ALGORITHM FOR GENERATING ORTHOGONAL MATRICES WITH RATIONAL ELEMENTS.

Ruslan A. Sharipov

Abstract. Special orthogonal $n \times n$ matrices with rational elements form the group $\mathrm{SO}(n, \mathbb{Q})$, where $\mathbb{Q}$ is the field of rational numbers. Theorem describing the structure of arbitrary matrix from this group is proved. This theorem yields an algorithm for generating such matrices by means of random number routines.

1. Introduction.

Orthogonal matrices from the group $\mathrm{O}(n, \mathbb{R})$ describe rotations (or possibly rotations with reflections) in n-dimensional Euclidean space $\mathbb{R}^n$. Pure rotations correspond to another classical group $\mathrm{SO}(n, \mathbb{R})$, which is subgroup in $\mathrm{O}(n, \mathbb{R})$. The following matrix represent elementary rotation in p-q coordinate plane

$$O^{[p]}_{[q]}(\varphi) = \begin{Vmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \dots & \alpha & \dots & -\beta & \dots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \dots & \beta & \dots & \alpha & \dots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{Vmatrix}. \tag{1.1}$$

(p and q mark the rows and columns of the elements α and β.)

Here $\alpha = \cos(\varphi)$, $\beta = \sin(\varphi)$, and φ is an angle of rotation. Matrices of the form (1.1) can be treated as elements of $\mathrm{SO}(2, \mathbb{R})$ embedded into $\mathrm{SO}(n, \mathbb{R})$. Matrix

$$\Omega = \begin{Vmatrix} \boxed{O^*} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \begin{matrix} 0 & \dots & 0 \end{matrix} & 1 \end{Vmatrix} \tag{1.2}$$

with $O^* \in \mathrm{SO}(n-1, \mathbb{R})$ then is an element of $\mathrm{SO}(n-1, \mathbb{R})$ embedded into $\mathrm{SO}(n, \mathbb{R})$. For orthogonal matrices over the field of reals there is the following theorem.

Theorem 1.1. *Each orthogonal matrix $O \in \mathrm{SO}(n,\mathbb{R})$ can be represented as a product $O = O^{[1]}_{[2]}(\varphi_1) \cdot \ldots \cdot O^{[n-1]}_{[n]}(\varphi_{n-1}) \cdot \Omega$, where first $n-1$ terms are matrices of elementary rotations* (1.1)*, and Ω is an orthogonal matrix of the form* (1.2)*.*

Angles $\varphi_1, \ldots, \varphi_{n-1}$ in theorem 1.1 are known as Euler angles (see Chapter VII in [1] for three dimensional case). These angles are restricted by inequalities

$$0 \leqslant \varphi_1 \leqslant 2\pi, \qquad\qquad 0 \leqslant \varphi_i \leqslant \pi \quad \text{for} \quad i = 2, \ldots, n-1.$$

Applying theorem 1.1 recursively to O, then to O^* in (1.2), and so on, we easily prove the following theorem.

Theorem 1.2. *Each orthogonal matrix $O \in \mathrm{SO}(n,\mathbb{R})$ can be represented as a product of $n(n-1)/2$ matrices of elementary rotations* (1.1)*.*

Theorem 1.1 is not valid for orthogonal matrices over the field of rational numbers. As for theorem 1.2, I don't know if it is valid or not for $O \in \mathrm{SO}(n,\mathbb{Q})$. However, there is an algorithm for constructing orthogonal matrices over the field of rational numbers. This algorithm is exhausting, this means that each orthogonal matrix $O \in \mathrm{SO}(n,\mathbb{Q})$ could be obtained by applying this algorithm.

2. Stereographic projection.

Let $\mathfrak{S}$ be unit sphere in $\mathbb{R}^n$. We take the point S with coordinates $(0,\ldots,0,-1)$ as south pole on this sphere. Then equatorial hyperplane α is given by the equation $x^n = 0$, where x^n is n-th coordinate of a point of $\mathbb{R}^n$ (we use upper indices for coordinates of vectors and points according to Einstein's tensorial notation, which is popular in differential geometry and in general relativity). Let's consider a ray $[SX\rangle$ starting at south pole S and passing through a point $X \in \mathfrak{S}$. This ray crosses equatorial hyperplane at some point Y (as shown on figure 2.1 for three dimensional case). For each X point Y is unique. If we denote by $\mathfrak{S}^\circ$ the unit sphere $\mathfrak{S}$ with pinned off south pole S, then we get a map $f\colon \mathfrak{S}^\circ \to \alpha$ that maps $\mathfrak{S}^\circ$ onto equatorial hyperplane α. This map is called *stereographic projection*. It is bijective and smooth. It's very important for us that stereographic projection is given by rational functions. Indeed, if $x^1, \ldots, x^n$ are coordinates of the point $X \in \mathfrak{S}^\circ$ and if $y^1, \ldots, y^{n-1}$ coordinates of the point $Y = f(X)$, then for $y^1, \ldots, y^{n-1}$, we get

$$y^s = \frac{x^s}{1+x^n} \quad \text{for} \quad s = 1, \ldots, n-1. \tag{2.1}$$

Inverse map $f^{-1}\colon Y \to X$ is also given by rational functions. Indeed, we have

$$x^n = \left(1 - \sum_{i=1}^{n-1} (y^i)^2\right) \Bigg/ \left(1 + \sum_{i=1}^{n-1} (y^i)^2\right). \tag{2.2}$$

For other coordinates of the point X from (2.1) and (2.2) we derive

$$x^s = \frac{2\,y^s}{\left(1+\sum\limits_{i=1}^{n-1}(y^i)^2\right)}, \quad \text{where} \quad s = 1, \ldots, n-1. \tag{2.3}$$

Rationality of the expressions (2.1), (2.2), and (2.3) mean that rational points of pinned sphere $\mathfrak{S}^\circ$ are in one-to-one correspondence with rational points of equatorial hyperplane α. As for south pole S, it is usually associated with infinite point $Y = \infty$ on α. Indeed, passing to the limit $Y \to \infty$ in formulas (2.2) and (2.3), one can get coordinates of the point S.

3. Orthogonal matrices and ONB's.

Let $O \in \mathrm{SO}(n, \mathbb{Q})$ be some orthogonal matrix. Its columns can be treated as vectors in $\mathbb{Q}^n$. Let's denote them $\mathbf{e}_1, \ldots, \mathbf{e}_n$. Orthogonality of O means that transposed matrix O^T coincides with inverse matrix O^{-1}:

$$O \cdot O^T = 1. \tag{3.1}$$

Written in explicit form the equality (3.1) means that $\mathbf{e}_1, \ldots, \mathbf{e}_n$ are vectors of unit length perpendicular to each other. They form so called ONB (orthonormal base) in $\mathbb{Q}^n$ with respect to standard scalar product

$$(\mathbf{X},\, \mathbf{Y}) = \sum_{i=1}^{n} x^i\, y^i.$$

Matrices from special orthogonal group $\mathrm{SO}(n, \mathbb{Q})$ obey additional restriction

$$\det Q = 1. \tag{3.2}$$

For base vectors (3.2) means that $\mathbf{e}_1, \ldots, \mathbf{e}_n$ form *right oriented* ONB (or, simply saying, *right* ONB). In three dimensional space $\mathbb{Q}^3$ this property can be visualized.

Orientation rule. Vectors $\mathbf{e}_1$, $\mathbf{e}_2$, $\mathbf{e}_3$ form *right triple* in $\mathbb{Q}^3$ if when looking from the end point of third vector $\mathbf{e}_3$ the shortest rotation from first vector $\mathbf{e}_1$ to second vector $\mathbf{e}_2$ is seen as counterclockwise rotation.

In physics (electricity and magnetism) this rule is formulated as the rule of right screw and also left hand rule (see [2] and [3]). In multidimensional spaces $n > 3$ one cannot visualize the concept of left and right since human has not visual experience of living in such spaces. However, one can understand it mathematically by means of theory of determinants and skew-symmetric polylinear forms. Indeed, one should first prescribe right orientation to standard base in $\mathbb{Q}^n$ composed by vectors

$$\mathbf{E}_1 = \begin{Vmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{Vmatrix}, \quad \mathbf{E}_2 = \begin{Vmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{Vmatrix}, \quad \ldots, \quad \mathbf{E}_n = \begin{Vmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{Vmatrix}, \tag{3.3}$$

then one should consider transition matrix S for transition from standard base (3.3) to another base $\mathbf{e}_1, \ldots, \mathbf{e}_n$. Its components are defined by the equality

$$\mathbf{e}_i = \sum_{j=1}^{n} S_i^j \cdot \mathbf{E}_j, \qquad i = 1, \ldots, n. \tag{3.4}$$

Definition 3.1. Base $\mathbf{e}_1, \ldots, \mathbf{e}_n$ in $\mathbb{Q}^n$ is called *right oriented* if $\det S > 0$. Otherwise, if $\det S < 0$ this base is called *left oriented*.

Other method of defining orientation in $\mathbb{Q}^n$ uses skew-symmetric polylinear forms. Remember, that polylinear n-form in $\mathbb{Q}^n$ is a $\mathbb{Q}$-numeric function with n vectorial arguments $\omega = \omega(\mathbf{X}_1, \ldots, \mathbf{X}_n)$ which is linear with respect to each its argument. Form ω is called completely skew-symmetric if its value change the sign upon permutation of any pair of arguments in it. It is known that completely skew-symmetric n-form in $\mathbb{Q}^n$ is determined uniquely up to a scalar factor. Therefore there is exactly one n-form ω normalized by the condition $\omega(\mathbf{E}_1, \ldots, \mathbf{E}_n) = 1$. It is called the form of volume. For the base $\mathbf{e}_1, \ldots, \mathbf{e}_n$ we have the equality

$$\omega(\mathbf{e}_1, \ldots, \mathbf{e}_n) = \det S \cdot \omega(\mathbf{E}_1, \ldots, \mathbf{E}_n),$$

where S is determined by (3.4). This means that the value of volume form ω can be used as a measure of orientation for the bases in $\mathbb{Q}^n$.

Note that if base $\mathbf{e}_1, \ldots, \mathbf{e}_n$ is composed by columns of orthogonal matrix O, then transition matrix S in (3.4) coincides with O. This means that constructing orthogonal matrix $O \in \mathrm{SO}(n, \mathbb{Q})$ is equivalent to choosing some right oriented ONB in $\mathbb{Q}^n$. One vector in this base (say last vector $\mathbf{e}_n$) can be constructed by means of stereographic projection as described in section 2 above. This is the first step in our algorithm for constructing orthogonal matrices. Then we should complement it with other $n-1$ vectors which should be unit vectors by length, perpendicular to each other and perpendicular to $\mathbf{e}_n$ as well. Below we use Cayley transformation for this purpose.

4. Cayley transformation.

Let A be skew-symmetric $n \times n$ square matrix. It is known that all eigenvalues of skew-symmetric matrix are purely imaginary numbers (some o them can be equal to zero, but they cannot be nonzero real numbers). Therefore $\det(1 - A)$ is nonzero. Let's consider the matrix $O = (1 + A) \cdot (1 - A)^{-1}$. Matrices $1 + A$ and $1 - A$ commutate with each other, therefore $(1 + A) \cdot (1 - A)^{-1} = (1 - A)^{-1} \cdot (1 + A)$. For this reason we denote $O = (1 + A) \cdot (1 - A)^{-1}$ by means of fraction

$$O = \frac{1 + A}{1 - A}. \tag{4.1}$$

Formula (4.1) is known as Cayley transformation (see book [4]). If A is skew-symmetric, as it is in our case, then O is orthogonal matrix with $\det O = 1$. Cayley transformation defines a map $\mathrm{so}(n, \mathbb{Q}) \to \mathrm{SO}(n, \mathbb{Q})$ similar to exponential map $\exp\colon \mathrm{so}(n, \mathbb{R}) \to \mathrm{SO}(n, \mathbb{R})$. But, in contrast to exponential map, it is rational, that is worth for our purposes. Cayley transformation is injective map. Indeed, if matrix

O is obtained by formula (4.1), then one can recover matrix A by formula

$$A = \frac{O-1}{O+1}. \tag{4.2}$$

However, one cannot apply formula (4.2) to arbitrary matrix $O \in \mathrm{SO}(n,\mathbb{Q})$. Matrices with eigenvalue $\lambda = -1$ are not suitable. This means that Cayley transformation is not surjective. Below we modify Cayley transformation and convert into algorithm able to yield each matrix $O \in \mathrm{SO}(n,\mathbb{Q})$.

Let's choose special skew-symmetric matrix. Taking $n-1$ rational numbers $y^1, \ldots, y^{n-1}$, we denote by $A[y^1,\ldots,y^{n-1}]$ skew–symmetric matrix of the form

$$A[y^1,\ldots,y^{n-1}] = \begin{Vmatrix} 0 & \ldots & 0 & y^1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & y^{n-1} \\ -y^1 & \ldots & -y^{n-1} & 0 \end{Vmatrix} \tag{4.3}$$

Substituting (4.3) into (4.1), we obtain orthogonal matrix

$$O[y^1,\ldots,y^{n-1}] = \frac{1+A[y^1,\ldots,y^{n-1}]}{1-A[y^1,\ldots,y^{n-1}]}. \tag{4.4}$$

By direct calculation one can find that n-th column in matrix (4.4) coincides with unit vector $\mathbf{e}_n$ constructed by means of stereographic projection in section 2. It's components are given by formulas (2.2) and (2.3). Let's denote by $\mathbf{e}_1, \ldots, \mathbf{e}_{n-1}$ other $n-1$ columns of matrix $O[y^1,\ldots,y^{n-1}]$. Completed by vector $\mathbf{e}_n$, they form ONB in $\mathbb{Q}^n$. Here are formulas for components of vector $\mathbf{e}_k$, where $k \neq n$:

$$\begin{aligned} x^s &= \frac{-2\,y^k\,y^s}{\left(1+\sum\limits_{i=1}^{n-1}(y^i)^2\right)} \quad \text{for} \quad s\neq k,\ s\neq n, \\ x^k &= 1-\frac{2\,(y^k)^2}{\left(1+\sum\limits_{i=1}^{n-1}(y^i)^2\right)}, \quad x^n = \frac{-2\,y^k}{\left(1+\sum\limits_{i=1}^{n-1}(y^i)^2\right)}. \end{aligned} \tag{4.5}$$

We can pass to the limit $Y \to \infty$ in (2.2) and (2.3). However, we cannot pass to this limit in (4.5). For infinite point $Y = \infty$ we set by definition

$$O[\infty] = \begin{Vmatrix} 1 & \ldots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \ldots & 1 & 0 & 0 \\ 0 & \ldots & 0 & -1 & 0 \\ 0 & \ldots & 0 & 0 & -1 \end{Vmatrix} \tag{4.6}$$

Theorem 4.1. *Each unit vector* $\mathbf{e} \in \mathbb{Q}^n$ *given by its stereographic coordinates* $y^1, \ldots, y^{n-1}$ *is canonically associated with some orthogonal matrix* $O \in \mathrm{SO}(n, \mathbb{Q})$.

Formulas (2.2), (2.3), (4.5), and (4.6) give explicit proof of theorem 4.1. By construction vector $\mathbf{e}$ is n-th column in matrix $O = O[y^1, \ldots, y^{n-1}]$.

Now let O be some arbitrary matrix from special orthogonal group $\mathrm{SO}(n, \mathbb{Q})$. We denote by $\mathbf{e}$ its n-th column. This is unit vector with rational components $x^1, \ldots, x^n$. Suppose that $y^1, \ldots, y^{n-1}$ are its stereographic coordinates (see formula (2.1) in section 2). They are also rational numbers. Therefore we can construct orthogonal matrix $O[y^1, \ldots, y^{n-1}]$ as described above. As a result we get two orthogonal matrices O and $O[y^1, \ldots, y^{n-1}]$ with the same n-th column in them. This is possible if and only if these matrices are bound by the relationship

$$O = O[y^1, \ldots, y^{n-1}] \cdot \Omega, \tag{4.7}$$

where Ω is orthogonal matrix of the form (1.2). Thus we have proved a theorem.

Theorem 4.2. *Each orthogonal matrix* $O \in \mathrm{SO}(n, \mathbb{Q})$ *can be represented as a product* (4.7)*, where* Ω *is a blockwise diagonal matrix determined by some element of orthogonal group* $\mathrm{SO}(n-1, \mathbb{Q})$.

Theorem 4.2 is analog of theorem 1.1, while rational parameters $y^1, \ldots, y^{n-1}$ are analogs of Euler angles $\varphi_1, \ldots, \varphi_{n-1}$. Applying this theorem recursively, for $O \in \mathrm{SO}(n, \mathbb{Q})$ we get the equality

$$O = O[y_1^1, \ldots, y_1^{n-1}] \cdot O[y_2^1, \ldots, y_2^{n-2}] \cdot \ldots \cdot O[y_{n-1}^1]. \tag{4.8}$$

Theorem 4.3. *Each orthogonal matrix* $O \in \mathrm{SO}(n, \mathbb{Q})$ *can be constructed by means of algorithm described above in form of product* (4.8).

Theorem 4.3 is analog of theorem 1.2. Note that the number of rational parameters y_j^i in (4.8) is equal to $n(n-1)/2$. This is exactly the same number as in the statement of theorem 1.2.

5. Concluding remarks.

I am not specialist in algebra and I am not specialist in number theory. I have encountered problem of generating orthogonal matrices with rational elements in designing computer programs for testing students (see [5]). Therefore it's quite possible that all above results are not new. However, I hope that gathered in one paper and formulated as computational algorithm they could be useful for practical purposes. In addition, I have collected some references (see [6–12]) related to the subject of present paper.

10. Acknowledgements.

I am grateful to V. A. Yuryev for helpful discussions. I am also grateful to Russian Fund for Basic Research and Academy of Sciences of the Republic Bashkortostan for financial support in 2001.

References

1. Kostrikin A. I., *Introduction to algebra*, Nauka publishers, Moscow, 1977.
2. Borovoy A. A., Finkelstein E. B., Heruvimov A. N., *Laws of electromagnetism*, Nauka publishers, Moscow, 1970.
3. Landsberg G. S. (ed.), *Elementary physics manual, Vol. 2*, Nauka publishers, Moscow, 1975.
4. Postnikov M. M., *Lie Groups and Lie algebras. Lectures on geometry, 5-th term*, Nauka publishers, Moscow, 1982.
5. Sharipov R. A., *Orthogonal matrices with rational components in composing tests for High School students*, Paper math.GM/0006230 in Electronic Archive at LANL[1] (2000).
6. Grave D. A., *Treatise on algebraic analysis*, vol. 1 and 2, Kiev, 1938–1939.
7. Smirnov G. P., *On the representation of zero by quadratic forms*, Transactions of Bashkir State University, vol. 20, issue 2, Ufa, 1965.
8. Smirnov G. P., *On the solution of some Diophantine equations containing quadratic forms*, Transactions of Bashkir State University, vol. 20, issue 1, Ufa, 1965.
9. Smirnov G. P., *Entire orthogonal matrices and methods of their construction*, Transactions of Bashkir State University, vol. 31, issue 3, Ufa, 1968.
10. Bruening J. T., Lohmeier T. R., Sebaugh Ch. L., *Symmetric Pythagorean triple preserving matrices*, Missouri Journal of Mathematical Sciences **13** (2001), no. 1.
11. Wojtowicz M., *Algebraic structures of some sets of Pythagorean triples*, Missouri Journal of Mathematical Sciences **13** (2001), no. 1.
12. Crasmareanu M., *A new method to obtain Pythagorean triple preserving matrices* (to appear).

Rabochaya str. 5, Ufa 450003, Russia
E-mail address: R_Sharipov@ic.bashedu.ru
r-sharipov@mail.ru
URL: http://www.geocities.com/r-sharipov

[1]Electronic Archive at Los Alamos National Laboratory of USA (LANL). Archive is accessible through Internet **http://arXiv.org**, it has mirror site **http://ru.arXiv.org** at the Institute for Theoretical and Experimental Physics (ITEP, Moscow).

This figure "f13-2.gif" is available in "gif" format from:

http://arXiv.org/ps/cs/0201007v1