Affine Grassmann Codes

Peter Beelen, Sudhir R. Ghorpade, and Tom Høholdt, *Fellow, IEEE*

***Abstract*—We consider a new class of linear codes, called affine Grassmann codes. These can be viewed as a variant of generalized Reed-Muller codes and are closely related to Grassmann codes. We determine the length, dimension, and the minimum distance of any affine Grassmann code. Moreover, we show that affine Grassmann codes have a large automorphism group and determine the number of minimum weight codewords.**

***Index Terms*—Automorphism group, Grassmann codes, number of minimum weight codewords.**

I. Introduction

REED-MULLER codes are among the most widely studied classes of linear error correcting codes. Numerous generalizations and variants of Reed-Muller codes have also been considered in the literature (see, for example, [2], [12, Ch. 13–15], [14, Ch. 1, Sec. 13; Ch. 11, Sec. 3.4.1; Ch. 16, Sec. 3; Ch. 17, Sec. 4] and the relevant references therein). In this paper, we introduce a class of linear codes that appears to be a genuinely distinct variant of Reed-Muller codes. As explained in Section VII, this new class of codes is intimately related to the so-called Grassmann codes, which have been of much current interest (see, for example, [6], [7], [9], [13], and the relevant references therein), and with this in view we call these the *affine Grassmann codes*. Roughly speaking, affine Grassmann codes are obtained by evaluating linear polynomials in the minors of a generic $\ell \times \ell'$ matrix at all points of the corresponding affine space over a finite field. Evidently, when $\ell = 1$, this gives the first order generalized Reed-Muller code $\mathrm{RM}(1, \ell')$. However, in general, the resulting code is distinct from higher order generalized Reed-Muller codes and determination of several of its properties appears to be rather nontrivial. Our main results include the determination of the minimal distance (Theorem 16) and a characterization as well as an explicit enumeration of the minimum weight codewords (Theorems 28 and 32). Further, we show that affine Grassmann codes have a large automorphism group (Theorem 21); this result could be viewed as an extension of the work of Delsarte, Goethals and MacWilliams [2, Thm. 2.3.1], Knörr and Willems [11] as well as Berger and Charpin [1] on the automorphisms of Reed-Muller codes. In geometric terms, some of our results could be viewed as a generalization of elementary facts about hyperplanes over finite fields to "determinantal hyperplanes". (See Remark 11 for greater details.) The auxiliary results obtained in the course of proving the main theorems and the techniques employed may also be of some independent interest.

Manuscript received November 05, 2009; revised April 01, 2010. Current version published June 16, 2010. The work was supported by the Danish FNU-grant: Algebraic Coding Theory.

P. Beelen and T. Høholdt are with the Department of Mathematics, Technical University of Denmark, DK 2800, Lyngby, Denmark (e-mail: p.beelen@mat.dtu.dk; T.Hoeholdt@mat.dtu.dk).

S. R. Ghorpade is with the Department of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400076 India (e-mail: srg@math.iitb.ac.in).

Communicated by G. Cohen, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2010.2048470

II. Preliminaries

Denote, as usual, by $\mathbb{F}_q$ the finite field with q elements. Fix positive integers ℓ and ℓ' and a $\ell \times \ell'$ matrix $X = (X_{ij})$ whose entries are algebraically independent indeterminates over $\mathbb{F}_q$. By $\mathbb{F}_q[X]$ we denote the polynomial ring in the $\ell\ell'$ indeterminates $X_{ij} (1 \leq i \leq \ell,\ 1 \leq j \leq \ell')$ with coefficients in $\mathbb{F}_q$. For convenience, we introduce the following notation for the rows and columns of the matrix X:

$$\mathbf{X}_i = (X_{i1} \cdots X_{i\ell'}) \text{ for } 1 \leq i \leq \ell$$

and

$$\mathbf{X}^j = \begin{pmatrix} X_{1j} \\ \vdots \\ X_{\ell j} \end{pmatrix} \text{ for } 1 \leq j \leq \ell'.$$

Recall that by a *minor* of X of order i we mean the determinant of an $i \times i$ submatrix of X. A minor of X of order i is sometimes referred to as an $i \times i$ minor of X. But in any case, it should be remembered that the minors of X are not matrices, but are elements of the polynomial ring $\mathbb{F}_q[X]$.

We are primarily interested in the linear space generated by all the minors of X. This is unchanged if we replace X by its transpose. With this in view, we shall always assume that $\ell \leq \ell'$. Further, we set

$$m = \ell + \ell' \quad \text{and} \quad \delta = \ell\ell'.$$

For $0 \leq i \leq \ell$, we let $\Delta_i(\ell, m)$ be the set of all $i \times i$ minors of X, where, as per standard conventions, the only 0×0 minor of X is 1. We define

$$\Delta(\ell, m) = \bigcup_{i=0}^{\ell} \Delta_i(\ell, m).$$

Definition 1: The linear space $\mathcal{F}(\ell, m)$ over $\mathbb{F}_q$ is the subspace of $\mathbb{F}_q[X]$ generated by $\Delta(\ell, m)$.

For example, if $\ell = \ell' = 2$, then $m = 4$, $\delta = 4$, and $\Delta_0(2, 4) = \{1\}$, while

$$\Delta_1(2, 4) = \{X_{11}, X_{12}, X_{21}, X_{22}\}$$

and

$$\Delta_2(2, 4) = \{X_{11}X_{22} - X_{12}X_{21}\}.$$

Thus a typical element of $\mathcal{F}(2, 4)$ looks like

$$a + b_1X_{11} + b_2X_{12} + b_3X_{21} + b_4X_{22} + c(X_{11}X_{22} - X_{12}X_{21}) \tag{1}$$

where $a, b_1, b_2, b_3, b_4, c \in \mathbb{F}_q$. Observe that $\#\Delta(2,4) = 6$, where for a finite set D, we denote by $\#D$ the cardinality of D. In general, we have the following.

Lemma 2: The cardinality of $\Delta(\ell, m)$ is $\binom{m}{\ell}$.

Proof: Since the entries of X are indeterminates, the number of minors of X of order i is the number of $i \times i$ submatrices of X. An $i \times i$ submatrix of X is obtained by choosing i rows among the ℓ rows and i columns among the ℓ' columns. Thus

$$\#\Delta_i(\ell, m) = \binom{\ell}{i}\binom{\ell'}{i} \quad \text{for } 0 \le i \le \ell.$$

Consequently

$$\#\Delta(\ell, m) = \sum_{i \ge 0} \binom{\ell}{\ell - i}\binom{\ell'}{i} = \binom{m}{\ell},$$

where the last equality follows from the so-called Chu-Vandermonde summation (see e.g., [8, Sec. 5.1, (5.27)]). ∎

We remark that an alternative proof of the above lemma can be obtained by observing that the minors of X (of arbitrary orders) are in a natural one-to-one correspondence with the $\ell \times \ell$ minors of the $\ell \times m$ matrix $(X|I)$ obtained by adjoining to X a $\ell \times \ell$ identity matrix.

The following basic result can be viewed as a very special case of the standard basis theorem or the straightening law of Doubilet, Rota and Stein (cf. [3], [5, Thm. 4.2]). In the case we are interested in, a much simpler proof can be given and this is included below.

Lemma 3: The elements of $\Delta(\ell, m)$ are linearly independent. In particular

$$\dim_{\mathbb{F}_q} \mathcal{F}(\ell, m) = \binom{m}{\ell}.$$

Proof: Suppose there is a linear dependence relation $\sum_{\mathcal{M} \in \Delta(\ell,m)} a_{\mathcal{M}} \mathcal{M} = 0$, where $a_{\mathcal{M}} \in \mathbb{F}_q$ for $\mathcal{M} \in \Delta(\ell, m)$. We will show by finite induction on $i (0 \le i \le \ell)$ that $a_{\mathcal{M}} = 0$ for all $\mathcal{M} \in \Delta_i(\ell, m)$. First, by specializing all the variables to zero (i.e., by substituting $X_{rs} = 0$ for all $r \in \{1, \ldots, \ell\}$ and $s \in \{1 \ldots, \ell'\}$ in the linear dependence relation), we see that the desired assertion holds when $i = 0$. Next, suppose $i > 0$ and $a_{\mathcal{M}} = 0$ for all $\mathcal{M} \in \Delta_j(\ell, m)$ and all $j < i$. Pick a minor $\mathcal{M} \in \Delta_i(\ell, m)$. By specializing all the variables except the ones occurring in $\mathcal{M}$ to zero, we obtain $a_{\mathcal{M}} = 0$. Repeating this procedure for each $i \times i$ minor, we obtain the induction step. This proves that the elements of $\Delta(\ell, m)$ are linearly independent. Consequently, $\dim_{\mathbb{F}_q} \mathcal{F}(\ell, m) = \#\Delta(\ell, m) = \binom{m}{\ell}$. ∎

Thanks to Lemma 3, every element of $\mathcal{F}(\ell, m)$ is a unique $\mathbb{F}_q$-linear combination of the elements of $\Delta(\ell, m)$. With this in view, we make the following definition.

Definition 4: Given $f = \sum_{\mathcal{M} \in \Delta(\ell,m)} a_{\mathcal{M}} \mathcal{M} \in \mathcal{F}(\ell, m)$, where $a_{\mathcal{M}} \in \mathbb{F}_q$ for every $\mathcal{M} \in \mathcal{F}(\ell, m)$, the support of f is the set

$$\operatorname{supp}(f) := \{\mathcal{M} \in \Delta(\ell, m) : a_{\mathcal{M}} \neq 0\}.$$

Note that the support of f is the empty set if and only if f is the zero polynomial.

We shall denote the space of all $\ell \times \ell'$ matrices with entries in $\mathbb{F}_q$ by $\mathbb{A}^\delta(\mathbb{F}_q)$, or simply by $\mathbb{A}^\delta$. Indeed, for fixed positive integers ℓ and ℓ', this space can be readily identified with the δ-dimensional affine space over $\mathbb{F}_q$, where $\delta = \ell\ell'$, as before. It is clear that for any $f \in \mathbb{F}_q[X]$ (and in particular, any $f \in \mathcal{F}(\ell, m)$) and $P \in \mathbb{A}^\delta$, the element $f(P)$ of $\mathbb{F}_q$ is well-defined. Now let us fix an enumeration $P_1, P_2, \ldots, P_{q^\delta}$ of $\mathbb{A}^\delta$.

Definition 5: The evaluation map of $\mathbb{F}_q[X]$ is the map

$$\mathrm{Ev} : \mathbb{F}_q[X] \to \mathbb{F}_q^{q^\delta}$$

defined by

$$\mathrm{Ev}(f) := \big(f(P_1), \ldots, f(P_{q^\delta})\big).$$

It is clear that the evaluation map Ev defined above is a surjective linear map. Also, it is well-known that the kernel of Ev is the ideal of $\mathbb{F}_q[X]$ generated by $\{X_{ij}^q - X_{ij} : 1 \le i \le \ell,\ 1 \le j \le \ell'\}$, and that this kernel contains no nonzero polynomial having degree $< q$ in each of the variables. (See, for example, [10, p. 11].) In particular, if $0 \neq f \in \mathcal{F}(\ell, m)$, then f cannot be in the kernel of Ev because $\deg_{X_{ij}}(f) \le 1$ for each variable X_{ij}. Thus the restriction of the evaluation map Ev to $\mathcal{F}(\ell, m)$ is injective. We are now ready to define the codes that are studied in the remainder of this paper.

Definition 6: The affine Grassmann code $C^{\mathbb{A}}(\ell, m)$ is the image of $\mathcal{F}(\ell, m)$ under the evaluation map Ev. The minimum distance of $C^{\mathbb{A}}(\ell, m) := \mathrm{Ev}(\mathcal{F}(\ell, m))$ will be denoted by $d(\ell, m)$.

Recall that a code C is said to be *degenerate* if there exists a coordinate position i such that $c_i = 0$ for all $c \in C$. It turns out that affine Grassmann codes are nondegenerate and their length and dimension are easily determined.

Lemma 7: The affine Grassmann code $C^{\mathbb{A}}(\ell, m)$ is a nondegenerate linear code of length q^δ and dimension $\binom{m}{\ell}$.

Proof: It is obvious that $C^{\mathbb{A}}(\ell, m)$ is a linear code of length $q^\delta = \#\mathbb{A}^\delta(\mathbb{F}_q)$. Moreover, since the constant polynomial 1, being the only element of $\Delta_0(\ell, m)$, is in $\mathcal{F}(\ell, m)$, and since $\mathrm{Ev}(1) = (1, \ldots, 1)$, it follows that $C^{\mathbb{A}}(\ell, m)$ is nondegenerate. Finally, since the evaluation map is injective on $\mathcal{F}(\ell, m)$, it follows from Lemma 3 that the dimension of $C^{\mathbb{A}}(\ell, m)$ is $\binom{m}{\ell}$. ∎

Example 8: Suppose $\ell = \ell' = 2$ and $q = 2$. Then $m = \delta = 4$ and the elements of $\mathcal{F}(2, 4)$ are of the form (1). The affine space $\mathbb{A}^\delta$ consists of the 2×2 matrices with entries in $\mathbb{F}_2 = \{0, 1\}$. There are 16 such matrices and, upon letting e_{ij} denote the 2×2 matrix with 1 in $(i, j)^{\text{th}}$ position and 0 elsewhere, $\mathbb{A}^\delta(\mathbb{F}_2)$ may be enumerated as $\mathbf{0}$, e_{11}, e_{12}, e_{21}, e_{22}, $e_{11} + e_{12}$, $e_{11}+e_{21}$, $e_{11}+e_{22}$, $e_{12}+e_{21}$, $e_{12}+e_{22}$, $e_{21}+e_{22}$, $e_{11}+e_{12}+e_{21}$, $e_{11}+e_{12}+e_{22}$, $e_{11}+e_{21}+e_{22}$, $e_{12}+e_{21}+e_{22}$, $e_{11}+e_{12}+e_{21}+e_{22}$, where $\mathbf{0}$ denotes the 2×2 zero matrix. Accordingly, the codewords of $C^{\mathbb{A}}(2, 4)$ consist of the elements of $\mathbb{F}_2^{16}$ of the form $a\mathbf{1} + \mathbf{v}$, where $\mathbf{1}$ denotes the 16-tuple all of whose coordinates are 1, whereas $\mathbf{v}$ denotes the 16-tuple given by $(0,\ b_1,\ b_2,\ b_3,\ b_4,\ b_1+b_2,\ b_1+b_3, b_1+b_4+c,\ b_2+b_3+c,\ b_2+b_4,\ b_3+b_4, b_1+b_2+b_3+c,\ b_1+b_2+b_4+$

$c,\ b_1+b_3+b_4+c, b_2+b_3+b_4+c,\ b_1+b_2+b_3+b_4)$. Here a, b_1, b_2, b_3, b_4, c vary over $\mathbb{F}_2$. As such, there are $2^6 = 64$ codewords, and it is clear that the code is nondegenerate and its dimension is 6; indeed, a $\mathbb{F}_2$-basis of $C^{\mathbb{A}}(2,4)$ is obtained by setting exactly one of a, b_1, b_2, b_3, b_4, c to be 1 and the others to be 0. Further, by listing the 64 codewords, it is easily seen that every nonzero codeword is of (Hamming) weight ≥ 6, and the codeword corresponding $a = b_1 = b_2 = b_3 = b_4 = 0$ and $c = 1$ is of weight 6. Thus, at least in the binary case, $C^{\mathbb{A}}(2,4)$ is a $[16, 6, 6]$-code.

We end this section by giving two lemmas on determinants that will be useful in the sequel.

Lemma 9: Let $Y = (Y_{ij})$ be a $\ell \times \ell$ matrix whose entries are independent indeterminates over $\mathbb{F}_q$ and let $B = (b_{ij})$ be a $\ell \times \ell$ matrix with entries in $\mathbb{F}_q$. Then there exists $h \in \mathcal{F}(\ell, 2\ell)$ such that

$$\det(Y+B) = \det(Y) + \sum_{1 \leq i,j \leq \ell} (-1)^{i+j} b_{ij} \det(Y^{ij}) + h,$$

with $\operatorname{supp}(h) \subseteq \bigcup_{i=0}^{\ell-2} \Delta_i(\ell, 2\ell)$ and where Y^{ij} denotes the $(\ell-1) \times (\ell-1)$ matrix obtained from Y by deleting the ith row and the jth column.

Proof: For a subset S of $\{1, \ldots, \ell\}$, denote by $(Y, B)_S$ the matrix obtained from Y by replacing for all $j \in S$, the jth column of Y by the jth column of B. By the multilinearity of the determinant, we readily see that

$$\det(Y+B) = \sum_S \det((Y,B)_S),$$

where the sum is over all subsets S of $\{1, \ldots, \ell\}$. Observe that if S is the empty set, then $\det((Y,B)_S) = \det(Y)$. Moreover, if S is singleton, say $S = \{j\}$, where $1 \leq j \leq \ell$, then by developing the determinant along the jth column we find that

$$\det((Y,B)_S) = \sum_{i=1}^{\ell} (-1)^{i+j} b_{ij} \det(Y^{ij}).$$

Finally, if $S \subseteq \{1, \ldots, \ell\}$ with $\#S = s \geq 2$, then using Laplace expansion along the columns indexed by the elements of S, we see that $\det((Y,B)_S)$ is a $\mathbb{F}_q$-linear combination of minors in $\Delta_{\ell-s}(\ell, 2\ell)$. This yields the desired result. ∎

We will also need the following well-known result whose proof can be found, for example, in [4, Ch. I, Sec. 2].

Lemma 10 (Cauchy-Binet): Let r and s be positive integers such that $r \leq s$, and let A be a $r \times s$ matrix and B a $s \times r$ matrix with entries in a commutative ring. For a subset I of $\{1, \ldots, s\}$ with $\#I = r$, denote by A^I the $r \times r$ submatrix of A formed by the jth columns of A for $j \in I$, and denote by B_I the $r \times r$ submatrix of B formed by the ith rows of B for $i \in I$. Then

$$\det(AB) = \sum_I \det(A^I) \det(B_I),$$

where the sum is over all subsets I of $\{1, \ldots, s\}$ of cardinality r.

Remark 11: As a warm-up for the results of the subsequent section, let us consider the case of $\ell = 1$ even though it is rather trivial. Here $\mathcal{F}(1,m)$ corresponds to the space of linear polynomials in ℓ' variables of the form $h = a_0 + a_1 X_{11} + \cdots + a_{\ell'} X_{1\ell'}$. For any such h, the Hamming weight of the corresponding codeword $\mathrm{Ev}(h)$ amounts to finding the number of $\mathbb{F}_q$-rational points on a hyperplane in $\mathbb{A}^{\ell'}$. Indeed, assuming that $\mathrm{Ev}(h)$ is nonzero, or equivalently that not all $a_0, a_1, \ldots, a_{\ell'}$ are zero, it is readily seen that

$$\begin{aligned} \mathrm{w_H}(\mathrm{Ev}(h)) &= \#\mathbb{A}^{\ell'}(\mathbb{F}_q) - \#H \\ &= \begin{cases} q^{\ell'} & \text{if } a_1 = \cdots = a_{\ell'} = 0, \\ q^{\ell'} - q^{\ell'-1} & \text{otherwise,} \end{cases} \end{aligned}$$

where H denotes the affine hyperplane $\{P \in \mathbb{A}^{\ell'}(\mathbb{F}_q) : h(P) = 0\}$. It follows that the minimum distance of $C^{\mathbb{A}}(1,m)$ is $q^{\ell'-1}(q-1)$, and also that the number of minimum weight codewords is $(q^{\ell'+1} - q)$. In a similar manner, the general case corresponds to finding the maximum number of points on a "determinantal hyperplane", i.e., the zero-set of an arbitrary nonzero element of $\mathcal{F}(\ell, m)$, and finding the minimum weight codewords corresponds to finding those determinantal hyperplanes where the maximum is attained.

III. Minimum Distance

In this section we will compute the minimum distance $d(\ell, m)$ of the affine Grassmann code $C^{\mathbb{A}}(\ell, m)$. We start by determining the Hamming weight of a maximal minor, obtaining thereby an upper bound for $d(\ell, m)$. As usual we denote by $\mathrm{w_H}(c)$ the Hamming weight of a codeword c.

Lemma 12: Let $\mathcal{M} \in \Delta_\ell(\ell, m)$. Then

$$\mathrm{w_H}(\mathrm{Ev}(\mathcal{M})) = q^{\delta - \ell^2} \prod_{i=0}^{\ell-1} (q^\ell - q^i).$$

In particular

$$d(\ell, m) \leq q^{\delta - \ell^2} \prod_{i=0}^{\ell-1} (q^\ell - q^i).$$

Proof: Without loss of generality we shall assume that $\mathcal{M}$ is the leading maximal minor, i.e., $\mathcal{M} = \det((X_{ij})_{1 \leq i,j \leq \ell})$. Let $P \in \mathbb{A}^\delta(\mathbb{F}_q)$ and let $(p_{ij})_{1 \leq i \leq \ell,\ 1 \leq j \leq \ell'}$ be the $\ell \times \ell'$ matrix with entries in $\mathbb{F}_q$ corresponding to P. It is clear that $\mathcal{M}(P) \neq 0$ if and only if the $\ell \times \ell$ submatrix $(p_{ij})_{1 \leq i,j \leq \ell}$ is nonsingular. This happens for exactly $\prod_{i=0}^{\ell-1}(q^\ell - q^i)$ values of p_{ij} with $1 \leq i, j \leq \ell$. The remaining $\ell\ell' - \ell^2$ values p_{ij} with $j > \ell$ do not play any role in the evaluation of $\mathcal{M}$ at P. Hence $\mathrm{w_H}(\mathrm{Ev}(\mathcal{M})) = q^{(\delta-\ell^2)} \prod_{i=0}^{\ell-1}(q^\ell - q^i)$. This implies the desired inequality for $d(\ell, m)$. ∎

We will show that the upper bound for $d(\ell, m)$ in the above lemma gives, in fact, the true minimum distance. To this end, the specialization maps defined below will be useful.

Definition 13: Let i, j be integers satisfying $1 \leq i \leq \ell$ and $1 \leq j \leq \ell'$, and let $\mathbf{a} = (a_1, \ldots, a_{\ell'}) \in \mathbb{F}_q^{\ell'}$ and $\mathbf{b} = (b_1, \ldots, b_\ell) \in \mathbb{F}_q^{\ell}$. The row-wise specialization map relative to $\mathbf{a}$ and i is the map

$$s_{\mathbf{a}}^{(i)} : \mathcal{F}(\ell, m) \to \mathcal{F}(\ell - 1, m - 1)$$

defined by

$$s_{\mathbf{a}}^{(i)}(f) := f\,|_{\mathbf{X}_i=\mathbf{a}},$$

i.e., $s_{\mathbf{a}}^{(i)}(f)$ is the element of $\mathcal{F}(\ell-1,m-1)$ obtained by substituting $(X_{i1},\ldots,X_{i\ell'})=(a_1,\ldots,a_{\ell'})$ in $f(X_{11},\ldots,X_{\ell\ell'})$. Further, if $\ell'>\ell$, then the column-wise specialization map relative to $\mathbf{b}$ and j is the map

$$t_{\mathbf{b}}^{(j)} : \mathcal{F}(\ell,m) \to \mathcal{F}(\ell,m-1)$$

defined by

$$t_{\mathbf{b}}^{(j)}(f) := f\,|_{\mathbf{X}^j=\mathbf{b}},$$

i.e., $t_{\mathbf{b}}^{(j)}(f)$ is the element of $\mathcal{F}(\ell,m-1)$ obtained by substituting $(X_{1j},\ldots,X_{\ell j})=(b_1,\ldots,b_\ell)$ in f. It may be noted that $s_{\mathbf{a}}^{(i)}$ and $t_{\mathbf{b}}^{(j)}$ are $\mathbb{F}_q$-linear maps.

Lemma 14: Let $f\in\mathcal{F}(\ell,m)$ and let i,j be integers satisfying $1\le i\le\ell$ and $1\le j\le\ell'$. Then

$$\mathrm{w_H}(\mathrm{Ev}(f)) = \sum_{\mathbf{a}\in\mathbb{F}_q^{\ell'}} \mathrm{w_H}\big(\mathrm{Ev}(s_{\mathbf{a}}^{(i)}(f))\big). \tag{2}$$

Moreover, if $\ell'>\ell$, then

$$\mathrm{w_H}(\mathrm{Ev}(f)) = \sum_{\mathbf{b}\in\mathbb{F}_q^{\ell}} \mathrm{w_H}\big(\mathrm{Ev}(t_{\mathbf{b}}^{(j)}(f))\big). \tag{3}$$

Proof: Given any $\mathbf{a}\in\mathbb{F}_q^{\ell'}$, the specialization $s_{\mathbf{a}}^{(i)}(f)$ is in $\mathcal{F}(\ell-1,m-1)$ and hence the codeword $\mathrm{Ev}(s_{\mathbf{a}}^{(i)}(f))$ has $q^{\delta-\ell'}$ coordinates; each of these coordinates can be computed by evaluating f at those points $P=(p_{ij})$ of $\mathbb{A}^\delta(\mathbb{F}_q)$ satisfying $(p_{i1},\ldots,p_{i\ell'})=\mathbf{a}$. As $\mathbf{a}$ varies over $\mathbb{F}_q^{\ell'}$, all the q^δ coordinates of $\mathrm{Ev}(f)$ will be accounted for. Thus the codeword $\mathrm{Ev}(f)$ can be partitioned into shorter codewords $\mathrm{Ev}(s_{\mathbf{a}}^{(i)}(f))$, $\mathbf{a}\in\mathbb{F}_q^{\ell'}$. This implies (2). The proof of (3) is similar. ∎

We shall now consider the special case $\ell=\ell'$, i.e., $m=2\ell$. In this case, X has a unique maximal minor and whenever it occurs in a polynomial in $\mathcal{F}(\ell,2\ell)$, all the submaximal minors occurring in that polynomial can be killed by a translation.

Lemma 15: Let $f\in\mathcal{F}(\ell,2\ell)$ be such that $\det(X)\in\mathrm{supp}(f)$ and the coefficient of $\det(X)$ in f equals 1. Then there exists a unique $\ell\times\ell$ matrix A with entries in $\mathbb{F}_q$ such that

$$f=\det(X+A)+h,$$

where $h\in\mathcal{F}(\ell,2\ell)$ with $\mathrm{supp}(h)\subseteq\bigcup_{i=0}^{\ell-2}\Delta_i(\ell,2\ell)$.

Proof: If $\ell=1$, then the desired result holds trivially with $h=0$. Assume that $\ell\ge 2$. For $1\le i,j\le\ell$, let X^{ij} denote the $(\ell-1)\times(\ell-1)$ submatrix of X obtained by deleting the ith row and the jth column, and let b_{ij} denote the coefficient of $\det(X^{ij})$ in f. Then there is $h_1\in\mathcal{F}(\ell,2\ell)$ such that

$$f=\det(X)+\sum_{1\le i,j\le\ell} b_{ij}\det(X^{ij})+h_1$$

and

$$\mathrm{supp}(h_1)\subseteq\bigcup_{i=0}^{\ell-2}\Delta_i(\ell,2\ell).$$

Now define $a_{ij}=(-1)^{i+j}b_{ij}$ for $1\le i,j\le\ell$ and let A denote the $\ell\times\ell$ matrix $(a_{ij})_{1\le i,j\le\ell}$. By Lemma 9, there is $h_2\in\mathcal{F}(\ell,2\ell)$ such that

$$\det(X+A)=\det(X)+\sum_{1\le i,j\le\ell} b_{ij}X^{ij}+h_2$$

and

$$\mathrm{supp}(h_2)\subseteq\bigcup_{i=0}^{\ell-2}\Delta_i(\ell,2\ell).$$

Thus $f=\det(X+A)+h$, where $h:=h_1-h_2$, and we have the desired result. ∎

We are now ready to prove the main result of this section.

Theorem 16: The minimum distance $d(\ell,m)$ of the code $C^{\mathbb{A}}(\ell,m)$ is given by

$$d(\ell,m)=q^{\delta-\ell^2}\prod_{i=0}^{\ell-1}(q^\ell-q^i). \tag{4}$$

Proof: We prove the theorem by induction on m. Note that $m\ge 2$ since $1\le\ell\le\ell'$. If $m=2$, then $\ell=\ell'=1$ and $\delta=1$, and so (4) follows from the observations in Remark 11 in this case. Now suppose $m>2$ and the theorem is true for all codes $C^{\mathbb{A}}(\ell,m-1)$, with $1\le\ell\le\lfloor(m-1)/2\rfloor$. We will prove (4) by considering separately the cases $\ell<\ell'$ and $\ell=\ell'$.

Case 1: $\ell<\ell'$. Let $f\in\mathcal{F}(\ell,m)$ and suppose $f\neq 0$. Then $\mathrm{supp}(f)$ is nonempty. Choose a minor $\mathcal{M}\in\mathrm{supp}(f)$ of the maximum possible order, say r, in the sense that $\mathcal{M}\in\Delta_r(\ell,m)$ and $\Delta_s(\ell,m)\cap\mathrm{supp}(f)=\emptyset$ for all $s>r$. Since $r\le\ell<\ell'$, there exists a column $\mathbf{X}^j$ of X such that the variables $X_{1j},\ldots,X_{\ell j}$ do not occur in $\mathcal{M}$. In particular, $t_{\mathbf{b}}^{(j)}(\mathcal{M})=\mathcal{M}$ for any $\mathbf{b}\in\mathbb{F}_q^\ell$. Since $\mathcal{M}$ is of maximum order in $\mathrm{supp}(f)$, this implies that $t_{\mathbf{b}}^{(j)}(f)$ is not the zero polynomial and therefore the codeword $\mathrm{Ev}(t_{\mathbf{b}}^{(j)}(f))$ is nonzero for any $\mathbf{b}\in\mathbb{F}_q^\ell$. Consequently, by Lemma 14 and the induction hypothesis, we see that

$$\begin{aligned}\mathrm{w_H}(\mathrm{Ev}(f)) &= \sum_{\mathbf{b}\in\mathbb{F}_q^\ell}\mathrm{w_H}(\mathrm{Ev}(t_{\mathbf{b}}^{(j)}(f)))\\ &\ge q^\ell d(\ell,m-1)\\ &= q^\ell q^{(\ell'-1)\ell-\ell^2}\prod_{i=0}^{\ell-1}(q^\ell-q^i)\\ &= q^{\delta-\ell^2}\prod_{i=0}^{\ell-1}(q^\ell-q^i).\end{aligned}$$

Since the above holds for any nonzero $f\in\mathcal{F}(\ell,m)$, we obtain

$$d(\ell,m)\ge q^{\delta-\ell^2}\prod_{i=0}^{\ell-1}(q^\ell-q^i).$$

This inequality together with Lemma 12 establishes the induction step.

Case 2: $\ell = \ell'$. In this case $m = 2\ell$ and X has only one $\ell \times \ell$ minor, namely $\mathcal{L} := \det(X)$. Let $f \in \mathcal{F}(\ell, 2\ell)$ be a nonzero polynomial. We will distinguish two subcases depending on whether or not the $\ell \times \ell$ minor $\mathcal{L}$ occurs in f.

Subcase 1: $\mathcal{L} \notin \operatorname{supp}(f)$. In this event, by a similar reasoning as in Case 1, there exists a row, say the ith row, such that $s_{\mathbf{a}}^{(i)}(f) \neq 0$ for all $\mathbf{a} \in \mathbb{F}_q^{\ell}$. Consequently, by Lemma 14 and the induction hypothesis, we see that

$$\begin{aligned}\mathrm{w_H}(\mathrm{Ev}(f)) &= \sum_{\mathbf{a}\in\mathbb{F}_q^{\ell}} \mathrm{w_H}(\mathrm{Ev}(s_{\mathbf{a}}^{(i)}(f))) \\ &\geq q^{\ell} d(\ell-1, 2\ell-1) \\ &= q^{\ell} q^{(\ell-1)\ell-(\ell-1)^2} \prod_{i=0}^{\ell-2} (q^{\ell-1} - q^i) \\ &= q^{\ell} \prod_{i=0}^{\ell-2} (q^{\ell} - q^{i+1}) \\ &> \prod_{i=0}^{\ell-1} (q^{\ell} - q^i).\end{aligned}$$

Thus from Lemma 12, we conclude that $\mathrm{Ev}(f)$ cannot be a minimum weight codeword of $C^{\mathbb{A}}(\ell, m)$ if $\det(X) \notin \operatorname{supp}(f)$.

Subcase 2: $\mathcal{L} \in \operatorname{supp}(f)$. In this event, by Lemma 15 there exists a $\ell \times \ell$ matrix A with entries in $\mathbb{F}_q$ such that $f = \det(X+A) + h$, where h is a $\mathbb{F}_q$-linear combination of $i \times i$ minors of X with $0 \leq i \leq \ell - 2$. If $h = 0$, then $f = \det(X + A)$ and since $\mathrm{Ev}(f)$ is obtained by evaluating f at all points of $\mathbb{A}^{\delta}(\mathbb{F}_q)$, we see that $\mathrm{w_H}(\mathrm{Ev}(\det(X+A))) = \mathrm{w_H}(\mathrm{Ev}(\det(X)))$; hence, by Lemma 12, we then find that $\mathrm{w_H}(\mathrm{Ev}(\det(X+A))) = \prod_{i=0}^{\ell-1}(q^{\ell} - q^i)$. Now suppose $h \neq 0$. Then $\ell \geq 2$ and as in Case 1, we can choose a minor $\mathcal{M} \in \operatorname{supp}(h)$ of maximum order, say r with $r \leq \ell - 2$, and find an integer i with $1 \leq i \leq \ell$ such that $s_{\mathbf{a}}^{(i)}(\mathcal{M}) = \mathcal{M}$ for all $\mathbf{a} \in \mathbb{F}_q^{\ell}$. Since $\mathcal{M}$ is of maximum order in $\operatorname{supp}(h)$, we see that $s_{\mathbf{a}}^{(i)}(h) \neq 0$ for all $\mathbf{a} \in \mathbb{F}_q^{\ell}$. Also, since $r \leq \ell - 2$, the nonzero polynomial $s_{\mathbf{a}}^{(i)}(h)$ is of (total) degree at most $\ell - 2$. On the other hand, by developing the resulting determinant along the ith row, we see that $s_{\mathbf{a}}^{(i)}(\det(X + A))$ is either the zero polynomial or a nonzero polynomial in $\mathbb{F}_q[X]$ of degree $\ell - 1$. It follows that $s_{\mathbf{a}}^{(i)}(f) \neq 0$ for all $\mathbf{a} \in \mathbb{F}_q^{\ell}$. Now, proceeding as in Subcase 1, we see that $\mathrm{w_H}(\mathrm{Ev}(f)) > \prod_{i=0}^{\ell-1}(q^{\ell} - q^i)$, and so from Lemma 12 we conclude that $\mathrm{Ev}(f)$ cannot be a minimum weight codeword.

Thus we have shown that $d(\ell, 2\ell) = \prod_{i=0}^{\ell-1}(q^{\ell} - q^i)$ and, therefore, established the induction step in Case 2. This completes the proof. ∎

Using the q-factorial function $[d]_q! := \prod_{i=1}^{d}(q^i - 1)$, the formula (4) for the minimum distance of $C^{\mathbb{A}}(\ell, m)$ can be more compactly written as follows:

$$d(\ell, m) = q^{\delta - \binom{\ell+1}{2}} [\ell]_q!. \tag{5}$$

Note that if $\ell = 1$, then (4) as well as (5) for $d(\ell, m)$ is in agreement with the observations in Remark 11.

Remark 17: By analyzing the proof of Theorem 16 in greater detail, one can show that if $\ell = \ell'$, then the minimum weight codewords of $C^{\mathbb{A}}(\ell, m)$ arise precisely from nonzero constant multiples of translates of the unique maximal minor, i.e., from polynomials of the form $\lambda \det(X + A)$, with $0 \neq \lambda \in \mathbb{F}_q$ and A a $\ell \times \ell$ matrix with entries in $\mathbb{F}_q$. Consequently, the number of minimum weight codewords in $C^{\mathbb{A}}(\ell, 2\ell)$ is equal to $(q - 1)q^{\ell^2}$. A more general version of these results will be proved in Sections V and VI.

IV. Automorphisms

Recall that the *(permutation) automorphism group* $\mathrm{Aut}(C)$ of a code $C \subseteq \mathbb{F}_q^n$ is the set of all permutations σ of $\{1, \ldots, n\}$ such that $(c_{\sigma(1)}, \ldots, c_{\sigma(n)}) \in C$ for all $c = (c_1, \ldots, c_n) \in C$. Evidently, $\mathrm{Aut}(C)$ is a subgroup of the symmetric group on $\{1, \ldots, n\}$. In this section, we shall show that the automorphism groups of affine Grassmann codes are large; more precisely, we shall show that $\mathrm{Aut}\left(C^{\mathbb{A}}(\ell, m)\right)$ contains a subgroup of order

$$q^{\delta} \prod_{i=0}^{\ell-1}(q^{\ell} - q^i) = n \prod_{i=0}^{\ell-1}(q^{\ell} - q^i) = q^{\ell^2} d(\ell, m) \tag{6}$$

where n and $d(\ell, m)$ denote the length and the minimum distance of $C^{\mathbb{A}}(\ell, m)$.

Denote, as usual, by $\mathrm{GL}_r(\mathbb{F}_q)$ the set of all invertible $r \times r$ matrices with entries in $\mathbb{F}_q$ and by $M_{r\times s}(\mathbb{F}_q)$ the set of all $r \times s$ matrices with entries in $\mathbb{F}_q$. Let $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ and $\mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)$. Define

$$\phi_{\mathbf{u},A} : \mathbb{A}^{\delta}(\mathbb{F}_q) \to \mathbb{A}^{\delta}(\mathbb{F}_q)$$

to be the affine transformation given by

$$\begin{aligned}\phi_{\mathbf{u},A}(P) &= PA^{-1} + \mathbf{u} \quad \text{for} \\ P &= (p_{ij})_{1\leq i\leq \ell,\, 1\leq j\leq \ell'} \in \mathbb{A}^{\delta}(\mathbb{F}_q).\end{aligned}$$

It is clear that the transformation $\phi_{\mathbf{u},A}$ gives a bijection of $\mathbb{A}^{\delta} = \mathbb{A}^{\delta}(\mathbb{F}_q)$ onto itself, and hence $\left(f(\phi_{\mathbf{u},A}(P))\right)_{P\in\mathbb{A}^{\delta}}$ will be a permutation of $(f(P))_{P\in\mathbb{A}^{\delta}}$ for any $f \in \mathbb{F}_q[X]$; we shall denote this permutation $\sigma_{\mathbf{u},A}$.

Lemma 18: Let $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ and $\mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)$. Then $\sigma_{\mathbf{u},A} \in \mathrm{Aut}\left(C^{\mathbb{A}}(\ell, m)\right)$.

Proof: Let r be any integer with $0 \leq r \leq \ell$. In view of Lemma 9, a $r \times r$ minor of $XA^{-1} + \mathbf{u}$ is a $\mathbb{F}_q$-linear combination of $i \times i$ minors of X, where $0 \leq i \leq r$. Consequently, if $f = f(X) \in \mathcal{F}(\ell, m)$, then $f(XA^{-1} + \mathbf{u}) \in \mathcal{F}(\ell, m)$. Moreover

$$\begin{aligned}\sigma_{\mathbf{u},A}(\mathrm{Ev}(f)) &= \left(f(\phi_{\mathbf{u},A}(P))\right)_{P\in\mathbb{A}^{\delta}(\mathbb{F}_q)} \\ &= \mathrm{Ev}\left(f(XA^{-1} + \mathbf{u})\right).\end{aligned}$$

It follows that $\sigma_{\mathbf{u},A} \in \mathrm{Aut}(C)$, where $C = C^{\mathbb{A}}(\ell, m) = \mathrm{Ev}(\mathcal{F}(\ell, m))$. ∎

Observe that $\phi_{\mathbf{0},I}$ is the identity transformation of $\mathbb{A}^{\delta}$, where $\mathbf{0}$ denotes the zero matrix in $M_{\ell\times\ell'}(\mathbb{F}_q)$ and I the identity matrix

in $\mathrm{GL}_{\ell'}(\mathbb{F}_q)$. Moreover, given any $A, B \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ and $\mathbf{u}, \mathbf{v} \in M_{\ell\times\ell'}(\mathbb{F}_q)$, we have

$$\phi_{\mathbf{u},A} \circ \phi_{\mathbf{v},B} = \phi_{\mathbf{w},AB} \quad \text{and} \quad \phi_{\mathbf{u},A}^{-1} = \phi_{\mathbf{u}',A^{-1}} \tag{7}$$

where $\mathbf{w} := \mathbf{v}A^{-1} + \mathbf{u}$ and $\mathbf{u}' = -\mathbf{u}A$. This leads to the following observation-cum-definition.

Definition 19: The set $\{\phi_{\mathbf{u},A} : A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q) \text{ and } \mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)\}$ forms a group with respect to composition of maps and this group will be denoted by $\mathfrak{G}(\ell, m)$.

We determine the group structure of $\mathfrak{G}(\ell, m)$ in the following proposition.

Proposition 20: As a group $\mathfrak{G}(\ell, m)$ is isomorphic to the semidirect product $M_{\ell\times\ell'}(\mathbb{F}_q) \rtimes_\theta \mathrm{GL}_{\ell'}(\mathbb{F}_q)$, where the homomorphism $\theta : GL_{\ell'}(\mathbb{F}_q) \to Aut(M_{\ell\times\ell'}(\mathbb{F}_q))$ is defined by $\theta(A)(B) := BA^{-1}$.

Proof: Recall that if G and H are any groups, and if $\theta : H \to \mathrm{Aut}(G)$ is any group homomorphism, then the semidirect product $G \rtimes_\theta H$ of G and H relative to θ is the group whose underlying set is $G \times H$ and whose group operation is defined by $(g, h)(g', h') = (g\theta(h)(g'),\ hh')$. In our case, G is the additive group $M_{\ell\times\ell'}(\mathbb{F}_q)$ and H is the multiplicative group $\mathrm{GL}_{\ell'}(\mathbb{F}_q)$, while $\theta : H \to \mathrm{Aut}(G)$ is given by $\theta(A)(\mathbf{u}) := \mathbf{u}A^{-1}$. Now observe that $\theta(A) \in \mathrm{Aut}(G)$ for all $A \in H$ and $\theta(A_1A_2) = \theta(A_1)\theta(A_2)$ for all $A_1, A_2 \in H$. So θ is indeed a homomorphism of H into $\mathrm{Aut}(G)$. Moreover, in view of (7), the group operation $(\mathbf{u}, A)(\mathbf{v}, B) = \left(\mathbf{u} + \mathbf{v}A^{-1}, AB\right)$ in $G \rtimes_\theta H$ is consistent with the group operation in $\mathfrak{G}(\ell, m)$. Thus $(\mathbf{u}, A) \mapsto \phi_{\mathbf{u},A}$ gives an isomorphism of $M_{\ell\times\ell'}(\mathbb{F}_q) \rtimes_\theta GL_{\ell'}(\mathbb{F}_q)$ onto $\mathfrak{G}(\ell, m)$. ∎

Theorem 21: The automorphism group of the affine Grassmann code $C^{\mathbb{A}}(\ell, m)$ contains a subgroup isomorphic to $\mathfrak{G}(\ell, m)$. In particular, $\#\mathrm{Aut}\left(C^{\mathbb{A}}(\ell, m)\right)$ is greater than or equal to the quantity in (6).

Proof: In view of Lemma 18, $\phi_{\mathbf{u},A} \mapsto \sigma_{\mathbf{u},A}$ gives a natural map from $\mathfrak{G}(\ell, m)$ into $\mathrm{Aut}\left(C^{\mathbb{A}}(\ell, m)\right)$. It is readily seen that this map is a group homomorphism. So it suffices to show that this homomorphism is injective. To this end, suppose $\sigma_{\mathbf{u},A}$ is the identity permutation for some $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ and $\mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)$. Then $\sigma_{\mathbf{u},A}(\mathrm{Ev}(f)) = \mathrm{Ev}(f)$ for all $f \in \mathcal{F}(\ell, m)$, i.e.

$$f(PA^{-1} + \mathbf{u}) = f(P)$$

for all $f \in \mathcal{F}(\ell, m)$ and all $P \in \mathbb{A}^\delta(\mathbb{F}_q)$. By choosing P to be the zero matrix and letting f vary over all possible 1×1 minors, we find that $\mathbf{u} = 0$. Further, by choosing $P = e_{ij}$, i.e., P to be the $\ell \times \ell'$ matrix with 1 in (i, j)th position and 0 elsewhere, and again letting f vary over all possible 1×1 minors, we see that A^{-1} is the identity matrix I. Hence $A = I$. ∎

We leave the question of the complete determination of the automorphism group $\mathrm{Aut}(C^{\mathbb{A}}(\ell, m))$ open for future investigation.

V. Characterization of Minimum Weight Codewords

In Section III, we have calculated the minimum distance $d(\ell, m)$ of the affine Grassmann code $C^{\mathbb{A}}(\ell, m)$. In this section, we will give an explicit characterization of all of its codewords of weight $d(\ell, m)$. One of the tools utilized will be a concept involving the specialization function $s_{\mathbf{a}}^{(i)}$ from Definition 13, which is defined later.

Definition 22: Let $f \in \mathcal{F}(\ell, m)$ and let i be an integer between 1 and ℓ. The ith row-vanishing locus of f is the set

$$V_f^{(i)} := \{\mathbf{a} \in \mathbb{F}_q^{\ell'} : s_{\mathbf{a}}^{(i)}(f) = 0\}.$$

It turns out that if a polynomial in $\mathcal{F}(\ell, m)$ is changed by a translation of the underlying matrix X to $X + \mathbf{u}$, then its ith row-vanishing locus is a translate of the corresponding locus of the transformed polynomial by the ith row of $\mathbf{u}$.

Lemma 23: Let $f \in \mathcal{F}(\ell, m)$ and let i be an integer between 1 and ℓ. Then

$$V_f^{(i)} = \mathbf{u}_i + V_{\phi_{\mathbf{u},I}(f)}^{(i)} \quad \text{for every } \mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)$$

where I denotes the identity matrix in $\mathrm{GL}_{\ell'}(\mathbb{F}_q)$.

Proof: Let $\mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)$ and let $g := \phi_{\mathbf{u},I}(f)$. Suppose $\mathbf{a} \in V_f^{(i)}$. Define $\mathbf{b} \in \mathbb{F}_q^{\ell'}$ by the relation $\mathbf{a} = \mathbf{u}_i + \mathbf{b}$. Note that

$$s_{\mathbf{b}}^{(i)}(g) = g(X)|_{\mathbf{X}_i=\mathbf{b}} = f(X + \mathbf{u})|_{\mathbf{X}_i=\mathbf{b}}. \tag{8}$$

Now $s_{\mathbf{a}}^{(i)}(f) = f|_{\mathbf{X}_i=\mathbf{a}} = 0$. In particular, the polynomial $f|_{\mathbf{X}_i=\mathbf{a}}$ evaluates to 0 for every specialization of the rows $\mathbf{X}_1, \ldots, \mathbf{X}_{i-1}, \mathbf{X}_{i+1}, \ldots, \mathbf{X}_\ell$ to arbitrary vectors in $\mathbb{F}_q^{\ell'}$. Since translations by a fixed vector in $\mathbb{F}_q^{\ell'}$ give a bijection of $\mathbb{F}_q^{\ell'}$ into itself, this implies that $g|_{\mathbf{X}_i=\mathbf{b}}$ evaluates to 0 for every specialization of the rows $\mathbf{X}_1, \ldots, \mathbf{X}_{i-1}, \mathbf{X}_{i+1}, \ldots, \mathbf{X}_\ell$ to arbitrary vectors in $\mathbb{F}_q^{\ell'}$. Hence by the injectivity of the evaluation map $\mathrm{Ev} : \mathcal{F}(\ell - 1, m - 1) \to \mathbb{F}_q^{(\ell-1)\ell'}$, we see that $g|_{\mathbf{X}_i=\mathbf{b}}$ is the zero polynomial. Thus, in view of (8), $\mathbf{b} \in V_g^{(i)}$, i.e., $\mathbf{a} \in \mathbf{u}_i + V_g^{(i)}$. This proves that $V_f^{(i)} \subseteq \mathbf{u}_i + V_g^{(i)}$. The reverse inclusion is proved similarly. ∎

Corollary 24: Let $f \in \mathcal{F}(\ell, m)$ and let i be an integer between 1 and ℓ. Then the ith row-vanishing locus is either empty or an affine linear space over $\mathbb{F}_q$, i.e., either $V_f^{(i)} = \emptyset$ or $V_f^{(i)} = \mathbf{a} + V$ for some $\mathbf{a} \in \mathbb{F}_q^{\ell'}$ and a $\mathbb{F}_q$-linear space V.

Proof: Suppose $V_f^{(i)} \neq \emptyset$. Then there exists some $\mathbf{a} \in V_f^{(i)}$. Let $\mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)$ be such that $\mathbf{u}_i = \mathbf{a}$ and $\mathbf{u}_j = \mathbf{0}$ for $1 \leq j \leq \ell$ with $j \neq i$. Also let $g := \phi_{\mathbf{u},I}(f)$. Then by Lemma 23, $V_f^{(i)} = \mathbf{a} + V_g^{(i)}$. It remains to show that $V_g^{(i)}$ is a subspace of $\mathbb{F}_q^{\ell'}$. To this end, first note that $\mathbf{0} \in V_g^{(i)}$, thanks to the choice of $\mathbf{a}$. Now observe that for any minor $\mathcal{M} \in \Delta(\ell, m)$, we have $s_{\mathbf{0}}^{(i)}(\mathcal{M}) = 0$ if $\mathcal{M}$ involves the ith row and $s_{\mathbf{0}}^{(i)}(\mathcal{M}) = \mathcal{M}$ otherwise. Since $s_{\mathbf{0}}^{(i)}(g) = 0$, Lemma 3 implies that g is a $\mathbb{F}_q$-linear combination of minors of X that involve the ith row. Hence using the multilinearity of the determinant, we readily

see that $V_g^{(i)}$ is closed under addition and scalar multiplication. ■

The following result is an analog of Lemma 23 for homogeneous linear transformations of the underlying matrix.

Lemma 25: Let $f \in \mathcal{F}(\ell, m)$ and let i be an integer between 1 and ℓ. Then

$$V^{(i)}_{\phi_{\mathbf{0},A}(f)} = V_f^{(i)} A := \left\{ \mathbf{a}A : \mathbf{a} \in V_f^{(i)} \right\}$$

for every $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$, where $\mathbf{0}$ denotes the zero matrix in $M_{\ell\times\ell'}(\mathbb{F}_q)$.

Proof: Let $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$. Consider $h := \phi_{\mathbf{0},A}(f)$, i.e., $h \in \mathcal{F}(\ell, m)$ given by $h(X) = f(XA^{-1})$. Observe that if, as before, $\mathbf{X}_1, \ldots, \mathbf{X}_\ell$ denote the row vectors of X, then $\mathbf{X}_1A^{-1}, \ldots, \mathbf{X}_\ell A^{-1}$ are the row-vectors of XA^{-1}. Thus the specialization $\mathbf{X}_i = \mathbf{a}A$ in h corresponds to the specialization $\mathbf{X}_i = \mathbf{a}$ in f. The rest of the proof is similar to that of Lemma 23. ■

Using the row-vanishing locus, one can obtain a useful estimate for the Hamming weight of a codeword from $C^{\mathbb{A}}(\ell, m)$.

Proposition 26: Let $f \in \mathcal{F}(\ell, m)$ and let i be an integer between 1 and ℓ. Suppose $t = \#V_f^{(i)}$. Then

$$\mathrm{w_H}(\mathrm{Ev}(f)) \geq \frac{q^{\ell'} - t}{q^{\ell'} - q^{\ell'-\ell}} d(\ell, m). \tag{9}$$

Proof: In view of Lemma 14 and the definition of $V_f^{(i)}$, we see that

$$\begin{aligned} \mathrm{w_H}(\mathrm{Ev}(f)) &= \sum_{\mathbf{a}\in\mathbb{F}_q^{\ell'}\setminus V_f^{(i)}} \mathrm{w_H}(\mathrm{Ev}(s_{\mathbf{a}}^{(i)}(f))) \\ &\geq \left(q^{\ell'} - t\right) d(\ell - 1, m - 1). \end{aligned} \tag{10}$$

On the other hand, by Theorem 16

$$d(\ell, m) = q^{\ell(\ell'-\ell)} \prod_{i=0}^{\ell-1} (q^\ell - q^i)$$

and

$$d(\ell - 1, m - 1) = q^{(\ell-1)(\ell'-\ell)} \prod_{j=0}^{\ell-2} (q^{\ell-1} - q^j).$$

Hence, by a direct computation, $d(\ell, m)/d(\ell - 1, m - 1) = q^{\ell'} - q^{\ell'-\ell}$. Combining this with (10), we obtain the desired result. ■

Proposition 26 has the following important corollary for minimum weight codewords, which will be the key to our characterization of such codewords.

Corollary 27: Let $f \in \mathcal{F}(\ell, m)$. If $\mathrm{Ev}(f)$ is a minimum weight codeword of $C^{\mathbb{A}}(\ell, m)$, then $\#V_f^{(i)} \geq q^{\ell'-\ell}$ for all $i \in \{1, \ldots, \ell\}$.

Proof: If $\#V_f^{(i)} < q^{\ell'-\ell}$ for some $i \in \{1, \ldots, \ell\}$, then by Proposition 26, we obtain $\mathrm{w_H}(\mathrm{Ev}(f)) > d(\ell, m)$. ■

We are now ready to formulate and prove a characterization of minimum weight codewords of $C^{\mathbb{A}}(\ell, m)$. Recall that if $Y = (Y_{ij})$ is any $\ell \times \ell'$ matrix and, as before, $\ell \leq \ell'$, then the *leading maximal minor* of Y is the minor formed by the first ℓ columns of Y, namely, $\det\left((Y_{ij})_{1\leq i,j\leq \ell}\right)$.

Theorem 28: Let $f \in \mathcal{F}(\ell, m)$. Then $\mathrm{Ev}(f)$ is a minimum weight codeword of $C^{\mathbb{A}}(\ell, m)$ if and only if f is in the $\mathfrak{G}(\ell, m)$-orbit of the leading maximal minor of X. In other words, $\mathrm{w_H}(\mathrm{Ev}(f)) = d(\ell, m)$ if and only if f is the leading maximal minor of Y, where $Y = XA^{-1} + \mathbf{u}$ for some $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ and $\mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)$.

Proof: Let $\mathcal{L} := \det\left((X_{ij})_{1\leq i,j\leq \ell}\right)$ denote the leading maximal minor of X. Suppose f is in the $\mathfrak{G}(\ell, m)$-orbit of $\mathcal{L}$. Then, as noted in Section IV, the codewords $\mathrm{Ev}(f)$ and $\mathrm{Ev}(\mathcal{L})$ differ from each other by a permutation of the coordinates. Hence $\mathrm{w_H}(\mathrm{Ev}(f)) = \mathrm{w_H}(\mathrm{Ev}(\mathcal{L})) = d(\ell, m)$, thanks to Lemma 12.

To prove the converse, suppose $\mathrm{w_H}(\mathrm{Ev}(f)) = d(\ell, m)$. Since $\ell' - \ell \geq 0$, Corollary 27 implies that $V_f^{(i)}$ is nonempty for each $i \in \{1, \ldots, \ell\}$. Choose $\mathbf{u}_i \in V_f^{(i)}$ for $1 \leq i \leq \ell$. Let $\mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)$ be the $\ell \times \ell'$ matrix whose ith row vector is $\mathbf{u}_i$ for $1 \leq i \leq \ell$, and let $g := \phi_{\mathbf{u},I}(f)$. Then g is in the $\mathfrak{G}(\ell, m)$-orbit of f and by Lemma 23

$$V_f^{(i)} = \mathbf{u}_i + V_g^{(i)} \quad \text{and} \quad \mathbf{0} \in V_g^{(i)} \quad \text{for each } i \in \{1, \ldots, \ell\}.$$

Thus, $s_{\mathbf{0}}^{(i)}(g) = 0$ for each $i \in \{1, \ldots, \ell\}$. Now observe that for any $\mathcal{M} \in \Delta(\ell, m)$ and any $i \in \{1, \ldots, \ell\}$, we have $s_{\mathbf{0}}^{(i)}(\mathcal{M}) = 0$ if $\mathcal{M}$ involves the ith row of X and $s_{\mathbf{0}}^{(i)}(\mathcal{M}) = \mathcal{M}$ otherwise. Consequently, if $g = \sum_{\mathcal{M}\in\Delta(\ell,m)} a_{\mathcal{M}}\mathcal{M}$, where $a_{\mathcal{M}} \in \mathbb{F}_q$ for $\mathcal{M} \in \Delta(\ell, m)$, then by Lemma 3, we see that $a_{\mathcal{M}} = 0$ for all $\mathcal{M} \in \cup_{i=0}^{\ell-1}\Delta_i(\ell, m)$. This proves that g is a $\mathbb{F}_q$-linear combination of $\ell \times \ell$ minors of X. In particular, if $\ell' = \ell$, then $\mathcal{L}$ being the only $\ell \times \ell$ minor of X, we obtain $g = c\mathcal{L}$ for some $c \in \mathbb{F}_q$ with $c \neq 0$. Since $\mathcal{L} = \phi_{\mathbf{0},D}(c\mathcal{L})$, where D denotes the $\ell' \times \ell'$ diagonal matrix $\mathrm{diag}\,(c, 1, \ldots, 1)$ in $\mathrm{GL}_{\ell'}(\mathbb{F}_q)$, we see that f is in the $\mathfrak{G}(\ell, m)$-orbit of $\mathcal{L}$ when $\ell' = \ell$.

Now suppose $\ell < \ell'$. Consider the first row-vanishing space $V_g^{(1)}$. In view of Corollary 24 and the fact that $\mathbf{0} \in V_g^{(1)}$, we see that $V_g^{(1)}$ is a linear space over $\mathbb{F}_q$. Moreover, Corollary 27 implies that the dimension of $V_g^{(1)}$ is at least $\ell' - \ell$. Hence we can choose linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{\ell'-\ell} \in V_g^{(1)}$. Let $\mathbf{b}$ be the $(\ell' - \ell) \times \ell'$ matrix whose ith row vector is $\mathbf{b}_i$ for $1 \leq i \leq \ell' - \ell$. Since $\mathbf{b}$ has full rank, there exists an invertible matrix $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ such that

$$\begin{aligned} \mathbf{b}A &= \left(\mathbf{0}_{(\ell'-\ell)\times\ell} \,\middle|\, I_{\ell'-\ell}\right) \\ &= \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}. \end{aligned}$$

Indeed, the matrix on the right is essentially the reduced column-echelon form of $\mathbf{b}$. We now consider the function $h = h(X) = \phi_{\mathbf{0},A}(g(X)) = g(XA^{-1})$. Clearly, h is in the $\mathfrak{G}(\ell, m)$-orbit of g and hence of f; in particular, $\mathrm{w_H}(\mathrm{Ev}(h)) = d(\ell, m)$ and h is a nonzero polynomial. By the multilinearity of the determinant,

it can, just as g, be written as a $\mathbb{F}_q$-linear combination of $\ell \times \ell$ minors of X. For $1 \leq j \leq \ell'$, let $\mathbf{e}_j$ denote the vector in $\mathbb{F}_q^{\ell'}$ with 1 in the jth position and 0 elsewhere. Observe that if $\mathcal{M} \in \Delta_\ell(\ell, m)$ is the minor formed by the columns of X indexed by $j_1, \ldots, j_\ell$, where $1 \leq j_1 < \cdots < j_\ell \leq \ell'$, then $s^{(1)}_{\mathbf{e}_j}(\mathcal{M}) = 0$ if $j \notin \{j_1, \ldots, j_\ell\}$, whereas $s^{(1)}_{\mathbf{e}_j}(\mathcal{M})$ is a nonzero polynomial (and, in fact, $\pm\mathcal{M}_1$, where $\mathcal{M}_1$ is a $(\ell-1) \times (\ell-1)$ minor of X) if $j \in \{j_1, \ldots, j_\ell\}$. Now by the choice of A and by Lemma 25, we have that $\mathbf{e}_j \in V_h^{(1)}$, for all j such that $\ell < j \leq \ell'$. Consequently, if $h = \sum_{\mathcal{M} \in \Delta_\ell(\ell,m)} a_{\mathcal{M}} \mathcal{M}$, where $a_{\mathcal{M}} \in \mathbb{F}_q$ for $\mathcal{M} \in \Delta_\ell(\ell, m)$, then by Lemma 3, we see that $a_{\mathcal{M}} = 0$ for all those $\mathcal{M}$ in $\Delta_\ell(\ell, m)$ that involve the jth column of X for some $j > \ell$. But the only $\ell \times \ell$ minor of X that does not involve the jth column of X for some $j > \ell$ is $\mathcal{L}$. Hence $h = c\mathcal{L}$ for some $c \in \mathbb{F}_q$ with $c \neq 0$. It follows that f is in the $\mathfrak{G}(\ell, m)$-orbit of $\mathcal{L}$. ∎

In case $\ell' = \ell$, the above theorem simplifies to the statement in Remark 17.

VI. Enumeration of Minimum Weight Codewords

In this section, we let $d = d(\ell, m)$ denote the minimum distance of $C^{\mathbb{A}}(\ell, m)$ and A_d the number of minimum weight codewords of $C^{\mathbb{A}}(\ell, m)$. Having characterized the codewords of weight d in the previous section, we now proceed to compute A_d. Equivalently, we determine the number of polynomials $f \in \mathcal{F}(\ell, m)$ giving rise to minimum weight codewords. We have seen in Section IV that the finite group $\mathfrak{G}(\ell, m)$ acts naturally on $\mathcal{F}(\ell, m)$. With this in view, we can use standard group theory together with Theorem 28 to obtain what follows.

Lemma 29: Let $\mathcal{L} = \det\left((X_{ij})_{1 \leq i,j \leq \ell}\right)$ be the leading maximal minor of X. Then

$$A_d = \frac{\#\mathfrak{G}(\ell, m)}{\#\mathrm{Stab}(\mathcal{L})},$$

where $\mathrm{Stab}(\mathcal{L})$ denotes the stabilizer of the minor $\mathcal{L}$.

Proof: By Theorem 28, the cardinality of the $\mathfrak{G}(\ell, m)$-orbit of $\mathcal{L}$ is equal to A_d. On the other hand, for any finite group acting on a finite set, the cardinality of the orbit of an element is equal to the index of its stabilizer. ∎

Thanks to Lemma 29, the computation of A_d reduces to the problem of finding the cardinality of the stabilizer of $\mathcal{L} := \det\left((X_{ij})_{1 \leq i,j \leq \ell}\right)$. To this end, let us begin by observing that if $f \in \mathcal{F}(\ell, m)$ is in the $\mathfrak{G}(\ell, m)$-orbit of $\mathcal{L}$, i.e., if $f = \phi_{\mathbf{u},A}(\mathcal{L})$ for some $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ and $\mathbf{u} \in M_{\ell \times \ell'}(\mathbb{F}_q)$, then

$$f = \det(XM + \mathbf{m}) \tag{11}$$

for some $M \in M_{\ell' \times \ell}(\mathbb{F}_q)$ of rank ℓ and $\mathbf{m} \in M_{\ell \times \ell}(\mathbb{F}_q)$. Indeed, it suffices to take M to be the $\ell' \times \ell$ matrix formed by the first ℓ columns of A^{-1} and $\mathbf{m}$ to be the $\ell \times \ell$ matrix formed by the first ℓ columns of $\mathbf{u}$, and observe that $\mathrm{rank}(M) = \ell$ since A is nonsingular and that the leading maximal minor of the $\ell \times \ell'$ matrix $XA^{-1} + \mathbf{u}$ is $\det(XM + \mathbf{m})$. We shall now analyze when a polynomial f given by (11) is in the stabilizer of $\mathcal{L}$. As usual, we denote by $\mathrm{SL}_\ell(\mathbb{F}_q)$ the special linear group of $\ell \times \ell$ matrices over $\mathbb{F}_q$, *viz.*, $\mathrm{SL}_\ell(\mathbb{F}_q) := \{A \in \mathrm{GL}_\ell(\mathbb{F}_q) : \det A = 1\}$.

Lemma 30: Let $\mathcal{L} = \det\left((X_{ij})_{1 \leq i,j \leq \ell}\right)$ be the leading maximal minor of X. Also let $M \in M_{\ell' \times \ell}(\mathbb{F}_q)$ be of rank ℓ and $\mathbf{m} \in M_{\ell \times \ell}(\mathbb{F}_q)$. Then $\mathcal{L} = \det(XM + \mathbf{m})$ if and only if $\mathbf{m} = \mathbf{0}$ and there exists $E \in \mathrm{SL}_\ell(\mathbb{F}_q)$ such that the first ℓ rows of ME form the $\ell \times \ell$ identity matrix, while the last $\ell' - \ell$ rows are zero. In this case, the matrix E in $\mathrm{SL}_\ell(\mathbb{F}_q)$ is uniquely determined by M.

Proof: We start by showing the uniqueness of the matrix E. Suppose

$$\begin{aligned} ME_1 &= \begin{pmatrix} \mathbf{I}_\ell \\ \mathbf{0} \end{pmatrix} \\ &= ME_2 \quad \text{for some } E_1,\ E_2 \in \mathrm{SL}_\ell(\mathbb{F}_q) \end{aligned}$$

where $\mathbf{I}_\ell$ denotes the $\ell \times \ell$ identity matrix and $\mathbf{0}$ the $(\ell' - \ell) \times \ell$ zero matrix. Then $M(E_2 - E_1) = 0$. Since M has full rank, this can only happen if $E_1 = E_2$.

To prove the equivalence, first suppose there exists $E \in \mathrm{SL}_\ell(\mathbb{F}_q)$ such that

$$ME = \begin{pmatrix} \mathbf{I}_\ell \\ \mathbf{0} \end{pmatrix} \tag{12}$$

and also suppose $\mathbf{m} = \mathbf{0}$. Then

$$\begin{aligned} \det(XM + \mathbf{m}) &= \det(XM) = \det(XME) \\ &= \det\left(X \begin{pmatrix} \mathbf{I}_\ell \\ \mathbf{0} \end{pmatrix}\right) = \mathcal{L}. \end{aligned}$$

Conversely, suppose $\mathcal{L} = \det(XM + \mathbf{m})$. Since M has full rank, there exists $N \in M_{\ell' \times \ell}(\mathbb{F}_q)$ such that $NM = \mathbf{m}$. Hence $\mathcal{L} = \det(XM + \mathbf{m}) = \det((X + N)M)$. Using the Cauchy-Binet formula (Lemma 10) and the notation therein, we now find

$$\mathcal{L} = \sum_I \det((X + N)^I) \det(M_I) \tag{13}$$

where the sum is over all subsets I of $\{1, \ldots, \ell'\}$ of cardinality ℓ. For any such I, Lemma 9 implies that $\det((X + N)^I)$ is the sum of $\det(X^I)$ and a $\mathbb{F}_q$-linear combination of minors of X^I of order $< \ell$. Hence, comparing terms of total degree ℓ in (13), we obtain

$$\mathcal{L} = \det(X^{I^*}) = \sum_I \det(X^I) \det(M_I) \tag{14}$$

where $I^* := \{1, \ldots, \ell\}$. Consequently, in view of Lemma 3, $\det(M_{I^*}) = 1$, while $\det(M_I) = 0$ for every $I \subseteq \{1, \ldots, \ell'\}$ with $\#I = \ell$ and $I \neq I^*$. Define $E := M_{I^*}^{-1}$. It is clear that $E \in \mathrm{SL}_\ell(\mathbb{F}_q)$. Moreover, by the choice of E, the first ℓ rows of ME form the $\ell \times \ell$ identity matrix $\mathbf{I}_\ell$. We claim that for any $i > \ell$, the ith row ME_i of ME is zero. To see this, write $ME_i = (b_1, \ldots, b_\ell)$. Choose any $j \in I^*$ and let $I := (I^* \cup \{i\}) \setminus \{j\}$. Then $I \subseteq \{1, \ldots, \ell'\}$ with $\#I = \ell$ and $\det(M_I) = 0$ since $I \neq I^*$. On the other hand, $\det(M_I) = \det(M_I E)$. Now, since the first $\ell - 1$ elements of I are contained in $\{1, \ldots, \ell\}$, the first $\ell - 1$ rows of the matrix $M_I E$ form the matrix obtained from $\mathbf{I}_\ell$ by deleting its jth row. This implies

that $0 = \det(M_I E) = \pm(M_I E)_{\ell j} = \pm(ME)_{ij}$. By varying j over I^*, we obtain $ME_i = (0, \ldots, 0)$. This proves the claim. It remains to show that $\mathbf{m} = \mathbf{0}$. We have noted earlier that there is $N \in M_{\ell \times \ell'}(\mathbb{F}_q)$ such that $\mathbf{m} = NM$. Hence

$$\begin{aligned}\mathcal{L} &= \det(XM + \mathbf{m}) = \det((X+N)M) \\ &= \det((X+N)ME) \\ &= \det((X_{ij} + N_{ij})_{1 \le i,j \le \ell})\end{aligned}$$

where the penultimate equality follows since $E \in \mathrm{SL}_\ell(\mathbb{F}_q)$ and the last equality follows since ME satisfies (12). Using Lemma 9 together with Lemma 3, by comparing the coefficients of $(\ell - 1) \times (\ell - 1)$ minors, we find $N_{ij} = 0$ for $1 \le i, j \le \ell$. But then $\mathbf{m}E = N(ME) = (N_{ij})_{1 \le i,j \le \ell} = \mathbf{0}$, thanks to (12). Since E is invertible, this implies that $\mathbf{m} = \mathbf{0}$. ∎

We are now ready to compute the cardinality of the stabilizer of the leading maximal minor.

Lemma 31: Let $\mathcal{L} = \det\left((X_{ij})_{1 \le i,j \le \ell}\right)$ be the leading maximal minor of X. Then

$$\#\mathrm{Stab}(\mathcal{L}) = \frac{q^{\ell(\ell'-\ell)}}{q-1} \prod_{i=\ell}^{\ell'-1} (q^{\ell'} - q^i) \prod_{j=0}^{\ell-1} (q^\ell - q^j).$$

Proof: Let $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ and $\mathbf{u} \in M_{\ell \times \ell'}(\mathbb{F}_q)$. Suppose $\phi_{\mathbf{u},A}(\mathcal{L}) = \mathcal{L}$. First we write $A = (M \,|\, R)$ where $M \in M_{\ell' \times \ell}(\mathbb{F}_q)$ and $R \in M_{\ell' \times (\ell' - \ell)}(\mathbb{F}_q)$ are matrices formed, respectively, by the first ℓ columns of A and the remaining $\ell' - \ell$ columns of A. Similarly, we write $\mathbf{u} = (\mathbf{m} \,|\, \mathbf{r})$. Then, as in (11), $\mathcal{L} = \det(XM + \mathbf{m})$. Hence by Lemma 30, $\mathbf{m} = \mathbf{0}$ and moreover, there exists a unique $E \in SL_\ell(\mathbb{F}_q)$ such that

$$A \left(\begin{array}{c|c} E & \mathbf{0} \\ \hline \mathbf{0} & I_{\ell' - \ell} \end{array} \right) = (ME \,|\, R) = \left(\begin{array}{c|c} \mathbf{I}_\ell & \\ \hline \mathbf{0} & R \end{array} \right) \qquad (15)$$

where $\mathbf{0}$ denotes the zero matrix of an appropriate size and, as before, $\mathbf{I}_\ell$ denotes the $\ell \times \ell$ identity matrix. The matrices R and $\mathbf{r}$ do not have any effect on $\phi_{\mathbf{u},A}(\mathcal{L})$ and can, therefore, be chosen freely. However, R has to be chosen in such a way that the matrix on the right-hand side (RHS) of (15) has full rank. This means that the last $\ell' - \ell$ rows of R must be linearly independent. It follows that $\#\mathrm{Stab}(\mathcal{L})$ is the product of $\#\mathrm{SL}_\ell(\mathbb{F}_q)$ and the following terms:

$$\begin{array}{ll} q^{\ell(\ell'-\ell)} & \text{for the choice of } \mathbf{r} \\ q^{\ell(\ell'-\ell)} & \text{for the first } \ell \text{ rows of } R, \text{ and} \\ \displaystyle\prod_{i=0}^{\ell'-\ell-1} (q^{\ell'-\ell} - q^i) & \text{for the last } \ell' - \ell \text{ rows of } R. \end{array}$$

Since $\#\mathrm{SL}_\ell(\mathbb{F}_q) = (q-1)^{-1} \prod_{j=0}^{\ell-1} (q^\ell - q^j)$, the lemma is proved. ∎

We now obtain the main result of this section concerning the number of codewords of $C^{\mathbb{A}}(\ell, m)$ of weight $d(\ell, m)$. The result is best formulated using the Gaussian binomial coefficient defined, for any integers k and n with $1 \le k \le n$, as follows:

$$\begin{aligned}\begin{bmatrix} n \\ k \end{bmatrix}_q &:= \frac{[n]_q!}{[k]_q![n-k]_q!} \\ &= \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})}. \end{aligned} \qquad (16)$$

It is well known that (16) is a monic polynomial in q of degree $k(n-k)$ with nonnegative integral coefficients. In particular, $\begin{bmatrix} n \\ n \end{bmatrix}_q = 1$.

Theorem 32: The number A_d of codewords of weight $d(\ell, m)$ of the affine Grassmann code $C^{\mathbb{A}}(\ell, m)$ is given by

$$A_d = (q-1) q^{\ell^2} \begin{bmatrix} \ell' \\ \ell \end{bmatrix}_q.$$

Proof: Using Proposition 20 we see that

$$\begin{aligned}\#\mathfrak{G}(\ell, m) &= \#M_{\ell \times \ell'}(\mathbb{F}_q) \cdot \#GL_{\ell'}(\mathbb{F}_q) \\ &= q^{\ell\ell'} \prod_{i=0}^{\ell'-1} (q^{\ell'} - q^i).\end{aligned}$$

Hence, the desired result follows from Lemmas 29 and 31. ∎

For $\ell = 1$, we obtain $A_d = q(q^{\ell'} - 1)$, whereas for $\ell' = \ell$, we obtain $A_d = (q-1)q^{\ell^2}$. This is in agreement with Remarks 11 and 17, respectively.

VII. Connection With Grassmann Codes

Grassmann codes, denoted by $C(\ell, m)$, are $[n, k]_q$-linear codes defined for any positive integers ℓ, m satisfying $1 \le \ell \le m$, where

$$n := \begin{bmatrix} m \\ \ell \end{bmatrix}_q := \frac{(q^m - 1)(q^m - q) \cdots (q^m - q^{\ell-1})}{(q^\ell - 1)(q^\ell - q) \cdots (q^\ell - q^{\ell-1})}$$

and

$$k := \binom{m}{\ell}.$$

The case $\ell = m$ is trivial and in general, there is a natural equivalence between $C(\ell, m)$ and $C(m - \ell, m)$. With this in view, we shall assume $1 \le \ell < m$ and that $m - \ell \ge \ell$. Thus, if we set $\ell' := m - \ell$, then we have $1 \le \ell \le \ell'$ and $\ell + \ell' = m$, exactly as in the basic set-up of Sections II through VI.

A quick way to define $C(\ell, m)$ is to say that these are linear codes associated to the projective system obtained from the Plücker embedding of the Grassmann variety $G_{\ell,m}$ in the projective space $\mathbb{P}^{k-1}$ over $\mathbb{F}_q$. Recall that the *Grassmann variety* (also known as the *Grassmannian*) $G_{\ell,m}$ over $\mathbb{F}_q$ is the space of all ℓ-dimensional subspaces of the m-dimensional vector space $\mathbb{F}_q^m$ over $\mathbb{F}_q$. The *Plücker embedding* maps $G_{\ell,m}(\mathbb{F}_q)$ into $\mathbb{P}^{k-1} = \mathbb{P}(\wedge^\ell \mathbb{F}_q^m)$ by sending a ℓ-dimensional subspace W

	$C(\ell,m)$	$C^{\mathbb{A}}(\ell,m)$
Length	$\begin{bmatrix} m \\ \ell \end{bmatrix}_q = q^\delta + q^{\delta-1} + 2q^{\delta-2} + \cdots$	q^δ
Dimension	$\binom{m}{\ell}$	$\binom{m}{\ell}$
Minimum distance	q^δ	$q^{\delta-\ell^2}\prod_{i=0}^{\ell-1}(q^\ell - q^i) = q^\delta - q^{\delta-1} - q^{\delta-2} + \cdots$
Number of min. weight codewords	$(q-1)\begin{bmatrix} m \\ \ell \end{bmatrix}_q = O(q^{\delta+1})$	$(q-1)q^{\ell^2}\begin{bmatrix} m-\ell \\ \ell \end{bmatrix}_q = O(q^{\delta+1})$

Fig. 1. A comparison of affine Grassmann and Grassmann codes.

spanned by $w_1, \ldots, w_\ell$ to the class of $w_1 \wedge \cdots \wedge w_\ell$. To obtain this a little more concretely, one can proceed as follows. Let

$$I(\ell,m) = \{(\alpha_1, \ldots, \alpha_\ell) \in \mathbb{Z}^\ell : 1 \le \alpha_1 < \cdots < \alpha_\ell \le m\}$$

be an indexing set [ordered, say, lexicographically] for the points of $\mathbb{P}^{k-1}(\mathbb{F}_q)$. Given any $\alpha \in I(\ell,m)$ and any $\ell \times m$ matrix $A = (a_{ij})$, let $p_\alpha(A)$ be the determinant of the αth submatrix of

$$A := \det\left(a_{i\alpha_j}\right)_{1\le i,j\le \ell}.$$

Now, for any $W \in G_{\ell,m}(\mathbb{F}_q)$, we can find a $\ell \times m$ matrix A_W whose rows give a basis of W, and then

$$p(W) = (p_\alpha(A_W))_{\alpha \in I(\ell,m)} \in \mathbb{P}^{k-1}$$

is called the *Plücker coordinate* of W. It is easy to see that this depends only on W and not on the choice of A_W. Moreover, the map $W \mapsto p(W)$ of $G_{\ell,m}(\mathbb{F}_q) \to \mathbb{P}^{k-1}$ is precisely the Plücker embedding; it is well-known that this is injective and its image equals the zero locus of certain quadratic polynomials. Henceforth, we shall identify W with $p(W)$. The definition of $C(\ell,m)$ as the codes corresponding to the projective system in $\mathbb{P}^{k-1}$ given by $G_{\ell,m}(\mathbb{F}_q)$ amounts to the following.

Let $\mathcal{G}(\ell,m) = (\wedge^\ell \mathbb{F}_q^m)^*$ denote the space of linear forms on $\wedge^\ell \mathbb{F}_q^m$ [this can be identified with $(\wedge^{m-\ell}\mathbb{F}_q^m)$] and let $\{Q_1, \ldots, Q_n\}$ be (arbitrary, but fixed, lifts of) points in $\wedge^\ell \mathbb{F}_q^m$ corresponding to the elements of $G_{\ell,m}(\mathbb{F}_q)$ in $\mathbb{P}^{k-1}$. Now the evaluation map

$$\mathrm{Ev} : \mathcal{G}(\ell,m) \to \mathbb{A}^n(\mathbb{F}_q)$$

defined by

$$\mathrm{Ev}(g) := (g(Q_1), \ldots, g(Q_n))$$

is injective (since the Plücker embedding is nondegenerate) and its image is precisely the Grassmann code $C(\ell,m)$.

To relate $C(\ell,m)$ to $C^{\mathbb{A}}(\ell,m)$, let us first note that the projective space $\mathbb{P}^{k-1}$ is covered by affine spaces $U_\alpha \simeq \mathbb{A}^{k-1}$, where $U_\alpha := \{p \in \mathbb{P}^{k-1} : p_\alpha = 1\}$ and α varies over $I(\ell,m)$. It is a classical fact that the intersection $B_\alpha := G_{\ell,m} \cap U_\alpha$ is isomorphic to an affine space of dimension $\delta := \ell\ell' = \ell(m-\ell)$. This isomorphism is described explicitly by the Basic Cell Lemma of [6]. In effect, if $W \in B_\alpha$, then the $\ell \times m$ matrix A_W associated to W can be chosen in such a way that the αth submatrix of A_W is the identity matrix. Now if B_W denotes the $\ell \times \ell'$ matrix formed by removing from A_W its αth submatrix, then the entries of B_W can be viewed as variables. Moreover, the k-tuple $p(W)$ formed by the $\ell \times \ell$ minors of A_W corresponds to the k-tuple formed by arbitrary sized minors of B_W. Thus, evaluating linear forms at points of the affine open cell B_α of $G_{\ell,m}$ corresponds to evaluating linear forms in arbitrary sized minors of B_W at the points of the δ-dimensional affine space over $\mathbb{F}_q$. In other words, the evaluation map $\mathrm{Ev} : \mathcal{G}(\ell,m) \to \mathbb{A}^n$ reduces to the evaluation map on $\mathcal{F}(\ell,m)$ considered in Section II.

Remark 33: We hope that the above discussion clarifies the genesis of the terminology *affine Grassmann* for the codes $C^{\mathbb{A}}(\ell,m)$ studied in this paper. Indeed, this terminology arises from the fact that in essence, we consider an affine open piece of the Grassmann variety instead of the full Grassmann variety. However, this terminology should not be confused with the so called *affine Grassmannian*, which is usually an infinite dimensional object obtained from the Laurent power series valued points of an algebraic group. Indeed, it appears unlikely that interesting and efficient codes could be built from the infinite dimensional affine Grassmannian, and hence there does not seem to be any harm in calling the codes $C^{\mathbb{A}}(\ell,m)$ as affine Grassmann codes.

It may be worthwhile to compare the basic parameters of $C(\ell,m)$ and $C^{\mathbb{A}}(\ell,m)$, see Fig. 1. While the results for $C^{\mathbb{A}}(\ell,m)$ are proved in the previous sections, those for $C(\ell,m)$ can be found, for example, in [13] and [6].

It may be noted that the two classes of codes are comparable. While the affine Grassmann codes are shorter than Grassmann codes and have a better rate, the Grassmann codes fare better in terms of the minimum distance and also the relative distance. In spite of the connection between the two codes indicated above, there does not seem to be a straightforward way to deduce the properties of one code directly from that of the other. However, the growing literature on Grassmann codes can provide pointers for further research on affine Grassmann codes, whereas the analogy of affine Grassmann codes with Reed-Muller codes and results obtained in this paper concerning their automorphisms may provide further impetus for the study of Grassmann codes.

ACKNOWLEDGMENT

S. R. Ghorpade author would like to thank the Department of Mathematics of the Technical University of Denmark for its warm hospitality during his visits in June 2008 and April 2009 when some of this work was carried out.

REFERENCES

[1] T. P. Berger and P. Charpin, "The automorphism group of generalized Reed-Muller codes," *Discr. Math.*, vol. 117, pp. 1–17, 1993.

[2] P. Delsarte, J. M. Goethals, and F. J. MacWilliams, "Generalized Reed-Muller codes and their relatives," *Inf. Control*, vol. 16, pp. 403–442, 1974.

[3] P. Doubilet, G. C. Rota, and J. Stein, "Foundations of combinatorics IX: Combinatorial methods in invariant theory," *Stud. Appl. Math.*, vol. 53, pp. 185–216, 1974.

[4] F. R. Gantmacher, *The Theory of Matrices*. New York: Chelsea, 1960, vol. 1.

[5] S. R. Ghorpade, "Abhyankar's work on young tableaux and some recent developments," in *Algebraic Geometry and its Applications (West Lafayette, 1990)*. New York: Springer-Verlag, 1994, pp. 233–265.

[6] S. R. Ghorpade and G. Lachaud, "Higher weights of Grassmann codes," in *Coding Theory, Cryptography and Related Areas (Guanajuato, 1998)*. Berlin/Heidelberg: Springer-Verlag, 2000, pp. 122–131.

[7] S. R. Ghorpade, A. R. Patil, and H. K. Pillai, "Decomposable subspaces, linear sections of Grassmann varieties, and higher weights of Grassmann codes," *Finite Fields Appl.*, vol. 15, pp. 54–68, 2009.

[8] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*. Reading, MA: Addison-Wesley, 1989.

[9] J. P. Hansen, T. Johnsen, and K. Ranestad, "Grassmann codes and Schubert unions," in *Arithmetic, Geometry and Coding Theory (Luminy, 2005), Séminaires et Congrès*. Paris: Soc. Math. France, 2009, vol. 21, pp. 103–121.

[10] J.-R. Joly, "Équations et variétés algébraiques sur un corps fini," *Enseign. Math.*, vol. 19, pp. 1–117, 1973.

[11] R. Knörr and W. Willems, "The automorphism groups of generalized Reed-Muller codes," *Astérisque*, vol. 181–182, pp. 195–207, 1990.

[12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. New York: Elsevier, 1977.

[13] D. Y. Nogin, "Codes associated to Grassmannians," in *Arithmetic, Geometry and Coding Theory (Luminy, 1993)*. Berlin, Germany: Walter de Gruyter, 1996, pp. 145–154.

[14] *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, vol. I and II.

Peter Beelen was born in Kampen, the Netherlands, on May 5, 1973. He received the Master's degree in mathematics from the University of Utrecht, The Netherlands, in 1996. In 2001, he received the Ph.D. degree in mathematics from the Technical University of Eindhoven, The Netherlands, on the thesis "Algebraic geometry and coding theory."

From September 2001 to September 2002, he was a Postdoctoral Researcher with the same university in Eindhoven and from September 2002 to August 2004, he was a Postdoctoral Researcher with the University of Essen, Germany. From October 2004 to January 2007, he worked as an Assistant Professor with the Department of Mathematics, Technical University of Denmark, Kgs. Lyngby. He is currently an Associate Professor with the Department of Mathematics, Technical University of Denmark. His research interests include various aspects of algebra and its applications, such as algebraic curves, boolean functions, coding theory, and function field theory.

Sudhir R. Ghorpade received the B.Sc., M.Sc. and Ph.D. degrees in mathematics from the University of Bombay, Indian Institute of Technology (IIT) Bombay, and Purdue University, West Lafayette, IN, in 1982, 1984, and 1989, respectively.

Since December 1989, he has been on the faculty of the IIT Bombay, where he is currently a Professor. He has held short-term visiting positions with the Institut de Mathématiques de Luminy, Marseille, France, Tata Institute of Fundamental Research, Mumbai, India, Université de la Mediterrannée, Aix-Marseille, France, Christian-Alberchts-Universität zu Kiel, Germany, Purdue University, West Lafayette, and the University of Tennessee, Knoxville. His research interests include algebraic geometry, coding theory, combinatorics, and commutative algebra.

Tom Høholdt (M'93–SM'96–F'00) was born in Copenhagen, Denmark, on April 26, 1945. He received the M.Sc. degree in mathematics from the University of Copenhagen in 1968.

He is a Professor of Mathematics with the Technical University of Denmark, Lyngby. His research interests include coding theory, signal analysis, sequence design, and other areas of applied (discrete) mathematics.

Dr. Høholdt served as an Associate Editor for Coding Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY from 1994 to 1996. He received the IEEE Information Theory Society 1991 Best Paper Award and received a prize from the Telecommunication Advancement Foundation in Japan in 1998. He received the G.A. Hagemann Goldmedal in May 2000 and is on the editorial board of the journal *Advances in Mathematics of Communications*.