A note on Additive Decomposition of Real Matrices

Chi-Kwong Li *and Edward Poon
Department of Mathematics, The College of William and Mary,
Williamsburg, Virginia 23187, USA.
E-mail: ckli@math.wm.edu, poon@math.wm.edu.

Abstract

The orthogonal orbit $\mathcal{O}(A)$ of an $n \times n$ real matrix A is the set of real matrices of the form P^tAP where $P^tP = I_n$. We show that $A/\|A\|$ is an affine sum of four orthogonal matrices, and note that A^t can always be written as an affine combination of no more than $2n-1$ matrices in $\mathcal{O}(A)$. This improves some recent results of Zhan, and answers some of his questions. Other related results are also discussed.

Keywords: Orthogonal matrices, orthogonal orbit.
AMS(MOS) subject classification: 15A18, 15A42

1 Introduction

Let $M_n(\mathbf{R})$ be the algebra of real $n \times n$ matrices. The orthogonal orbit $\mathcal{O}(A)$ of $A \in M_n(\mathbf{R})$ is the set of matrices of the form Q^tAQ where $Q \in M_n(\mathbf{R})$ is an orthogonal matrix, i.e., $Q^tQ = I_n$. In studying matrices and matrix inequalities, it is useful to decompose a matrix as a sum of special types of matrices. It is well known that if A is an $n \times n$ complex matrix with $\|A\| \leq 1$, then A is the average of two unitary matrices (see [2]); consequently, every $n \times n$ complex matrix is a linear combination of two unitary matrices. Zhan [3] showed that if $A \in M_n(\mathbf{R})$ then A is a linear combination of n orthogonal matrices, and asked whether there is a fixed positive integer k such that every A can be written as the real combination of at most k orthogonal matrices; see [3, Observation 7 and Question 3]. We give an affirmative answer to his question and improve his result by showing that if $A \in M_n(\mathbf{R})$, then $A/\|A\|$ is an affine combination of no more than four orthogonal matrices (see Proposition 1). Moreover, we also prove that if $A \in M_n(\mathbf{R})$ satisfies $\|A\| \leq 1$, then A can be written as a convex combination of a small number of orthogonal matrices (see Proposition 2).

In the same paper [3], Zhan showed that if $A \in M_n(\mathbf{R})$ then A^t is a linear combination

*Research partially supported by an NSF grant.

of $2^n + (n-1)n2^{n-1}$ matrices in $\mathcal{O}(A)$, and asked the following questions (Problems 1 and 2 in [3]).

Problem. *Find the smallest positive integers $k = k(n)$ and $m = m(n)$ for which one can find $k(n)$ orthogonal matrices Q_j (fixed independently of A) or $m(n)$ orthogonal matrices W_j (which may depend on A) such that A^t is a linear combination of $Q_j^t A Q_j$ (or $W_j^t A W_j$).*

We show that $k(n) \leq \frac{1}{2}(n^4 - n^2 - 2n + 2)$ and $m(n) \leq 2n - 1$; see Propositions 3 and 6. Note that our bounds on $k(n)$ and $m(n)$ are polynomial in n whereas the bounds of Zhan are exponential in n. Nonetheless, we believe that there is still much room for improvement.

Denote by

$$\operatorname{diag}(d_1, \ldots, d_n)$$

the $n \times n$ diagonal matrix whose (j,j)-entry is d_j. Let $A = (a_{ij}) \in M_n(\mathbf{R})$, and let

$$\Delta(A) = \operatorname{diag}(a_{11}, \ldots, a_{nn}).$$

A related problem is to write $\Delta(A)$ as a combination of matrices in $\mathcal{O}(A)$. Zhan in [3] showed that one can use such a combination to help express A^t as a combination of matrices in $\mathcal{O}(A)$. We will also discuss improving this scheme and some related results.

2 Combinations of Orthogonal Matrices

Proposition 1 *If $A \in M_n(\mathbf{R})$ then $A/\|A\|$ is an affine combination of no more than four orthogonal matrices. More precisely, there are orthogonal matrices X, Y, Z (depending on A) such that*

$$A/\|A\| = (X + X^t + Y - Z)/2. \tag{1}$$

Proof. By the singular value decomposition, there are orthogonal matrices P, Q such that $D = P(A/\|A\|)Q = \operatorname{diag}(a_1, \ldots, a_n)$ where $0 \leq a_1 \leq \cdots \leq a_n = 1$. First suppose $n = 2k$ is even. Let R be the direct sum of k copies of the matrix

$$\frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Then R is orthogonal and $R^t D R = B_1 \oplus \cdots \oplus B_k$, where for $j = 1, \ldots, k$,

$$B_j = \begin{pmatrix} b_j & c_j \\ c_j & b_j \end{pmatrix} \quad \text{with} \quad 2b_j = a_{2j-1} + a_{2j} \quad \text{and} \quad 2c_j = a_{2j} - a_{2j-1}. \tag{2}$$

Let $\hat{X}, \hat{Y}, \hat{Z} \in M_n$ be such that

$$\hat{X} = X_1 \oplus \cdots \oplus X_k, \quad \hat{Y} = Y_1 \oplus \cdots \oplus Y_k, \quad \hat{Z} = Z_1 \oplus \cdots \oplus Z_k,$$

with

$$X_j = \begin{pmatrix} b_j & \sqrt{1-b_j^2} \\ -\sqrt{1-b_j^2} & b_j \end{pmatrix}, \quad Y_j = \begin{pmatrix} \sqrt{1-c_j^2} & c_j \\ c_j & -\sqrt{1-c_j^2} \end{pmatrix},$$

$$Z_j = \begin{pmatrix} \sqrt{1-c_j^2} & -c_j \\ -c_j & -\sqrt{1-c_j^2} \end{pmatrix}, \qquad \text{for } j = 1, \ldots, k.$$

Thus $\hat{X}, \hat{Y}, \hat{Z}$ are orthogonal matrices satisfying

$$B_1 \oplus \cdots \oplus B_k = (\hat{X} + \hat{X}^t + \hat{Y} - \hat{Z})/2,$$

and so setting $X = P^t R \hat{X} R^t Q^t$, $Y = P^t R \hat{Y} R^t Q^t$, $Z = P^t R \hat{Z} R^t Q^t$ shows that (1) holds.

If $n = 2k+1$ is odd, then there exists an orthogonal matrix R such that

$$R^t D R = B_1 \oplus \cdots \oplus B_k \oplus [1],$$

where B_j has the form (2). One can construct X, Y, Z as above by appending the one-by-one identity matrix to $\hat{X}, \hat{Y}, \hat{Z}$. One readily checks that (1) is valid. □

It is known that a matrix $A \in M_n(\mathbf{R})$ with $\|A\| \leq 1$ is a convex combination of orthogonal matrices. The next result concerns the number of matrices needed in the combination. For a nonnegative integer r, let

$$f(r) = \begin{cases} r+1 & \text{if } r \leq 4, \\ [\log_2 r] + 3 & \text{otherwise,} \end{cases}$$

where $[x]$ denotes the integral part of $x \in [0, \infty)$.

Proposition 2 *Suppose $A \in M_n(\mathbf{R})$ satisfies $\|A\| \leq 1$. If $I - A^*A$ has rank not larger than r, then A is a convex combination of no more than $f(r)$ orthogonal matrices.*

In applying the above proposition, if there is no information about the rank of $I - A^*A$, one can let $r = n$; if $\|A\| = 1$, then one can let $r = n - 1$.

Proof. Let $D = \operatorname{diag}(a_1, \ldots, a_n)$ with $0 \leq a_1 \leq \cdots \leq a_n \leq 1$ and $P, Q \in M_n(\mathbf{R})$ be orthogonal matrices such that $A = PDQ$.

First suppose that $I - A^*A$ has rank n, i.e., $a_n < 1$. Then $v = (a_1, \ldots, a_n)^t \in \mathbf{R}^n$ satisfies $l_\infty(v) \leq 1$. (Here $l_\infty(v) = \max_j |a_j|$.) By the Caratheodory Theorem, v is a convex combination of no more than $n+1$ extreme points of $\mathcal{B} = \{u \in \mathbf{R}^n : l_\infty(u) \leq 1\}$. It is well known that the set of extreme points of $\mathcal{B}$ is the set

$$\mathcal{E} = \{u = (u_1, \ldots, u_n)^t \in \mathbf{R}^n : |u_j| = 1,\ j = 1, \ldots, n\}.$$

It follows that $v = \sum_{j=1}^k t_j w_j$ for some $k \leq n+1$, $w_j \in \mathcal{E}$, and $t_1, \ldots, t_k > 0$ with $t_1 + \cdots + t_k = 1$. Now, let W_j be the diagonal orthogonal matrix such that $W_j(1, \ldots, 1)^t = w_j$ for each $j \in \{1, \ldots, k\}$. Then $D = \sum_{j=1}^k t_j W_j$, and thus $A = P(\sum_{j=1}^k t_j W_j)Q$.

Also, we can use the real version of [1, Proposition 2.2] (the proof for the real symmetric case is exactly the same as the complex Hermitian case) to conclude that $D = \sum_{j=1}^{m} s_j Q_j$, where $m \leq [\log_2 n] + 2$, $s_1, \ldots, s_m > 0$, $s_1 + \cdots + s_m = 1$, and $Q_1, \ldots, Q_m \in M_n(\mathbf{R})$ are real symmetric idempotents. Note that $P_j = 2Q_j - I$ is orthogonal for each $j = 1, \ldots, m$, and

$$D = \sum_{j=1}^{m} s_j (I + P_j)/2 = \frac{1}{2} I + \sum_{j=1}^{m} \frac{s_j}{2} P_j.$$

It follows that

$$A = P \left(\frac{1}{2} I + \sum_{j=1}^{m} \frac{s_j}{2} P_j \right) Q$$

is a convex combination of $m + 1 \leq [\log_2 n] + 3$ orthogonal matrices.

Now, suppose $I - A^*A$ has rank r, i.e., $a_{r+1} = \cdots = a_n = 1$. Then $D = D_1 \oplus I_{n-r}$. We can apply the previous argument to D_1 and write it as a convex combination of orthogonal matrices $V_1, \ldots, V_k$ with $k \leq f(r)$. Then A is a convex combination of the orthogonal matrices $P(V_1 \oplus I_{n-r})Q, \ldots, P(V_k \oplus I_{n-r})Q$, and the result follows. □

It would be nice to improve our bounds in Propositions 1 and 2, or show that they are optimal.

3 Combinations of Matrices from Orthogonal Orbits

Recall that a *generalized permutation matrix* is a product of a permutation and a diagonal matrix with diagonal entries in $\{1, -1\}$. The following result answers Problem 1 in [3] (see also the problem in our introduction).

Proposition 3 *There exist a positive integer k with $k \leq \frac{1}{2}(n^4 - n^2 - 2n + 2)$, generalized permutation matrices $Q_1, \ldots, Q_k$, and real numbers $r_1, \ldots, r_k$ summing to 1 such that, for any $A \in M_n(\mathbf{R})$,*

$$A^t = \sum_{j=1}^{k} r_j Q_j^t A Q_j. \tag{3}$$

We remark that (3) actually holds for $n \times n$ matrices over any field containing the rational numbers.

Proof. Given $P, Q \in M_n(\mathbf{R})$, let $P \otimes Q$ denote the map defined by $P \otimes Q(A) = PAQ^t$ for any $A \in M_n(\mathbf{R})$. Then the first assertion is equivalent to writing the transpose operator $T(A) = A^t$ as an affine combination of at most $\frac{1}{2}(n^4 - n^2 - 2n + 2)$ operators of the form $Q_i \otimes Q_i$, where Q_i are generalized permutations. Lemma 2 in [3] shows that the transpose operator lies in the span of $\{P \otimes P : P \in M_n(\mathbf{R}),\ P \text{ is a generalized permutation}\}$ (with rational coefficients). This span is a subspace of (actually equals) the space M of operators

acting on $M_n(\mathbf{R})$ which fix I and leave the subspace of symmetric matrices of trace zero and the subspace of skew-symmetric matrices invariant. Note that

$$\dim M = \left(\frac{n^2+n-2}{2}\right)^2 + \left(\frac{n^2-n}{2}\right)^2 = \frac{1}{2}\left(n^4 - n^2 - 2n + 2\right).$$

To see this, one can write down the operator matrix of a linear operator in M with respect to a basis which is a union of the bases of the symmetric matrices with trace zero, skew-symmetric matrices, and the identity matrix. Now, taking $A = I_n$ in (3), we see that the coefficients sum up to one, i.e., the combination is affine. The first assertion follows. Note that all the above arguments can be limited to the field of rational numbers. This justifies our remark after the proposition. □

Recall that $\Delta(A)$ denotes the diagonal matrix obtained from $A \in M_n(\mathbf{R})$ by setting its off-diagonal entries to 0. It is interesting and useful to express $\Delta(A)$ as a combination of matrices in $\mathcal{O}(A)$. First note that if the set of diagonal orthogonal matrices with $(1,1)$-entry equal to 1 is denoted by $\{R_1, \ldots, R_{2^{n-1}}\}$, then

$$\Delta(A) = \frac{1}{2^{n-1}} \sum_{j=1}^{2^{n-1}} R_j^t A R_j. \tag{4}$$

So, $\Delta(A)$ belongs to the convex hull of $\mathcal{O}(A) \subseteq \{X \in M_n(\mathbf{R}) : \operatorname{tr} X = \operatorname{tr} A\}$. By the Caratheodory Theorem, $\Delta(A)$ is a convex combination of no more than n^2 matrices in $\mathcal{O}(A)$. The situation will be much improved if $M_n(\mathbf{R})$ has a Hadamard matrix H, i.e., $H \in M_n(\mathbf{R})$ with entries in $\{1, -1\}$ and $H^t H = nI_n$. In such a case, we have

$$\Delta(A) = \frac{1}{n} \sum_{j=1}^{n} H_j^t A H_j,$$

where H_j is the diagonal matrix such that $H_j(1, \ldots, 1)^t$ equals the jth column of H. In general, let m be the smallest integer larger than or equal to n such that there is a Hadamard matrix in $M_m(\mathbf{R})$, and apply the above argument to $\tilde{A} = A \oplus 0_{m-n}$ to get

$$\Delta(\tilde{A}) = \frac{1}{m} \sum_{j=1}^{m} \tilde{H}_j^t \tilde{A} \tilde{H}_j,$$

for some diagonal orthogonal matrices $\tilde{H}_j \in M_m(\mathbf{R})$. Let H_j be the leading $n \times n$ submatrix of $\tilde{H}_j$ for $j = 1, \ldots, m$. Then

$$\Delta(A) = \frac{1}{m} \sum_{j=1}^{m} H_j^t A H_j.$$

In connection with the above discussion, we have the following definition and result.

Definition 4 *For a positive integer n, let $h(n) \geq n$ be the smallest integer such that there is a $h(n) \times h(n)$ Hadamard matrix.*

Proposition 5 *For any $A \in M_n(\mathbf{R})$, the matrix $\Delta(A)$ can be written as the average of no more than $h(n)$ matrices in $\mathcal{O}(A)$.*

It is known that $M_n(\mathbf{R})$ has Hadamard matrices if $n = 2^k$, $k \geq 0$. Thus, Proposition 5 allow one to exhibit the diagonal of a matrix as an average of (much) fewer terms than suggested in (4) and the bound n^2 in the discussion afterward. To see this, observe that if $n = 2^k$ then $h(n) = n$, and if $2^k < n < 2^{k+1}$, then $h(n) \leq 2^{k+1} \leq 2(n-1)$. One readily verifies $h(n) = 2^{n-1}$ for $n \leq 2$ and $h(n) \leq 2(n-1) \leq 2^{n-1}$ for $n > 2$. Similarly one can check that $h(n) \leq n^2$.

We can use Proposition 5 to improve the result in [3] related to Problem 2 in the paper (see also the problem in our introduction). We exclude the trivial case $n = 1$ in our statement.

Proposition 6 *Let $A \in M_n(\mathbf{R})$ and $n > 1$. Then A^t can be expressed as an affine combination of no more than $h(n) + 1 \leq 2n - 1$ matrices in $\mathcal{O}(A)$.*

Proof. Write $A = A_1 + A_2$ where $A_1 = (A + A^t)/2$, $A_2 = (A - A^t)/2$. Then there is an orthogonal matrix P and a diagonal matrix D such that $A_1 = P^t D P$, and $A = P^t(D + B)P$, where B is skew-symmetric and thus has all diagonal entries equal to zero. By Proposition 5, $D = \Delta(D + B)$ (and hence $A_1 = P^t D P$) can be expressed as an affine combination of no more than $h(n)$ matrices in $\mathcal{O}(D + B) = \mathcal{O}(A)$. It follows that $A^t = 2A_1 - A$ is an affine combination of no more that $h(n) + 1$ matrices in $\mathcal{O}(A)$. Finally, the inequality follows from the argument preceding the proposition. □

We thank Professors Man-Duen Choi and Pei-Yuan Wu for some helpful discussions.

References

[1] M.D. Choi and P.Y. Wu, Convex combinations of projections, Linear Algebra Appl. 136 (1990), 25-42.

[2] P.Y. Wu, Additive combinations of special operators, Functional analysis and operator theory (Warsaw, 1992), 337–361, Banach Center Publ., 30, Polish Acad. Sci., Warsaw, 1994.

[3] X. Zhan, Span of the orthogonal orbit of real matrices, Linear and Multilinear Algebra 49 (2001), 337-346.