Linear codes associated to skew-symmetric determinantal varieties

Beelen, Peter; Singh, Prasant

Published in:
Finite Fields and Their Applications

Link to article, DOI:
10.1016/j.ffa.2019.03.004

Publication date:
2019

Document Version
Peer reviewed version

LINEAR CODES ASSOCIATED TO SKEW-SYMMETRIC DETERMINANTAL VARIETIES

PETER BEELEN AND PRASANT SINGH

Abstract. In this article we consider linear codes coming from skew-symmetric determinantal varieties, which are defined by the vanishing of minors of a certain fixed size in the space of skew-symmetric matrices. In odd characteristic, the minimum distances of these codes are determined and a recursive formula for the weight of a general codeword in these codes is given.

1. Introduction

Let $\mathbb{F}_q$ be the finite field with q elements. From a mathematical point of view, an $\mathbb{F}_q$-linear error-correcting code is a subspace of the vector space $\mathbb{F}_q^n$. Algebraic varieties V defined over $\mathbb{F}_q$ are a rich source of such codes and various constructions of codes from a given variety exist. A very natural and much-studied construction of codes uses the points in $V(\mathbb{F}_q)$, the set of $\mathbb{F}_q$-rational points of V, as columns of a matrix. A code is then obtained by considering this matrix as generator matrix of the code. To construct the matrix, an order of the points will need to be chosen. In case the variety V is contained in a projective space $\mathbb{P}^{k-1}$, a choice of representatives of the $\mathbb{F}_q$-rational points also needs to be made. Allowing any family of $\mathbb{F}_q$-rational points of $\mathbb{P}^{k-1}$ in this setup, leads to a more general construction of codes studied in [21]. There, such a family of points was called a projective system. In the setting of projective systems, it was observed that different choices of ordering and representatives of the points, give rise to equivalent codes. In particular the minimum distance and weight distribution of the resulting codes are independent on these choices. Another observation from [21] is that if the projective system is not contained in a hyperplane of $\mathbb{P}^{k-1}$, then the dimension of the resulting code is k.

Let $C \subset \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear code arising in this way from a projective variety $V \subset \mathbb{P}^{k-1}$ defined over $\mathbb{F}_q$. The Hamming weight $\mathrm{w}_H(c)$ of a codeword $c = (c_1, \ldots, c_n) \in C$ is defined as $\mathrm{w}_H(c) := \#\{i : c_i \neq 0\}$. However, by construction $n - \mathrm{w}_H(c)$, then equals the number of common $\mathbb{F}_q$-rational points on the intersection of V and a certain hyperplane H defined over $\mathbb{F}_q$ depending on c. Therefore questions about the possible weights of codewords, can be rephrased in terms of intersections of $\mathbb{F}_q$-rational hyperplanes with V. Codes coming from the Grassmannian variety have

Date: March 21, 2019.

been studied from this point of view in [18, 19, 15, 6, 4]. Similarly, toric varieties were used to construct codes in [7, 17], flag varieties were used in [16], and so on. For an overview see for example [12] and the references therein. Using classical determinantal varieties of generic matrices, a class of codes called determinantal codes were introduced and studied in [2, 3]. As was shown there, determinantal codes have relatively few weights. More precisely, let $\ell \leq m$ be natural numbers and $\mathbf{Det}(t, \ell, m)$ be the projective variety consisting of $\ell \times m$ matrices with coefficients in $\mathbb{F}_q$ of rank $\leq t$. Then the corresponding code has at most ℓ weights. Apart from the determinantal varieties of generic matrices, other classically studied determinantal varieties are associated to for example symmetric and skew-symmetric matrices. For more details about these varieties one may refer to [8, 9, 20]. Inspired by this, we consider in this article codes associated to skew-symmetric determinantal varieties $\mathbf{Det_A}(2t, m)$ consisting of all $m \times m$ skew symmetric matrices with coefficients in $\mathbb{F}_q$. We will call these codes *skew determinantal codes*. The lengths and the dimensions of these codes are easily determined, since the number of $\mathbb{F}_q$-rational points on $\mathbf{Det_A}(2t, m)$ is well known and the variety is nondegenerately embedded in $\mathbb{P}^{\binom{m}{2}-1}$. However, the determination of the minimum distance requires some work. In fact, we will compute all possible nonzero weights a codeword of a skew determinantal code can have and then determine the least nonzero weight among them. Equivalently, we determine the possible number of $\mathbb{F}_q$-rational intersection points that an $\mathbb{F}_q$-rational hyperplane and $\mathbf{Det_A}(2t, m)$ can have. It turns out that like determinantal codes, only few possibilities can occur, namely at most $\lfloor m/2 \rfloor$.

2. Preliminaries: Skew-symmetric Determinantal Varieties

We begin this section by recalling the definition of skew-symmetric determinantal varieties. Let $\mathbb{F}_q$ be a finite field with q elements and let m be a positive integer. By a *skew-symmetric* or *anti-symmetric* matrix A of size m over $\mathbb{F}_q$, we always mean that A is an $m \times m$ matrix over $\mathbb{F}_q$ with all diagonal entries zero and $A^T = -A$. If the characteristic of the field $\mathbb{F}_q$ is not 2 then the condition $A^T = -A$ is enough for A to be skew-symmetric. Let $\mathbb{A}_m$ be the set of all skew-symmetric matrices of size m over $\mathbb{F}_q$. It is well known that $\mathbb{A}_m$ is an $\mathbb{F}_q$-vector space of dimension $\binom{m}{2}$ and hence one can think of $\mathbb{A}_m$ as the affine space $\mathbb{A}(\mathbb{F}_q)^{\binom{m}{2}}$.

Let t be an integer satisfying $t \leq m$. We define

$$\mathbb{A}(t, m) := \{A \in \mathbb{A}_m \,:\, 1 \leq \operatorname{rank}(A) \leq t\}$$

and

$$A(t, m) := \{A \in \mathbb{A}_m : \operatorname{rank}(A) = t\}.$$

Note that $\mathbb{A}(t, m) = \emptyset$ for $t \leq 0$ and $A(t, m) = \mathbb{A}(t, m) \setminus \mathbb{A}(t-1, m)$ for $t \geq 1$.

It is well known that the rank of a skew-symmetric matrix is even (see for example [1]). Therefore we have, $A(2t+1, m) = \emptyset$ for every nonnegative integer t.

Consequently, we get $\mathbb{A}(2t,m) = \mathbb{A}(2t+1,m)$. By definition we have

$$\mathbb{A}(2t,m) = \bigcup_{r=1}^{t} A(2r,m)$$

and the union is disjoint. If $n_a(2r,m)$ and $N_a(2t,m)$ denote the cardinality of the sets $A(2r,m)$ and $\mathbb{A}(2t,m)$, then

$$N_a(2t,m) = \sum_{r=1}^{t} n_a(2r,m). \tag{1}$$

Explicit expressions for $n_a(2r,m)$ in terms of r, m and q are well known in the literature (for odd characteristic see Theorem 3 in [5], for even characteristic see [13] or Chapt. 15, §2, Theorem 2 in [14]). Indeed $n_a(0,m) = 1$ and more generally for any $r \geq 0$

$$n_a(2r,m) = q^{r(r-1)} \frac{\prod_{i=0}^{2r-1} (q^{m-i} - 1)}{\prod_{i=0}^{r-1} (q^{2(r-i)} - 1)}. \tag{2}$$

Let $\mathbb{P}(\mathbb{A}_m)$ be the projective space over $\mathbb{A}_m$. Since $\mathbb{A}_m$ is an $\binom{m}{2}$ dimensional vector space, we can write $\mathbb{P}(\mathbb{A}_m) = \mathbb{P}^{\binom{m}{2}-1}$. For any non-zero matrix $A \in \mathbb{A}_m$ we denote by $[A]$ the corresponding homogeneous point of $\mathbb{P}^{\binom{m}{2}-1}$. More precisely, if $A = (a_{ij}) \in \mathbb{A}_m \setminus \{0\}$, then $[A] = [a_{1\,2} : \cdots : a_{m-1,m}]$, with all a_{ij} such that $i < j$ occurring as coordinates in $[A]$. Let $\mathbf{Det_A}(2t,m)$ be the image of the set $\mathbb{A}(2t,m)$ under this natural map $\mathbb{A}_m \setminus \{0\} \to \mathbb{P}^{\binom{m}{2}-1}$. The set $\mathbf{Det_A}(2t,m) \subseteq \mathbb{P}(\mathbb{A}_m)$ is a projective variety. More precisely, let $\mathbf{X} = (X_{ij})_{m\times m}$ be an $m \times m$ matrix in m^2 indeterminates X_{ij} over $\mathbb{F}_q$. Then $\mathbf{Det_A}(2t,m)$ is given as the zero locus of all $2t+1$ minors of $\mathbf{X}$ and linear polynomials $X_{ij} + X_{ji}$ and X_{ii} for every $1 \leq i \leq j \leq m$. Note that this describes $\mathbf{Det_A}(2t,m)$ as a subset of $\mathbb{P}^{m^2-1}$, but the linear equations $X_{ij} + X_{ji}$ and X_{ii} determine an $\binom{m}{2} - 1$ dimensional projective subspace of $\mathbb{P}^{m^2-1}$, which we previously had identified with $\mathbb{P}(\mathbb{A}_m)$. It is not hard to show that if $t > 0$, then $\mathbf{Det_A}(2t,m)$ is not contained in a hyperplane of $\mathbb{P}^{\binom{m}{2}-1}$, or in other words that $\mathbf{Det_A}(2t,m)$ is nondegenerately embedded in $\mathbb{P}^{\binom{m}{2}-1}$. Indeed let a pair (k,ℓ) be given such that $1 \leq k < \ell \leq m$. Then the skew-symmetric matrix A defined by $A_{k,\ell} = 1, A_{\ell,k} = -1$ and $A_{ij} = 0$ otherwise, is mapped to the projective point $[A] = [0 : \cdots : 0 : 1 : 0 : \cdots : 0] \in \mathbb{P}^{\binom{m}{2}-1}$ with a 1 in the position corresponding to the pair (k,ℓ). Hence $\mathbf{Det_A}(2t,m)$ contains $\binom{m}{2}$ projective points in general position, implying that it is not contained in a hyperplane.

We call $\mathbf{Det_A}(2t,m)$ a *skew-symmetric determinantal variety.* One can indeed show that it is a variety in the usual sense, but we will not need this fact here. Let $\Lambda_a(2t,m)$ denote the number of $\mathbb{F}_q$-rational points of $\mathbf{Det_A}(2t,m)$, then $\Lambda_a(2t,m)$

is given by

$$\Lambda_a(2t,m) = \frac{N_a(2t,m)}{q-1},$$

where the value of $N_a(2t,m)$ is determined by equations (1) and (2).

3. Linear Codes Associated to the Determinantal Variety $\mathbf{Det_A}(2t,m)$

Using the $\mathbb{F}_q$-rational points of $\mathbf{Det_A}(2t,m)$ as a projective system, yields a linear code $C_{\mathbf{A}}(2t,m)$ which we call a skew determinantal code. In order to make this precise, let $N := \Lambda_a(2t,m)$ and let $B_1,\ldots,B_N$ be representatives of all the $\mathbb{F}_q$-rational points of $\mathbf{Det_A}(2t,m)$. Note that for all i we have $B_i \in \mathbb{F}_q^{\binom{m}{2}}$. An element $B = (b_{ij})_{1\le i<j\le m} \in \mathbb{F}_q^{\binom{m}{2}}$ gives rise to a unique skew-symmetric matrix $A = (a_{ij})$ by setting $a_{ij} := b_{ij}$ if $i<j$, $a_{ii} := 0$, and $a_{ij} := -b_{ji}$ if $i>j$. Therefore we will with slight abuse of notation identify $\mathbb{F}_q^{\binom{m}{2}}$ with the space of skew-symmetric $m\times m$ matrices.

By construction, the matrix $G(2t,m)$ with columns $B_1,\ldots,B_N$ is a generator matrix of $C_{\mathbf{A}}(2t,m)$. Clearly therefore, the length of $C_{\mathbf{A}}(2t,m)$ equals $N = \Lambda_a(2t,m)$. Further, since from the previous section, we know that the $\mathbb{F}_q$-rational points of $\mathbf{Det_A}(2t,m)$ are not contained in any hyperplane of $\mathbb{P}^{\binom{m}{2}-1}$, the dimension of $C_{\mathbf{A}}(2t,m)$ equals $\binom{m}{2}$. In this section, we will determine the minimum distance of $C_{\mathbf{A}}(2t,m)$ in case q is odd. The case q is even seems more involved and could be interesting for future work. For the remainder of this article m and t will be assumed to be integers such that $m>0$ and $0\le 2t\le m$.

Another way to describe $C_{\mathbf{A}}(2t,m)$ is as the image of an evaluation map. Let $\mathbb{F}_q[\mathbf{X}]_1$ denotes the vector space of linear homogeneous polynomials in variables X_{ij}, $1\le i<j\le m$. Consider the evaluation map

$$\mathrm{Ev} : \mathbb{F}_q[\mathbf{X}]_1 \to \mathbb{F}_q^N \text{ defined by } f(\mathbf{X}) = \sum f_{ij}X_{ij} \mapsto (f(B_1),\ldots,f(B_N)).$$

The evaluation map Ev defined above is a linear map. Moreover, varying the pairs (i,j) with $1\le i<j\le m$, $\mathrm{Ev}(X_{ij})$ are precisely the $\binom{m}{2}$ rows of the matrix $G(2t,m)$. Therefore the image of Ev equals $C_{\mathbf{A}}(2t,m)$. Since $\mathbb{F}_q[\mathbf{X}]_1$ is an $\binom{m}{2}$-dimensional vector space over $\mathbb{F}_q$, the map Ev is a bijection. In order to determine the minimum distance of $C_{\mathbf{A}}(2t,m)$ we consider a related code $\widehat{C}_{\mathbf{A}}(2t,m)$ defined as the image of another evaluation map

$$\widehat{\mathrm{Ev}} : \mathbb{F}_q[\mathbf{X}]_1 \to \mathbb{F}_q^{N_a(2t,m)} \text{ defined by } f(\mathbf{X}) \to (f(A))_{A\in\mathbb{A}(2t,m)}.$$

Note that in the definition of $\widehat{\mathrm{Ev}}$ we implicitely used the identification of elements in $\mathbb{F}_q^{\binom{m}{2}}$ and $m\times m$ skew-symmetric matrices mentioned in the beginning of this section. The weights of the codewords in $C_{\mathbf{A}}(2t,m)$ and $\widehat{C}_{\mathbf{A}}(2t,m)$ are directly related to each other as the following easy lemma shows.

Lemma 3.1. *Let $f \in \mathbb{F}_q[\mathbf{X}]_1$ be a polynomial. Then the Hamming weights of the codewords* $\mathrm{Ev}(f)$ *and* $\widehat{Ev}(f)$ *satisfy*

$$\mathrm{w}_H(\widehat{\mathrm{Ev}}(f)) = (q-1)\,\mathrm{w}_H(\mathrm{Ev}(f)).$$

Proof. The proof of the lemma is a simple consequence of the fact that for every $f \in \mathbb{F}_q[\mathbf{X}]_1$ and any $A \in \mathbb{A}(2t,m)$, we have

$$f(A) \neq 0 \iff f(\alpha A) \neq 0 \text{ for all } \alpha \in \mathbb{F}_q^*.$$

□

In view of the above lemma, in order to compute the minimum distance of the code $C_{\mathbf{A}}(2t,m)$, it is enough to calculate the minimum distance of the code $\widehat{C}_{\mathbf{A}}(2t,m)$.

To proceed further, let us write $M := N_a(2t,m)$ and $\mathbb{A}(2t,m) = \{A_1,\dots,A_M\}$ in some fixed order. Note that codewords of $\widehat{C}_{\mathbf{A}}(2t,m)$ are indexed by the set $\mathbb{A}(2t,m)$ therefore, for every codeword $c \in \widehat{C}_{\mathbf{A}}(2t,m)$ and any $A_i \in \mathbb{A}(2t,m)$ we use the notation $c(A_i)$ to denote the A_i^{th} coordinate of the codeword c. From now on we always fix $\mathbb{F}_q$ as a finite field with characteristic of $\mathbb{F}_q$ not equal to 2.

Theorem 3.2. *For any codeword $(c_A)_{A\in\mathbb{A}(2t,m)} \in \widehat{C}_{\mathbf{A}}(2t,m)$, there exist a unique skew-symmetric matrix $F \in \mathbb{A}_m$ such that*

$$c_A = -\operatorname{tr}(FA) \text{ for every } A \in \mathbb{A}(2t,m).$$

Proof. Let $c \in \widehat{C}_{\mathbf{A}}(2t,m)$ and let $f \in \mathbb{F}_q[\mathbf{X}]_1$ be the linear polynomial such that $c = \widehat{\mathrm{Ev}}(f)$. In particular $c_A = f(A)$. Writing $f = \sum_{i<j} f'_{ij}X_{ij}$, define the $m\times m$ matrix $F := (f_{ij})$ by $f_{ij} := f'_{ij}/2$ if $i<j$, $f_{ii} := 0$ and $f_{ij} := -f'_{ji}/2$ if $i>j$. Note that F is skew-symmetric. We claim that for any $A = (a_{ij}) \in \mathbb{A}(2t,m)$ it holds that $f(A) = -\operatorname{tr}(FA)$, which would show the existence of the matrix F in the theorem. Indeed, we have

$$\begin{aligned} f(A) = \sum_{i<j} f'_{ij}a_{ij} &= \sum_{i<j}(f_{ij}-f_{ji})a_{ij} = \sum_{i<j} f_{ij}a_{ij} - \sum_{i<j} f_{ji}a_{ij} \\ &= -\sum_{i<j} f_{ij}a_{ji} - \sum_{j>i} f_{ji}a_{ij} = -\sum_{i=1}^{m}\sum_{j=1}^{m} f_{ij}a_{ji} = -\operatorname{tr}(FA). \end{aligned}$$

Here we used $a_{ij} = -a_{ji}$ in the fourth equality and $a_{ii} = 0$ in the fifth.

To show uniqueness, suppose that there exist two skew-symmetric matrices $F = (f_{ij})$ and $G = (g_{ij})$ such that $\operatorname{tr}(FA) = \operatorname{tr}(GA)$ for all $A \in \mathbb{A}(2t,m)$. For $k<\ell$, define the matrix $E(k,\ell)$ as the matrix with zero entries everywhere except for the coordinates (k,ℓ), respectively (ℓ,k), where the matrix has entry 1, respectively -1. Since $t \geq 1$, we have $E(k,\ell) \in \mathbb{A}(2t,m)$. Moreover, $\operatorname{tr}(FE(k,\ell)) = -f_{k\ell} + f_{\ell k} = -2f_{k\ell}$ and similarly $\operatorname{tr}(FE(k,\ell)) = -2g_{k\ell}$. Hence $F = G$ follows. □

Note that the assumption that q is odd is crucial in the above theorem. Indeed, if q is even the theorem is not true, since it is not hard to show that $\operatorname{tr}(FA) = 0$ for any two skew-symmetric matrices F and A. Also note that since both $\mathbb{F}_q[\mathbf{X}]_1$ and the space of skew-symmetric matrices $\mathbb{A}_m$, are vector spaces of the same dimension $\binom{m}{2}$, any word of the form $(-\operatorname{tr}(FA))_A$ is a codeword of $\widehat{C}_{\mathbf{A}}(2t, m)$. As a consequence of the theorem, we will see that the code $\widehat{C}_{\mathbf{A}}(2t, m)$ (and hence $C_{\mathbf{A}}(2t, m)$) only can have few weights.

Corollary 3.3. *If $c = (-\operatorname{tr}(FA))_{A\in\mathbb{A}(2t,m)} \in \widehat{C}_{\mathbf{A}}(2t, m)$ for a skew-symmetric matrix F, then the Hamming weight of c only depends on the rank of F. Moreover, there are at most $\lfloor m/2\rfloor$ possibilities for the Hamming weight of a nonzero codeword $c \in C_{\mathbf{A}}(2t, m)$.*

Proof. Let $c = (c_A)_{A\in\mathbb{A}(2t,m)} \in \widehat{C}_{\mathbf{A}}(2t, m)$ be a nonzero codeword. By Theorem 3.2, there exists a nonzero skew-symmetric matrix F such that $c_A = -tr(FA)$ for all $A \in \mathbb{A}(2t, m)$. By Theorem 4 in [1] or alternatively Chapter XV, Corollary 8.2 in [11], there exist a nonsingular $m \times m$ matrix L such that

$$LFL^T = \begin{bmatrix} E & & & & \\ & E & & & \\ & & \ddots & & \\ & & & E & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix}, \text{ with } E = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

The number of occurrences of the matrix E depends on the rank of F. Specifically, if the rank of F, which necessarily is even, equals $2k$ for some $1 \le k \le m/2$, then the matrix E occurs k times. Since L is nonsingular, the mapping $A \mapsto L^T AL$ is a permutation of $\mathbb{A}(2t, m)$. For every matrix A, we have $\operatorname{tr}((LFL^T)A) = \operatorname{tr}(F(L^T AL))$. Therefore, the Hamming weights of the codewords c and $(\operatorname{tr}((LFL^T)A))_{A\in\mathbb{A}(2t,m)}$ are the same. In particular, the Hamming weight of c only depends on the rank of F. The first part of the corollary now follows.

Since k needs to be an integer satisfying $1 \le k \le m/2$, we see that there are only $\lfloor m/2\rfloor$ possible ranks for F. This shows that there are at most $\lfloor m/2\rfloor$ possibilities for the Hamming weight of c. By Lemma 3.1, the second part of the corollary follows. □

To determine the minimum distance of $C_{\mathbf{A}}(2t, m)$, we need to determine which of the possible $\lfloor m/2\rfloor$ weights is the smallest. In order to do that, let us fix some notations. If $c = (-\operatorname{tr}(FA))_{A\in\mathbb{A}(2t,m)} \in \widehat{C}_{\mathbf{A}}(2t, m)$ for a skew-symmetric matrix F of rank $2k$, we define $\mathrm{W}_{2k}(2t, m) := \mathrm{w}_H(c)$. By Corollary 3.3, this is a valid definition, since $\mathrm{w}_H(c)$ does not depend on the choice of F. For $0 \le 2k \le m$, define

the skew-symmetric $m \times m$ matrix of rank $2k$

$$E_{2k} := \begin{bmatrix} E & & & & \\ & E & & & \\ & & \ddots & & \\ & & & E & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix}, \tag{3}$$

with E as in the proof of Corollary 3.3 occurring exactly k times. Then

$$\mathrm{W}_{2k}(2t, m) = |\{A \in \mathbb{A}(2t, m) \,:\, \mathrm{tr}(E_{2k}A) \neq 0\}|.$$

If we define

$$\mathrm{S}_{2k}(2r, m) := \{A \in A(2r, m) \,:\, \mathrm{tr}(E_{2k}A) \neq 0\} \text{ and } \mathrm{w}_{2k}(2r, m) := |\mathrm{S}_{2k}(2r, m)|,$$

then

$$\mathrm{W}_{2k}(2t, m) = \sum_{r=1}^{t} \mathrm{w}_{2k}(2r, m). \tag{4}$$

Our next goal is to find recursive formulas for $\mathrm{W}_{2k}(2t, m)$, that we will use as the key ingredient to show which of the $\mathrm{W}_{2k}(2t, m)$ is the smallest. Note that this approach is inspired by [3], where a similar approach was developed to determine the minimum distance of the determinantal code introduced in [2].

Theorem 3.4. *Let m and $0 < 2k \leq m$ be fixed. Let $0 < 2r \leq m$ and $\mathrm{w}_{2k}(2r, m)$ be as defined above. Then*

$$\begin{aligned} \mathrm{w}_{2k}(2r, m) = {} & q^{2r}\mathrm{w}_{2k-2}(2r, m-2) + (q-1)q^{2r-1}\left(n_a(2r, m-1) - n_a(2r, m-2)\right) \\ & + (q-1)q^{m-2}n_a(2r-2, m-1) - q^{2r-2}\mathrm{w}_{2k-2}(2r-2, m-2) \\ & - (q-1)q^{2r-3}\left(n_a(2r-2, m-1) - n_a(2r-2, m-2)\right). \end{aligned}$$

Proof. Given a matrix $A \in A(2r, m)$, denote by A' the matrix obtained by deleting the $(2k)^{th}$ row and column of the matrix A. Then A' is a skew-symmetric matrix of rank between $2r-2$ and $2r$. Since the rank of a skew-symmetric matrix is even, the rank of A' can be either $2r$ or $2r-2$. Now consider the map

$$\phi : \mathrm{S}_{2k}(2r, m) \to A(2r, m-1) \bigcup A(2r-2, m-1), \text{ defined by } A \mapsto A'.$$

We use this map to count the cardinality of the set $\mathrm{S}_{2k}(2r, m)$ which is $\mathrm{w}_{2k}(2r, m)$. Using the map ϕ we get,

$$\mathrm{w}_{2k}(2r, m) = \sum_{A' \in A(2r, m-1)} |\phi^{-1}(A')| + \sum_{A' \in A(2r-2, m-1)} |\phi^{-1}(A')|.$$

For any matrix A', let A'_{2k-1} denote the $(2k-1)^{th}$ row of A'. We divide each sum in the above expression in two different terms, depending on whether A'_{2k-1} is zero or non-zero. Rewriting the above expression, we get

$$\begin{aligned}\mathrm{w}_{2k}(2r,m) = &\sum_{\substack{A'\in A(2r,m-1)\\ A'_{2k-1}=0}} |\phi^{-1}(A')| + \sum_{\substack{A'\in A(2r,m-1)\\ A'_{2k-1}\neq 0}} |\phi^{-1}(A')| \\ &+ \sum_{\substack{A'\in A(2r-2,m-1)\\ A'_{2k-1}=0}} |\phi^{-1}(A')| + \sum_{\substack{A'\in A(2r-2,m-1)\\ A'_{2k-1}\neq 0}} |\phi^{-1}(A')|.\end{aligned} \tag{5}$$

We divide the counting of the fibers $\phi^{-1}(A')$ in four different cases corresponding to the four summations in this equation. Given a row or column vector $v = (v_1, \ldots, v_m) \in \mathbb{F}_q^m$, we will use the phrase *shortened row or column vector* for the vector $v' \in \mathbb{F}_q^{m-1}$ obtained from v by deleting its $(2k)^{th}$ coordinate. In this way, we can for example say that the rows of A' are obtained by shortening rows of the matrix A and likewise for columns. We will use the $m \times m$ matrix E_{2k} defined in equation (3), but whenever we write E_{2k-2} in the proof below, we will mean an $(m-1) \times (m-1)$ matrix of rank $2k-2$ of the form as in equation (3).

Case 1: Let $A' \in A(2r, m-1)$ and $A'_{2k-1} = 0$. Let $A \in \phi^{-1}(A')$. Since A and A' have the same rank $2r$, we conclude that the shortened $(2k)^{th}$ column of A lies in the column space of A'. This in particular means that the entry $A_{2k-1,2k}$ is a linear combination of the entries in A'_{2k-1} and hence zero. Hence, $\mathrm{tr}(E_{2k-2}A') = \mathrm{tr}(E_{2k}A) \neq 0$, where the inequality follows by our assumption that $A \in \mathrm{S}_{2k}(2r, m)$. Therefore, the first summation in equation (5) runs over $\mathrm{w}_{2k-2}(2r, m-2)$ many matrices A' and for any such A' we get $|\phi^{-1}(A')| = q^{2r}$, since the dimension of the column space of A' equals $2r$. Therefore in total, we get

$$\sum_{\substack{A'\in A(2r,m-1)\\ A'_{2k-1}=0}} |\phi^{-1}(A')| = q^{2r}\mathrm{w}_{2k-2}(2r, m-2). \tag{6}$$

Case 2: Let $A' \in A(2r, m-1)$ and $A'_{2k-1} \neq 0$. As in the previous case, for any $A \in \phi^{-1}(A')$ the shortened $(2k)^{th}$ column of A must lie in the column span of A'. Moreover, we require that $2A_{2k-1,2k} \neq \mathrm{tr}(E_{2k-2}A')$. Since A'_{2k-1} is assumed to be non zero, the projection map from the column space of A' to the $(2k-1)^{th}$ coordinate is nonzero. Since the column space of A' has dimension $2r$, we see that for a given A', there are exactly $q^{2r} - q^{2r-1}$ possibilities to choose the $(2k)^{th}$ column of A such that $2A_{2k-1,2k} \neq \mathrm{tr}(E_{2k-2}A')$. In other words: $|\phi^{-1}(A')| = q^{2r} - q^{2r-1}$. Further, the number of matrices $A' \in A(2r, m-1)$ such that $A'_{2k-1} \neq 0$ is given by $n_a(2r, m-1) - n_a(2r, m-2)$. In total we get

$$\sum_{\substack{A'\in A(2r,m-1)\\ A'_{2k-1}\neq 0}} |\phi^{-1}(A')| = (q-1)q^{2r-1}(n_a(2r, m-1) - n_a(2r, m-2)). \tag{7}$$

Case 3: Let $A' \in A(2r-2, m-1)$ and $A'_{2k-1} = 0$. This is the most complex case therefore, we divide the counting in several subcases.

First, we count the number of $A \in \phi^{-1}(A')$ satisfying $A_{2k-1,2k} = 0$. Since $A_{2k-1,2k} = 0$, we have $m-2$ positions in the $(2k)^{th}$ column of A that are undetermined. Moreover, the shortened $(2k)^{th}$ column of A can not be in the column span of A'. Since A' is of rank $2r-2$ and $A'_{2k-1} = 0$, this leaves exactly $q^{m-2} - q^{2r-2}$ possibilities for the matrix A. Further, in all these cases we get $\mathrm{tr}(E_{2k-2}A') = \mathrm{tr}(E_{2k}A) \neq 0$. Therefore, there are $\mathrm{w}_{2k-2}(2r-2, m-2)$ many possibilities for A'.

Second, we count the number of $A \in \phi^{-1}(A')$ satisfying $A_{2k-1,2k} \neq 0$. We further divide this in two parts depending on $\mathrm{tr}(E_{2k-2}A')$ being zero or non-zero. If $\mathrm{tr}(E_{2k-2}A') = 0$, then $\mathrm{tr}(E_{2k}A) = -2A_{2k-1,2k} \neq 0$. Hence, the only restriction we have is that the shortened $(2k)^{th}$ column of A can not be in the column span of A'. However, since we assign a nonzero value to $A_{2k-1,2k}$, this is guaranteed. The remaining positions can be chosen arbitrarily. Therefore, in this case we get $n_a(2r-2, m-2) - \mathrm{w}_{2k-2}(2r-2, m-2)$ many matrices A' with $\mathrm{tr}(E_{2k-2}A') = 0$ and for any such A', the cardinality of the fiber is $(q-1)q^{m-2}$.

If $\mathrm{tr}(E_{2k-2}A') \neq 0$, then in addition to $A_{2k-1,2k} \neq 0$ we require $2A_{2k-1,2k} \neq \mathrm{tr}(E_{2k-2}A')$, leaving $q-2$ possible values for $A_{2k-1,2k}$. We have $\mathrm{w}_{2k-2}(2r-2, m-2)$ many possibilities for the matrix A', since we assumed $\mathrm{tr}(E_{2k-2}A') \neq 0$. For a given A', we have $(q-2)q^{m-2}$ many matrices A in the fiber $\phi^{-1}(A')$. Adding all together, we obtain

(8)
$$\begin{aligned}\sum_{\substack{A' \in A(2r-2,m-1)\\ A'_{2k-1}=0}} |\phi^{-1}(A')| &= (q^{m-2} - q^{2r-2})\mathrm{w}_{2k-2}(2r-2, m-2)\\ &+ (q-1)q^{m-2}\left(n_a(2r-2, m-2) - \mathrm{w}_{2k-2}(2r-2, m-2)\right)\\ &+ (q-2)q^{m-2}\mathrm{w}_{2k-2}(2r-2, m-2).\end{aligned}$$

Case 4: Finally, let $A' \in A(2r-2, m-1)$ and $A'_{2k-1} \neq 0$. Since A' is of rank $2r-2$, the shortened $(2k)^{th}$ column of A must not lie in the column span of A'. Further, $2A_{2k-1,2k} \neq \mathrm{tr}(E_{2k-2}A')$. Like in Case 2, we consider the projection map on the $(2k-1)^{th}$ coordinate. First of all, we require $2A_{2k-1,2k} \neq \mathrm{tr}(E_{2k-2}A')$, leaving $q^{m-1} - q^{m-2}$ a priori possibilities for the $(2k)^{th}$ column of A. However, since the shortened $(2k)^{th}$ column of A cannot lie in the column span of A', $q^{2r-2} - q^{2r-3}$ many of these possibilities need to be excluded. This shows that for a given A' as above, $|\phi^{-1}(A')| = (q^{m-1} - q^{m-2}) - (q^{2r-2} - q^{2r-3})$. Also, there are $n_a(2r-2, m-1) - n_a(2r-2, m-2)$ many matrices A' satisfying $A' \in A(2r-2, m-1)$ and $A'_{2k-1} \neq 0$. All together, we get

(9)
$$\sum_{\substack{A' \in A(2r-2,m-1)\\ A'_{2k-1}\neq 0}} |\phi^{-1}(A')| = (q-1)(q^{m-2} - q^{2r-3})(n_a(2r-2, m-1) - n_a(2r-2, m-2)).$$

Now the theorem follows from equations (5), (6), (7), (8), and (9). □

We will use Theorem 3.4 to find expressions for the weights $\mathrm{W}_{2k}(2t,m)$ of the codewords in $\widehat{C}_{\mathbf{A}}(2t,m)$. It will be convenient for every $0 \leq r \leq t$ to introduce the quantity

(10)
$$P_m(2k,2r) := q^{2r}\mathrm{w}_{2k-2}(2r,m-2) + (q-1)q^{2r-1}\left(n_a(2r,m-1) - n_a(2r,m-2)\right).$$

Note that by our conventions $P_m(2k,0) = 0$. Theorem 3.4 has the following corollary.

Corollary 3.5. *Let t and k be integers such that $0 < 2t \leq m$ and $0 < 2k \leq m$. Then*

$$\mathrm{W}_{2k}(2t,m) = P_m(2k,2t) + (q-1)q^{m-2}N_a(2t-2,m-1).$$

Proof. Using Theorem 3.4 and the quantity $P_m(2k,2r)$ defined in equation (10), a direct computation shows that

$$\mathrm{w}_{2k}(2r,m) = P_m(2k,2r) - P_m(2k,2r-2) + (q-1)q^{m-2}n_a(2r-2,m-1).$$

Then equation (4) implies that

$$\mathrm{W}_{2k}(2t,m) = P_m(2k,2t) - P_m(2k,0) + (q-1)q^{m-2}\sum_{r=1}^{t} n_a(2r-2,m-1).$$

The corollary now follows. □

Theorem 3.6. *The minimum distance of the code $C_{\mathbf{A}}(2t,m)$ is given by*

$$\frac{\mathrm{W}_2(2t,m)}{q-1} = (q^{m-2t}-1)q^{m+2t-4}n_a(2t-2,m-2) \ + \ q^{m-2}N_a(2t-2,m-1).$$

Proof. First we show that $\mathrm{W}_2(2t,m)$ is the minimum distance of $\widehat{C}_{\mathbf{A}}(2t,m)$. Lemma 3.1 then implies that $\mathrm{W}_2(2t,m)/(q-1)$ is the minimum distance of $C_{\mathbf{A}}(2t,m)$.

We know that the weight of a non-zero codeword of $\widehat{C}_{\mathbf{A}}(2t,m)$ is among $\mathrm{W}_{2k}(2t,m)$ where $1 \leq k \leq \left\lfloor \frac{m}{2} \right\rfloor$. From Corollary 3.5, we get

$$\mathrm{W}_{2k}(2t,m) - \mathrm{W}_2(2t,m) = P_m(2k,2t) - P_m(2,2t).$$

Using equation (10) and taking into account that $\mathrm{w}_0(2t,m-2) = 0$, we get

$$\mathrm{W}_{2k}(2t,m) - \mathrm{W}_2(2t,m) = q^{2t}\mathrm{w}_{2k-2}(2t,m-2). \tag{11}$$

In particular, we get $\mathrm{W}_{2k}(2t,m) \geq \mathrm{W}_2(2t,m)$ for every $1 \leq k \leq \left\lfloor \frac{m}{2} \right\rfloor$ and hence $\mathrm{W}_2(2t,m)$ is the minimum distance of the code $\widehat{C}_{\mathbf{A}}(2t,m)$.

To finish the proof, it is sufficient to show that

$$\mathrm{W}_2(2t,m) = (q-1)(q^{m-2t}-1)q^{m+2t-4}n_a(2t-2,m-2) + (q-1)q^{m-2}N_a(2t-2,m-1).$$

Corollary 3.5 implies that

$$\mathrm{W}_2(2t,m) \ = \ P_m(2,2t) + (q-1)q^{m-2}N_a(2t-2,m-1).$$

Therefore, we only need to show that

$$P_m(2,2t) = (q-1)(q^{m-2t}-1)q^{m+2t-4}n_a(2t-2,m-2).$$

From equation (10), we have

$$P_m(2,2t) = q^{2t}\mathrm{w}_0(2t,m-2) + (q-1)q^{2t-1}\left(n_a(2t,m-1) - n_a(2t,m-2)\right).$$

Since $\mathrm{w}_0(2t,m-2)=0$, equation (2) implies

$$\begin{aligned}
P_m(2,2t) &= (q-1)q^{2t-1}\left\{ q^{t(t-1)}\frac{\prod_{i=0}^{2t-1}(q^{m-1-i}-1)}{\prod_{i=0}^{t-1}(q^{2(t-i)}-1)} - q^{t(t-1)}\frac{\prod_{i=0}^{2t-1}(q^{m-2-i}-1)}{\prod_{i=0}^{t-1}(q^{2(t-i)}-1)}\right\}\\
&= (q-1)q^{2t-1}\left\{ q^{t(t-1)}\frac{\prod_{i=0}^{2t-2}(q^{m-2-i}-1)}{\prod_{i=0}^{t-1}(q^{2(t-i)}-1)}\left(q^{m-1}-q^{m-2t-1}\right)\right\}\\
&= (q-1)q^{2t-1}\left\{ q^{m-2t-1}\left(q^{m-2t}-1\right)q^{t(t-1)}\frac{\prod_{i=0}^{2(t-1)-1}(q^{m-2-i}-1)}{\prod_{i=0}^{(t-1)-1}(q^{2(t-i)}-1)}\right\}\\
&= (q-1)(q^{m-2t}-1)q^{m+2t-4}q^{(t-1)(t-2)}\frac{\prod_{i=0}^{2(t-1)-1}(q^{m-2-i}-1)}{\prod_{i=0}^{(t-1)-1}(q^{2(t-i)}-1)}\\
&= (q-1)(q^{m-2t}-1)q^{m+2t-4}n_a(2t-2,m-2).
\end{aligned}$$

This completes the proof of the theorem. □

Remark 3.7. Recall that $1 \le t \le \lfloor m/2 \rfloor$. In the extremal choices of t, the code $C_{\mathbf{A}}(2t,m)$ is equal to well known previously studied codes. For $t=1$, the determinantal variety $\mathbf{Det}_{\mathbf{A}}(2t,m)$ is simply the line Grassmann variety $G(2,m)$. Hence in this case the code $C_{\mathbf{A}}(2t,m)$ is a particular instance of the Grassmann codes studied in [15]. In fact from [15], the complete weight enumerator of the code $C_{\mathbf{A}}(2,m)$ can be obtained. From Nogin's results it is easy to show that $\mathrm{W}_2(2,m) < \cdots < \mathrm{W}_{2\lfloor m/2\rfloor}(2,m)$.

For $t = \lfloor \frac{m}{2} \rfloor$, we have $\mathbf{Det}_{\mathbf{A}}(2t,m) = \mathbb{P}^{\binom{m}{2}-1}$. Hence in this case $C_{\mathbf{A}}(2t,m)$ is a first order projective Reed–Muller code. Projective Reed–Muller codes were introduced in [10]. It is well known that first order projective Reed–Muller codes are constant weight codes. Indeed equation (11) implies that $\mathrm{W}_2(2\lfloor m/2\rfloor,m) = \mathrm{W}_{2k}(2\lfloor m/2\rfloor,m)$ for every k.

It is in general not clear how the elements in the sequence $\mathrm{W}_{2k}(2t,m)$, $2 \leq 2k \leq m$ are ordered. However, in case $1 < t < \lfloor m/2 \rfloor$, we are able to determine the minimum among them.

Theorem 3.8. *Suppose that* $4 \leq 2k \leq m$ *and* $4 \leq 2t \leq m-2$. *Then* $\mathrm{W}_2(2t,m) < \mathrm{W}_{2k}(2t,m)$. *Moreover, the number of minimum weight codeword in* $C_{\mathbf{A}}(2t,m)$ *equals* $(q^m-1)(q^{m-1}-1)/(q^2-1)$.

Proof. Using equation (11), the first part of the theorem follows once we show that $\mathrm{w}_{2k-2}(2t,m-2) > 0$. Equation (9) in the proof of Theorem 3.4 implies that

$$\mathrm{w}_{2k-2}(2t,m-2) \geq (q-1)(q^{m-4}-q^{2t-3})(n_a(2t-2,m-3)-n_a(2t-2,m-4)).$$

Using a similar computation as in the proof of Theorem 3.6, we can rewrite the right-hand side of this inequality and obtain that

$$\mathrm{w}_{2k-2}(2t,m-2) \geq (q-1)(q^{m-2t-1}-1)(q^{m-2t}-1)q^{m+2t-8}n_a(2t-4,m-4).$$

Since $t \geq 2$, equation (2) implies that $\mathrm{w}_{2k-2}(2t,m-2) > 0$.

Since $\mathrm{W}_2(2t,m) < \mathrm{W}_{2k}(2t,m)$, Theorem 3.2 implies that minimum weight codewords bijectively correspond to matrices $F \in A(2,m)$. Hence the number of minimum weight codewords equals $|A(2,m)| = n_a(2,m) = (q^m-1)(q^{m-1}-1)/(q^2-1)$. In the last equality, we used equation (2). □

4. Acknowledgements

Prasant Singh is supported by the HCØrsted-COFUND postdoctoral grant *Understanding Schubert Codes*.

Peter Beelen would like to acknowledge the support from The Danish Council for Independent Research (DFF-FNU) for the project *Correcting on a Curve*, Grant No. 8021-00030B.

The authors would also like to thank the referees for their valuable comments and suggestions.

References

[1] A.A. Albert, Symmetric and alternate matrices in an arbitrary field I, *Trans. Amer. Math. Soc.* **43** (1938), no. 3, 386–436.

[2] P. Beelen, S.R. Ghorpade and S.U. Hasan, Linear codes associated to determinantal varieties, *Discrete Math.* **338** (2015), 1493–1500.

[3] P. Beelen and S.R. Ghorpade, Hyperplane Sections of Determinantal Varieties over Finite Fields and Linear Codes, preprint available arXiv:1809.04690.

[4] P. Beelen and F. Piñero, The structure of dual Grassmann codes, *Des. Codes Cryptogr.* **79** (2016), 451–470.

[5] L. Carlitz, Representations by skew forms in a finite field, *Arch. Math.* (Basel) **5** (1954), 19–31.

[6] S.R. Ghorpade and G. Lachaud, Higher weights of Grassmann codes, *Coding Theory, Cryptography and Related Areas* (Guanajuato, 1998), J. Buchmann, T. Høholdt, H. Stichtenoth and H. Tapia-Recillas Eds., Springer-Verlag, Berlin, 2000, 122–131.

[7] J. Hansen, Toric surfaces and error correcting codes, *Coding Theory, Cryptography and Related Areas* (Guanajuato, 1998), J. Buchmann, T. Høholdt, H. Stichtenoth and H. Tapia-Recillas Eds., Springer-Verlag, Berlin, 2000, 132–142.

[8] J. Harris and L.W. Tu, On symmetric and skew-symmetric determinantal varieties, *Topology* **23** (1984), 71–84.

[9] T. Jôzefiak, A. Lascoux and P. Pragacz, Classes of determinantal varieties associated with symmetric and skew-symmetric matrices, *Izv. Akad. Nauk SSSR Ser. Mat.* **18** (1981), 662–673.

[10] G. Lachaud, Projective Reed–Muller codes, Coding theory and applications, *Lecture Notes in Comput. Sci.* **311**, Springer, Berlin, 1988, 125–129.

[11] S. Lang, Algebra, Third edition, Addison-Wesley Publishing Company, Reading, MA, 1994.

[12] J.B. Little, Codes from Higher Dimensional Varieties, Chapter 7 in *Advances in Algebraic Geometry Codes. Series on Coding Theory and Cryptology* vol.5, World Scientific Publishing Co. Pte. Ltd., 2008, 257–293.

[13] F.J. MacWilliams, Orthogonal matrices over finite fields, *Amer. Math. Monthly* **76** (1969), 152–164.

[14] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[15] D.Yu. Nogin, Codes associated to Grassmannians, *Arithmetic, Geometry and Coding Theory* (Luminy, 1993), R. Pellikaan, M. Perret, S. G. Vlăduţ, Eds., Walter de Gruyter, Berlin, 1996, 145–154.

[16] F. Rodier, Codes from flag varieties over a finite field, *J. Pure Appl. Algebra* **178** (2003), 203–214.

[17] D. Ruano, On the parameters of r-dimensional toric codes, *Finite Fields and Their Applications* **13** (2007), 962–976.

[18] C.T. Ryan, An application of Grassmannian varieties to coding theory, *Congr. Numer.* **157** (1987), 257–271.

[19] C.T. Ryan, Projective codes based on Grassmann varieties, *Congr. Numer.* **157** (1987), 273–279.

[20] I.R. Shafarevich, Basic Algebraic Geometry 1: Varieties in Projective Space, Translated by M. Reid, Springer-Verlag Berlin Heidelberg, 2013.

[21] M. Tsfasman, S. Vlăduţ and D. Nogin, Algebraic Geometric Codes: Basic Notions, Math. Surv. Monogr., vol. 139, Amer. Math. Soc., Providence, 2007.

Department of Applied Mathematics and Computer Science,
Technical University of Denmark,
Matematiktorvet 303B, 2800 Kgs. Lyngby, Denmark.
E-mail address: pabe@dtu.dk

Department of Applied Mathematics and Computer Science,
Technical University of Denmark,
Matematiktorvet 303B, 2800 Kgs. Lyngby, Denmark.
E-mail address: psinghprasant@gmail.com