Acknowledgement. We thank one of the referees for some suggestions regarding the presentation of the material and for bringing [1] to our notice.

REFERENCES

1. R. D. Byrd, Simultaneous complements in finite-dimensional vector spaces, *Amer. Math. Monthly*, 93 (1986) 641–642.
2. I. N. Herstein, Topics in Algebra, second edition, 1975.
3. B. Levinger, Review of [4] in *Math. Reviews*, 87b: 15003.
4. N. J. Lord, Simultaneous complements in finite-dimensional vector spaces, *Amer. Math. Monthly*, 92 (1985) 492–493.

The Generation of All Rational Orthogonal Matrices

HANS LIEBECK AND ANTHONY OSBORNE
Department of Mathematics, University of Keele, Staffordshire, ST5 5BG, England

In a letter to this MONTHLY [1] John Cremona shows how to generate all 3×3 orthogonal matrices with rational coefficients. His method is based on the real algebra of quaternions. By a further application of quaternions one can obtain 4×4 rational orthogonal matrices. (See du Val [2].)

In this note we show how to generate all $n \times n$ rational orthogonal matrices and hence all orthonormal bases of the rational vector space $\mathbf{Q}^n$. At the same time we obtain all real orthogonal matrices and all complex unitary matrices. Our method is based on a further piece of mathematics from the last century—Cayley's formula for orthogonal matrices.

Preliminaries. Let A and B be $n \times n$ matrices. We shall say that B *is equivalent to* A, and write $B \sim A$, if and only if there exists a diagonal matrix D with diagonal entries selected from the set $\{-1, 1\}$ such that $B = DA$. Clearly B is equivalent to A if and only if, for each $i = 1, \ldots, n$, the ith row of B is $\pm i$th row of A. The relation $\sim$ is an equivalence relation on the set of $n \times n$ matrices, and the equivalence class $\mathscr{E}(A)$ which contains A has at most 2^n members.

LEMMA. *Let A be an $n \times n$ matrix over a field of characteristic $\neq 2$. Then at least one of the matrices in $\mathscr{E}(A)$ does not have eigenvalue* 1.

Proof. By induction on n. For $n = 1$ the result is true, since the 1×1 matrices A and $-A$ cannot both be [1] over a field of characteristic $\neq 2$. Proceeding by way of contradiction let n be the least order for which the lemma is false. Then there exists an $n \times n$ matrix A such that all matrices in $\mathscr{E}(A)$ have eigenvalue 1. Thus for any matrix $DA \in \mathscr{E}(A)$, there exists $\mathbf{x} \neq \mathbf{0}$ such that $DA\mathbf{x} = \mathbf{x}$. Hence $A\mathbf{x} = D\mathbf{x}$, and so the matrix $A - D$ is singular. Consider the determinant function

$$d(t_1, \ldots, t_n) = \det(A - \operatorname{diag}(t_1, \ldots, t_n)).$$

We have that $d(t_1, \ldots, t_n) = 0$ for all 2^n choices of $t_i = \pm 1$, $i = 1, \ldots, n$.

Expanding $d(t_1, \ldots, t_n)$ according to the first row, we obtain

$$d(t_1, \ldots, t_n) = (a_{11} - t_1)d^*(t_2, \ldots, t_n) + \text{terms independent of } t_1. \quad (1)$$

By the induction hypothesis the determinant $d^*(t_2, \ldots, t_n)$ of order $n-1$ is non-zero for at least one choice of $t_j = \pm 1$, $j = 2, \ldots, n$. Make such a choice: $t_2, \ldots, t_n = \lambda_2, \ldots, \lambda_n$.

We have $d(1, \lambda_2, \ldots, \lambda_n) = 0$ and $d(-1, \lambda_2, \ldots, \lambda_n) = 0$. From (1)

$$(a_{11} - 1)d^*(\lambda_2, \ldots, \lambda_n) = (a_{11} + 1)d^*(\lambda_2, \ldots, \lambda_n).$$

Hence $a_{11} - 1 = a_{11} + 1$ which is clearly false in a field of characteristic $\neq 2$. So the lemma is proved.

Construction of $n \times n$ orthogonal matrices. Let F be a subfield of the field of real numbers. By Cayley's formula [**3** p. 289] the mapping $S \mapsto (S - I)^{-1}(S + I)$ gives a one-one correspondence between the set of $n \times n$ skew-symmetric matrices S over F and the set of $n \times n$ orthogonal matrices over F which do not have 1 as an eigenvalue. The inverse correspondence is given by $A \mapsto (A - I)^{-1}(A + I)$.

Now let A be any $n \times n$ orthogonal matrix over F. Then the equivalence class $\mathscr{C}(A)$ consists of orthogonal matrices, and by the Lemma at least one of these, B say, does not have eigenvalue 1. By the Cayley correspondence there exists a skew-symmetric matrix S over F such that $B = (S - I)^{-1}(S + I)$. Thus we have the following result.

THEOREM. *The set of all $n \times n$ orthogonal matrices over F is generated by the $n \times n$ orthogonal matrices $(S - I)^{-1}(S + I)$, where S is skew-symmetric over F, and their equivalence classes.*

The same technique can be used to generate all unitary matrices by considering the complex field and replacing "orthogonal" by "unitary" and "skew-symmetric" by "skew-hermitian" in the above analysis.

It is worth pointing out that the $n \times n$ orthogonal matrices $(S - I)^{-1}(S + I)$ referred to in the theorem all have determinant $(-1)^n$. (Proof: $\det(S + I) = \det(S + I)^T = \det(-S + I) = (-1)^n \det(S - I)$, from which the result follows.) So they represent reflections when n is odd and rotations when n is even. Consequently every $n \times n$ reflection matrix when n is even and every $n \times n$ rotation matrix when n is odd is equivalent but not equal to a matrix of the form $(S - I)^{-1}(S + I)$. This can also be seen from [**4**] Theorem B, which states that every reflection of a (Euclidean) space of even dimension and every rotation of a space of odd dimension has a fixed vector. The corresponding orthogonal matrices then have eigenvalue 1 and, therefore, do not feature in the Cayley correspondence.

In particular, John Cremona's 3×3 rotation matrix $M(a, b, c, d)$ is given for the case $d \neq 0$ by

$$M(a, b, c, d) = D(S - I)^{-1}(S + I),$$

where S is the 3×3 skew-symmetric matrix which has a/d, $-b/d$, $-c/d$ above the diagonal, and $D = \operatorname{diag}(1, 1, -1)$.

This note provides a theoretical method of generating all orthogonal matrices over a real field F, but as a practical classroom aid it is of limited use. The reader interested in a simple technique of generating a large class of 3×3 rational orthogonal matrices is referred to our Teaching Note [**5**].

We are grateful to a referee for some of the observations following our theorem.

REFERENCES

1. John Cremona, Letter to the Editor, *Amer. Math. Monthly*, 94 (1987) 757.
2. Patrick du Val, Homographies, Quaternions and Rotations, Oxford University Press, 1964.
3. F. R. Gantmacher, The Theory of Matrices, Vol. I, Chelsea, 1960.
4. A. M. Adelberg, Reflections have reversed vectors, *Amer. Math. Monthly*, 79 (1972) 59–62.
5. Anthony Osborne and Hans Liebeck, Orthogonal bases of $\mathbb{R}^3$ with integer coordinates and integer lengths, *Amer. Math. Monthly*, 96 (1989) 49–53.

Hypocycloids, Continued Fractions, and Distribution Modulo One

NORMAN RICHERT*
Division of Mathematics and Systems Design, University of Houston, Clear Lake, Houston, TX 77058

In simulation and Monte Carlo approximation schemes, a random sequence (pseudorandom, really) is needed. How this sequence might be generated is a long story. Donald Knuth [2] encapsulates some of the difficulties neatly in *The Art of Computer Programming, Volume 2*, where he says that "*random numbers should not be generated with a method chosen at random*. Some theory should be used." A sequence with some very nice properties is the so-called $(n\theta)$ sequence. Let θ be irrational. Let a sequence $\{x_n\}$ in $[0, 1)$ be defined by $x_n = (n\theta)$, $n = 1, 2, \ldots$, where $(\cdot)$ denotes the fractional part. Let us explore this sequence.

One way to visualize what the sequence is doing is to imagine a circle of circumference θ rolling to the right on the real line. The circle has a distinguished point P, which begins at zero. Then the sequence consists of the set of positive points where P touches the line, as long as each interval from integer k to $k + 1$ is understood as a copy of $[0, 1)$. So the points could be viewed as the set of cusp points of the cycloid. Better still, roll the real line up into a circle of circumference 1 by identifying the integer points. Now the cycloid is a hypocycloid, at least if the circumference of the rolling circle is less than 1. There is no loss of generality in supposing this, so assume in what follows that $0 < \theta < 1$.

Calculus students are frequently asked to find parametric equations for a hypocycloid, using the angle between the x-axis and the line of centers of the two circles as the parameter. Frequently, $\theta = .25$ is illustrated as a special case, the hypocycloid of four cusps, because the parametric equations have a particularly simple form in that case. It is easy to infer a family of hypocycloids of q-cusps, where $\theta = 1/q$, $q \geqslant 2$. The associated sequences could hardly be described as random. From a theoretical point of view, things get more interesting if θ is irrational. Then the curve is not closed and $\{(n\theta)\}$ is not a periodic sequence. However, on a computer all numbers are rational, and plotters have only a finite resolution. So for the purposes of this discussion the rational/irrational distinction

*Appreciation is expressed to Marquette University Computer Services for the use of the large-format drum-pen plotter used in the figures.