Yet more elementary proofs that the determinant of a symplectic matrix is 1

F. Bünger[a], S.M. Rump[a,b]

[a]*Institute for Reliable Computing, Hamburg University of Technology, Am Schwarzenberg-Campus 3, Hamburg 21071, Germany*
[b]*Faculty of Science and Engineering, Waseda University, 3-4-1 Okubo, Shinjuku-ku, Tokyo 169-8555, Japan*

Abstract

It seems to be of recurring interest in the literature to give alternative proofs for the fact that the determinant of a symplectic matrix is one. We state four short and elementary proofs for symplectic matrices over general fields. Two of them seem to be new.

Keywords: symplectic matrix, determinant, transvection, isometry
2010 MSC: 15B57, 65F40, 11C20, 51A50

1. Introduction

Let $\mathbb{K}$ be a field and $n \in \mathbb{N} := \{1, 2, \ldots\}$. A matrix $S \in \mathbb{K}^{2n\times 2n}$ is called J-symplectic if

$$S^T JS = J \tag{1}$$

for regular and skew-symmetric $J \in \mathbb{K}^{2n\times 2n}$, i.e., $J^T = -J$. If the characteristic char($\mathbb{K}$) of the field $\mathbb{K}$ is two, i.e., if $1 = -1$, then $J^T = J$, and additionally $J_{i,i} = 0$

Email addresses: `florian.buenger@tuhh.de` (F. Bünger), `rump@tuhh.de` (S.M. Rump)

for all $i \in \{1, \ldots, 2n\}$ is assumed in this case. The symplectic (matrix) group[1]

$$\mathrm{Sp}(J) := \mathrm{Sp}(2n, \mathbb{K}) := \{S \in \mathbb{K}^{2n\times 2n} \mid S^T J S = J\} \tag{2}$$

is, up to isomorphism, independent of the particular choice of J.[2] In matrix theory often

$$J := \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \tag{3}$$

is taken as the default, where $I := I_n \in \mathbb{K}^{n\times n}$ is the identity matrix of order n. Clearly, (1) immediately gives

$$(\det S)^2 \det J = \det(S^T J S) = \det J$$

so that $\det J \neq 0$ implies $\det S \in \{-1, 1\}$. It is one of the basic, well-known facts on symplectic matrices that

$$\det S = 1 \quad \text{for all } S \in \mathrm{Sp}(2n, \mathbb{K}). \tag{4}$$

Note that this is trivial for $\mathrm{char}(\mathbb{K}) = 2$ since then $1 = -1$, but for $\mathrm{char}(\mathbb{K}) \neq 2$ it is not obvious. In text books on classical groups like [1] or [15] this result is mostly stated as a corollary of another basic fact, namely that the symplectic group is generated by so-called symplectic transvections, i.e., each $S \in \mathrm{Sp}(2n, K)$ can be written as a product

$$S = \prod_{i=1}^{r} E_i \tag{5}$$

[1] The first notion of symplectic groups goes back to Jordan [9] in 1870, where in §VIII, p.171, he calls these groups 'groupes abélien', a name which was not yet occupied by commutative groups at that time. Later, in 1901, Dickson [6], Chapter II, p. 89, called these groups 'abelien linear groups'. The nowadays used name 'symplectic group' was invented by Weyl [16] in 1939. It is a Greek word for the Latin word 'complex' which was already occupied in mathematics by the complex numbers, see [11] for more history on symplectic geometry. The name 'symplectic group' was later used and made public by Dieudonné [3], [4] and also by van der Waerden in his famous books on modern algebra.

[2] For another skew-symmetric $\tilde{J} \in \mathbb{K}^{2n\times 2n}$, with $\tilde{J}_{ii} = 0$ if $\mathrm{char}(\mathbb{K}) = 2$, there always exists a regular matrix A such that $\tilde{J} = A^T J A$ with the property that S is J-symplectic, if, and only if, $\tilde{S} := A^{-1} S A$ is $\tilde{J}$-symplectic. The conjugation by A, i.e., the mapping $\mathrm{Sp}(J) \to \mathrm{Sp}(\tilde{J})$, $S \mapsto A^{-1} S A$ is a group isomorphism which does not change determinants, i.e., $\det S = \det(A^{-1} S A)$ for all $S \in \mathrm{Sp}(J)$.

of transvections $E_i \in \mathrm{Sp}(2n, \mathbb{K})$, $i = 1, ..., r$, $r \in \mathbb{N}$. A symplectic transvection has the form

$$E = E_{\alpha,v} := I + \alpha v v^T J, \quad \alpha \in \mathbb{K}\backslash\{0\},\ v \in \mathbb{K}^{2n}\backslash\{0\}, \tag{6}$$

where in this formula $I = I_{2n}$ denotes the identity matrix of order $2n$. Since $v^T J v = 0$,

$$E^T J E \ := \ (I - \alpha J v v^T) J (I + \alpha v v^T J) = J - \alpha^2 J v (v^T J v) v^T J = J$$

shows that a symplectic transvection is indeed a symplectic matrix. From $E_{\alpha,v} E_{-\alpha,v} = I - \alpha^2 v (v^T J v) v^T J = I$ it follows that $E_{\alpha,v}^{-1} = E_{-\alpha,v}$ is again a symplectic transvection. Moreover, $(E - I)^2 = \alpha^2 v (v^T J v) v^T J = 0$ implies that all eigenvalues of E are one so that $\det E = 1$. Hence, (5) implies $\det S = 1$.

The fact that transvections have determinant 1 can also be derived in an elementary way as follows. A transvection is a rank-1 update of the identity matrix, so

$$\begin{pmatrix} I & 0 \\ w^T & 1 \end{pmatrix} \begin{pmatrix} I + u w^T & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} I & 0 \\ -w^T & 1 \end{pmatrix} = \begin{pmatrix} I & u \\ 0 & 1 + w^T u \end{pmatrix}$$

shows for $u := \alpha v$ and $w^T := v^T J$ that $\det E_{\alpha,v} = 1 + \alpha v^T J v = 1$.

It is not known to the authors who discovered first that symplectic groups are solely generated by transvections. This became nowadays some kind of common knowledge.[3] An elementary short proof in matrix notation is stated in Section 4. In this context we want to mention the famous papers by Dieudonné [5] and Callan [2], where moreover the minimum number r of factors in a representation (5) is determined. These papers are much more involved.

Another standard proof of the determinant property (4) uses the identity $\mathrm{Pf}(J) = \mathrm{Pf}(S^T J S) = \det(S)\mathrm{Pf}(J)$ on Pfaffians and $\mathrm{Pf}(J) \neq 0$. However, a more direct proof seems to be of recurring interest, see [10], [7], [12].

We contribute two elementary short proofs in Section 2. To the best of our knowledge these proofs seem to be new. In Section 3 we give yet another elementary short proof based on Jordan normal forms. This is in principle known but

[3] This knowledge goes back to the very first notion of symplectic groups by Jordan [9]. There, in Theorem 221, p. 174, Jordan proved for $\mathbb{K} = \mathbf{GF}(p)$ that the symplectic group is generated by a little bit different set of generators containing symplectic transvections. Since it can easily be seen that all these generators have determinant one, Jordan already deduced (4) in a remark on p. 176. The same result was more or less repeated by Dickson[6], Theorem 114, p. 92, for $\mathbb{K} = \mathbf{GF}(p^m)$, $m \in \mathbb{N}$.

we are not aware of a short and concise statement in the literature that is valid for arbitrary fields. Therefore we considered such a proof also as noteworthy.

2. Proof by block determinants

For preparation, the following trivial lemma is proven by elementary linear algebra.

Lemma 1. *Let $M \in \mathbb{K}^{n\times n}$.*

a) *M is equivalent to $D := \operatorname{diag}(I_m, 0_{n-m})$, that is, there are regular $A, B \in \mathbb{K}^{n\times n}$ such that $AMB = D$, where I_m is the identity matrix of order $m := \operatorname{rank}(M)$ and 0_{n-m} is the zero matrix of order $n-m$.*[4]

b) *There is regular $R \in \mathbb{K}^{n\times n}$ such that MR is symmetric, i.e., $MR = R^T M^T$.*

Proof: a) Let P be a permutation matrix such that the first m columns of $MP = [M_1, M_2]$, $M_1 \in \mathbb{K}^{n,m}$, $M_2 \in \mathbb{K}^{n,n-m}$, are linearly independent. The columns of M_1 can be extended to a basis of $\mathbb{K}^n$, i.e., there is a $M_3 \in \mathbb{K}^{n,n-m}$ such that $Q := [M_1, M_3]$ is regular. Now $I = Q^{-1}Q = [Q^{-1}M_1, Q^{-1}M_3]$ means $Q^{-1}M_1 = \begin{pmatrix} I_m \\ 0 \end{pmatrix}$ so that $M' := Q^{-1}MP = [Q^{-1}M_1, Q^{-1}M_2] = \begin{pmatrix} I_m & U \\ 0 & V \end{pmatrix}$ for suitable $U \in \mathbb{K}^{m,n-m}$ and $V \in \mathbb{K}^{n-m,n-m}$. Since M and M' have the same rank, necessarily $V = 0$ must hold true. The matrix $R := \begin{pmatrix} I_m & -U \\ 0 & I_{n-m} \end{pmatrix}$ is regular and fulfills

$$Q^{-1}MPR = M'R = \begin{pmatrix} I_m & U \\ 0 & 0 \end{pmatrix}\begin{pmatrix} I_m & -U \\ 0 & I_{n-m} \end{pmatrix} = \begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix} .$$

Thus, assertion a) holds true for $A := Q^{-1}$ and $B := PR$.

b) By a) there are regular A and B such that $AMB = \operatorname{diag}(I_m, 0_{n-m}) =: D$. The matrix $R := BA^{-T}$ is regular and $MR = A^{-1}AMBA^{-T} = A^{-1}DA^{-T}$ is symmetric. □

For proving (4), we take J as defined in (3) and $S \in \operatorname{Sp}(2n, \mathbb{K})$. The partition $S = \begin{pmatrix} V & W \\ X & Y \end{pmatrix}$ implies

$$S^TJS = \begin{pmatrix} V^T & X^T \\ W^T & Y^T \end{pmatrix}\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\begin{pmatrix} V & W \\ X & Y \end{pmatrix} = \begin{pmatrix} V^T & X^T \\ W^T & Y^T \end{pmatrix}\begin{pmatrix} X & Y \\ -V & -W \end{pmatrix} = J,$$

[4]Note that this is obvious if a singular value decomposition is at hand, such as for $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$.

so that

$$V^T X = X^T V \qquad \text{and} \qquad W^T Y = Y^T W \qquad \text{and} \qquad Y^T V - W^T X = I. \tag{7}$$

2.1. *Proof I*

If V is the zero matrix, then the partition of S and the last equality in (7) imply

$$\det S = (-1)^n \det W \det X = (-1)^n \det W^T X = (-1)^n \det(-I) = 1.$$

Henceforth, we may assume that $m := \operatorname{rank}(V) > 0$. By Lemma 1 a) applied to $M := V$ there are regular matrices $A, B \in \mathbb{K}^{n\times n}$ such that $D := AVB = \operatorname{diag}(I_m, 0_{n-m})$. The matrices $\widehat{A} := \operatorname{diag}(A, A^{-T})$ and $\widehat{B} := \operatorname{diag}(B, B^{-T})$ are symplectic, and so is $\widehat{S} := \widehat{A}S\widehat{B} = \begin{pmatrix} D & * \\ * & * \end{pmatrix}$. Moreover, $\det \widehat{S} = \det S$ by $\det \widehat{A} = 1 = \det \widehat{B}$. Thus, w.l.o.g. we may assume that $\widehat{S} = S$, i.e., $V = D$. The first equality in (7) yields

$$(X^T V)^T = X^T V = \begin{pmatrix} X_{11}^T & X_{21}^T \\ X_{12}^T & X_{22}^T \end{pmatrix} \begin{pmatrix} I_m & \\ & 0 \end{pmatrix} = \begin{pmatrix} X_{11}^T & 0 \\ X_{12}^T & 0 \end{pmatrix} = \begin{pmatrix} X_{11} & X_{12} \\ 0 & 0 \end{pmatrix}.$$

Hence,

$$X_{11}^T = X_{11} \qquad \text{and} \qquad X_{12} = 0 \qquad \text{and} \qquad X = \begin{pmatrix} X_{11} & 0 \\ X_{21} & X_{22} \end{pmatrix}. \tag{8}$$

Since J itself is symplectic, also $S^T = JS^{-1}J^{-1}$ is symplectic so that the same argument gives $W = \begin{pmatrix} W_{11} & W_{12} \\ 0 & W_{22} \end{pmatrix}$. The third equality of (7) supplies

$$I = Y^T V - W^T X = \begin{pmatrix} Y_{11}^T & Y_{21}^T \\ Y_{12}^T & Y_{22}^T \end{pmatrix} \begin{pmatrix} I_m & \\ & 0 \end{pmatrix} - \begin{pmatrix} W_{11}^T & 0 \\ W_{12}^T & W_{22}^T \end{pmatrix} \begin{pmatrix} X_{11} & 0 \\ X_{21} & X_{22} \end{pmatrix}$$

wherefore

$$W_{22}^T X_{22} = -I_{n-m} \qquad \text{and} \qquad Y_{11}^T - W_{11}^T X_{11} = I_m. \tag{9}$$

Using the Schur complement, the first equality of (8), and (9) we finally compute:

$$
\begin{aligned}
\det S &= \det\left(\begin{array}{c|ccc} I_m & 0 & W_{11} & W_{12} \\ \hline 0 & 0 & 0 & W_{22} \\ X_{11} & 0 & Y_{11} & Y_{12} \\ X_{21} & X_{22} & Y_{21} & Y_{22} \end{array}\right) = \det\left(\begin{pmatrix} 0 & 0 & W_{22} \\ 0 & Y_{11} & Y_{12} \\ X_{22} & Y_{21} & Y_{22} \end{pmatrix} - \begin{pmatrix} 0 \\ X_{11} \\ X_{21} \end{pmatrix}\begin{pmatrix} 0 & W_{11} & W_{12} \end{pmatrix}\right) \\
&= \det\begin{pmatrix} 0 & 0 & W_{22} \\ 0 & Y_{11} - X_{11}W_{11} & * \\ X_{22} & * & * \end{pmatrix} = (-1)^{n-m} \det\begin{pmatrix} W_{22} & * & * \\ 0 & Y_{11} - X_{11}W_{11} & * \\ 0 & 0 & X_{22} \end{pmatrix} \\
&= (-1)^{n-m} \det W_{22} \det(Y_{11} - X_{11}W_{11}) \det X_{22} \\
&= (-1)^{n-m} \det(W_{22}^T X_{22}) \det(Y_{11}^T - W_{11}^T X_{11}) = (-1)^{n-m} \det(-I_{n-m}) \det I_m = 1,
\end{aligned}
$$

where the fourth equality uses that W_{22} and X_{22} are matrices of order $n - m$. □

2.2. *Proof II*

Contrary to Proof I the following proof avoids the subdivision of the four subblocks V, W, X, Y of S by using a trick like in [14]. [5]

By Lemma 1 b) applied to $M := W^T$ there is a regular matrix $R \in \mathbb{K}^{n\times n}$ such that $W^T R = R^T W$. We will work in the commutative polynomial ring $\mathbb{K}[x]$. Define $Y_x := Y + xR \in \mathbb{K}[x]^{n\times n}$ and $S_x := \begin{pmatrix} V & W \\ X & Y_x \end{pmatrix}$. Using (7) we obtain $Y_x^T W = Y^T W + xR^T W = W^T Y + xW^T R = W^T Y_x$ and

$$
\begin{pmatrix} Y_x^T & -W^T \\ 0 & I \end{pmatrix}\begin{pmatrix} V & W \\ X & Y_x \end{pmatrix} = \begin{pmatrix} Y_x^T V - W^T X & Y_x^T W - W^T Y_x \\ X & Y_x \end{pmatrix} = \begin{pmatrix} Y_x^T V - W^T X & 0 \\ X & Y_x \end{pmatrix}.
$$

Therefore, $\det Y_x \det S_x = \det(Y_x^T V - W^T X) \det Y_x$, i.e.,

$$
\left(\det S_x - \det(Y_x^T V - W^T X)\right) \det Y_x = 0. \tag{10}
$$

Now, $\det Y_x = \det(Y + xR) = \det(xI - (-YR^{-1})) \det R$ is the $\det R$-multiple (and thus a nonzero-multiple) of the characteristic polynomial of $-YR^{-1}$. Hence, $\det Y_x$

---

[5] Silvester [14] proved that a block matrix $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbb{K}^{2n\times 2n}$, $A, B, C, D \in \mathbb{K}^{n\times n}$, has determinant $\det M = \det(AD - BC)$ if C and D commute, i.e., if $CD = DC$. The key idea in his proof is to substitute D by $D_x := D + xI$ and to use a Schur complement-like formula for the determinant in the polynomial ring $\mathbb{K}[x]$. Actually this trick was implicitly already done by Schur [13], p. 216-217, thanks to P. Batra for pointing to this reference.

is not the zero polynomial, so that (10) implies $\det S_x - \det(Y_x^T V - W^T X) = 0$. Thus, the polynomials $\det S_x$ and $\det(Y_x^T V - W^T X)$ are identical. Evaluating at $x = 0$ and using the third equality in (7) gives

$$\det S = \det(Y^T V - W^T X) = \det I = 1. \qquad \square$$

3. Proof by Jordan decomposition

The following lemma is an elementary first step in the course of determining the normal forms of isometries, see [8], 'Hilfssatz' 8.5, p. 567.[6]

Lemma 2. *Let $S \in \mathrm{Sp}(2n, \mathbb{K})$, and let $p, q \in \mathbb{K}[x]\backslash\{0\}$ be polynomials such that $p^*(x) := x^{\deg(p)} p(x^{-1})$ and q are relatively prime to each other in $\mathbb{K}[x]$. Then $v^T J w = 0$ for all $v \in \mathrm{kern}(p(S))$ and all $w \in \mathrm{kern}(q(S))$.*

Proof: Set $d := \deg(p)$. The assumption $\gcd(p^*, q) = 1$ supplies polynomials $r, s \in \mathbb{K}[x]$ such that $rp^* + sq = 1$. For $v \in \mathrm{kern}(p(S))$ and $w \in \mathrm{kern}(q(S))$ we use $S^T J = JS^{-1}$ to compute:

$$\begin{aligned} 0 &= (p(S)v)^T JS^d r(S)w = v^T p(S^T) JS^d r(S) w = v^T JS^d p(S^{-1}) r(S) w \\ &= v^T J p^*(S) r(S) w = v^T J(p^*(S) r(S) + s(S) q(S)) w = v^T J w. \end{aligned} \qquad \square$$

The third proof of (4) does not need that J has the default form (3).

Rewriting $S^T JS = J$ as $S^{-1} = J^{-1} S^T J$ for $S \in \mathrm{Sp}(2n, \mathbb{K})$ shows that S^T is similar to S^{-1}. Since every quadratic matrix is similar to its transpose, S is similar to S^{-1}. Hence, in a Jordan decomposition in a decomposition field $\mathbb{F}$ of the characteristic polynomial $\chi_S(x) = \det(xI - S)$, each Jordan block for an eigenvalue $\alpha \in \mathbb{F}\backslash\{-1, 1\}$ has a corresponding distinct Jordan block of the same size for the eigenvalue $\alpha^{-1} \neq \alpha$. Thus, those Jordan blocks for eigenvalues $\alpha \neq \pm 1$ produce a subdeterminant one.

Clearly the Jordan blocks for the eigenvalue 1 also produce a subdeterminant one, so that it remains to show that the Jordan blocks for the eigenvalue -1 produce a subdeterminant one.

[6] A complete classification of the normal forms of symplectic (and also orthogonal and unitary) isometries over arbitrary fields is given in [8], 'Hauptsatz' 8.9, p. 570. From that classification the determinant property (4) follows immediately, however, this would mean to use a sledgehammer to crack a nut.

Let $m \in \mathbb{N}$ be the sum of the sizes of all such Jordan blocks, i.e., m is the algebraic multiplicity of the eigenvalue -1. Then $p := (x+1)^m$ divides $\chi_S(x)$ and $q := \chi_S(x)/p$ is not divisible by $x+1$. Hence, $p^* = p$ and q are relatively prime to each other, and Lemma 2 yields that $U := \operatorname{kern}(p(S))$ and $V := \operatorname{kern}(q(S))$ are J-perpendicular, i.e., $u^T J v = 0$ for all $u \in U$ and $v \in V$. Since $U \oplus V = \mathbb{K}^{2n}$, necessarily U is J-regular, meaning that for an arbitrary basis $u_1, \ldots, u_m$ of U the Gramian matrix $\widehat{J} := (u_i^T J u_j)_{1 \leqslant i,j \leqslant m}$ is regular. Since $\widehat{J}$ is skew-symmetric (with $\widehat{J}_{i,i} = 0$ for all i if $\operatorname{char}(\mathbb{K}) = 2$), m must necessarily be even. Hence, the Jordan blocks for the eigenvalue -1 produce a subdeterminant $(-1)^m = 1$. Therefore, $\det S = 1$. □

4. Proof by generating transvections

Finally, as mentioned in the introduction, we give a short and elementary proof that every $S \in \mathrm{Sp}(2n, \mathbb{K})$ is a product of symplectic transvections. As noted in the introduction, symplectic transvections have determinant 1, so that $\det S = 1$ follows. For the fourth proof it is also not needed that J has the default form (3).

The proof proceeds by induction on $m := \operatorname{rank}(S - I)$, where I is the identity matrix of order $2n$ in this section. If $m = 0$, then $S = I$. As noted in the introduction, the inverse E^{-1} of a symplectic transvection E is again a symplectic transvection so that $S = I = EE^{-1}$ is the product of two symplectic transvections. Now let $m > 0$. Then $S \neq I$ and there is a $u \in \mathbb{K}^{2n}$ such that $v := (S - I)u \neq 0$. Consider a symplectic transvection $E := I + \alpha v v^T J$, $\alpha \in \mathbb{K} \backslash \{0\}$. If w is fixed by S, then it is also fixed by S^{-1}, wherefore

$$v^T J w = u^T S^T J w - u^T J w = u^T J S^{-1} w - u^T J w = 0$$

implies $ESw = Ew = w + v^T J w = w$. Thus, we conclude that for all $u \in \mathbb{K}^{2n}$ with $v := (S - I)u \neq 0$ and all $\alpha \in \mathbb{K} \backslash \{0\}$ the transvection $E := I + \alpha v v^T J$ fulfills

$$\operatorname{kern}(S - I) \subseteq \operatorname{kern}(ES - I). \tag{11}$$

Case 1: There exists $u \in \mathbb{K}^{2n}$ such that $\alpha := u^T J S u \neq 0$. In particular this means that $Su \neq u$ or equivalently $v := (S - I)u \neq 0$. Take $E := I + \alpha^{-1} v v^T J$ and use $(Su)^T J (Su) = 0$ to compute

$$ESu \;=\; Su + \alpha^{-1} v v^T J S u = Su - \alpha^{-1} v (u^T J S u) = Su - v = u.$$

Thus, u is fixed by $S' := ES$ but not by S. Using (11) we see that

$$\mathrm{kern}(S - I) \oplus \mathbb{K}u \subseteq \mathrm{kern}(S' - I)$$

so that $m' := \mathrm{rank}(S' - I) < \mathrm{rank}(S - I) = m$. By induction S' is a product of symplectic transvections and therefore also S.

Case 2: $u^T JS u = 0$ for all $u \in \mathbb{K}^{2n}$. Then JS is skew-symmetric since

$$0 = (u + v)^T JS(u + v) = v^T JS u + u^T JS v$$

for all $u, v \in \mathbb{K}^{2n}$. Thus, $-JS = (JS)^T = S^T J^T = -S^T J = -JS^{-1}$ shows that $S^2 = I$, i.e., S is an involution. Take some $u \in \mathbb{K}^n$ with $v := (S - I)u \neq 0$ and set $E := I + vv^T J$ and $S' := ES$. By (11), $m' := \mathrm{rank}(S' - I) \leqslant \mathrm{rank}(S - I) = m$. Since JS is regular, there is some $w \in \mathbb{K}^n$ such that $\beta := v^T JS w \neq 0$. By assumption $w^T JS w = 0$, and using $S^T J = JS^{-1} = JS$ and $0 = S^2 - I = (S - I)(S + I)$ we deduce

$$\begin{aligned}
\alpha &:= w^T JS' w = w^T JS w + w^T Jv(v^T JS w) = \beta w^T Jv = -\beta v^T Jw \\
&= -\beta(v^T J(S + I)w - v^T JS w) = -\beta u^T (S^T - I)J(S + I)w + \beta^2 \\
&= -\beta u^T J(S - I)(S + I)w + \beta^2 = \beta^2 \neq 0.
\end{aligned}$$

Hence, S' fulfills the assumption of Case 1 with $u := w$ and we may proceed as before to find a second symplectic transvection E' with

$$m'' := \mathrm{rank}(E'ES) = \mathrm{rank}(E'S') < m' \leqslant m.$$

By induction $E'ES$ is a product of transvections, and so is S. □

5. Acknowledgement

The authors would like to thank an anonymous referee for helpful comments.

References

[1] E. Artin. *Geometric Algebra*. Wiley Interscience Publishers, INC., New York, Wiley Classics Library Edition, 1988.

[2] D. Callan. The Generation of $\mathrm{Sp}(\mathbb{F}_2)$ by Transvections. *Journal of Algebra*, 42, 378-390, 1976.

[3] J. Dieudonné. *Sur les groupes classiques*. Hermann, Paris, 1948.

[4] J. Dieudonné. *La géométries des groupes classiques*. Springer, Berlin et al., 1955.

[5] J. Dieudonné. Sur les générateurs des groupes classiques. *Summa Bras. Mathem.*, 3, 149-178, 1955.

[6] L.E. Dickson. *Linear groups, with an exposition of the Galois Field theory*. Teubner, Leipzig, 1901.

[7] F.M. Dopico, C.R. Johnson. Complementary bases in symplectic matrices and a proof that their determinant is one. *Linear Algebra Appl.*, 419, 772-778, 2006.

[8] B. Huppert. *Angewandte Lineare Algebra*. de Gruyter, Berlin, New York, 1990.

[9] C. Jordan. *Traité des substitutions et des équations algébriques*. Gauthier-Villars, Paris, 1870.

[10] D.S. Mackey, N. Mackey. On the determinant of symplectic matrices. Numerical Analysis Report No. 422, Manchester Center for Computational Mathematics, Manchester, England, 2003.

[11] C.-M. Marle. The inception of Symplectic Geometry: the works of Lagrange and Poisson during the years 1808-1810. *Letters in Mathematical Physics*, 90:3, doi:10.1007/s11005-009-0347-y, 2009.

[12] D. Rim. An Elementary Proof That Symplectic Matrices Have Determinant One. *arXiv:1505.04240v3 [math.HO]*, 2015.

[13] I. Schur. Über Potenzreihen, die im Innern des Einheitskreises beschränkt sind. *Journal für die reine und angewandte Mathematik*, 147, 205-232, 1917.

[14] J.R. Silvester. Determinants of Block Matrices. *Math. Gaz.*, 84(501), 460-467, 2000.

[15] D.E. Taylor. *The Geometry of the Classical Groups*. Heldermann Verlag, Berlin, 1992.

[16] H. Weyl. *The Classical Groups. Their Invariants and Representations*. Princeton University Press, Princeton, New Jersey, 1939.