ON THE DECOMPOSITION OF ORTHOGONALITIES INTO SYMMETRIES

PETER SCHERK

1. Let $\mathfrak{F}$ be a field of characteristic $\neq 2$, and let $\mathfrak{R}_n$ denote the space of all column vectors over $\mathfrak{F}$ with n components. In the following, Greek letters denote elements of $\mathfrak{F}$, while small italics $[\neq m, n, r, s]$ stand for vectors in $\mathfrak{R}_n$, and n-rowed squared matrices over $\mathfrak{F}$ are denoted by capital letters. A prime indicates transposition.

Let G be a fixed regular symmetric matrix. Thus

$$G = G', \qquad |G| \neq 0.$$

Two vectors a and b are called perpendicular if $a'Gb=0$. Two subspaces $\mathfrak{R}^*$ and $\mathfrak{R}^{**}$ are perpendicular if $x'Gy=0$ for all $x\subset\mathfrak{R}^*$, $y\subset\mathfrak{R}^{**}$. Obviously, these relations are symmetric. The vectors perpendicular to a given vector respectively to a given m-space form an $(n-1)$-space, respectively $(n-m)$-space.

We call the matrix T orthogonal if it leaves the expression $x'Gy$ unchanged for all x and y. This condition is equivalent to

$$T'GT = G. \tag{1}$$

If in addition

$$\text{rank } (T - I) = 1,$$

T is called a symmetry (cf. Lemma 2; I = unit matrix).

Cartan proved that every orthogonality can be decomposed into a product of n or less than n symmetries. A proof of his theorem can be found in Dieudonné's book.[1]

The purpose of this note is to show that the minimum number of symmetries into which an orthogonality T can be decomposed is in general equal to

$$m = \text{rank } (T - I).$$

An exception occurs if and only if $G(T-I)$ is skew-symmetric. In that case, this minimum number is equal to $m+2$. For a detailed description of this case cf. the last part of this note.

2. LEMMA 1. *The following three sets of properties of a matrix A are equivalent*:

Presented to the Society, September 2, 1949; received by the editors June 14, 1949.

[1] Dieudonné, *Sur les groupes classiques*, Actualités Scientifiques et Industrielles no. 1040, Paris, 1948, pp. 20–22.

(a) *rank* $(A-I)=1$, $A^2=I$;
(b) 1 *is an* $(n-1)$*-fold*, -1 *a simple eigenvalue of* A;
(c) *There are two vectors a and b such that*

$$A = I + ab' \tag{2}$$

and

$$b'a = -2. \tag{3}$$

PROOF. Obviously

$$\begin{array}{l} \text{rank } (A - I) = 1 \\ \updownarrow \\ 1 \text{ is an } (n-1)\text{-fold eigenvalue of } A \\ \updownarrow \\ (2) \text{ holds for suitable } a \neq 0,\ b \neq 0. \end{array} \tag{4}$$

(a)→(b): The first part of (b) implies that A has exactly one other eigenvalue α, and this eigenvalue is simple. From $Ax=\alpha x$ it follows by means of (a) that

$$x = Ix = A^2x = A\cdot\alpha x = \alpha\cdot Ax = \alpha^2 x.$$

Since $x\neq 0$ and $\alpha\neq 1$, $\alpha=-1$.
(b)→(c): From our assumptions, there exists an $x\neq 0$ so that

$$0 = (A + I)x = (2I + ab')x = 2x + b'x\cdot a.$$

Thus a and x are linearly dependent. We may choose $x=a$ and obtain $(2+b'a)a=0$ and therefore (3).
(c)→(a): From (3)

$$A^2 = (I + ab')(I + ab') = I + 2ab' + a(b'a)b' = I + 2ab' - 2ab' = I.$$

We call the vector a isotropic if $a'Ga=0$.

LEMMA 2. *The following three sets of properties of a matrix A are equivalent*:
(a) *A is orthogonal, rank* $(A-I)=1$;
(b) *There exists a non-isotropic vector a such that*

$$A = I - \frac{2aa'G}{a'Ga}; \tag{5}$$

(c) *A maps some non-isotropic vector a on* $-a$ *and every vector perpendicular to a on itself.*

PROOF. We first observe that (5) is equivalent to the combined three statements (2), (3), and

(6) Ga and b are linearly dependent.

(a)→(b): By means of (4) we obtain (2). Thus, A being orthogonal, we have

$$0 = A'GA - G = (I + ba')G(I + ab') - G$$

or

$$0 = b \cdot a'G(I + ab') + Ga \cdot b'. \tag{7}$$

This formula implies (6). Substituting $Ga = \lambda b$ into (7), we obtain

$$0 = \lambda bb'(I + ab') + \lambda bb' = 2\lambda bb' + \lambda b(b'a)b'$$

hence

$$\lambda(2 + b'a) \cdot bb' = 0.$$

G being regular, $\lambda \neq 0$. Thus (3) is also satisfied.

(c)→(b): The assumptions (b) of Lemma 1 hold. This implies (2) and (3). From (2), $Ax = x$ is equivalent to $b'x = 0$, and from our assumptions, it is also equivalent to $a'Gx = 0$. Thus (6) also holds.

Obviously, (a) and (c) follow from (b).

We had defined symmetries as matrices possessing the properties (a). Thus Lemma 2 gives us two alternate definitions. From Lemma 1, we obtain the following

COROLLARY. *If A is a symmetry, then*

$$A^2 = I. \tag{8}$$

LEMMA 3.

$$\text{rank } (AB - I) \leqq \text{rank } (A - I) + \text{rank } (B - I). \tag{9}$$

PROOF. Put

$$r = \text{rank } (A - I), \qquad s = \text{rank } (B - I).$$

The vectors x with $Ax = x$, respectively $Bx = x$, form an $(n - r)$-space, respectively $(n - s)$-space. If x lies in the intersection of these two subspaces, then $ABx = Ax = x$. Thus this intersection lies in the eigenspace of AB belonging to the eigenvalue 1. The dimension of this eigenspace is therefore greater than or equal to that of this intersection. Hence it is greater than or equal to $n - r - s$. This implies (9).

If we apply (9) repeatedly to a product T of m symmetries, we get

$$\text{rank } (T - I) \leqq m.$$

Thus we obtain the following

COROLLARY. *An orthogonality T cannot be the product of less than rank* $(T-I)$ *symmetries.*

3. LEMMA 4. *Let*

$$\text{rank } S > 1, \tag{10}$$

$$S + S' \neq 0. \tag{11}$$

Then, there exists a vector b such that

$$b'Sb \neq 0 \tag{12}$$

and

$$S + S' \neq \frac{1}{b'Sb}(Sb\cdot b'S + S'b\cdot b'S'). \tag{13}$$

PROOF. We have

$$x'(S + S')x = x'Sx + x'S'x = x'Sx + (x'Sx)' = 2x'Sx. \tag{14}$$

Thus, on account of (11), there are vectors b satisfying (12). We may assume that at least one vector b_1 exists that is a solution of both (12) and

$$S + S' = \frac{1}{b'Sb}(Sb\cdot b'S + S'b\cdot b'S'). \tag{15}$$

Put

$$c = Sb_1, \qquad d = S'b_1, \qquad \alpha = b_1'Sb_1. \tag{16}$$

Then from (12)

$$c \neq 0, \qquad d \neq 0, \qquad \alpha = b_1'c = b_1'd \neq 0, \tag{17}$$

and from (15)

$$S + S' = \frac{1}{\alpha}(cd' + dc'). \tag{18}$$

Thus, (14) and (18) imply

$$x'Sx = \frac{1}{2}x'(S + S')x = \frac{1}{\alpha}c'x\cdot d'x.$$

In particular, the quadric

$$\mathfrak{Q} \equiv x'Sx = 0$$

is identical with the pair of [not necessarily different] $(n-1)$-spaces

$c'x=0$ and $d'x=0$.

Now let b be any solution of both (12) and (15). Then Sb and $S'b$ are different from zero, and comparing (15) with (18), we see that either Sb is a multiple of c and $S'b$ is one of d, or Sb is a multiple of d, while $S'b$ is one of c.

We first consider the case that a solution b_2 of (12) and (15) exists such that Sb_2 is not a multiple of c. Then Sb_2 is a multiple of d, and the vectors c and d are linearly independent. Replacing b_2 by a suitable multiple, we may assume

$$Sb_2 = d, \qquad S'b_2 = \beta c, \qquad \beta \neq 0. \tag{19}$$

Substituting $b=b_2$ into (15), we obtain

$$S + S' = \frac{\beta}{b_2' Sb_2}(dc' + cd'),$$

and therefore, on account of (18),

$$b_2' Sb_2 = \alpha\beta.$$

Thus (19) implies

$$b_2' d = \alpha\beta, \qquad b_2' c = \alpha. \tag{20}$$

The vectors

$$S(b_1 \pm b_2) = c \pm d$$

are multiples neither of c nor of d [cf. (16) and (19)]. Hence the two vectors $b_1 \pm b_2$ cannot solve the system (12), (15). Now, from (16), (17), (19), (20)

$$\begin{aligned}(b_1 + b_2)'S(b_1 + b_2) &- (b_1 - b_2)'S(b_1 - b_2) \\ &= 2(b_1' Sb_2 + b_2' Sb_1) = 2(b_1' d + b_2' c) = 2(\alpha + \alpha) = 4\alpha \neq 0.\end{aligned}$$

Hence, at least one of the two vectors $b_1 \pm b_2$ satisfies (12). As it cannot satisfy (15), it is a solution of both (12) and (13).

Suppose now that every solution b of (12) and (15) is mapped by S on a multiple of c. The set of all vectors x for which Sx is a multiple of c form a subspace $\mathfrak{R}_c$ of $\mathfrak{R}_n$. From (10), $\mathfrak{R}_c$ is a proper subspace of $\mathfrak{R}_n$. Hence its dimension is not greater than $n-1$. It suffices to show that there are vectors in $\mathfrak{R}_n$ that belong neither to $\mathfrak{R}_c$ nor to the quadric $\mathfrak{Q}$.

We had $b_1 \subset \mathfrak{R}_c - \mathfrak{Q}$. Since $\mathfrak{Q}$ was a pair of $(n-1)$-spaces, there exists a vector $b_2 \subset \mathfrak{Q} - \mathfrak{R}_c$. Thus, the straight line

$$b = (1 - \lambda)b_1 + \lambda b_2 \tag{21}$$

lies neither in $\mathfrak{R}_c$ nor in $\mathfrak{Q}$. Hence it has exactly one point in common with $\mathfrak{R}_c$ and at most two points with the pair $\mathfrak{Q}$ of $(n-1)$-spaces. Altogether, the straight line (21) meets the union $\mathfrak{R}_c+\mathfrak{Q}$ in not more than three points. If $\mathfrak{F}$ is not the prime field $\mathfrak{F}_3$ of three elements, this line contains more than three points. In particular, it contains points outside of $\mathfrak{R}_c+\mathfrak{Q}$.

If $\mathfrak{F}=\mathfrak{F}_3$, then an $(n-1)$-space contains 3^{n-1} points. Since $\mathfrak{R}_c$ has a dimension not greater than $n-1$ and since $\mathfrak{R}_c$ and $\mathfrak{Q}$ have the origin in common, the set $\mathfrak{R}_c+\mathfrak{Q}$ contains less than 3.3^{n-1} points, thus fewer points than the whole $\mathfrak{R}_n$. Hence, there are points outside of $\mathfrak{R}_c+\mathfrak{Q}$.[2]

LEMMA 5. *Suppose T is orthogonal, $G(T-I)$ is not skew-symmetric, and*

$$m = \text{rank } (T - I) > 1.$$

Then there exists an orthogonality U such that

(a) *T is the product of U by a symmetry,*

(b) *rank $(U-I)=m-1$,*

(c) *$G(U-I)$ is not skew-symmetric.*

PROOF. Put

$$T_0 = T - I, \qquad S = GT_0.$$

We rewrite the orthogonality definition (1) in terms of T_0 and S:

$$T'GT - G = (T_0 + I)'G(T_0 + I) - G = 0$$

or

$$T_0'GT_0 + S + S' = 0. \tag{22}$$

G being regular, we have

$$\text{rank } S = \text{rank } T_0 = m > 1.$$

Thus S satisfies the assumptions of Lemma 4, and there is a vector b such that

$$b'Sb \neq 0 \tag{23}$$

and

[2] The proof of Lemma 4 can be simplified considerably if the case $\mathfrak{F}=\mathfrak{F}_3$ is excluded. If $\mathfrak{F}$ is the real field, this lemma is trivial. The matrix $Sb\cdot b'S+S'b\cdot b'S, -b'Sb(S+S')$ depends continuously on b. If it vanishes outside of the quadric $\mathfrak{Q}$ identically, then it will also vanish on $\mathfrak{Q}$. Hence $Sb\cdot b'S+S'b\cdot b'S'=0$ for all $b\subset\mathfrak{Q}$. Therefore, $\mathfrak{Q}$ would be contained in the pair of at most $(n-2)$-dimensional subspaces $Sb=0$ and $S'b=0$, which is impossible.

(24) $$S + S' \neq \frac{1}{b'Sb}(Sb \cdot b'S + S'b \cdot b'S').$$

Let $\mathfrak{N}_{n-m}$ be the eigenspace belonging to the eigenvalue 1 of T. From the regularity of G and of $T = T_0 + I$

(25) $$x \subset \mathfrak{N}_{n-m} \leftrightarrow T_0x = 0 \leftrightarrow Sx = 0 \leftrightarrow S'x = 0 \quad [\text{cf. } (22)].$$

In particular, from (23),

(26) $$b \not\subset \mathfrak{N}_{n-m}.$$

Define

(27) $$a = T_0b.$$

Then, from (25),

(28) $$a'Gx = b'S'x = 0 \qquad \text{for all } x \subset \mathfrak{N}_{n-m}.$$

Furthermore, (27), (22), and (14) yield

$$a'Ga = b'T_0'GT_0b = -b'(S + S')b = -2b'Sb.$$

Thus, from (27) and (23)

(29) $$a'Ga = -2b'Sb = -2b'Ga \neq 0.$$

We now put

(30) $$A = I - \frac{2aa'G}{a'Ga}, \qquad U = AT.$$

Thus, A is a symmetry [cf. Lemma 2]; and with A and T, U is an orthogonality. From (8)

$$T = A^2T = AU.$$

We now verify that U also has the required properties (b) and (c). If $x \subset \mathfrak{N}_{n-m}$, then on account of (28)

$$Ux = ATx = Ax = x - \frac{2a'Gx}{a'Ga} \cdot a = x.$$

Furthermore, we obtain from (30), (27), and (29)

$$(T - A)b = \left(T_0 + \frac{2aa'G}{a'Ga}\right)b = a + \frac{2a'Gb}{a'Ga}a = a - a = 0,$$

hence

$$Ub = ATb = A^2b = b.$$

Thus the eigenspace of U belonging to the eigenvalue 1 contains both $\mathfrak{R}_{n-m}$ and b. As $b \not\subset \mathfrak{R}_{n-m}$ [cf. (26)], its dimension is not less than $n-m+1$, that is,

$$\text{rank } (U - I) \leqq m - 1.$$

Thus our assertion (b) follows by applying Lemma 3 to $T = AU$.

It remains to be shown that $G(U-I)$ is not skew-symmetric. We have

$$U - T = AT - I = \left(I - \frac{2aa'G}{a'Ga}\right)(T_0 + I) - I$$
$$= T_0 - 2\frac{T_0bb'T_0'G(T_0 + I)}{-2b'Sb} = T_0 - \frac{T_0bb'S}{b'Sb}$$

[cf. (27), (29), and (22)]. Thus

$$G(U - I) = S - \frac{Sbb'S}{b'Sb},$$

and (c) follows from (24).

Theorem 1. *Suppose T is orthogonal and $G(T-I)$ is not skew-symmetric. Then T can be written as a product of m = rank $(T-I)$ symmetries, but not of less than m.*

Proof. For $m=0$ and $m=1$ our statement is trivial [cf. Lemma 2]. Suppose it is proved up to $m-1 \geqq 1$. From the corollary of Lemma 3, T cannot be a product of fewer than m symmetries. Thus, our theorem follows from Lemma 5 and our induction assumption.

4. From now on we assume not only that T is orthogonal but also that $G(T-I)$ is skew-symmetric. Put $T_0 = T - I$, m = rank T_0. Being the rank of the skew-symmetric matrix GT_0, m is even. As the case $m=0$ is trivial, we may assume $m \geqq 2$.

From our assumptions

$$GT_0 + T_0'G = 0. \tag{31}$$

Hence

$$T'GT - G = (T_0' + I)G(T_0 + I) - G = T_0'GT_0 + GT_0 + T_0'G = 0$$

implies

$$T_0'GT_0 = 0. \tag{32}$$

We obtain from (31) and (32) $GT_0^2 + T_0'GT_0 = GT_0^2 = 0$. Since G is regular, it follows that

$$T_0^2 = 0. \tag{33}$$

Our definition of m implies that T_0 maps the whole space $\mathfrak{R}_n$ on an m-space $\mathfrak{R}_m$, and the set of the vectors x with $T_0x=0$ forms an $(n-m)$-space $\mathfrak{R}_{n-m}$. From (33)

$$\mathfrak{R}_m \subset \mathfrak{R}_{n-m} \tag{34}$$

therefore

$$m \leqq n - m \quad \text{or} \quad m \leqq n/2.$$

If $x \subset \mathfrak{R}_m$, $y \subset \mathfrak{R}_{n-m}$, then $x=T_0z$ for some z, and $T_0y=0$. From (31)

$$x'Gy = z'T_0'Gy = - z'GT_0y = 0.$$

So, the two spaces $\mathfrak{R}_m$ and $\mathfrak{R}_{n-m}$ are perpendicular. Since the vectors perpendicular to $\mathfrak{R}_{n-m}$ form an m-space containing $\mathfrak{R}_m$, this m-space is equal to $\mathfrak{R}_m$. Hence, a vector is perpendicular to $\mathfrak{R}_{n-m}$ if and only if it lies in $\mathfrak{R}_m$. We obtain from (34) that $\mathfrak{R}_m$ is perpendicular to itself. In particular, every vector in $\mathfrak{R}_m$ is isotropic.

Let

$$A = I - \frac{2aa'G}{a'Ga} \tag{35}$$

be an arbitrary symmetry. Thus a may be any non-isotropic vector. Since it cannot lie in $\mathfrak{R}_m$, it is not perpendicular to $\mathfrak{R}_{n-m}$, and the $(n-1)$-space $\mathfrak{R}_{n-1}$ perpendicular to a does not contain $\mathfrak{R}_{n-m}$. The intersection

$$\mathfrak{R}_{n-m-1} = \mathfrak{R}_{n-1} \cdot \mathfrak{R}_{n-m} \tag{36}$$

of these two spaces is therefore an $(n-m-1)$-space.

Let $U=AT$. We first show that $\mathfrak{R}_{n-m-1}$ is the eigenspace of U belonging to the eigenvalue 1. This implies in particular that

$$\text{rank } (U - I) = m + 1. \tag{37}$$

If $x \subset \mathfrak{R}_{n-m-1}$, then from (36) and (35) $Ux=ATx=Ax=x$.

Conversely, suppose $Ux=x$. Then $Tx=A^2Tx=AUx=Ax$ and hence

$$T_0x = (T - I)x = (A - I)x = - \frac{2a'Gx}{a'Ga} \cdot a, \tag{38}$$

From (38) and (32)

$$x'T_0'GT_0x = \left(\frac{2a'Gx}{a'Ga}\right)^2 a'Ga = 0.$$

Since $a'Ga \neq 0$, this implies $a'Gx = 0$ or $x \subset \mathfrak{R}_{n-1}$. Going back to (38), we obtain $T_0x = 0$ or $x \subset \mathfrak{R}_{n-m}$. Thus $x \subset \mathfrak{R}_{n-m-1}$. This proves the above statement.

Since m is even,

$$\text{rank}\, G(U - I) = \text{rank}\,(U - I) = m + 1$$

is odd. Hence, $G(U-I)$ cannot be skew-symmetric.

From Theorem 1, U is a product of $m+1$ symmetries. Hence $T = AU$ can be written as a product of $m+2$ symmetries. Suppose we have expressed T as a product of k symmetries. Then we may put $T = AU$ where A is a symmetry (35) and U is the product of $k-1$ symmetries. Since $U = AT$, we arrive again at (37). From the corollary to Lemma 3,

$$k - 1 \geqq m + 1, \quad \text{that is,} \quad k \geqq m + 2.$$

So we have the following theorem.

THEOREM 2. *Suppose T is orthogonal and $G(T-I)$ is skew-symmetric. Let*

$$m = \textit{rank}\,(T - I).$$

Then

$$m \equiv 0 \pmod 2 \quad \textit{and} \quad m \leqq n/2, \tag{39}$$

and T can be decomposed into a product of $m+2$ but not fewer than $m+2$ symmetries.

In order to find these transformations $T \neq I$, we choose a basis whose $m > 0$ first vectors span $\mathfrak{R}_m$. If $m < n/2$, the next $n - 2m$ vectors of this basis shall lie in $\mathfrak{R}_{n-m}$. Since

$$x'Gy = y'Gx = 0 \qquad \text{for all } x \subset \mathfrak{R}_m,\ y \subset \mathfrak{R}_{n-m},$$

G has in these coordinates the form

$$G = \begin{pmatrix} 0 & 0 & G_1' \\ 0 & G_2 & * \\ G_1 & * & * \end{pmatrix} \text{ if } m < \frac{n}{2}, \quad G = \begin{pmatrix} 0 & G_1' \\ G_1 & * \end{pmatrix} \text{ if } m = \frac{n}{2}. \tag{40}$$

Here G_1 and G_2 are regular square matrices; G_1 is m-rowed, G_2 is

$(n-2m)$-rowed and symmetric. We have

$$T_0 x \subset \mathfrak{R}_m \quad \text{for all} \quad x \subset \mathfrak{R}_n \quad \text{and} \quad T_0 y = 0 \quad \text{for all} \quad y \subset \mathfrak{R}_{n-m}.$$

Hence

$$T_0 = \begin{pmatrix} 0 & T_1 \\ 0 & 0 \end{pmatrix}$$

where T_1 is an m-rowed squared matrix. Its regularity follows from rank $T_0 = m$. We obtain

$$GT_0 = \begin{pmatrix} 0 & 0 \\ 0 & G_1T_1 \end{pmatrix}.$$

Thus (32) and (33) are satisfied. Finally, GT_0 is skew-symmetric if and only if the same holds true of G_1T_1. This leads to the following construction:

Choose $n \geqq 4$ arbitrarily, $m > 0$ according to (39) and then G according to (40). Then

$$T_0 = \begin{pmatrix} 0 & G_1^{-1}T_2 \\ 0 & 0 \end{pmatrix}$$

where T_2 may be any m-rowed regular skew-symmetric matrix.

If we take, for example, $n=4$, $m=2$,

$$G_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad T_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

we may put

$$G = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad T_0 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$ [3]

UNIVERSITY OF SASKATCHEWAN

[3] Professor Coxeter has made the following comment on the last example: "A space with two space-like and two time-like dimensions admits a transformation leaving a whole plane invariant although it is not merely a rotation. The explanation is, of course, that this invariant plane is isotropic."