m_j|\} \quad (j = 1, \dots, s).$$

Тогда существуют простое p ,

$$p \equiv 1 \pmod{l}, \quad p \leq c(s) R \ln^s R \equiv T$$

и целое положительное число a , $(a, p) = 1$, $a^{\frac{p-1}{l}} \not\equiv 1 \pmod{p}$, для отыскания которых согласно алгоритму, состоящему в последовательном выполнении следующих действий

Шаг 1. Находится $K(E) = \prod_{m \in E} N(m)$;

Шаг 2. Методом решета Эратосфена находятся все простые числа p из промежутка $(1, 18 s \ln K(E))$;

Шаг 3. Непосредственной проверкой каждого простого p , $p \equiv 1 \pmod{l}$, $p \in (1, 18 s \ln K(E))$ находится такое p , которое не делит $K(E)$;

Шаг 4. Находится целое a такое, что $a^{\frac{p-1}{l}} \not\equiv 1 \pmod{p}$ достаточно выполнить $T \ln \ln T$ элементарных арифметических операций, такие, что для сетки

$$\xi_k(a) = \left(\frac{k}{p}, \left\{ \frac{k}{p} a^{\frac{p-1}{l}} \right\}, \dots, \left\{ \frac{k}{p} a^{\frac{p-1}{l}(s-1)} \right\} \right) \quad (k = 1, \dots, p)$$

имеет место соотношение

$$D_s(\xi_1(a), \dots, \xi_p(a)) << \frac{\ln^{2s} T}{T}.$$

Однако реализация этого алгоритма является достаточно трудоемким процессом. Поэтому обратимся к вычислительным экспериментам для нахождения сетки $\{\xi_k(a)\}_{k=1}^p$.

Положим

$$b_r(x) = \sum_{m=(m_1, \dots, m_s) \in Z^s} (\bar{m}_1 \dots \bar{m}_s)^{-r} e^{2\pi i(m_1 x_1 + \dots + m_s x_s)},$$

где $r > 1$ и $\bar{m}_j = \max\{1, |m_j|\}, j = 1, \dots, s$.

Справедлива

Теорема В (М.Б. Сихов, Н. Темиргалиев; Математические заметки, 2010, том 87, №6, стр.948-950). *При данных $r > 1$ и $s = 1, 2, \dots$, существуют положительные величины c_1, c_2, c_3, β_1 и β_2 такие, что для всякого целого положительного p и для всякого целочисленного вектора $(a_1, \dots, a_s)$ неравенство*

$$c_3(s) \frac{(\ln p)^{\frac{s-1}{2}}}{p} \leq D_s \left[\left\{ \left(\frac{a_1}{p} k, \dots, \frac{a_s}{p} k \right) \right\}_{k=1}^p \right] \leq c_1(s) \frac{(\ln p)^{\beta_1(s)}}{p}$$

выполнено тогда и только тогда, когда

$$\left| \frac{1}{p} \sum_{k=1}^p b_r \left(\frac{a_1}{p} k, \dots, \frac{a_s}{p} k \right) - 1 \right| \leq c_2(s) \frac{(\ln p)^{\beta_2(s)}}{p}.$$

Отсюда следует, что в тех случаях, когда функция $b_r(x)$ может быть представлена в виде элементарной функции, а к таковым относятся случаи целых положительных r , установление равномерной распределенности сетки

$$\left(\frac{k}{p}, \left\{ \frac{a^{\frac{p-1}{l}}}{p} k \right\}, \dots, \left\{ \frac{a^{\frac{p-1}{l}(s-1)}}{p} k \right\} \right) (k = 1, 2, \dots, p)$$

сводится к вычислению величины

$$\Delta(s, r, a, p) \equiv \left| 1 - \frac{1}{p} \sum_{k=1}^p b_r \left(\frac{k}{p}, \left\{ \frac{a^{\frac{p-1}{l}}}{p} k \right\}, \dots, \left\{ \frac{a^{\frac{p-1}{l}(s-1)}}{p} k \right\} \right) \right|,$$

где функция $b_r(x)$ при целых положительных r есть алгебраический многочлен Бернулли.

Выпишем функции $b_r(x)$

при $r = 4$:

$$\sum_{m=(m_1, \dots, m_s) \in Z^s} (\overline{m_1} \dots \overline{m_s})^{-4} e^{2\pi i(m, x)} = \prod_{j=1}^s \left[1 + \frac{\pi^4}{45} - \frac{2\pi^4}{3} x_j^2 (1 - x_j)^2 \right],$$

при $r = 6$:

$$\sum_{m=(m_1, \dots, m_s) \in Z^s} (\overline{m_1} \dots \overline{m_s})^{-6} e^{2\pi i(m, x)} = \prod_{j=1}^s \left[1 + \frac{(2\pi)^6}{6!} \left(\frac{1}{42} - \frac{1}{2} x_j^2 + \frac{5}{2} x_j^4 - 3x_j^5 + x_j^6 \right) \right],$$

при $r = 8$:

$$\sum_{m=(m_1, \dots, m_s) \in Z^s} (\overline{m_1} \dots \overline{m_s})^{-8} e^{2\pi i(m, x)} = \prod_{j=1}^s \left[1 + \frac{(2\pi)^8}{8!} \left(\frac{1}{30} - \frac{2}{3} x_j^2 + \frac{7}{3} x_j^4 - \frac{14}{3} x_j^6 + 4x_j^7 - x_j^8 \right) \right],$$

при $r = 10$:

$$\begin{aligned} & \sum_{m=(m_1, \dots, m_s) \in Z^s} (\overline{m_1} \dots \overline{m_s})^{-10} e^{2\pi i(m, x)} = \\ & = \prod_{j=1}^s \left[1 + \frac{(2\pi)^{10}}{10!} \left(\frac{5}{66} - \frac{3}{2} x_j^2 + 5x_j^4 - 7x_j^6 + \frac{15}{2} x_j^8 - x_j^9 + x_j^{10} \right) \right]. \end{aligned}$$

Результаты проведенных нами вычислительных экспериментов оформлены в виде таблицы, где p – число узлов, a – целое число, такое что $(a, p) = 1$, $a^{\frac{p-1}{l}} \not\equiv 1 \pmod{p}$.

Вычисления организованы в следующем порядке.

Даны простое $l = s + 1 \geq 3$ и целое $r \geq 2$, выписываются в порядке возрастания простые числа $p, p \equiv 1 \pmod{l}$. Из них последовательно выбираются p , для каждого из которых находится целое положительное число $a = a(p, s)$ такое, что $a^{\frac{p-1}{l}} \not\equiv 1 \pmod{p}$. По полученному числу $a = a(p, s)$ находятся целые положительные числа $a_2 = a_2(a, p, s), \dots, a_s = a_s(a, p, s)$,

$$a_t \equiv a^{\frac{p-1}{l}(t-1)} \pmod{p}, 1 \leq a_t < p (t = 2, \dots, s), a_1 \equiv 1,$$

затем вычисляются величины

$$\Delta \equiv \Delta(s, r, p, a) = \beta_p 10^{-\tau}, 1 \leq \beta_p < 10.$$

Величины $\Delta(s, r, p, a)$ разбиваются на группы с одинаковым показателем $\tau (\tau = 1, 2, \dots)$, из которых в искомую таблицу выносятся значения коэффициентов $a_2, \dots, a_s$ с наименьшим числом узлов p и с наименьшей погрешностью Δ .

В таблице нумерация коэффициентов производится последовательно по строкам. При этом параметр a заносится во второй столбец (первый столбец отведен числу узлов p), коэффициент a_2 – в третий столбец и т.д. до случая s переменных. Случаи $s = 6, s = 10, s = 12$ приведены в Таблицах 1-3.

Таблица 1 – Значения $a_2, \dots, a_s$ и величины $\Delta(s, r, p, a)$ при $s = 6$

p	a	a_2	a_3	a_4	a_5	a_6	$\Delta(s, r, p, a)$	
							$r = 4$	$r = 6$
379	2	125	86	138	195	119	7.6E-01	1.4E-01
421	2	359	18	176	324	25	5.9E-01	1.1E-01
449	2	359	18	176	324	25	5.7E-01	1.1E-01
463	2	118	34	308	230	286	5.4E-01	1.1E-01
1009	2	105	935	302	431	859	9.3E-02	5.6E-03
...	...	...	...	...	...	...	...	...
75209	2	66662	23270	39115	63309	26732	9.8E-07	1.2E-10
94207	2	13212	85580	10546	1599	23620	8.5E-07	1.6E-10
109537	2	99712	28528	17583	96411	37901	3.3E-07	2.5E-11
215503	2	57262	58499	206609	160864	149639	7.2E-08	2.7E-12
243671	2	135142	218714	155088	28773	182619	5.2E-08	1.9E-12
476981	2	8824	115073	388584	325788	465806	8.1E-09	1.3E-13
501019	2	130214	200798	32219	332779	353434	8.7E-09	1E-13
965189	2	863106	758445	225078	651860	166036	9.1E-10	3.9E-15

Таблица 2 – Значения $a_2, \dots, a_s$ и величины $\Delta(s, r, p, a)$ при $s = 10$

p	a	$a_2, \dots, a_{10}$	$\Delta(s, r, p, a)$		
			$r = 4$	$r = 6$	$r = 8$
23231	2	690,9680,9394,21943, 5341,572,21544,9883,9538	7,1E-01	3.9E-02	3.3E-03
25873	2	16747,24562,10860,11103, 18563,10466,10400,17637,671	8.5E-01	5.7E-02	5E-03
28183	2	18418,12136,1475,26321, 4395,5534,15484,535,17763	6.5E-01	4.2E-02	3.7E-03
29569	2	4699,22127,10169,627, 18942,5768,18628,8732,19465	6.1E-01	3.7E-02	3E-03

117833	2	14328,26498,5418,94990, 45570,14307,79109,38125,99045	9.3E-02	3.6E-03	2E-04
298651	2	230692,86617,6507,92918, 62382,231258,147802,52965,192068	9.8E-03	9E-05	1.1E-06
311323	2	275448,6343,21988,72982, 308503,298848,169474,258440,286586	9E-03	7.1E-05	7.5E-07
347887	2	103500,113496,83558,130067, 99148,195161,148506,27566,59713	9.8E-03	1.2E-04	2.1E-06

Таблица 3 – Значения $a_2, \dots, a_s$ и величины $\Delta(s, r, p, a)$ при $s = 12$

p	a	$a_2, \dots, a_{12}$	$\Delta(s, r, p, a)$		
			$r = 4$	$r = 6$	$r = 8$
232961	2	171101,42214,134770,103107,40199,148535, 72662,111175,189142,142105,168035	5E-01	2.2E-02	1.6E-03
246247	2	77327,95275,112179,168711,241931,167600, 25590,203285,241950,159331,112086	7.5E-01	3.6E-02	2.6E-03
251057	2	136464,19264,24649,39450,89549,15261, 59289,157,85003,11764,104038	8.3E-01	4.5E-02	3.4E-03
251707	2	44381,65886,6347,26074,93115,11289, 120179,244576,166495,103903,46803	9.3E-01	5.1E-02	3.5E-03
255763	2	211008,129972,176812,86160,47951,60328, 110351,24525,118421,244794,108398	8.6E-01	5.3E-02	4.6E-03
258337	2	257215,225536,118868,190333,91073,117546, 123595,53379,42946,123607,39915	8E-01	4.7E-02	4.2E-03

в более развернутом изложении на стр. 44-66 номера журнала

Темиргалиев Н. К вопросу о научно-исследовательской и научно-методологической отчетности и контроле//Вестник Евразийского национального университета имени Л.Н. Гумилева. Серия Математика. Компьютерные науки. Механика. 2026. Т. 153. № 4. С. 6–91.