Decomposition of symplectic matrices into products of symplectic unipotent matrices of index 2

Xin Hou
Capital Normal University, Beijing, houge19870512@126.com

Zhengyi Xiao
Beihang University, Beijing, xiaozhengyi@buaa.edu.cn

Yajing Hao
Beihang University, Beijing

Qi Yuan
Beihang University, Beijing

DECOMPOSITION OF SYMPLECTIC MATRICES INTO PRODUCTS OF SYMPLECTIC UNIPOTENT MATRICES OF INDEX 2^*

XIN HOU[†], ZHENGYI XIAO[‡], YAJING HAO[‡], AND QI YUAN[‡]

Abstract. In this article, it is proved that every symplectic matrix can be decomposed into a product of three symplectic unipotent matrices of index 2, i.e., every complex matrix A satisfying $A^T J A = J$ with $J = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$ is a product of three matrices B_i satisfying $B_i^T J B_i = J$ and $(B_i - I)^2 = 0$ $(i = 1, 2, 3)$.

Key words. Symplectic matrices, Product of unipotent matrices, Symplectic Jordan Canonical Form.

AMS subject classifications. 15A23, 20H20.

1. Introduction.

Decomposition of elements in a matrix group into products of matrices with a special nature (such as unipotent matrices, involutions and so on) is a popular topic studied by many scholars. In the $n \times n$ matrix ring $M_n(F)$ over a field F, a unipotent matrix of index k refers to a matrix A satisfying $(A - I_n)^k = 0$. Fong and Sourour in [4] proved that every matrix in the group $\mathrm{SL}_n(\mathbb{C})$ (the special linear group over complex field $\mathbb{C}$) is a product of three unipotent matrices (without limitation on the index). Wang and Wu in [6] gave a further result that every matrix in the group $\mathrm{SL}_n(\mathbb{C})$ is a product of four unipotent matrices of index 2.

In particular, decompositions of symplectic matrices have drawn considerable attention from numerous scholars (see [1, 3]). Set $J = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$. A matrix A is called *symplectic* if it satisfies $A^T J A = J$. Denote by $\mathrm{Sp}_{2n}(F)$ the group consisting of all the $2n \times 2n$ symplectic matrices over a field F. Some scholars have focused on expressing an arbitrary symplectic matrix in $\mathrm{Sp}_{2n}(F)$ as a product of symplectic involutions or symplectic unipotents. In [2], Cruz proved that every complex symplectic matrix of size greater than two is a product of four symplectic involutions. In [7], You proved that every symplectic matrix over a commutative ring satisfying the first stable range condition is a product of three symplectic unipotents. The contribution of this article is that the index of unipotents may be taken to be 2. For the complex field $\mathbb{C}$, we will prove that every symplectic matrix in $\mathrm{Sp}_{2n}(\mathbb{C})$ can be expressed as a product of three symplectic unipotent matrices of index 2.

Our main result is the following theorem.

THEOREM 1.1. *Every complex symplectic matrix in* $\mathrm{Sp}_{2n}(\mathbb{C})$ *can be decomposed into a product of three symplectic unipotent matrices of index* 2. *Moreover, three is the smallest such number.*

2. Proof of the main result.

First, let us declare some notations frequently used in the proof. Denote by $\mathcal{SU}(k)$ the set of all matrices that can be written as a product of k symplectic unipotent matrices of index 2. Denote $\mathrm{diag}(A, B)$ by $A \oplus B$. Set

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix},$$

where each A_{ij} is a matrix of size m, and each B_{ij} is a matrix of size n for $i, j \in \{1, 2\}$. Denote by $A \boxplus B$ the *expanding sum* of A and B, i.e., the following matrix:

$$\begin{bmatrix} A_{11} \oplus B_{11} & A_{12} \oplus B_{12} \\ A_{21} \oplus B_{21} & A_{22} \oplus B_{22} \end{bmatrix},$$

which is a matrix of size $2(m + n)$. We have $(A \boxplus B) \cdot (C \boxplus D) = (A \cdot C) \boxplus (B \cdot D)$. We can verify the following remark.

REMARK 2.1. Let A and B be two matrices of size m, and let C be a matrix of size n.

(a) If B is symplectically similar to A, then $A \in \mathcal{SU}(k)$ if and only if $B \in \mathcal{SU}(k)$.

(b) If $A \in \mathcal{SU}(k_1)$ and $C \in \mathcal{SU}(k_2)$, then $A \boxplus C \in \mathcal{SU}(l)$, where $l = \max\{k_1, k_2\}$.

Denote by $J_k(\lambda)$ the Jordan block of size k with eigenvalue λ. Abbreviate $(P^{-1})^T$ and $(P^T)^{-1}$ to P^{-T}. Denote by $\varepsilon(k)$ the matrix

$$\begin{bmatrix} J_k(1) & \begin{bmatrix} 0_{k-1,k} \\ u \end{bmatrix} \\ 0 & J_k(1)^{-T} \end{bmatrix},$$

where $u = [(-1)^{k+1}, (-1)^k, \ldots, 1]$ is the last row vector of $J_k(1)^{-T}$. Then $\varepsilon(k)$ is similar to $J_{2k}(1)$.

Now let us present a canonical form of symplectic matrices under symplectic similarity, which is also called the *Symplectic Jordan Canonical Form* of symplectic matrices (see [2, 3]). It is sufficient to prove Theorem 1.1 for the Symplectic Jordan Canonical Form in the following lemma.

LEMMA 2.2. (Cruz [2], Lemma 5) *Each symplectic matrix is symplectically similar to the expanding sum of matrices of the form* $J_k(\lambda) \oplus J_k(\lambda)^{-T}$ ($\lambda \notin \{0, \pm 1\}$), $J_{2k+1}(\lambda) \oplus J_{2k+1}(\lambda)^{-T}$ ($\lambda \in \{\pm 1\}$) *and* $\pm \varepsilon(k)$.

From Lemma 2.2, we need only prove the result for each matrix block in the Symplectic Jordan Canonical Form to get the main result.

Let us introduce the following two lemmas first.

LEMMA 2.3. (Horn and Merino [5], Theorem 20) *Let P and Q be both symplectic. Then P and Q are similar if and only if P and Q are symplectically similar.*

LEMMA 2.4. (Wang and Wu [6], Lemma 3.2) *If T is an $n \times n$ invertible cyclic matrix (i.e., its minimal polynomial equals its characteristic polynomial) and $\alpha_1, \ldots, \alpha_n$ are complex numbers satisfying $\alpha_1 \cdots \alpha_n = \det(T)$, then there exist matrices A and B such that $T = AB$, $(A - I_n)^2 = 0$, and B is cyclic with eigenvalues $\alpha_1, \ldots, \alpha_n$.*

Now let us begin with some examples of 2×2 matrices.

$$\begin{bmatrix} I\,L \\ A\,S \end{bmatrix}$$

LEMMA 2.5. *A 2×2 matrix is symplectic unipotent if and only if its determinant is 1 and its trace is 2 (i.e., its two eigenvalues are both 1).*

Proof. Let A be a symplectic unipotent 2×2 matrix. We know that the polynomial $p(x) = (x-1)^2$ satisfies $p(A) = 0$. Therefore, the only eigenvalue of A is 1.

Conversely, if A has two eigenvalues 1, then $A - I_2$ has two eigenvalues 0. Since the order of A is 2, we can conclude that $(A - I_2)^2 = 0$, which shows that A is unipotent. That A is symplectic can be derived from the fact that $\det(A) = 1$. □

LEMMA 2.6. *The matrix*

$$\begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix}, \quad \lambda \neq -1$$

is a product of two symplectic unipotent matrices of index 2.

Proof. Observe that

$$\begin{bmatrix} \frac{2\lambda}{1+\lambda} & -\lambda \\ \frac{(\lambda-1)^2}{\lambda(\lambda+1)^2} & \frac{2}{1+\lambda} \end{bmatrix} \begin{bmatrix} \frac{2\lambda}{1+\lambda} & 1 \\ -\frac{(\lambda-1)^2}{(\lambda+1)^2} & \frac{2}{1+\lambda} \end{bmatrix} = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix}$$

and that both matrices on the left side are symplectic unipotent of index 2 by Lemma 2.5. □

LEMMA 2.7. *The matrix*

$$\begin{bmatrix} -1 & a \\ 0 & -1 \end{bmatrix}, \quad a \neq 0$$

is a product of two symplectic unipotent matrices of index 2.

Proof. Observe that

$$\begin{bmatrix} 1 & 0 \\ -\frac{4}{a} & 1 \end{bmatrix} \begin{bmatrix} -1 & a \\ -\frac{4}{a} & 3 \end{bmatrix} = \begin{bmatrix} -1 & a \\ 0 & -1 \end{bmatrix}$$

and that both matrices on the left side are symplectic unipotent of index 2 by Lemma 2.5. □

LEMMA 2.8. *The matrix $-I_2$*

(a) *is a product of three symplectic unipotent matrices of index 2,*

(b) *is not a product of two symplectic unipotent matrices of index 2.*

Proof. (a) Observe that

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & a \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The first matrix on the left side is a symplectic unipotent matrix of index 2, while the second matrix is a product of two by Lemma 2.7. Therefore, we have $-I_2 \in \mathcal{SU}(3)$.

(b) Let A be a 2×2 matrix with its entries being $a_{ij}(i, j \in \{1, 2\})$. Supposing $A \in \mathcal{SU}(1)$, let us determine the conditions that the entries a_{ij} satisfy.

According to Lemma 2.5, we only need to calculate the trace and determinant of A: $a_{11} + a_{22} = 2$, $a_{11}a_{22} - a_{12}a_{21} = 1$. Therefore, $a_{22} = 2 - a_{11}$, $a_{12}a_{21} = a_{11}a_{22} - 1 = -(a_{11} - 1)^2$.

If $a_{12} = 0$, A becomes a lower triangular matrix

$$(2.1) \qquad\qquad A = \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix}.$$

Otherwise, $a_{12} \neq 0$, we set $a_{11} = x$, $a_{12} = y$, and then

$$(2.2) \qquad A = \begin{bmatrix} x & y \\ \frac{-(x-1)^2}{y} & 2-x \end{bmatrix}.$$

Matrices of the two forms (2.1) and (2.2) cover all the elements in $\mathcal{SU}(1)$. The matrix $-I_2$ cannot be written as any product of form (2.1), since the set of all the matrices of form (2.2) is isomorphic to the additive group $\mathbb{C}$. Next we will prove that $-I_2$ cannot be written either as a product of one matrix of from (2.1) and another of form (2.2), or as a product of two matrices of form (2.2).

Case (1): If

$$-I_2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix} \cdot \begin{bmatrix} x & y \\ \frac{-(x-1)^2}{y} & 2-x \end{bmatrix},$$

then by comparing the (1,1)-entry, we get $x = -1$, by comparing the (2,1)-entry, we get $y = -4/a$, and by comparing the (2,2)-entry, we get $x = 5$, a contradiction.

The proof of

$$-I_2 \neq \begin{bmatrix} x & y \\ \frac{-(x-1)^2}{y} & 2-x \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix}$$

for any a, x, y is similar.

Case (2): We will prove $-I_2$ cannot be written as a product of two matrices of form (2.2). Set

$$B = \begin{bmatrix} p & q \\ \frac{-(p-1)^2}{q} & 2-p \end{bmatrix}$$

and $C = A \cdot B$. Then, we have

$$C = \begin{bmatrix} xp - \frac{y(p-1)^2}{q} & xq + y(2-p) \\ -\frac{p(x-1)^2}{y} + \frac{(x-2)(p-1)^2}{q} & -\frac{q(x-1)^2}{y} + (2-x)(2-p) \end{bmatrix}.$$

If we require $c_{12} = c_{21} = 0$, we can deduce that $p = x$, $q = \frac{x-2}{x}y$. Under this condition, we have $c_{11} = (c_{22})^{-1} = \frac{x}{2-x}$, which can never equal -1. $\qquad \square$

Now we begin to deal with the Jordan blocks in the Symplectic Jordan Canonical Form.

LEMMA 2.9. $J_k(1) \oplus J_k(1)^{-T} \in \mathcal{SU}(2)$.

Proof. For each natural number k, we define two $k \times k$ matrices:

$$R_k = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \oplus \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \ \ S_k = [1] \oplus \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \oplus \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \oplus [1], \quad \text{if } k \text{ is even,}$$

$$R_k = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \oplus \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \oplus [1], \ \ S_k = [1] \oplus \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \oplus \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \text{if } k \text{ is odd.}$$

One checks that $(RS) \oplus (RS)^{-T} = (R \oplus R^{-T})(S \oplus S^{-T})$. It is similar to $J_k(1) \oplus J_k(1)^{-T}$ by calculating the rank of $RS - I$. Since $R \oplus R^{-T} \in \mathcal{SU}(1)$, $S \oplus S^{-T} \in \mathcal{SU}(1)$. According to Lemma 2.3, we have $J_k(1) \oplus J_k(1)^{-T} \in \mathcal{SU}(2)$. $\qquad \square$

LEMMA 2.10. $J_k(\lambda) \oplus J_k(\lambda)^{-T}$ $(\lambda \neq 0)$ *is a product of three symplectic unipotent matrices of index* 2.

Proof. Case (1): If $\lambda^k \neq -1$, according to Lemma 2.4, we have the decomposition:

$$J_k(\lambda) = UB,$$

where B is similar to $J_{k-1}(1) \oplus [\lambda^k]$. Therefore,

$$J_k(\lambda) \oplus J_k(\lambda)^{-T} = (U \oplus U^{-T}) \cdot (B \oplus B^{-T}),$$

where $B \oplus B^{-T}$ is symplectically similar to

$$(J_{k-1}(1) \oplus [\lambda^k]) \oplus (J_{k-1}(1)^{-T} \oplus [\lambda^{-k}]) = \left((J_{k-1}(1) \oplus J_{k-1}(1)^{-T}) \boxplus ([\lambda^k] \oplus [\lambda^{-k}]) \right).$$

According to Lemma 2.6, $[\lambda^k] \oplus [\lambda^{-k}]$ belongs to $\mathcal{SU}(2)$. According to Lemma 2.9, $J_{k-1}(1) \oplus J_{k-1}(1)^{-T}$ belongs to $\mathcal{SU}(2)$. Thus, $B \oplus B^{-T} \in \mathcal{SU}(2)$ by Remark 2.1. Since $U \oplus U^{-T}$ is a symplectic unipotent matrix of index 2 itself, $J_k(\lambda) \oplus J_k(\lambda)^{-T}$ can be decomposed into a product of three symplectic unipotent matrices of index 2 in this case.

Case (2): If $\lambda^k = -1$, let a be an arbitrary complex number other than ± 1. Using Lemma 2.4, we can similarly conclude that:

$$J_k(\lambda) \oplus J_k(\lambda)^{-T} = (U \oplus U^{-T}) \cdot (B \oplus B^{-T}),$$

where $B \oplus B^{-T}$ is symplectically similar to

$$(J_{k-2}(1) \oplus [a] \oplus [-a^{-1}]) \oplus (J_{k-1}(1)^{-T} \oplus [a^{-1}] \oplus [-a])$$
$$= \left((J_{k-2}(1) \oplus J_{k-2}(1)^{-T}) \boxplus ([a] \oplus [a^{-1}]) \boxplus ([-a^{-1}] \oplus [-a]) \right).$$

According to Lemma 2.6, $[a] \oplus [a^{-1}]$ and $[-a^{-1}] \oplus [-a]$ belong to $\mathcal{SU}(2)$. According to Lemma 2.9, $J_{k-2}(1) \oplus J_{k-2}(1)^{-T} \in \mathcal{SU}(2)$. Thus, by Remark 2.1, $B \oplus B^{-T} \in \mathcal{SU}(2)$. Therefore, $J_k(\lambda) \oplus J_k(\lambda)^{-T} \in \mathcal{SU}(3)$. $\quad\square$

By Lemma 2.10, we have the following corollary for the second kind of Jordan blocks of the Symplectic Jordan Canonical Form in Lemma 2.2.

COROLLARY 2.11. $J_{2k+1}(\lambda) \oplus J_{2k+1}(\lambda)^{-T} (\lambda \in \{\pm 1\})$ *is a product of three symplectic unipotent matrices of index* 2.

LEMMA 2.12. $\varepsilon(k)$ *is a product of three symplectic unipotent matrices of index* 2.

Proof. Denote by E_{ij} the matrix with the unique nonzero entry equal to 1 in the position (i, j). We can write $\varepsilon(k) = (J_k(1) \oplus J_k(1)^{-T}) \cdot P$, where $P = \begin{bmatrix} I_k & E_{kk} \\ 0 & I_k \end{bmatrix} \in \mathcal{SU}(1)$. According to Lemma 2.9, $J_k(1) \oplus J_k(1)^{-T}$ belongs to $SU(2)$. Thus, $\varepsilon(k) \in \mathcal{SU}(3)$. $\quad\square$

LEMMA 2.13. $-\varepsilon(k)$ *is a product of three symplectic unipotent matrices of index* 2.

Proof. Case (1): k is even. Suppose that $k = 2m$. Set

$$S = \underbrace{B \boxplus \cdots \boxplus B}_{m}, \quad \text{where } B = J_2(-1)^{-1} \oplus J_2(-1)^T.$$

By Lemma 2.7, $B \in \mathcal{SU}(2)$. By Remark 2.1 (b), $S \in \mathcal{SU}(2)$. Set

$$T = I_2 \boxplus \underbrace{C \boxplus \cdots \boxplus C}_{m-1} \boxplus J_2(1), \quad \text{where } C = J_2(1) \oplus J_2(1)^{-T}.$$

Xin Hou, Zhengyi Xiao, Yajing Hao, and Qi Yuan

By Remark 2.1 (b), $T \in \mathcal{SU}(1)$. Let $R = ST$. Then $R \in \mathcal{SU}(3)$, since $S \in \mathcal{SU}(2)$ and $T \in \mathcal{SU}(1)$.

Now we claim that $-\varepsilon(k)$ is similar to R. Observing that $-\varepsilon(k)$ has only one eigenvalue -1, and that $\operatorname{rank}(-\varepsilon(k) + I) = 2k - 1$, we can deduce that $-\varepsilon(k)$ is similar to $J_{2k-1}(-1)$ (not necessarily symplectically similar). Similarly, R also satisfies these conditions, therefore similar to $J_{2k-1}(-1)$ as well (not necessarily symplectically similar as well). Thus, we can conclude that the two symplectic matrices $-\varepsilon(k)$ and R are similar. According to Lemma 2.3, we can draw the conclusion that the two matrices are symplectically similar. Since $R \in \mathcal{SU}(3)$, $-\varepsilon(k) \in \mathcal{SU}(3)$ as well by Remark 2.1 (a).

Case (2): k is odd. Suppose that $k = 2m + 1$. Set

$$S = \underbrace{B \boxplus \cdots \boxplus B}_{m} \boxplus J_2(-1)^{-1}, \quad \text{where } B = J_2(-1)^{-1} \oplus J_2(-1)^{T}.$$

By Lemma 2.7 and Remark 2.1 (b), $S \in \mathcal{SU}(2)$. Set

$$T = I_2 \boxplus \underbrace{C \boxplus \cdots \boxplus C}_{m}, \quad \text{where } C = J_2(1) \oplus J_2(1)^{-T}.$$

According to Remark 2.1 (b), $T \in \mathcal{SU}(1)$. Let $R = ST$. By using R, the proof when k is odd is almost identical to that when k is even. □

Now we can prove our main result.

Proof of Theorem 1.1. An arbitrary symplectic matrix A is symplectically similar to the canonical form in Lemma 2.2. According to Remark 2.1, we only need to prove the result for each matrix block in Lemma 2.2. The conclusion that $J_k(\lambda) \oplus J_k(\lambda)^{-T} (\lambda \notin \{0, \pm 1\}) \in \mathcal{SU}(3)$ is proved in Lemma 2.10. That $J_{2k+1}(\lambda) \oplus J_{2k+1}(\lambda)^{-T} (\lambda \in \{\pm 1\}) \in \mathcal{SU}(3)$ is given in Corollary 2.11. That $\pm\varepsilon(k) \in \mathcal{SU}(3)$ is proved respectively in Lemma 2.12 and Lemma 2.13. Hence, every complex symplectic matrix can be decomposed into a product of three symplectic unipotent matrices of index 2 and from Lemma 2.8 (b) we can conclude that three is the smallest such number, since $-I_2$ cannot be decomposed into a product of two symplectic unipotent matrices of index 2. □

REFERENCES

[1] M. Benzi and N. Razouk. On the Iwasawa decomposition of a symplectic matrix. *Appl. Math. Lett.*, 20:260–265, 2007.

[2] R.J. de la Cruz. Each symplectic matrix is a product of four symplectic involutions. *Linear Algebra Appl.*, 466:382–400, 2015.

[3] R.J. de la Cruz and D.Q. Granario. Products of symplectic normal matrices. *Linear Algebra Appl.*, 543:162–172, 2018.

[4] C.K. Fong and A.R. Sourour. The group generated by unipotent operators. *Proc. Amer. Math. Soc.*, 97:453–458, 1986.

[5] R.A. Horn and D.I. Merino. Contragredient equivalence: A canonical form and some applications. *Linear Algebra Appl.*, 214:43–92, 1995.

[6] J.-H. Wang and P.Y. Wu. Products of unipotent matrices of index 2. *Linear Algebra Appl.*, 149:111–123, 1991.

[7] H. You. Commutators and unipotents in symplectic groups. *Acta Math. Sinica (N.S.)*, 10:173–179, 1994.