Quasi–Monte Carlo Method Based on Algebraic Number Theory (S.M. Voronin: *"The Breath of Real Mathematics — from Fermat's Problem to Quadrature Formulas"*)

The natural problem of approximate integration became particularly relevant during the development of the atomic bomb in the United States, when the American mathematician von Neumann created the method now widely known as the "Monte Carlo method." Later, the Soviet mathematician N.M. Korobov proposed a new, more computationally efficient number-theoretic approach to this problem. Subsequently, intensive research in this direction was carried out in Germany (E. Hlawka), in China (including Vice-President of the Chinese Academy of Sciences Hua Luogeng and Academician Wang Yuan, who also worked on their country's nuclear project), as well as by many mathematicians from other countries.

However, despite the efforts of these internationally recognized scientific schools, the problem of constructing an effective algorithm for uniformly distributed grids remained unsolved.

One of the main achievements of N. Temirgaliev (1989) is the solution of this long-standing problem, which resisted the efforts of mathematicians from various countries and was referred to in the American journal *Contemporary Mathematics* as "central in numerical integration," a status motivated by the rapid development of computer technology:

Which constitutes the desired random multidimensional sequence

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

will be extracted from the Monte Carlo method according to the rule

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

in which, for an unboundedly increasing sequence of positive integers N, a well-defined algorithm is used to compute positive integers $a_1, \dots, a_s$such that the corresponding s-dimensional sequence defined by $\{\dots\}$(fractional part), $a = (a_1, \dots, a_s)$)

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

is uniformly distributed.

Let $s$be a positive integer. A finite set $\{\eta_k\}_{k=1}^{N}$of points in the s-dimensional unit cube $[0,1]^s$is called a grid, and the points $\eta_k$are called its nodes.

The discrepancy (first studied as an independent concept under the term "dispersion of intensity"; the introduction of the term itself is attributed to van der Corput) of a grid $\{\eta_k\}_{k=1}^{N} \subset [0,1]^s$ is defined as the quantity

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

where $J$is a parallelepiped in $[0,1]^s$with sides parallel to the coordinate axes, $|\,J\,|$ is its s-dimensional volume, G_J is the number of points among $\eta_1, \dots, \eta_N$that lie in J, and $\chi_B(x)$is the characteristic function of the set B.

The discrepancy is a quantitative measure of the deviation of the ratio $G_J/N$of grid points $\eta_1, \dots, \eta_N$ lying in a box J from the ideal distribution $\frac{|J|}{1}$, expressed as the ratio of the measure of $J$to the measure of the entire unit cube. In this way, it allows one to quantitatively distinguish "good" distributions from "bad" ones.

A sequence of grids $\left\{\eta_k^{(N_t)}\right\}_{k=1}^{N_t} \subset [0,1]^s$, where $\{N_t\}_{t=1}^{\infty}$is a sufficiently dense increasing sequence of positive integers (growing no faster than a polynomial rate), is called uniformly distributed on $[0,1]^s$ if, for some positive constants $c(s)$and $\beta(s)$, and for all $t \geq 1$, the inequality holds:

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

Let us turn to the construction of grids. In 1959, N.M. Korobov proved that for any positive integer N, there exist integers $a_1, \dots, a_s$, coprime with N, such that the grid $(*)$ corresponding to these numbers is uniformly distributed. Later, grids of type $(*)$ were rediscovered in 1962 by E. Hlawka from different considerations, and the application of divisor theory also leads to the same class of grids.

The theoretical and practical interest in constructing grids of type $(*)$ is explained, in particular, by the following fact. In the general case, storing a grid of size Nrequires sNreal numbers.

A key advantage of grids of type $(*)$ is that they are completely determined—independently of the value of N—by specifying $s + 1$integers

$$(N, a_1(N), \dots, a_s(N)) \in \mathbb{Z}^{s+1},$$

and can be generated with approximately $\asymp N$elementary arithmetic operations. Moreover, each coordinate of every grid point is a simple fraction with a relatively small denominator N.

For example, in dimension $s = 10$and with a grid size $N = 10^6$, the amount of data required to store the grid in computer memory is $sN = 10^7$numbers, whereas in the case of a grid of type $(*)$, storage and representation require only $s + 1 = 11$integers (independently of the number of nodes N). Thus, for uniformly distributed grids of type $(*)$, which, following S.M. Nikolsky's suggestion, we refer to as a "Korobov grid," one deals with an extreme compression of information from volume sNdown to $s + 1$, and consequently with extremely efficient storage in computer memory.

Let $l \geq 3$ – prime number, $\theta = \cos\frac{2\pi}{l} + i\sin\frac{2\pi}{l} = e^{i\frac{2\pi}{l}}$ and let

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

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

Algorithm for constructing uniformly distributed grids:

Theorem A (E.A. Bailov, M.B. Sihov, N. Temirgaliev; *Journal of Computational Mathematics and Mathematical Physics*, 2014, Vol. 54, No. 7, pp. 1059–1077). Let $l = s + 1 \geq 3$ be a prime number and $r > 1$. Let $R > 1$be given and

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

Then there exist a prime p, $p \equiv 1(modl), p \leq c(s)R^l n^s, R \equiv T$, *and a positive integer* a, *with* $(a, p) = 1$ *and* $a^{(p-1)/l} \not\equiv 1(modp)$, *which can be found according to the algorithm consisting of the following steps:*

Step 1. *Compute*

$$K(E) = \prod_{m \in E} N(m);$$

Step 2. *Using the sieve of Eratosthenes, find all prime numbers* p*in the interval* $(1{,}18sln\,K(E))$*;*

Step 3. *By direct checking of each prime* p*, with* $p \equiv 1(modl)$*,* $p \in (1{,}18sln\,K(E))$*, find such a* p*that does not divide* $K(E)$*;*

Step 4. *Find an integer* a*such that*

$$a^{(p-1)/l} \not\equiv 1(modp).$$

It is sufficient to perform a finite number of elementary arithmetic operations such that for the grid

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

the following relation holds

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

However, implementing this algorithm is rather labor-intensive. Therefore, we turn to computational experiments to construct the grid $\{\xi_k(a)\}_{k=1}^{p}$.

Let us set

$$b_r(x) = \sum_{m=(m_1,\dots,m_s)\in Z^s} (\overline{m}_1 \dots \overline{m}_s)^{-r} e^{2\pi i(m_1x_1+\cdots+m_sx_s)},$$

for $r > 1$ and $\overline{m}_j = \max\{1, |m_j|\}, j = 1, \dots, s$.

Theorem B (M.B. Sihov, N. Temirgaliev; *Mathematical Notes*, 2010, Vol. 87, No. 6, pp. 948–950) is valid. For given $r > 1$and $s = 1,2,...$, there exist positive constants c_1, c_2, c_3, β_1, and β_2 such that for any positive integer $p$and any integer vector $(a_1, \dots, a_s)$, the inequality

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

is satisfied if and only if

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

It follows that in cases where the function $b_r(x)$can be represented as an elementary function—such cases include positive integer values of r—the establishment of the uniform distribution of the grid reduces to showing that

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

reduces to the computation of the quantity

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

where the function $b_r(x)$, for positive integer r, is the Bernoulli polynomial.

Let us list the functions $b_r(x)$

for $r = 4$:

$$\sum_{m=(m_1,\dots,m_s)\in Z^s} (\overline{m}_1 \dots \overline{m}_s)^{-4} e^{2\pi i(m,x)} = \prod_{j=1}^{s}\left[1 + \frac{\pi^4}{45} - \frac{2\pi^4}{3}x_j^2(1 - x_j)^2\right],$$

for $r = 6$:

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

for $r = 8$:
$$\sum_{m=(m_1,\dots,m_s)\in Z^s} (\overline{m_1}\dots\overline{m_s})^{-8} e^{2\pi i(m,x)}$$
$$= \prod_{j=1}^{s} 1+\frac{(2\pi)^8}{8!}\left(\frac{1}{30}-\frac{2}{3}x_j^2+\frac{7}{3}x_j^4-\frac{14}{3}x_j^6+4x_j^7-x_j^8\right)$$
for $r = 10$:

$$\sum_{m=(m_1,\dots,m_s)\in Z^s} (\overline{m_1}\dots\overline{m_s})^{-10} e^{2\pi i(m,x)} =$$

$$= \prod_{j=1}^{s}\left[1+\frac{(2\pi)^{10}}{10!}\left(\frac{5}{66}-\frac{3}{2}x_j^2+5x_j^4-7x_j^6+\frac{15}{2}x_j^8-x_j^9+x_j^{10}\right)\right].$$

The results of our computational experiments are presented in a table, where $p$is the number of nodes, and $a$is an integer such that $(a,p)=1$ and $a^{(p-1)/l}\not\equiv 1(\mathrm{mod}p)$.

The computations are organized in the following order.

Given a prime $l=s+1\geq 3$ and an integer $r\geq 2$, the prime numbers $p$satisfying $p\equiv 1(\mathrm{mod}l)$ are listed in increasing order. From them, values of $p$are selected successively, and for each such p, a positive integer $a=a(p,s)$ is found such that
$$a^{(p-1)/l}\not\equiv 1(\mathrm{mod}p).$$

For the obtained number $a=a(p,s)$, positive integers $a_2=a_2(a,p,s),\dots,a_s=a_s(a,p,s)$are defined by $a_t\equiv a^{(p-1)/l\,(t-1)}(\mathrm{mod}p)$,$1\leq a_t<p, t=2,\dots,s$, with $a_1\equiv 1$. Then the quantities $\Delta\equiv\Delta(s,r,p,a)=\beta_p 10^{-\tau}, 1\leq\beta_p<10$ are computed.

The quantities $\Delta(s,r,p,a)$ are divided into groups with the same index τ ($\tau =$ "$1,2,\dots$"), from which the values of the coefficients $a_2,\dots,a_s$ are extracted into the resulting table. These correspond to the cases with the smallest number of nodes p and the smallest error Δ.

In the table, the coefficients are numbered sequentially row by row. The parameter a is placed in the second column (the first column is reserved for the number of nodes p), the coefficient a_2 in the third column, and so on up to the case of s variables. The cases $s = 6, s = 10$, and $s = 12$ are presented in Tables 1–3.

Table 1 – Values of $a_2, \ldots, a_s$ and the quantities $\Delta(s, r, p, a)$ for $s = 6$

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

Table 2 – Values of $a_2, \ldots, a_s$ and the quantities $\Delta(s, r, p, a)$ for $s = 10$

p	a	$a_2,\ldots,a_{10}$	$\Delta(s,r,p,a)$		
			$r = 4$	$r = 6$	$r = 8$
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

Table 3 – Values of $a_2, \ldots, a_s$ and the quantities $\Delta(s, r, p, a)$ for $s = 12$

p	a	$a_2,\ldots,a_{12}$	$\Delta(s,r,p,a)$		
			$r=4$	$r=6$	$r=8$
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

in a more detailed exposition on pages 44–66 of the journal issue

Temirgaliyev N. K voprosu o nauchno-issledovatel'skoi i nauchno-metodologicheskoi otchetnosti i kontrole [On the Issue of Research and Scientific-Methodological Reporting and Oversight], Vestnik Evraziiskogo natsional'nogo universiteta imeni L.N. Gumileva. Seriya Matematika. Komp'yuternye nauki. Mekhanika [Bulletin of L.N. Gumilyov Eurasian National University. Mathematics, Computer Science, Mechanics Series]. 2026. Vol. 153. № 4. P. 6–91.