RANK PROPERTIES OF SUBSPACES OF SYMMETRIC AND HERMITIAN MATRICES OVER FINITE FIELDS

JEAN-GUILLAUME DUMAS, ROD GOW*, AND JOHN SHEEKEY

Abstract. We investigate constant rank subspaces of symmetric and hermitian matrices over finite fields, using a double counting method related to the number of common zeros of the corresponding subspaces of symmetric bilinear and hermitian forms. We obtain optimal bounds for the dimensions of constant rank subspaces of hermitian matrices, and good bounds for the dimensions of subspaces of symmetric and hermitian matrices whose non-zero elements all have odd rank.

1. Introduction

Let K be a field and let m and n be positive integers with $m \leq n$. Let $M_{m\times n}(K)$ denote the vector space of $m \times n$ matrices with entries in K. When $m = n$, we write $M_n(K)$ in place of $M_{n\times n}(K)$. We also let $S_n(K)$ denote the subspace of all symmetric matrices in $M_n(K)$. For any non-zero subspace U of $M_{m\times n}(K)$, we let $U^\times$ denote the subset of non-zero elements in U. Given a positive integer s, we let K^s denote the s-dimensional vector space of row vectors of size s over K.

Let r be an integer satisfying $1 \leq r \leq m$. We say that a subspace $\mathcal{M}$ of $M_{m\times n}(K)$ is a *constant rank t* subspace if each element of $\mathcal{M}^\times$ has rank t. Much research has been devoted to the study of constant rank subspaces, especially in the case K is the field of real or complex numbers. See, for example, the references of [3] for papers on constant rank subspaces written before 1996, and [1] for some later references.

In this paper, we investigate constant rank subspaces of symmetric and hermitian matrices over finite fields, using a double counting method. Among our main results is the following. Let q be a power of a prime and let $\mathbb{F}_q$ denote the finite field of size q. Let $\mathcal{M}$ be a constant rank t $\mathbb{F}_q$-subspace of $n \times n$ hermitian matrices over $\mathbb{F}_{q^2}$. Then if t is odd, $\dim \mathcal{M} \leq t$, whereas if t is even, $\dim \mathcal{M} \leq 2n - t$. Both bounds are best possible. We also present versions of this result for symmetric matrices. Our findings are not restricted to constant rank spaces. For example, we show the following result. Let $\mathcal{M}$ be a non-zero $\mathbb{F}_q$-subspace of hermitian matrices. Suppose that each element of $\mathcal{M}^\times$ has odd rank and let t be the maximum rank of an element of $\mathcal{M}$. Then $\dim \mathcal{M} \leq t$. Moreover, if $\mathcal{M}^\times$ also contains elements of rank less than t, then $\dim M \leq t - 1$.

1991 *Mathematics Subject Classification.* 15A03, 15A33.

Key words and phrases. matrix, rank, constant rank subspace, symmetric matrix, hermitian matrix, common zeros.

* Corresponding author.

The second and third authors were supported by Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006. The work of the first author was done while visiting the Claude Shannon Institute, University College Dublin, 2009-2010.

2. Symmetric bilinear and hermitian forms

Let q be a power of an odd prime and let V be a finite dimensional vector space over $\mathbb{F}_q$. Let f be a symmetric bilinear form defined on $V \times V$. Modulo its radical, f defines a non-degenerate symmetric bilinear form, which we shall denote by f'.

Definition 1. Let f be a symmetric bilinear form defined on $V \times V$. Suppose that f has even rank $2k$. We set $w(f) = 1$ if f' has Witt index k and $w(f) = -1$ if f' has Witt index $k-1$.

Let S be a symmetric matrix in $S_n(\mathbb{F}_q)$. We recall that S defines in the usual way a symmetric bilinear form on $\mathbb{F}_q^n \times \mathbb{F}_q^n$, which we shall denote by f_S. The rank of f_S is the same as the rank of the matrix S.

Definition 2. Let S be a non-zero symmetric matrix of even rank $2k$ in $S_n(\mathbb{F}_q)$, where q is a power of an odd prime. We set

$$w(S) = w(f_S),$$

where $w(f_S)$ is defined as above. We say that S is of *positive* type if $w(S) = 1$, otherwise, we say that S is of *negative* type.

Lemma 1. *Let q be a power of an odd prime and let V be a vector space of dimension n over $\mathbb{F}_q$. Let f be a symmetric bilinear form defined on $V \times V$. Then the number of vectors v in V with $f(v,v) = 0$ equals*

$$q^{n-1} + w(f)q^{n-k} - w(f)q^{n-k-1}$$

if f has even rank $2k$, and equals q^{n-1} if f has odd rank.

Proof. When f is non-degenerate, the formula for the number of vectors with the stated property is given in [5, Theorem 6.26] (where the quantity denoted by $\eta((-1)^{n/2}\Delta)$ is the same as our $w(f)$). The general formula follows from the non-degenerate case by taking into account the q^{n-2k} vectors in the radical of f. □

We consider next the finite field $\mathbb{F}_{q^2}$, where q is a power of an arbitrary prime. Given $\lambda \in \mathbb{F}_{q^2}$, we adopt the convention that

$$\overline{\lambda} = \lambda^q.$$

The bar operator is $\mathbb{F}_q$-linear and has order 2 on $\mathbb{F}_{q^2}$

Our next lemma is a version of Lemma 1 for hermitian forms.

Lemma 2. *Let W be a vector space of dimension n over $\mathbb{F}_{q^2}$ and let g be a hermitian form of rank $k \leq n$ defined on $W \times W$. Then the number of vectors $w \in W$ with $g(w,w) = 0$ is*

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

Proof. When g is non-degenerate, the formula for the number of isotropic vectors is given in [6, Lemma 10.4]. The general formula follows from the non-degenerate case by taking into account the $q^{2(n-k)}$ vectors in the radical of g.

□

3. A counting theorem for subspaces of hermitian forms

Let W be a vector space of dimension n over $\mathbb{F}_{q^2}$. The set of hermitian forms defined on $W \times W$ is naturally a vector space of dimension n^2 over $\mathbb{F}_q$ under the usual operations of addition and multiplication by scalars in $\mathbb{F}_q$.

Let $\mathcal{M}$ be an $\mathbb{F}_q$-subspace of hermitian forms of dimension r defined on $W \times W$ and let $N_{\mathcal{M}}(0)$ denote the number of vectors w in W with $H(w,w) = 0$ for all $H \in \mathcal{M}$. Our main result of this section is a formula for $N_{\mathcal{M}}(0)$ in terms of the ranks of the elements of $\mathcal{M}$. Our proof is a straightforward generalization of an elegant double counting formula of Fitzgerald and Yucas, [2, Theorem 2].

Theorem 1. *Let W be a vector space of dimension n over $\mathbb{F}_{q^2}$ and let $\mathcal{M}$ be an $\mathbb{F}_q$-subspace of hermitian forms of dimension r defined on $W \times W$. Let $N_{\mathcal{M}}(0)$ denote the number of vectors w in W with $H(w,w) = 0$ for all $H \in \mathcal{M}$. Then we have*

$$N_{\mathcal{M}}(0) = q^{2n-r} + \sum_{k=1}^{n} (-1)^k A_k q^{2n-r-k},$$

where A_k is the number of hermitian forms of rank $k \geq 1$ in $\mathcal{M}$.

Proof. Let $H_1, \ldots, H_r$ be an $\mathbb{F}_q$-basis for $\mathcal{M}$. Let

$$v = (\lambda_1, \ldots, \lambda_r)$$

be an element of $\mathbb{F}_q^r$. We define $H_v \in \mathcal{M}$ by

$$H_v = \lambda_1 H_1 + \cdots + \lambda_r H_r.$$

Given $x \in W$, we have

$$H_v(x,x) = \sum_{i=1}^{r} \lambda_i H_i(x,x) = v \cdot \varepsilon(x),$$

where the dot denotes the usual dot product in $\mathbb{F}_q^r$ and

$$\varepsilon(x) = (H_1(x,x), \ldots, H_r(x,x)).$$

Given $u \in \mathbb{F}_q^r$, let $N(u)$ denote the number of $x \in W$ with $\varepsilon(x) = u$. Fixing $v \in \mathbb{F}_q^r$, we have

$$\sum_{u \in \mathbb{F}_q^r, u \cdot v = 0} N(u) = N(H_v = 0),$$

where $N(H_v = 0)$ is the number of elements w in W with $H_v(w,w) = 0$.

We now sum this equation over all elements v of $(\mathbb{F}_q^r)^\times$. Taking into account that there are $q^{r-1} - 1$ vectors u in $(\mathbb{F}_q^r)^\times$ with $u \cdot v = 0$, we obtain

$$(q^r - 1) N_{\mathcal{M}}(0) + (q^{r-1} - 1) \sum_{0 \neq u \in \mathbb{F}_q^r} N(u) = \sum_{k=1}^{n} A_k q^{2n-k-1} (q^k + (-1)^k (q-1)),$$

where we have used Lemma 2 to evaluate the terms $N(H_v = 0)$.

Clearly,

$$\sum_{k=1}^{n} A_k q^{2n-k-1} (q^k + (-1)^k (q-1)) = q^{2n-1}(q^r - 1) + \sum_{k=1}^{n} (-1)^k A_k q^{2n-k-1} (q-1),$$

since

$$\sum_{k=1}^{n} A_k = q^r - 1.$$

Similarly,

$$\sum_{0 \neq u \in \mathbb{F}_q^r} N(u) = \sum_{u \in \mathbb{F}_q^r} N(u) - N_{\mathcal{M}}(0) = q^{2n} - N_{\mathcal{M}}(0).$$

Substituting these terms, we obtain

$$(q^r-1)N_{\mathcal{M}}(0)+(q^{r-1}-1)(q^{2n}-N_{\mathcal{M}}(0)) = q^{2n-1}(q^r-1)+(q-1)\sum_{k=1}^{n}(-1)^k A_k q^{2n-k-1}$$

and this simplifies to the equality

$$N_{\mathcal{M}}(0) = q^{2n-r} + \sum_{k=1}^{n}(-1)^k A_k q^{2n-r-k},$$

as required. □

Corollary 1. *Suppose we have r hermitian forms defined on $W \times W$, where $\dim W = n$. Then if $n > r$, the number of common zeros of the forms is divisible by q and hence the forms have a non-trivial common zero in $\mathbb{F}_{q^2}$.*

Proof. We may suppose that the forms are linearly independent over $\mathbb{F}_q$, since if the result we wish to prove holds for r linearly independent forms, it will clearly hold for any r forms. Let $\mathcal{M}$ be the $\mathbb{F}_q$-subspace spanned by the forms. Clearly, $\dim \mathcal{M} = r$ in this case. By hypothesis, if k denotes the rank of any element of $\mathcal{M}$, $2n-r-k > 0$. It follows from Theorem 1 that q divides $N_{\mathcal{M}}(0)$. Since $N_{\mathcal{M}}(0) \geq 1$, the result follows. □

More generally, the argument above proves that q^{n-r} divides $N_{\mathcal{M}}(0)$, a result in the spirit of the Chevalley-Warning theorem.

4. Subspaces of symmetric and hermitian matrices with specified ranks

Let A be a matrix in $M_n(\mathbb{F}_{q^2})$. As usual, we let $\overline{A}$ denote the matrix obtained by applying the bar automorphism of $\mathbb{F}_{q^2}$ to all entries of A. We say that A is *hermitian* if

$$\overline{A}^T = A,$$

where T denotes the transpose operator. We let $H_n(\mathbb{F}_q)$ denote the subset of all hermitian matrices in $M_n(\mathbb{F}_{q^2})$. $H_n(\mathbb{F}_q)$ is a vector space of dimension n^2 over $\mathbb{F}_q$.

Given an hermitian matrix A in $H_n(\mathbb{F}_q)$, we recall that we may define an hermitian form, f_A, say, on $W \times W$, where $W = (\mathbb{F}_{q^2})^n$, by setting

$$f_A(u, v) = uA\overline{v}^T$$

for all u and v in W. We may thus identify hermitian forms with hermitian matrices and $\mathbb{F}_q$-subspaces of $H_n(\mathbb{F}_q)$ with $\mathbb{F}_q$-subspaces of hermitian forms defined on $W \times W$.

We will use this identification of subspaces, together with Theorem 1, to bound the dimension of a subspace $\mathcal{M}$ of hermitian matrices in which all non-zero elements have odd rank. Thus, when we talk of $N_{\mathcal{M}}(0)$ for such a subspace of hermitian

matrices, we mean the corresponding number for the subspace of hermitian forms derived from $\mathcal{M}$.

Theorem 2. *Let $\mathcal{M}$ be a non-zero $\mathbb{F}_q$-subspace of $H_n(\mathbb{F}_q)$ of dimension r. Suppose that each element of $\mathcal{M}^\times$ has odd rank and let t be the maximum rank of an element of $\mathcal{M}$. Then $r \leq t$. Moreover, if $\mathcal{M}^\times$ also contains elements of rank less than t, then $r \leq t-1$.*

Proof. It follows from Theorem 1 that, since element in $\mathcal{M}^\times$ has odd rank,

$$N_{\mathcal{M}}(0) = q^{2n-r} - \sum_{k\geq 1} A_k q^{2n-r-k}.$$

We note also that if k is the rank of some element of $\mathcal{M}^\times$, then

$$q^{2n-r-k} \geq q^{2n-r-t}.$$

Furthermore, we clearly have $N_{\mathcal{M}}(0) \geq 1$. It follows that

$$q^{2n-r} - \sum_{k\geq 1} A_k q^{2n-r-t} \geq q^{2n-r} - \sum_{k\geq 1} A_k q^{2n-r-k} = N_{\mathcal{M}}(0) \geq 1.$$

However, since

$$\sum_{k\geq 1} A_k = q^r - 1,$$

we obtain

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

This inequality implies that $r \leq t$.

Suppose now that the different odd numbers that occur as the ranks of the elements of $\mathcal{M}^\times$ are $t_1, \ldots, t_s$, where $s > 1$ and

$$t = t_1 > t_2 > \cdots > t_s.$$

Suppose that there are B_i elements of rank t_i for $1 \leq i \leq s$. Then we have

$$N_{\mathcal{M}}(0)q^r = q^{2n} - \sum_{i=1}^{s} B_i q^{2n-t_i} \geq q^r$$

and hence

$$q^t - \sum_{i=1}^{s} B_i q^{t-t_i} \geq q^{t+r-2n} > 0.$$

Then since

$$\sum_{i=1}^{s} B_i = q^r - 1,$$

we obtain

$$q^t \geq q^r - 1 + \sum_{i=2}^{s} B_i(q^{t-t_i} - 1).$$

We know that $r \leq t$ by the earlier part of this argument. Suppose if possible that $r = t$ in this case. Then we have

$$q^t \geq q^t - 1 + \sum_{i=2}^{s} B_i(q^{t-t_i} - 1)$$

which is clearly a contradiction, since $B_2 \geq 1$ and $q^{t-t_2} - 1 \geq 3$. Consequently, $r \leq t-1$ when two or more odd ranks occur. □

Corollary 2. *Let $\mathcal{N}$ be a non-zero $\mathbb{F}_q$-subspace of hermitian forms of dimension r defined on $W \times W$, where W has dimension n over $\mathbb{F}_{q^2}$. Suppose that each element of $\mathcal{N}^\times$ has odd rank. Then $N_{\mathcal{N}}(0) > 1$ unless n is odd, $r = n$ and all elements of $\mathcal{N}^\times$ are non-degenerate.*

Proof. Let t be the maximum rank of an element of $\mathcal{N}^\times$. Then we know that $r \leq t$ by Theorem 2. Since we have

$$N_{\mathcal{N}}(0) = \sum_{k=0}^{n} (-1)^k A_k q^{2n-r-k}$$

by Theorem 1, $N_{\mathcal{N}}(0)$ is divisible by q^{2n-r-t} and hence greater than 1 (since certainly $N_{\mathcal{N}}(0) \geq 1$) unless $r = t = n$. In this case, n is odd. Moreover, Theorem 2 implies that $\mathcal{N}^\times$ contains only elements of rank t and hence each element of $\mathcal{N}^\times$ is non-degenerate. □

We note conversely that if n is odd and $\mathcal{N}$ is an n-dimensional subspace of hermitian forms in which each element of $\mathcal{N}^\times$ is non-degenerate, then $N_{\mathcal{N}}(0) = 1$. Such subspaces exist, as follows, for example, by Lemma 3 below.

Corollary 3. *Let $\mathcal{M}$ be a non-zero $\mathbb{F}_q$-subspace of $n \times n$ symmetric matrices of dimension r. Suppose that each element of $\mathcal{M}^\times$ has odd rank and let t be the maximum rank of an element of $\mathcal{M}$. Then $r \leq t$. Moreover, if $\mathcal{M}^\times$ contains elements of rank less than t, then $r \leq t - 1$.*

Proof. We may consider $\mathcal{M}$ to be an $\mathbb{F}_q$-subspace of hermitian matrices in $H_n(\mathbb{F}_q)$. Since the rank of a matrix does not change under field extension, $\mathcal{M}$ satisfies the hypotheses of Theorem 2 and the corollary is an immediate consequence of the theorem. □

To construct illustrative examples, we shall use the following embedding theorem for finite fields. We include a proof for lack of a convenient reference, but the result is not new.

Lemma 3. *For any positive integer n, the finite field $\mathbb{F}_{q^n}$ can be embedded into $M_n(\mathbb{F}_q)$ as an n-dimensional subspace of symmetric matrices.*

Proof. Let f be an irreducible monic polynomial of degree n over $\mathbb{F}_q$ and let A be the companion matrix of f. Then the polynomials in A provide us with an embedding of $\mathbb{F}_{q^n}$ into $M_n(\mathbb{F}_q)$ as an n-dimensional subspace, $\mathcal{M}$, say, in which each non-zero element is invertible. Now there exists an invertible symmetric matrix X, say, in $S_n(\mathbb{F}_q)$ satisfying

$$XAX^{-1} = A^T.$$

Furthermore, for any non-zero polynomial g in $\mathbb{F}_q[x]$ of degree less than n, $Z = Xg(A)$ is also symmetric and satisfies

$$ZAZ^{-1} = A^T.$$

See, for example, [4, p.77]. As explained in Section 5, the determinant mapping from $\mathcal{M}$ to $\mathbb{F}_q$ is surjective, since the norm mapping from $\mathbb{F}_{q^n}$ into $\mathbb{F}_q$ is surjective. Consequently, we may find a polynomial g such that $Z = Xg(A)$ has determinant 1. When q is odd, the theory of symmetric bilinear forms over $\mathbb{F}_q$ shows that we may write

$$Z = Y^T Y$$

and then we find that YAY^{-1} is symmetric. When q is a power of 2, and n is odd, X is symmetric but not alternating, since the rank of an alternating matrix is even. When q is a power of 2, and n is even, explicit calculation of A, as given in [4, p.77], shows that if X is alternating and

$$f = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_0,$$

then

$$a_1 = a_3 = \cdots = a_{n-1} = 0.$$

But this implies that f is the square of a polynomial, since $\mathbb{F}_q$ is perfect, and hence f is reducible, a contradiction. We deduce that the original X is symmetric but not alternating whenever q is a power of 2. In this case, we can write $X = W^T W$ for some invertible W in $M_n(\mathbb{F}_q)$ and then

$$WAW^{-1}$$

is symmetric. The construction of YAY^{-1} or WAW^{-1} provides us with the required symmetric embedding. □

We consider some examples to indicate that Corollary 3 is sharp or reasonably sharp. We observe first that Lemma 3 implies that if $t \leq n$ is an odd positive integer, $M_n(\mathbb{F}_q)$ contains a t-dimensional subspace of symmetric matrices whose non-zero elements all have rank t. We may take this subspace to consist of matrices of the form

$$\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix},$$

where A runs over a t-dimensional subspace of $S_t(\mathbb{F}_q)$, all of whose non-zero elements are invertible.

Next, let k be a positive integer and let $\lambda_1, \ldots, \lambda_{k+1}$ be arbitrary elements of any field K. Consider all $(2k+1) \times (2k+1)$ matrices of the form $A = (a_{ij})$, where $1 \leq i, j \leq 2k+1$, and

$$a_{ij} = \lambda_{(i+j)/2}$$

if $i + j$ is even and less than $2k + 3$. Otherwise, a_{ij} is zero. The subset of all such matrices is a subspace, $\mathcal{S}_{k+1}$, say, of $S_{2k+1}(K)$ of dimension $k + 1$ in which the non-zero matrices have odd rank

$$1, 3, \ldots, 2k+1.$$

Thus for example, $\mathcal{S}_3$ consists of elements of the form

$$\begin{pmatrix} \lambda_1 & 0 & \lambda_2 & 0 & \lambda_3 \\ 0 & \lambda_2 & 0 & \lambda_3 & 0 \\ \lambda_2 & 0 & \lambda_3 & 0 & 0 \\ 0 & \lambda_3 & 0 & 0 & 0 \\ \lambda_3 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Suppose now that ℓ is an odd integer greater than 1. If in the example above, we replace the entries λ_i, $1 \leq i \leq k+1$, by arbitrary $\ell \times \ell$ matrices A_i, $1 \leq i \leq k+1$, in an embedding of $\mathbb{F}_{q^\ell}$ into $M_\ell(\mathbb{F}_q)$ as an ℓ-dimensional subspace of symmetric matrices, we obtain a $(k+1)\ell$-dimensional subspace of $S_{(2k+1)\ell}(\mathbb{F}_q)$, whose non-zero elements have rank

$$\ell, 3\ell, \ldots, (2k+1)\ell.$$

We turn to the problem of giving a dimension bound for constant even rank subspaces of hermitian matrices.

Theorem 3. *Let $\mathcal{M}$ be a non-zero $\mathbb{F}_q$-subspace of $H_n(\mathbb{F}_q)$ of dimension r. Suppose that each element of $\mathcal{M}^\times$ has even rank $2t$. Then $r \leq 2n - 2t$.*

Proof. Theorem 1 implies that

$$N_{\mathcal{M}}(0) = q^{2n-r} + (q^r - 1)q^{2n-r-2t} = \frac{q^{2n-2t}(q^{2t} + q^r - 1)}{q^r}.$$

Since q is relatively prime to $q^{2t} + q^r - 1$ and N is an integer, we must have $r \leq 2n - 2t$. □

We show next that the bound just obtained is sharp. Our example uses a form of the doubling process described in [3].

Theorem 4. *Let t be a positive integer with $2t \leq n$. Then there exists an $\mathbb{F}_q$-subspace of $H_n(\mathbb{F}_q)$ of dimension $2n - 2t$ in which each non-zero element has even rank $2t$.*

Proof. We embed $\mathbb{F}_{q^{2(n-t)}}$ into $M_{n-t}(\mathbb{F}_{q^2})$ via the regular representation. The resulting subspace of matrices, $\mathcal{N}$, say, whose non-zero elements are all invertible, has dimension $2(n-t)$ when considered over $\mathbb{F}_q$. Let A be an element of rank t in $M_{t\times(n-t)}(\mathbb{F}_{q^2})$. Then the subspace $\mathcal{M} = A\mathcal{N}$, consisting of all left multiples of elements of $\mathcal{N}$ by A, is a constant rank t subspace of $M_{t\times(n-t)}(\mathbb{F}_{q^2})$. Consider now the subset $\mathcal{S}$, say, of $M_n(\mathbb{F}_{q^2})$ consisting of all elements of the form

$$\begin{pmatrix} 0_t & C \\ \overline{C}^T & 0_{n-t} \end{pmatrix},$$

where C runs over the elements of $\mathcal{M}$, and O_t and O_{n-t} denote the zero matrices of size $t \times t$ and $(n-t) \times (n-t)$, respectively. It is straightforward to see that each element of $\mathcal{S}^\times$ is hermitian and has rank $2t$. Furthermore, $\mathcal{S}$ is a subspace of dimension $2(n-t)$ when considered over $\mathbb{F}_q$. Thus $\mathcal{S}$ satisfies the hypotheses of Theorem 3, and its existence implies that the conclusion of the theorem regarding dimension is sharp.

□

5. Bounds for subspaces of symmetric bilinear forms

We begin by obtaining a version of Theorem 1 for subspaces of symmetric bilinear forms. As the proof is a straightforward generalization of our earlier proof, using Lemma 1 in place of Lemma 2, we omit the details.

Theorem 5. *Let V be a vector space of dimension n over $\mathbb{F}_q$, where q is a power of an odd prime, and let $\mathcal{M}$ be an $\mathbb{F}_q$-subspace of symmetric bilinear forms of dimension r defined on $V \times V$. Let $N_{\mathcal{M}}(0)$ denote the number of vectors v in V with $f(v, v) = 0$ for all $f \in \mathcal{M}$. Then we have*

$$N_{\mathcal{M}}(0) = q^{n-r} + \sum_{k\geq 1}^{n} (A_{2k} - B_{2k})q^{n-r-k},$$

where A_{2k} is the number of symmetric forms of rank $2k > 0$ and positive type in $\mathcal{M}$, and B_{2k} is the number of symmetric forms of rank $2k > 0$ and negative type in $\mathcal{M}$.

In the spirit of Corollary 1, we have the following theorem, which is a well known consequence of the Chevalley-Warning theorem. See, for example, [5, Corollaries 6.6, 6.9].

Corollary 4. *Suppose we have r symmetric bilinear forms defined on $V \times V$, where V is a vector space of dimension n over $\mathbb{F}_q$ and q is a power of an odd prime. Then if $n > 2r$, the number of common zeros of the forms is divisible by q and hence the forms have a non-trivial common zero.*

We proceed to apply Theorem 5 to investigate even constant rank subspaces of symmetric matrices.

Theorem 6. *Suppose that q is odd and $\mathcal{M}$ is a non-zero constant rank $2t$ subspace of $S_n(\mathbb{F}_q)$ of dimension r. Then*

$$r \leq n - t$$

if $w(S) = 1$ for all non-zero S,

$$r \leq t$$

if $w(S) = -1$ for all non-zero S, and

$$r \leq n.$$

if $\mathcal{M}$ contains equal numbers of non-zero elements of each type.

Proof. Suppose first that $w(S) = \varepsilon$, say, for all $S \in \mathcal{M}^\times$. Then we have

$$N_{\mathcal{M}}(0) = \frac{q^{n-t}}{q^r}(q^t + \varepsilon q^r - \varepsilon).$$

Since $N_{\mathcal{M}}(0)$ is an integer and $q^t + \varepsilon q^r - \varepsilon$ is relatively prime to q, it is straightforward to see that

$$r \leq n - t$$

if $\varepsilon = 1$. If $\varepsilon = -1$, the fact that $N_{\mathcal{M}}(0)$ is positive implies that

$$r \leq t.$$

Finally, if $\mathcal{M}$ contains equal numbers of non-zero elements of each type,

$$N_{\mathcal{M}}(0) = q^{n-r}$$

and this implies that $r \leq n$. □

Theorem 5 implies that if $\mathcal{M}$ is an $\mathbb{F}_q$-subspace of symmetric bilinear forms of dimension r defined on $V \times V$, then

$$N_{\mathcal{M}}(0) = q^{n-r}$$

whenever $\mathcal{M}$ contains no non-zero elements of even rank. This of course leads to the conclusion that $r \leq n$. However, we have already proved a stronger form of this inequality in Corollary 3, which we may use to prove the following result.

Corollary 5. *Let $\mathcal{M}$ be an $\mathbb{F}_q$-subspace of symmetric bilinear forms defined on $V \times V$, where q is a power of an odd prime. Suppose that $\mathcal{M}$ contains no non-zero elements of even rank, and let t be the largest rank of an element of $\mathcal{M}^\times$. Then*

$$N_{\mathcal{M}}(0) = q^d,$$

where $d \geq n - t$. Thus $N_{\mathcal{M}}(0)$ is a power of q greater than 1 unless n is odd, $\mathcal{M}$ has dimension n and all elements of $\mathcal{M}^\times$ have rank n.

It seems to be more difficult to find sufficient conditions for $N_{\mathcal{M}}(0)$ to be greater than 1 when $\mathcal{M}$ contains elements of even rank. Here we describe one special case, when n is even and $\mathcal{M}^\times$ consists of elements of maximal rank n.

Corollary 6. *Suppose that $n = 2m$ is even and $\mathcal{M}$ is a constant rank n $\mathbb{F}_q$-subspace of symmetric bilinear forms defined on $V \times V$, where q is a power of an odd prime. Suppose also that $\dim \mathcal{M} = m + d$, where $0 \leq d \leq m$. Then*

$$N_{\mathcal{M}}(0) > 1,$$

unless

$$A = \frac{(q^m+1)(q^d-1)}{2}, \quad B = \frac{(q^m-1)(q^d+1)}{2},$$

where A is the number of elements of positive type in $\mathcal{M}^\times$ and B is the number of elements of negative type.

Proof. Suppose that $N_{\mathcal{M}} = 1$. Then we have

$$1 = q^{m-d} + (A - B)q^{-d},$$

by Theorem 5. Since $A + B = q^{m+d} - 1$, the result follows easily. □

Theorem 8, proved later, implies that for any integer d with $0 \leq d \leq m$, there exists a constant rank n subspace $\mathcal{M}$ of symmetric bilinear forms defined on $V \times V$, where $\dim \mathcal{M} = m + d$ and $N_{\mathcal{M}}(0) = 1$, so that the distribution of the elements of each type in $\mathcal{M}$ is as described in Corollary 6.

In general we do not know how many non-zero elements of the two types are in a constant rank subspace and thus we have not been able to use Theorem 5 to bound the dimension of such a subspace. The following example, found by computer searching, provides a 5-dimensional constant rank 4 subspace of $S_5(\mathbb{F}_3)$ in which there are 220 elements of positive type, and 22 of negative type.

Example 1. Consider the 5-dimensional subspace $\mathcal{M}$ of $S_5(\mathbb{F}_3)$ consisting of the linear span of the matrices

$$\begin{pmatrix} 2&2&2&1&2\\ 2&2&1&2&2\\ 2&1&0&1&1\\ 1&2&1&2&0\\ 2&2&1&0&0 \end{pmatrix}, \quad \begin{pmatrix} 0&0&0&0&0\\ 0&0&0&0&1\\ 0&0&0&1&0\\ 0&0&1&1&0\\ 0&1&0&0&0 \end{pmatrix}, \quad \begin{pmatrix} 0&0&0&1&1\\ 0&0&0&2&0\\ 0&0&0&2&2\\ 1&2&2&1&0\\ 1&0&2&0&0 \end{pmatrix},$$

$$\begin{pmatrix} 0&2&0&2&0\\ 2&1&2&0&0\\ 0&2&0&0&0\\ 2&0&0&1&1\\ 0&0&0&1&0 \end{pmatrix}, \quad \begin{pmatrix} 2&2&1&2&0\\ 2&2&1&2&1\\ 1&1&0&1&2\\ 2&2&1&2&2\\ 0&1&2&2&0 \end{pmatrix}.$$

A computer calculation shows that $\mathcal{M}$ is a 5-dimensional constant rank 4 space with the stated distribution of types.

The doubling process described in [3] and already used in Section 4 enables us to show that the bound described in Theorem 6 is sharp when all non-zero elements in the subspace have positive type.

Theorem 7. *Let t be a positive integer with $2t \leq n$. Then there exists a subspace of $S_n(\mathbb{F}_q)$ of dimension $n - t$ in which each non-zero element has even rank $2t$ and positive type.*

Proof. Following the proof of Theorem 4, we may construct a constant rank t subspace $\mathcal{M}$, say, of $M_{t\times(n-t)}(\mathbb{F}_q)$ of dimension $n-t$. Consider now the subset $\mathcal{S}$, say, of $M_n(\mathbb{F}_q)$ consisting of all elements of the form

$$\begin{pmatrix} 0_t & C \\ C^T & 0_{n-t} \end{pmatrix},$$

where C runs over the elements of $\mathcal{M}$, and O_t and O_{n-t} denote the zero matrices of size $t\times t$ and $(n-t)\times(n-t)$, respectively. It is straightforward to see that each element S of $\mathcal{S}^\times$ is symmetric and has rank $2t$. We claim furthermore that $w(S)=1$. For the existence of the zero matrix O_{n-t} as a submatrix of S implies that the symmetric bilinear form f_S defined by S has a totally isotropic subspace of dimension $n-t$. This subspace contains the radical of f_S, and modulo the radical, its image is a totally isotropic subspace for f'_S of dimension t. Since f'_S has rank $2t$, it follows that its Witt index is t and hence $w(S)=1$, as claimed. Finally, since $\mathcal{S}$ is a subspace of dimension $n-t$, it meets the requirements of the theorem. □

We would like to investigate if the bound described in Theorem 6 is sharp in the case when all non-zero elements in a subspace of symmetric matrices have the same rank and the same negative type. To do this, we begin by recalling some facts about the embedding of a field into a matrix ring.

Suppose that we embed the field $\mathbb{F}_{q^{2m}}$ into $M_{2m}(\mathbb{F}_q)$ by its regular representation over $\mathbb{F}_q$. Then we obtain an $2m$-dimensional subspace, $\mathcal{M}$, say, of $M_{2m}(\mathbb{F}_q)$ in which each non-zero element is invertible. Given $S\in\mathcal{M}$, we have

$$\det S = N(S),$$

where we identify S with an element of $\mathbb{F}_{q^{2m}}$ and N denotes the norm mapping from $\mathbb{F}^\times_{q^{2m}}$ to $\mathbb{F}^\times_q$.

Theorem 8. *Let m be a positive integer. Then there exists an m-dimensional subspace of $S_{2m}(\mathbb{F}_q)$ in which each non-zero element has rank $2m$ and negative type.*

Proof. We first recall that an invertible symmetric matrix S in $S_{2m}(\mathbb{F}_q)$ satisfies $w(S)=-1$ if and only if $\det S$ is a non-square in $\mathbb{F}^\times_q$, except when m is odd and $q\equiv 3 \mod 4$, in which case the condition is that $\det S$ is a square.

We consider the field $\mathbb{F}_{q^{2m}}$ and its subfield $\mathbb{F}_{q^m}$. Let

$$N : \mathbb{F}^\times_{q^{2m}} \to \mathbb{F}^\times_q$$

be the norm mapping, which is well known to be a surjective homomorphism. We claim that each element $x\in\mathbb{F}^\times_{q^m}$ is a square in $\mathbb{F}^\times_{q^{2m}}$. To prove this, we must show that

$$x^{(q^{2m}-1)/2}=1.$$

This is clear, however, since $x^{q^m-1}=1$ and hence

$$x^{(q^{2m}-1)/2} = x^{(q^m-1)(q^m+1)/2} = 1,$$

as required. Thus, since N is a homomorphism, $N(x)$ is a square in $\mathbb{F}^\times_q$.

Finally, consider an embedding of $\mathbb{F}_{q^{2m}}$ into $S_{2m}(\mathbb{F}_q)$ by symmetric matrices. Let $\mathcal{A}$ be the image of $\mathbb{F}_{q^m}$ under this embedding. $\mathcal{A}$ is a subspace of dimension m in which each non-zero element has rank $2m$ and square determinant, by what we have proved above. Thus if m is odd and $q\equiv 3 \mod 4$, $\mathcal{A}$ is a subspace of $S_{2m}(\mathbb{F}_q)$ with

the required property. In all other cases, let w be an element of $\mathbb{F}_{q^{2m}}$ with $N(w)$ a non-square in $\mathbb{F}_q^\times$. Then $\mathcal{A}w$ is a subspace with the required property (here, we think of w as a symmetric matrix in the embedding of $\mathbb{F}_{q^{2m}}$ into $S_{2m}(\mathbb{F}_q)$).

□

Corollary 7. *For each integer d with $0 \leq d \leq m$, there exists a constant rank n subspace $\mathcal{M}_d$ of symmetric bilinear forms defined on $V \times V$, where $\dim \mathcal{M}_d = m + d$, $N_{\mathcal{M}}(0) = 1$ and the number of non-zero elements in $\mathcal{M}_d$ of positive type is $(q^m + 1)(q^d - 1)/2$.*

Proof. Let $\mathcal{M}$ denote the image of the field $\mathbb{F}_{q^{2m}}$ under its embedding into $S_{2m}(\mathbb{F}_q)$. We have seen in Theorem 8 that $\mathcal{M}$ contains a subspace $\mathcal{M}_0$, say, of dimension m in which each non-zero element has negative type. Let $\mathcal{M}_d$ denote any subspace of $\mathcal{M}$ of dimension $m+d$ which contains $\mathcal{M}_0$. Clearly, as the elements of M_0 have no common non-trivial zeros, the same is true for $\mathcal{M}_d$. Thus, there are

$$\frac{(q^m + 1)(q^d - 1)}{2}$$

elements of positive type, and $(q^m - 1)(q^d + 1)/2$ elements of negative type in $\mathcal{M}_d$, by Corollary 6. □

The following corollary on the maximum dimension of a constant rank subspace of $M_{m\times n}(\mathbb{F}_q)$ has been obtained without the restriction to odd q, [1, Theorem 6].

Corollary 8. *Let $\mathcal{M}$ be a non-zero subspace of $M_{m\times n}(\mathbb{F}_q)$ of dimension r. Suppose that all elements of $\mathcal{M}^\times$ have the same rank t. Suppose also that q is odd. Then*

$$r \leq m + n - t.$$

Proof. Consider the r-dimensional subspace $\mathcal{N}$, say, of $S_{m+n}(\mathbb{F}_q)$ consisting of all matrices

$$\begin{pmatrix} 0_m & C \\ C^T & 0_n \end{pmatrix},$$

where C runs over the elements of $\mathcal{M}$. Each such non-zero matrix has rank $2t$ and positive type, as we showed earlier. It follows from Theorem 6 that

$$r \leq m + n - t,$$

as claimed.

□

6. Constant rank 3 subspaces of symmetric matrices

It seems reasonable to ask if a constant rank k subspace of symmetric matrices over an arbitrary field has dimension at most k when k is odd. We have proved this is true for a finite field, and an application of the Kronecker pair theory, discussed below, shows that over an algebraically closed field, the maximum dimension of an odd constant rank subspace of symmetric matrices is 1. As an indication that a general result for all fields might be true, we shall present a proof that, over an arbitrary field, the maximum dimension of a constant rank 3 subspace of symmetric matrices is 3.

Let V be a finite dimensional vector space over the field K and let f and g be symmetric bilinear forms defined on $V \times V$. A basic result in the theory of bilinear forms, due essentially to Kronecker, shows that there is a decomposition

$$V = V_1 \perp V_2 \perp V_3$$

of V into subspaces V_1, V_2 and V_3. This decomposition is orthogonal with respect to both f and g. See, for example, the treatment of this subject given in [7, Theorem 3.1].

We may choose the notation so that f is non-degenerate on V_1, g is non-degenerate on V_2, and V_3 is the orthogonal direct sum (with respect to f and g) of *basic singular subspaces*. We allow the possibility that any of the V_i is a zero subspace and also that g is non-degenerate on V_1, or f is non-degenerate on V_2.

A basic singular subspace U, say, with respect to f and g, has odd dimension, $2r + 1$, say, and the restriction of each of f and g to $U \times U$ has even rank $2r$. We note in particular that a one-dimensional basic singular subspace is contained in the radical of both f and g.

For our purposes in this paper, we need to know that if U is a 3-dimensional basic singular subspace, we can choose a basis of U so that the matrices of f and g are, respectively

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & \lambda \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & \mu \end{pmatrix},$$

where λ and μ are elements of K. Provided that K has characteristic different from 2, we may further choose the basis of U so that

$$\lambda = \mu = 0,$$

although this fact is not required in the development of our work here.

We note the important fact for our investigation that if a and b are elements of K, not both 0, the symmetric form $af + bg$ also has rank 2 on $U \times U$. The following is our basic result for investigating constant rank 3 subspaces of symmetric matrices.

Lemma 4. *Let f and g be symmetric bilinear forms of rank 3 defined on $V \times V$. Suppose that $af + bg$ has rank 3 for all a, b in K, with a and b not both 0. Then provided $|K| \geq 4$, f and g have the same radical.*

Proof. Following the notation of our earlier discussion, we have to show that V_3 has codimension 3 in V and equals the radical of both f and g.

Since f and g both have rank 3, it is clear that

$$\dim V_1 + \dim V_2 \leq 6.$$

Moreover, since V_3 is the sum of basic singular subspaces, it can contain at most one basic singular summand of dimension greater than 1.

Suppose then that V_3 contains a basic singular summand U, say, of dimension $2r + 1 > 1$. As both f and g have rank $2r$ on $U \times U$, it follows that $r = 1$ and $\dim U = 3$. We deduce then that

$$\dim V_1 \leq 1, \quad \dim V_2 \leq 1.$$

Consideration of essentially identical cases shows that we need only examine what happens when

$$\dim V_1 = \dim V_2 = 1$$

or when

$$\dim V_1 = 1, \quad V_2 = 0.$$

Neglecting one-dimensional basic singular subspaces, which are in the common radical, we see that f and g are represented by the 5×5 matrices

$$\begin{pmatrix} c & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & \lambda \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & d & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \mu \end{pmatrix},$$

when $\dim V_1 = \dim V_2 = 1$, and by the the 4×4 matrices

$$\begin{pmatrix} c & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & \lambda \end{pmatrix}, \quad \begin{pmatrix} d & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & \mu \end{pmatrix}$$

when $\dim V_1 = 1$, $V_2 = 0$.

Here, c, d, λ, μ are elements of K, with c and d both non-zero. However, in the former case,

$$f + g \text{ has rank 4,}$$

whereas in the latter case,

$$df - cg \text{ has rank 2.}$$

We have a contradiction in each case, and it follows that V_3 is contained in the common radical of f and g.

To finish the proof, it suffices to assume that $V_3 = 0$ and $\dim V \leq 6$. We proceed to consider the various essentially different possibilities in turn.

Suppose first that $\dim V_1 = 3$. Consideration of ranks then implies that f is zero on V_2. Now if g is also non-degenerate on V_1, then $V_2 = 0$ and we have the situation described in the lemma. Thus, if the situation described in the lemma does not obtain, we can assume that g is degenerate on $V_1 \times V_1$, and hence $\dim V_2 \geq 1$. Now if $\dim V_2 = 3$, g must be 0 on $V_1 \times V_1$. This, however, clearly implies that $f + g$ has rank 6, which is not the case. Thus, if the lemma does not hold, the supposition that $\dim V_1 = 3$ implies that

$$1 \leq \dim V_2 \leq 2.$$

With respect to suitable bases in V_1 and V_2, we may take f and g to be represented by the matrices

$$\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix},$$

where A and B are 3×3, A and C are invertible, and B singular.

Suppose first that $\dim V_1 = 3$, $\dim V_2 = 2$. Then B has rank 1. Now $A + B$ has rank at least 2, since the sum of two matrices of rank 1 has rank at most 2. It follows that $f + g$ has rank at least 4, contrary to hypothesis. Suppose next that $\dim V_1 = 3$, $\dim V_2 = 1$. Then B has rank 2. For any element λ of K, $\lambda A + B$ is invertible unless $-\lambda$ is an eigenvalue of $A^{-1}B$. Since $A^{-1}B$ has at most three different eigenvalues, we can choose λ so that $\lambda A + B$ is invertible if $|K| \geq 4$, and this means that $\lambda f + g$ has rank 4, again a contradiction.

There remains the case that $\dim V_1 = \dim V_2 = 2$ to resolve. Here, we may assume that f and g are represented by the symmetric matrices

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, \quad \begin{pmatrix} C & 0 \\ 0 & D \end{pmatrix},$$

where A, B, C and D are 2×2, A and D are invertible, and B and C both have rank 1. For any non-zero element λ of K, the matrix

$$\begin{pmatrix} \lambda A + C & 0 \\ 0 & \lambda B + D \end{pmatrix}$$

is invertible unless $-\lambda$ is an eigenvalue of $A^{-1}C$ and $-\lambda^{-1}$ is an eigenvalue of $D^{-1}B$. Since $A^{-1}C$ and $D^{-1}B$ are 2×2 matrices of rank 1, there are at most two values of λ to avoid and hence we can find λ so that $\lambda f + g$ has rank 4 if $|K| \geq 4$. This contradiction completes the proof.

□

The following example shows that the hypothesis on the size of the field is necessary. Suppose that $|K| \leq 3$ and f and g are respectively represented by the matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

All non-trivial linear combinations of f and g have rank 3, yet f and g have different radicals.

Corollary 9. *Let $\mathcal{S}$ be a subspace of symmetric bilinear forms defined on $V \times V$, where V is a finite dimensional vector space over the field K. Suppose that each non-zero element of $\mathcal{S}$ has rank 3. Then if $|K| \geq 4$, we have*

$$\dim \mathcal{S} \leq 3$$

and each non-zero element of $\mathcal{S}$ has the same radical.

Proof. It follows from Lemma 4 that each non-zero element of $\mathcal{S}$ has the same radical, R, say, when $|K| \geq 4$. Let N be a complement of R in V. Then $\dim N = 3$ and it is clear that the restriction of $\mathcal{S}$ to $N \times N$ defines a subspace $\mathcal{S}'$, say, of symmetric bilinear forms on $N \times N$ with

$$\dim \mathcal{S} = \dim \mathcal{S}'.$$

Each element of $\mathcal{S}'$ is non-degenerate and it follows that

$$\dim \mathcal{S}' \leq 3.$$

This is what we wanted to prove. □

We do not know if the final part of Corollary 9 holds when $|K| \leq 3$. Nonetheless, Theorem 2 and Corollary 9 imply the following result.

Corollary 10. *Let $\mathcal{S}$ be a subspace of $S_n(K)$. Suppose that each element of $\mathcal{S}^\times$ has rank 3. Then* $\dim \mathcal{S} \leq 3$.

References

[1] J.-G. Dumas, R. Gow, G. McGuire and J. Sheekey, *Subspaces of matrices with special rank properties*, Linear Algebra Appl. **433** (2010), 191-202.

[2] R. W. Fitzgerald and J. L. Yucas, *Pencils of quadratic forms over finite fields*, Discrete Mathematics **283** (2004), 71-79.

[3] B. Ilic and J. M. Landsberg, *On symmetric degeneracy loci, spaces of matrices of constant rank and dual varieties*, Math. Annalen **314** (1999), 159–174.

[4] I. Kaplansky, *Linear Algebra and Geometry*, Allyn and Bacon, Boston, 1969.

[5] R. Lidl and H. Niederreiter, *Finite Fields*, Addison–Wesley, Reading, Mass., 1983.

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

[7] W. C. Waterhouse, *Pairs of quadratic forms*, Invent. Math. **37** (1976), 157-164.

Laboratoire Jean Kuntzmann, Université de Grenoble, France
E-mail address: jean-guillaume.dumas@imag.fr

School of Mathematical Sciences, University College Dublin, Ireland
E-mail address: rod.gow@ucd.ie

School of Mathematical Sciences, University College Dublin, Ireland
E-mail address: johnsheekey@gmail.com