ON THE VANISHING OF SUBSPACES OF ALTERNATING BILINEAR FORMS

ROD GOW AND RACHEL QUINLAN

Abstract. Given a field F and integer $n \geq 3$, we introduce an invariant $s_n(F)$ which is defined by examining the vanishing of subspaces of alternating bilinear forms on 2–dimensional subspaces of vector spaces. This invariant arises when we calculate the largest dimension of a subspace of $n \times n$ skew-symmetric matrices over F which contains no elements of rank 2. We show how to calculate $s_n(F)$ for various families of field F, including finite fields. We also prove the existence of large subgroups of the commutator subgroup of certain p–groups of class 2 which contain no non–identity commutators.

1. Introduction

Let F be a field and let n and k be integers, with $n \geq 3$ and $k \geq 2$. Let V be a vector space of dimension n over F and let α be a subset of k alternating bilinear forms defined on $V \times V$. Following Buhler, Gupta and Harris, [5], we let $m(\alpha)$ be the maximum of the dimensions of those subspaces of V that are totally isotropic with respect to all the forms in α. We then set

$$d(F, n, k) = \min m(\alpha),$$

where α ranges over all subsets of k alternating bilinear forms defined on $V \times V$. The results of [5] show that evaluation of $d(F, n, k)$ is difficult, but the main theorem of that paper may be stated as follows.

Theorem 1. *Suppose that F has characteristic different from 2 and $k \geq 2$. Then*

$$d(F, n, k) \leq \left[\frac{2n + k}{k + 2}\right],$$

where $[x]$ denotes the greatest integer $\leq x$. If F is algebraically closed, equality holds above.

We now introduce a numerical invariant of the field F, based on the definition of $d(F, n, k)$ just given.

Definition 1. Let $n \geq 3$ be an integer. We set $s_n(F)$ to be that positive integer r satisfying

$$d(F, n, r) = 1$$
$$d(F, n, r - 1) \geq 2.$$

In the next section of this paper, we show how $s_n(F)$ is related to the study of certain special subspaces of $V \wedge V$, namely, those that contain no non–zero decomposable elements (in other words, elements of the form $x \wedge y$). The existence

1991 *Mathematics Subject Classification.* 15A75, 15A33, 12E15, 20D15.

of such subspaces is equivalent to the existence of subgroups of the commutator subgroup of certain nilpotent groups of class 2 that contain no non–identity pure commutators. Furthermore, given the identification of $V \wedge V$ with the space $A_n(F)$ of $n \times n$ skew–symmetric matrices over F, we see that subspaces of $V \wedge V$ that contain no non–zero decomposable elements correspond to subspaces of $A_n(F)$ that contain no elements of rank 2.

The final section of this paper is devoted to the evaluation of $s_n(F)$ for certain fields F, including finite fields. Theorem 1 implies that, if F has characteristic different from 2,

$$s_n(F) \leq 2n-3$$

and equality holds in this case if F is algebraically closed. Buhler, Gupta and Harris, [5], Section 3, also showed that

$$s_n(\mathbb{R}) = 2n-3 = 2^{k+1}-1$$

when $n = 2^k + 1$. Now it is straightforward to see that $s_n(F) \geq n-1$ if n is even and $s_n(F) \geq n$ if n is odd. We show that $s_n(F) = n-1$ if and only if there is an $(n-1)$–dimensional subspace of alternating bilinear forms defined on $V \times V$ with the property that each non–zero form in the subspace has rank n. We are then able to use properties of the quaternions and octonions to deduce that

$$s_4(F) = 3, \quad s_8(F) = 7$$

for any real field F. Since it is trivial to see that $s_n(F) \leq s_{n+1}(F)$, the theorem of [5] previously cited implies that

$$s_n(\mathbb{R}) \geq n,$$

except possibly when n is a power of 2. A famous result of Adams, [1], implies that we indeed have

$$s_n(\mathbb{R}) \geq n,$$

for all n, except when $n = 4$ or $n = 8$. We feel that the calculation of $s_n(\mathbb{R})$ when n is a power of 2 is a problem worth investigating.

We also introduce the concept of a subspace of alternating bilinear forms realizing the value of $s_n(F)$. Such a subspace has dimension $s_n(F)$ and vanishes on no 2–dimensional subspace of V. When F is a finite field and n is odd, we characterize the subspaces realizing the value of $s_n(F)$ as those n–dimensional subspaces of forms in which each non–zero element has rank $n-1$.

Throughout this paper, we adopt the following notation. $M_n(F)$ denotes the algebra of $n \times n$ matrices over F, $A_n(F)$ denotes the subspace of skew–symmetric matrices in $M_n(F)$, and $\mathrm{char}(F)$ denotes the characteristic of F. When $\mathrm{char}(F) = 2$, we take $A_n(F)$ to consist of those symmetric matrices whose diagonal entries are all 0. We will often identify $A_n(F)$ with the vector space $\mathrm{Alt}(V)$ consisting of all alternating bilinear forms defined on $V \times V$. We say that a subspace of $M_n(F)$ is a k–subspace if all its non–zero elements have rank k. We let $V^\times$ denote the subset of non–zero elements of V and adopt similar notation for the non–zero elements of subspaces of $\mathrm{Alt}(V)$.

2. Subspaces of $V \wedge V$ containing no decomposable elements

We assume as before that V is a vector space of dimension n over F. Let $V \wedge V$ denote the exterior square of V. We say that an element z of $V \wedge V$ is *decomposable* if we have $z = x \wedge y$ for suitable x and y in V.

Let f be an element of $\mathrm{Alt}(V)$ and let $\{v_1, \ldots, v_n\}$ be a basis of V. We may define a linear form f^* on $V \wedge V$ by setting

$$f^*(v_i \wedge v_j) = f(v_i, v_j)$$

and extending to all of $V \wedge V$ by linearity. We note then that

$$f^*(x \wedge y) = f(x, y)$$

for any x and y.

Let $k = s_n(F)$ and let $f_1, \ldots, f_k$ be k elements of $\mathrm{Alt}(V)$ with the property that there is no 2–dimensional subspace of V on which all the f_i vanish. We define a linear transformation

$$\omega : V \wedge V \to F^k$$

by

$$\omega(z) = (f_1^*(z), \ldots, f_k^*(z))$$

for all $z \in V \wedge V$.

Theorem 2. *With the notation previously introduced, ω is surjective and the kernel of ω is a subspace of codimension $s_n(F)$ in $V \wedge V$ which contains no non–zero decomposable elements. Moreover, any subspace of $V \wedge V$ containing no non–zero decomposable elements has codimension at least $s_n(F)$.*

Proof. We first show that ω is surjective. Let e_i be the standard basis vector of F^k whose single non–zero component is 1 occurring in the i–th position. We show that e_i is in the image of ω. Now as $s_n(F) = k$, there is a 2–dimensional subspace U_i, say, of V that is isotropic for the $k-1$ forms $f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_k$ but is not isotropic for f_i. Let x_i, y_i be basis vectors for U_i with $f_i(x_i, y_i) = 1$. Then we have

$$\omega(x_i \wedge y_i) = e_i,$$

as required.

We next show that the kernel of ω contains no non–zero decomposable element. For suppose that

$$\omega(x \wedge y) = 0.$$

Then we have

$$f_1(x, y) = \ldots = f_k(x, y) = 0.$$

Since the f_i do not simultaneously vanish on any 2–dimensional subspace of V, x and y must be linearly dependent and hence $x \wedge y = 0$.

Finally, let U be a subspace of $V \wedge V$ that contains no non-zero decomposable elements and let t be the codimension of U in $V \wedge V$. Let $\{u_1, \ldots, u_t\}$ be a basis of any complementary subspace of U in $V \wedge V$. For all x and y in V, we can write

$$x \wedge y + U = \sum_{i=1}^{t} g_i(x, y) u_i + U,$$

where $g_i(x, y) \in F$. We may easily verify that each g_i is in $\mathrm{Alt}(V)$. Since U contains no non–zero decomposable elements, we can not have

$$g_i(x, y) = 0$$

for all i when x and y are linearly independent. Thus we have a subset of t alternating bilinear forms that do not vanish on any 2–dimensional subspace of V. It follows that $d(F,n,t)=1$, and since $d(F,n,k-1)=2$, we must have $t\geq k=s_n(F)$, as required. □

We would like next to show how to construct some nilpotent groups of class 2 using $V\wedge V$. We shall assume that $\mathrm{char}(F)\neq 2$ in the ensuing discussion. Let $G_n(F)$ denote the set of all ordered pairs (u,x), where $u\in V$ and $x\in V\wedge V$. We define a multiplication on such pairs by setting

$$(u,x)(v,y)=(u+v,x+y+x\wedge y).$$

It is straightforward to check that the multiplication is associative, $(0,0)$ is an identity element, and

$$(u,x)^{-1}=(-u,-x).$$

Thus $G_n(F)$ is a group under the given multiplication. We may easily check that $(0,V\wedge V)$ is the centre $Z(G_n(F))$ of $G_n(F)$.

Let g and h be elements of $G_n(F)$ with

$$g=(u,x),\quad h=(v,y)$$

and let $[g,h]$ denote the commutator $g^{-1}h^{-1}gh$. A simple calculation reveals that

$$[g,h]=(0,2u\wedge v).$$

Thus commutators in the group correspond to decomposable elements of $V\wedge V$. Now it is a routine matter to check that the commutator subgroup $G_n(F)'$, which is generated by the commutators, coincides with $Z(G_n(F))$. We see in particular that $G_n(F)$ is nilpotent of class 2.

Let U be a subspace of $V\wedge V$ which contains no non–zero decomposable elements and has codimension $s_n(F)$. Then $(0,U)$ is a subgroup of $G_n(F)'$ that contains no non–identity commutators and is in some sense as large as possible with this property. We can quantify this statement more exactly if we restrict attention to the prime field $\mathbb{F}_p$, where p is an odd prime.

Let $G_n(p)$ denote the finite group $G_n(\mathbb{F}_p)$. We have $G_n(p)=p^{n(n+1)/2}$ and

$$|Z(G_n(p))|=|G_n(p)'|=p^{n(n-1)/2}.$$

$G_n(p)$ is the unique (Schur) covering group of exponent p of an elementary abelian p–group of order p^n. If we refer ahead to Corollary 8 we find that

$$s_n(\mathbb{F}_p)=n,$$

and thus we have the following result.

Theorem 3. *Let $G_n(p)$ denote the covering group of exponent p of an elementary abelian group of order p^n, where $n\geq 3$. Then $G_n(p)'=Z(G_n(p))$ and $|G_n(p)'|=p^{n(n-1)/2}$. There is a subgroup of order $p^{n(n-3)/2}$ in $G_n(p)'$ which contains no non–identity commutators. No subgroup of $G_n(p)'$ with this property has larger order.*

The group $G_n(F)$ appears in [4], Exercise 16, p.151, where the reader is required to prove that, for $n\geq 4$, there are elements in the commutator subgroup which are not commutators. As far as we know, however, a note of the existence of large subgroups of non–commutators has not appeared in the research literature before now. We remark that covering groups of exponent p^2 of an elementary abelian p–group also exist and they have the same property as that described in Theorem 3. The same is true for $p=2$, where all the covering groups have exponent 4.

We conclude this section by considering an application of the theory we have developed to the study of subspaces of $A_n(F)$. It is well known that there is a linear isomorphism between $V \wedge V$ and $\mathrm{Alt}(V^*)$, where V^* is the dual space of V. The isomorphism is defined in the following way. Let $\{v_1, \dots, v_n\}$ be a basis of V and let

$$z = \sum_{1 \le i < j \le n} a_{ij} v_i \wedge v_j$$

be any element of $V \wedge V$. Define

$$\varepsilon_z : V^* \times V^* \longrightarrow K$$

by

$$\varepsilon_z(\theta, \phi) = \sum a_{ij} \left(\theta(v_i)\phi(v_j) - \theta(v_j)\phi(v_i)\right).$$

for all θ and ϕ in V^*. It is straightforward to verify that ε_z is in $\mathrm{Alt}(V^*)$ and the mapping $z \to \varepsilon_z$ is an isomorphism between $V \wedge V$ and $\mathrm{Alt}(V^*)$. The rank of ε_z is the dimension of the subspace of V associated with z. (We recall that the subspace V_z associated to z is the smallest subspace U of V such that $z \in U \wedge U$.) Thus ε_z has rank 2 precisely when z is non–zero and decomposable. More informally, the isomorphism above associates with z the $n \times n$ skew–symmetric matrix $A = (a_{ij})$, where $a_{ji} = -a_{ij}$ for $j > i$, and $a_{ii} = 0$ for all i.

Our discussion concerning the isomorphism between $V \wedge V$ and $\mathrm{Alt}(V^*)$ implies that Theorem 2 is equivalent to the following statement about subspaces of $A_n(F)$.

Theorem 4. *There is a subspace of $A_n(F)$ that has dimension $n(n-1)/2 - s_n(F)$ and contains no elements of rank 2. Any subspace of $A_n(F)$ that contains no elements of rank 2 has dimension at most $n(n-1)/2 - s_n(F)$.*

We recall that the rank of a skew–symmetric matrix is even. Thus a non–zero matrix in the subspace described in Theorem 4 has rank equal to one of the integers

$$4,\ 6, \dots,\ 2[n/2].$$

We now consider a simple application of Theorem 4, where we use the results of [5] to determine $s_5(F)$ in some special cases. We recall here that a k–subspace of $M_n(F)$ is a subspace all of whose non–zero elements have rank k.

Corollary 1. *Let F be either an algebraically closed field with $\mathrm{char}(F) \neq 2$ or the field of real numbers. Then there is a 4–subspace of $A_5(F)$ of dimension 3, and this is the largest dimension of such a 4–subspace of $A_5(F)$.*

We would like to make some further comments about Corollary 1. Atkinson proved in [3], Theorem A, that when F is algebraically closed, the largest dimension of a 4–subspace of $M_5(F)$ is 3, so that part of Corollary 1 is anticipated by Atkinson's theorem. On the other hand, it is straightforward to find a 4–subspace of $M_5(\mathbb{R})$ of dimension 4, and this is the largest dimension of such a subspace, as implied by a theorem of Meshulam, [9], Theorem 2.

Following earlier work on k–subspaces, we say that two subspaces M and N of $M_n(F)$ are *equivalent* if there exist invertible matrices A and B in $M_n(F)$ with

$$AMB = N.$$

We make a similar definition for subspaces of $A_n(F)$.

Definition 2. Let M and N be subspaces of $A_n(F)$. We say that M and N are equivalent (as subspaces of $A_n(F)$) if there is an invertible matrix A in $M_n(F)$ with

$$AMA^T = N,$$

where A^T denotes the transpose of A.

Equivalent subspaces lie in the same orbit under the natural action of the general linear group $GL_n(F)$ on subspaces of skew–symmetric matrices. The following result shows that, for an algebraically closed field F with $\mathrm{char}(F) \neq 2$, the equivalence of subspaces of $A_n(F)$ under the original definition implies equivalence in the sense of Definition 2.

Lemma 1. *Suppose that F is an algebraically closed field with $\mathrm{char}(F) \neq 2$. Let M and N be subspaces of $A_n(F)$. Suppose that there are invertible matrices A and B in $M_n(F)$ with $AMB = N$. Then there exists an invertible matrix D with $DMD^T = N$.*

Proof. Let $\{X_1, \dots, X_m\}$ be a basis of M. Then the subset $\{Y_1, \dots, Y_m\}$ of N, where

$$Y_i = AX_iB$$

for $1 \leq i \leq m$, is a basis of N. Taking transposes, we obtain

$$B^T X_i A^T = Y_i = AX_iB.$$

Thus

$$CX_i = X_iC^T, \quad 1 \leq i \leq m,$$

where $C = A^{-1}B^T$. It follows easily that for any polynomial f in $F[x]$,

$$f(C)X_i = X_i f(C)^T$$

for all i.

Now as F is algebraically closed and $\mathrm{char}(F) \neq 2$, there is a polynomial p in $F[x]$ with

$$p(C)^2 = C.$$

See, for example, [7], Theorem 68. We set $D = Ap(C)$ and consider DX_iD^T. We calculate that

$$\begin{aligned} DX_iD^T &= Ap(C)X_ip(C)^TA^T \\ &= AX_i(p(C)^2)^TA^T \\ &= AX_iC^TA^T \\ &= AX_iB = Y_i. \end{aligned}$$

It follows that

$$DMD^T = N,$$

as required. □

We note that the same proof holds if we consider subspaces of symmetric matrices.

Corollary 2. *Let F be an algebraically closed field with $\mathrm{char}(F) \neq 2$. Let M and N be 4–subspaces of $A_5(F)$, each of dimension 3. Then M and N are equivalent in the sense of Definition 2.*

Proof. By a theorem of Atkinson, [3], Theorem A, there exist invertible matrices A and B in $M_5(F)$ with $AMB = N$. The result follows from Lemma 1. □

3. On the calculation of $s_n(F)$ and properties of related subspaces

We begin by setting up some general machinery relating to bilinear forms.

Definition 3. Let M be a subspace of $\mathrm{Alt}(V)$ and u an element of $V^\times$. We set

$$M_u = \{f \in M : u \in \mathrm{rad}\, f\}$$

and

$$V_u^M = \{v \in V : f(u,v) = 0 \text{ for all } f \in M\}.$$

It is straightforward to see that M_u, V_u^M are subspaces of M, V, respectively. Moreover, since for any $u \in V^\times$ and $f \in M$, $f(u,u) = 0$, it follows that $u \in V_u^M$ and hence dim $V_u^M \geq 1$. An important fact for the subsequent development is that dim $V_u^M = 1$ precisely when M does not vanish on any 2–dimensional subspace containing u. We note also that $M_u = 0$ for all $u \in V^\times$ if and only each element of $M^\times$ has maximal rank n (and is thus non–degenerate).

We can now reinterpret the previous definition of $s_n(F)$ by making the following observation. A finite set α of elements of $\mathrm{Alt}(V)$ vanishes on a subspace of V precisely when all the elements of the subspace spanned by α vanish on this subspace. Hence

$$s_n(F) = \min \dim N,$$

where N runs over those subspaces N of $\mathrm{Alt}(V)$ that satisfy dim $V_u^N = 1$ for all $u \in V^\times$.

To save time in enunciating our various results, we make the following definition.

Definition 4. We say that a subspace M of $\mathrm{Alt}(V)$ realizes the value of $s_n(F)$ if dim $M = s_n(F)$ and dim $V_u^M = 1$ for all $u \in V^\times$.

The point then to notice is that the subspaces which realize the value of $s_n(F)$ are the minimal subspaces of $\mathrm{Alt}(V)$ which vanish on no 2–dimensional subspace of V. Our purpose in this section is to calculate $s_n(F)$ for various fields F and to investigate whether subspaces realizing the value of $s_n(F)$ have distinguishing properties.

Our next theorem is a useful result linking the dimensions of M_u and V_u^M.

Theorem 5. *Given a subspace M of* $\mathrm{Alt}(V)$ *and an element u of $V^\times$, we have*

$$\dim M - \dim M_u = \dim V - \dim V_u^M.$$

Proof. Fixing $u \in V^\times$, we define a bilinear pairing $\varepsilon : M \times V \to F$ by

$$\varepsilon(f,v) = f(u,v)$$

for $f \in M$ and $v \in V$. Following the notation of [2], the left kernel of the pairing is M_u and the right kernel is V_u^M. The result follows from [2], Theorem 1.11. □

The following lemma is an immediate consequence of this theorem.

Lemma 2. *Let M be a subspace of* $\mathrm{Alt}(V)$ *that realizes the value of* $s_n(F)$. *Then*

$$\dim M_u = s_n(F) - (n-1)$$

for all $u \in V^\times$.

Corollary 3. *We have* $s_n(F) \geq n-1$ *if* n *is even and* $s_n(F) \geq n$ *if* n *is odd.*

Proof. Let M be a subspace of $\mathrm{Alt}(V)$ that realizes the value of $s_n(F)$. Then the previous lemma yields that

$$0 \leq \dim M_u = s_n(F) - (n-1)$$

for all $u \in V^\times$. This clearly implies that $s_n(F) \geq n-1$. Suppose now that n is odd. We can improve the estimate for $s_n(F)$ in the following way. Each element in M is degenerate when n is odd and hence there is some $u \in V^\times$ with $\dim M_u \geq 1$. The inequality above becomes

$$1 \leq \dim M_u = s_n(F) - (n-1)$$

and the fact that $s_n(F) \geq n$ is immediate. □

We note that the inequalities for $s_n(F)$ are implied by [6], Satz 1.

Corollary 4. *We have* $s_n(F) = n-1$ *if and only if there is an* $(n-1)$*–dimensional subspace of* $\mathrm{Alt}(V)$ *all of whose non–zero elements have rank* n.

Proof. Suppose that $s_n(F) = n-1$ and let M be a subspace of $\mathrm{Alt}(V)$ that realizes the value of $s_n(F)$. Then Lemma 2 yields that

$$\dim M_u = s_n(F) - (n-1) = 0$$

for all $u \in V^\times$. This implies that each element of $M^\times$ has rank n, and since $\dim M = s_n(F) = n-1$, M will serve as the required subspace.

Conversely, let N be an $(n-1)$–dimensional subspace of $\mathrm{Alt}(V)$ with the property that each element of $N^\times$ has rank n. Then we have $N_u = 0$ for each $u \in V^\times$ and hence we obtain

$$\dim V_u^N = \dim V - \dim N + \dim N_u = 1.$$

It follows that $s_n(F) \leq n-1$ and, since we already know that $s_n(F) \geq n-1$, we deduce that $s_n(F) = n-1$.

□

We may reinterpret Corollary 4 by saying that $s_n(F) = n-1$ if and only if there is an n–subspace of $A_n(F)$ of dimension $n-1$. Such subspaces seem to be uncommon, and they do not exist when F is finite. This fact seems to be well known, but we include a proof here following the ideas of Heineken, [6], Satz 1. Note that there is no need to exclude the characteristic 2 case, as Heineken appears to do in his proof.

Lemma 3. *Let* $n = 2m$ *be an even positive integer and let* F *be a finite field. Suppose that* M *is an* n*–subspace of* $A_n(F)$ *of dimension* r*. Then we have* $r \leq m$.

Proof. Let S be any element of $A_n(F)$ and let s_{ij} be the (i,j)–entry of S, where $i < j$. The theory of the Pfaffian, [8], p.588, shows that there is a homogeneous polynomial Pf of degree m in $m(2m-1)$ variables, whose coefficients lie in the prime field, such that

$$\det S = Pf(s_{12}, \ldots, s_{2m-1,2m})^2.$$

Now let $\{X_1, \ldots, X_r\}$ be a basis for M. We may then express any element S of M in the form

$$S = \lambda_1 X_1 + \cdots + \lambda_r X_r,$$

where the $\lambda_i \in F$. The properties of the Pfaffian previously outlined imply that there is a homogeneous polynomial Q in $F[z_1, \dots, z_r]$ of degree m in r variables such that

$$\det S = Q(\lambda_1, \dots, \lambda_r)^2.$$

By the Chevalley–Warning theorem, Q has a non–trivial zero in F if $r > m$. See, for example, [10], Chapter 1, Corollary 1. Since all non–zero elements of M have non–zero determinant, we deduce that $r \leq m$. □

We remark that it is easy to construct examples of n–subspaces of $A_n(F)$ of dimension $n/2$ when n is even and F is finite.

Corollary 5. *Let F be a finite field. Then we have $s_n(F) \geq n$ for $n \geq 3$.*

We continue with the theme that n–subspaces of $A_n(F)$ of dimension $n-1$ are uncommon by showing that when $F = \mathbb{R}$, they can only exist when n is one of 2, 4, or 8.

Theorem 6. *Suppose that $n \geq 3$. Then $s_n(\mathbb{R}) \geq n$ except when $n = 4$ or $n = 8$.*

Proof. We know that $s_n(F) \geq n - 1$ for any field F and that $s_n(F) = n - 1$ if and only if there is an n–subspace of $A_n(F)$ of dimension $n - 1$. Suppose then that M is an n–subspace of $A_n(\mathbb{R})$ of dimension $n - 1$. Let N be the subspace of $M_n(\mathbb{R})$ consisting of all elements $X + \lambda I_n$, where X runs over the elements of M and λ runs over $\mathbb{R}$. Clearly, $\dim N = n$ and each non-zero element of N is invertible, since a real skew–symmetric matrix has no real non–zero eigenvalues. Thus N is an n–subspace of $M_n(\mathbb{R})$ of dimension n. By [1], Theorem 1.1, such a subspace exists if and only if $n = \rho(n)$, where ρ is the Radon–Hurwitz function. Given the definition of ρ, it is easy to check that $\rho(n) = n$ only when $n = 2$, 4, or 8. (We will show that the cases $n = 4$ and $n = 8$ are exceptional after this proof.) □

As we remarked in the introduction, the work of [5] implies that better inequalities than $s_n(\mathbb{R}) \geq n$ are available, except possibly when n is a power of 2.

We proceed next to show why there are two exceptional cases $s_4(\mathbb{R}) = 3$ and $s_8(\mathbb{R}) = 7$, and begin by considering the real octonions $\mathbb{O}$. Let $e_0 = 1$, e_1, …, e_7 denote a standard basis of unit octonions. We say that an octonion is *pure* if it is a linear combination of e_1, …, e_7. We have the relations

$$e_i^2 = -1, \quad e_i e_j = -e_j e_i$$

for $1 \leq i \neq j \leq 7$. Moreover, if e is any of the e_i different from e_0,

$$e e_j = \pm e_k$$

for $0 \leq j \leq 7$, where k and the relevant sign are determined by a definite rule. Since the equality

$$e e_j = \varepsilon e_k,$$

where $\varepsilon = \pm 1$, implies that

$$e e_k = -\varepsilon e_j,$$

we see that in the regular representation of $\mathbb{O}$ on itself, e is represented by a skew–symmetric matrix with a single non–zero entry in each row and column, the non–zero entry being ± 1. It follows that each non–zero pure octonion is also represented by a skew–symmetric matrix, and this matrix is invertible, since the octonion has an inverse. Thus the pure octonions provide us with an 8–subspace of $A_8(\mathbb{R})$ of dimension 7. We may likewise use the pure quaternions to construct a 4–subspace of $A_4(\mathbb{R})$ of dimension 3. Since we may define division algebras of quaternions and octonions over any subfield F of $\mathbb{R}$, using F–linear combinations of the standard basis elements, we have proved the following result.

Theorem 7. *Let F be a subfield of $\mathbb{R}$. Then*

$$s_4(F) = 3, \quad s_8(F) = 7.$$

We note in passing that the example given at the end of [5] to show that $d(\mathbb{R}, 4, 3) = 1$ is incorrect, since the three alternating bilinear forms presented there have a common isotropic subspace. In the notation of [5], $\alpha_1 + \alpha_2$ has rank 2, whereas it must have rank 4 if the three forms are to have the desired property.

The following data represent our current knowledge of $s_n(\mathbb{R})$ for small values of n.

Theorem 8. *We have $s_4(\mathbb{R}) = 3$, $s_n(\mathbb{R}) = 7$ for $5 \leq n \leq 8$, and $s_9(\mathbb{R}) = 15$.*

Proof. We have already proved that $s_4(\mathbb{R}) = 3$, and the values of $s_5(\mathbb{R})$ and $s_9(\mathbb{R})$ are special cases of a theorem proved in [5]. Since $s_n(F) \leq s_{n+1}(F)$ is trivially true for any field F, the fact that $s_5(\mathbb{R}) = s_8(\mathbb{R})$ implies that $s_6(\mathbb{R}) = s_7(\mathbb{R}) = 7$ also. □

Theorem 8 implies the following unusual property of $A_8(F)$ when F is real. Analogous results hold for $A_n(F)$ when F is a field satisfying $s_n(F) = n - 1$.

Corollary 6. *Let F be a subfield of $\mathbb{R}$. Then there exist subspaces M and N of $A_8(F)$ with $\dim M = 21$, $\dim N = 7$ and $A_8(F) = M \oplus N$. M contains no elements of rank 2, whereas all non–zero elements of N have rank 2. Similarly, there exist subspaces P and Q of $A_8(F)$ with $\dim P = 21$, $\dim Q = 7$ and $A_8(F) = P \oplus Q$. P contains no elements of rank 8, whereas all non–zero elements of Q have rank 8.*

Proof. Since we know that $s_8(F) = 7$, the existence of the subspace M is guaranteed by Theorem 4. We may take N to be any 2–subspace of dimension 7 (such subspaces certainly exist). Similarly, we may take P to consist of those matrices in $A_8(F)$ whose top row is a zero row, and Q to be the subspace of $A_8(F)$ obtained from the regular representation of the octonions over F. □

We next use an observation of [5] to calculate $s_n(F)$ for many fields F whenever n is odd.

Theorem 9. *Suppose that F has a cyclic Galois extension of degree n. Then if n is odd, $s_n(F) = n$, and if n is even, $s_n(F) = n$ or $n - 1$.*

Proof. It is shown in [5], p.277, that $d(F, n, n) = 1$ under the given hypothesis on F. The result then follows from Corollary 3. □

Theorem 9 is a result of broad applicability, since many important fields satisfy its hypothesis for all $n \geq 2$. We include here a brief proof of a well known result which shows that Theorem 9 applies to all algebraic number fields.

Lemma 4. *Let F be an algebraic number field and let $n \geq 2$ be an integer. Then F has a cyclic Galois extension of degree n.*

Proof. Let p be a prime number and let $\mathbb{Q}_p$ be the field obtained by adjoining a primitive p–th root of unity to $\mathbb{Q}$. We claim that for all but finitely many p, $F \cap \mathbb{Q}_p = \mathbb{Q}$. To prove this, we note that as F is an extension of $\mathbb{Q}$ of finite degree, F has only finitely many subfields. If therefore there were infinitely many primes p for which $F \cap \mathbb{Q}_p \neq \mathbb{Q}$, there would be different primes r and s for which $\mathbb{Q}_r \cap \mathbb{Q}_s \neq \mathbb{Q}$. But it is a familiar result of the theory of cyclotomic fields that $\mathbb{Q}_r \cap \mathbb{Q}_s = \mathbb{Q}$ if $r \neq s$. Thus our claim follows.

Now there are infinitely many primes p satisfying $p \equiv 1 \pmod n$. Let p be such a prime with $F \cap \mathbb{Q}_p = \mathbb{Q}$. Then the compositum $F\mathbb{Q}_p$ is a cyclic Galois extension of F of degree $p-1$, [8], Chapter 6, Theorem 1.12. It follows that $F\mathbb{Q}_p$ contains a cyclic Galois extension of F of degree n. □

Corollary 7. *Let F be an algebraic number field. Then $s_n(F) = n$ if n is odd and $s_n(F) = n-1$ or n if n is even.*

We may obviously ask whether we can have $s_n(F) = n-1$ for suitable algebraic number field F and values of n. Theorem 7 has provided examples for $n = 4$ and $n = 8$ when F is a real algebraic number field. We speculate that the general problem may be related to properties of skew fields over F.

The following corollary of Theorem 9 is required for the proof of Theorem 3 and is used in our final investigation of subspaces realizing the value of $s_n(F)$.

Corollary 8. *Let F be a finite field. Then for $n \geq 3$, $s_n(F) = n$.*

Knowing now that $s_n(F) = n$ for a finite field F, it is of interest to study those subspaces of $\mathrm{Alt}(V)$ which realize this value. For odd n, we proceed to characterize these subspaces as precisely the subspaces of dimension n in which each non–zero element has rank $n-1$.

Theorem 10. *Let F be a finite field and let $n \geq 3$ be an odd integer. Let M be an n–dimensional subspace of $\mathrm{Alt}(V)$. Then M realizes the value of $s_n(F)$ if and only if each element of $M^\times$ has rank $n-1$.*

Proof. Let $|F| = q$. Since $\dim M = \dim V$, it follows from Theorem 5 that M realizes the value of $s_n(F)$ if and only if $\dim M_u = 1$ for all $u \in V^\times$.

Suppose then that $\dim M_u = 1$ for all $u \in V^\times$. Let Ω denote the set of all ordered pairs (f, u), where $f \in M^\times$ and $u \in \mathrm{rad}\, f^\times$. We note that if $(f, u) \in \Omega$, then $f \in M_u^\times$. Thus for fixed $u \in V^\times$, there are exactly $q-1$ elements (f, u) in Ω and hence

$$|\Omega| = (q-1)(q^n - 1).$$

Now since n is odd, $\dim \mathrm{rad}\, f \geq 1$ for each $f \in M$. Thus, setting $\dim \mathrm{rad}\, f = n(f)$, we have

$$|\Omega| = \sum_{f \in M^\times} (q^{n(f)} - 1) \geq (q-1)(q^n - 1),$$

with equality only if $n(f) = 1$ for all $f \in M^\times$. Since equality holds in this inequality, we deduce that $n(f) = 1$ for all $f \in M^\times$ and hence each element of $M^\times$ has rank $n-1$.

Conversely, if $n(f) = 1$ for all $f \in M^\times$, we also obtain $|\Omega| = (q-1)(q^n - 1)$ and then an identical argument as that above implies that $\dim M_u = 1$ for all $u \in M^\times$. □

The proof just given shows that if M is an n–dimensional subspace of $\mathrm{Alt}(V)$ in which all non–zero elements have rank $n-1$, there is a one–to–one correspondence between the one–dimensional subspaces of M and the one–dimensional subspaces of V, given by $\langle f \rangle \leftrightarrow \mathrm{rad}\, f$ for $f \in M^\times$.

We use the argument above to show that n is the largest dimension of a subspace of $\mathrm{Alt}(V)$ in which all non–zero elements have rank $n-1$.

Corollary 9. *Let F be a finite field and $n \geq 3$ be an odd integer. Let M be a subspace of* $\mathrm{Alt}(V)$ *with the property that each element of $M^\times$ has rank $n-1$. Then* $\dim M \leq n$.

Proof. It suffices to show that we cannot have $\dim M = n+1$. Now if $\dim M = n+1$, the equality

$$\dim\, M_u = \dim\, M - \dim\, V + \dim\, V_u^M,$$

implies that $\dim\, M_u \geq 2$ for all $u \in V^\times$, and since $\dim\, \mathrm{rad}\, f = 1$ for each $f \in M^\times$, the counting argument used in the proof above yields the inequality

$$(q-1)(q^{n+1}-1) \geq (q^2-1)(q^n-1).$$

This is a contradiction and hence $\dim\, M \leq n$, as claimed. □

We conclude by considering an analogue of Theorem 10 for even n

Theorem 11. *Let F be a finite field with $|F| = q$ and let $n \geq 4$ be an even integer. Let M be an n–dimensional subspace of* $\mathrm{Alt}(V)$ *that realizes the value of $s_n(F)$ and let S be the number of elements of rank n in M. Then*

$$\frac{q(q^n-1)}{q+1} \leq S < q^n - 1.$$

Proof. Our supposition on M implies that $\dim M_u = 1$ for all $u \in V^\times$. Let Ω denote the set of all ordered pairs (f, u), where $f \in M^\times$ has rank less than n and $u \in \mathrm{rad}\, f^\times$. Then since $\dim M_u = 1$, we have $|\Omega| = (q-1)(q^n-1)$. On the other hand, if f has rank less than n, $\dim\, \mathrm{rad}\, f \geq 2$, since n is even. Thus if R is the number of elements in M of rank less than n,

$$R(q^2-1) \leq |\Omega| = (q-1)(q^n-1).$$

This gives a upper bound for R and since $R + S = q^n - 1$, we obtain the lower bound for S. That $S < q^n - 1$ follows because $\dim M_u > 0$ for all $u \in V^\times$. □

The lower bound for S would be precise if we knew that $M^\times$ contains no elements of rank less than $n-2$. Thus the lower bound is achieved when $n = 4$,

References

[1] J. F. Adams, *Vector fields on spheres*, Ann. of Math. **75** (1962), 603–632.

[2] E. Artin, *Geometric Algebra*, Interscience Publishers, Inc., New York, 1957.

[3] M. D. Atkinson, *A problem of Westwick on k–spaces*, Linear and Multilinear Algebra **16** (1984), 263–273.

[4] N. Bourbaki, *Elements of Mathematics. Algebra I*, Chapters 1–3. Springer Verlag, Berlin–Heidelberg–New York, 1989.

[5] J. Buhler, R. Gupta and J. Harris, *Isotropic subspaces for skewforms and maximal abelian subgroups of p–groups*, J. Algebra **108** (1987), 269–279.

[6] H. Heineken, *Gruppen mit kleinen abelschen Untergruppen*, Arch. Math. **29** (1977), 20–31.

[7] I. Kaplansky, *Linear Algebra and Geometry*, Alleyn & Bacon, Boston, 1969.

[8] S. Lang, *Algebra*, 3rd ed., Addison–Wesley, Reading, Mass., 1993.

[9] R. Meshulam, *On k–spaces of real matrices*, Linear and Multilinear Algebra **26** (1990), 39–41.

[10] J. P. Serre, *A Course in Arithmetic*, Springer Verlag, Berlin–Heidelberg–New York, 1973.

Mathematics Department, University College, Belfield, Dublin 4, Ireland
E-mail address: rod.gow@ucd.ie, rachel.quinlan@ucd.ie