Method of Spectral Tests of Multiplicative Congruential Random Number Generators[1]

Naoya Nakazawa[2] and Hiroshi Nakazawa[3]

1. Background of the Invention

1.1. Field of the Invention

Inheriting the preceding report[4] to be denoted **I** hereafter, we extend considerations to higher degree spectral tests. Descriptions in **I** were centered around periodic structures of multiplicative congruential random number generators, handling new problems that arose with the discovery of significant roles of a series of extended 2nd degree spectral tests. Shortly after the submission of this invention to Patent Offices of Nations, inventors came to realize further inconsistencies in prior arts of spectral tests with degrees $l \geq 3$, in evaluating generated l-tules of consecutive random numbers regarding their statistical uniformity and independence. Analyses lead them to the conclusion that higher degree tests need further revisions. Devised after hard efforts on difficult problems, the revisions gifted inventors with conspicuous successes in finding several, though not many as yet, generators with outstanding performances with periods $T \approx 2^{49}$ or larger.[5]

The research processes presented below are around a shortest vector problem but, as stated, with rather comprehensive changes in its aim from the one so far adopted in the prior arts of the field. It will be impressive to state what has come and will come to be disclosed. A decisive fact is that the true problem was not the one aimed at in traditional art. Rather, we should look for generators (viz. sets of integers (d, z) to produce multiplicative congruential random numbers) that realize a set of *suitable* forms of integer lattices associated. The present series of inventions aimed first to find designs of multiplicative congruential long-period generators that nevertheless give their *computable*

[1]Uploaded in *http://www.nakazawa-patents.jp* on June 5, 2014

[2]nmail@nakazawa-patents.jp

[3]nmail@nakazawa-patents.jp

[4]Nakazawa and Nakazawa (2014): Naoya Nakazawa and Hiroshi Nakazawa, *Constructive design of uniform and independent random number generators*, posted April 29, 2014 in this URL *http://nakazawa-patents.jp* with the filename invention1.pdf.

[5]The noted magnitude of the period may intuitively be understood that the fast but small desktop computer with Intel Core (TM) i7-3930K CPU generates one random number in $10^{-6}\,\mathrm{sec}$, and the period $T = 2^{49}$ will be used up in 17.85 years. However, the matter changes drastically with present supercomputers. We might assume that one random number is produced in 10 floating point operations or in about $10/10^{16} \approx 2^{-50}\,\mathrm{sec}$. Thus the period $T \approx 2^{50}$ will be used up in 1 sec, if multiplicative congruential generators are run fully in parallel. This suggests that one day generation on a supercomputer will require a multiplicative congruential generator to have desirably a period $T \approx 2^{17} \times 2^{50} \approx 2^{67}$ or larger.

spectral tests. Structural analyses revealed that the design of the modulus d with factors formed by two odd primes is the most efficient to this end. Putting aside the framework of principles that all uniform random number sequences of any finite length T are realizable by multiplicative congruential sequences,[6] the clue to understand the noted structural excellence is in Theorem of Sun Tzu and the intuitive invariance to be accompanied by uniform and independent random number sequences: Roughly speaking, two uniform and independent sequences of random numbers should be shuffled into another uniform and independent random numbers. The efforts in this instinctive line of truth, however, were not much fruitful with the use of conventional ways of spectral tests. Inventors may now explain why this was so. The conventional spectral tests, formulated so as to find lattices with the smallest distances between their co-called *parallel and neighboring hyperplanes*, were not statistically correct in view of their aim. The revision of this direction of tests to the right form brought the computation on track, and salvaged excellent generators so far overlooked to their true valuations. Since spectral tests require extremely heavy computation, this firmly established prospect of success will be all invaluable to start with works for them.

We denote (d, z, n) for the multiplicative congruential random number generator comprising a natural number $d > 0$ for the *modulus*, an integer z coprime with d for the *multiplier*, and an integer n with the name *initial value* as the specifier of the starting random number. The integer n is also called *seed*, and restricted to be coprime with d to avoid unnecessary complications. The generator (d, z, n), or (d, z) if n is irrelevant to arguments, solves the recursive equivalence relations

$$n_1 :\equiv n \bmod (d), \quad n_{k+1} :\equiv z n_k \bmod (d), \quad 0 < n_k < d, \quad k = 1, 2, \cdots,$$

gives the solution sequence of integers $\{n_k \equiv n z^{k-1} \bmod (d) |\ 0 < n_k < d, \quad k = 1, 2, \cdots\}$, and emits the sequence $\{v_k := n_k/d |\ 0 < v_k < 1, \ \ k = 1, 2, \cdots\}$ of real or rational numbers for uniform and independent random numbers. The goal is to ascertain the precision, in the statistical sense, of this output sequence as claimed random numbers.

1.2. Spectral Tests of General Degrees

We reflect on spectral tests again, taking the general l-th degree with $l = 2, 3, \cdots$. For a while integers are taken without equivalence modulo d. Tests take l-consecutive *integer* outputs

$$\boldsymbol{Q}_k := (n_k, n_{k+1}, \cdots, n_{k+l-1}) = n z^{k-1} \boldsymbol{e}_1, \quad \boldsymbol{e}_1 := (1, z, z^2, \cdots, z^{l-1}), \quad k = 1, 2, \cdots$$

emitted from the generator (d, z, n), regarding $\boldsymbol{Q}_k$ freely as a (row position) vector or coordinates of a point in the Euclidean space E_l of l-dimension. A point $\boldsymbol{Q}_k{}'$ with coordinates equivalent to those of

[6] See **I** for this detail.

$\boldsymbol{Q}_k$ modulo d are obtained by d-translations along coordinate axes. Along $j = 2, 3, \cdots, l$ axes such translations are effected respectively by adding integral multiples of vectors,

$$\begin{aligned}
\boldsymbol{e}_2 &:= (0, d, 0, 0, \cdots, 0, 0),\\
\boldsymbol{e}_3 &:= (0, 0, d, 0, \cdots, 0, 0),\\
\boldsymbol{e}_4 &:= (0, 0, 0, d, \cdots, 0, 0),\\
&\cdots\cdots\cdots\cdots\cdots\\
\boldsymbol{e}_{l-1} &:= (0, 0, 0, 0, \cdots, d, 0),\\
\boldsymbol{e}_l &:= (0, 0, 0, 0, \cdots, 0, d).
\end{aligned}$$

Along the 1st axes the translation is realized by adding integral multiples of the following:

$$\boldsymbol{e}_1{}' := (d, 0, 0, 0, \cdots, 0, 0) = d\boldsymbol{e}_1 - z\boldsymbol{e}_2 - z^2\boldsymbol{e}_3 - z^3\boldsymbol{e}_4 - \cdots - z^{l-1}\boldsymbol{e}_l.$$

Therefore, the points $\{\boldsymbol{Q}_k |\ k = 1, 2, \cdots\}$ and all of their d-equivalents are contained in the set of vectors:

$$\begin{aligned}
G_l &:= G_l(d, z) = G_l(\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l)\\
&:= \{c_1\boldsymbol{e}_1 + c_2\boldsymbol{e}_2 + \cdots + c_l\boldsymbol{e}_l |\ c_1, c_2, \cdots, c_l \text{ are integers}\}.
\end{aligned}$$

This set G_l defines the lattice spanned by basis vectors or bases $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$ in the l-dimensional Euclidean space E_l. These basis vectors are linearly independent with their determinant $d^{l-1} \neq 0$, which represents the volume of the parallelepiped spanned by them.

Let C_d denote a hypercube in E_l with its sides $[0, d)$ along axes. Denote $\boldsymbol{Q}_k{}'$ for the point in C_d equivalent to $\boldsymbol{Q}_k$ modulo d. Supplied from the process of generating l-tuples of random numbers, the points $\boldsymbol{Q}_k{}'$ for $k = 1, 2, \cdots$ occupy their *seats* consecutively on lattice points in the hypercube C_d. Since these points of random numbers are restricted to have only integer coordinates coprime with d, they cannot occupy all of the d lattice points[7] in C_d. In one period of the generator (d, z, n) l-tuples of random numbers can occupy at most $d - 1$ of these lattice points, as the example of an odd prime $d = p$ and its primitive root z with the order $\varphi(p) = p - 1$ readily convinces us. See **I** and the references cited therein for details of these periodic structures.

The l-th degree spectral tests have little concern with noted processes of seat-taking by (d, z) outputs, and concentrate on the *valuation of the geometrical distribution of seats* prepared by the lattice G_l in E_l, estimating whether the configuration is adequate as seats for l-tuples of random numbers emitted from a uniform and independent random number generator. The meaning of this

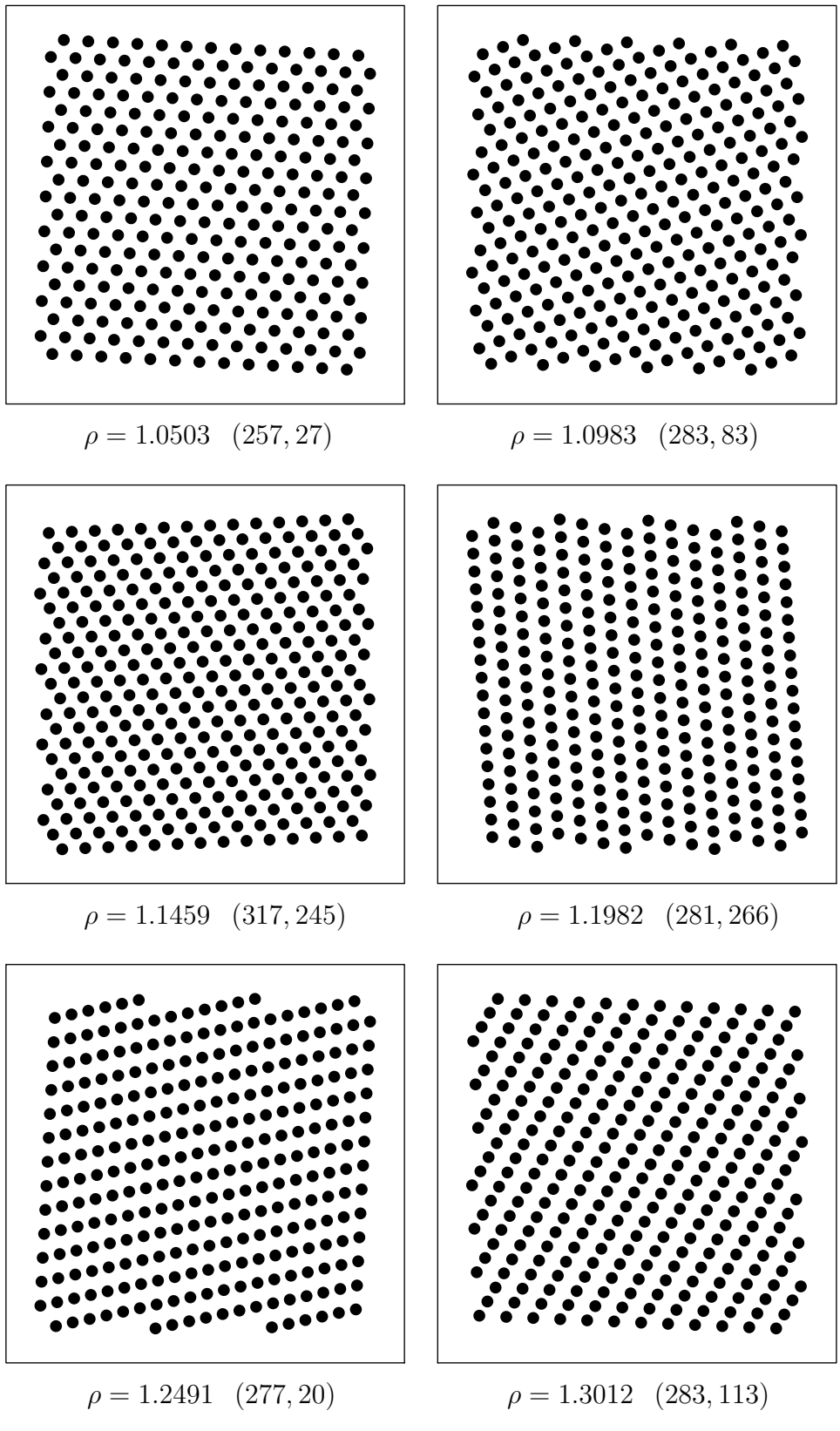
[7]The total number of lattice points in C_d is d for any dimension l, because the first coordinate c_1 of the lattice point

$$c_1\boldsymbol{e}_1 + c_2\boldsymbol{e}_2 + \cdots + c_l\boldsymbol{e}_l = (c_1, c_1z + c_2d, c_1z^2 + c_3d, \cdots, c_1z^{l-1} + c_ld)$$

gives d distinct integer values of the 1st coordinate $0 \leq c_1 < d$ in C_d, while the j-th coordinate $0 \leq c_1z^{j-1} + c_jd < d$ selects the integer c_j uniquely without freedom for any $j = 2, 3, \cdots, l$.

statement will be grasped most clearly by visual experiences. See **Figure 1** posted below in two

Figure 1 Geometry of 2-tuples of random numbers and spectral test valuation ρ



$\rho = 1.0503 \quad (257, 27)$

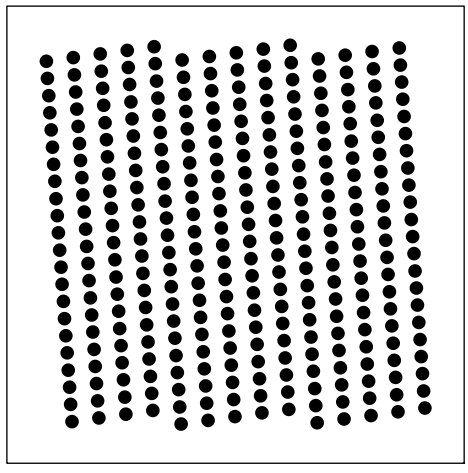
$\rho = 1.0983 \quad (283, 83)$

$\rho = 1.1459 \quad (317, 245)$

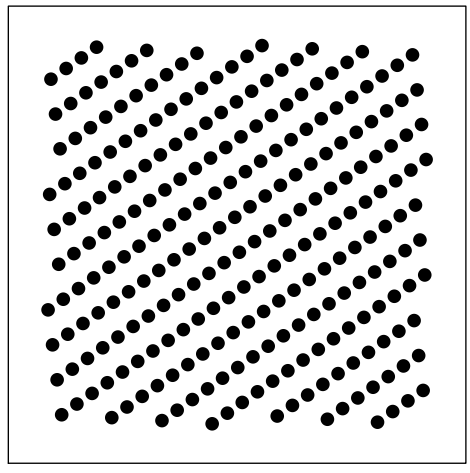
$\rho = 1.1982 \quad (281, 266)$

$\rho = 1.2491 \quad (277, 20)$

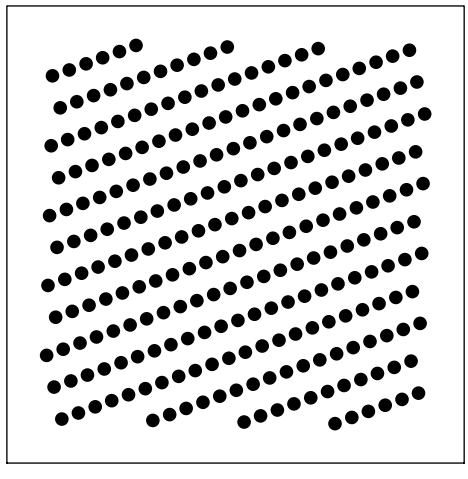
$\rho = 1.3012 \quad (283, 113)$



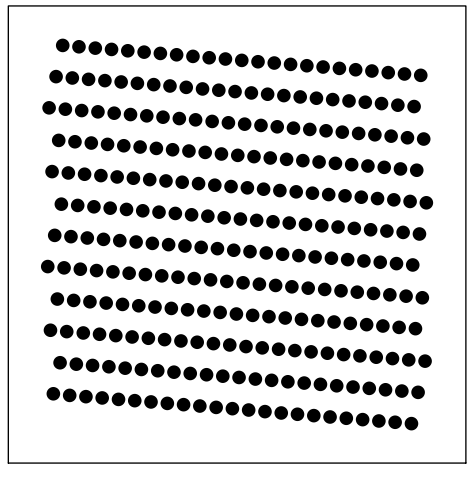
$\rho = 1.3501 \quad (311, 297)$



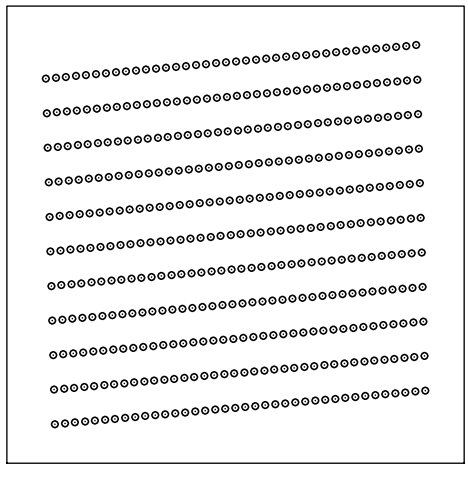
$\rho = 1.3947 \quad (251, 76)$



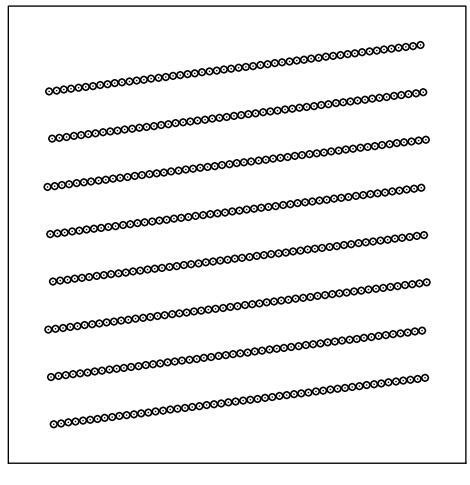
$\rho = 1.4547 \quad (251, 46)$



$\rho = 1.4959 \quad (281, 117)$



$\rho = 1.9915 \quad (419, 381)$



$\rho = 2.7283 \quad (419, 262)$

pages.[8] They show final states of occupation of seats on respective lattices. As each of **Fig. 1** is

[8]The illustrations have been posted in **I**. Readers are asked to be patient with this duplication, in view of the significance of this visual comprehension.

plotted by taking points $\{\boldsymbol{Q}_k := (n_k, n_{k+1}) |\ \ k = 1, 2, \cdots\}$ in the time order of emission, readers may see the motion picture of noted seat-taking processes if these plots are reproduced *sufficiently slowly* by reading softwares. Values of (d, z) are chosen small in order to make plots decipherable to our eyes. Points are in the square C_d. Outer square frames are drawn slightly larger so as to include C_d inside.

Plots at the start show neat arrays of emitted points close to the so-called triangular lattice formed by regular triangles. If consecutive 2-tuples of random numbers take seats in these neatly distributed positions in, hopefully, some randomly looking manner, we have few reasons to deny the statistical hypothesis that consecutive 2-tuples of random numbers appear uniformly with independence. On the contrary, we see at the end of **Figure 1** such distributions of lattice points that appear to be packed into a few distinct lines with conspicuously large separations between them. If points of 2-tuples appear on seats arranged in this manner, we shall find strong direction-dependence of their distribution and will be suggested that consecutive random number pairs appear correlated with dubious independence. Spectral tests give a number $\rho = \rho_d^{(2)}(z) > 1$ as the quantitative valuation of these impressions to the (d, z) generator; see **Figure 1** with ρ noted for $G_2(d, z)$ lattices with the understanding that ρ closer to 1 from above is better.

2. Basis Vectors of Lattices

Arguments on lattices will be started with a restrictive but explicit definition by vectors in the Euclidean space E_l, and with another general but abstract definition. A lattice to be discussed is a set of row vectors in E_l which are formed as integral linear combinations of a given set of l linearly independent basis vectors. These basis vectors and their (integral) linear combinations are identified at places with position vectors, with points or with the set of coordinates in E_l, if explicit pictures clarify circumstances better and facilitate our intuitive, geometrical thinking.

A more general but abstract definition is given in terms of groups. A *discrete* set G will be said to form a lattice if the operation of *addition* is defined between any elements a, b, c of G fulfilling the following 4 axioms.

0) Any two elements $a, b \in G$ may be added to give another in G, $a + b = b + a \in G$.

1) The addition is associative, $(a + b) + c = a + (b + c)$.

2) There exists an element $0 \in G$ that gives $a + 0 = a$.

3) For any $a \in G$ there exists an element $-a \in G$ that gives $a + (-a) = 0$.

It is obvious that the lattice defined by basis vectors satisfies these 4 axioms. We shall mainly proceed with the first explicit image of the lattice.

The parallelepiped formed by lattice basis vectors is fundamental in our arguments. Since the

choice of basis vectors is not unique, the parallelopiped is also non-unique, particularly in its shape. The following comprehension is convenient in dealing with this circumstance.

Corollary 1. Let G be a given lattice in the Euclidean space E_l. A set S of lattice vectors will be called *basal*, if the parallelepiped spanned by the set has a non-vanishing volume and contains no lattice point inside nor on surfaces (including edges) except for the vertices.

(A) Consider a set S consisting of l lattice vectors of G. The vectors in S form the basis of G if and only if they are basal. Any set of basis vectors of G, or equivalently any basal set of l lattice vectors of G, spans one and the same non-zero volume.

(B) Take two basal sets of row lattice vectors $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$ and $\{\boldsymbol{e}_1{}', \boldsymbol{e}_2{}', \cdots, \boldsymbol{e}_l{}'\}$ and form respective $l \times l$ matrices M and M'. They are linear transformations $M' = UM$ and $M = U^{-1}M'$ of each other by a unimodular matrix U and its inverse, where a unimodular matrix U is an $l \times l$ matrix formed by integer components with $\det U = \pm 1$.

(C) Let M be the matrix formed by an arbitrary basal set of row lattice vectors of G and U be an arbitrary unimodular matrix. Then the matrix $M' = UM$ has its row vectors which form a basal set of basis vectors of G.

(Proof) **(A)** Let a basal set S of lattice vectors be given with its parallelepiped V. Assume that V has a volume $v > 0$ implying the linear independence of basal vectors. Name a vertex of V as Q. Any parallelepiped is space-filling by geometry. Translations of points of V, realized by adding an arbitrary lattice vector $\boldsymbol{a}$, let the vertex Q visit all lattice points of G. In the while V tiles the space without overlap nor opening, because the inside and surfaces of V are not lattice points excepting vertices. Thus, the set S consists of basis vectors of G. Properties of the volume v is manifest.[9] The converse statement, that a set of basis vectors form a basal set, will be obvious.

(B) The set of basis vectors $\{\boldsymbol{e}_1{}', \boldsymbol{e}_2{}', \cdots, \boldsymbol{e}_l{}'\}$ consists of lattice vectors, and are represented by the original basis vectors $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$ by *integral* linear combinations. Interrelations are written compactly in the matrix forms $M' = UM$, with an integer matrix U. Assertion **(A)** demands that determinants of M and M' are $\pm v$, so that $|\det M'| = |\det U| \cdot |\det M|$ or $|\det U| = 1$ holds true. This stipulates $\det U = \pm 1$. Thus, the matrix U is unimodular with a unimodular inverse.

(C) A unimodular transformation by a matrix U is a linear transformation, and maps a line of E_l to a unique line, a lattice point to a unique lattice point, and the point at infinity to the point at infinity. Let a basal set of basis vectors span a parallelepiped V. The unimodular matrix U transforms V to a parallelepiped V' spanned by row vectors of the matrix M', and transforms the inside, the surfaces or the edges of V to those of V' by this topology. Therefore, the appearance of a lattice point inside,

[9] We may of course argue as follows. Take a sphere of radius R with the center at Q, denote its volume as v_R and assume the number of lattice points in the sphere to be n_R. The convergence $\lim_{R\to\infty} v_R/n_R =: v$ is readily seen. This v is the one and the same volume of the parallelepiped.

on the surface or on edges excepting vertices, of V' is a contradiction and false. Thus $M' = UM$ consists of a basal set of row vectors, with its manifest converse. The assertion **(C)** is true. ■

Conveniences given by unimodular transformations as stated in **(C)** are invaluable. Experiences of their power will be met soon below.

3. Parallel Adjacent Lattice Hyperplanes and Simplexes

Take the case of our space E_3 with $l = 3$ for intuitiveness and visual clarity. Assume that a lattice G is given in E_3 spanned by a basal set of lattice vectors $\{\overrightarrow{Q_0Q_1}, \overrightarrow{Q_0Q_2}, \overrightarrow{Q_0Q_3}\}$ which by definition are linearly independent and form a set of basis vectors of G. Denote $v > 0$ for the volume of the parallelepiped spanned by them.

For later continuity of notations, we note here that vectors $\{\boldsymbol{a} := \overrightarrow{Q_1Q_2}, \boldsymbol{b} := \overrightarrow{Q_1Q_3}, \boldsymbol{c} := \overrightarrow{Q_0Q_1}\}$ also form a basal set, because the inverse transformation $\overrightarrow{Q_0Q_1} = \boldsymbol{c},\ \overrightarrow{Q_0Q_2} = \boldsymbol{a} + \boldsymbol{c},\ \overrightarrow{Q_0Q_3} = \boldsymbol{b} + \boldsymbol{c}$ is unimodular with the determinant -1. Therefore, the plane spanned by $\boldsymbol{a}$ and $\boldsymbol{b}$ is a side surface of a parallelepiped[10] spanned by $\{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}\}$. Take a 2-dimensional plane Π including this side surface plane spanned by $\boldsymbol{a}$ and $\boldsymbol{b}$. Consider the lattice G as a set of lattice points, define $G_\Pi := G \cap \Pi$ as a set of points. The set of position vectors on G_Π is a subgroup of G, and the set $\{\boldsymbol{a}, \boldsymbol{b}\}$ is a basal set of vectors in G_Π, because otherwise the original $\{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}\}$ cannot be basal in G.

We name the plane Π as an $l - 1 = 2$-dimensional lattice plane of the latice G. This plane may be translated to the neighboring parallel plane Π' in E_3 by adding the vector $-\boldsymbol{c} = \overrightarrow{Q_1Q_0}$. This Π' is the opposite surface of the parallelepiped spanned by $\{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}\}$; Π' may also be said as a 2-dimensional lattice plane that passes through Q_0. There can exist no lattice points of G between Π and Π'. We rephrase that Π and Π' are $l - 1 = 2$-dimensional *parallel and neighboring* lattice planes.[11]

These 3-dimensional preliminary arguments give us almost the whole of structures arising in the general dimension $l \geq 2$ with spectral tests. We evade brain-twisting geometrical images of higher dimensions, and set out directly to summarize relevant results. Assume that a lattice G is given in E_l with a basal set of l basis vectors $\{\overrightarrow{Q_1Q_2}, \overrightarrow{Q_1Q_3}, \cdots, \overrightarrow{Q_1Q_l}, \overrightarrow{Q_1Q_0}\}$. The $l - 1$ basis vectors $\{\overrightarrow{Q_1Q_2}, \overrightarrow{Q_1Q_3}, \cdots, \overrightarrow{Q_1Q_l}\}$ span an $(l-1)$-dimensional hyperplane Π, which includes a side surface (or rather, an $l - 1$ dimensional hyperplane) of a lattice parallelepiped or a unit cell of *(another)* basal set of lattice vectors. Its intersection with the lattice G gives the $(l-1)$-dimensional sublattice G_{l-1} of G including l points $\{Q_1, Q_2, \cdots, Q_l\}$. The parallel translation of Π_{l-1} by the vector $-\overrightarrow{Q_0Q_1}$ gives one more of hyperplane sublattice Π'_{l-1} which is parallel and adjacent to Π_{l-1}. Finally, define

[10] This parallelepiped is different from the one spanned by $\{\overrightarrow{Q_0Q_1}, \overrightarrow{Q_0Q_2}, \overrightarrow{Q_0Q_3}\}$, but both are unit cells or building blocks of the lattice G in the terminology of physicists, though two unit cells are distinct.

[11] Any two planes containing opposite surfaces of a parallelepiped spanned by arbitrary set of basis vectors are parallel and neighboring lattice (hyper)planes of $l - 1$-dimension.

the linear hull spanned by the basal set of l-vectors $\{\overrightarrow{Q_0Q_1}, \overrightarrow{Q_0Q_2}, \cdots, \overrightarrow{Q_0Q_l}\}$ in E_l as

$$\{\boldsymbol{r} = c_1\overrightarrow{Q_0Q_1} + c_2\overrightarrow{Q_0Q_2} + \cdots + c_l\overrightarrow{Q_0Q_l} |\ \ c_j \geq 0, \quad c_1 + c_2 + \cdots + c_l \leq 1\}$$

and call it the l-simplex spanned by vectors $\{\overrightarrow{Q_0Q_1}, \overrightarrow{Q_0Q_2}, \cdots, \overrightarrow{Q_0Q_l}\}$. We regard it also as a cone with the vertex Q_0 on the $(l-1)$-dimensional base hyperplane B spanned by $l-1$ vectors $\{\overrightarrow{Q_1Q_2}, \overrightarrow{Q_1Q_3}, \cdots, \overrightarrow{Q_1Q_l}\}$. We have now a clear overview on the distance between parallel and neighboring $(l-1)$-dimensional lattice hyperplanes Π and Π'; it is the height of the vertex Q_0 in the l-simplex to the base hyperplane B of $(l-1)$-dimension. This conclusion is general.

Corollary 2. Let a lattice G of l-dimensional position vectors be given in the Euclidean space E_l for $l \geq 2$.

(A) The distance λ, between any pair of $(l-1)$-dimensional parallel and neighboring lattice hyperplanes, is the height of a vertex, in an l-simplex spanned by a basal set of l-lattice vectors, to its base $(l-1)$-hyperplane.

(B) Conversely, consider any l-simplex spanned by an arbitrary basal set of l lattice vectors. The height λ of its arbitrary vertex, to the base $(l-1)$-dimensional hyperplane facing it, is the distance of some pair of parallel and neighboring lattice hyperplanes. **(End of Corollary 2)**

The above gives the basis of spectral tests of (d, z, n) generators in the following form.

Theorem 3. The largest distance between parallel and neighboring $(l-1)$-dimensional lattice hyperplanes of a lattice G in the space E_l is the largest of heights of vertices, in all l-simplexes spanned by basal sets of lattice vectors with one and the same hypervolume, to $(l-1)$-dimensional base hyperplanes that respectively face the vertices. In an l-simplex formed by a basal set of lattice vectors of G, the vertex with the largest height is the one that faces the $(l-1)$-dimensional base hyperplane with the smallest hyperarea in the l-simplex. **(End of Theorem 3)**

It was noted that any unit cells of a lattice of our concern have one and the same volume v. As cones constructing unit cells, l-simplexes spanned by basal sets of basis vectors, or more briefly basal l-simplexes, also have one and the same volume $v/l!$, as multiple integral construction will readily convince us. Though this explicit value is not much interesting, the overview is transparent; in a lattice the largest distance of parallel and neighboring $(l-1)$-dimensional lattice hyperplanes may be sought considering only the largest height of vertices in basal l-simplexes with one and the same volume. This prospect will be a great help to spectral test problems, but there still remains a multitude of ways to take basal l-simplexes. Which is the noted basal l-simplex with the smallest base hyperplanes of $(l-1)$-dimension? The answer is simple in the ideal form of regular simplexes.

4. Regular Simplexes

As plots in **Fig.1** indicate, the geometrically adequate form of a basal $l = 2$-simplex forming lattices of our concern in E_2 is a regular triangle. In the general l-dimension it is the form of a regular simplex, which is defined as follows.

Definition 4. A regular l-simplex with $l + 1$ vertices is defined by the restriction that all of its edges, $l(l + 1)/2$ in number, have one and the same length. **(End of Definition 4)**.

The first notable fact is that the definition determines a unique shape. This is seen inductively. For some later conveniences we show this process of induction as a corollary.

Corollary 5. For any dimension $l \geq 2$ the regular l-simplex S_l with $l + 1$ vertices is constructed on a regular $(l - 1)$-simplex S_{l-1} by taking a point in E_l that is equidistantly located to all l vertices of S_{l-1}. The geometrical shape of a regular l-simplex is thus unique.

(Proof) We proceed inductively with the dimension $l = 2, 3, \cdots$. In E_2 the regular 2-simplex is the regular triangle, which is the unique form as the construction with a compass on a line element (a regular 1-simplex) shows. In E_3 with $l = 3$ a regular 3-simplex should be constructed with a vertex facing a regular 2-simplex or a regular triangle. Its $l + 1 = 4$-th vertex should take its position at equal distances from vertices of the regular triangle. Thus the 4-th vertex can only have its location on the perpendicular line from the centroid of the base regular 2-simplex, and the unique possible shape is a regular tetrahedron. This inductive and unique construction of a regular l-simplex proceeds indefinitely to any dimension $l \geq 2$. We complete this proof of existence and uniqueness by computing the unique form of a regular l-simplex in the following theorem adapted to spectral test problems. ■

Theorem 6. The form of the regular l-simplex is unique for any $l \geq 2$. With its volume $d^{l-1}/l!$ given, this unique form of the regular l-simplex realizes one and the same height $\mu_d^{(l)}$ for any of its vertex from the base $(l - 1)$-dimensional lattice hyperplane. There holds

$$\mu_d^{(l)} = l^{-1/2}(l + 1)^{(l-1)/(2l)} d^{(l-1)/l}.$$

(Proof) Assume $l \geq 2$ and take the following vectors issuing from O:

$$\begin{aligned}
\boldsymbol{e}_1{}' := \overrightarrow{OQ_1} &= (b, a, a, \cdots, a, a), \\
\boldsymbol{e}_2{}' := \overrightarrow{OQ_2} &= (a, b, a, \cdots, a, a), \\
\boldsymbol{e}_3{}' := \overrightarrow{OQ_3} &= (a, a, b, \cdots, a, a), \\
&\cdots\cdots\cdots \\
\boldsymbol{e}_{l-1}{}' := \overrightarrow{OQ_{l-1}} &= (a, a, a, \cdots, b, a), \\
\boldsymbol{e}_l{}' := \overrightarrow{OQ_l} &= (a, a, a, \cdots, a, b).
\end{aligned}$$

Here $a, b \neq 0$ are constants to be determined by the following two requirements:

(1) These vectors span the volume d^{l-1} by the absolute value of their determinant.

(2) They form a regular l-simplex.

Assumed vector forms are linearly independent. They have one and the same $\|\boldsymbol{e}_j{}'\|^2 = (l-1)a^2 + b^2$ as the square of their Euclidean length for any $1 \le j \le l$. Also, they give $(\boldsymbol{e}_i{}', \boldsymbol{e}_j{}') = (l-2)a^2 + 2ab$ as inner products for any $i \ne j$, implying any pair of vectors $\overrightarrow{OQ_j}$ for $1 \le j \le l$ form an equal angle between them. From these relations, or from the direct computation we have:

$$\|\boldsymbol{e}_i{}' - \boldsymbol{e}_j{}'\|^2 = \|\overrightarrow{Q_iQ_j}\|^2 = 2(b-a)^2, \quad i \ne j, \quad 1 \le i, j \le l.$$

This implies that l points $\{Q_1, Q_2, \cdots, Q_l\}$ form a regular $(l-1)$-simplex, in accordance with what was seen in induction processes. If only this length is the same as $\|\boldsymbol{e}_k{}'\|$ for any $1 \le k \le l$, the form spanned is the regular l-simplex as sought. By the way, the unit vector $\boldsymbol{e}_0{}' := (1, 1, 1, \cdots, 1, 1)/l^{1/2}$ gives the inner product

$$(\boldsymbol{e}_0{}', \boldsymbol{e}_j{}') = \{(l-1)a + b\}/l^{1/2} =: \mu \quad (1 \le j \le l).$$

This μ is the distance or the height of the vertex O to the centroid of the $(l-1)$-dimensional base hyperplane spanned by $\{Q_1, Q_2, \cdots, Q_l\}$. Therefore, μ is the one and the same height of any vertex to its facing base hyperplane of $(l-1)$-dimension (which by itself is a regular $(l-1)$-simplex) in the regular l-simplex spanned. Finally, these vectors with unknowns have the determinant,

$$\begin{vmatrix} b & a & a & \cdot & \cdot & \cdot & a & a \\ a & b & a & \cdot & \cdot & \cdot & a & a \\ a & a & b & \cdot & \cdot & \cdot & a & a \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a & a & a & \cdot & \cdot & \cdot & b & a \\ a & a & a & \cdot & \cdot & \cdot & a & b \end{vmatrix} = \begin{vmatrix} s & s & s & \cdot & \cdot & \cdot & s & s \\ a & b & a & \cdot & \cdot & \cdot & a & a \\ a & a & b & \cdot & \cdot & \cdot & a & a \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a & a & a & \cdot & \cdot & \cdot & b & a \\ a & a & a & \cdot & \cdot & \cdot & a & b \end{vmatrix} = \begin{vmatrix} s & 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ a & c & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ a & 0 & c & \cdot & \cdot & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a & 0 & 0 & \cdot & \cdot & \cdot & c & 0 \\ a & 0 & 0 & \cdot & \cdot & \cdot & 0 & c \end{vmatrix} = sc^{l-1},$$

with $s := (l-1)a + b$ and $c := b - a$. This gives the final restriction $d^{l-1} = sc^{l-1}$ to determine a and b. Putting $b = \xi a$, we arrive at the equations to be solved, $\xi^2 + (l-1) = 2(\xi - 1)^2$. Some algebra gives the same answer to both solutions of ξ, and we have for $l \ge 2$,

$$\mu = \overline{\mu}_d^{(l)} = l^{-1/2}(l+1)^{(l-1)/(2l)} d^{(l-1)/l}. \qquad \blacksquare$$

The explicit forms of $\mu_d^{(l)}$ are as follows for $2 \le l \le 6$:

$$\begin{aligned} \overline{\mu}_d^{(2)} &:= 2^{-1/2} 3^{1/4} d^{1/2} \approx 0.93060 d^{1/2}, \\ \overline{\mu}_d^{(3)} &:= 3^{-1/2} 4^{2/6} d^{2/3} \approx 0.91649 d^{2/3}, \\ \overline{\mu}_d^{(4)} &:= 4^{-1/2} 5^{3/8} d^{3/4} \approx 0.91429 d^{3/4}, \\ \overline{\mu}_d^{(5)} &:= 5^{-1/2} 6^{4/10} d^{4/5} \approx 0.91575 d^{4/5}, \\ \overline{\mu}_d^{(6)} &:= 6^{-1/2} 7^{5/12} d^{5/6} \approx 0.91844 d^{5/6}. \end{aligned}$$

Fishman and Moore (1986) quoted the geometry of numbers for *the smallest value* $\overline{\lambda}_d^{(l)}$ *of the largest distance* $\lambda_d^{(l)}(z)$ *of parallel and neighboring lattice hyperplanes in the* l*-dimensional lattice* $G_l(d, z)$*,*

and conducted their epoch making exhaustive spectral tests on primitive roots of the Mersenne prime modulus $d = 2^{31} - 1$. Values of $\{\overline{\lambda}_d^{(l)} |\ 2 \le l \le 6\}$ in their Eq. (15) are as follows:

$$\overline{\lambda}_d^{(2)} := \overline{\mu}_d^{(2)} = 2^{-1/2} 3^{1/4} d^{1/2} \approx 0.93060 d^{1/2},$$
$$\overline{\lambda}_d^{(3)} := 2^{-1/6} d^{2/3} \approx 0.80909 d^{2/3},$$
$$\overline{\lambda}_d^{(4)} := 2^{-1/4} d^{3/4} \approx 0.84090 d^{3/4},$$
$$\overline{\lambda}_d^{(5)} := 2^{-3/10} d^{4/5} \approx 0.81225 d^{4/5},$$
$$\overline{\lambda}_d^{(6)} := 2^{-1/2} 3^{1/12} d^{5/6} \approx 0.77490 d^{5/6}.$$

These are smaller than $\overline{\mu}_d^{(l)}$ for $l \ge 3$. In brief, Fishman and Moore performed spectral tests taking the global minima of largest distances for neighboring parallel lattice hyperplanes as the values to be realized by (d, z) generators.

As **Theorem 3**, as well as forthcoming **Theorem 7** and **Corollary 8** show, methods of traditional spectral tests are all natural in the point to look for $\lambda_d^{(l)}(z)$, the smallest value of the largest distance between parallel and neighboring $(l-1)$-dimensional lattice hyperplanes, in the lattice $G_l(d, z)$. However, differences in noted ideal values are not only conspicuous but also give decisive qualitative differences to the results of spectral tests. For one thing, the new criteria are certainly respecting the invariance that appropriate ways of shuffling of two uniform and independent random number sequences should give again a sequence with uniformity and indepence. The method to use two odd-prime-power moduluses was introduced by the present inventors with the aim to exploit this invariance, as a promising method to lessen the heavy burden of spectral test computation. To their dismay, efforts with various trials regarding choices of component generators were not much successful in obtaining shuffled generators of excellence in the traditional criteria. In contrast, the adoption of new criteria based on regular simplex values immediately lead inventors to magnificent successes, which strongly suggests that valuations based on $\mu_d^{(l)}$ are successful in respecting the noted invariance in the shuffling.

Readers are asked to consult the homepage of inventors, *http://www10.plala.or.jp/h-nkzw/*, for details of results. Also, the Catalogue of good and excellent generators will soon be posted in Store of Nakazawa Patents, *http://nakazawa-patents.jp*, together with the associated Technological Reports and Guidances how the successful spectral test computation are to be lead, and some further knowhows, such as the parallel generation of random numbers, cares in spectral tests and generation with the use of only double precision computation, and so forth, will also be posted in separate URLs noted in the Store of Nakazawa Patents.

Before turning to other problems, there is a need to discuss with a lattice G in the space E_l for $l \ge 2$ with regular l-simplexes as its building blocks, how its largest distance λ between parallel and

neighboring $(l-1)$-dimensional lattice hyperplanes may be expressed. Consider the case $l=2$. Even if a lattice G in the plane E_2 may have a regular 2-simplex (or a regular triangle connecting nearest 3 lattice points of G) as is building blocks, there exist multitudes of other 2-simplex forms that may give building blocks likewise. From **Theorem 3** we have only that λ is the largest height of vertices taken over all vertices of possible 2-simplexes. However, the restriction, that the areas of any 2-simplexes take one and the same value in a lattice G, stipulates that the shortest base line of 2-simplexes or triangles among all possible shapes should give the largest height of the vertex or λ. What, then, is the triangle that gives this shortest base line? The answer is manifestly the shortest lattice vector connecting neighboring lattice points in G, which is certainly the basal regular triangle or the regular 2-simplex. Therefore, any vertex of any basal regular 2-simplex has this λ as its height.

We may go ahead to a lattice G in E_3 that has basal 3-simplexes (or regular tetrahedrons) as its building blocks. The arguments proceeds just the same, and the problem is to find the regular 3-simplex that has its 2-dimensional base hyperplane (or a triangle forming the side) that has the smallest 2-dimensional area among all 3-simplexes. The trivial answer is the triangle formed by the *neighboring nearest* 3 lattice points of G, or the regular and the smallest triangle (i.e. a regular 2-simplex) that may be formed by lattice points. The distance λ is the height of any vertices of a regular 3-simplex.

Let us proceed one further step. In the dimension $l=4$ the 3-dimensional base hyperplane of a 4-simplex is a 3-simplex (or a tetrahedron) formed by 4 lattice points. The smallest 3-dimensional hyperarea (or the 3-dimensional volume) that this tetrahedron can have is formed by 4 neighboring and nearest lattice points in a basal regular 4-simplex, and the distance λ is the height of any vertices of a regular basal 4-simplex in G.

We shall need no more arguments to see through the following.

Theorem 7. Call a lattice G in the Euclidean space E_l with $l \geq 2$ to be *regular* if G has regular basal l-simplexes as its building blocks. A regular lattice G has the largest distance λ between its parallel and neighboring $(l-1)$-dimensional lattice hyperplanes as the height of any vertex in its basal regular l-simplex to the facing $(l-1)$-dimensional base hyperplane. **(End of Theorem 7)**

This theorem shows that the largest distance λ of parallel and neighboring lattice hyperplanes is a good discriminator for us to judge whether the lattice G is regular or not. There exist a few matters to be noted, however. The one is that a regular lattice G in E_l requires irrational coordinates for its lattice points, while the lattice $G_l(d,z)$ associated with l-tuples of consecutive random numbers generated from (d,z) generator are restricted to have integral or rational coordinates, and can never realize a regular lattice in the strict sense of words. Yet, noted regular lattice structures provide us with an invaluable chance to exploit the continuity of real numbers to integer problems of $G_l(d,z)$,

as a kind of Diophantine approximation.

The other point is indicated by the following.

Corollary 8. Let G be a reguglar lattice in the l-dimensional space E_l. Denote λ for the largest distance between its parallel and neighboring $(l-1)$ -dimensional lattice hyperplanes. Infinitesimal deformations of the geometry of G to G' make λ change to $\lambda' > \lambda$. Stated differently, the regular form of a lattice is geometrically a local minimum in the variation of λ.

(Proof) The largest distance λ is associated with basal l-simplexes of G with the smallest $(l-1)$-dimensional base lattice hyperplanes (which are by themselves regular $(l-1)$-simplexes) with the hyperarea S with the property that any other form of basal l-simplex has its base $(l-1)$-simplex with the hyperarea not smaller than S. Assume that some infinitesimal deformation of the lattice G to G', which keeps the hypervolume of basal l-simplexes invariant, can induce the change $\lambda \to \lambda'$ with $\lambda' < \lambda$. We discuss that this is absurd. If the assumption is true, then the largest base hyperarea S' of any basal l-simplexes of the lattice G' will fulfill $S' > S$. This will contradict the condition that all basal l-simplexes of G and G' should have the same hypervolume.[12] ■

Implications of **Corollary 8** is not small. Since reference values satisfy $\overline{\mu}_d^{(l)} > \overline{\lambda}_d^{(l)}$ for $l \geq 3$, and the geometry of numbers predict that lattices with their $\lambda_d^{(l)}(z)$ in the inverval $(\overline{\lambda}_d^{(l)}, \overline{\mu}_d^{(l)})$ may arise, some lattices $G_l(d,z)$ may give values $\mu_d^{(l)}(z) := \lambda_d^{(l)}(z)/\overline{\mu}_d^{(l)} \leq 1$. In fact, a generator listed in Fishman and Moore (1986) has this property, upon the transformation to the present $\mu_d^{(6)}(z)$:

$$d = 2^{31} - 1, \quad z = 1226874159, \quad \lambda_d^{(6)}(z) = 1.18426026, \quad \mu_d^{(6)}(z) = 0.99917993 < 1.$$

This primitive root multiplier z gives

$$\lambda_d^{(2)}(z^2) = 3.51885751, \quad \lambda_d^{(2)}(z^3) = 2.19846315,$$

as posted in **List 2 (c)** of **I**. Therefore, the multiplier z cannot be passable to start with. But it is interesting what arises in the space E_6 with the valuation $\mu_d^{(6)}(z) < 1$.

The present inventors insist to post **Corollary 8** not as a conjecture. This is based on experiences of the computation of spectral tests. A generator (p,z) of a prime p and its primitive root z is tested by the 2nd degree spectral tests of (p, z^k) for $1 \leq k \leq 12$. Two generators (p_j, z_j) for $j = 1, 2$, taken from sets of primes and their primitive roots that passed the 1st stage 2nd degree tests, are then combined to a generator (d,z) by $d = p_1 p_2$ and $z \equiv z_j \bmod (p_j)$, generators (d, z^k) for $1 \leq k \leq 6$

[12]The reasoning here is incomplete, and a more rigorous arguments will be needed. Despite efforts inventors could not find a truly convincing proof, though the conclusion seems all natural. Thus, this **Corollary** will need to be stated as a conjecture. However, there exist side evidences obtained from computations of spectral tests that support this **Corollary**; see later remarks. We therefore let this **Corollary** go as it is. Inventors shall be deeply obliged if Readers kindly communicate to N. and H. Nakazawa in *nmail@nakazawa-patens.jp*; inventors then shall post them, if not inconvenient to contributors, in this homepage with contributors' names.

are examined by the 2nd stage 2nd degree tests, and finally (d, z) underwent 3rd to 6th degree spectral tests. Watching how the combined generator passers behave in the final 3rd to 6th degree tests,[13] we saw no trace of valuations that are smaller than or equal to 1. This indicates that the first stage 2nd degree tests will be efficient enough to expel exotic forms of lattices with $\mu_d^{(l)}(z) \leq 1$ for $l \geq 3$, and to select only generators that are in the *attracting basins of local minima at regular l-simplex forms*. We should admit that this is yet not completely proven. Theoretical as well as computational contributions from readers are waited for at *nmail@nakazawa-patents.jp*.

5. Cocluding Remarks

5.1. The Claim Stated in the Patent Application of Invention 2

The claim of the patent of the present invention applied to Patent Offices of Nations are as follows. Please note that there are a few adaptations of symbols to the present report.

Claim[14]

What is claimed is a new method of spectral tests, on multiplicative congruential generator (d, z, n) or (d, z) comprising an odd integer d for the modulus and an integer z coprime with d for the multiplier and an integer n coprime with d for the *seed* and generating the sequence of integers $\{n_k :\equiv nz^{k-1} \bmod (d) |\ 1 \leq n_k \leq d,\ \ k = 1, 2, \cdots\}$ consecutively and giving the output random number sequence by realizing the arithmetic $\{v_k := n_k/d |\ 0 \leq v_k \leq 1,\ \ k = 1, 2, \cdots\}$, the new method being based on the valuation of the geometrical form of the lattice $G_l(d, z)$, wherein l-consecutive integer outputs of the generator (d, z, n) $\{Q_k := (m_k, n_{k+1}, \cdots, n_{k+l-1}) |\ k = 1, 2, \cdots\}$ take their seats, through the computation of the largest distance $\lambda_d^{(l)}(z)$ between parallel and neighboring lattice hyperplanes of $G_l(d, z)$ and evaluating $\mu_d^{(l)}(z) := \lambda_d^{(l)}(z)/\overline{\mu}_d^{(l)}$ of the generator (d, z) on the basis of new reference values

$$\overline{\mu}_d^{(l)} := l^{-1/2}(l+1)^{(l-1)/(2l)} d^{(l-1)/l},\ \ l \geq 3,$$

and judging (d, z) to be passable if conditions

$$1 < \mu_d^{(l)}(z) < R_l, \quad 3 \leq l \leq 6,$$

are fulfilled for the prescribed levels $\{R_l > 1 |\ 3 \leq l \leq 6\}$.

[13] Luckily or unluckily to say, noted tests take quite long time, and outputting results of tests of all degrees gives no burden to the computation.

[14] In the specification submitted to Patent Offices of Nations there was an omission of the restriction for the integer d that $d > 0$ should hold. We post it below with this flaw corrected. Though this restriction is obvious by the statement $1 \leq n_k \leq d$ given further below, inventors express their sincere regrets for their carelessness to Patent Offices of Nations.

5.2. Procedures for Spectral Tests

Let there be given a lattice G in the space E_l for $l \geq 2$. Spectral tests aim to compute the largest distances between parallel and neighboring lattice hyperplanes, and **Theorem 3** reduces the problem to the search of the basal l-simplex that has the vertex with the largest height from its facing base $(l-1)$-dimensional lattice hyperplane among all basal l-simplexes with one and the same hypervolume. If the lattice G has a regular basal l-simplex i.e. if G is a regular lattice, the search is not necessary as shown in Theorem 7. A general lattice does not give us such a simple circumstance. And, even if the lattice might be regular, it may happen that we do not know of the existence of a regular basal l-simplex. In such general cases we should perform spectral tests to obtain the noted largest distance λ between parallel and neighboring $(l-1)$-dimensional lattice hyperplanes, and give the valuation $\mu := \lambda/\overline{\mu}$ to infer how close the lattice G is to the regular case.[15]

We now discuss the procedure of this search for the largest distance between $(l-1)$-dimensional parallel and neighboring lattice hyperplanes, assuming that a set of basis vectors $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$ of G is given. The search is facilitated by the well-known *dual* lattice vectors.

Definition 9. Let row vectors $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$ be a set of basis vectors of G in E_l with $l \geq 2$. Denote M for the matrix formed by these basis vectors as rows.

(A) Let M^{-1} be the inverse matrix of M, and row vectors of ${}^tM^{-1}$ be denoted as $\{\boldsymbol{f}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_l\}$, where ${}^tM^{-1}$ is the transpose of the matrix M^{-1}. These (row) vectors $\{\boldsymbol{f}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_l\}$ are named as *dual basis vectors* corresponding to the basal set $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$ of G.

(B) The lattice G^*,

$$G^* := \{c_1\boldsymbol{f}_1 + c_2\boldsymbol{f}_2 + \cdots + c_l\boldsymbol{f}_l |\ \ c_j \text{ runs all integers for } 1 \leq j \leq l\},$$

spanned by dual lattice basis vectors will be called the dual lattice G^* of G, **(End of Definition 9)**

Corollary 10. Let G be a lattice in E_l. The dual lattice G^* is unique irrespective of the choice of the set of basis vectors that defines the set of dual basis vectors.

(Proof) Let there be given a basal set of lattice vectors $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$, the matrix M formed by them as rows, and the matrix $M^* := {}^tM^{-1}$ of dual lattice row vectors. Any other choice of basis

[15] Here should be noted a difficult problem arising with the higher dimension l. We have noted that in E_l a generator (d, z) gives only $N \approx d/2$ or $d/4$ of consecutive l-tuples. Therefore, the hypercube of unit volume can be divided meaningfully only into subhypercubes of side length $1/d^{1/l}$ in each of which one consecutive l-tuple of random number point can be distributed, if at all. If $d \approx 2^{52}$ is the case, we see little problems with the consecutive 2-points emitted, because $l = 2$ gives $1/d^{1/2} \approx 2^{-26}$ is sufficiently small. But $l = 6$ gives $1/d^{1/l} \approx 2^{-8} \approx 1/256$. Therefore, the distribution in subhypercubes in E_6 may be discussed only in a rather coarse scale. Is it that the good distribution of seats in this coarse scale in fact ensure the good statistical distribution of random number points? We do not have a decisive answer as yet. However, one certain thing is that a regular distribution of seats will be less problematic than the distribution of seats concentrated in fewer number of $(l-1)$-dimensional lattice hyperplanes with large separation between them. Thus we demand that the results of $2 \leq l \leq 6$ should be good for a generator to be excellent, admitting, as we hear to be from predecessors in random number problems, the lower degree performances, in particular those of the 2nd degree tests, will be the most significant.

vectors of the lattice G will give the matrix $M' = UM$ with a unimodular matrix U. Therefore, $M = U^{-1}M'$ holds true, and we have

$$M^* = {}^t(U^{-1}M')^{-1} = {}^tU\,{}^t(M')^{-1} = {}^tU(M')^*.$$

Since ${}^tU$ is a unimodular matrix, the lattice G^* spanned by the basal set of row vectors of M^* and the lattice $(G')^*$ spanned by those of ${}^tU(M')^*$ are identical. ■

We are now nearing the principle of spectral tests.

Theorem 11. Let there be given in E_l a lattice G. The largest distance λ, between paralle and neighboring $(l-1)$-dimensional lattice hyperplanes of G, is given by the following:

$$\lambda = 1/\|\boldsymbol{f}_{\min}\|.$$

Here $\boldsymbol{f}_{\min}$ is the dual lattice vector $\boldsymbol{f} \in M^*$ whose non-zero Euclidean length $\|\boldsymbol{f}\|$ is the shortest.

(Proof) From **Theorem 3** λ is a height of a vertex in an l-simplex spanned by a basal set of lattice vectors of G. Let the basal set of vectors, which are of course a set of basis vectors, of G be $\{\overrightarrow{Q_0Q_1}, \overrightarrow{Q_0Q_2}, \cdots, \overrightarrow{Q_0Q_l}\}$. Consider the height of the vertex Q_0 to the $(l-1)$-dimensional facing base hyperplane spanned by $\boldsymbol{e}_2 := \overrightarrow{Q_1Q_2}, \boldsymbol{e}_3 := \overrightarrow{Q_1Q_3}, \cdots, \boldsymbol{e}_l := \overrightarrow{Q_1Q_l}$. We use again the trick that these $(l-1)$-vectors and $\boldsymbol{e}_1 := -\overrightarrow{Q_0Q_1}$ are a unimodular transformation of the given set of basal vectors, so that $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$ may be taken as the basis vectors, which give the dual basis (row) vectors $\{\boldsymbol{f}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_l\}$. The definition of dual basis vectors may be written in the form of inner products,

$$(\boldsymbol{e}_j, \boldsymbol{f}_k) = \delta_{jk}, \quad 1 \le j, k \le l.$$

Therefore, the dual vector $\boldsymbol{f}_1$ is orthogonal to all of $\{\boldsymbol{e}_2, \boldsymbol{e}_3, \cdots, \boldsymbol{e}_l\}$. Put λ for the height of the vertex Q_0 in the originaly given basal l-simplex to the facing $(l-1)$-dimensional base hyperplane which is now spanned by $\{\boldsymbol{e}_2, \boldsymbol{e}_3, \cdots, \boldsymbol{e}_l\}$. We have at once

$$\lambda = |(\boldsymbol{e}_1, \boldsymbol{f}_1)|/\|\boldsymbol{f}_1\| = 1/\|\boldsymbol{f}_1\|.$$

Taking the largest of this value over all basal l-simplexes (hence over all basal l simplexes of dual lattice) and over all their vertices, we obtain the assertion. ■

The final clue to spectral tests requires the explicit form of the $G_l(d, z)$ lattice. We note for clarity again basis vectors of this lattice given previously in p. 3,

$$\begin{aligned}
\boldsymbol{e}_1 &:= (1, z, z^2, z^3, \cdots, z^{l-2}, z^{l-1}),\\
\boldsymbol{e}_2 &:= (0, d, 0, 0, \cdots, 0, 0),\\
\boldsymbol{e}_3 &:= (0, 0, d, 0, \cdots, 0, 0),\\
\boldsymbol{e}_4 &:= (0, 0, 0, d, \cdots, 0, 0),
\end{aligned}$$

$$\cdots\cdots\cdots\cdots\cdots,$$
$$\boldsymbol{e}_{l-1} := (0,0,0,0,\cdots,d,0),$$
$$\boldsymbol{e}_{l} := (0,0,0,0,\cdots,0,d).$$

Their dual basis vectors are traditionally and conveniently taken in the following form:

$$\boldsymbol{f}_1{}' := (d,0,0,0,\cdots,0,0),$$
$$\boldsymbol{f}_2{}' := (-z,1,0,0,\cdots,0,0),$$
$$\boldsymbol{f}_3{}' := (-z^2,0,1,0,\cdots,0,0),$$
$$\boldsymbol{f}_4{}' := (-z^3,0,0,1,\cdots,0,0),$$
$$\cdots\cdots\cdots\cdots\cdots,$$
$$\boldsymbol{f}_{l-1}{}' := (-z^{l-2},0,0,0,\cdots,1,0),$$
$$\boldsymbol{f}_l{}' := (-z^{l-1},0,0,0,\cdots,0,1).$$

It will be at once to see that these give the matrix $M^{*\prime}$ with $M\,{}^tM^{*\prime} = dI$. Therefore, $\boldsymbol{f}_{\min}{}'/d$ should replace $\boldsymbol{f}_{\min}$ in **Theorem 11**. We thus have:

Corollary 12. In the lattice $G_l(d,z)$ of the multiplicative congruential generator (d,z), the largest distance λ between parallel and neighboring $(l-1)$-dimensional lattice hyperplanes is given by

$$\lambda = d/\|\boldsymbol{f}_{\min}{}'\|,$$

where $\boldsymbol{f}_{\min}{}'$ is the shortest vector in the traditional dual lattice of spectral tests spanned conveniently by the set of *integer* basis vectors$\{\boldsymbol{f}_1{}', \boldsymbol{f}_2{}', \cdots, \boldsymbol{f}_l{}'\}$. **(End of Corollary 12)**

In this form the search of the traditional shortest dual integer vector is facilitated with integer cartesian coordinates. It is not that all of vectors $\boldsymbol{f}' = (x_1, x_2, \cdots, x_l)$ with integer coordinates are dual lattice vectors. But the discrimination is easy.

Lemma 13. A vector $\boldsymbol{f}' = (x_1, x_2, \cdots, x_l)$ with integer cartesian coordinates is a traditional dual lattice vector for the lattice $G_l(d,z)$, if and only if the following holds true:

$$x_1 + zx_2 + z^2x_3 + \cdots + z^{l-2}x_{l-1} + z^{l-1}x_l \equiv 0 \bmod (d).$$

(Proof) Suppose that the condition is satisfied. Then an integer k exists and gives

$$x_1 + zx_2 + z^2x_3 + \cdots + z^{l-2}x_{l-1} + z^{l-1}x_l = kd,$$
$$\boldsymbol{f}' = (kd - zx_2 - z^2x_3 - \cdots - z^{l-2}x_{l-1} - z^{l-1}x_l, x_2, x_3, \cdots, x_{l-1}, x_l)$$
$$= k\boldsymbol{f}_1{}' + x_2\boldsymbol{f}_2{}' + x_3\boldsymbol{f}_3{}' + \cdots + x_{l-1}\boldsymbol{f}_{l-1}{}' + x_l\boldsymbol{f}_l{}'.$$

This is an integral linear combination of $\{\boldsymbol{f}_1{}', \boldsymbol{f}_2{}', \cdots, \boldsymbol{f}_l{}'\}$ or a dual lattice vector in the sense of spectral tests, and the *if* part is proved. Take a vector $\boldsymbol{f}'$ with integral coefficients $\{c_1, c_2, \cdots, c_l\}$ in

the form $\boldsymbol{f}' = c_1 \boldsymbol{f}_1{}' + c_2 \boldsymbol{f}_2{}' + \cdots + c_l \boldsymbol{f}_l{}'$. We have

$$\boldsymbol{f}' = (c_1 d - z c_2 - z^2 c_3 - \cdots - z^{l-1} c_l, c_2, c_3, \cdots, c_l).$$

Therefore, the condition $x_1 + z x_2 + z^2 x_3 + \cdots + z^{l-2} x_{l-1} + z^{l-1} x_l = c_1 d \equiv 0 \bmod (d)$ is satisfied. This proves the *only if* part. ■

5.3. An Example

Actual procedures of spectral tests form a gigantic conglomerate of arts of computing with integer arithmetic, together with a heap of efforts needed for optimization. The restriction to integers is a great help in that any length of computations do not introduce any accumulation of errors, such as the truncation and round off errors of real arithmetic. But we need to be careful with a modulus d as large as $d \approx 2^{48}$; relevant integers on the stage will readily give their products which go out of 8 Bytes limitations. If you are able to use 16 Bytes integers, you should do so at any cost. The constrution of d with two large integers will lessen such burdens by the powerful aid of Sun Tzu's theorem, but at the expense of longer computing times.

From their experiences, the inventors feel that a solved problem will be a great help in debugging programs, in estimating necessary computing times, and (of course) in *feeling* how laborious the finding of an excellent generator could be. Thus we close this report with one such example, which might be not very much attractive, but which in fact is a great progress compared with the precedents.

The modulus d is constructed as

$$d = 2473412495072041 = p_1 p_2 \approx 2^{51.14}, \quad p_1 = 78825767, \quad p_2 = 31378223.$$

The multiplier z consists of primitive roots z_1 of p_1 and z_2 of p_2;

$$z_1 = 13798799, \quad z_2 = 588527, \quad z = 1629813080852781 \equiv z_j \bmod (p_j), \quad j = 1, 2.$$

The answer to be obtained with (d, z) is the following:

degree of tests	2	3	4	5	6
spectral test valuations	1.16151106	1.24863727	1.23847495	1.14057211	1.12413372

multiplier	z^2	z^3	z^4	z^5	z^6
2nd degree valuations	1.05738174	1.13282851	1.24149179	1.16041734	1.21926692

Trials should be commenced with 2nd degree tests which will soon reward the noted results. In contrast, 5th and 6th degree tests are time consuming. The computer of the inventors took about 3 days for them. But, of course, the true difficulty is not in this particular computation; it is in the time-consuming search process with uncertain prospect over which a sudden reversal brings us a

conviction of success. The inventors sincerely wish willing explorers to join the exploration in the desert of integers with all barren outlook, and experience the joy of finding a clear spring or a brilliant gem stone, for generators with still longer periods and brighter excellences.