Decomposition of Matrices into Three Involutions

Kang-Man Liu*
Department of Applied Mathematics
National Chiao Tung University
Hsinchu, Taiwan, Republic of China

Submitted by Richard A. Brualdi

ABSTRACT

In this paper, we generalize some results of C. S. Ballantine concerning products of three $n \times n$ complex involutions. We prove that each $n \times n$ complex matrix A with determinant ± 1 and $\dim\ker(A-\alpha) \leqslant [n/2]$ for all $\alpha \in \mathbf{C}$ is the product of three involutions. On the other hand, we show that if an $n \times n$ complex matrix A is the product of three involutions, then $m \leqslant (2n+r)/3$ and $m \leqslant [3n/4]$, where $m = \dim\ker(A-\beta)$ and $r = \dim\ker(A-\beta^{-3})$ for any β, $\beta \neq 0$ and $\beta^4 \neq 1$. We also completely characterize products of three 5×5 complex involutions.

0. INTRODUCTION

A square matrix A over some field is an *involution* if A^2 is the identity matrix. Wonenburger [9] proved that an $n \times n$ matrix A over a field with characteristic $\neq 2$ is the product of two involutions if and only if A is similar to A^{-1}. Djokovic [5] proved it for arbitrary fields. Since then, it has also been proved by other people independently [1, 2, 7]. In [6], Gustafson, Halmos, and Radjavi showed that every $n \times n$ matrix over a field F with determinant ± 1 is the product of at most four involutions. Moreover, four is the smallest such number. In 1985, Sourour [8] gave a short proof for the special case when F has at least $n+2$ elements.

*This paper is adapted from the author's Master's thesis written at National Chiao Tung University under the guidance of Professor Pei Yuan Wu.

655 Avenue of the Americas, New York, NY 10010 0024-3795/88/$3.50

In [3], Ballantine proved that every matrix over an arbitrary field F with determinant ± 1 having no more than two nontrivial invariant factors is the product of three involutions over F. Moreover, he showed that if an $n \times n$ matrix A over a field F is the product of three involutions, then $m \leqslant 3n/4$, where $m = \dim\ker(A - \beta I)$ for any $\beta \in F$, $\beta^4 \neq 1$. He also characterized products of three $n \times n$ involutions for the special cases when $n \leqslant 4$ or F has prime order $\leqslant 5$.

In this paper, we generalize all these results for matrices over the complex field $\mathbb{C}$. More precisely, we prove that each $n \times n$ complex matrix A with determinant ± 1 and $\dim\ker(A - \alpha) \leqslant [n/2]$ for any $\alpha \in \mathbb{C}$ is the product of three involutions (Theorem 2.5). Moreover, we show that if an $n \times n$ complex matrix A is the product of three involutions, then $m \leqslant (2n + r)/3$ and $m \leqslant [3n/4]$, where $m = \dim\ker(A - \beta)$ and $r = \dim\ker(A - \beta^{-3})$ for any β, $\beta \neq 0$ and $\beta^4 \neq 1$ (Theorem 3.1). We also completely characterize products of three 5×5 complex involutions (Theorem 3.2).

1. NOTATION AND PRELIMINARY DEFINITIONS

A matrix is called *cyclic* if its characteristic and minimal polynomials coincide. By an *elementary Jordan matrix* $J_k(\lambda)$ is meant a square matrix of size k of the form

$$\begin{bmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \end{bmatrix}.$$

Let $\operatorname{tr}(A)$ denote the trace of A, and $\sigma(A)$ denote the set of all eigenvalues of a matrix A. Denote by I the identity matrix, by I_n the $n \times n$ identity matrix, and by 0_n the $n \times n$ zero matrix. Denote by $T(n)$ the set of all $n \times n$ complex involutions, and by $T(n)^k$ the set of all matrices which are products of k matrices from $T(n)$.

For complex matrices, Djokovic [5] proved the following theorem, which is also our main tool in proving results for products of three involutions.

THEOREM 1.1. *Let A be a complex invertible matrix. Assume that A is similar to $\sum_i \oplus J_{k_i}(\lambda_i)$, where each $J_{k_i}(\lambda_i)$ is an elementary Jordan matrix* *belonging to* λ_i *of size* k_i. *Then the following are equivalent*:

(1) *A is similar to* A^{-1};

(2) *except those* $J_{k_i}(\lambda_i)$ *with* $\lambda_i = \pm 1$, *all the rest are in pairs* $J_{k_j}(\lambda_j)$ *and* $J_{k_l}(\lambda_l)$ *such that* $k_j = k_l$ *and* $\lambda_j \lambda_l = 1$;

(3) *A is the product of two involutions.*

2. SUFFICIENT CONDITIONS

Our main result in this section is Theorem 2.5, which gives a sufficient condition for a complex matrix expressible as the product of three involutions and generalizes a sufficient condition in [3]. To prove this theorem, we need the following lemmas.

LEMMA 2.1. *Let T be an invertible cyclic matrix of order n. If* $\alpha_1, \alpha_2, \dots, \alpha_n$ *are complex numbers satisfying* $\alpha_1 \alpha_2 \cdots \alpha_n = -\det T$, *then there exist an involution P and a cyclic B with* $\sigma(B) = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ *such that* $T = PB$.

Proof. Since T is cyclic, $T = ST_1S^{-1}$, where S is invertible and

$$T_1 = \left[\begin{array}{c|c} 0 & a_0 \\ \hline I_{n-1} & \begin{matrix} a_1 \\ \vdots \\ a_{n-1} \end{matrix} \end{array}\right].$$

Let $\{\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \alpha_n\}$ be the roots of the polynomial equation

$$\lambda^n + d_{k-1}\lambda^{n-1} + \cdots + d_2\lambda^2 + d_1\lambda + a_0 = 0.$$

If

$$B_1 = \left[\begin{array}{c|c} 0 & -a_0 \\ \hline I_{n-1} & \begin{matrix} -d_1 \\ -d_2 \\ \vdots \\ -d_{n-1} \end{matrix} \end{array}\right],$$

then B_1 is cyclic, $\sigma(B_1)=\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ and $\det B_1=\alpha_1\alpha_2\cdots\alpha_n=-\det T$.

Let

$$P_1=\left[\begin{array}{c|c} -1 & 0 \\ \hline x_1 & \\ x_2 & \\ \vdots & I_{n-1} \\ x_{n-1} & \end{array}\right],$$

where $x_i=-a_0^{-1}(d_i+a_i)$, $1\leqslant i\leqslant n-1$. Note that P_1 is an involution and

$$P_1T_1=\left[\begin{array}{c|c} -1 & 0 \\ \hline x_1 & \\ x_2 & \\ \vdots & I_{n-1} \\ x_{n-1} & \end{array}\right]\left[\begin{array}{c|c} 0 & a_0 \\ \hline & a_1 \\ & a_2 \\ I_{n-1} & \vdots \\ & a_{n-1} \end{array}\right]$$

$$=\left[\begin{array}{c|c} 0 & -a_0 \\ \hline & a_0x_1+a_1 \\ & a_0x_2+a_2 \\ I_{n-1} & \vdots \\ & a_0x_{n-1}+a_{n-1} \end{array}\right]$$

$$=\left[\begin{array}{c|c} 0 & -a_0 \\ \hline & -d_1 \\ & -d_2 \\ I_{n-1} & \vdots \\ & -d_{n-1} \end{array}\right]=B_1.$$

Hence $T_1=P_1B_1$. Let $P=SP_1S^{-1}$ and $B=SB_1S^{-1}$. We have $T=ST_1S^{-1}=SP_1S^{-1}SB_1S^{-1}=PB$ and $\sigma(B)=\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$. ■

Lemma 2.2. *Let A be an $n\times n$ complex matrix with determinant ± 1. If $A=A_1\oplus A_2\oplus\cdots\oplus A_m$, where each A_i is a square matrix of order l_i at least 2 and each A_i is cyclic, then A is the product of three involutions.*

Proof. We distinguish two cases. Let $a_i = -\det A_i$, $1 \leqslant i \leqslant m$, and α be sufficiently large, say, $\alpha \geqslant h^m$, where $h = \max_{1 \leqslant i \leqslant m}|a_i| + 1$.

Case 1: *m is odd and* $\det A = -1$, *or m is even and* $\det A = 1$. Applying Lemma 2.1, we obtain m involutions P_i such that $\sigma(P_1A_1) = \{\alpha, \alpha^{-1}a_1, 1, \dots, 1\}$ and $\sigma(P_iA_i) = \{\alpha(a_1 \cdots a_{i-1})^{-1}, \alpha^{-1}(a_1a_2 \cdots a_i), 1, \dots, 1\}$, $2 \leqslant i \leqslant m$, where the 1's may be absent. Let $P = P_1 \oplus P_2 \oplus \cdots \oplus P_m$. Then P is an involution and $PA = P_1A_1 \oplus P_2A_2 \oplus \cdots \oplus P_mA_m$. Note that by our choice of α the eigenvalues of PA except the 1's are pairwise reciprocal and distinct. Hence PA is the product of two involutions by Theorem 1.1, and A is the product of three involutions.

Case 2: *m is odd and* $\det A = 1$, *or m is even and* $\det A = -1$.

(I) If there exists some A_i, with $l_i \geqslant 3$, say $l_1 \geqslant 3$, by the same method as in Case 1, there exist m involutions P_i such that $\sigma(P_1A_1) = \{-\alpha, \alpha^{-1}a_1, -1, 1, \dots, 1\}$ and $\sigma(P_iA_i) = \{\alpha(a_1 \cdots a_{i-1})^{-1}, \alpha^{-1}(a_1a_2 \cdots a_i), 1, \dots, 1\}$, $2 \leqslant i \leqslant m$, where the 1's may be absent. As before, A is the product of three involutions.

(II) If A is not as in (I), then $l_i = 2$ for $i = 1, 2, \dots, m$. Again, we consider two cases:

⟨1⟩ If $a_i \neq a_j$ for some $i \neq j$, say $a_1 \neq a_2$, then $A_1 \oplus A_2$ is similar to either B_2 or $B_1 \oplus \beta$, where B_2 is cyclic, B_1 is a 3×3 cyclic matrix, and β is a scalar.

If $A_1 \oplus A_2$ is similar to B_2, then A is similar to $B_2 \oplus A_3 \oplus \cdots \oplus A_m$, which reduce to Case 1.

If $A_1 \oplus A_2$ is similar to $B_1 \oplus \beta$, then choose δ such that $\beta, \beta^{-1}, -\delta, \delta^{-1}a_1a_2$ are distinct and $\delta \geqslant \alpha$. Applying Lemma 2.1, we obtain m involutions P_i such that $\sigma(P_1B_1) = \{\beta^{-1}, -\delta, \delta^{-1}a_1a_2\}$, $\sigma(P_2\beta) = \{\beta\}$, and $\sigma(P_iA_i) = \{\sigma(a_1a_2 \cdots a_{i-1})^{-1}, \sigma^{-1}(a_1a_2 \cdots a_i), 1, \dots, 1\}$, $3 \leqslant i \leqslant m$, where the 1's may be absent. Using the same technique as in Case 1, we can prove this case.

⟨2⟩ If all a_i's are equal, say $a_i = a$ for all i, then $a^m = -1$. By Lemma 2.1, there exist m involutions P_i such that

$$\sigma(P_iA_i) = \{a^{1-i}, a^i\}, \qquad 1 \leqslant i \leqslant m \text{ and } a^{2i-1} \neq 1.$$

Let $P = P_1 \oplus P_2 \oplus \cdots \oplus P_m$. By the same method as in Case 1, the proof is complete. ∎

The main idea of constructing a new basis in the proofs of Lemmas 2.3 and 2.4 comes from [4].

Lemma 2.3. *Let A_1 be a complex invertible matrix of order $2k$. If $A_1 = B_1 \oplus D_1$, where B_1 is a square matrix of order $k \geqslant 2$,*

$$B_1 = \begin{bmatrix} \beta & & & & & \\ 1 & \beta & & & & \\ & 1 & \cdot & & & \\ & & \cdot & \cdot & & \\ & & & \cdot & \cdot & \\ & & & & 1 & \beta \end{bmatrix},$$

and $D_1 = \alpha I_k$ is a $k \times k$ scalar matrix, $\alpha \neq \beta$, then, for any $\alpha_1, \ldots, \alpha_k$, $\beta_1, \ldots, \beta_k$ satisfying $\alpha_i \beta_i = -\alpha\beta$, $1 \leqslant i \leqslant k$, there exist an involution P and a $2k \times 2k$ matrix C with $\sigma(C) = \{\alpha_1, \alpha_2, \ldots, \alpha_k, \beta_1, \beta_2, \ldots, \beta_k\}$ and $PA_1 = C$.

Proof. Let $A = A_1 - \beta I_{2k}$ and $\gamma = \alpha - \beta$. Then

$$A = \left[\begin{array}{cccc|c} 0 & & & & \\ 1 & 0 & & & 0 \\ & \ddots & \ddots & & \\ & & 1 & 0 & \\ \hline & & 0 & & \gamma I_k \end{array}\right].$$

Let $e_i = \langle \delta_{1i}, \delta_{2i}, \ldots, \delta_{ni} \rangle^t$, $1 \leqslant i \leqslant n$, where $n = 2k$ and

$$\delta_{ik} = \begin{bmatrix} 1 & \text{if} & i = k \\ 0 & \text{if} & i \neq k, \end{bmatrix}$$

and let $f = e_1 + e_2 + \cdots e_k$. Then the vectors $f, Af, \ldots, A^{k-1}f$ are linearly independent. Let $e_i' = A^{i-1}f + e_{k+i}$ and $e_{k+i}' = A^i f + \gamma e_{k+i}$ for $1 \leqslant i \leqslant k$. Then

$$\begin{aligned} e_{i+1}' - e_{k+i}' &= A^i f + e_{k+i+1} - \left(A^i f + \gamma e_{k+i}\right) \\ &= e_{k+i+1} - \gamma e_{k+i} \end{aligned} \qquad (*)$$

for $i = 1, 2, \ldots, k-1$, and $Ae_i' = e_{k+i}$, $1 \leqslant i \leqslant k$.

Since the set $\{f, Af, \ldots, A^{k-1}f, e_{k+1}, e_{k+2}, \ldots, e_{2k}\}$ forms a basis, so does the set $D = \{e'_1, e'_2, \ldots, e'_k, Ae'_1, Ae'_2, \ldots, Ae'_k\}$. Moreover,

$$
\begin{aligned}
Ae'_{k+i} &= A^{i+1}f + \gamma^2 e_{k+i} \\
&= e'_{k+i+1} - \gamma e_{k+i+1} + \gamma^2 e_{k+i} \\
&= e'_{k+i+1} - \gamma(e_{k+i+1} - \gamma e_{k+i}) \\
&= e'_{k+i+1} - \gamma(e'_{i+1} - e'_{k+i}) \qquad [\text{by } (*)] \\
&= -\gamma e'_{i+1} + e'_{k+i+1} + \gamma e'_{k+i}, \qquad 1 \leqslant i \leqslant k-1,
\end{aligned}
$$

and

$$Ae'_{2k} = A(\gamma e_{2k}) = \gamma^2 e_{2k} = \gamma e'_{2k}.$$

Relative to the basis D, the matrix representation of A is of the form

$$A_2 = \left[\begin{array}{c|c} 0 & E_1 \\ \hline I_k & E_2 \end{array}\right],$$

where

$$E_1 = \begin{bmatrix} 0 & & & \\ -\gamma & 0 & & \\ & \ddots & \ddots & \\ & & -\gamma & 0 \end{bmatrix} \quad \text{and} \quad E_2 = \begin{bmatrix} \gamma & & & \\ 1 & \gamma & & \\ & \ddots & \ddots & \\ & & 1 & \gamma \end{bmatrix}$$

are both of size k.

We conclude that A is similar to A_2. Let

$$S = \left[\begin{array}{c|c} I_k & -\beta I_k \\ \hline 0 & I_k \end{array}\right].$$

Then

$$SA_2S^{-1}=\left[\begin{array}{c|c} I_k & -\beta I_k \\ \hline 0 & I_k \end{array}\right]\left[\begin{array}{c|c} 0 & E_1 \\ \hline I_k & E_2 \end{array}\right]\left[\begin{array}{c|c} 0 & \beta I_k \\ \hline 0 & I_k \end{array}\right]$$

$$=\left[\begin{array}{c|c} -\beta I_k & -\beta^2 I_k + E_1 - \beta E_2 \\ \hline I_k & \beta I_k + E_2 \end{array}\right].$$

Hence $A_1 = A + \beta I_{2k}$ is similar to the matrix

$$A_3=\left[\begin{array}{c|c} 0 & -\beta^2 I_k + E_1 - \beta E_2 \\ \hline I_k & 2\beta I_k + E_2 \end{array}\right],$$

say, $A_1 = VA_3V^{-1}$. Let $E_3 = -\beta^2 I_k + E_1 - \beta E_2$ and $E_4 = 2\beta I_k + E_2$. Then

$$E_3=\begin{bmatrix} -\alpha\beta & & & \\ -\alpha & -\alpha\beta & & \\ & \ddots & \ddots & \\ & & -\alpha & -\alpha\beta \end{bmatrix},$$

$$E_4=\begin{bmatrix} \alpha+\beta & & & \\ 1 & \alpha+\beta & & \\ & \ddots & \ddots & \\ & & 1 & \alpha+\beta \end{bmatrix},$$

and

$$A_3=\left[\begin{array}{c|c} 0 & E_3 \\ \hline I_k & E_4 \end{array}\right].$$

If

$$P_1=\left[\begin{array}{c|c} -I_k & 0 \\ \hline (Q-E_4)E_3^{-1} & I_k \end{array}\right],$$

where Q is an arbitrary $k\times k$ matrix, then P_1 is an involution and

$$P_1A_3=\left[\begin{array}{c|c}0 & -E_3\\ \hline I_k & Q\end{array}\right].$$

If $\lambda\neq 0$, we have

$$P_1A_3-\lambda I_{2k}=\left[\begin{array}{c|c}-\lambda I_k & -E_3\\ \hline I_k & Q-\lambda I_k\end{array}\right]=\left[\begin{array}{c|c}-\lambda I_k & 0\\ \hline I_k & I_k\end{array}\right]\left[\begin{array}{c|c}I_k & \lambda^{-1}E_3\\ \hline 0 & E_5\end{array}\right],$$

where $E_5=Q-\lambda I_k-\lambda^{-1}E_3$. If we choose

$$Q=\begin{bmatrix}c_1 & & & \\ & c_2 & & \\ & & \ddots & \\ & & & c_k\end{bmatrix},$$

where $c_i=\alpha_i+\beta_i$, $1\leqslant i\leqslant k$, then

$$E_5=\begin{bmatrix}d_1 & & & & \\ -\alpha_1 & d_2 & & & \\ & -\alpha & \ddots & & \\ & & \ddots & \ddots & \\ & & & -\alpha & d_k\end{bmatrix},$$

where $d_i=c_i-\lambda+\lambda^{-1}\alpha\beta$. Since

$$\det\left[\begin{array}{c|c}I_k & \lambda^{-1}E_3\\ \hline 0 & E_5\end{array}\right]=\det E_5,$$

we have $\sigma(P_1A_3)=\{\alpha_1,\alpha_2,\ldots,\alpha_k,\beta_1,\beta_2,\ldots,\beta_k\}$.

Let $P=VP_1V^{-1}$ and $PA_1=C$. Then $PA_1=VP_1V^{-1}VA_3V^{-1}=VP_1A_3V^{-1}$ and $\sigma(PA_1)=\sigma(P_1A_3)$. The proof is complete. ∎

LEMMA 2.4. *Let A_1 be a $2n\times 2n$ complex invertible matrix. If $A_1 = B\oplus D$, where D is a scalar matrix αI_m of order m, and*

$$B=\begin{bmatrix}\alpha & & & & \\ 1 & \alpha & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & \alpha\end{bmatrix}$$

is a square matrix of order $l\geqslant 3$, $l-m\geqslant 2$, then, for any $\alpha_1,\dots,\alpha_n$, $\beta_1,\dots,\beta_n$ satisfying $\alpha_i\beta_i=-\alpha^2$, $1\leqslant i\leqslant n$, there exist an involution P and a $2n\times 2n$ matrix C with $\sigma(C)=\{\alpha_1,\alpha_2,\dots,\alpha_n,\beta_1,\beta_2,\dots,\beta_n\}$ and $PA_1=C$. Moreover, we may choose some $\lambda_1\in\sigma(C)$ such that $2\leqslant \dim\ker(C-\lambda_1)\leqslant n$.

Proof. Let $A=A_1-\alpha I_{2n}$. Then

$$A=\left[\begin{array}{cccc|c}0 & & & & \\ 1 & 0 & & & \\ & \ddots & \ddots & & 0\\ & & 1 & 0 & \\ \hline & & 0 & & 0_m\end{array}\right].$$

Let $e_i=\langle\delta_{1,i},\delta_{2,i},\dots,\delta_{2n,i}\rangle^t$, $1\leqslant i\leqslant 2n$, and $f=e_1+e_2+\cdots+e_l$. Then the vectors $f, Af,\dots,A^{l-1}f$ are linearly independent.

Let $k=n-m$, $A^0f=f$, $e_i'=A^{2i-2}f$ if $1\leqslant i\leqslant k$, and $e_{k+i}'=A^{2k-2+i}f+e_{l+i}$ if $1\leqslant i\leqslant m$. Let $e_{n+i}'=Ae_i'$, $1\leqslant i\leqslant n$. Then $e_{n+i}'=A^{2i-1}f$ if $1\leqslant i\leqslant k$, and $e_{n+k+i}'=A^{2k-1+i}f$ if $1\leqslant i\leqslant m$. Since the set of vectors $\{f, Af,\dots,A^{l-1}f,e_{l+1},e_{l+2},\dots,e_{2n}\}$ forms a basis, so does the set

$$\{f, Af,\dots,A^{l-1}f, A^{2k-1}f+e_{l+1}, A^{2k}f+e_{l+2},\dots,A^{l-2}f+e_{2n}\}.$$

That is, the set $D=\{e_1',e_2',\dots,e_{2n}'\}$ forms a basis. Under this change of basis, A is similar to

$$A_2=\begin{bmatrix}0_n & E_1\\ I_n & E_2\end{bmatrix},$$

where

$$E_1 = \left[\begin{array}{cccc|c} 0 & & & & \\ 1 & 0 & & & 0 \\ & \ddots & \ddots & & \\ & & 1 & 0 & \\ \hline & & 0 & & 0_{n-k} \end{array}\right] \quad \text{and}$$

$$E_2 = \left[\begin{array}{c|cccc} 0_{k-1} & & 0 & & \\ \hline & 0 & & & \\ 0 & 1 & 0 & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{array}\right],$$

and thus $A_1 = A + \alpha I_{2n}$ is similar to the matrix

$$A_3 = \left[\begin{array}{c|c} 0 & -\alpha^2 I_n + E_1 - \alpha E_2 \\ \hline I_n & 2\alpha I_n + E_2 \end{array}\right].$$

Say, $A_1 = VA_3V^{-1}$. By the same method as in proving Lemma 2.3, the proof is complete. ■

THEOREM 2.5. *Let A be an $n \times n$ complete matrix with determinant ± 1. If $\dim\ker(A - \alpha I) \leqslant [n/2]$ for all $\alpha \in \mathbb{C}$, then A is the product of three involutions.*

Proof. A is similar to the Jordan canonical form $A_1 = V_1 \oplus V_2 \oplus \cdots \oplus V_k \oplus C_1 \oplus C_2 \oplus \cdots \oplus C_m$, where each

$$V_i = \begin{bmatrix} \lambda_i & & & \\ 1 & \lambda_i & & \\ & \ddots & \ddots & \\ & & 1 & \lambda_i \end{bmatrix}$$

is a square matrix of order $\omega_i \geqslant 2$, and each C_i is a scalar matrix $\alpha_i I_{l_i}$ of order l_i with $l_i \geqslant l_{i+1}$, $1 \leqslant i \leqslant m-1$. It is understood that $\alpha_i \neq \alpha_j$ if $i \neq j$ and that either the V_i's or the C_i's may be absent.

Case I: If the C_i's are absent or $l_1 \leqslant \sum_{i=2}^{m} l_i$, then A_1 is similar to $A_2 = D_1 \oplus D_2 \oplus \cdots \oplus D_{m_1}$, where each D_i is cyclic and of size $\geqslant 2$. The conclusion follows from Lemma 2.2.

Case II: If A_1 is not as in Case I, then $l_1 > \sum_{i=2}^{m} l_i$. Let $h_2 = \sum_{i=2}^{m} l_i$ and $h_1 = l_1 - h_2$. Then $C_1 \oplus C_2 \oplus \cdots \oplus C_m$ is similar to $C_1' \oplus E_1 \oplus E_2 \oplus \cdots \oplus E_{h_2}$, where C_1' is a scalar matrix $\alpha_1 I_{h_1}$ of order h_1 and

$$E_i = \left[\begin{array}{c|c} \alpha_1 & 0 \\ \hline 0 & e_i \end{array}\right],$$

where e_i is one of $\alpha_2, \alpha_3, \ldots, \alpha_m$ for each $i = 1, 2, \ldots, h_2$. Hence A_1 is similar to $A_2 = V_1 \oplus V_2 \oplus \cdots \oplus V_k \oplus C_1' \oplus E_1 \oplus E_2 \oplus \cdots \oplus E_{h_2}$.

Let k_2 be the number of V_i's with eigenvalue α_1, $k_1 = k - k_2$, and s be the number of V_i's with order $\omega_i \geqslant 3$. We may assume that α_1 is not the eigenvalue of $V_1, V_2, \ldots, V_{k_1}$. Then A_2 is similar to either

$$A_3 = R_1 \oplus R_2 \oplus \cdots \oplus R_t \oplus V_{t+1} \oplus \cdots \oplus V_{k_1} \oplus B_1 \oplus B_2 \oplus \cdots$$
$$\oplus B_s \oplus V_{k_1+s+1} \oplus \cdots \oplus V_k \oplus E_1 \oplus E_2 \oplus \cdots \oplus E_{h_2}$$

or

$$A_4 = B_1 \oplus B_2 \oplus \cdots \oplus B_s \oplus V_{k_1+s+1} \oplus \cdots \oplus V_k \oplus E_1 \oplus E_2 \oplus \cdots \oplus E_{h_2} \oplus \alpha_1,$$

where

$$R_1 = V_1 \oplus \alpha_1 I_d, \qquad 0 < d \leqslant \omega_1,$$
$$R_i = V_i \oplus \alpha_1 I_{\omega_i}, \qquad 2 \leqslant i \leqslant t,$$
$$B_j = V_{k_1+j} \oplus \alpha_1 I_{r(j)},$$

$0 < r(j) \leqslant \omega_{k_1+j} - 2$, $r(j) + \omega_{k_1+j} = 2q_j$ for some integer $q_j \geqslant 2$, $j = 1, 2, \ldots, s$. It is understood that if $k_1 = 0$, then

$$A_3 = B_1 \oplus B_2 \oplus \cdots \oplus B_s \oplus V_{k_1+s+1} \oplus \cdots \oplus V_k \oplus E_1 \oplus E_2 \oplus \cdots E_{h_2}.$$

Let $a_i = (-1)^{\omega_i} \det R_i$ and $u_i = -\alpha_1 \lambda_i$, $1 \leqslant i \leqslant t$; $v_j = \det V_j$, $t+1 \leqslant j \leqslant k_1$ and $k_1 + s + 1 \leqslant j \leqslant k$. Let $u = -\alpha_1^2$, $b_j = (-1)^{q_j} \det B_j$, $1 \leqslant j \leqslant s$, and $\varphi_i = -\det E_i$, $1 \leqslant i \leqslant h_2$.

For simplicity, we may assume that $u^{\eta} \neq 1$ if $0 < \eta < q_i$, $1 \leqslant i \leqslant s$, $u_1^{\eta_1} \neq 1$ if $0 < \eta_1 \leqslant d$, and $u_i^{\eta_2} \neq 1$ if $0 < \eta_2 < \omega_i$, $2 \leqslant i \leqslant t$. Let $\epsilon = 1$ and $l = d + \sum_{i=2}^{2} \omega_i + \sum_{j=1}^{s} q_j + h_2 + k - t - s$. To prove that there exists an involution P such that PA_3 is similar to its inverse, we choose α sufficiently large, say $\alpha \geqslant \xi^n$, where $\xi = \max_{\lambda \in \sigma(A)} |\lambda| + 1$. We now distinguish five cases.

(1) *Assume that* $d = \omega_1$ *and* $(-1)^l \det A_3 = 1$. Applying Lemmas 2.1, 2.3, and 2.4, we obtain $k + h_2$ involutions P_i such that

$$\sigma(P_i R_i) = \left\{ \rho_i\left(1, u_i^{-1}, u_i^{-2}, \dots, u_i^{-\omega_i + 1}\right), \rho_i^{-1}\left(u_i, u_i^2, \dots, a_i\right) \right\},$$

where $\rho_i = \rho(a_0 a_1 \cdots a_{i-1})^{-1}$, $a_0 = 1$, $1 \leqslant i \leqslant t$;

$$\sigma(P_j V_j) = \left\{ \xi_j, \xi_j^{-1} v_j, \epsilon, \dots, \epsilon \right\},$$

where $\xi_j = \rho_t(a_t v_t v_{t+1} \cdots v_{j-1})^{-1}$, $v_t = 1, t + 1 \leqslant j \leqslant k_1$, and ϵ may be absent;

$$\sigma\left(P_{k_1+i} B_i\right) = \left\{ \zeta_i\left(1, u^{-1}, u^{-2}, \dots, u^{-q_i + 1}\right), \zeta_i^{-1}\left(u, u^2, \dots, b_i\right) \right\},$$

where $\zeta_i = \xi_{k_1}(b_0 b_1 \cdots b_{i-1})^{-1}$, $b_0 = 1$, $1 \leqslant i \leqslant s$;

$$\sigma\left(P_j V_j\right) = \left\{ \theta_j, \theta_j^{-1} v_j, \epsilon, \dots, \epsilon \right\},$$

where $\theta_j = \zeta_s(b_s v_{k_1+s} v_{k_1+s+1} \cdots v_{j-1})^{-1}$, $v_{k_1+s} = 1$, $k_1 + s + 1 \leqslant j \leqslant k$, and ε may be absent; and

$$\sigma(P_{k+i} E_i) = \left\{ \beta_i, \beta_i^{-1} \varphi_i \right\},$$

where $\beta_i = \theta_k(v_k \varphi_0 \varphi_1 \cdots \varphi_{i-1})^{-1}$, $\varphi_0 = 1$, $1 \leqslant i \leqslant h_2$. Let $P = P_1 \oplus P_2 \oplus \cdots \oplus P_{k+h_2}$. Then P is an involution and PA is similar to its inverse by Theorem 1.1. Hence A is the product of three involutions.

(2) *Assume that* $d = \omega_1$ *and* $(-1)^l \det A_3 = -1$. We want to show that there exists an involution P_1 with $\det P_1 = (-1)^{d+1}$ such that $\sigma(P_1 R_1) = \{ \alpha_1, \alpha_1^{-1}, \rho, \rho^{-1} u_1^2, -\rho(u_1^{-2}, u_1^{-3}, \dots, u_1^{1-d}), -\rho^{-1}(u_1^3, \dots, u_1^d) \}$. Let

$$P_1 = \left[\begin{array}{c|c} P_1' & 0 \\ \hline 0 & P_2' \end{array} \right],$$

where P_1' is a 4×4 matrix and P_2' is a $(2d-4)\times(2d-4)$ matrix. Since R_1 is similar to W,

$$W=\left[\begin{array}{c|c} W_1 & 0 \\ \hline W_3 & W_2 \end{array}\right],$$

where

$$W_3=\left[\begin{array}{c|c} 0 & 1 \\ \hline 0_{3\times(d-2)} & 0 \end{array}\right],$$

$$W_1=\begin{bmatrix} \alpha_1 & 0 & 0 & 0 \\ 0 & \alpha_1 & 0 & 0 \\ 0 & 0 & \lambda_1 & 0 \\ 0 & 0 & 1 & \lambda_1 \end{bmatrix},$$

$$W_2=\alpha_1 I_{d-2}\oplus\begin{bmatrix} \lambda_1 & & & & \\ 1 & \lambda_1 & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda_1 \end{bmatrix}_{(d-2)\times(d-2)}$$

Then

$$P_1W=\left[\begin{array}{c|c} P_1' & 0 \\ \hline 0 & P_2' \end{array}\right]\left[\begin{array}{c|c} W_1 & 0 \\ \hline W_3 & W_2 \end{array}\right]=\left[\begin{array}{c|c} P_1'W_1 & 0 \\ \hline P_2'W_3 & P_2'W_2 \end{array}\right],$$

and there exist an involution P_1' such that

$$\sigma(P_1'W_1)=\left\{\alpha_1,\alpha_1^{-1},\rho,-\rho^{-1}u_1^2\right\}$$

and an involution P_2' such that

$$\sigma(P_2'W_2)=\left\{-\rho\left(u_1^{-2},u_1^{-3},\ldots,u_1^{1-d}\right),-\rho^{-1}\left(u_1^3,u_1^4,\ldots,u_1^d\right)\right\}.$$

Hence $\sigma(P_1R_1)=\sigma(P_1W)=\{\alpha_1,\alpha_1^{-1},-\rho(-1,u_1^{-2},u_1^{-3},\ldots,u_1^{1-d}),$

$-\rho^{-1}(u_1^2, u_1^3, \ldots, u_1^d)\}$. By the same method as in Case (1), the proof is complete.

(3) *Assume that* $d < \omega_1$ *and* $\eta = (-1)^l \det A_3$, *where* $\eta = \pm 1$. We want to prove that there exists an involution P_1 with $\det P_1 = (-1)^d$ such that $\sigma(P_1R_1) = \{\eta, \rho, \eta\rho^{-1}\tau, \eta\rho\tau^{-1}(1, u_1^{-1}, u_1^{-2}, \ldots, u_1^{2-d}), \eta\rho^{-1}\tau(u_1, u_1^2, \ldots, u_1^{d-1}), \epsilon, \ldots, \epsilon\}$.

(i) If $d = 1$, then R_1 is cyclic and there exists an involution P_1 such that $\sigma(P_1R_1) = \{\eta, \rho, \eta\rho^{-1}b\}$, where $b = -\det R_1$.

(ii) $d \geqslant 2$. Let

$$P_1 = \left[\begin{array}{c|c} P_1' & 0 \\ \hline 0 & P_2' \end{array}\right],$$

where P_1' is a $(\omega_1 - d + 2)\times(\omega_1 - d + 2)$ matrix and P_2' is a $(2d-2)\times(2d-2)$ matrix. Since R_1 is similar to T,

$$T = \left[\begin{array}{c|c} T_1 & 0 \\ \hline T_3 & T_2 \end{array}\right],$$

where

$$T_3 = \left[\begin{array}{c|c} 0 & 1 \\ \hline 0_r & 0 \end{array}\right], \qquad r = (2d-3)\times(\omega_1 - d + 1),$$

$$T_2 = \alpha_1 I_{d-1} \oplus \begin{bmatrix} \lambda_1 & & & \\ 1 & \lambda_1 & & \\ & \ddots & \ddots & \\ & & 1 & \lambda_1 \end{bmatrix}_{(d-1)\times(d-1)},$$

and

$$T_1 = \begin{bmatrix} \alpha_1 & & & & & \\ 0 & \lambda_1 & & & & \\ & 1 & \lambda_1 & & & \\ & & 1 & \ddots & & \\ & & & \ddots & \ddots & \\ & & & & 1 & \lambda_1 \end{bmatrix}$$

is cyclic. Then

$$P_1T = \left[\begin{array}{c|c} P_1' & 0 \\ \hline 0 & P_2' \end{array}\right]\left[\begin{array}{c|c} T_1 & 0 \\ \hline T_3 & T_2 \end{array}\right] = \left[\begin{array}{c|c} P_1'T_1 & 0 \\ \hline P_2'T_3 & P_2'T_2 \end{array}\right],$$

and there exist an involution P_1' such that $\sigma(P_1'\mathrm{T}_1) = \{\eta, \rho, \eta\rho^{-1}\tau, \epsilon, \dots, \epsilon\}$, where $\tau = -\det T_1$ and $\epsilon = 1$ may be absent, and an involution P_2' from Lemma 2.3 such that

$$\sigma(P_2'T_2) = \left\{\eta\rho\tau^{-1}\left(1, u_1^{-1}, u_1^{-2}, \dots, u_1^{2-d}\right), \eta\rho^{-1}\tau\left(u_1, u_1^2, \dots, u_1^{d-1}\right)\right\}.$$

So $\sigma(P_1R_1) = \sigma(P_1T) = \{\eta, \rho, \eta\rho^{-1}\tau, \eta\rho\tau^{-1}(1, u_1^{-1}, u_1^{-2}, \dots, u_1^{2-d}), \epsilon, \dots, \epsilon, \eta\rho^{-1}\tau(u_1, u_1^2, \dots, u_1^{d-1})\}$ and $\det P_1 = (-1)^d$. As in the proof for case (1), we have A as the product of three involutions.

(4) *Assume that* $k_1 = 0$ *and* $(-1)^l \det A_3 = -1$. If $\omega_{s+1} \geqslant 3$, by the same method as in case (1), we take

$$\sigma(P_{s+1}V_{s+1}) = \left\{\theta_{s+1}, -\theta_{s+1}^{-1}v_{s+1}, -1, \epsilon, \dots, \epsilon\right\},$$

$$\sigma(P_jV_j) = \left\{-\theta_j, -\theta_j^{-1}v_j, \epsilon, \dots, \epsilon\right\}, \qquad s+2 \leqslant j \leqslant k,$$

$$\sigma(P_{k+i}E_i) = \left\{-\beta_i, -\beta_i^{-1}\varphi_i\right\}, \qquad 1 \leqslant i \leqslant h_2,$$

and complete the proof as before. Hence we may assume that $\omega_i = 2$ for $s+1 \leqslant i \leqslant k$. Again, we consider two cases:

(4-1) If $\varphi_i \neq \varphi_j$ for some $i \neq j$, say $\varphi_1 \neq \varphi_2$, then $E_1 \oplus E_2$ is similar to $E_1' \oplus \alpha_1$, where E_1' is cyclic. By Lemma 2.1, there exists an involution P_{k+1} such that

$$\sigma(P_{k+1}E_1') = \left\{\alpha_1^{-1}, \beta_1, -\beta_1^{-1}\varphi_1\varphi_2\right\}.$$

So $\sigma((P_{k+1} \oplus 1)(E_1 \oplus E_2)) = \{\alpha_1, \alpha_1^{-1}, \beta_1, -\beta_1^{-1}\varphi_1\varphi_2\}$. As in case (1), if we take $P_{k+2} = 1$ and $\sigma(P_{K+i}E_i) = \{-\beta_i, -\beta_i^{-1}\varphi_i\}$, $3 \leqslant i \leqslant h_2$, then the proof is complete.

(4-2) Assume that all the E_i's are absent or $\varphi_1 = \varphi_i$ for $i = 1, 2, \dots, h_2$. Since $(-1)^l \det A_3 = -1$, we have $u^{l-h_2}\varphi_1^{h_2} = -1$. For simplicity, we may assume that $u^{\eta_1}\varphi_1^{\eta_2} \neq 1$ for all positive integers $\eta_1 \leqslant q - h_2$ and $\eta_2 \leqslant h_2$. Let $\varphi = \varphi_1$. To choose in pairs c_i and d_i such that

$c_i d_i = u$ and $c_i \neq d_i$, $1 \leqslant i \leqslant l - h_2$, or in pairs c_j' and d_j' such that $c_j' d_j' = \varphi$ and $c_j' \neq d_j'$, $1 \leqslant j \leqslant h_2$, we now distinguish seven subcases.

⟨1⟩ If $h_2 = 0$, we take $G_1 = \{-1, -u\}$ and $G_2 = \{-u^{-1}, -u^2, \dots, -u^{1-l}, -u^l\}$.

⟨2⟩ If $h_2 = 1$ and $u^y \neq 1$ for $y = 1,3,5,\dots,2l-3$, we take $G_1 = \{1, \varphi\}$ and $G_2 = \{-1, -u, -u^{-1}, -u^2, \dots, -u^{2-l}, -u^{l-1}\}$.

⟨3⟩ If $h_2 = 1$ and there exists an integer y with $y = 2y_1 + 1$ and $l - h_2 < y < 2l - 2h_2 - 1$ such that $u^y = 1$, we take $G_1 = \{\alpha_1, -\alpha_1^{-1}\varphi\}$ and $G_2 = \{\alpha_1^{-1}, \alpha_1 u, \alpha_1^{-1}u^{-1}, \alpha_1 u^2, \dots, \alpha_1^{-1}u^{2-l}, \alpha_1 u^{l-1}\}$.

⟨4⟩ If $h_2 \geqslant 2$ and $\varphi^x \neq 1$ for $x = 1,3,5,\dots,2h_2 - 1$ and $u^y \neq 1$ for $y = 1,3,5,\dots,2l - 2h_2 - 1$, we take

$$G_1 = \{1, \varphi, \varphi^{-1}, \varphi^2, \dots, \varphi^{1-h_2}, \varphi^{h_2}\}$$

and

$$G_2 = \{-1, -u, -u^{-1}, -u^2, \dots, -u^{1-l+h_2}, -u^{l-h_2}\}.$$

⟨5⟩ If $h_2 \geqslant 2$ and $\varphi^x \neq 1$ for $x = 1,3,5,\dots,2h_2 - 1$ and there exists an integer y with $y = 2y_1 + 1$ and $l - h_2 < y \leqslant 2l - 2h_2 - 1$ such that $u^y = 1$, we take

$$G_1 = \{1, \varphi, \varphi^{-1}, \varphi^2, \dots, \varphi^{2-h_2}, \varphi^{h_2-1}\}$$

and

$$G_2 = \{-1, -u, -u^{-1}, -u^2, \dots, -u^{1-y_1}, -u^{y_1}, -u^{-y_1},$$
$$-u^{y_1}\varphi, -u^{-y_1}\varphi^{-1}, -u^{y_1+1}\varphi, \dots, -u^{1+h_2-l}\varphi^{-1}, -u^{l-h_2}\varphi\}.$$

⟨6⟩ If $h_2 \geqslant 2$ and there exists an integer x with $x = 2s_1 + 1$ and $h_2 < x \leqslant 2h_2 - 1$ such that $\varphi^x = 1$, and $u^y \neq 1$ for $y = 1,3,5,\dots,2l - 2h_2 - 1$, we take

$$G_1 = \{1, \varphi, \varphi^{-1}, \varphi^2, \dots, \varphi^{-s_1}, \varphi^{s_1}u, \varphi^{-s_1}u^{-1}, \varphi^{s_1+1}u,$$
$$\varphi^{-s_1-1}u^{-1}, \varphi^{s_1+2}u, \dots, \varphi^{1-h_2}u^{-1}, \varphi^{h_2}u\}$$

and

$$G_2 = \{ -1, -u, -u^{-1}, -u^2, \dots, -u^{h_2-l+2}, -u^{l-h_2-1} \}.$$

⟨7⟩ If $h_2 \geqslant 2$ and there exists an integer x with $x = 2s_1 + 1$ and $h_2 < x \leqslant 2h_2 - 1$ such that $\varphi^x = 1$, and there exists an integer y with $y = 2y_1 + 1$ and $l - h_2 < y \leqslant 2l - 2h_2 - 1$ such that $u^y = 1$, we take

$$G_1 = \{1, \varphi, \varphi^{-1}, \varphi^2, \dots, \varphi^{-s_1}, \varphi^{s_1}u, \varphi^{-s_1}u^{-1}, \varphi^{s_1+1}u,$$
$$\varphi^{-s_1-1}u^{-1}, \varphi^{s_1+2}u, \dots, \varphi^{2-h_2}u^{-1}, \varphi^{h_2-1}u \}$$

and

$$G_2 = \{ -1, -u, -u^{-1}, -u^{-2}, \dots, -u^{1-y_1}, -u^{y_1}, -u^{-y_1},$$
$$-u^{y_1}\varphi, -u^{-y_1}\varphi^{-1}, -u^{-y_1+1}\varphi, \dots, -u^{2+h_2-l}\varphi^{-1}, -u^{l-h_2-1}\varphi \}$$

By Lemmas 2.1 and 2.4, there exist $k + h_2$ involutions P_i such that

$$\left(\bigcup_{i=1}^{s} \sigma(P_iB_i) \right) \cup \left(\bigcup_{u=s+1}^{k} \sigma(P_iV_i) \right) \cup \left(\bigcup_{i=1}^{h_2} \sigma(P_iE_i) \right) = G_1 \cup G_2.$$

Let $P = P_1 \oplus P_2 \oplus \cdots \oplus P_{k+h_2}$. Then P is an involution and PA is similar to its inverse by Theorem 1.1 Hence A is the product of three involutions.

(5) *Assume that A is similar to A_4.* As in the proof for case (4-1), we may assume that $\omega_i = 2$ for $s + 1 \leqslant i \leqslant k$. Again, we consider two cases:

(5-1) Assume that each E_i is absent or $\varphi_1 = \varphi_i$ for $i = 1, 2, \dots, h_2$. As in the proof for case (4-2), we have A is the product of three involutions.

(5-2) If $h_2 \geqslant 2$ and $\varphi_i \neq \varphi_j$ for some $i \neq j$, say, $\varphi_1 \neq \varphi_2$, then

$$E_1 \oplus E_2 = \left[\begin{array}{c|c} \varphi_1 & 0 \\ \hline 0 & \varphi_2 \end{array} \right] \oplus \left[\begin{array}{c|c} \varphi_1 & 0 \\ \hline 0 & \varphi_3 \end{array} \right]$$

is similar to $E_2'\oplus\alpha_1$, where

$$E_2'=\begin{bmatrix}\varphi_1 & & \\ & \varphi_2 & \\ & & \varphi_3\end{bmatrix}.$$

Hence A_4 is similar to

$$A_4'=B_1\oplus B_2\oplus\cdots\oplus B_s\oplus V_{s+1}\oplus\cdots\oplus V_k\oplus E_2'\oplus E_3\oplus E_4\oplus\cdots\oplus E_{h_2}\oplus\alpha_1 I_2,$$

and A_4' is similar to

$$A_5=B_1'\oplus B_2'\oplus\cdots\oplus B_{t_1}'\oplus V_{t_1+1}\oplus\cdots\oplus V_k\oplus E_2'\oplus E_3\cdots\oplus E_{h_2},$$

where each B_i', $B_i'=V_i\oplus\alpha_1 I_{\delta(i)}$, $0<\delta(i)\leqslant\omega_i-2$, and $\delta(i)+\omega_i=2d_i$ for some integer $d_i\geqslant 2$, $1\leqslant i\leqslant t_1$. By the same method as in case (1), the proof is thus complete. ■

3. NECESSARY CONDITIONS

THEOREM 3.1. *Let A be an $n\times n$ complex matrix, $\beta^4\neq 1$, $\beta\neq 0$, $m=\dim\ker(A-\beta I)$, and $r=\dim\ker(A-\beta^{-3}I)$. If A is the product of three involutions, then $m\leqslant(2n+r)/3$ and $m\leqslant[3n/4]$.*

Proof. Let P_1 be an involution and $l=\dim\ker(P_1A-\beta I)+\dim\ker(P_1A+\beta I)$. Then $2m-n\leqslant l$. If $A=P_1P_2P_3$, where P_i's are involutions, then $P_1A=P_2P_3$. Since P_1A is similar to its own inverse, we have

$$P_1A=SDS^{-1}, \tag{1}$$

where D is in Jordan canonical form and D is similar to D^{-1}.

By (1), we obtain

$$P_1A-\beta^{-2}A^{-1}P_1=SD^{-1}S^{-1}. \tag{2}$$

Multiplying (2) by β^{-2} and subtracting it from (1), we get

$$A^{-1}P_1=S(D-\beta^{-2}D^{-1})S^{-1}.$$

For simplicity, we will assume that D is of the form

$$\left[\begin{array}{cc|c|c} \alpha & 0 & \multirow{2}{*}{0} & \multirow{2}{*}{0} \\ 0 & 1/\alpha & & \\ \hline \multicolumn{2}{c|}{0} & V & 0 \\ \hline \multicolumn{2}{c|}{0} & 0 & V_1 \end{array}\right], \tag{3}$$

where

$$V=\begin{bmatrix} t & 0 & 0 \\ 1 & t & 0 \\ 0 & 1 & t \end{bmatrix} \quad \text{and} \quad V_1=\begin{bmatrix} t^{-1} & 0 & 0 \\ 1 & t^{-1} & 0 \\ 0 & 1 & t^{-1} \end{bmatrix}.$$

Then

$$D^{-1}=\left[\begin{array}{cc|c|c} \alpha^{-1} & 0 & \multirow{2}{*}{0} & \multirow{2}{*}{0} \\ 0 & \alpha & & \\ \hline \multicolumn{2}{c|}{0} & V^{-1} & 0 \\ \hline \multicolumn{2}{c|}{0} & 0 & V_1^{-1} \end{array}\right], \tag{4}$$

where

$$V^{-1}=\begin{bmatrix} t^{-1} & 0 & 0 \\ -t^{-2} & t^{-1} & 0 \\ t^{-3} & -t^{-2} & t^{-1} \end{bmatrix} \quad \text{and} \quad V_1^{-1}=\begin{bmatrix} t & 0 & 0 \\ -t^2 & t & 0 \\ t^3 & -t^2 & t \end{bmatrix}.$$

It follows from (3) and (4) that

$$D-\beta^{-2}D^{-1}=\left[\begin{array}{cc|c|c} \lambda_1 & 0 & & \multirow{2}{*}{0} \\ 0 & \lambda_2 & & \\ \hline \multicolumn{2}{c|}{0} & E & 0 \\ \hline \multicolumn{2}{c|}{0} & 0 & F \end{array}\right],$$

where

$$E=\begin{bmatrix} \eta_1 & 0 & 0 \\ \epsilon & \eta_1 & 0 \\ -\beta^{-2}t^{-3} & \epsilon & \eta_1 \end{bmatrix}, \qquad F=\begin{bmatrix} \eta_2 & 0 & 0 \\ \zeta & \eta_2 & 0 \\ -\beta^{-2}t^3 & \zeta & \eta_2 \end{bmatrix},$$

$\lambda_1 = \alpha - \beta^{-2}\alpha^{-1}$, $\lambda_2 = \alpha^{-1} - \beta^{-2}\alpha$, $\eta_1 = t - \beta^{-2}t^{-1}$, $\eta_2 = t^{-1} - \beta^{-2}t$, $\epsilon = \beta^{-2}t^{-2} + 1$, and $\zeta = \beta^{-2}t^2 + 1$.

Since $\lambda_1 = 0$ if and only if $\alpha^2 = \beta^{-2}$, $\lambda_2 = 0$ if and only if $\alpha^2 = \beta^2$, $\eta_1 = 0$ if and only if $t^2 = \beta^{-2}$, and $\eta_2 = 0$ if and only if $t^2 = \beta^2$, we have

$$\operatorname{rank}(D - \beta^{-2}D^{-1}) = \operatorname{rank}(P_1A - \beta^{-2}A^{-1}P_1) = n - l.$$

Since $P_1A - \beta^{-2}A^{-1}P_1 = P_1(A - \beta^{-3}I) + \beta^{-3}(A - \beta I)A^{-1}P_1$, we have $\operatorname{rank}(P_1(A - \beta^{-3}I)) \leqslant \operatorname{rank}(P_1A - \beta^{-2}A^{-1}P_1) + \operatorname{rank}(\beta^{-3}(A - \beta I)A^{-1}P_1)$. By $n - l \leqslant 2n - 2m$, $\operatorname{rank}(\beta^{-3}(A - \beta I)A^{-1}P_1) = n - m$, and $\operatorname{rank}(P_1(A - \beta^{-3}I)) = n - r$, we obtain

$$n - r \leqslant n - m + 2n - 2m,$$

i.e., $m \leqslant (2n + r)/3$ and $m \leqslant [3n/4]$. ■

For 5×5 matrices, we have the following characterization:

THEOREM 3.2. *Let A be a 5×5 complex matrix. Then $A \in T(5)^3$ if and only if one of the following holds:*

(1) $\det A = -1$ *and, for any* $\beta^4 \neq 1$, $\dim\ker(A - \beta I_5) \leqslant 3$ *and A is not similar to* $B = \beta I_3 \oplus I_2$;

(2) $\det A = 1$ *and, for any* $\beta^4 \neq 1$, $\dim\ker(A - \beta I_5) \leqslant 3$ *and A is not similar to* $\beta I_3 \oplus (-I_2)$.

Proof. Since $A \in T(5)^3$ if and only if $-A \in T(5)^3$, we need only prove (1).

$\Leftarrow$: In view of Theorem 2.5, we only need to show this for the case $m = 3$. Here A is either similar to $A_1 = D_1 \oplus \beta \oplus \beta$ or $A_2 = C_1 \oplus C_2 \oplus \beta$, where D_1 is cyclic, $C_1 = C_2$, and C_1 is either

$$\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} \beta & 0 \\ 1 & \beta \end{bmatrix}.$$

Let $a = \det C_1$. If $\beta^2 a = -1$, then $\beta = 1$ or $\alpha = 1$ from $\det A = -1$, which contradicts that $\beta^4 \neq 1$ and A is similar to B. So $\beta^2 a \neq -1$. By Lemma 2.1, there exist three involutions P_i such that $\sigma(P_1D_1) = \{\beta^{-1}, -\beta^{-1}, -1\}$, $\sigma(P_2C_1) = \{\beta^{-1}, -a\beta\}$, and $\sigma(P_3C_2) = \{-1, a\}$. Let $V = P_1 \oplus 1 \oplus -1$ and $V_2 = P_2 \oplus P_3 \oplus 1$. Then $V_1A_1 = P_1C_1 \oplus \beta \oplus -\beta$, $\sigma(V_1A_1) = \{\beta, \beta^{-1}, -\beta, -\beta^{-1}, -1\}$, $V_2A_2 = P_2C_1 \oplus P_3C_2 \oplus \beta$, and $\sigma(V_2A_2) = \{-1, a, -a\beta, \beta, \beta^{-1}\}$.

Therefore V_1A_1 is similar to its inverse, and so is V_2A_2. That is, $A_1 \in T(5)^3$ and $A_2 \in T(5)^3$. Hence $A \in T(5)^3$.

$\Rightarrow$: By Theorem 3.1, we obtain $m \leqslant 3$. It remains to prove that $B \notin T(5)^3$. If $B = \beta I_3 \oplus I_2 \in T(5)^3$, say $B = P_1P_2P_3$, where the P_i's are involutions, then, assuming

$$P_1 = \begin{bmatrix} C & D \\ E & F \end{bmatrix}$$

with C and F of sizes 2 and 3, respectively,

$$P_1B = \begin{bmatrix} C & D \\ E & F \end{bmatrix}\begin{bmatrix} \beta I_3 & 0 \\ 0 & I_2 \end{bmatrix} = \begin{bmatrix} \beta C & D \\ \beta E & F \end{bmatrix}$$

is similar to

$$B^{-1}P_1 = \begin{bmatrix} \beta^{-1} I_3 & 0 \\ 0 & I_2 \end{bmatrix}\begin{bmatrix} C & D \\ E & F \end{bmatrix} = \begin{bmatrix} \beta^{-1} C & \beta^{-1} D \\ E & F \end{bmatrix}.$$

Since

$$(P_1B)^2 = \begin{bmatrix} \beta^2C^2 + \beta DE & \beta CD + DF \\ \beta^2 EC + \beta FE & \beta ED + F^2 \end{bmatrix},$$

$$(B^{-1}P_1)^2 = \begin{bmatrix} \beta^{-2}C^2 + \beta^{-1}DE & \beta^{-2}CD + \beta^{-1}DF \\ \beta^{-1}C + FE & \beta^{-1}ED + F^2 \end{bmatrix},$$

$\operatorname{tr}(P_1B) = \operatorname{tr}(B^{-1}P_1)$, $\beta^3 = -1$, and $\operatorname{tr}(P_1B)^2 = \operatorname{tr}(B^{-1}P_1)^2$, we have

$$\operatorname{tr} C = 0 \tag{1}$$

and

$$\operatorname{tr} C^2 + 2 \operatorname{tr} DE = 0. \tag{2}$$

Since

$$P_1^2 = \begin{bmatrix} C^2 + DE & CD + DF \\ ED + FE & ED + F^2 \end{bmatrix} = \begin{bmatrix} I_3 & 0 \\ 0 & I_2 \end{bmatrix},$$

we have

$$C^2 + DE = I_3, \qquad ED + F^2 = I_2, \qquad CD + DF = 0, \qquad EC + FE = 0. \tag{3}$$

From (3), we obtain

$$\operatorname{tr} C^2 + \operatorname{tr} DE = 3 \quad \text{and} \quad \operatorname{tr} DE + \operatorname{tr} F^2 = 2. \tag{4}$$

By (2) and (4), we get

$$\operatorname{tr} DE = -3, \qquad \operatorname{tr} F^2 = 5, \quad \text{and} \quad \operatorname{tr} C^2 = 6. \tag{5}$$

Since $\operatorname{tr} C = 0$, $\operatorname{tr} C^2 = 6$, $DE = I_3 - C^2$, and rank $DE \leqslant 2$, we have either $\sigma(C) = \{1, 1, -2\}$ or $\sigma(C) = \{-1, -1, 2\}$. So rank $DE = 1$ which implies that

$$\operatorname{rank} D = 1 \quad \text{or} \quad \operatorname{rank} E = 1. \tag{$*$}$$

As in the proof of Theorem 3.1, we have

$$\operatorname{rank}\left(P_1 B - \beta^{-2} B^{-1} P_1\right) = \operatorname{rank}\left(P_1 B - \beta^2 B^{-1} P_1\right). \tag{6}$$

From ($*$) and

$$P_1 B - \beta^2 B^{-1} P_1 = \begin{bmatrix} 0 & (1-\beta)D \\ (\beta - \beta^2)E & (1-\beta^2)F \end{bmatrix},$$

we obtain

$$\operatorname{rank}\left(P_1 B - \beta^2 B^{-1} P_1\right) \leqslant 3. \tag{7}$$

$$\begin{aligned} P_1 B - \beta^{-2} B^{-1} P_1 &= \begin{bmatrix} (1+\beta)C & 2D \\ 2\beta E & (1+\beta)F \end{bmatrix} \\ &= \begin{bmatrix} (1+\beta)C & 0 \\ 2\beta E & I_2 \end{bmatrix} \\ &\quad \times \begin{bmatrix} I_3 & 2(1+\beta)^{-1} C^{-1} D \\ 0 & (1+\beta)F - 4\beta(1+\beta)^{-1} E C^{-1} D \end{bmatrix}, \end{aligned} \tag{8}$$

so

$$\operatorname{rank}\left(P_1 B - \beta^{-2} B^{-1} P_1\right) \geqslant 3. \tag{9}$$

From (6), (7), (8), and (9), we get

$$(1+\beta)F - 4\beta(1+\beta)^{-1} E C^{-1} D = 0_2. \tag{10}$$

Multiplying (10) by $(1+\beta)F$ and comparing with (3), we obtain

$$(1+\beta)^2 F^2 + 4\beta E D = 0_2,$$

which contradicts (5). Hence $B \notin T(5)^3$. ■

REFERENCES

1 C. S. Ballantine, Some involutory similarities, *Linear and Multilinear Algebra* 3:19–23 (1975).
2 C. S. Ballantine, Author's addendum to Some involutory similarities, *Linear and Multilinear Algebra* 4:69 (1976).
3 C. S. Ballantine, Products of involutory matrices I, *Linear and Multilinear Algebra* 5:53–62 (1977).
4 J. Barria and P. R. Halmos, Weakly transitive matrices, *Illinois J. Math.* 28:370–378 (1984).
5 D. Ž. Djokovic, Products of two involutions, *Arch. Math.* (*Basel*) 18:582–584 (1967).
6 W. H. Gustafson, P. R. Halmos, and H. Radjavi, Products of involutions, *Linear Algebra Appl.* 13:157–162 (1976).
7 F. Hoffman and E. C. Paige, Products of two involutions in the general linear group, *Indiana Univ. Math. J.* 20:1017–1020 (1971).
8 A. R. Sourour, A factorization theorem for matrices, *Linear and Multilinear Algebra* 19:141–147 (1986).
9 M. J. Wonenburger, Transformations which are products of two involutions, *J. Math. Mech.* 16:327–338 (1966).

Received 8 July 1987; final manuscript accepted 4 December 1987