Strongly Real Elements of Orthogonal Groups in Even Characteristic

Johanna Rämö

Queen Mary University of London,
School of Mathematical Sciences,
Mile End Road,
London E1 4NS
j.ramo@qmul.ac.uk

Abstract

Suppose that both n and q are even. We show that the finite simple group $\Omega_n^\varepsilon(q)$ is strongly real if and only if $4 \mid n$. We also prove that the unipotent elements in the finite simple group $\Omega_n^\varepsilon(q)$ are strongly real.

Keywords: Strongly real, involution, orthogonal groups, finite simple groups

1 Introduction

Suppose that G is a group and $g \in G$. The element g is called *real* if there is an element x of G that inverts g, that is, $x^{-1}gx = g^{-1}$. An involution is an element of order two. The element g is called *strongly real* if there is an involution x of G that inverts g. The group G is called real if all the elements are real, and strongly real if all the elements are strongly real.

We consider the following problem: "Which finite simple groups are strongly real?" It is equivalent to Problem 14.82 in the Kourovka Notebook [9]: "Describe the finite simple groups in which every element is a product of two involutions."

The problem has been solved for several finite simple groups. The alternating groups A_n are strongly real if and only if $n \in \{5, 6, 10, 14\}$ [1], and it has been shown that $\mathrm{PSp}_{2n}(q)$ is strongly real if $q \not\equiv 3 \pmod 4$ [3, 5, 6]. Knüppel and Thomsen [7] have determined which of the orthogonal groups in odd characteristic are strongly real, and Galt [4] has also obtained similar results. Kolesnikov and Nuzhin [8] have shown that of the sporadic groups, only J_1 and J_2 are strongly real.

On the other hand, Tiep and Zalesski [11] have listed all the quasisimple groups that are real. Since a group cannot be strongly real if it is not real, we only need to consider the real groups. From these results it follows that the only groups that need to be dealt with are the orthogonal groups $\Omega_n^\varepsilon(q)$ in even characteristic, and the groups ${}^3\mathrm{D}_4(q)$. Thus far, all the groups considered have been strongly real if and only if they are real.

Here we will consider the simple groups $\Omega_n^\varepsilon(q)$ where q is even. When the characteristic is even and dimension is odd, the ortogonal groups are isomorphic with symplectic groups, which we already know to be strongly real. Hence, we do not need to consider them. In their paper, Tiep and Zalesski proved that $\Omega_n^\varepsilon(q)$ is real if and only if 4 divides n. The following theorem shows that the group is strongly real if and only if it is real.

Theorem 1.1. *Suppose that n and q are even. The finite simple group $\Omega_n^\varepsilon(q)$ is strongly real if and only if $4 \mid n$.*

We will also prove that the unipotent elements in this group are always strongly real.

Theorem 1.2. *When n and q are even, the unipotent elements of the finite simple group $\Omega_n^\varepsilon(q)$ are strongly real.*

2 Preliminaries

2.1 Orthogonal transformations

Suppose that V is a finite-dimensional vector space over a finite field F. A *quadratic form* is a mapping $Q: V \to F$ satisfying

$$Q(au + bv) = a^2Q(u) + abB(u, v) + b^2Q(v)$$

for all $u, v \in V$ and $a, b \in F$, where B is a symmetric bilinear form. The form B is called the associated bilinear form of Q. The form B is *non-degenerate* if

$$\mathrm{rad}(B) = \{v \in V \mid B(u, v) = 0 \text{ for all } u \in V\} = 0.$$

The subspace $\mathrm{rad}(B)$ is called the radical of B. The form Q is *regular* if

$$\mathrm{rad}(Q) = \{v \in \mathrm{rad}(B) \mid Q(v) = 0\} = 0.$$

A linear transformation S of V is called *orthogonal* if $Q(vS) = Q(v)$ for all $v \in V$. The orthogonal transformations of V form a group $\mathrm{O}(V)$. We can also denote this group $\mathrm{O}^{\varepsilon}_n(q)$, where n is the dimension of V, q the order of F and ε the type of the quadratic form Q ($+$,$-$ or 0).

The orthogonal group $\mathrm{O}(V)$ has a subgroup $\Omega(V)$ which in almost all cases coincides with the derived group $\mathrm{O}(V)'$. Apart from a few exceptions, the quotient group $\mathrm{P}\Omega(V) = \Omega(V)/\left(\Omega(V) \cap \{1, -1\}\right)$ is simple.

2.2 Cyclic and bicyclic spaces

A vector space V is called *cyclic* relative to S if it has a basis

$$\{v, vS, \ldots, vS^{n-1}\},$$

where v is some element of V. The element v is called a generator of V, and the order $p(x)$ of v is defined to be the polynomial of least degree having the property $vp(S) = 0$. The order $p(x)$ is equal to the minimal polynomial of S, and $\deg(p(x)) = \dim(V)$.

A vector space V is called *bicyclic* if we have $V = U \oplus W$, where U and W are cyclic relative to S, and have generators of the same order.

2.3 The reciprocal of a polynomial

Let $p(x)$ be a polynomial. The *reciprocal* of $p(x)$ is the monic polynomial $\tilde{p}(x) = p(0)^{-1}x^n p(x^{-1})$, where $n = \deg(p(x))$. The polynomial $p(x)$ is called self-reciprocal if $p(x) = \tilde{p}(x)$. The following result follows from the fact that either $x+1$ or $x-1$ divides every self-reciprocal polynomial of odd degree.

Lemma 2.1. *The only irreducible self-reciprocal monic polynomials of odd degree are $x+1$ and $x-1$.*

3 Finding the involutions

From now on, we will assume that V is endowed with a regular quadratic form Q with the associated bilinear form B. Let S be an orthogonal transformation of V.

The following theorem is proved by Wonenburger [12] in odd characteristic, Gow [5] and Ellers and Nolte [3] in even characteristic, and by Djoković [2] in all characteristics.

Theorem 3.1. *The transformation S is a product of two orthogonal involutions of V.*

This means that there is an orthogonal involution of V that inverts S. Namely, if $S = H_1H_2$, where H_1 and H_2 are involutions, then $H_1SH_1 = H_1H_1H_2H_1 = H_2H_1 = S^{-1}$. Also $H_2SH_2 = S^{-1}$. We will show that in some cases these involutions are in $\Omega(V)$.

Wonenburger [12] has shown that the space V can be decomposed into cyclic and bicyclic subspaces that are S-invariant, non-degenerate and orthogonal to each other. The results hold in both even and odd characteristic. We describe here briefly how the decomposition is done.

Let $p(x)$ be the minimal polynomial of S. We can write $p(x) = \prod r_i(x)^{h_i}$, where either $r_i(x)$ is self-reciprocal and irreducible, or $r_i(x) = g_i(x)\tilde{g}_i(x)$, where $g_i(x)$ is irreducible but not self-reciprocal. Denote $K_i = \ker(r_i(S)^{h_i})$. Now we have $V = \bigoplus K_i$. The subspaces K_i are non-degenerate and orthogonal to each other. Each K_i is a direct sum of non-degenerate cyclic and bicyclic subspaces that are orthogonal to each other.

For the cyclic subspaces, the minimal polynomial of S is either of the form $r(x)^h$, where $r(x)$ is self-reciprocal and irreducible, or $(g(x)\tilde{g}(x))^h$, where $g(x)$ is irreducible but not self-reciprocal. If we have a bicyclic subspace $U \oplus W$,

then the minimal polynomial of both $S|_U$ and $S|_W$ is $r(x)^h$, where $r(x)$ is irreducible and self-reciprocal.

Decompose the space V into cyclic and bicyclic subspaces, say $V = \bigoplus V_j$. For each subspace V_j it is relatively easy to find an orthogonal involution H_j that inverts $S|_{V_j}$. Now $H = \bigoplus H_j$ is an involution that inverts S. Since the subspaces are orthogonal to each other, H is an orthogonal transformation of V.

3.1 Even characteristic

We will henceforth assume that the characteristic of the field F is even. If the dimension of the vector space V is odd, the orthogonal group is isomorphic with a symplectic group. Hence, we can assume that the dimension of the space V is even.

We wish to show that if the dimension of V is divisible by four and S is in $\Omega(V)$, then we can choose the inverting involution H in such a way that it is an element of $\Omega(V)$. In fact, we will show that for all the orthogonal transformations of V, the inverting involution can be chosen to be in $\Omega(V)$.

In even characteristic we can use the following well-known criterion to determine whether an orthogonal transformation is in $\Omega(V)$.

Proposition 3.2. *The element A of $\mathrm{O}(V)$ is in $\Omega(V)$ if and only if $\mathrm{rank}(I + A)$ is even.*

Proof. When the characteristic is two and the dimension of V is even, the group $\Omega(V)$ can be defined to be the set of all elements of $\mathrm{O}(V)$ for which the dimension of the fixed space is even.

Suppose that $A \in \mathrm{O}(V)$, and assume that the dimension of $\mathrm{fix}(A)$ is k. Now $\mathrm{rank}(I + A) = \dim(V) - k$. Since $\dim(V)$ is even, we know that k is even if and only if $\mathrm{rank}(I + A)$ is even. □

Now we just need to find an inverting involution H_j for each cyclic and bicyclic subspace V_j in the decomposition of V, and calculate $\mathrm{rank}(I + H_j)$. Then we consider the sum of the ranks to find out if $H = \bigoplus H_j$ is an element of $\Omega(V)$.

3.2 Cyclic subspaces

Suppose that we have a cyclic space $V = \langle v, vS, \ldots vS^{n-1} \rangle$.

Proposition 3.3. *We can find an orthogonal involution J such that $JSJ = S^{-1}$, and*

$$\operatorname{rank}(I+J) = \begin{cases} \textit{even} & \textit{if } n \equiv 0 \textit{ or } n \equiv 1 \pmod 4 \\ \textit{odd} & \textit{if } n \equiv 2 \textit{ or } n \equiv 3 \pmod 4. \end{cases}$$

Proof. Let $vS^iJ = vS^{n-i-1}$ for all $i \in \{0, \ldots, n-1\}$. With respect to the basis $v, vS, \ldots, vS^{n-1}$, we can write

$$J = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

Gow [5] has shown that J is an orthogonal involution that conjugates S to its inverse.

We give here another proof for the orthogonality of J, as the involution will be needed also in the bicyclic case, and we want to have a closer look at its properties. It is enough to prove that J preserves B and Q for the basis vectors. We know that S preserves B, so it follows that

$$B(vS^iJ, vS^jJ) = B(vS^{n-i-1}, vS^{n-j-1}) = B(vS^j, vS^i)$$

for all $i, j \in \{0, \ldots, n-1\}$. This means that $JBJ^T = B^T$. Since B is symmetric, we know that J preserves B. Similarly,

$$Q(vS^iJ) = Q(vS^{n-i-1}) = Q(vS^i)$$

for all $i \in \{0, \ldots, n-1\}$, and we can conclude that J is orthogonal.

Since we have

$$I + J = \begin{bmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \cdots & 1 & 0 \\ 1 & 0 & \cdots & 0 & 1 \end{bmatrix},$$

the rank of $I + J$ is even if $n \equiv 0$ or $n \equiv 1 \pmod 4$, and odd if $n \equiv 2$ or $n \equiv 3 \pmod 4$. □

Proposition 3.4. *If $n \equiv 2 \pmod 4$ and S is unipotent, we can find an orthogonal involution K such that $KSK = S^{-1}$ and $\operatorname{rank}(I+K)$ is even.*

Proof. Suppose that the minimal polynomial of S is $p(x) = \sum_{k=0}^{n} a_k x^k$. Since $p(x)$ is self-reciprocal, we have $a_0 = 1 = a_n$ and $a_k = a_{n-k}$ for all $k \in \{1, \ldots, n-1\}$.

Let K be the linear transformation defined by $vS^iK = vS^{n-i}$ for all $i \in \{0, \ldots, n-1\}$. We can write

$$K = \begin{bmatrix} 1 & a_1 & a_2 & \cdots & a_2 & a_1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

Ellers and Nolte [3] have shown that K is an orthogonal involution that conjugates S to its inverse.

Now we have

$$I + K = \begin{bmatrix} 0 & a_1 & a_2 & \cdots & a_2 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 1 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 1 & \cdots & 1 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

We notice that if n is odd, then the first row is linearly dependent on the other rows. On the other hand, if n is even, then all the elements in row $\frac{n}{2}+1$ are equal to zero. Hence, we have

$$\operatorname{rank}(I+K) = \begin{cases} \frac{n-1}{2} & \text{if } n \text{ is odd} \\ \frac{n-2}{2} & \text{if } n \text{ is even and } a_{n/2} = 0 \\ \frac{n}{2} & \text{if } n \text{ is even and } a_{n/2} \neq 0. \end{cases}$$

Suppose then that S is unipotent and $n \equiv 2 \pmod 4$. Let m be such that $n = 4m+2$. Since S is unipotent, we have $p(x) = (x+1)^n$, and hence

$a_k = \binom{n}{k}$ for all $k \in \{0, \ldots, n\}$. We notice that

$$\begin{aligned} a_{n/2} = a_{2m+1} &= \binom{n}{2m+1} \\ &= \sum_{k=0}^{2m+1} \binom{2m+1}{k}\binom{2m+1}{2m+1-k} \\ &= 2\sum_{k=0}^{m} \binom{2m+1}{k}\binom{2m+1}{2m+1-k} \\ &= 0 \end{aligned}$$

because the characteristic of F is even. Thus, we know that $\operatorname{rank}(I+K) = \frac{n-2}{2} = 2m$. □

3.3 Bicyclic subspaces

Suppose now that we have a bicyclic space $V = U \oplus W$, where

$$U = \langle u, uS, \ldots uS^{n-1} \rangle \text{ and } W = \langle w, wS, \ldots wS^{n-1} \rangle.$$

3.3.1 Even dimension

We assume first that the dimension n is even.

Proposition 3.5. *We can find an orthogonal involution L such that $LSL = S^{-1}$ and $\operatorname{rank}(I+L)$ is even.*

Proof. Let L be the linear transformation defined by $uS^iL = vS^{n-i}$ and $wS^iL = wS^{n-i}$ for all $i \in \{0, \ldots, n-1\}$. Now we can write

$$L = \begin{bmatrix} K & 0 \\ 0 & K \end{bmatrix},$$

where K is the involution defined in Proposition 3.4.

The proof of Lemma 4 in [3] shows that the involution L is orthogonal and inverts S. We notice that $\operatorname{rank}(I+L) = 2 \cdot \operatorname{rank}(I+K)$, which proves the claim. □

3.3.2 Odd dimension

Unfortunately, we cannot use the involution L when n is odd, because it might not be orthogonal. The case of bicyclic subspaces where n is odd turns out to be the most difficult, and we need to know very well what the forms B and Q look like before we can show that the involutions we choose to use are orthogonal.

Suppose that the dimension n is odd. By Lemma 2.1, we know that the mimimal polynomial of both $S|_U$ and $S|_W$ is $p(x) = (x+1)^n$, where n is odd. Let $v_1, v_2, \ldots, v_n$ be a basis of U with respect to which $S|_U$ is in the Jordan normal form, and $v_{n+1}, v_{n+2}, \ldots, v_{2n}$ a basis of W with respect to which $S|_W$ is in the Jordan normal form. Now

$$\begin{aligned} v_1 S &= v_1 \\ v_2 S &= v_1 + v_2 \\ &\vdots \\ v_n S &= v_{n-1} + v_n \\ v_{n+1} S &= v_{n+1} \\ v_{n+2} S &= v_{n+1} + v_{n+2} \\ &\vdots \\ v_{2n} S &= v_{2n-1} + v_{2n}. \end{aligned}$$

We begin by proving some lemmas that describe the forms B and Q. We write the matrix of B in block form

$$B = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix},$$

where the blocks correspond to the subspaces U and W with respect to the bases $v_1, \ldots, v_n$ and $v_{n+1}, \ldots, v_{2n}$.

The following lemma shows that the entries of each block are determined recursively.

Lemma 3.6. *If $i \in \{2, \ldots, n\} \cup \{n+2, \ldots, 2n\}$ and $j \in \{1, \ldots, n-1\} \cup \{n+1, \ldots, 2n-1\}$, then*

$$B(v_i, v_j) = B(v_{i-1}, v_j) + B(v_{i-1}, v_{j+1}).$$

Proof. Let $i \in \{2, \ldots, n\} \cup \{n+2, \ldots, 2n\}$ and $j \in \{1, \ldots, n-1\} \cup \{n+1, \ldots, 2n-1\}$. Now

$$\begin{aligned} B(v_i, v_{j+1}) &= B(v_i S, v_{j+1} S) = B(v_{i-1} + v_i, v_j + v_{j+1}) \\ &= B(v_{i-1}, v_j) + B(v_{i-1}, v_{j+1}) + B(v_i, v_j) + B(v_i, v_{j+1}). \end{aligned}$$

Hence, $B(v_i, v_j) = B(v_{i-1}, v_j) + B(v_{i-1}, v_{j+1})$. □

The first $n-1$ entries in the top row of each block B_i are equal to zero.

Lemma 3.7. *Suppose that $j \in \{1, \ldots, n-1\}$. Then*

$$\begin{aligned} &a) \quad B(v_1, v_j) = 0 \\ &b) \quad B(v_{n+1}, v_{n+j}) = 0 \\ &c) \quad B(v_1, v_{n+j}) = 0 \\ &d) \quad B(v_{n+1}, v_j) = 0. \end{aligned}$$

Proof. a) Let $j \in \{1, \ldots, n-1\}$. Since $B(v_1, v_{j+1}) = B(v_1 S, v_{j+1} S) = B(v_1, v_j) + B(v_1, v_{j+1})$, we have $B(v_1, v_j) = 0$.

Parts b), c) and d) are proved similarly. □

Except for the first row and last column of each block B_i, we have an explicit formula for the entries of B.

Lemma 3.8. *Suppose that $i \in \{2, \ldots, n\}$ and $j \in \{1, \ldots, n-1\}$. Then*

$$\begin{aligned} &a) \quad B(v_i, v_j) = \sum_{k=1}^{i+j-n} \binom{i-k-1}{n-j-1} B(v_k, v_n) \\ &b) \quad B(v_{n+i}, v_{n+j}) = \sum_{k=1}^{i+j-n} \binom{i-k-1}{n-j-1} B(v_{n+k}, v_{2n}) \\ &c) \quad B(v_i, v_{n+j}) = \sum_{k=1}^{i+j-n} \binom{i-k-1}{n-j-1} B(v_k, v_{2n}) \\ &d) \quad B(v_{n+i}, v_j) = \sum_{k=1}^{i+j-n} \binom{i-k-1}{n-j-1} B(v_{n+k}, v_n). \end{aligned}$$

Proof. a) We prove the claim by induction on i. Suppose first that $i = 2$. Now we have

$$\sum_{k=1}^{i+j-n} \binom{i-k-1}{n-j-1} B(v_k, v_n) = \sum_{k=1}^{1} \binom{-k+1}{n-j-1} B(v_k, v_n)$$
$$= \binom{0}{n-j-1} B(v_k, v_n) = \begin{cases} B(v_1, v_n) & \text{if } j = n-1 \\ 0 & \text{if } j \neq n-1. \end{cases}$$

On the other hand, we have

$$B(v_i, v_j) = B(v_2, v_j) = B(v_1, v_j) + B(v_1, v_{j+1}) = B(v_1, v_{j+1})$$
$$= \begin{cases} B(v_1, v_n) & \text{if } j = n-1 \\ 0 & \text{if } j \neq n-1. \end{cases}$$

by Lemmas 3.6 and 3.7 a), so the claim holds when $i = 2$.

Suppose then that the claim holds for some $i \in \{2, \ldots, n-1\}$. From Lemma 3.6 it follows that $B(v_{i+1}, v_j) = B(v_i, v_j) + B(v_i, v_{j+1})$. If $j \neq n-1$, we can use the induction hypothesis and Pascal's rule to obtain

$$\begin{aligned} & B(v_i, v_j) + B(v_i, v_{j+1}) \\ &= \sum_{k=1}^{i+j-n} \binom{i-k-1}{n-j-1} B(v_k, v_n) + \sum_{k=1}^{i+j-n+1} \binom{i-k-1}{n-j-2} B(v_k, v_n) \\ &= \sum_{k=1}^{i+j-n+1} \binom{i-k-1}{n-j-1} B(v_k, v_n) + \sum_{k=1}^{i+j-n+1} \binom{i-k-1}{n-j-2} B(v_k, v_n) \\ &= \sum_{k=1}^{i+j-n+1} \binom{i-k}{n-j-1} B(v_k, v_n). \end{aligned}$$

If $j = n-1$, we have by the induction hypothesis

$$\begin{aligned} & B(v_i, v_j) + B(v_i, v_{j+1}) = B(v_i, v_{n-1}) + B(v_i, v_n) \\ &= \sum_{k=1}^{i-1} \binom{i-k-1}{0} B(v_k, v_n) + B(v_i, v_n) = \sum_{k=1}^{i} \binom{i-k}{0} B(v_k, v_n) \\ &= \sum_{k=1}^{i+j-n+1} \binom{i-k}{n-j-1} B(v_k, v_n). \end{aligned}$$

This means that the claim holds for $i+1$.

Parts b), c) and d) are proved similarly. □

Each block B_i is anti-triangular.

Lemma 3.9. *Suppose that* $i \in \{1, \ldots, n\}$.

$$\begin{aligned} &a) \quad \textit{If } j \in \{1, \ldots, n-i\}, \textit{ then } B(v_i, v_j) = 0. \\ &b) \quad \textit{If } j \in \{n+1, \ldots, 2n-i\}, \textit{ then } B(v_{n+i}, v_j) = 0. \\ &c) \quad \textit{If } j \in \{n+1, \ldots, 2n-i\}, \textit{ then } B(v_i, v_j) = 0. \end{aligned}$$

Proof. a) If $i = 1$, then the claim holds by Lemma 3.7 a). Therefore, we can assume that $i > 1$, and use Lemma 3.8 a) to obtain

$$B(v_i, v_j) = \sum_{k=1}^{i+j-n} \binom{i-k-1}{n-j-1} B(v_k, v_n).$$

Because $j \leq n - i$, we have $i + j - n \leq 0$, and hence $B(v_i, v_j) = 0$.

Parts b) and c) are proved similarly. □

The entries on the anti-diagonal of a block B_i are all equal.

Lemma 3.10. *Suppose that* $i \in \{1, \ldots, n\}$. *Then*

$$\begin{aligned} &a) \quad B(v_i, v_{n-i+1}) = B(v_1, v_n) \\ &b) \quad B(v_{n+i}, v_{2n-i+1}) = B(v_{n+1}, v_{2n}) \\ &c) \quad B(v_i, v_{2n-i+1}) = B(v_1, v_{2n}). \end{aligned}$$

Proof. a) The claim clearly hold holds if $i = 1$, so we can assume that $i > 1$ and use Lemma 3.8 a). Now

$$B(v_i, v_{n-i+1}) = \sum_{k=1}^{1} \binom{i-k-1}{i-2} B(v_k, v_n) = B(v_1, v_n).$$

Parts b) and c) are proved similarly. □

The formula that gives the entries of B_i takes a particularly simple form on the entries right below the anti-diagonal of B_i.

Lemma 3.11. *Suppose that $i \in \{2, \dots, n\}$. Then*

$$a) \quad B(v_i, v_{n-i+2}) = \begin{cases} B(v_2, v_n) & \text{if } i \text{ is even} \\ B(v_2, v_n) + B(v_1, v_n) & \text{if } i \text{ is odd} \end{cases}$$

$$b) \quad B(v_{n+i}, v_{2n-i+2}) = \begin{cases} B(v_{n+2}, v_{2n}) & \text{if } i \text{ is even} \\ B(v_{n+2}, v_{2n}) + B(v_{n+1}, v_{2n}) & \text{if } i \text{ is odd.} \end{cases}$$

$$c) \quad B(v_i, v_{2n-i+2}) = \begin{cases} B(v_2, v_{2n}) & \text{if } i \text{ is even} \\ B(v_2, v_{2n}) + B(v_1, v_{2n}) & \text{if } i \text{ is odd.} \end{cases}$$

Proof. a) By Lemma 3.8 a) we have

$$\begin{aligned} B(v_i, v_{n-i+2}) =& \sum_{k=1}^{2} \binom{i-k-1}{i-3} B(v_k, v_n) \\ =& \binom{i-2}{i-3} B(v_1, v_n) + \binom{i-3}{i-3} B(v_2, v_n) \\ =& (i-2) B(v_1, v_n) + B(v_2, v_n). \end{aligned}$$

Now the claim follows.

Parts b) and c) are proved similarly. □

Lemma 3.12. *Suppose that $n > 1$.*

a) We have $B(v_1, v_n) = 0$, $Q(v_1) = 0$ and $B(v_1, v_{2n}) \neq 0$.

b) We have $B(v_{n+1}, v_{2n}) = 0$, $Q(v_{n+1}) = 0$ and $B(v_{n+1}, v_n) \neq 0$.

Proof. a) Since n is odd, we have $B(v_n, v_2) = B(v_2, v_n) + B(v_1, v_n)$ by Lemma 3.11 a). It follows that $B(v_1, v_n) = 0$.

Because

$$Q(v_2) = Q(v_2 S) = Q(v_1 + v_2) = Q(v_1) + Q(v_2) + B(v_1, v_2)$$

and $B(v_1, v_2) = 0$ by Lemma 3.7 a), we know that $Q(v_1) = 0$. From parts a) and c) of Lemma 3.9 it follows that $B(v_1, v_j) = 0$ for all $j \in \{1, \dots, n-1, n+1, \dots 2n-1\}$, and we have just seen that $B(v_1, v_n) = 0$. If $B(v_1, v_{2n}) = 0$, then $v_1 \in \mathrm{rad}(V)$. Since V is regular, we must have $v_1 = 0$ which is impossible. Thus, we know that $B(v_1, v_{2n}) \neq 0$.

b) The proof is similar. □

In the block B_1, every other entry in the last column is determined by the entries above it. The same holds for $B_2 + B_3$.

Lemma 3.13. *Suppose that $i \in \{1, \ldots, n\}$ is odd. Then*

$$B(v_i, v_n) = \sum_{k=1}^{i-1} a_k B(v_k, v_n)$$

and

$$B(v_i, v_{2n}) + B(v_{n+i}, v_n) = \sum_{k=1}^{i-1} a_k \left(B(v_k, v_{2n}) + B(v_{n+k}, v_n)\right)$$

for some $a_1, \ldots, a_{i-1} \in F$.

Proof. We start by showing that we can find such $a_1, \ldots, a_{i-1} \in F$ that the first equation holds. Let $s = \frac{n+i}{2}$. By Lemma 3.8 a), we have

$$B(v_s, v_s) = \sum_{k=1}^{i} \binom{s-k-1}{n-s-1} B(v_k, v_n).$$

The last term of this sum is

$$\binom{\frac{n-i}{2} - 1}{\frac{n-i}{2} - 1} B(v_i, v_n) = B(v_i, v_n),$$

and hence we have

$$B(v_s, v_s) = \sum_{k=1}^{i-1} \binom{s-k-1}{n-s-1} B(v_k, v_n) + B(v_i, v_n).$$

Since $B(v_s, v_s) = 0$, it follows that

$$B(v_i, v_n) = \sum_{k=1}^{i-1} \binom{s-k-1}{n-s-1} B(v_k, v_n).$$

This means that we can choose $a_k = \binom{s-k-1}{n-s-1}$.

Next, we need to prove that the second equation of the claim holds for the $a_1, \ldots a_{i-1}$ that we have chosen. By parts c) and d) of Lemma 3.8, we

have

$$\begin{aligned} &B(v_s, v_{n+s}) + B(v_{n+s}, v_s) \\ =&\sum_{k=1}^{i} \binom{s-k-1}{n-s-1} (B(v_k, v_{2n}) + B(v_{n+k}, v_n)). \end{aligned}$$

As above, we now notice that

$$\begin{aligned} &B(v_s, v_{n+s}) + B(v_{n+s}, v_s) \\ =&\sum_{k=1}^{i-1} \binom{s-k-1}{n-s-1} (B(v_k, v_{2n}) + B(v_{n+k}, v_n)) + B(v_i, v_{2n}) + B(v_{n+i}, v_n). \end{aligned}$$

Because $B(v_s, v_{n+s}) + B(v_{n+s}, v_s) = 0$, it follows that

$$\begin{aligned} B(v_i, v_{2n}) + B(v_{n+i}, v_n) =& \sum_{k=1}^{i-1} \binom{s-k-1}{n-s-1} (B(v_k, v_{2n}) + B(v_{n+k}, v_n)) \\ =& \sum_{k=1}^{i-1} a_k (B(v_k, v_{2n}) + B(v_{n+k}, v_n)). \end{aligned}$$

□

Example 3.14. If $n = 5$, then the matrix of B is

$$\left[\begin{array}{ccccc|ccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & c_1 \\ 0 & 0 & 0 & 0 & a_1 & 0 & 0 & 0 & c_1 & c_2 \\ 0 & 0 & 0 & a_1 & a_2 & 0 & 0 & c_1 & c_1+c_2 & * \\ 0 & 0 & a_1 & a_1+a_2 & * & 0 & c_1 & c_2 & * & * \\ 0 & a_1 & a_2 & * & * & c_1 & c_1+c_2 & * & * & * \\ \hline 0 & 0 & 0 & 0 & c_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & c_1 & c_1+c_2 & 0 & 0 & 0 & 0 & b_1 \\ 0 & 0 & c_1 & c_2 & * & 0 & 0 & 0 & b_1 & b_2 \\ 0 & c_1 & c_1+c_2 & * & * & 0 & 0 & b_1 & b_1+b_2 & * \\ c_1 & c_2 & * & * & * & 0 & b_1 & b_2 & * & * \end{array}\right]$$

for some $a_i, b_i, c_i, d_i \in F$.

Next we show that the basis can be chosen in such a way that $B_1 = B_2 + B_3$. We can also assume that $B(v_n, v_{2n}) = Q(v_n)$.

Lemma 3.15. *We can choose the basis $v_1, \ldots, v_{2n}$ in such a way that the following hold:*

$$\begin{aligned} &a) \quad B(v_i, v_j) = B(v_i, v_{n+j}) + B(v_{n+i}, v_j) \text{ for all } i, j \in \{1, \ldots, n\} \\ &b) \quad B(v_n, v_{2n}) = Q(v_n) \end{aligned}$$

Proof. a) Consider first the case $n = 1$. We have $B(v_1, v_1) = 0 = B(v_1, v_2) + B(v_2, v_1)$, and from the proof of Lemma 3.12 a) it follows that $B(v_1, v_2) = Q(v_1)$. Hence the claims hold.

Suppose then that $n > 2$. By Lemma 3.6, the values $B(v_i, v_j)$ are determined recursively. Hence, it is enough to prove the claim when $i = 1$ and $j \in \{1, \ldots, n\}$, and when $i \in \{2, \ldots, n\}$ and $j = n$.

Case 1: We start by showing that the claim holds when $i = 1$ and $j \in \{1, \ldots, n\}$. If $j \neq n$, then we have $B(v_1, v_{n+j}) + B(v_{n+1}, v_j) = 0$ by parts c) and d) of Lemma 3.7. If $j = n$, we substitute $i = n$ in Lemma 3.10 c), to obtain $B(v_1, v_{2n}) + B(v_{n+1}, v_n) = 2B(v_1, v_{2n}) = 0$.

On the other hand, we have $B(v_1, v_j) = 0$ by Lemmas 3.7 a) and 3.12 a). Hence, the claim holds when $i = 1$.

Case 2: Next we prove that the claim holds when $i = 2$ and $j = n$. Suppose first that $B(v_2, v_n) \neq 0$. From Lemma 3.11 c), substituting $i = n$, we obtain

$$B(v_2, v_{2n}) + B(v_{n+2}, v_n) = B(v_2, v_{2n}) + B(v_2, v_{2n}) + B(v_1, v_{2n}) = B(v_1, v_{2n}).$$

We will show that the basis can be chosen in such a way that $B(v_2, v_n) = B(v_1, v_{2n})$.

By Lemma 3.12 a), we have $B(v_1, v_{2n}) \neq 0$. Denote

$$a = \frac{B(v_2, v_n)}{B(v_1, v_{2n})},$$

and let

$$v_i' = \begin{cases} v_i & \text{if } i \in \{1, \ldots, n\} \\ a v_i & \text{if } i \in \{n+1, \ldots, 2n\}. \end{cases}$$

Since S is still in the Jordan normal form with respect to the basis $v_1', \ldots, v_{2n}'$, all the earlier results hold, and the basis can be changed. We have

$$B(v_1', v_{2n}') = aB(v_1, v_{2n}) = B(v_2, v_n) = B(v_2', v_n'),$$

so the claim holds if $B(v_2, v_n) \neq 0$.

Hence, we can suppose that $B(v_2, v_n) = 0$. We can also assume that $B(v_{n+2}, v_{2n}) = 0$ because otherwise we could interchange the spaces $U = \langle v_1, v_2, \ldots, v_n \rangle$ and $W = \langle v_{n+1}, v_{n+2}, \ldots, v_{2n} \rangle$.

Let

$$v_i' = \begin{cases} v_i + v_{n+i} & \text{if } i \in \{1, \ldots n\} \\ v_i & \text{if } i \in \{n+1, \ldots 2n\}. \end{cases}$$

As before, we can change to the basis $v_1', \ldots, v_{2n}'$. Since we assumed that $B(v_2, v_n) = 0 = B(v_{n+2}, v_{2n})$, it follows that

$$\begin{aligned} B(v_2', v_n') &= B(v_2, v_n) + B(v_2, v_{2n}) + B(v_{n+2}, v_n) + B(v_{n+2}, v_{2n}) \\ &= B(v_{n+2}, v_{2n}) + B(v_2, v_{2n}) + B(v_{n+2}, v_n) + B(v_{n+2}, v_{2n}) \\ &= B(v_2', v_{2n}') + B(v_{n+2}', v_n'). \end{aligned}$$

Thus, the claim holds when $i = 2$ and $j = n$.

Case 3: Finally, we will show that we can choose $B(v_i, v_n) = B(v_i, v_{2n}) + B(v_{n+i}, v_n)$ for all $i \in \{3, \ldots n\}$. Suppose that i is the smallest index for which $B(v_i, v_n) \neq B(v_i, v_{2n}) + B(v_{n+i}, v_n)$.

Assume first that i is odd. By Lemma 3.13, the values $B(v_i, v_n)$ and $B(v_i, v_{2n}) + B(v_{n+i}, v_n)$ depend only on the values of the form for indices smaller than i, and they do that in exactly the same way. Since we know that the equality holds for all the smaller indices, we must have $B(v_i, v_n) = B(v_i, v_{2n}) + B(v_{n+i}, v_n)$.

Now we know that i is even. Let

$$b = \frac{\sum_{k=1}^{i-2} \binom{n-1-k}{n-1-i} B(v_k, v_{2n}) + B(v_{i-1}, v_{2n}) + B(v_i, v_n)}{B(v_1, v_{2n})}$$

and denote

$$v_l' = \begin{cases} v_l & \text{if } l \in \{1, \ldots i-2\} \\ v_l + b v_{l-i+2} & \text{if } l \in \{i-1, \ldots n\} \\ v_l & \text{if } l \in \{n+1, \ldots 2n\}. \end{cases}$$

We notice that S is still in the Jordan normal form with respect to the basis $v_1', \ldots, v_{2n}'$. If $l \in \{1, \ldots, i-2\}$, then

$$B(v_l', v_n') = B(v_l, v_n) + bB(v_l, v_{n-i+2}) = B(v_l, v_n)$$

by Lemma 3.9 a). Also, we have

$$\begin{aligned} B(v'_{i-1}, v'_n) =& B(v_{i-1}, v_n) + bB(v_{i-1}, v_{n-i+2}) + bB(v_1, v_n) + b^2 B(v_1, v_{n-i+2}) \\ =& B(v_{i-1}, v_n) \end{aligned}$$

by Lemmas 3.10 a) and 3.9 a). This means that the change of basis does not affect the values of the form for indices smaller than i.

By Lemma 3.8 c), we have

$$B(v'_n, v'_{n+i}) = \sum_{k=1}^{i} \binom{n-k-1}{n-i-1} B(v'_k, v'_{2n}).$$

It follows that

$$B(v'_i, v'_{2n}) + B(v'_{n+i}, v'_n) = \sum_{k=1}^{i-1} \binom{n-k-1}{n-i-1} B(v'_k, v'_{2n}). \tag{1}$$

Since i is even and n is odd, we know that $\binom{n-i}{n-i-1} = n-i$ is odd. Therefore, the coefficient of $B(v'_{i-1}, v'_{2n})$ in the sum (1) is equal to 1. Now we have

$$\begin{aligned} & \sum_{k=1}^{i-1} \binom{n-k-1}{n-i-1} B(v'_k, v'_{2n}) \\ =& \sum_{k=1}^{i-2} \binom{n-k-1}{n-i-1} B(v'_k, v'_{2n}) + B(v'_{i-1}, v'_{2n}) \\ =& \sum_{k=1}^{i-2} \binom{n-k-1}{n-i-1} B(v_k, v_{2n}) + B(v_{i-1}, v_{2n}) + bB(v_1, v_{2n}) \\ =& B(v_i, v_n) \end{aligned}$$

by the definition of b.

On the other hand, we notice that

$$B(v'_i, v'_n) = B(v_i, v_n) + bB(v_i, v_{n-i+2}) + bB(v_2, v_n) + b^2 B(v_2, v_{n-i+2}).$$

Since i is even, we have $B(v_i, v_{n-i+2}) = B(v_2, v_n)$ by Lemma 3.11 a). Also, since $i \geq 3$, we must in fact have $i \geq 4$. Now it follows from Lemma 3.9 a) that $B(v_2, v_{n-i+2}) = 0$. Hence, we have $B(v'_i, v'_n) = B(v_i, v_n)$, and can conclude that $B(v'_i, v'_{2n}) + B(v'_{n+i}, v'_n) = B(v'_i, v'_n)$.

b) Let

$$c = \frac{B(v_n, v_{2n}) + Q(v_n)}{B(v_1, v_{2n})},$$

and denote

$$v_i' = \begin{cases} v_i & \text{if } i \in \{1, \dots n-1\} \\ v_i + cv_1 & \text{if } i = n \\ v_i & \text{if } i \in \{n+1, \dots 2n\}. \end{cases}$$

We notice that S is still in the Jordan normal form with respect to the basis $v_1', \dots v_{2n}'$. We need to make sure that the change of basis does not affect the results of part a).

Firstly, we notice that if $i, j \neq n$, then $B(v_i', v_j') = B(v_i, v_j)$. Also, the statement of part a) clearly holds if $i, j = n$.

This means that we can suppose that $i \neq n$ and $j = n$. From Lemma 3.7 a), we obtain

$$B(v_i', v_n') = B(v_i, v_n) + cB(v_i, v_1) = B(v_i, v_n).$$

Also, we have

$$\begin{aligned} B(v_i', v_{2n}') + B(v_{n+i}', v_n') =& B(v_i, v_{2n}) + B(v_{n+i}, v_n) + cB(v_{n+i}, v_1) \\ =& B(v_i, v_{2n}) + B(v_{n+i}, v_n) \end{aligned}$$

by Lemma 3.7 c). Hence, the results of part a) hold for the basis $v_1', \dots, v_{2n}'$.

Now we have

$$B(v_n', v_{2n}') = B(v_n, v_{2n}) + cB(v_1, v_{2n}) = Q(v_n)$$

by the definition of c.

On the other hand, we notice that

$$Q(v_n') = Q(v_n + cv_1) = Q(v_n) + c^2 Q(v_1) + cB(v_1, v_n) = Q(v_n)$$

by Lemma 3.12 a). Thus, we can choose the basis in such a way that $B(v_n, v_{2n}) = Q(v_n)$.

□

Now we know enough about the forms B and Q, and can finally introduce the involutions that are used in this section.

Proposition 3.16. *We can find an orthogonal involution M such that $MSM = S^{-1}$ and* $\operatorname{rank}(I + M)$ *is odd.*

Proof. Denote $u = v_n$ and $w = v_{2n}$. We notice that $U = \langle u, uS, \ldots, uS^{n-1} \rangle$ and $W = \langle w, wS, \ldots, wS^{n-1} \rangle$.

Let M be the linear transformation defined by $uS^iM = uS^{n-i-1}$ and $wS^iM = uS^{n-i-1} + wS^{n-i-1}$ for all $i \in \{0, \ldots, n-1\}$. We can write

$$M = \begin{bmatrix} J & 0 \\ J & J \end{bmatrix},$$

where J is the involution defined in Proposition 3.3.

Now M is an involution and $\operatorname{rank}(I + M) = n$. Next, we will show that M inverts S. Let S' be the matrix of $S|_U$ and $S|_W$. Since we know by Proposition 3.3 that $JS'J = (S')^{-1}$, it follows that

$$MSM = \begin{bmatrix} J & 0 \\ J & J \end{bmatrix} \begin{bmatrix} S' & 0 \\ 0 & S' \end{bmatrix} \begin{bmatrix} J & 0 \\ J & J \end{bmatrix} = \begin{bmatrix} JS'J & 0 \\ 2JS'J & JS'J \end{bmatrix} = S^{-1}.$$

Finally, we need to show that M preserves the quadratic form Q. It is enough to show that M preserves B and Q for the basis vectors. Recall that we have written B in block form

$$B = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix}.$$

This was done with respect to the basis $v_1, \ldots, v_{2n}$. However, since we have changed the basis, the blocks are now written with respect to the basis

$$u, uS, \ldots, uS^{n-1}, w, wS, \ldots, wS^{n-1}.$$

Notice that this change of basis does not affect the result of Lemma 3.15 a), and we can still assume that $B_1 = B_2 + B_3$.

We will first prove that M preserves B, and begin by observing that

$$\begin{aligned} MBM^T &= \begin{bmatrix} J & 0 \\ J & J \end{bmatrix} \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix} \begin{bmatrix} J & J \\ 0 & J \end{bmatrix} \\ &= \begin{bmatrix} JB_1J & JB_1J + JB_2J \\ JB_1J + JB_3J & JB_1J + JB_3J + JB_2J + JB_4J \end{bmatrix}. \end{aligned}$$

Since S preserves B, we have $S'B_i(S')^T = B_i$ for every $i \in \{1, \ldots, 4\}$. This means that each B_i can in fact be regarded as a bilinear form that is preserved by S'. From the proof of Proposition 3.3, it follows that $JB_iJ = B_i^T$ for every i.

Using this, and and observing that $B_1^T = B_1$, $B_4^T = B_4$ and $B_2 = B_3^T$, we obtain

$$MBM^T = \begin{bmatrix} B_1 & B_1 + B_3 \\ B_1 + B_2 & B_1 + B_2 + B_3 + B_4 \end{bmatrix}.$$

By Lemma 3.15, we can assume that $B_1 = B_2 + B_3$, and hence we have

$$MBM^T = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix} = B.$$

This means that M preserves B.

Because S preserves Q, we have

$$Q(uS^iM) = Q(uS^{n-1-i}) = Q(uS^i)$$

for all $i \in \{0, \ldots, n-1\}$. Also,

$$\begin{aligned} Q(wS^iM) &= Q(uS^{n-1-i} + wS^{n-1-i}) \\ &= Q(uS^{n-1-i}) + Q(wS^{n-1-i}) + B(uS^{n-1-i}, wS^{n-1-i}) \\ &= Q(u) + Q(w) + B(u, w). \end{aligned}$$

for all $i \in \{0, \ldots, n-1\}$. By Lemma 3.15, we can choose $B(u, w) = B(v_n, v_{2n}) = Q(v_n) = Q(u)$, and hence $Q(wS^iM) = Q(w) = Q(wS^i)$. Thus, M preserves the quadratic form Q. □

Proposition 3.17. *We can find an orthogonal involution N such that $NSN = S^{-1}$ and $\operatorname{rank}(I + N)$ is even.*

Proof. Let N be the linear transformation of V defined by $uS^iN = uS^{n-i}$ and $wS^iN = wS^{n+1-i}$ for all $i \in \{0, \ldots, n-1\}$.

Let P be the linear transformation of W defined by $wS^iP = wS^{n+1-i}$ for all $i \in \{0, \ldots, n-1\}$. Now we can write

$$N = \begin{bmatrix} K & 0 \\ 0 & P \end{bmatrix},$$

where K is the linear transformation defined in Proposition 3.4.

The proof of Lemma 4 in [3] shows that N is an orthogonal involution that conjugates S to its inverse. We will show that $\operatorname{rank}(I+N)$ is even.

We know by Lemma 2.1 that the minimal polynomial of $S|_W$ is $p(x) = (x+1)^n$. Suppose that $p(x) = \sum_{k=0}^{n} a_i x^i$, where $a_i \in F$. We notice that $a_1 = \binom{n}{1} = n$ is odd, and therefore $a_1 = a_{n-1} = 1$.

Since $S^n = \sum_{k=0}^{n-1} a_i S^i$, we have

$$\begin{aligned} S^{n+1} =& \sum_{k=0}^{n-1} a_i S^{i+1} = \sum_{k=1}^{n-1} a_{i-1} S^i + S^n = \sum_{k=1}^{n-1} a_{i-1} S^i + \sum_{k=0}^{n-1} a_i S^i \\ =& a_0 + \sum_{k=1}^{n-1} (a_{i-1} + a_i) S^i. \end{aligned}$$

Now we can write

$$P = \begin{bmatrix} a_0 & a_0+a_1 & a_1+a_2 & a_2+a_3 & \cdots & a_{n-3}+a_{n-2} & a_{n-2}+a_{n-1} \\ a_0 & a_1 & a_2 & a_3 & \cdots & a_{n-2} & a_{n-1} \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 1+a_2 & a_2+a_3 & \cdots & a_3+a_2 & a_2+1 \\ 1 & 1 & a_2 & a_3 & \cdots & a_2 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

It follows that

$$I+P=\begin{bmatrix} 0 & 0 & 1+a_2 & a_2+a_3 & \cdots & a_3+a_2 & a_2+1 \\ 1 & 0 & a_2 & a_3 & \cdots & a_2 & 1 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 1 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & \cdots & 1 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Because n is odd, all the entries in row $\frac{n+3}{2}$ are equal to zero. Also, the top row is linearly dependent of the rows $3-n$. On the other hand, the second row is clearly linearly independent. Now we have $\operatorname{rank}(I+P) = 1+\frac{n-3}{2} = \frac{n-1}{2}$.

In the proof of Proposition 3.4 we noticed that $\operatorname{rank}(I+K) = \frac{n-1}{2}$. Now $\operatorname{rank}(I+N) = \operatorname{rank}(I+K)+\operatorname{rank}(I+P) = n-1$, and therefore $\operatorname{rank}(I+N)$ is even. □

4 The proofs of the theorems

We will now give the proofs of Theorems 1.1 and 1.2.

Proof of Theorem 1.1. Suppose that V is a vector space of even dimension over a field whose characteristic is even. Tiep and Zalesski [11] have shown that $\Omega(V)$ is not real if the dimension of V is not divisible by four. Hence, we can assume that 4 divides $\dim(V)$.

We decompose V into cyclic and bicyclic subspaces V_i as in Section 3. If the dimension of a subspace V_i is divisible by four, then it is either a cyclic space or a bicyclic space consisting of two cyclic spaces of even dimension. By Propositions 3.3 and 3.5, the involution H_i can be chosen in such a way that $\operatorname{rank}(I+H_i)$ is even.

If we have a subspace of dimension 2 (mod 4), then it is either a cyclic space or a bicyclic space consisting of two cyclic spaces of odd dimension. By Propositions 3.3 and 3.16, the involution H_i can be chosen in such a way that $\operatorname{rank}(I+H_i)$ is odd.

Suppose that we have a subspace V_i of odd dimension. Now V_i cannot be bicyclic. Since the dimension is odd, the minimal polynomial of $S|_{V_i}$ cannot be of the form $(g_i(x)\tilde{g}_i(x))^{h_i}$. Hence, it must be of the form $r_i(x)^{h_i}$, where $r_i(x)$ is self-reciprocal and irreducible. Since the degree of $r_i(x)$ has to be

odd, it follows from Lemma 2.1 that $r(x) = x + 1$. However, in this case the subspace is degenerate. (This follows for example from the proof of Lemma 3.12.) Hence, we do not have cyclic spaces of odd dimension.

Since $4 \mid \dim(V)$, and none of the spaces V_i has odd dimension, we must have an even number of subspaces of dimension 2 (mod 4). Now we know that $\sum \operatorname{rank}(I + H_i) = \operatorname{rank}(I + H)$ is even. Thus, we can conclude that $\Omega(V)$ is strongly real. □

Proof of Theorem 1.2. Let V be a vector space of even dimension over a field whose characteristic is even. Suppose that $S \in \Omega(V)$ is unipotent. Decompose V into cyclic and bicyclic subspaces V_i as above.

Suppose first that we have a cyclic subspace V_i. As was noted above, we cannot have a cyclic space of odd dimension, and hence the dimension of V_i must be even. By Propositions 3.3 and 3.4, the involution H_i can be chosen in such a way that $\operatorname{rank}(I + H_i)$ is even.

Assume then that we have a bicyclic subspace V_i. By Propositions 3.5 and 3.17, the involution H_i can be chosen in such a way that $\operatorname{rank}(I + H_i)$ is even.

Now $\sum \operatorname{rank}(I + H_i) = \operatorname{rank}(I + H)$ is even, and therefore $H \in \Omega(V)$. Thus, S is strongly real.

□

5 Acknowledgements

The author is grateful to Professor R. A. Wilson for helpful discussions and useful remarks.

References

[1] C. Bagiński. On sets of elements of the same order in the alternating group A_n. *Publ. Math. Debrecen* **34** (1987), 313–315.

[2] D. Ž. Djoković. The product of two involutions in the unitary group of a hermitian form. *Indiana Univ. Math. J.* **21** (1971), 449–456.

[3] E. W. Ellers and W. Nolte. Bireflectionality of orthogonal and symplectic groups. *Arch. Math.* **39** (1982), 113–118.

[4] A. A. Galt. Strongly real elements in finite simple orthogonal groups. (*Siberian Math. J.*, to appear).

[5] R. Gow. Products of two involutions in classical groups of characteristic 2. *J. Algebra* **71** (1981), 583–591.

[6] R. Gow. Commutators in the symplectic group. *Arch. Math.* **50** (1988), 204–209.

[7] F. Knüppel and G. Thomsen. Involutions and commutators in orthogonal groups. *J. Austral. Math. Soc.* (Series A) **64** (1998), 1–36.

[8] S. G Kolesnikov and Ja. N. Nuzhin. On strong reality of finite simple groups. *Acta Appl. Math.* **85** (2005), 195–203.

[9] V. D. Mazurov and E. I. Khukhro. *The Kourovka notebook: Unsolved problems in group theory*, 14th edn. (Russian Academy of Sciences Siberian Division, Institute of Mathematics, Novosibirsk, 1999).

[10] D. E. Taylor. *The geometry of the classical groups* (Heldermann, Berlin 1992).

[11] Pham Huu Tiep and A. E. Zalesski. Real conjugacy classes in algebraic groups and finite groups of Lie type. *J. Group Theory* **8** (2005), 291–315.

[12] M. J. Wonenburger. Transformations which are products of two involutions. *J. Math. Mech.* **16** (1966), 327–338.