Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

PRODUCTS OF SKEW-INVOLUTIONS*

JESUS PAOLO E. JOVEN† AND AGNES T. PARAS†

Abstract. It is shown that every $2n$-by-$2n$ matrix over a field $\mathbb{F}$ with determinant 1 is a product of (i) four or fewer skew-involutions ($A^2 = -I$) provided $\mathbb{F} \neq \mathbb{Z}_3$, and (ii) eight or fewer skew-involutions if $\mathbb{F} = \mathbb{Z}_3$ and $n > 1$. Every real symplectic matrix is a product of six real symplectic skew-involutions, and an explicit factorization of a complex symplectic matrix into two symplectic skew-involutions is given.

Key words. Involution, Skew-involution, Symplectic matrix, Binomial coefficients, Toeplitz matrix, Persymmetric matrix.

AMS subject classifications. 15A23, 15B05, 15B10, 05A10.

1. Introduction. Let $M_n(\mathbb{F})$ be the set of all n-by-n matrices with entries in a field $\mathbb{F}$, $SL_n(\mathbb{F})$ be the set of all matrices in $M_n(\mathbb{F})$ with determinant 1, and $\operatorname{char}\mathbb{F}$ denote the characteristic of $\mathbb{F}$. Suppose $A \in M_n(\mathbb{F})$. We say that A is an *involution* if $A^2 = I_n$, while A is called a *skew-involution* if $A^2 = -I_n$. Denote by Ω_{2n} the skew-involution given by:

$$\Omega_{2n} = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix} \in M_{2n}(\mathbb{F}).$$

We say $B \in M_{2n}(\mathbb{F})$ is *symplectic* if $B^\top \Omega_{2n} B = \Omega_{2n}$, and B is *skew-symplectic* if $B^\top \Omega_{2n} B = -\Omega_{2n}$.

In 1976, Gustafson *et al.* proved that every matrix in $M_n(\mathbb{F})$ with determinant ± 1 is a product of at most four involutions [9]. In 1966, Wonenburger proved that every symplectic matrix over $\mathbb{F}$ is a product of two skew-symplectic involutions provided $\operatorname{char}\mathbb{F} \neq 2$ [13]. In 1981, Gow proved that if $\operatorname{char}\mathbb{F} = 2$, then every symplectic matrix over $\mathbb{F}$ is a product of two symplectic involutions [8]. In 2020, Ellers and Villa showed that every symplectic matrix over $\mathbb{F}$ of size at least 4 is a product of 6 or fewer symplectic involutions provided -1 is a square in $\mathbb{F}$ [6].

Suppose $p(x) = x^2 + 1$ has a root $a \in \mathbb{F}$. Then, P is an involution if and only if $\pm aP$ is a skew-involution. If $A \in M_n(\mathbb{F})$ has determinant ± 1, then $A = E_1E_2E_3E_4$, where each $E_i \in M_n(\mathbb{F})$ is an involution [9]. Since $\pm aE_i$ is a skew-involution for each i, we can write $A = (aE_1)(-aE_2)(aE_3)(-aE_4)$ as a product of four skew-involutions. If $\operatorname{char}\mathbb{F} = 2$, then an involution is a skew-involution, and every symplectic over $\mathbb{F}$ is a product of two symplectic skew-involutions. If $\operatorname{char}\mathbb{F} \neq 2$ and $B \in M_{2n}(\mathbb{F})$ is symplectic, then $B = S_1S_2$ where each S_j is a skew-symplectic involution [13]. Since S is a skew-symplectic involution if and only if $\pm aS$ is a symplectic skew-involution, we can write $B = (aS_1)(-aS_2)$ as a product of two symplectic skew-involutions.

Suppose $p(x) = x^2 + 1$ has no root in $\mathbb{F}$. If $P \in M_n(\mathbb{F})$ is a skew-involution, then the minimal polynomial of P is $p(x)$, which is irreducible in $\mathbb{F}[x]$. By the rational canonical form theorem, P is similar to

*Received by the editors on January 29, 2023. Accepted for publication on March 14, 2023. Handling Editor: João Filipe Queiró. Corresponding Author: Agnes T. Paras.

†Institute of Mathematics, College of Science, University of the Philippines, Diliman, Quezon City 1101, Philippines (jpjoven@math.upd.edu.ph, agnes@math.upd.edu.ph).

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

$$\bigoplus_k C(x^2+1) = \bigoplus_k \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Hence, $n = 2k$, $\det P = 1$, and $Q \in M_n(\mathbb{F})$ is a skew-involution if and only if Q similar to P. Thus, if A is a product of skew-involutions, then $A \in SL_{2k}(\mathbb{F})$ when $p(x)$ has no root in $\mathbb{F}$.

In this paper, we consider products of skew-involutions in $SL_{2n}(\mathbb{F})$. In Section 2, we include some elementary properties of skew-involutions. In Section 3, we show that every $A \in SL_{2n}(\mathbb{F})$ is a product of skew-involutions if and only if $\mathbb{F} \neq \mathbb{Z}_3$ or $n > 1$. We prove in Section 4 that every real symplectic matrix is a product of six or fewer real symplectic skew-involutions. We provide an explicit factorization of a complex symplectic matrix into two symplectic skew-involutions in Section 5.

2. Preliminaries. Our notation is standard as in [10]. We denote a diagonal matrix of size n with (i,i)-entry d_i by $\operatorname{diag}(d_1, d_2, \ldots, d_n)$, and the n-by-n Jordan block corresponding to $\lambda \in \mathbb{F}$ by $J_n(\lambda)$. Let $\mathrm{Sp}_{2n}(\mathbb{F})$ denote the group of symplectic matrices in $M_{2n}(\mathbb{F})$. The following proposition gives a description of the blocks of a symplectic matrix when it is partitioned conformal to Ω_{2n}.

PROPOSITION 2.1. *Let*

$$A = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix},$$

such that each $A_i \in M_n(\mathbb{F})$. *Then,* $A \in \mathrm{Sp}_{2n}(\mathbb{F})$ *if and only if both* $A_1 A_2^\top$ *and* $A_3 A_4^\top$ *are symmetric, and* $A_1 A_4^\top - A_2 A_3^\top = I$. *If* $n = 1$, *then* $A \in \mathrm{Sp}_2(\mathbb{F})$ *if and only if* $A \in SL_2(\mathbb{F})$.

Let $A \in M_n(\mathbb{F})$ be nonsingular. By Proposition 2.1, the following matrices are symplectic:

$$A \oplus A^{-\top} \text{ and } \begin{bmatrix} 0 & -A^{-\top} \\ A & 0 \end{bmatrix}.$$

Observe that

$$A \oplus A^{-1} = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix} \begin{bmatrix} 0 & -A^{-1} \\ A & 0 \end{bmatrix} = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix} \begin{bmatrix} 0 & A^{-1} \\ A & 0 \end{bmatrix}$$

is a product of two skew-involutions and a product of two involutions. If, in addition, A is symmetric, then $A \oplus A^{-1}$ is a product of two symplectic skew-involutions. This proves the following.

LEMMA 2.2. *If* $A \in M_n(\mathbb{F})$ *is nonsingular, then* $A \oplus A^{-1}$ *is*

(a) *a product of two involutions,*
(b) *a product of two skew-involutions, and*
(c) *a product of two symplectic skew-involutions, when* A *is symmetric.*

Let $A = [A_{ij}] \in M_{2k}(\mathbb{F})$ and $B = [B_{ij}] \in M_{2m}(\mathbb{F})$, where $A_{ij} \in M_k(\mathbb{F})$ and $B_{ij} \in M_m(\mathbb{F})$ for $i, j \in \{1, 2\}$. We define the *expanding sum* of A and B by:

$$A \boxplus B := \begin{bmatrix} A_{11} \oplus B_{11} & A_{12} \oplus B_{12} \\ A_{21} \oplus B_{21} & A_{22} \oplus B_{22} \end{bmatrix} \in M_{2k+2m}(\mathbb{F}).$$

Observe that $A \boxplus B$ is permutation similar to $A \oplus B$. Moreover, $A \boxplus B$ is symplectic if and only if both A and B are symplectic. The preceding statement also holds if 'symplectic' is replaced with 'involution' or 'skew-involution'. In addition, if $C \in M_{2k}(\mathbb{F})$ and $D \in M_{2m}(\mathbb{F})$, then $(A \boxplus B)(C \boxplus D) = AC \boxplus BD$. The preceding discussion gives us the following.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

Proposition 2.3. *Let $P \in M_{2k}(\mathbb{F})$ and $Q \in M_{2m}(\mathbb{F})$ be (symplectic) skew-involutions. Then $P \oplus Q$ is a skew-involution, and P^{-1}, $P^\top$, $-P$, and $P \boxplus Q$ are (symplectic) skew-involutions. If $R \in M_{2k}(\mathbb{F})$ is (symplectic) nonsingular, then RPR^{-1} is also a (symplectic) skew-involution.*

Let $C \in SL_{2k}(\mathbb{F})$ and $D \in SL_{2l}(\mathbb{F})$ be products of m symplectic skew-involutions, say $C = C_1 \cdots C_m$ and $D = D_1 \cdots D_m$. Then,

$$C \boxplus D = (C_1 \boxplus D_1) \cdots (C_m \boxplus D_m)$$

is a product of m symplectic skew-involutions. This gives us the following.

Proposition 2.4. *Let $C \in SL_{2k}(\mathbb{F})$ and $D \in SL_{2l}(\mathbb{F})$ be products of m (symplectic) skew-involutions for some positive integer m. Then, $C \oplus D$ is a product of m skew-involutions, and $C \boxplus D$ is a product of m (symplectic) skew-involutions.*

Let $A \in SL_{2n}(\mathbb{F})$ be an involution. If $\operatorname{char} \mathbb{F} \neq 2$, then A is similar to $I_{2k} \oplus -I_{2n-2k}$ for some nonnegative integer k. Since we can write I_{2m} as a product of two skew-involutions for any positive integer m, we have the following by Propositions 2.3 and 2.4.

Proposition 2.5. *If $\operatorname{char} \mathbb{F} \neq 2$, then every involution $A \in SL_{2n}(\mathbb{F})$ is a product of two skew-involutions. If $\operatorname{char} \mathbb{F} = 2$, then every involution is a skew-involution.*

3. Products of skew-involutions in $SL_{2n}(\mathbb{F})$.

Let $A \in SL_{2n}(\mathbb{F})$. We divide our discussion into three cases: (i) $|\mathbb{F}| \geq 4$, (ii) $n = 1$ and $\mathbb{F} = \mathbb{Z}_3$, and (iii) $n > 1$ and $\mathbb{F} = \mathbb{Z}_3$.

3.1. Case when $|\mathbb{F}| \geq 4$.

A lower triangular matrix is called *special* if all entries in its first subdiagonal are nonzero. An upper triangular matrix is *special* if its transpose is special lower triangular. If we can write a matrix A as a product of a special lower triangular L and a special upper triangular U, we call $A = LU$ a *special LU factorization* of A. The following result by Botha [2, Theorem 1] provides a characterization of a nonsingular matrix similar to one with a special LU factorization.

Theorem 3.1. *Let $A \in M_n(\mathbb{F})$ denote a nonsingular, nonscalar matrix over a field $\mathbb{F}$ with at least four elements, and let $\beta_1, \ldots, \beta_n$, $\gamma_1, \ldots, \gamma_n$ denote nonzero elements in $\mathbb{F}$ (repeats among the β's or γ's are labeled consecutively) such that $\det A = \Pi_{i=1}^n \beta_i \gamma_i$. Then there exists a matrix similar to A with a special LU factorization such that the ith diagonal entry of L and U are β_i and γ_i, respectively, if and only if $\operatorname{rank}(A - \beta_i \gamma_i I_n) > 1$ for each i.*

We make use of the above theorem to prove the following.

Theorem 3.2. *If $\mathbb{F}$ is a field with at least four elements, then every $A \in SL_{2n}(\mathbb{F})$ is a product of four skew-involutions.*

Proof. Let $\mathbb{F}$ be a field with at least four elements. If $A \in SL_2(\mathbb{F})$, then there exists nonzero $d \in \mathbb{F}$ such that $d \neq d^{-1}$. By Theorem 3.1, there exist $B, C \in M_2(\mathbb{F})$, both having eigenvalues d and d^{-1}, such that $A = BC$. Since $d \neq d^{-1}$, B and C are similar to $\operatorname{diag}(d, d^{-1})$. It follows from Lemma 2.2 and Proposition 2.3 that B and C are products of two skew-involutions. Thus, A is a product of four skew-involutions.

Let $n > 1$ and $A \in SL_{2n}(\mathbb{F})$. If A is nonscalar, then $\operatorname{rank}(A - I_{2n}) \geq 1$. If $\operatorname{rank}(A - I_{2n}) = 1$, then there exist $2n - 1$ Jordan blocks corresponding to 1 in the Jordan canonical form of A. Since $\det A = 1$, the

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

eigenvalue 1 has algebraic multiplicity $2n$. Thus, A is similar to $J_2(1) \oplus I_{2n-2}$. Observe that we can write

$$J_2(1) \oplus I_{2n-2} = \left(\begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix} \oplus [-1] \oplus I_{2n-3} \right) \left(\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \oplus [-1] \oplus I_{2n-3} \right).$$

Since both factors are involutions in $SL_{2n}(\mathbb{F})$, it follows from Propositions 2.5 and 2.3 that A is product of four skew-involutions.

Suppose $\operatorname{rank}(A - I_{2n}) > 1$. If $\mathbb{F}$ has at least four elements, there exists nonzero $c \in \mathbb{F}$ such that $c \neq c^{-1}$. Since $\operatorname{rank}\left(A - cc^{-1}I_{2n}\right) = \operatorname{rank}(A - I_{2n}) > 1$, we may take $\beta_i = \gamma_{i+n} = c$ and $\beta_{i+n} = \gamma_i = c^{-1}$ for $i = 1, 2, \ldots, n$ and apply Theorem 3.1 to conclude that A is similar to a matrix with special LU factorization:

$$\begin{bmatrix} c & & & & & & & \\ * & c & & & & & & \\ & \ddots & \ddots & & & & & \\ & & * & c & & & & \\ & & & * & c^{-1} & & & \\ & & & & * & c^{-1} & & \\ & & & & & \ddots & \ddots & \\ & & & & & & * & c^{-1} \end{bmatrix} \begin{bmatrix} c^{-1} & * & & & & & & \\ & c^{-1} & \ddots & & & & & \\ & & \ddots & * & & & & \\ & & & c^{-1} & * & & & \\ & & & & c & * & & \\ & & & & & c & \ddots & \\ & & & & & & \ddots & * \\ & & & & & & & c \end{bmatrix}.$$

Since both factors are special and $c \neq c^{-1}$, each factor is similar to $J_n(c) \oplus J_n(c)^{-1}$ which, by Lemma 2.2, is a product of two skew-involutions. It follows from Proposition 2.3 that A is a product of four skew-involutions.

Suppose $\alpha \in \mathbb{F}$ such that $A = \alpha I_{2n}$ and $\alpha^{2n} = 1$. As in the proof of [2, Theorem 6], we may write $A = BC$ where

$$B = \operatorname{diag}\left(\alpha^2, \alpha^4, \ldots, \alpha^{4n-2}, \alpha^{4n}\right) \text{ and } C = \operatorname{diag}\left(\alpha^{4n-1}, \alpha^{4n-3}, \ldots, \alpha^3, \alpha\right).$$

By applying permutation matrices to B and C, we obtain

$$B' = \left(\bigoplus_{i=1}^{n-1} \begin{bmatrix} \alpha^{2i} & 0 \\ 0 & \alpha^{4n-2i} \end{bmatrix} \right) \oplus \begin{bmatrix} \alpha^{2n} & 0 \\ 0 & \alpha^{4n} \end{bmatrix},$$

and

$$C' = \left(\bigoplus_{i=1}^{n-1} \begin{bmatrix} \alpha^{4n-(2i-1)} & 0 \\ 0 & \alpha^{2i-1} \end{bmatrix} \right) \oplus \begin{bmatrix} \alpha^{2n+1} & 0 \\ 0 & \alpha^{2n-1} \end{bmatrix},$$

which are similar to B and C, respectively. Except for the last summand of B' which is I_2, each direct summand of B' and C' is of the form $\operatorname{diag}\left(\alpha^i, \alpha^{-i}\right)$ since $\alpha^{2n} = 1$. By Lemma 2.2, each direct summand of B' and C' is a product of two skew-involutions. By Propositions 2.3, 2.4, and 2.5, it follows that A is a product of four skew-involutions. ∎

3.2. Case when $n = 1$ and $\mathbb{F} = \mathbb{Z}_3$. Observe that $A \in SL_2(\mathbb{F})$ is a skew-involution if and only if

$$A = \begin{bmatrix} a & b \\ c & -a \end{bmatrix}, \text{ where } a^2 + bc = -1, \text{ with } b, c \neq 0.$$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

If $\mathbb{F} = \mathbb{Z}_3$, then, by first setting all possible values of $a \in \mathbb{Z}_3$ in the above equation, we obtain that A is a skew-involution if and only if A is one of the following matrices or their additive inverses:

$$\hat{\imath} := \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \hat{\jmath} := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \hat{k} := \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}. \tag{3.1}$$

It can be verified that (a) $\hat{\imath}\hat{\jmath} = \hat{k} = -\hat{\jmath}\hat{\imath}$, (b) $\hat{\jmath}\hat{k} = \hat{\imath} = -\hat{k}\hat{\jmath}$, and (c) $\hat{k}\hat{\imath} = \hat{\jmath} = -\hat{\imath}\hat{k}$. Thus, $A \in SL_2(\mathbb{Z}_3)$ is a product of skew-involutions if and only if A belongs to the set $\mathcal{Q} := \left\{I_2, \hat{\imath}, \hat{\jmath}, \hat{k}, -I_2, -\hat{\imath}, -\hat{\jmath}, -\hat{k}\right\}$. Since $J_2(1) \in SL_2(\mathbb{Z}_3)$ is not in $\mathcal{Q}$, not every $A \in SL_2(\mathbb{Z}_3)$ can be written as a product of skew-involutions.

Proposition 3.3. *The group generated by the set of all skew-involutions in $M_2(\mathbb{Z}_3)$ is isomorphic to the quaternion group Q_8.*

3.3. Case when $n > 1$ and $\mathbb{F} = \mathbb{Z}_3$. Suppose $n > 1$ and let $A \in SL_{2n}(\mathbb{F})$ be a direct sum of Jordan blocks with eigenvalue 1. Since A is similar to A^{-1}, it is known that A is a product of two involutions [5, Theorem 1]. However, the determinant of an involution is ± 1. We show that A can be written as a product of two involutions in $SL_{2n}(\mathbb{F})$; hence, A is a product of four skew-involutions by Proposition 2.5. Instead of considering $J_k(1)$ for some positive integer k, we look at the similar companion matrix $C\left((x-1)^k\right)$. If we write $(x-1)^k = \sum_{i=0}^{k} c_i x^i$, then $C\left((x-1)^k\right) = G_k B_k$ where

$$G_k := \begin{bmatrix} -c_0 & 0 & \cdots & 0 \\ -c_1 & 0 & \cdots & 1 \\ \vdots & \vdots & ⋰ & \vdots \\ -c_{k-1} & 1 & \cdots & 0 \end{bmatrix} \quad \text{and} \quad B_k := \begin{bmatrix} & & & 1 \\ & & ⋰ & \\ & 1 & & \\ 1 & & & \end{bmatrix}. \tag{3.2}$$

Observe that when k is even, we have $c_0 = 1$ and $c_i = c_{k-i}$ for each i. Otherwise, we have $c_0 = -1$ and $c_i = -c_{k-i}$ for each i. Thus, G_k and B_k are involutions for each positive integer k.

Suppose k is even. If $k = 4m-2$ for some positive integer m, then both G_k and B_k have determinant -1. If $k = 4m$, then G_k and B_k are in $SL_k(\mathbb{F})$.

Suppose k is odd. Since $C\left((x-1)^k\right) = G_k B_k = (-G_k)(-B_k)$, we can write $C\left((x-1)^k\right)$ as a product of two involutions with determinant -1, or as a product of two involutions in $SL_k(\mathbb{F})$. This gives us the following.

Lemma 3.4. *Let k be a positive integer. If $k \not\equiv 2 \bmod 4$, then $J_k(1)$ is a product of two involutions in $SL_k(\mathbb{F})$. If $k \equiv 2 \bmod 4$ or k is odd, then $J_k(1)$ is a product of two involutions with determinant -1.*

We use Lemma 3.4 to prove the following.

Lemma 3.5. *Let $\epsilon \in \{1, -1\}$ and $A \in M_{4n}(\mathbb{F})$ have Jordan form J consisting of Jordan blocks corresponding to ϵ. Then, A is a product of four skew-involutions.*

Proof. It is enough to consider the case $\epsilon = 1$, since $J_k(-1)$ is similar to $-J_k(1)$. Without loss of generality, we may write

$$J = \left(\bigoplus_{i=1}^{\alpha} J_{4r_i}(1)\right) \oplus \left(\bigoplus_{j=1}^{\beta} J_{4s_j-2}(1)\right) \oplus \left(\bigoplus_{k=1}^{2\gamma} J_{2t_k-1}(1)\right), \tag{3.3}$$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

for some nonnegative integers α,β,γ. By Lemma 3.4, we can express $J_p(1)$ as a product of two involutions in $SL_p(\mathbb{F})$ when $p \not\equiv 2 \bmod 4$, and as a product of two involutions with determinant -1 when $p \equiv 2 \bmod 4$. If β is even, then J is a product of two involutions in $SL_{4n}(\mathbb{F})$. Suppose β is odd. Since J is of size $4n$, we have $\gamma > 0$. We can write $J_{2t_1-1}(1)$ as a product of two involutions with determinant -1 and the remaining odd-sized blocks as a product of two involutions with determinant 1. Hence, J is a product of two involutions in $SL_{4n}(\mathbb{F})$ when β is odd. By Propositions 2.5 and 2.3, A is a product of four skew-involutions. ◻

Suppose $A \in M_6(\mathbb{Z}_3)$ has Jordan form J consisting of Jordan blocks with eigenvalue 1. Then, J has the form given by equation (3.3) for some nonnegative integers α,β,γ. As in the proof of Lemma 3.5, we have that J is a product of four skew-involutions if β is even, or if β is odd and $\gamma > 0$. If β is odd and $\gamma = 0$, then J is $J_6(1)$, $J_4(1) \oplus J_2(1)$, or $J_2(1) \oplus J_2(1) \oplus J_2(1)$.

If $J = J_6(1)$, then, since $(x-1)^6 = x^6 + x^3 + 1$ in $\mathbb{Z}_3[x]$, J is similar to

$$C\left(x^6+x^3+1\right) = \begin{bmatrix} -1 & & & & & \\ 0 & -1 & & & & \\ 0 & & 1 & & & \\ -1 & & & 1 & & \\ 0 & & & & 1 & \\ 0 & & & & & 1 \end{bmatrix} \begin{bmatrix} 0 & & & & & 1 \\ -1 & 0 & & & & \\ & 1 & 0 & & & \\ & & 1 & 0 & & \\ & & & 1 & 0 & \\ & & & & 1 & 0 \end{bmatrix}. \tag{3.4}$$

It can be verified that the first factor in equation (3.4) is an involution in $SL_6(\mathbb{Z}_3)$ and that the second factor is similar to $C(x^6+1)$ via $[-1] \oplus I_5$. Since

$$C(x^6+1) = \left[\begin{array}{ccc|ccc} & & 1 & & & 1 \\ & 1 & & & 1 & \\ 1 & & & 1 & & \\ \hline & & 1 & & & -1 \\ & 1 & & & -1 & \\ 1 & & & -1 & & \end{array}\right] \left[\begin{array}{ccc|ccc} 0 & -1 & 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 \\ \hline 0 & -1 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

is a product of two skew-involutions in $SL_6(\mathbb{Z}_3)$, it follows from Propositions 2.5 and 2.3 that J is a product of four skew-involutions.

If $J = J_4(1) \oplus J_2(1)$, then J is similar to $J_1 = C((x-1)^4) \oplus C((x-1)^2)$, which can be written as:

$$J_1 = \left[\begin{array}{cccc|cc} -1 & & & & & \\ 1 & 1 & & & & \\ 0 & & 1 & & & \\ 1 & & & 1 & & \\ \hline & & & & -1 & \\ & & & & 2 & 1 \end{array}\right] \left[C(x^4-1) \oplus C(x^2-1)\right]. \tag{3.5}$$

Since the first factor is an involution in $SL_6(\mathbb{Z}_3)$, it suffices to show that $C(x^4-1) \oplus C(x^2-1)$ is a product of two skew-involutions. Consider the skew-involutions $\hat{\imath}$ and $\hat{k}$ defined in equation (3.1) and the involution B_2 defined in equation (3.2). Since

$$C(x^4-1) \oplus C(x^2-1) = \begin{bmatrix} \hat{\imath} & -\hat{\imath} & I_2 \\ -\hat{\imath} & \hat{\imath} & I_2 \\ I_2 & I_2 & 0 \end{bmatrix} \begin{bmatrix} \hat{k} & -\hat{k} & -B_2 \\ -\hat{k} & \hat{k} & -B_2 \\ -B_2 & -B_2 & 0 \end{bmatrix}$$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

is a product of two skew-involutions, it follows from Proposition 2.3 that J is a product of four skew-involutions.

Let $J = J_2(1) \oplus J_2(1) \oplus J_2(1)$. Since $J_2(1)^3 = I_2$ in $M_2(\mathbb{Z}_3)$, we can write

$$J = \left(J_2(1) \oplus J_2(1)^{-1} \oplus I_2\right)\left(I_2 \oplus J_2(1)^{-1} \oplus J_2(1)\right).$$

By Lemma 2.2, both I_2 and $J_2(1) \oplus J_2(1)^{-1}$ are products of two skew-involutions. Hence, J is a product of four skew-involutions. This proves the following.

Lemma 3.6. *If $\epsilon \in \{1, -1\}$ and $A \in M_6(\mathbb{Z}_3)$ has Jordan form consisting of Jordan blocks with eigenvalue ϵ, then A is a product of four skew-involutions.*

The following theorem by Sourour [12, Theorem 1] decomposes a nonsingular nonscalar matrix into a product of matrices with prescribed eigenvalues.

Theorem 3.7. *Let $A \in M_n(\mathbb{F})$ be a nonsingular, nonscalar matrix over a field $\mathbb{F}$, and let β_j, γ_j ($1 \le j \le n$) be elements in $\mathbb{F}$ such that $\Pi_{i=1}^n \beta_i\gamma_i = \det A$. Then, there exist $B, C \in M_n(\mathbb{F})$ with eigenvalues $\beta_1, \ldots, \beta_n$ and $\gamma_1, \ldots, \gamma_n$, respectively, such that $A = BC$. Furthermore, B and C can be chosen so that B is lower triangularizable and C is simultaneously upper triangularizable.*

Suppose $n > 1$ and let $A \in SL_{2n}(\mathbb{Z}_3)$. If A is scalar, then $A = \pm I_{2n}$ is an involution, which is a product of two skew-involutions by Proposition 2.5. If A is nonscalar, then, by Theorem 3.7, we can write $A = BC$ for some $B, C \in SL_{2n}(\mathbb{Z}_3)$ with eigenvalues $\beta_1, \ldots \beta_{2n}$ and $\beta_1^{-1}, \ldots \beta_{2n}^{-1}$, respectively. If n is even, we take $\beta_i = 1$ for each i so that B and C are similar to Jordan matrices with eigenvalue 1. If n is odd, say $n = 2k+3$ for some nonnegative integer k, we take $\beta_i = 1$ for $i = 1, \ldots, 6$, and $\beta_i = -1$ for $i = 7, \ldots, 2n$ so that B and C are similar to a direct sum of a 6-by-6 Jordan matrix with eigenvalue 1 and a $4k$-by-$4k$ Jordan matrix with eigenvalue -1. By Lemmas 3.5 and 3.6 and Proposition 2.4, B and C are products of four skew-involutions. This shows the following theorem.

Theorem 3.8. *If $n > 1$, then every $A \in SL_{2n}(\mathbb{Z}_3)$ is a product of eight or fewer skew-involutions.*

Since every $A \in SL_{2n}(\mathbb{F})$ can be written as a product of four skew-involutions when $x^2 + 1$ has a root in $\mathbb{F}$, we obtain the following from Theorems 3.2 and 3.8, and Proposition 3.3.

Theorem 3.9. *Every $A \in SL_{2n}(\mathbb{F})$ is a product of skew-involutions if and only if $\mathbb{F} \neq \mathbb{Z}_3$ or $n > 1$.*

4. Products of real symplectic skew-involutions. If $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, let $U_n(\mathbb{F})$ denote the set of all unitary matrices in $M_n(\mathbb{F})$. If $\mathbb{F} = \mathbb{R}$, then $U_n(\mathbb{R})$ is the set of all real orthogonal matrices. We recall the *Euler decomposition* of a symplectic matrix [7, Equation 1.28], and for brevity, we call an orthogonal symplectic matrix as *orthosymplectic.*

Theorem 4.1. *Let $A \in \mathrm{Sp}_{2n}(\mathbb{R})$. Then there exist real orthosymplectic P and P' and positive diagonal D such that*

$$A = P\left(D \oplus D^{-1}\right)P'. \tag{4.6}$$

Let $A \in M_n(\mathbb{C})$. Write $A = X + iY$ where $X, Y \in M_n(\mathbb{R})$, and define the mapping $L : M_n(\mathbb{C}) \to M_{2n}(\mathbb{R})$ by:

$$L(X + iY) = \begin{bmatrix} X & -Y \\ Y & X \end{bmatrix}. \tag{4.7}$$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

The next proposition is Lemma 29 and Proposition 30 in [3].

PROPOSITION 4.2. *The mapping L in equation (4.7) is an algebra monomorphism, that is, L is an injective linear transformation over $\mathbb{R}$ such that*

$$L(AB) = L(A)L(B),$$

for all $A, B \in M_n(\mathbb{C})$. The restriction of L to $U_n(\mathbb{C})$ is an isomorphism of $U_n(\mathbb{C})$ onto $U_{2n}(\mathbb{R}) \cap \mathrm{Sp}_{2n}(\mathbb{R})$.

Proposition 4.2 establishes a one-to-one correspondence between the set of complex unitary matrices and the set of real orthosymplectic matrices. That is, $U = X + iY$ is unitary if and only if

$$A = \begin{bmatrix} X & -Y \\ Y & X \end{bmatrix}, \text{ with } XX^\top + YY^\top = I \text{ and } XY^\top = YX^\top. \tag{4.8}$$

THEOREM 4.3. *Every $A \in \mathrm{Sp}_{2n}(\mathbb{R})$ is a product of six real symplectic skew-involutions.*

Proof. Let $A \in \mathrm{Sp}_{2n}(\mathbb{R})$. By Theorem 4.1, there exist orthosymplectic P and P', and positive diagonal D such that $A = P\left(D \oplus D^{-1}\right)P'$. If we set $Q := P(D \oplus D^{-1})P^{-1}$ and $R := PP'$, then $A = QR$. Observe that Q is symplectic and that, by Lemma 2.2, $D \oplus D^{-1}$ can be written as a product of two symplectic skew-involutions. By Proposition 2.3, Q is a product of two symplectic skew-involutions. Now, R is orthosymplectic since P and P' are orthosymplectic. Thus, there exist $X, Y \in M_n(\mathbb{R})$ such that

$$R = \begin{bmatrix} X & -Y \\ Y & X \end{bmatrix}, \text{ with } XX^\top + YY^\top = I \text{ and } XY^\top = YX^\top.$$

By Proposition 4.2, we have $U := X + iY \in U_n(\mathbb{C})$. Hence, there exists unitary T such that

$$T^*UT = \mathrm{diag}\left(\cos\theta_1 + i\sin\theta_1, \ldots, \cos\theta_n + i\sin\theta_n\right),$$

for some $\theta_1, \ldots, \theta_n \in \mathbb{R}$. By Proposition 4.2, there exists a real orthosymplectic S such that

$$S^{-1}RS = \boxplus_{j=1}^{n} \begin{bmatrix} \cos\theta_j & -\sin\theta_j \\ \sin\theta_j & \cos\theta_j \end{bmatrix}.$$

Since each summand in the expanding sum is in $SL_2(\mathbb{R})$, it follows from Theorem 3.2 and Propositions 2.4 and 2.3 that R is a product of four symplectic skew-involutions. Thus, A is a product of six symplectic skew-involutions. ∎

5. Products of complex symplectic skew-involutions. Let $A \in \mathrm{Sp}_{2n}(\mathbb{C})$. Since $x^2 + 1$ has a root in $\mathbb{C}$, then A is a product of two symplectic skew-involutions. The following lemma gives a canonical form of a symplectic matrix under symplectic similarity, called the *symplectic Jordan form* [4, Lemma 5].

LEMMA 5.1. *Each symplectic complex matrix is symplectically similar to the expanding sum of matrices of the following forms:*

- $J_k(\lambda) \oplus J_k(\lambda)^{-\top}$ *for* $\lambda \neq 0, \pm 1$,
- $J_{2k-1}(\epsilon) \oplus J_{2k-1}(\epsilon)^{-\top}$ *for* $\epsilon = \pm 1$, *or*
- $\pm\mathcal{E}(k)$, *where*

$$\mathcal{E}(k) := \begin{bmatrix} J_k(1) & U_k \\ 0 & J_k(1)^{-\top} \end{bmatrix} \in M_{2k}(\mathbb{C}), \tag{5.9}$$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

and $U_k = [u_{ij}] \in M_k(\mathbb{C})$ *such that*

$$u_{ij} = \begin{cases} 0 & \text{if } i \neq k, \\ (-1)^{k-j} & \text{if } i = k. \end{cases} \tag{5.10}$$

By Proposition 2.3, it is enough to show that each matrix in Lemma 5.1 can be written as a product of two symplectic skew-involutions.

Let k be a positive integer and $\lambda \neq 0$. Let B_k be the k-by-k backward identity matrix in equation (3.2). Define the symplectic matrices:

$$S_k := \begin{bmatrix} 0 & B_k \\ -B_k & 0 \end{bmatrix} \quad \text{and} \quad T_k(\lambda) := \begin{bmatrix} 0 & -\left[J_k(\lambda)^\top B_k\right]^{-\top} \\ J_k(\lambda)^\top B_k & 0 \end{bmatrix}. \tag{5.11}$$

Since $B_k^\top = B_k^{-1} = B_k$, and $B_k J_k(\lambda) B_k = J_k(\lambda)^\top$, we have that S_k and $T_k(\lambda)$ are skew-involutions such that $S_k T_k(\lambda) = J_k(\lambda) \oplus J_k(\lambda)^{-\top}$. This gives us the following lemma.

Lemma 5.2. *If* k *is a positive integer and* $\lambda \neq 0$*, then* $J_k(\lambda) \oplus J_k(\lambda)^{-\top}$ *is a product of two symplectic skew-involutions.*

It remains to show that $\mathcal{E}(k)$, as defined in equation (5.9), is a product of two symplectic skew-involutions. To do this, we recall some important identities involving binomial coefficients and properties of persymmetric matrices.

5.1. Binomial coefficients.

We use the convention that for any nonnegative $r, s \in \mathbb{Z}$,

$$\binom{s}{r} = \begin{cases} 0 & \text{if } s < r \\ \dfrac{s!}{r!(s-r)!} & \text{if } s \geq r \end{cases},$$

and observe that $\binom{s}{r} = \binom{s}{s-r}$. When r is a positive integer, the binomial coefficient $\binom{-r}{s}$ is given by:

$$\binom{-r}{s} = (-1)^s \binom{r+s-1}{s}, \quad \text{for non-negative } s \in \mathbb{Z}. \tag{5.12}$$

The following are identities involving binomial coefficients [11, Chapter 2, Section 6].

Theorem 5.3. *Let* $s, t \in \mathbb{Z}$*, where* $s \geq 0$ *and* $t > 0$*.*

1. *For all* $x, y \in \mathbb{Z}$*,*

$$\sum_{r=0}^{s} \binom{x}{r}\binom{y}{s-r} = \binom{x+y}{s}. \tag{5.13}$$

2. *For* $r = 0, 1, 2, \ldots, t-1$*,*

$$\sum_{k=0}^{r} (-1)^k \binom{t}{k} = (-1)^r \binom{t-1}{r}. \tag{5.14}$$

When $r = t$*, we have* $\sum_{k=0}^{t} (-1)^k \binom{t}{k} = 0$*.*

Equation (5.13) is called the *Chu–Vandermonde identity*, or the *Vandermonde convolution formula*. This identity is generalized to $x, y \in \mathbb{C}$ in [11].

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

5.2. Persymmetric matrices. If $P \in M_n(\mathbb{F})$, define

$$P^F := B_n P^\top B_n.$$

If $P^F = P$, we say that the matrix P is *persymmetric*. The transpose of P is obtained by flipping P along its main diagonal, while P^F is obtained by flipping P along its main anti-diagonal (or the northeast-to-southwest diagonal), that is, if $P = [p_{ij}]$ and $P^F = \left[p^F_{ij}\right]$, then $p^F_{ij} = p_{n-j+1,n-i+1}$. For instance, every Toeplitz matrix is persymmetric since each diagonal from left to right has equal entries. It can be observed that

$$B_n^F = B_n \quad \text{and} \quad \left(P^F\right)^\top = B_n P B_n = \left(P^\top\right)^F.$$

Moreover, the following hold for all $c \in \mathbb{F}$ and $A, B \in M_n(\mathbb{F})$:

$$\left(A^F\right)^F = A, \quad (cA)^F = cA^F, \quad (A+B)^F = A^F + B^F, \quad (AB)^F = B^F A^F.$$

LEMMA 5.4. *If $A, B \in M_n(\mathbb{F})$ are persymmetric, then so are $A^\top$, $\alpha A + \beta B$ for any $a, b \in \mathbb{F}$, and A^{-1} if A is nonsingular.*

5.3. The matrix $\mathcal{E}(n)$. Let n be a positive integer and let $\mathcal{E}(n)$ be defined as in equation (5.9). We define

$$P_n := \begin{bmatrix} 1 & -1 & 1 & -1 & \cdots & (-1)^{n-1} \\ 0 & -1 & 2 & -3 & \cdots & (-1)^{n-1}\binom{n-1}{1} \\ 0 & 0 & 1 & -3 & \cdots & (-1)^{n-1}\binom{n-1}{2} \\ 0 & 0 & 0 & -1 & \cdots & (-1)^{n-1}\binom{n-1}{3} \\ \vdots & \vdots & \vdots & \vdots & \searrow & \vdots \\ 0 & 0 & 0 & 0 & \cdots & (-1)^{n-1} \end{bmatrix}, \tag{5.15}$$

and

$$Q_n := \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 & \binom{n}{1} \\ \vdots & \vdots & \iddots & 1 & \binom{n}{1} & \binom{n}{2} \\ 0 & 0 & \iddots & \binom{n}{1} & \binom{n}{2} & \binom{n}{3} \\ 0 & 1 & \iddots & \vdots & \vdots & \vdots \\ 1 & \binom{n}{1} & \cdots & \binom{n}{n-3} & \binom{n}{n-2} & \binom{n}{n-1} \end{bmatrix}. \tag{5.16}$$

Observe that P_n is an involution, Q_n is symmetric, and

$$J_n(1) P_n J_n(1) = P_n. \tag{5.17}$$

Let $Y_n := iP_n$ and $Z_n := i(-1)^n Q_n$ and set

$$X_n := \begin{bmatrix} Y_n & Z_n \\ 0 & Y_n^{-\top} \end{bmatrix}. \tag{5.18}$$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

Note that Z_n is symmetric, since Q_n is symmetric. Since P_n is an involution, we have Y_n is a skew-involution and, by equation (5.17),

$$J_n(1)Y_nJ_n(1) = Y_n. \tag{5.19}$$

We claim that X_n is a symplectic skew-involution and that $\mathcal{E}(n)$ is similar to $\mathcal{E}(n)^{-1}$ via X_n to obtain the following result.

Lemma 5.5. *If n is a positive integer, then $\mathcal{E}(n)$ is a product of two symplectic skew-involutions.*

By Lemmas 5.1, 5.2, and 5.5, we have the following theorem.

Theorem 5.6. *Each complex symplectic matrix is a product of two complex symplectic skew-involutions.*

To show that the matrix X_n as defined in equation (5.18) is a symplectic skew-involution, it suffices to show that $Y_nZ_n = (-1)^{n+1}P_nQ_n$ is symmetric by Proposition 2.1, or, equivalently, P_nQ_n is symmetric. Since Q_n is symmetric and $Q_n = R_nB_n$, where R_n is the Toeplitz matrix

$$R_n = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ \binom{n}{1} & 1 & 0 & \cdots & 0 & 0 \\ \binom{n}{2} & \binom{n}{1} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \binom{n}{n-2} & \binom{n}{n-3} & \binom{n}{n-4} & \cdots & 1 & 0 \\ \binom{n}{n-1} & \binom{n}{n-2} & \binom{n}{n-3} & \cdots & \binom{n}{1} & 1 \end{bmatrix}, \tag{5.20}$$

we have P_nQ_n is symmetric if and only if $P_nR_nB_n = R_nB_nP_n^\top$, which holds if and only if $P_nR_n = R_nB_nP_n^\top B_n = R_n^F P_n^F = (P_nR_n)^F$. Thus, it is enough to show that P_nR_n is persymmetric.

If $P_n = [p_{ij}]$ and $R_n = [r_{ij}]$, then

$$p_{ij} = \begin{cases} 0 & \text{if } i > j, \\ (-1)^{j+1}\binom{j-1}{i-1} = (-1)^{i+1}\binom{-i}{j-i} & \text{if } i \le j, \end{cases} \tag{5.21}$$

and

$$r_{ij} = \begin{cases} 0 & \text{if } i < j, \\ \binom{n}{i-j} & \text{if } i \ge j. \end{cases} \tag{5.22}$$

We establish some identities involving P_n, R_n, and U_n.

5.4. Some technical lemmas. Let P_n, R_n, and U_n be defined as in equations (5.21), (5.22), and (5.10) respectively.

Lemma 5.7. *For any positive integer n, we have $P_nP_n^F = (-1)^{n+1}R_n^\top$.*

Proof. Since P_n and P_n^F are upper triangular and R_n is lower triangular, both $P_nP_n^F$ and $R_n^\top$ are upper triangular. If $i \le j$, then the (i,j)-entry of $P_nP_n^F$ is

$$\sum_{k=i}^{j} p_{ik}p_{n-j+1,n-k+1} = \sum_{k=i}^{j} \left[(-1)^{i+1}\binom{-i}{k-i}\right]\left[(-1)^{n-j}\binom{j-n-1}{j-k}\right].$$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

We re-index the above summation using $m = k - i$ and apply equation (5.13) to get

$$(-1)^{n+i-j+1}\sum_{m=0}^{j-i}\binom{-i}{m}\binom{j-n-1}{j-i-m} = (-1)^{n+i-j+1}\binom{j-i-n-1}{j-i}.$$

Since $j - i < n + 1$, we apply equation (5.12) to obtain

$$(-1)^{n+i-j+1}\binom{j-i-n-1}{j-i} = (-1)^{n+1}\binom{n}{j-i} = (-1)^{n+1}r_{ji},$$

which is the (i, j)-entry of $(-1)^{n+1}R_n^\top$. Thus, $P_nP_n^F = (-1)^{n+1}R_n^\top$. ∎

LEMMA 5.8. *For any positive integer n, we have $P_nB_nP_n = B_nP_nB_n = \left(P_n^\top\right)^F$.*

Proof. Observe that the (i, j)-entry of $(P_nB_n)P_n$ is given by $\sum_{k=1}^{n} p_{i,n-k+1}p_{kj}$. Let $m := \min\{n - i + 1, j\}$. Since p_{rs} and $\binom{s}{r}$ are 0 when $s < r$, we have

$$\sum_{k=1}^{n} p_{i,n-k+1}p_{kj} = \sum_{k=1}^{m}\left[(-1)^{i+1}\binom{-i}{n-k+1-i}\right]\left[(-1)^{k+1}\binom{-k}{j-k}\right].$$

We apply equation (5.12) to $\binom{-k}{j-k}$ and re-index the summation from $k = 0$ to $m - 1$ to obtain

$$\sum_{k=1}^{m}(-1)^{i+j}\binom{-i}{n-k+1-i}\binom{j-1}{j-k} = (-1)^{i+j}\sum_{k=0}^{m-1}\binom{-i}{n-k-i}\binom{j-1}{j-1-k}.$$

Since $\binom{r}{s} = \binom{r}{s-r}$ for any nonnegative $r, s \in \mathbb{Z}$ with $r \geq s$, we obtain

$$\sum_{k=1}^{n} p_{i,n-k+1}p_{kj} = (-1)^{i+j}\sum_{k=0}^{m-1}\binom{j-1}{k}\binom{-i}{n-i-k}. \tag{5.23}$$

Observe that when $k > j - 1$, we have $\binom{j-1}{k} = 0$. If $m = j$, then $j \leq n - i + 1$ and the terms corresponding to $k = j, j + 1, \ldots, n - i$ are 0. Hence, we may assume, without loss of generality, that $m = n - i + 1$, and apply equation (5.13) on equation (5.23) to obtain

$$\sum_{k=1}^{n} p_{i,n-k+1}p_{kj} = (-1)^{i+j}\binom{j-1-i}{n-i}. \tag{5.24}$$

If $j > i$, then $j - 1 - i \geq 0$. Since $j - 1 < n$, we have $0 \leq j - 1 - i < n - i$, and so the (i, j)-entry of $P_nB_nP_n$ is 0. Since P_n is upper triangular, we have $B_nP_nB_n = \left(P_n^\top\right)^F$ is lower triangular, and so the corresponding (i, j)-entries of $P_nB_nP_n$ and $\left(P_n^\top\right)^F$ are equal to 0 when $j > i$. Suppose $j \leq i$. Then $j - i - 1 < 0$ and, using equation (5.12) on equation (5.24), the (i, j)-entry of $P_nB_nP_n$ is

$$\sum_{k=1}^{n} p_{i,n-k+1}p_{kj} = (-1)^{n+j}\binom{-(j-1-i)+n-i-1}{n-i} = (-1)^{n-j}\binom{n-j}{n-i},$$

which is equal to $p_{n-i+1,n-j+1}$ or the (i, j)-entry of $B_nP_nB_n$. ∎

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

LEMMA 5.9. *The matrix $P_nU_n + (-1)^n Q_n J_n(1)^{-\top}$ is symmetric.*

Proof. Let $P_n = [p_{ij}]$ and $U_n = [u_{ij}]$ be defined as in equations (5.21) and (5.10), respectively. Since only the last row of U_n is non-zero, the (i,j)-entry of P_nU_n is given by:

$$p_{in}u_{nj} = (-1)^{j-1}\binom{n-1}{i-1}. \tag{5.25}$$

If $J_n(1)^{-\top} = [c_{ij}]$, then

$$c_{ij} = \begin{cases} 0 & \text{if } i < j, \\ (-1)^{i-j} & \text{if } i \geq j. \end{cases}$$

Since $Q_n = R_nB_n$, it follows that the (i,j)-entry of $Q_nJ_n(1)^{-\top}$ is given by:

$$\sum_{k=1}^{n} r_{i,n-k+1}c_{k,j} = \sum_{k=m}^{n}(-1)^{k-j}\binom{n}{i-n+k-1}, \text{ for } m := \max\{n-i+1, j\}.$$

By re-indexing the summation from $l = 0$ to $n - m$, we have

$$\sum_{l=0}^{n-m}(-1)^{l+m-j}\binom{n}{i-n+l+m-1}. \tag{5.26}$$

If $n - i + 1 \geq j$, then $m = n - i + 1$ and equation (5.26) becomes

$$\sum_{l=0}^{i-1}(-1)^{l+n-i+1-j}\binom{n}{l} = (-1)^{n-i-j+1}\sum_{l=0}^{i-1}(-1)^{l}\binom{n}{l}.$$

By equation (5.14), the (i,j)-entry of $Q_nJ_n(1)^{-\top}$ is given by:

$$\sum_{k=1}^{n} r_{i,n-k+1}c_{k,j} = (-1)^{n-j}\binom{n-1}{i-1} \text{ when } i+j \leq n+1. \tag{5.27}$$

If $j > n - i + 1$, then $t := i + j - n - 1$ is a positive integer. Since $Q_nJ_n(1)^{-\top} = R_n\left(B_nJ_n(1)^{-\top}\right)$ and $r_{pq} = c_{pq} = 0$ when $p < q$, the (i,j)-entry of $Q_nJ_n(1)^{-\top}$ is

$$\sum_{k=1}^{n} r_{ik}c_{n-k+1,j} = \sum_{k=1}^{n-j+1} r_{ik}c_{n-k+1,j}.$$

By subtracting i from both limits of summation, we may re-index from $k = 1 - i$ to $n + 1 - i - j = -t$ to obtain

$$\sum_{k=1-i}^{-t} r_{i,k+i}c_{n-k-i+1,j} = \sum_{k=1-i}^{-t}(-1)^{n+1-i-j-k}\binom{n}{-k}.$$

If we set $l = -k$, then

$$\sum_{k=1-i}^{-t}(-1)^{n+1-i-j-k}\binom{n}{-k} = (-1)^{-t}\sum_{l=t}^{i-1}(-1)^{l}\binom{n}{l}. \tag{5.28}$$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

Since

$$\sum_{l=t}^{i-1}(-1)^l\binom{n}{l} = \sum_{l=0}^{i-1}(-1)^l\binom{n}{l} - \sum_{l=0}^{t-1}(-1)^l\binom{n}{l}, \tag{5.29}$$

it follows from equations (5.14) and (5.29) that we can write equation (5.28) as:

$$(-1)^{-t}\left[(-1)^{i-1}\binom{n-1}{i-1} - (-1)^{t-1}\binom{n-1}{t-1}\right].$$

Thus, the (i,j)-entry of $Q_nJ_n(1)^{-\top}$ is given by:

$$\sum_{k=1}^{n} r_{i,n-k+1}c_{k,j} = (-1)^{n-j}\binom{n-1}{i-1} + \binom{n-1}{t-1}, \text{ when } i+j>n+1. \tag{5.30}$$

If t_{ij} is the (i,j)-entry of $P_nU_n + (-1)^nQ_nJ_n(1)^{-\top}$, it follows from equations (5.25), (5.27), and (5.30) that

$$t_{ij} = \begin{cases} 0 & \text{if } i+j \le n+1, \\ (-1)^n\binom{n-1}{i+j-n-2} & \text{if } i+j > n+1. \end{cases} \tag{5.31}$$

Since $t_{ij} = t_{ji}$, it follows that $P_nU_n + (-1)^nQ_nJ_n(1)^{-\top}$ is symmetric. □

We are now ready to prove Lemma 5.5.

5.5. Proof of Lemma 5.5. We first show that P_nR_n is persymmetric. Observe that, by Lemma 5.7, we have $P_nR_n = (-1)^{n+1}P_n\left(P_n^F\right)^\top P^\top = (-1)^{n+1}P_n(B_nP_nB_n)P_n^\top$. Since P_n is an involution, it follows from Lemmas 5.8 and 5.7 that

$$(P_nB_nP_n)B_nP_n^\top = (P_nB_nP_n)P_n^\top\left(P_n^\top B_nP_n^\top\right) = (P_n^\top)^F P_n^\top P_n^F = (-1)^{n+1}R_nP_n^F.$$

Hence, $P_nR_n = R_nP_n^F$, and, since R_n is persymmetric, we have $P_nR_n = R_nP_n^F = R_n^FP_n^F = (P_nR_n)^F$. Thus, P_nR_n is persymmetric and the matrix X_n defined in equation (5.18) is a symplectic skew-involution.

We now show that $\mathcal{E}(n)$ is similar to $\mathcal{E}(n)^{-1}$ via X_n. It suffices to show that $X_n\mathcal{E}(n) = -\left(X_n\mathcal{E}(n)\right)^{-1}$, i.e. $X_n\mathcal{E}(n)$ is a skew-involution. Since

$$X_n\mathcal{E}(n) = \begin{bmatrix} Y_nJ_n(1) & Y_nU_n + Z_nJ_n(1)^{-\top} \\ 0 & Y_n^{-\top}J_n(1)^{-\top} \end{bmatrix},$$

we set

$$V_n := Y_nJ_n(1) \text{ and } W_n := Y_nU_n + Z_nJ_n(1)^{-\top}.$$

Then $X_n\mathcal{E}(n)$ is a skew-involution if and only if V_n is a skew-involution and $V_nW_n = W_nV_n^\top$. It follows from equation (5.19) that V_n is a skew-involution. Since $X_n\mathcal{E}(n)$ is symplectic, we have $V_nW_n^\top = W_nV_n^\top$. To show that $V_nW_n = W_nV_n^\top$ $(= V_nW_n^\top)$, it is enough to show that W_n is symmetric since V_n is nonsingular. Since $Y_n = iP_n$ and $Z_n = i(-1)^nQ_n$, we have $W_n = iP_nU_n + i(-1)^nQ_nJ_n(1)^{-\top}$. It follows from Lemma 5.9 that W_n is symmetric. Since both X_n and $X_n\mathcal{E}(n)$ are symplectic skew-involutions, we can write

$$\mathcal{E}(n) = \left(X_n^{-1}\right)\left(X_n\mathcal{E}(n)\right),$$

which proves Lemma 5.5.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 39, pp. 136-150, March 2023.

Remark 5.10. In the above discussion, a symplectic A similar to A^{-1} via a symplectic skew-involution B can be written as a product of two symplectic skew-involutions B^{-1} and BA. Thus, if $S \in \mathrm{Sp}_{2n}(\mathbb{C})$, there exists a symplectic R such that RSR^{-1} is the expanding sum Q of matrices found in Lemma 5.1. Since each summand of the form $J_k(\lambda) \oplus J_k(\lambda)^{-\top}$ can be written as $S_k T_k(\lambda)$ where S_k and $T_k(\lambda)$ are defined as in equation (5.11), and $\mathcal{E}(m)$ can be written as $X_m^{-1}(X_m\mathcal{E}(m))$ where X_m is defined as in equation (5.18), then we can write $S = \left(R^{-1}A_1R\right)\left(R^{-1}A_2R\right)$, where A_1 is an expanding sum of matrices S_{k_i} or $X_{k_j}^{-1}$, and A_2 is an expanding sum of matrices $T_{k_i}(\lambda)$ or $X_{k_j}\mathcal{E}(k_j)$.

If $S \in \mathrm{Sp}_{2n}(\mathbb{C})$, then $S = C_1C_2$ where C_1 and C_2 are symplectic skew-involutions. Observe that $(C_1\Omega_{2n})^\top = \Omega_{2n}^{-1}C_1^\top = C_1^{-1}\Omega_{2n}^{-1} = C_1\Omega_{2n}$, that is, $C_1\Omega_{2n}$ is symmetric. Similarly, $\Omega_{2n}^{-1}C_2$ is symmetric. Thus, $S = (C_1\Omega_{2n})\left(\Omega_{2n}^{-1}C_2\right)$ is a product of two symplectic symmetric matrices. Analogous to the result of Bosch [1, Theorem 1] where every complex square matrix can be decomposed into a product of two complex symmetric matrices, we have the following.

Corollary 5.11. *Every complex symplectic matrix can be written as a product of two complex symplectic symmetric matrices.*

Acknowledgment. The work of the authors was supported by the MacArthur and Josefina Delos Reyes Research Grant and the U.P. Diliman Mathematics Foundation Inc.

REFERENCES

[1] A.J. Bosch. The factorization of a square matrix into two symmetric matrices. *Am. Math. Mon.*, 93:462–464, 1986.
[2] J.D. Botha. Spectrally arbitrary, nonderogatory factorization over a general field. *Linear Algebra Appl.*, 433:1–11, 2010.
[3] M.A. de Gosson. *Symplectic Methods in Harmonic Analysis and in Mathematical Physics.* Birkhäuser, 2011.
[4] R.J. de la Cruz. Every symplectic matrix is a product of four symplectic involutions. *Linear Algebra Appl.*, 466:382–400, 2015.
[5] D.Ž. Djoković. Products of two involutions. *Arch. Math.*, 18:582–584, 1967.
[6] E.W. Ellers and O. Villa. Generation of the symplectic group by involutions. *Linear Algebra Appl.*, 591:154–159, 2020.
[7] A. Ferraro, S. Olivares, and M.G.A. Paris. *Gaussian States in Continuous Variable Quantum Information.* Bibliopolis, Napoli, 2005.
[8] R. Gow. Products of two involutions in classical groups of characteristic 2. *J. Algebra*, 71:583–591, 1981.
[9] W.H. Gustafson and P.R. Halmos. Products of involutions. *Linear Algebra Appl.*, 13:157–162, 1976.
[10] R.A. Horn and C.R. Johnson. *Matrix Analysis.* Cambridge University Press, New York, 1985.
[11] S. Roman. *The Umbral Calculus.* Academic Press, New York, 1984.
[12] A.R. Sourour. A factorization theorem for matrices. *Linear and Multilinear Algebra*, 19:2, 141–147, 1986.
[13] M.J. Wonenburger. Transformations which are products of two involutions. *J. Appl. Math. Mech.*, 16:327–338, 1966.