

2003

## An algorithm that carries a square matrix into its transpose by an involutory congruence transformation

Dragomir Z. Djokovic  
djokovic@math.uwaterloo.ca

F. Szechtman

K. Zhao

Follow this and additional works at: <http://repository.uwyo.edu/ela>

---

### Recommended Citation

Djokovic, Dragomir Z.; Szechtman, F.; and Zhao, K.. (2003), "An algorithm that carries a square matrix into its transpose by an involutory congruence transformation", *Electronic Journal of Linear Algebra*, Volume 10.  
DOI: <https://doi.org/10.13001/1081-3810.1116>

This Article is brought to you for free and open access by Wyoming Scholars Repository. It has been accepted for inclusion in Electronic Journal of Linear Algebra by an authorized editor of Wyoming Scholars Repository. For more information, please contact [scholcom@uwyo.edu](mailto:scholcom@uwyo.edu).

## AN ALGORITHM THAT CARRIES A SQUARE MATRIX INTO ITS TRANSPOSE BY AN INVOLUTORY CONGRUENCE TRANSFORMATION\*

D.Ž. ĐOKOVIĆ<sup>†</sup>, F. SZECHTMAN<sup>‡</sup>, AND K. ZHAO<sup>§</sup>

**Abstract.** For any matrix  $X$  let  $X'$  denote its transpose. It is known that if  $A$  is an  $n$ -by- $n$  matrix over a field  $F$ , then  $A$  and  $A'$  are congruent over  $F$ , i.e.,  $XAX' = A'$  for some  $X \in \text{GL}_n(F)$ . Moreover,  $X$  can be chosen so that  $X^2 = I_n$ , where  $I_n$  is the identity matrix. An algorithm is constructed to compute such an  $X$  for a given matrix  $A$ . Consequently, a new and completely elementary proof of that result is obtained.

As a by-product another interesting result is also established. Let  $G$  be a semisimple complex Lie group with Lie algebra  $\mathfrak{g}$ . Let  $\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1$  be a  $\mathbf{Z}_2$ -gradation such that  $\mathfrak{g}_1$  contains a Cartan subalgebra of  $\mathfrak{g}$ . Then L.V. Antonyan has shown that every  $G$ -orbit in  $\mathfrak{g}$  meets  $\mathfrak{g}_1$ . It is shown that, in the case of the symplectic group, this assertion remains valid over an arbitrary field  $F$  of characteristic different from 2. An analog of that result is proved when the characteristic is 2.

**Key words.** Congruence of matrices, Transpose, Rational solution, Symplectic group.

**AMS subject classifications.** 11E39, 15A63, 15A22.

**1. Introduction.** Let  $F$  be a field and  $M_n(F)$  the algebra of  $n$ -by- $n$  matrices over  $F$ . For  $X \in M_n(F)$ , let  $X'$  denote the transpose of  $X$ . In a recent paper [5], the following theorem is proved.

**THEOREM 1.1.** *If  $A \in M_n(F)$ , then there exists  $X \in \text{GL}_n(F)$  such that*

$$(1.1) \quad XAX' = A'.$$

Subsequently, the first author of that paper was informed that this result was not new. Indeed, R. Gow [7] proved in 1979 the following result.

**THEOREM 1.2.** *If  $A \in \text{GL}_n(F)$ , then there exists  $X \in \text{GL}_n(F)$  such that  $XAX' = A'$  and  $X^2 = I_n$ .*

The latter theorem is much stronger than the former except that  $A$  is required to be nonsingular. This restriction was removed in [3], yielding

**THEOREM 1.3.** *If  $A \in M_n(F)$ , then there exists  $X \in \text{GL}_n(F)$  such that*

$$(1.2) \quad XAX' = A', \quad X^2 = I_n.$$

---

\*Received by the editors on 12 June 2003. Accepted for publication on 8 December 2003. Handling Editor: Robert Guralnick.

<sup>†</sup>Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada (djokovic@uwaterloo.ca). Research was supported in part by the NSERC Grant A-5285.

<sup>‡</sup>Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada. Current Address: Department of Mathematics and Statistics, University of Regina, Regina, Saskatchewan, S4S 0A2, Canada (szecht@math.uregina.ca).

<sup>§</sup>Institute of Mathematics, Academy of Mathematics and System Sciences, Chinese Academy of Sciences, Beijing 100080, P.R. China, and Department of Mathematics, Wilfrid Laurier University, Waterloo, Ontario, N2L 3C5, Canada (kzhao@mail2.math.ac.cn). Research supported by the NSF of China (Grant 10371120).

We point out that the proof of Theorem 1.1 in [5] and that of Theorem 1.2 in [7] are based on the previous work of C. Riehm [9]. In section 3 we shall indicate how Theorem 1.3 can be derived from Theorem 1.2 by means of a result of P. Gabriel [6] (as restated by W.C. Waterhouse in [11]).

In a certain sense, Theorem 1.1 is quite surprising (and so is Theorem 1.3). Indeed the matrix equation (1.1) is equivalent to a system of  $n^2$  quadratic equations in  $n^2$  variables  $x_{ij}$ , the entries of the matrix  $X = [x_{ij}]$ . There is no apparent reason why this system of quadratic equations should have a nonsingular rational solution, i.e., a solution  $X \in \text{GL}_n(F)$ . (Note that if  $A$  is nonsingular then (1.1) implies that  $\det(X) = \pm 1$ .)

Let us illustrate this point with an example. Say,  $n = 3$  and the given matrix is

$$A = \begin{bmatrix} a & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad a \neq 0.$$

Writing the unknown matrix  $X$  as

$$X = \begin{bmatrix} x & y & z \\ u & v & w \\ p & q & r \end{bmatrix},$$

the above mentioned system of quadratic equations is:

$$\begin{aligned} ax^2 + xy + yz &= a, & axu + xv + yw &= 0, \\ axp + xq + yr &= 0, & axu + yu + zv &= 1, \\ au^2 + uv + vw &= 0, & aup + uq + vr &= 0, \\ axp + yp + zq &= 0, & aup + vp + wq &= 1, \\ ap^2 + pq + qr &= 0. \end{aligned}$$

It is not obvious that this system has a nonsingular rational solution. Nevertheless such a solution exists, for instance the matrix

$$X = \begin{bmatrix} 2 & -a & 1 \\ 2a^{-1} & -1 & 2a^{-1} \\ -1 & a & 0 \end{bmatrix}$$

with determinant  $-1$ . In fact, we have  $X^2 = I_3$ .

The proofs of the first two theorems above are rather complicated and they neither explain why a nonsingular rational solution exists nor do they provide a simple method for finding such a solution. The main objective of this paper is to construct an algorithm for solving this problem, i.e., to prove the following theorem.

**THEOREM 1.4.** *For any field  $F$ , there exists an algorithm which solves the system (1.2). More precisely, the input of the algorithm is a positive integer  $n$  and an arbitrary matrix  $A \in M_n(F)$ , and the output is a matrix  $X \in \text{GL}_n(F)$  which is a solution of the system (1.2).*

The proof is given in section 4. We point out that we do not assume that there is an algorithm for factoring polynomials in  $F[t]$  into product of irreducible polynomials. The GCD-algorithm is sufficient. Our algorithm is applicable to arbitrary  $F$  and  $n$  and so we obtain a new proof of Theorem 1.3. This proof is completely elementary in the sense that it is independent from the work of Riehm and Gabriel and it uses only the standard tools of Linear Algebra and some elementary facts about the symplectic group.

We shall see that Theorem 1.3 is closely related to (the rational version of) a special case of a theorem of L.V. Antonyan on  $\mathbf{Z}_2$ -graded complex semisimple Lie algebras, which may seem surprising. Let us first state Antonyan's theorem [2, Theorem 2]:

**THEOREM 1.5.** *Let  $\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1$  be a  $\mathbf{Z}_2$ -graded complex semisimple Lie algebra and  $G$  a connected complex Lie group with Lie algebra  $\mathfrak{g}$ . Then the following are equivalent:*

- (i)  $\mathfrak{g}_1$  contains a Cartan subalgebra of  $\mathfrak{g}$ .
- (ii) Every  $G$ -orbit in  $\mathfrak{g}$  (under the adjoint action) meets  $\mathfrak{g}_1$ .

As a motivation for his theorem, Antonyan mentions the following well known fact: Every complex (square) matrix is similar to a symmetric one. On the other hand, the corresponding statement is utterly false for real matrices. We shall be concerned with another special case of Antonyan's theorem, namely the one dealing with the symplectic group. As we shall prove, in this case the rational version of his result is valid.

A matrix  $A = [a_{ij}] \in M_n(F)$  is said to be an *alternate* matrix if  $A' = -A$  and all diagonal entries  $a_{ii}$  are 0. Of course, the latter condition follows from the former if the characteristic of  $F$  is not two.

In the concrete matrix style, let us define the symplectic group  $\mathrm{Sp}_n(F)$ ,  $n = 2m$  even, over any field  $F$  by:

$$(1.3) \quad \mathrm{Sp}_n(F) = \{X \in \mathrm{GL}_n(F) : X' J X = J\},$$

where  $J \in M_n(F)$  is a fixed nonsingular alternate matrix. Recall that  $\mathrm{Sp}_n(F)$  acts on its Lie algebra

$$\mathfrak{sp}_n(F) = \{Z \in M_n(F) : Z' J + J Z = 0\}$$

via the adjoint action  $(X, Z) \rightarrow X Z X^{-1}$ . It also acts on the space  $\mathrm{Sym}_n(F)$  of symmetric matrices  $S \in M_n(F)$  via the congruence action  $(X, S) \rightarrow X S X'$ . These two modules are isomorphic. An explicit isomorphism is given by  $S \rightarrow Z = -J^{-1} S$ .

In order to state our result it is convenient to fix

$$(1.4) \quad J = \begin{bmatrix} 0 & I_m \\ -I_m & 0 \end{bmatrix}.$$

Then we shall prove the following result.

**THEOREM 1.6.** *Let  $F$  be any field and let  $n = 2m$  be even.*

- (i) If the characteristic is not 2 and  $A \in \text{Sym}_n(F)$ , then there exists  $X \in \text{Sp}_n(F)$  such that

$$(1.5) \quad XAX' = \begin{bmatrix} B & 0 \\ 0 & C \end{bmatrix},$$

where  $B, C \in \text{Sym}_m(F)$ .

- (ii) If the characteristic is 2 and  $A \in M_n(F)$  satisfies  $A + A' = J$ , then there exists  $X \in \text{Sp}_n(F)$  such that

$$(1.6) \quad XAX' = \begin{bmatrix} B & I_m \\ 0 & C \end{bmatrix},$$

where  $B$  is invertible and  $B, C \in \text{Sym}_m(F)$ .

When  $F = \mathbf{C}$ , the assertion (i) is a special case of Theorem 1.5. We leave to the reader the task of reformulating part (i) of our result in terms of the adjoint action of  $\text{Sp}_n(F)$ . One should point out that for special fields there exist more precise results. For instance, if  $F = \mathbf{C}$  or  $F = \mathbf{R}$ , then the canonical forms (under simultaneous congruence) are known for pairs consisting of a symmetric and a skew-symmetric matrix. We refer the reader to the important survey paper of R.C. Thompson [10] and the extensive bibliography cited there.

In the last section we state two open problems concerning the congruence action of  $\text{SL}_n(F)$  on  $M_n(F)$ .

**2. Preliminaries.** As usual, we set  $F^* = F \setminus \{0\}$ . We denote by  $I_n$  the identity matrix of order  $n$ . As in Linear Algebra, we say that  $E \in \text{GL}_n(F)$  is an *elementary matrix* if it is obtained from  $I_n$  by one of the following operations:

- (i) Multiply a row by a nonzero scalar different from 1.
- (ii) Add a nonzero scalar multiple of a row to another row.
- (iii) Interchange two rows.

If  $E$  is an elementary matrix, then  $A \rightarrow EA$  is an *elementary row transformation* and  $A \rightarrow AE'$  is an *elementary column transformation*. We shall refer to  $A \rightarrow EAE'$  as an *elementary congruence transformation* or ECT for short.

For later use, we state the following trivial lemma concerning an arbitrary matrix  $A \in M_n(F)$ .

LEMMA 2.1. *Let  $A \in M_n(F)$ . If  $B = PAP'$  with  $P \in \text{GL}_n(F)$  and  $YBY' = B'$  for some  $Y \in \text{GL}_n(F)$ , then  $X = P^{-1}YP$  is a solution of (1.1). Moreover, if  $Y^2 = I_n$  then also  $X^2 = I_n$ .*

This lemma shows that, when considering the problem of finding rational nonsingular solutions of equation (1.1) or the system (1.2), we may without any loss of generality replace the matrix  $A$  with any matrix  $B = PAP'$ , where  $P \in \text{GL}_n(F)$ .

Let  $V$  be a vector space over  $F$  and assume that  $V$  is equipped with a nondegenerate alternate bilinear form  $f$ . The group of all  $u \in \text{GL}(V)$  such that  $f(u(x), u(y)) = f(x, y)$  for all  $x, y \in V$  is the symplectic group of  $(V, f)$  and will be denoted by  $\text{Sp}(V, f)$  or  $\text{Sp}_n(F)$  if  $\dim(V) = n$  and  $V$  and  $f$  are fixed. Note that  $n$  must be even. In this paper,  $f$  will be given usually by its matrix. If  $f(v, w) = 1$ , then we say that  $(v, w)$

is a *symplectic pair*. We shall need the following well known fact about symplectic groups.

PROPOSITION 2.2. *The symplectic group  $\text{Sp}(V, f)$  is transitive on the set of nonzero vectors of  $V$ . More generally, it is transitive on sequences*

$$(v_1, w_1, v_2, w_2, \dots, v_k, w_k)$$

of orthogonal symplectic pairs  $(v_i, w_i)$ .

We denote by  $J_m$  the direct sum of  $m$  blocks

$$(2.1) \quad \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

and by  $N_r$  the nilpotent lower triangular Jordan block of size  $r$ .

For the sake of convenience, we shall say that a matrix  $A \in M_n(F)$  *splits* if we can construct  $P \in \text{GL}_n(F)$  such that  $PAP'$  is a direct sum of two square matrices of size  $< n$ .

In the proof of the main result we shall use the square-free factorization algorithm for the polynomial ring  $F[t]$ . A nonzero polynomial is *square-free* if it is not divisible by the square of any irreducible polynomial. Let  $p \in F[t]$  be a monic polynomial. By using the GCD-algorithm, one can find the factorization  $p = p_1 p_2 \cdots p_k$ , where  $p_i$ 's are monic square-free polynomials of positive degree and such that  $p_i | p_{i-1}$  for  $1 < i \leq k$ . Such an algorithm is described in [4, Appendix 3]. We say that  $p = p_1 p_2 \cdots p_k$  is the *square-free factorization* of  $p$  and that  $p_1$  is the *square-free part* of  $p$ . We wish to remind the reader that we do not assume the existence of a prime factorization algorithm in  $F[t]$ , and this is the main reason for using the square-free factorization.

**3. Proofs of Theorems 1.3 and 1.6.** The first of these theorems is an easy consequence of the following important proposition, which will be used also later in the proof of our main result.

PROPOSITION 3.1. *Let  $A \in M_n(F)$ ,  $n \geq 1$ , and  $\det(A) = 0$ . Then there is a recursive algorithm which constructs  $P \in \text{GL}_n(F)$  such that  $PAP' = N_r \oplus B$  for some  $r$  ( $1 \leq r \leq n$ ) and some  $B \in M_{n-r}(F)$ .*

*Proof.* Let us write  $A = [a_{ij}]$  and let  $d$  be the defect of  $A$ , i.e., the dimension of the nullspace of  $A$ . By hypothesis,  $d \geq 1$ . Without any loss of generality, we may assume that the first  $d$  rows of  $A$  are 0.

Assume that the first  $d$  columns of  $A$  are linearly dependent. By performing suitable ECT's on the first  $d$  rows and columns, we may assume that the first column of  $A$  is also 0. Then  $A = N_1 \oplus B$  with  $N_1 = [0]$  and we are done.

Otherwise we have  $n \geq 2d$  and by performing suitable ECT's on the last  $n - d$  rows and columns, we may assume that

$$A = \begin{bmatrix} 0 & 0 & 0 \\ A_{21} & A_{22} & A_{23} \\ 0 & * & * \end{bmatrix},$$

where  $A_{21} = I_d$  and the diagonal blocks are square. By subtracting suitable linear combinations of the first  $d$  columns from the other columns (using ECT's), we may

further simplify  $A$  and assume that the blocks  $A_{22}$  and  $A_{23}$  are 0. Thus

$$A = \begin{bmatrix} 0 & 0 & 0 \\ I_d & 0 & 0 \\ 0 & * & Z \end{bmatrix}.$$

If  $n = 2d$ , then  $A$  splits as the direct sum of  $d$  copies of  $N_2$  and we are done.

We may now assume that  $n > 2d$ . Consider first the case where  $Z$  is nonsingular. By subtracting suitable linear combinations of the last  $n - 2d$  columns (via ECT's) from the previous  $d$  columns, we may assume that the starred block is 0. As a side-effect, the blocks  $A_{22}$  and  $A_{23}$  may be spoiled. These blocks can be again converted to zero by adding suitable linear combinations of the first  $d$  columns. Then  $A$  splits as the direct sum of  $Z$  and  $d$  copies of  $N_2$ .

Next we consider the case where  $Z$  is singular. Since  $Z$  is of size  $n - 2d < n$ , we may apply our recursive algorithm to it and so we may assume that  $A$  has the form:

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ I_d & 0 & 0 & 0 \\ 0 & A_{32} & N_s & 0 \\ 0 & A_{42} & 0 & A_{44} \end{bmatrix},$$

where  $s \geq 1$ . By subtracting suitable linear combinations of the  $s$  columns containing the block  $N_s$  from the columns containing  $A_{32}$  (using ECT's), we may assume that all the rows of  $A_{32}$  but the first are 0. As a side-effect, the zero blocks in the second block-row may be spoiled but we can convert them back to 0 as before. Note that the first row of  $A_{32}$  must be nonzero. By using ECT's whose matrices have the form  $Y \oplus (Y')^{-1} \oplus I_{n-2d}$ , we may assume that the first entry of the first row of  $A_{32}$  is 1, while all other entries are 0.

Assume that  $n = 2d + s$ . If  $d = 1$ , then  $A = N_n$  and we are done. If  $d > 1$ , then  $A$  splits, i.e., by permuting (simultaneously) rows and columns we can transform  $A$  into a direct sum  $N_2 \oplus B$ , where  $N_2$  comes from the principal submatrix occupying the positions  $d$  and  $2d$ .

From now on we assume that  $n > 2d + s$ . Let  $X$  be the  $n - 2d - s$ -by- $n - d - s - 1$  matrix obtained from  $(A_{42}, A_{44})$  by deleting its first column  $v$ . We leave to the reader to check that  $X$  has rank  $n - 2d - s$ . Hence by adding a suitable linear combination of the columns of  $A$  containing the submatrix  $X$  to the  $d + 1$ -column (via ECT's), we may assume that the first column  $v$  of  $A_{42}$  is 0. That might affect the blocks in the second block-row but  $A_{21}$  will remain nonsingular. As before, we can convert to 0 the blocks of  $A$  in the second block-row except  $A_{21}$  itself. Additionally, we may assume that  $A_{21} = I_d$ . It is now easy to see that  $A$  splits, i.e., by permuting (simultaneously) rows and columns we can transform  $A$  into a direct sum  $N_{s+2} \oplus B$ . (This Jordan block comes from the principal submatrix occupying the positions 1,  $d + 1$ , and those of the block  $N_s$ .)  $\square$

*Proof of Theorem 1.3.* On the basis of the above proposition, we see that in order to extend Gow's theorem to obtain Theorem 1.3, it suffices to observe that, for each positive integer  $r$ , there exists a permutation matrix  $P_r$  such that  $P_r^2 = I_r$  and

$P_r N_r P_r' = N_r'$ . We can take  $P_r$  to be the permutation matrix with 1's at the positions  $(i, r + 1 - i)$  with  $1 \leq i \leq r$ . This completes the proof of Theorem 1.3.  $\square$

*Proof of Theorem 1.6.* Let  $F$ ,  $m$ ,  $n$ , and  $A$  be as in the statement of the theorem and let  $J$  be as in (1.4).

(i) By hypothesis, the characteristic of  $F$  is not 2. By Theorem 1.3, there exists  $Y \in \text{GL}_n(F)$  such that  $Y'(A + J)Y = A - J$  and  $Y^2 = I_n$ . Thus we have

$$(3.1) \quad Y'JY = -J, \quad Y'AY = A.$$

Let  $V = F^n$  be the space of column vectors. Denote by  $E^+$  (resp.  $E^-$ ) the eigenspace of  $Y$  for the eigenvalue +1 (resp. -1). We note that  $J^2 = -I_n$ . Hence, for  $v, w \in E^+$ ,

$$v'Jw = (Yv)'Jw = v'Y'Jw = -v'JYw = -v'Jw.$$

As the characteristic of  $F$  is not 2,  $v'Jw = 0$ . Thus  $E^+$  is totally isotropic with respect to the nondegenerate skew-symmetric bilinear form defined by  $J$ . The same is true for  $E^-$ . Since  $V = E^+ \oplus E^-$ , we conclude that each of these eigenspaces has dimension  $m$ . By Proposition 2.2, there exists a  $T \in \text{Sp}_n(F)$  which maps  $E^+$  (resp.  $E^-$ ) onto the subspace spanned by the first (resp. last)  $m$  standard basis vectors of  $V$ . Equivalently, we have

$$P := TYT^{-1} = \begin{bmatrix} I_m & 0 \\ 0 & -I_m \end{bmatrix}.$$

Then  $X := (T')^{-1} \in \text{Sp}_n(F)$  and the second equality in (3.1) gives  $PXAX' = XAX'P$  and, consequently, (1.5) holds. Thus (i) is proved.

(ii) Now suppose the characteristic of  $F$  is 2. By Theorem 1.3, there exists  $Y \in \text{GL}_n(F)$  such that  $Y'AY = A'$  and  $Y^2 = I_n$ . Thus we have  $Y'A'Y = A$  and  $Y'JY = J$ . Denote by  $E$  the eigenspace of  $Y$  for the eigenvalue 1. As  $Y^2 = I_n$ , we have  $\dim(E) \geq m$ . For  $v, w \in E$ , we have  $v'Jw = v'(A + A')w = v'(A + Y'AY)w = 0$ . We conclude that  $E$  is totally isotropic with respect to the nondegenerate alternate bilinear form defined by  $J$ . Therefore  $\dim(E) \leq m$ . The two inequalities for  $\dim(E)$  imply that  $\dim(E) = m$ .

By Proposition 2.2, there is a  $T \in \text{Sp}_n(F)$  which maps  $E$  onto the subspace spanned by the first  $m$  standard basis vectors of  $V$ . Equivalently, we have

$$P := TYT^{-1} = \begin{bmatrix} I_m & S \\ 0 & I_m \end{bmatrix},$$

for some invertible  $S \in \text{Sym}_m(F)$ . Then  $Q := (T')^{-1} \in \text{Sp}_n(F)$  and  $Y'AY = A'$  gives  $P'Q'Q' = Q'A'Q'P$ . As  $Q'Q' + (Q'Q')' = J$ , we can write

$$Q'Q' = \begin{bmatrix} B & I_m + Z \\ Z' & W \end{bmatrix}$$

with  $B, W \in \text{Sym}_m(F)$  and deduce that  $B = S^{-1}$  and  $SZ \in \text{Sym}_m(F)$ . Consequently,

$$R = \begin{bmatrix} I_m & 0 \\ Z'S & I_m \end{bmatrix} \in \text{Sp}_n(F).$$

Then  $X = RQ$  satisfies (1.6) with  $B = S^{-1}$  and  $C = W + Z'S + Z'SZ$ . This concludes the proof of Theorem 1.6.  $\square$



**4. The description of the algorithm.** In this section we prove our main result, Theorem 1.4. Our algorithm operates recursively, i.e., we reduce the problem for matrices  $A$  of size  $n$  to the case of matrices of smaller size.

We now begin the description of our algorithm. Let  $A = [a_{ij}] \in M_n(F)$  be given. Throughout this section we shall use the following notation:  $A_0 := A + A'$  and  $A_1 := A - A'$ . The first of these matrices is symmetric and the second one is alternate. If the characteristic is 2, then  $A_0 = A_1$ . The rank of  $A_1$  is even, say  $2m$ .

By Lemma 2.1, we may replace  $A$  by any matrix congruent to it. Hence without any loss of generality we may assume that  $A_1$  is *normalized*, i.e.,

$$A_1 = \begin{bmatrix} J_m & 0 \\ 0 & 0 \end{bmatrix}.$$

Let  $G$  denote the subgroup of  $GL_n(F)$  that preserves the matrix  $A_1$ , i.e.,

$$G = \{X \in GL_n(F) : X'A_1X = A_1\}.$$

For  $S \in G$ , we say that  $A \rightarrow SAS'$  is a *symplectic congruence transformation* or SCT. An ECT can be an SCT only if  $2m < n$ . If it is not an SCT, we can compose it with another ECT to obtain an SCT. For instance, if  $m > 0$  and we multiply the first row and column by a nonzero scalar  $\lambda \neq 1$ , then we also have to multiply the second row and column by  $\lambda^{-1}$ . An *elementary* SCT is an SCT which is either an ECT or a product of two ECT's none of which is an SCT by itself.

The main idea of the algorithm is to find  $P \in GL_n(F)$  such that, when we replace  $A$  with  $PAP'$ , the system (1.2) has an obvious solution  $Y$ . Then Lemma 2.1 provides a solution  $X$  for the original system.

We distinguish four cases:

- (a)  $\det(A_1) = 0$  and the characteristic is not 2.
- (b)  $\det(A_1) \neq 0$ ,  $\det(A_0) = 0$  and the characteristic is not 2.
- (c)  $\det(A_1) = 0$  and the characteristic is 2.
- (d)  $\det(A_0A_1) \neq 0$ .

Each of these cases will be treated separately. We set  $V = F^n$ , considered as the space of column vectors, and we shall use its standard basis  $\{e_1, e_2, \dots, e_n\}$ .

**4.1. Algorithm for case (a).** The characteristic of  $F$  is not 2,  $2m < n$ , and we set  $k = n - 2m$ .

In this case, our recursive algorithm will construct an involutory matrix  $Y \in GL_n(F)$  and a sequence of ECT's with the following properties: After transforming  $A$  with this sequence of ECT's,  $Y$  and the new  $A$  satisfy the following conditions:

- (i)  $A_1$  is normalized, i.e.,  $A_1 = J_m \oplus 0$ .
- (ii)  $YAY' = A'$ .
- (iii) All entries of the last  $k$  rows and columns of  $Y$  are 0 except the diagonal entries (which are  $\pm 1$ ).

We remark that if  $A = B \oplus C$ , where  $B$  and  $C$  are square matrices of smaller size, and if our algorithm works for  $B$  and  $C$ , then it also works for  $A$ .

If  $m = 0$ , we take  $Y = I_n$ . From now on we assume that  $m \geq 1$ . Let us partition the symmetric matrix  $A_0$  into four blocks:

$$A_0 = \begin{bmatrix} B & C \\ C' & D \end{bmatrix},$$

where  $B$  is of size  $2m$ . Assume that  $D \neq 0$ . Then we may assume that its last diagonal entry is not 0. By elementary row operations and corresponding column operations, we can make all other entries in the last row and column of  $A_0$  vanish. (These operations do not affect  $A_1$ .) Hence  $A$  splits.

From now on we assume that  $D = 0$ . If the rank of  $C$  is smaller than  $k$ , then we may assume that the last column of  $C$  is zero and so  $A$  splits. Thus we may assume that  $C$  has rank  $k$ . Our next goal is to simplify the block  $C = [c_{ij}]$ . Note that if  $X \in G$  is block-diagonal:

$$X = \begin{bmatrix} X_1 & 0 \\ 0 & X_2 \end{bmatrix}, \quad X_1 \in \text{Sp}_{2m}(F), \quad X_2 \in \text{GL}_k(F),$$

then the effect of the SCT:  $A \rightarrow XAX'$  on the block  $C$  is given by  $C \rightarrow X_1CX_2'$ .

Let  $v_j$  denote the  $j$ -th column of  $A$ .

Assume that there exist  $p, q$  such that  $2m < p, q \leq n$  and  $v_p' A_1 v_q \neq 0$ . By applying a suitable SCT (of the type mentioned above), we may further assume that  $c_{2m-1, k-1} = c_{2m, k} = 1$  and all other entries of the last two rows and columns of  $C$  vanish. Next by subtracting multiples of the last two columns of  $A$  from the first  $2m - 2$  columns (via ECT's), we can assume that also the first  $2m - 2$  entries of the last two rows of  $B$  vanish. If  $n > 4$ , then  $A$  splits. Otherwise,  $n = 4$ , we can assume that  $B = 0$  and then take  $Y = \text{diag}(1, -1, 1, -1)$ .

It remains to consider the case where  $v_p' A_1 v_q = 0$  for all  $p, q > 2m$ , i.e., the columns of  $C$  form a basis of a  $k$ -dimensional totally isotropic space (with respect to  $J_m$ ). Since  $\text{Sp}_{2m}(F)$  acts transitively on such bases, without any loss of generality, we may assume that

$$(4.1) \quad c_{2m, k} = c_{2m-2, k-1} = \cdots = c_{2m-2k, 1} = 1$$

while all other entries of  $C$  are 0. Since the column-space of  $C$  is totally isotropic, we must have  $k \leq m$ .

By subtracting suitable multiples of the last  $k$  columns from the first  $2m$  columns (via ECT's), we may assume that each of the rows  $2m - 2k + 2, 2m - 2k + 4, \dots, 2m$  of  $A_0$  has a single nonzero entry. (The corresponding columns have the same property.)

In order to help the reader visualize the shape of the matrix  $A_0$  at this point, we give an example. We take  $m = 5$  and  $k = 2$ . Then  $A_0$  has the form:

$$A_0 = \left[ \begin{array}{cccccccccccc|cc} & & & & & & & & & & & & 0 & 0 \\ & & & & & & & & & & & & 0 & 0 \\ & & & & & & & & & & & & 0 & 0 \\ & & & & & & & & & & & & 0 & 0 \\ & & & & & & & & & & & & 0 & 0 \\ & & & & & & & & & & & & 0 & 0 \\ & & & & & & & & & & & & 0 & 0 \\ & & & & & & & & & & & & 0 & 0 \\ & & & & & & & & & & & & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ & & & & & & & & & & & & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{array} \right],$$

where the blank entries have not been specified.

In order to give a simple formula for the matrix  $P$  (which provides the solution of our problem for the matrix  $A$ ), it will be convenient to perform a congruence transformation which is not an SCT. For that purpose we just rearrange the rows of  $A$  so that the rows  $2m - 2k + 1, 2m - 2k + 3, \dots, 2m - 1$  come before the rows  $2m - 2k + 2, 2m - 2k + 4, \dots, 2m$  (and similarly the columns). We continue (as in programming) to refer to this new matrix as the matrix  $A$ . Now  $A_1$  is no longer normalized. The matrices  $A_0$  and  $A_1$  have the following form

$$A_0 = \begin{bmatrix} R_1 & R_2 & 0 & 0 \\ R'_2 & R_3 & 0 & 0 \\ 0 & 0 & 0 & I_k \\ 0 & 0 & I_k & 0 \end{bmatrix}, \quad A_1 = \begin{bmatrix} J_{m-k} & 0 & 0 & 0 \\ 0 & 0 & I_k & 0 \\ 0 & -I_k & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

where all the blocks, except those in the first row and column, are square of size  $k$ .

We now introduce a truncated version of the problem, in which we replace  $A$  with its principal submatrix  $\bar{A}$  obtained by deleting the last  $2k$  rows and columns. Define  $\bar{A}_0$  and  $\bar{A}_1$  similarly. These truncated matrices have all size  $n - 2k (= 2m - k)$ . Note that  $\bar{A}_1$  is already normalized and has rank  $2(m - k)$ . Hence, by using recursion, our algorithm can compute a matrix  $\bar{P} \in GL_{n-2k}(F)$  and an involutory matrix  $\bar{Y}$  satisfying the conditions (i-iii). In particular,

$$\bar{Y}\bar{P}\bar{A}_0(\bar{P})'\bar{Y} = \bar{P}\bar{A}_0(\bar{P})', \quad \bar{P}\bar{A}_1(\bar{P})' = \bar{A}_1 \quad \text{and} \quad \bar{Y}\bar{A}_1\bar{Y} = -\bar{A}_1.$$

We now show that we can use  $\bar{P}$  and  $\bar{Y}$  to construct  $P \in GL_n(F)$  and an involutory matrix  $Y$ , such that

$$YPA_0P'Y = PA_0P', \quad PA_1P' = A_1 \quad \text{and} \quad YA_1Y = -A_1.$$

Let us partition  $\bar{P}$  as follows:

$$\bar{P} = \begin{bmatrix} P_1 & P_2 \\ P_3 & P_4 \end{bmatrix},$$

where  $P_4$  is of size  $k$ . The matrix  $\bar{A}_1$  has the form  $J_{m-k} \oplus 0$ . The equation  $\bar{P}\bar{A}_1(\bar{P})' = \bar{A}_1$  implies that  $P_1 J_{m-k} P_1' = J_{m-k}$  and  $P_3 = 0$ .

Our matrix  $P$  is now given by the following formula:

$$P = \begin{bmatrix} P_1 & P_2 & 0 & Q_1 \\ 0 & P_4 & 0 & Q_2 \\ P_5 & P_6 & (P_4')^{-1} & Q_3 \\ 0 & 0 & 0 & P_4 \end{bmatrix},$$

where

$$\begin{aligned} P_5 &= -(P_1^{-1} P_2 P_4^{-1})' J_{m-k}, \\ P_6 &= -\frac{1}{2} (P_4')^{-1} P_2' J_{m-k} P_2, \\ Q_1 &= -(P_1 R_1 + P_2 R_2') P_5' P_4 - (P_1 R_2 + P_2 R_3) P_6' P_4, \\ Q_2 &= -P_4 (R_2' P_5' + R_3 P_6') P_4, \\ Q_3 &= -\frac{1}{2} (P_5 R_1 P_5' + P_5 R_2 P_6' + P_6 R_2' P_5' + P_6 R_3 P_6') P_4. \end{aligned}$$

Clearly  $P$  is invertible. It is easy to verify that  $PA_1P' = A_1$  and that  $PA_0P'$  has the same shape as  $A_0$  except that the blocks  $R_1$ ,  $R_2$  and  $R_3$  may be different from those in  $A_0$ . Recall that  $\bar{P}\bar{A}_1(\bar{P})' = \bar{A}_1$  and that  $\bar{Y} = \Delta \oplus \Lambda$ , where  $\Lambda$  is a diagonal matrix of size  $k$ . Moreover,  $\bar{Y}$  commutes with  $\bar{P}\bar{A}_0(\bar{P})'$  and anti-commutes with  $\bar{A}_1$ . Set  $Y = \bar{Y} \oplus (-\Lambda) \oplus (-\Lambda)$ . It is easy to verify that  $Y$  commutes with  $PA_0P'$  and anti-commutes with  $A_1$ . Consequently, the conditions (ii) and (iii) are satisfied. By transforming  $A$  with a suitable permutation matrix, we may also satisfy the condition (i).

This completes the treatment of case (a).

**4.2. Algorithm for case (b).** We recall that the characteristic is not 2,  $n = 2m$ ,  $A_1 = J_m$ , and  $A_0$  is singular. We define here the symplectic group,  $\text{Sp}_n(F)$ , by using definition (1.3) with  $J = J_m$ . Let  $N$  be the nullspace of  $A_0$ , i.e.,  $N = \{v \in V : A_0v = 0\}$  and let  $d$  be its dimension. Since  $\det(A_0) = 0$ , we have  $d > 0$ .

In this case, our recursive algorithm will construct an involutory matrix  $Y \in \text{GL}_n(F)$  and a sequence of ECT's with the following properties: After transforming  $A$  with this sequence of ECT's,  $Y$  and the new  $A$  satisfy the following conditions:

- (i)  $A_1$  is normalized, i.e.,  $A_1 = J_m$ .
- (ii)  $YAY' = A'$ .
- (iii) Exactly  $d$  rows and  $d$  columns of  $A_0$  are 0, and the corresponding rows and columns of  $Y$  have all entries 0 except the diagonal entries (which are  $\pm 1$ ).

Again we remark that if  $A = B \oplus C$ , where  $B$  and  $C$  are square matrices of smaller size, and if our algorithm works for  $B$  and  $C$ , then it also works for  $A$ .

Assume that there exist  $v, w \in N$  such that  $v'A_1w = 1$ . Then it is easy to construct a matrix  $P \in \text{Sp}_n(F)$  having  $v$  and  $w$  as its first two columns. Hence the first two columns (and rows) of  $P'A_0P$  are zero. If  $m = 1$ , then  $Y = \text{diag}(1, -1)$  works, otherwise  $P'AP$  splits. Thus we may assume that  $v'A_1w = 0$  for all vectors

$v, w \in N$ . Since  $\det(A_1) \neq 0$ , we deduce that  $d \leq m$ . Then we can construct  $P \in \text{Sp}_n(F)$  such that its columns in positions  $n, n-2, \dots, n-2d+2$  form a basis of  $N$ . We replace  $A$  with  $P'AP$ .

If  $d = m$ , then  $Y = \text{diag}(1, -1, \dots, 1, -1)$  satisfies (ii) and (iii) and we are done.

Now assume that  $d < m$ . Recall that  $\{e_n, e_{n-2}, \dots, e_{n-2d+2}\}$  is a basis of  $N$ . We set  $\bar{m} = m - d$  and define  $\bar{A}_0$  to be the submatrix of  $A_0$  of size  $\bar{n} = 2\bar{m}$  in the upper left hand corner. We denote by  $\bar{N}$  the nullspace of  $\bar{A}_0$  and by  $\bar{d}$  its dimension.

Assume that  $\bar{d} = 0$ , i.e.,  $\bar{A}_0$  is nonsingular. Then, by applying a suitable sequence of elementary SCT's, we may assume that the  $n - \bar{n}$ -by- $\bar{n}$  submatrix of  $A_0$  just below the submatrix  $\bar{A}_0$  is zero. This means that  $A$  splits.

Now assume that  $\bar{d} > 0$ . By using recursion, we may assume that we already have an involutory matrix  $\bar{Y} \in \text{GL}_{\bar{n}}(F)$  and that  $\bar{Y}$  and  $\bar{A}$  satisfy the conditions (i-iii) above.

For convenience, we partition the set of the first  $\bar{n}$  rows (and similarly columns) of  $A_0$  in two parts: We say that one of these rows or columns is of the *first kind* if it contains a nonzero entry of the submatrix  $\bar{A}_0$  and otherwise it is of the *second kind*. The sequence of elementary SCT's that we are going to construct has the additional property that it will not alter the submatrix  $\bar{A}_0$ .

Denote by  $B$  the  $\bar{d}$ -by- $d$  submatrix of  $A_0$  in the intersection of the rows of the second kind and the columns in positions  $n-1, n-3, \dots, n-2d+1$ . Since  $d$  is the dimension of  $N$ ,  $B$  must have rank  $\bar{d}$ . By using elementary SCT's which act only on the last  $2d$  columns (and rows), we can modify  $B$  without spoiling the zero entries of  $A_0$  which were established previously and assume that  $B = (I_{\bar{d}}, 0)$ , i.e.,  $B$  consists of the identity matrix of size  $\bar{d}$  followed by  $d - \bar{d}$  zero columns.

Let us illustrate the shape of the matrix  $A_0$  at this stage by an example where  $n = 2m = 18$ ,  $d = 5$ , and  $\bar{d} = 4$ . We point out that the submatrix made up of the starred entries is nonsingular. Hence a row or column of  $A_0$  is of the first kind if and only if it contains a star entry. The submatrix  $\bar{A}_0$  is the block of size 8 in the upper left hand corner.

$$A_0 = \left[ \begin{array}{cccccccc|cccccccc}
 * & * & * & 0 & * & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 * & * & * & 0 & * & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 * & * & * & 0 & * & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 * & * & * & 0 & * & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
 \hline
 & & & 1 & & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & & & 0 & & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & & & 0 & & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & & & 0 & & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & & & 0 & & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
 \end{array} \right].$$

By subtracting suitable multiples of the columns of  $A_0$  of the first kind (using elementary SCT's) from the columns in positions  $n - 1, n - 3, \dots, n - 2d + 1$ , we may assume that all entries of  $A_0$  in the intersection of the latter columns and the rows of the first kind are zero. In the above example this means that all blank entries in the first eight rows (and columns) are being converted to zero.

We can now use elementary SCT's to convert to zero all entries in the  $2d$ -by- $2d$  submatrix of  $A_0$  in the lower right hand corner, except those in the  $2(d - \bar{d})$ -by- $2(d - \bar{d})$  submatrix in the same corner. Similarly, if  $d > \bar{d}$ , we can diagonalize the (nonsingular) square submatrix of size  $d - \bar{d}$  in the intersection of rows and columns in positions  $n - 1, n - 3, \dots, n - 2(d - \bar{d}) + 1$ .

We extend  $\bar{Y}$  to  $Y$  as follows. Let  $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{\bar{d}}$  be the entries in the diagonal of  $\bar{Y}$  occurring in the rows of  $A_0$  of the second kind. We set the diagonal entries of  $Y$  in positions  $\bar{n} + 1, \bar{n} + 3, \dots, \bar{n} + 2\bar{d} - 1$  to be  $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{\bar{d}}$ . Furthermore, we set the diagonal entries of  $Y$  in positions  $\bar{n} + 2, \bar{n} + 4, \dots, \bar{n} + 2\bar{d}$  to be equal to  $-\varepsilon_1, -\varepsilon_2, \dots, -\varepsilon_{\bar{d}}$ . Finally, the last  $2(d - \bar{d})$  diagonal entries of  $Y$  are set to be  $1, -1, \dots, 1, -1$ . One verifies that  $Y, A_0$  and  $A_1$  satisfy the conditions (i-iii) above.

This completes the treatment of case (b).

**4.3. Algorithm for case (c).** In this case, the characteristic of  $F$  is 2,  $2m < n$ , and we set  $k = n - 2m$ . We recall that  $A_1 = J_m \oplus 0$ . Let us partition  $A$  into four blocks:

$$A = \begin{bmatrix} B & C \\ C' & D \end{bmatrix},$$

where  $B + B' = J_m$  and  $D' = D$  is of size  $k$ . In this case our recursive algorithm will produce a solution  $X$  of (1.2) of the form

$$X = \begin{bmatrix} X_1 & X_2 \\ 0 & I_k \end{bmatrix}.$$

Assume that  $D$  is non-alternate. Then we can assume that its last entry  $a_{nn} \neq 0$ . By adding suitable multiples of the last row of  $A$  to other rows (via ECT's), we may assume that  $a_{nn}$  is the sole nonzero entry in the last row and column. If  $n = 1$ , i.e.,  $m = 0$  and  $k = 1$ , then we can take  $X = I_1$ . Otherwise  $A$  splits and we can use recursion.

Next assume that  $D$  is alternate and nonzero. Then we may assume that it is the direct sum of a symmetric matrix of size  $k - 2$  and the block  $J_1$ . We can now proceed in the same way as above to convert to 0 the last two columns of  $C$ . If  $m = 0$  and  $k = 2$ , then  $n = 2$  and we can take  $X = I_2$ . Otherwise  $A$  splits and we can use recursion.

Hence, we may now assume that  $D = 0$ . We can also split  $A$  if the rank of  $C$  is less than  $k$ . Thus we may assume that  $C$  has rank  $k$ .

Assume that the  $k$ -dimensional space spanned by the columns of  $C$  is not totally isotropic (with respect to  $J_m$ ). If  $n > 4$ , we can split  $A$  as in subsection 4.1. Otherwise  $n = 4$  and we may assume that  $C = I_2$ . Then

$$X = \begin{bmatrix} I_2 & B \\ 0 & I_2 \end{bmatrix}$$

is a solution of (1.2) and has the desired form. Hence we may now assume that the above space is totally isotropic. Consequently,  $k \leq m$ . As in the previous section, we may also assume that (4.1) holds and all other entries of  $C$  are 0.

By adding suitable multiples of the last  $k$  columns to the first  $2m - 2k$  columns (via ECT's), we may assume that the first  $2m - 2k$  entries of the rows  $2m - 2k + 2, 2m - 2k + 4, \dots, 2m$  of  $B$  are 0. The corresponding columns have the same property. By using the same argument, we can also assume that all entries in the intersection of the rows  $2m - 2k + 2, 2m - 2k + 4, \dots, 2m$  and columns  $2m - 2k + 1, 2m - 2k + 3, \dots, 2m - 1$  of  $B$  are 0. As  $A + A' = J$  remains valid, all entries in the intersection of the rows  $2m - 2k + 1, 2m - 2k + 3, \dots, 2m - 1$  and columns  $2m - 2k + 2, 2m - 2k + 4, \dots, 2m$  of  $B$  are 0, except that the entries just above the diagonal are equal to 1. This completes the first subroutine of the algorithm.

In order to help the reader visualize the shape of the matrix  $A$  at this point, we give an example. We take  $m = 6$  and  $k = 3$ . Then  $A$  has the form:

$$A = \left[ \begin{array}{cccccc|cccc} & & & & & & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & & & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & & & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & & & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & & & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & & & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & & & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline & & & & & & \bullet & 1 & \bullet & 0 & \bullet & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \star & 0 & \star & 0 & \star \\ & & & & & & \bullet & 0 & \bullet & 1 & \bullet & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \star & 0 & \star & 0 & \star \\ & & & & & & \bullet & 0 & \bullet & 0 & \bullet & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \star & 0 & \star & 0 & \star \\ \hline & & & & & & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \hline & & & & & & 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right],$$

where the blank, bullet, and star entries remain unspecified.

In order to give a simple formula for the matrix  $X$ , it will be convenient to perform a congruence transformation which is not an SCT. For that purpose we just rearrange the rows of  $A$  so that the rows  $2m - 2k + 1, 2m - 2k + 3, \dots, 2m - 1$  come before the rows  $2m - 2k + 2, 2m - 2k + 4, \dots, 2m$  (and similarly the columns). Now  $A_1$  is no longer normalized. The matrices  $A$  and  $A_1$  have the following form

$$A = \begin{bmatrix} A_{11} & A_{12} & 0 & 0 \\ A'_{12} & A_{22} & I_k & 0 \\ 0 & 0 & A_{33} & I_k \\ 0 & 0 & I_k & 0 \end{bmatrix}, \quad A_1 = \begin{bmatrix} J_{m-k} & 0 & 0 & 0 \\ 0 & 0 & I_k & 0 \\ 0 & I_k & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

where all the blocks, except those in the first row and column, are square of size  $k$ . As  $A + A' = A_1$ , the matrices  $A_{22}$  and  $A_{33}$  are symmetric and  $A_{11} + A'_{11} = J_{m-k}$ .

Let us illustrate these modifications in the example given above. Then the new matrix  $A$  has the following shape:



$$A = \left[ \begin{array}{cccc|ccc|ccc} & & & & & & & & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & & & & & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & & & & & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & & & & & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & & & & & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & & & & & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & & & & & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline & & & & \bullet & \bullet & \bullet & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & \bullet & \bullet & \bullet & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & \bullet & \bullet & \bullet & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \star & \star & \star & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \star & \star & \star & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \star & \star & \star & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{array} \right],$$

where the bullet (resp. star) entries are those of  $A_{22}$  (resp.,  $A_{33}$ ).

Assume that  $A_{22}$  is non-alternate. By performing congruence transformation on  $A$  with a suitable block-diagonal matrix  $I_{2(m-k)} \oplus Z \oplus (Z')^{-1} \oplus Z$ , we can assume that  $A_{22}$  is a diagonal matrix (see [8]) and that its last diagonal entry is nonzero. By using elementary SCT's, we can assume that the last column of  $A_{12}$  is 0. As a side-effect of these elementary SCT's, the zero blocks just below  $A'_{12}$  and  $A_{22}$  may be spoiled (and the block  $A_{33}$  may be altered). This damage can be easily repaired by using elementary SCT's which add multiples of the last  $k$  columns to the first  $2m - k$  columns. By adding suitable multiples of the last  $k$  columns (and rows) we may assume that the symmetric matrix  $A_{33}$  is diagonal. If  $n = 3$ , i.e.,  $m = k = 1$ , then we can take

$$X = \left[ \begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 1 \end{array} \right].$$

Otherwise  $A$  splits (with one of the blocks of size 3).

Next assume that  $A_{22}$  is alternate and nonzero. Then we may assume that it is the direct sum of a symmetric matrix of size  $k - 2$  and the block  $J_1$ . We can now proceed in the same way as above to convert to 0 the last two columns of  $A_{12}$  and to diagonalize  $A_{33}$ . If  $n = 6$ , i.e.,  $m = k = 2$ , then we can take

$$X = \left[ \begin{array}{cc|cc} I_2 & 0 & I_2 & \\ 0 & I_2 & 0 & \\ \hline 0 & 0 & I_2 & \end{array} \right].$$

Otherwise  $A$  splits and we can use recursion.

Hence, we may now assume that  $A_{22} = 0$ .

We now introduce a truncated version of the problem, in which we replace  $A$  with its principal submatrix  $\bar{A}$  obtained by deleting the last  $2k$  rows and columns. The truncated matrix,  $\bar{A}$ , is of size  $n - 2k (= 2m - k)$ . Let  $\bar{A}_1$  be the corresponding submatrix of  $A_1$ , i.e.,  $\bar{A}_1 = \bar{A} + (\bar{A})' = J_{m-k} \oplus 0$ .

By using recursion, our algorithm can compute a matrix  $\bar{X} \in \text{GL}_{n-2k}(F)$  of the form

$$\bar{X} = \begin{bmatrix} X_1 & X_2 \\ 0 & I_k \end{bmatrix}$$

such that  $(\bar{X})^2 = I_{n-2k}$  and  $\bar{X}\bar{A}(\bar{X})' = (\bar{A})'$ . The last condition is equivalent to  $\bar{X}\bar{A}$  being a symmetric matrix. In terms of the blocks of  $\bar{A}$  and  $\bar{X}$ , we have

$$X_1^2 = I_{2(m-k)}, X_1X_2 = X_2, X_1A_{12} = A_{12}, X_1A_{11} + X_2A'_{12} \in \text{Sym}_{2(m-k)}(F).$$

We now use  $\bar{X}$  to construct the desired  $X \in \text{GL}_n(F)$ . Our matrix  $X$  is given by the following formula:

$$X = \begin{bmatrix} X_1 & X_2 & 0 & X_3 \\ 0 & I_k & 0 & X_4 \\ X_5 & X_6 & I_k & A_{33} \\ 0 & 0 & 0 & I_k \end{bmatrix},$$

where

$$\begin{aligned} X_3 &= A_{11}J_{m-k}X_2 + A_{12}X'_2J_{m-k}A_{11}J_{m-k}X_2, \\ X_4 &= I_k + A'_{12}J_{m-k}X_2, \\ X_5 &= X'_2J_{m-k}, \\ X_6 &= X'_2J_{m-k}A_{11}J_{m-k}X_2. \end{aligned}$$

The matrix  $X_6$  is symmetric. Indeed we have:

$$X'_6 = X'_2J_{m-k}A'_{11}J_{m-k}X_2 = X'_2J_{m-k}(A_{11} + J_{m-k})J_{m-k}X_2 = X_6 + X'_2J_{m-k}X_2.$$

Since  $X_1X_2 = X_2$ , the column-space of  $X_2$  is contained in the 1-eigenspace of  $X_1$ . On the other hand, we know from the proof of Theorem 1.6 that this eigenspace is a maximal totally isotropic subspace (with respect to  $J_{m-k}$ ). Hence  $X'_2J_{m-k}X_2 = 0$  and so  $X'_6 = X_6$ . It is now straightforward to verify that  $XA$  is symmetric.

It remains to verify that  $X^2 = I_n$ . Note that the column-space of  $I_{2(m-k)} + X_1$  and also of  $A_{12}$  is contained in the 1-eigenspace of  $X_1$ . The same argument as above shows that  $X'_2J_{m-k}(I_{2(m-k)} + X_1) = 0$  and  $A'_{12}J_{m-k}X_2 = 0$ . The first of these equalities can be rewritten as  $X'_1J_{m-k}X_2 = J_{m-k}X_2$ . By using these equalities, we

find that

$$\begin{aligned}
 X_5 X_1 + X_5 &= X_2' J_{m-k} (I_{2(m-k)} + X_1) = 0, \\
 X_5 X_2 &= X_2' J_{m-k} X_2 = 0, \\
 X_1 X_3 + X_2 X_4 + X_3 &= X_1 A_{11} J_{m-k} X_2 + A_{11} J_{m-k} X_2 + X_2 + X_2 A_{12}' J_{m-k} X_2 \\
 &= (A_{11}' X_1' + A_{12} X_2') J_{m-k} X_2 + A_{11} J_{m-k} X_2 + X_2 \\
 &= A_{11}' X_1' J_{m-k} X_2 + A_{11} J_{m-k} X_2 + X_2 \\
 &= A_{11}' J_{m-k} X_2 + A_{11} J_{m-k} X_2 + X_2 = 0, \\
 X_5 X_3 + X_6 X_4 &= X_2' J_{m-k} A_{12} X_2' J_{m-k} A_{11} J_{m-k} X_2 \\
 &\quad + X_2' J_{m-k} A_{11} J_{m-k} X_2 A_{12}' J_{m-k} X_2 = 0.
 \end{aligned}$$

Thus  $X^2 = I_n$  as claimed.

This completes the treatment of case (c).

**4.4. Algorithm for case (d).** In this case there is no restriction on the characteristic of  $F$ ,  $n = 2m$ , both matrices  $A_0$  and  $A_1$  are nonsingular, and we have  $A_1 = J_m$ . In view of Proposition 3.1, we may also assume that  $\det(A) \neq 0$ . Thus all three bilinear forms:

$$\begin{aligned}
 \langle x, y \rangle &= x' A y, \quad x, y \in V, \\
 \langle x, y \rangle_0 &= x' A_0 y, \quad x, y \in V, \\
 \langle x, y \rangle_1 &= x' A_1 y, \quad x, y \in V
 \end{aligned}$$

are nondegenerate. The second form is symmetric and the third is alternate. If  $W$  is a subspace of  $V$ , there are two kinds of orthogonal complements with respect to the first form: The *right orthogonal complement*

$$W^\perp = \{y \in V : \langle x, y \rangle = 0, \forall x \in W\},$$

and the *left orthogonal complement*

$${}^\perp W = \{y \in V : \langle y, x \rangle = 0, \forall x \in W\}.$$

Set  $S = J_m A$ , an invertible matrix which we also consider as a linear operator on  $V$ . We make  $V$  into a module over the polynomial algebra  $F[t]$  by letting  $t$  act as the multiplication by  $S$ . We write  $f \cdot x$  for the action of  $f \in F[t]$  on  $x \in V$ . We denote by  $*$  the involutorial automorphism of the  $F$ -algebra  $F[t]$  which sends  $t$  to  $-1 - t$ . Thus if  $f \in F[t]$ , then  $f^* \in F[t]$  is defined by  $f^*(t) = f(-1 - t)$ . One can check without difficulty that  $f^* = f$  holds if and only if  $f(t) = g(t + t^2)$  for some  $g \in F[t]$ . If the characteristic of  $F$  is not 2, then  $f^* = -f$  holds if and only if  $f(t) = (2t + 1)g(t + t^2)$  for some  $g \in F[t]$  and, consequently, if  $f \neq 0$ , then  $f^* = -f$  implies that  $f$  has odd degree.

It is straightforward to verify that for all  $x, y \in V$  we have

$$\begin{aligned} \langle x, t \cdot y \rangle &= -\langle (1+t) \cdot x, y \rangle, \\ \langle x, t \cdot y \rangle_1 &= -\langle (1+t) \cdot x, y \rangle_1, \\ \langle x, t \cdot y \rangle_1 &= -\langle x, y \rangle, \\ \langle x, y \rangle + \langle y, x \rangle &= \langle x, y \rangle_0, \\ \langle x, y \rangle - \langle y, x \rangle &= \langle x, y \rangle_1. \end{aligned}$$

The first two of these identities imply that

$$\begin{aligned} \langle x, f \cdot y \rangle &= \langle f^* \cdot x, y \rangle, \quad \forall x, y \in V, \quad \forall f \in F[t]; \\ \langle x, f \cdot y \rangle_1 &= \langle f^* \cdot x, y \rangle_1, \quad \forall x, y \in V, \quad \forall f \in F[t]. \end{aligned}$$

The second and third imply that if a subspace  $W$  of  $V$  is  $S$ -invariant (i.e., an  $F[t]$ -submodule), then

$${}^\perp W = W^\perp = W^{\perp_1},$$

and we shall denote this subspace simply by  $W^\perp$ .

Let  $f$  denote the minimal polynomial of  $S$  and let  $f = f_1 f_2 \cdots f_k$  be its square-free factorization. Since  $J_m S' = -J_m A' J_m = -J_m A J_m - J_m = -(I_n + S) J_m$  and  $S'$  is similar to  $S$ , we conclude that  $S$  and  $-I_n - S$  are similar matrices. This implies that  $f^* = \pm f$ , and so each  $f_i^* = \pm f_i$ . If the characteristic of  $F$  is not 2, since  $2S + I_n = J_m A_0$  and  $A_0$  is nonsingular, we conclude that  $2t + 1$  does not divide  $f$ . Hence  $f^* = f$  in all cases, and also  $f_i^* = f_i$  for all  $i$ 's.

Let  $f_1 = gh$  where  $g^* = g$  and  $h^* = h$  are monic polynomials. We set

$$V_g = \bigcup_{i \geq 0} \ker(g(S)^i)$$

and define  $V_h$  similarly. Then  $V = V_g \oplus V_h$  and  $V_g^\perp = V_h$ . Consequently, if  $g^* = g$  is a monic divisor of  $f_1$ , then

$$(4.2) \quad V = V_g \oplus V_g^\perp.$$

Assume that  $f_i \neq f_1$  for some  $i$ . Then  $g = f_i$  and  $h = f_1/f_i = h^*$  are relatively prime monic nonconstant polynomials. Hence (4.2) is valid. Clearly, we can construct the subspace  $V_g$  and so we obtain a splitting of  $A$ .

From now on we assume that  $f_i = f_1$  for all  $i = 2, \dots, k$ , i.e.,  $f = f_1^k$ . For  $0 \leq i \leq k$ , we denote by  $V_i$  the kernel of the operator  $f_1(S)^{k-i}$ . In particular,  $V_0 = V$  and  $V_k = 0$ . Set  $\overline{V} = V/V_1$  and, for  $x \in V$ ,  $\bar{x} = x + V_1$ . The bilinear form  $V \times V \rightarrow F$  defined by  $(x, y) \rightarrow \langle x, f_1^{k-1} \cdot y \rangle_0$  has  $V_1$  as its (left and right) radical. It induces a nondegenerate bilinear form  $\overline{V} \times \overline{V} \rightarrow F$  given by  $(\bar{x}, \bar{y}) \rightarrow \langle x, f_1^{k-1} \cdot y \rangle$ . This form is not skew-symmetric because

$$\langle x, f_1^{k-1} \cdot y \rangle + \langle y, f_1^{k-1} \cdot x \rangle = \langle x, f_1^{k-1} \cdot y \rangle + \langle f_1^{k-1} \cdot y, x \rangle = \langle x, f_1^{k-1} \cdot y \rangle_0$$

and  $\langle \cdot, \cdot \rangle_0$  is nondegenerate.

Therefore we can choose  $v \in V$  such that  $\bar{v}$  is a non-isotropic vector with respect to the above form, i.e., if  $w = f_1^{k-1} \cdot v$ , then  $\langle v, w \rangle \neq 0$ . Let  $W = F[t] \cdot v$  be the cyclic submodule generated by  $v$  and set  $U = W \cap W^\perp$ . Of course,  $U$  is also cyclic, say  $U = F[t] \cdot u$ , where  $u = g \cdot v$  and  $g$  is a monic divisor of  $f$ . Since  $0 = \langle u, v \rangle = \langle g \cdot v, v \rangle = \langle v, g^* \cdot v \rangle$ , we deduce that  $g^* \cdot v \in U$ , i.e.,  $g$  divides  $g^*$ . It follows that  $g^* = g$ . Thus  $f = gh$ , with  $h^* = h$  also monic. As  $\langle v, w \rangle \neq 0$ , we have  $w \notin U$  which implies that  $f_1$  does not divide  $h$ . Thus  $h_1$ , the square-free part of  $h$ , is a proper divisor of  $f_1$  and  $h_1^* = h_1$ . If  $h_1 \neq 1$ , then by applying an argument used above we can construct a splitting of  $A$ . Otherwise  $U = 0$ , i.e.,  $V = W \oplus W^\perp$ . If  $W \neq V$ , then again  $A$  splits. Hence we may assume that  $V = W$ .

The vectors  $S^i v$  for  $0 \leq i < n$  form a basis of  $V$ . Hence if  $W_0$  is the subspace of  $V$  with basis  $\{v_i = (t + t^2)^{i-1} \cdot v : 1 \leq i \leq m\}$  and  $W_1 = t \cdot W_0$ , then  $V = W_0 \oplus W_1$ . Since

$$\langle (t + t^2)^i \cdot v, (t + t^2)^j \cdot v \rangle_1 = (-1)^{i+j} \langle t^{i+j} \cdot v, t^{i+j} \cdot v \rangle_1 = 0,$$

we have  $W_0^{\perp 1} = W_0$  and similarly  $W_1^{\perp 1} = W_1$ . Since

$$\begin{aligned} \langle t(t + t^2)^i \cdot v, (t + t^2)^j \cdot v \rangle &= (-1)^{i+j} \langle t^{i+j+1} \cdot v, t^{i+j} \cdot v \rangle \\ &= (-1)^{i+j} \langle t^{i+j+1} \cdot v, t^{i+j+1} \cdot v \rangle_1 = 0, \end{aligned}$$

we have also  $W_1^\perp = W_0$ . Hence there exists a unique ordered basis  $\{w_1, \dots, w_m\}$  of  $W_1$  such that  $\{v_1, w_1, \dots, v_m, w_m\}$  is a symplectic basis of  $V$ . Denote by  $P$  the matrix whose columns are the vectors  $v_1, v_2, \dots, v_m, w_1, w_2, \dots, w_m$  (in this order). Since  $\langle w_j, v_i \rangle = 0$ , we have  $\langle v_i, w_j \rangle = \langle v_i, w_j \rangle_1$  for all  $i, j$ . We infer that

$$P'AP = \begin{bmatrix} B & I_m \\ 0 & C \end{bmatrix}$$

for some invertible symmetric matrices  $B$  and  $C$ . It remains to observe that

$$Y = \begin{bmatrix} -I_m & C^{-1} \\ 0 & I_m \end{bmatrix}$$

is involutory and satisfies  $YP'APY' = P'A'P$ .

This completes the description of our algorithm (and the proof of Theorem 1.4).

**5. Two open problems.** We denote by  $F$  an arbitrary field. The matrices will be denoted by lower case latin letters. We set  $M_n = M_n(F)$  and  $G = \text{SL}_n(F)$ . The congruence action of  $G$  on  $M_n$  is defined by  $a \cdot x = axa'$  ( $a \in G, x \in M_n$ ). It is one of the several most important group actions studied in Linear Algebra. (One usually considers the restriction of this action to symmetric or skew-symmetric matrices.)

Let  $F[M_n]$  be the algebra of polynomial functions on  $M_n$ . The congruence action of  $G$  on  $M_n$  induces an action of  $G$  on  $F[M_n]$  by

$$(a \cdot f)(x) = f(a^{-1} \cdot x) = f(a^{-1}x(a')^{-1}),$$

where  $a \in G$ ,  $f \in F[M_n]$ , and  $x \in M_n$ .

When  $F = \mathbf{C}$ , Adamovich and Golovina [1] have computed the subalgebra,  $\mathbf{C}[M_n]^G$ , of  $G$ -invariants in  $\mathbf{C}[M_n]$ . More precisely, they have shown that this subalgebra is isomorphic to a polynomial algebra over  $\mathbf{C}$  in  $[(n+1)/2]$  explicitly given algebraically independent generators.

One can ask many interesting questions about the congruence action of  $G$  on  $M_n$  but we shall state only two of them.

**Problem 1** *Extend the results of Adamovich and Golovina to algebraically closed fields of prime characteristic (or to arbitrary fields).*

**Problem 2** *If  $F$  is algebraically closed and  $x \in M_n$ , determine which  $G$ -orbits are contained in the Zariski closure of the orbit  $G \cdot x$ .*

In connection with Proposition 3.1 we would like to make the following remark. This proposition shows that an arbitrary  $A \in M_n(F)$  is congruent to the direct sum of various nilpotent Jordan blocks  $N_r$  and a nonsingular matrix  $X$  (where either of these two types may be missing). By applying the well known theory of matrix pencils  $\lambda A + \mu B$  to the special pencils  $\lambda A + \mu A'$ , it is easy to see that the nilpotent Jordan blocks  $N_r$  are indecomposable under congruence and that the sizes of Jordan blocks  $N_r$  and their multiplicities in the above decomposition are uniquely determined by  $A$ . As shown by Gabriel [6],  $X$  is unique up to congruence. In the statement of Gabriel's theorem as given by Waterhouse [11], instead of the Jordan blocks  $N_r$ , more complicated singular indecomposable blocks  $B_r$  are used. Since for each size  $r \geq 1$  there is only one (up to congruence) singular indecomposable matrix of size  $r$ , the matrices  $B_r$  and  $N_r$  must be congruent. This can be also shown directly by constructing a permutation matrix  $P$  such that  $PB_rP' = N_r$ .

**Acknowledgement.** An anonymous referee of an earlier mini-version of this paper is to be thanked for pointing out the references [7] and [11].

#### REFERENCES

- [1] O.M. Adamovich and E.O. Golovina. Invariants of a pair of bilinear forms (in Russian). *Vestnik Moskovskogo Universiteta, Matematika*, 32:15–18, 1977.
- [2] L.V. Antonyan. On the classification of homogeneous elements of  $\mathbf{Z}_2$ -graded semisimple Lie algebras (in Russian). *Vestnik Moskovskogo Universiteta, Seriya I Matematika, Mekhanika*, 29–34. 1982.
- [3] C.S. Ballantine and E.L. Yip. Congruence and conjunctivity of matrices to their adjoints. *Linear Algebra and its Applications*, 41: 33–72, 1981.
- [4] J.H. Davenport. *On the Integration of Algebraic Functions*. Lecture Notes in Computer Science 102. Springer-Verlag, Berlin, 1981.
- [5] D.Ž. Đoković and Kh. Ikramov. A square matrix is congruent to its transpose. *Journal of Algebra* 257:97–105, 2002.
- [6] P. Gabriel. Appendix: Degenerate bilinear forms. *Journal of Algebra*, 31:67–72, 1974.
- [7] R. Gow. The equivalence of an invertible matrix to its transpose. *Linear and Multilinear Algebra*, 8:329–336, 1980.
- [8] I. Kaplansky. *Linear Algebra and Geometry, A second course*. Allyn and Bacon, Boston, 1969.
- [9] C. Riehm. The equivalence of bilinear forms. *Journal of Algebra*, 31:45–66, 1974.
- [10] R.C. Thompson. Pencils of complex and real symmetric and skew matrices. *Linear Algebra and its Applications*, 147:323–371, 1991.
- [11] W.C. Waterhouse. The number of congruence classes in  $M_n(\mathbf{F}_q)$ . *Finite Fields and their Applications*, 1:57–63, 1995.