DUALS OF AFFINE GRASSMANN CODES AND THEIR RELATIVES

PETER BEELEN, SUDHIR R. GHORPADE, AND TOM HØHOLDT

ABSTRACT. Affine Grassmann codes are a variant of generalized Reed-Muller codes and are closely related to Grassmann codes. These codes were introduced in a recent work [2]. Here we consider, more generally, affine Grassmann codes of a given level. We explicitly determine the dual of an affine Grassmann code of any level and compute its minimum distance. Further, we ameliorate the results of [2] concerning the automorphism group of affine Grassmann codes. Finally, we prove that affine Grassmann codes and their duals have the property that they are linear codes generated by their minimum-weight codewords. This provides a clean analogue of a corresponding result for generalized Reed-Muller codes.

1. INTRODUCTION

Fix a finite field $\mathbb{F}_q$ with q elements and positive integers ℓ, ℓ' with $\ell \le \ell'$; set

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

Briefly put, the affine Grassmann code $C^{\mathbb{A}}(\ell, m)$ is the q-ary linear code obtained by evaluating linear polynomials in the minors of a generic $\ell \times \ell'$ matrix X at all points of the δ-dimensional affine space of $\ell \times \ell'$ matrices with entries in $\mathbb{F}_q$. Evidently, when $\ell = 1$, this gives the first order generalized Reed-Muller code $\mathrm{RM}(1, \ell')$. However, in general, $C^{\mathbb{A}}(\ell, m)$ is only a subcode of the ℓ^{th} order generalized Reed-Muller code $\mathrm{RM}(\ell, \delta)$. The length n and the dimension k of $C^{\mathbb{A}}(\ell, m)$ are given by

$$n = q^{\delta} \quad \text{and} \quad k = \binom{m}{\ell}.$$

Affine Grassmann codes were introduced in [2], where the following was shown.

- The minimum distance of $C^{\mathbb{A}}(\ell, m)$ is
$$d(\ell, m) := q^{\delta - \ell^2} \prod_{j=0}^{\ell-1} (q^{\ell} - q^{j}) = q^{\delta} \prod_{i=1}^{\ell} \left(1 - \frac{1}{q^i}\right). \tag{1}$$
- The (permutation) automorphism group of $C^{\mathbb{A}}(\ell, m)$ contains a subgroup isomorphic to the semidirect product $M_{\ell \times \ell'}(\mathbb{F}_q) \rtimes_{\theta} \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ of the additive group of $\ell \times \ell'$ matrices over $\mathbb{F}_q$ with the multiplication group of $\ell' \times \ell'$ nonsingular matrices over $\mathbb{F}_q$, where $\theta : GL_{\ell'}(\mathbb{F}_q) \to \mathrm{Aut}(M_{\ell \times \ell'}(\mathbb{F}_q))$ is the homomorphism defined by $\theta(A)(\mathbf{u}) := \mathbf{u}A^{-1}$.
- The minimum-weight codewords of $C^{\mathbb{A}}(\ell, m)$ are precisely the evaluations of leading maximal minors (formed by the ℓ rows and the first ℓ columns) of X', where $X' = XA^{-1} + \mathbf{u}$ for some $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ and $\mathbf{u} \in M_{\ell \times \ell'}(\mathbb{F}_q)$.
- The number of minimum-weight codewords of $C^{\mathbb{A}}(\ell, m)$ is given, in terms of the Gaussian binomial coefficients (defined below for any $a \ge b \ge 0$), by
$$(q-1)q^{\ell^2} \begin{bmatrix} \ell' \\ \ell \end{bmatrix}_q \quad \text{where} \quad \begin{bmatrix} a \\ b \end{bmatrix}_q := \frac{(q^a - 1)(q^a - q) \cdots (q^a - q^{b-1})}{(q^b - 1)(q^b - q) \cdots (q^b - q^{b-1})}. \tag{2}$$

Date: November 5, 2011.

In this paper we continue the study of affine Grassmann codes and give an explicit description of the dual of $C^{\mathbb{A}}(\ell, m)$. As a result, it will be seen that affine Grassmann codes are almost always self-orthogonal. Moreover, we determine precisely the minimum distance of $C^{\mathbb{A}}(\ell, m)^{\perp}$ and show that it is at most 4. Thus, it is seen that the parity check matrix of $C^{\mathbb{A}}(\ell, m)$ is rather sparse and that an affine Grassmann code may be regarded as a LDPC code. Further, following a suggestion by an anonymous referee of [2], we augment the abovementioned result on the automorphism group of $C^{\mathbb{A}}(\ell, m)$ by showing that $\mathrm{Aut}(C)$ contains, in fact, a larger group that is essentially obtained by taking the product of the general linear group $\mathrm{GL}_{\ell}(\mathbb{F}_q)$ with the semidirect product $M_{\ell\times\ell'}(\mathbb{F}_q) \rtimes_{\theta} \mathrm{GL}_{\ell'}(\mathbb{F}_q)$. It will also be seen that the full automorphism group can, in fact, be even larger. Finally, we show that the affine Grassmann codes as well as their duals have the property that the minimum-weight codewords generate the code. This can be viewed as an analogue of the classical result that binary Reed-Muller codes are generated by their minimum-weight codewords; see, e.g., MacWilliams and Sloane [9, Ch. 13, §6]. Such a result is not true, in general, for q-ary generalized Reed-Muller codes, and in this case, a complete characterization of generation by the minimum-weight codewords was obtained by Ding and Key [5, Thm. 1] (see also part (v) of Proposition 4 below). A special case $\ell = 1$ of our results corresponds to their result for the generalized Reed-Muller codes $\mathrm{RM}(1, \delta)$ and $\mathrm{RM}(\delta(q-1)-2, \delta)$.

Following a suggestion of D. Augot, we shall consider in this paper a mild generalization of $C^{\mathbb{A}}(\ell, m)$ obtained by choosing a nonnegative integer $r \le \ell$ and then restricting the function space to linear polynomials in the $i \times i$ minors of X for $i \le r$. The resulting linear codes are denoted by $C^{\mathbb{A}}(\ell, m; r)$ and called *affine Grassmann codes* of *level* r. Note that the first order Reed-Muller codes of length q^{δ} as well as the affine Grassmann codes are special cases; indeed, $C^{\mathbb{A}}(\ell, m; 1) = \mathrm{RM}(1, \delta)$ and $C^{\mathbb{A}}(\ell, m; \ell) = C^{\mathbb{A}}(\ell, m)$. Moreover, by varying the levels, we obtain a nice filtration, compatible with the Reed-Muller filtration:

$$\begin{array}{ccccccc}
C^{\mathbb{A}}(\ell, m; 1) & \subset & C^{\mathbb{A}}(\ell, m; 2) & \subset & \cdots & \subset & C^{\mathbb{A}}(\ell, m; \ell) \\
\| & & \bigcap & & & & \bigcap \\
\mathrm{RM}(1, \delta) & \subset & \mathrm{RM}(2, \delta) & \subset & \cdots & \subset & \mathrm{RM}(\ell, \delta)
\end{array}$$

In general, for any $r \ge 0$, the length n and the dimension k_r of $C^{\mathbb{A}}(\ell, m; r)$ are given by

$$n = q^{\delta} \quad \text{and} \quad k_r = \sum_{i=0}^{r} \binom{\ell}{i}\binom{\ell'}{i}, \tag{3}$$

whereas the formula (1) generalizes nicely to the following:

$$\text{minimum distance of } C^{\mathbb{A}}(\ell, m; r) = q^{\delta} \prod_{i=1}^{r} \left(1 - \frac{1}{q^i}\right). \tag{4}$$

The augmentation of the result concerning the automorphism group, an explicit description of the dual, determination of the minimum distance of the dual, and the result concerning generation by minimum-weight codewords are all obtained more generally, in the case of affine Grassmann codes of any given level. However, for the duals $C^{\mathbb{A}}(\ell, m; r)^{\perp}$, it is shown that generation by minimum-weight codewords is valid for $r = 1$ and $r = \ell$, but not, in general, for $1 < r < \ell$.

2. Preliminaries

Let $X = (X_{ij})$ be a $\ell \times \ell'$ matrix whose entries are algebraically independent indeterminates over $\mathbb{F}_q$. By R we denote the integral rectangle $[1, \ell] \times [1, \ell']$, i.e.,

$$\mathsf{R} := \left\{(i, j) \in \mathbb{Z}^2 : 1 \le i \le \ell \text{ and } 1 \le j \le \ell'\right\}.$$

By $\mathbb{F}_q[X]$ we denote the polynomial ring in the $\ell\ell'$ variables X_{ij} (where (i,j) vary over R) with coefficients in $\mathbb{F}_q$. The set of all monomials in $\mathbb{F}_q[X]$ will be denoted by $\mathbb{M}(\ell,m)$. Note that every $\mu \in \mathbb{M}(\ell,m)$ is of the form

$$\mu = \prod_{(i,j)\in\mathsf{R}} X_{ij}^{\alpha_{ij}} \quad \text{for some nonnegative integers } \alpha_{ij}$$

The exponents α_{ij} ($(i,j) \in \mathsf{R}$) are uniquely determined by μ and their sum is denoted by $\deg \mu$; also, we write $\deg_{X_{ij}} \mu = \alpha_{ij}$. We say that the monomial μ is *reduced* (resp: *squarefree*) if $0 \le \deg_{X_{ij}} \mu \le q-1$ (resp: $0 \le \deg_{X_{ij}} \mu \le 1$) for all $(i,j) \in \mathsf{R}$. These two notions coincide when $q = 2$. The set of all reduced monomials in $\mathbb{F}_q[X]$ will be denoted by $\overline{\mathbb{M}}(\ell,m)$ and the $\mathbb{F}_q$-linear space generated by $\overline{\mathbb{M}}(\ell,m)$ will be denoted by $\mathfrak{R}(\ell,m)$. Elements of $\mathfrak{R}(\ell,m)$ are called *reduced polynomials*. There is a natural surjective map from $\mathbb{M}(\ell,m)$ to $\overline{\mathbb{M}}(\ell,m)$ that sends a monomial μ to the unique monomial $\bar{\mu}$ obtained from μ as follows: whenever an exponent α_{ij} of X_{ij} is $\ge q$, replace it by r_{ij}, where $r_{ij} \equiv \alpha_{ij} (\text{mod } q-1)$ and $1 \le r_{ij} \le q-1$. This map extends by $\mathbb{F}_q$-linearity to a surjective $\mathbb{F}_q$-vector space homomorphism $\mathbb{F}_q[X] \to \mathfrak{R}(\ell,m)$, which may be referred to as the *reduction map*. We will denote the image of $f \in \mathbb{F}_q[X]$ under the reduction map by $\bar{f}$, and call $\bar{f}$ the *reduced polynomial* corresponding to f.

The set $\mathbb{M}(\ell,m)$ is obviously a $\mathbb{F}_q$-basis of $\mathbb{F}_q[X]$ and hence every $f \in \mathbb{F}_q[X]$ can be uniquely written as $\sum_{\mu\in\mathbb{M}(\ell,m)} c_\mu \mu$, where $c_\mu \in \mathbb{F}_q$ for each $\mu \in \mathbb{M}(\ell,m)$ and $c_\mu = 0$ for all except finitely many μ's. A monomial μ for which $c_\mu \ne 0$ will be referred to as a *term* of f, and we let

$$\mathrm{Term}(f) := \{\mu \in \mathbb{M}(\ell,m) : c_\mu \ne 0\}.$$

Note that $\mathrm{Term}(f)$ is the empty set if and only if f is the zero polynomial. For $0 \ne f \in \mathbb{F}_q[X]$, the (total) degree and the degree in the variable X_{ij} are given by

$$\deg f := \max\{\deg \mu : \mu \in \mathrm{Term}(f)\} \text{ and } \deg_{X_{ij}} f := \max\{\deg_{X_{ij}} \mu : \mu \in \mathrm{Term}(f)\}.$$

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 $\mathbb{A}^\delta$. Fix an enumeration $P_1, P_2, \ldots, P_{q^\delta}$ of $\mathbb{A}^\delta$. The map

$$\mathrm{Ev} : \mathbb{F}_q[X] \to \mathbb{F}_q^{q^\delta} \quad \text{defined by} \quad \mathrm{Ev}(f) := \big(f(P_1), \ldots, f(P_{q^\delta})\big)$$

will be referred to as the *evaluation map* of $\mathbb{F}_q[X]$. It is clear that the evaluation map Ev defined above is a surjective linear map, and also that $\mathrm{Ev}(f) = \mathrm{Ev}(\bar{f})$ for every $f \in \mathbb{F}_q[X]$. Thus, the restriction of Ev to $\mathfrak{R}(\ell,m)$ is also surjective. In fact, it is well-known that this restriction is injective as well. (See, e.g., [7, p. 11].) In other words, reduced polynomials can be identified with functions from $\mathbb{A}^\delta$ to $\mathbb{F}_q$.

Remark 1. Although the reduction map from $\mathbb{F}_q[X]$ onto $\mathfrak{R}(\ell,m)$ is $\mathbb{F}_q$-linear, it is not multiplicative, i.e., $\overline{fg}$ need not be equal to $\bar{f}\bar{g}$, in general. In fact, the product of reduced monomials need not be a reduced monomial. However, if $f, g \in \mathbb{F}_q[X]$ are polynomials in disjoint sets of variables, then $\overline{fg} = \bar{f}\bar{g}$.

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. For $0 \le i \le \ell$, let $\Delta_i(\ell,m)$ be the subset of $\mathbb{F}_q[X]$ consisting of all $i \times i$ minors of X, where, as per standard conventions, the only 0×0 minor of X is 1. For $0 \le r \le \ell$, we define

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

and $\mathcal{F}(\ell,m;r)$ to be the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q[X]$ generated by $\Delta(\ell,m;r)$. Often $\Delta(\ell,m;\ell)$ and $\mathcal{F}(\ell,m;\ell)$ will just be denoted by $\Delta(\ell,m)$ and $\mathcal{F}(\ell,m)$, respectively.

Observe that $\deg_{X_{ij}} \mathcal{M} \le 1$ for all $\mathcal{M} \in \Delta(\ell, m)$ and $(i,j) \in \mathsf{R}$. In particular, $\mathcal{F}(\ell, m) \subseteq \mathfrak{R}(\ell, m)$. Next, we record the following basic result. It is an easy consequence of Lemma 2 of [2] and its proof together with Lemma 3 of [2].

Proposition 2. *For every $r \in \{0, 1, \dots, \ell\}$, the elements of $\Delta(\ell, m; r)$ are linearly independent. In particular,*

$$\dim_{\mathbb{F}_q} \mathcal{F}(\ell, m; r) = \sum_{i=0}^{r} \binom{\ell}{i}\binom{\ell'}{i} \quad \text{and} \quad \dim_{\mathbb{F}_q} \mathcal{F}(\ell, m) = \binom{m}{\ell}.$$

Thanks to Proposition 2, every $f \in \mathcal{F}(\ell, m)$ is a unique $\mathbb{F}_q$-linear combination of the elements of $\Delta(\ell, m)$, say $f = \sum_{\mathcal{M} \in \Delta(\ell,m)} a_{\mathcal{M}} \mathcal{M}$, where $a_{\mathcal{M}} \in \mathbb{F}_q$ for every $\mathcal{M} \in \Delta(\ell, m)$. We define the *support* of f to be the set

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

Note that the support of f is the empty set if and only if f is the zero polynomial. Also note that for $0 \le r \le \ell$ and $f \in \mathcal{F}(\ell, m; r)$, the sets $\mathrm{supp}(f)$ and $\mathrm{Term}(f)$ coincide only when $r \le 1$.

For any nonnegative integer $r \le \ell$, the image of $\mathcal{F}(\ell, m; r)$ under the evaluation map Ev will be denoted by $C^{\mathbb{A}}(\ell, m; r)$ and called the *affine Grassmann code of level* r. As in [2], we will write $C^{\mathbb{A}}(\ell, m) = C^{\mathbb{A}}(\ell, m; \ell)$ and refer to this simply as the *affine Grassmann code* (corresponding to the fixed parameters ℓ and ℓ', or equivalently, ℓ and m). The following result is a consequence of Proposition 2. Its proof is similar to that of Lemma 7 of [2], and is hence omitted.

Proposition 3. *For each $r \in \{0, 1, \dots, \ell\}$, the affine Grassmann code of level r is a nondegenerate linear code of length n and dimension k_r given by* (3).

Finally, in this section we review some basic facts about generalized Reed-Muller codes, which will be useful in the sequel. First, recall that for any nonnegative integer $r \le \delta(q-1)$, the r^{th} order generalized Reed-Muller code of length q^δ, denoted $\mathrm{RM}_q(r, \delta)$ or simply $\mathrm{RM}(r, \delta)$, is the image of $\{\mu \in \mathfrak{R}(\ell, m) : \deg \mu \le r\}$ under the evaluation map Ev. Some of its fundamental properties are the following.

Proposition 4. *Let r be a nonnegative integer $\le \delta(q-1)$, and let Q, R be unique integers such that $\delta(q-1) - r = Q(q-1) + R$ and $0 \le R < q-1$. Then:*

(i) $\mathrm{RM}(r, \delta)$ *is nondegenerate linear code of length q^δ and*

$$\dim \mathrm{RM}(r, \delta) = \sum_{i=0}^{r} \sum_{j=0}^{\delta} (-1)^j \binom{\delta}{j} \binom{\delta + i - jq - 1}{i - jq}.$$

In particular, if $r \le q-1$, then the dimension of $\mathrm{RM}(r, \delta)$ is $\binom{\delta+r}{r}$.

(ii) *The minimum distance of $\mathrm{RM}(r, \delta)$ is $(R+1)q^Q$ and the number of minimum-weight codewords of $\mathrm{RM}(r, \delta)$ is given, in terms of the Gaussian binomial coefficients (defined in* (2) *above), by*

$$\begin{cases} \left(q^{\delta - Q + 1} - q^{\delta - Q}\right) \begin{bmatrix} \delta \\ Q \end{bmatrix}_q & \text{if } R = 0, \\ \\ \left(q^{\delta} - q^{\delta - Q - 1}\right) \begin{bmatrix} \delta \\ Q+1 \end{bmatrix}_q \dbinom{q}{R+1} & \text{if } R > 0. \end{cases}$$

(iii) *If $r \ge 1$, then the (permutation) automorphism group of $\mathrm{RM}(r, \delta)$ is isomorphic to the affine general linear group $\mathrm{AGL}_\delta(\mathbb{F}_q)$ of transformations $\mathbb{F}_q^\delta \to \mathbb{F}_q^\delta$ of the form $\mathbf{x} \mapsto M\mathbf{x} + \mathbf{u}$, where $M \in \mathrm{GL}_\delta(\mathbb{F}_q)$ and $\mathbf{u} \in \mathbb{F}_q^\delta$.*

(iv) *The dual of* $\mathrm{RM}(r, \delta)$ *is* $\mathrm{RM}(\delta(q-1) - r - 1, \delta)$.

(v) *Write* $q = p^t$, *where* p *is a prime number and* $t \geq 1$. *Then* $\mathrm{RM}(r, \delta)$ *is generated by its minimum-weight codewords if and only if* $\delta = 1$ *or* $t = 1$ *or* $r < p$ *or* $r > (\delta - 1)(q - 1) + p^{t-1} - 2$.

A proof of the assertions in Proposition 4 can be found, for example, in: [1, §5.4] (parts (i) and (iv)), [4] (part (ii)), [3] (part (iii)), and [5] (part (v)).

3. Minimum distance

For a positive integer $r \leq \ell$, we shall denote by $\mathcal{L}_r$ the r^{th} leading principal minor of the $\ell \times \ell'$ matrix X. In other words, $\mathcal{L}_r$ is the determinant of the submatrix of X formed by the first r rows and the first r columns. Also, we set $\mathcal{L}_0 := 1$. Often we write $\mathcal{L}_\ell$ simply as $\mathcal{L}$ and refer to it as the *leading maximal minor.*

Theorem 5. *Let* r *be a nonnegative integer* $\leq \ell$. *Then*

$$\textit{minimum distance of } C^{\mathbb{A}}(\ell, m; r) = q^\delta \prod_{i=1}^{r} \left(1 - \frac{1}{q^i}\right). \tag{5}$$

Moreover, $\mathrm{Ev}\,(\mathcal{L}_r)$ *is a minimum-weight codeword of* $C^{\mathbb{A}}(\ell, m; r)$.

Proof. Let $f \in \mathcal{F}(\ell, m; r)$ be such that $f \neq 0$. Then there is a nonnegative integer $s \leq r$ such that $\mathrm{supp}(f) \cap \Delta_s(\ell, m)$ is nonempty, but $\mathrm{supp}(f) \cap \Delta_i(\ell, m)$ is empty for each $i > s$. Choose a minor $\mathcal{M} \in \mathrm{supp}(f) \cap \Delta_s(\ell, m)$ and let Y be the corresponding $s \times s$ submatrix of X. In view of Proposition 2, any specialization $\tilde{f}$ of f, obtained by substituting arbitrary values in $\mathbb{F}_q$ for the $\delta - s^2$ variables not occurring in Y, is a nonzero linear combination of minors of Y. It follows that

$$\mathrm{w_H}\left(\mathrm{Ev}(f)\right) \geq d(s, 2s) q^{\delta - s^2},$$

where $\mathrm{w_H}(c)$ denotes the the (Hamming) weight of a codeword c and $d(s, 2s)$ denotes the minimum distance of the affine Grassmann code $C^{\mathbb{A}}(s, 2s)$ corresponding to the $s \times s$ matrix Y. Using (1) (i.e., Theorem 16 of [2]) with $\ell = \ell' = s$, we see that

$$\mathrm{w_H}\left(\mathrm{Ev}(f)\right) \geq \left(q^{s^2} \prod_{i=1}^{s} \left(1 - \frac{1}{q^i}\right)\right) q^{\delta - s^2} \geq q^\delta \prod_{i=1}^{r} \left(1 - \frac{1}{q^i}\right).$$

On the other hand, it is readily seen that $\mathcal{L}_r \in \mathcal{F}(\ell, m; r)$ and

$$\mathrm{w_H}\left(\mathrm{Ev}\left(\mathcal{L}_r\right)\right) = q^{\delta - r^2} \#\mathrm{GL}_r(\mathbb{F}_q) = q^{\delta - r^2} \prod_{j=0}^{r-1} \left(q^r - q^j\right) = q^\delta \prod_{i=1}^{r} \left(1 - \frac{1}{q^i}\right).$$

This yields (5) and also shows that $\mathrm{Ev}\,(\mathcal{L}_r)$ is a minimum-weight codeword. □

It may be tempting to believe that, as in the case of affine Grassmann codes, every minimum-weight codeword of $C^{\mathbb{A}}(\ell, m; r)$ is essentially of the form $\mathcal{L}_r$, i.e., it is equal to $\mathrm{Ev}\,(\mathcal{L}')$, where $\mathcal{L}'$ is the r^{th} leading principal minor of the $\ell \times \ell'$ matrix X', where $X' = XA^{-1} + \mathbf{u}$ for some $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ and $\mathbf{u} \in M_{\ell \times \ell'}(\mathbb{F}_q)$. However, the following example shows that if $r < \ell$, then this need not be the case even when X' is, more generally, of the form $BXA^{-1} + \mathbf{u}$, where $A, \mathbf{u}$ are as above and $B \in \mathrm{GL}_\ell(\mathbb{F}_q)$.

Example 6. Assume that $\ell \geq 2$ and let (c_{ij}) be any $\ell \times \ell'$ matrix over $\mathbb{F}_q$ of rank ≥ 2. Then some 2×2 minor of (c_{ij}) is nonzero. Consider $C^{\mathbb{A}}(\ell, m; 1) = \mathrm{RM}(1, \delta)$. We know from Reed-Muller theory (or alternatively, Remark 11 of [2]) that any linear polynomial in $\mathbb{F}_q[X]$ in which some X_{ij} occurs with a nonzero coefficient gives rise to a minimum-weight codeword. In particular, $\mathrm{Ev}(f)$ is a minimum-weight codeword of $C^{\mathbb{A}}(\ell, m; 1)$, where

$$f = \sum_{i=1}^{\ell} \sum_{j=1}^{\ell'} c_{ij} X_{ij}.$$

However, f is not the first leading principal minor of any $\ell \times \ell'$ matrix of the form $BXA + \mathbf{u}$. Indeed if this were the case for some $B = (b_{ij}) \in \mathrm{GL}_\ell(\mathbb{F}_q)$, $A = (a_{ij}) \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$, and $\mathbf{u} = (u_{ij}) \in M_{\ell \times \ell'}(\mathbb{F}_q)$, then

$$\sum_{i=1}^{\ell} \sum_{j=1}^{\ell'} c_{ij} X_{ij} = u_{11} + \sum_{i=1}^{\ell} \sum_{j=1}^{\ell'} b_{1i} X_{ij} a_{j1}.$$

Consequently, $u_{11} = 0$ and $c_{ij} = b_{1i} a_{j1}$ for $1 \le i \le \ell$ and $1 \le j \le \ell'$. But this is a contradiction since it is readily seen that every 2×2 minor of the $\ell \times \ell'$ matrix $(b_{1i} a_{j1})$ is always zero.

4. 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 S_n on $\{1, \ldots, n\}$. In this section, we shall observe that the result stated in the introduction about the automorphism groups of affine Grassmann codes being large can be extended a little further.

For any $B \in \mathrm{GL}_\ell(\mathbb{F}_q)$, $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$, and $\mathbf{u} \in M_{\ell \times \ell'}(\mathbb{F}_q)$, define

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

to be the affine transformation given by

$$\psi_{\mathbf{u},A,B}(P) = BPA^{-1} + \mathbf{u} \quad \text{ for } P = (p_{ij})_{1 \le i \le \ell,\, 1 \le j \le \ell'} \in \mathbb{A}^\delta(\mathbb{F}_q),$$

It is clear that the transformation $\psi_{\mathbf{u},A,B}$ gives a bijection of $\mathbb{A}^\delta(\mathbb{F}_q) = \{P_1, \ldots, P_n\}$ onto itself, and hence there is a unique permutation σ of $\{1, \ldots, n\}$ such that

$$(\psi_{\mathbf{u},A,B}(P_1), \ldots, \psi_{\mathbf{u},A,B}(P_n)) = \left(P_{\sigma(1)}, \ldots, P_{\sigma(n)}\right).$$

We shall denote this permutation σ by $\sigma_{\mathbf{u},A,B}$ and for any $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$, we will often write $\sigma_{\mathbf{u},A,B}(c)$ for the n-tuple $(c_{\sigma(1)}, \ldots, c_{\sigma(n)})$.

Lemma 7. *Let r be a nonnegative integer $\le \ell$ and let $B \in \mathrm{GL}_\ell(\mathbb{F}_q)$, $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$, and $\mathbf{u} \in M_{\ell \times \ell'}(\mathbb{F}_q)$. Then $\sigma_{\mathbf{u},A,B} \in \mathrm{Aut}\left(C^{\mathbb{A}}(\ell, m; r)\right)$.*

Proof. From Lemma 18 of [2] and with its proof, we know that if $f = f(X)$ is in $\mathcal{F}(\ell, m; r)$, then $f(XA^{-1} + \mathbf{u}) \in \mathcal{F}(\ell, m; r)$. Now consider the product BX and let s be any integer with $0 \le s \le r$. Observe that any $s \times s$ minor of BX is of the form $\det(B_s X^s)$, where B_s is a $s \times \ell$ submatrix of B and X^s is a $\ell \times s$ submatrix of X. Hence by the Cauchy-Binet formula (cf. [2, Lemma 10]), every $s \times s$ minor of BX is a $\mathbb{F}_q$-linear combination of $s \times s$ minors of X. Consequently, if $f \in \mathcal{F}(\ell, m; r)$, then $f(BXA^{-1} + \mathbf{u}) \in \mathcal{F}(\ell, m; r)$. Moreover,

$$\sigma_{\mathbf{u},A,B}(\mathrm{Ev}(f)) = \left(f(\psi_{\mathbf{u},A,B}(P))\right)_{P \in \mathbb{A}^\delta(\mathbb{F}_q)} = \mathrm{Ev}\left(f(BXA^{-1} + \mathbf{u})\right).$$

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

Notice that $\psi_{\mathbf{0},I_{\ell'},I_\ell}$ is the identity transformation of $\mathbb{A}^\delta$, where $\mathbf{0}$ denotes the zero matrix in $M_{\ell \times \ell'}(\mathbb{F}_q)$ and $I_{\ell'}$ (resp: I_ℓ) denotes the $\ell' \times \ell'$ (resp: $\ell \times \ell$) identity matrix over $\mathbb{F}_q$. Moreover, given any $A, A' \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$, $B, B' \in \mathrm{GL}_\ell(\mathbb{F}_q)$, and $\mathbf{u}, \mathbf{v} \in M_{\ell \times \ell'}(\mathbb{F}_q)$, we have

$$\psi_{\mathbf{u},A,B} \circ \psi_{\mathbf{v},A',B'} = \psi_{\mathbf{w},AA',BB'} \quad \text{and} \quad \psi_{\mathbf{u},A,B}^{-1} = \psi_{\mathbf{u}',A^{-1},B^{-1}}, \tag{6}$$

where $\mathbf{w} := B\mathbf{v}A^{-1} + \mathbf{u}$ and $\mathbf{u}' = -B^{-1}\mathbf{u}A$. It follows that

$$\mathfrak{H}(\ell, m) := \{\psi_{\mathbf{u},A,B} \,:\, A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q),\ B \in \mathrm{GL}_{\ell}(\mathbb{F}_q),\ \text{and } \mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)\}$$

is a group with respect to composition of maps. We determine the group structure of $\mathfrak{H}(\ell, m)$ in the following result, which is an analogue of Proposition 20 of [2].

Proposition 8. *Let $\Gamma(\ell, \ell')$ denote the factor group G/Z, where G is the direct product $\mathrm{GL}_\ell(\mathbb{F}_q) \times \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ and Z is the normal subgroup of G given by $\{(\lambda I_\ell,\ \lambda I_{\ell'}) : \lambda \in \mathbb{F}_q^*\}$. Then as a group $\mathfrak{H}(\ell, m)$ is isomorphic to the semidirect product $M_{\ell\times\ell'}(\mathbb{F}_q) \rtimes_\theta \Gamma(\ell, \ell')$, where $\theta : \Gamma(\ell, \ell') \to Aut(M_{\ell\times\ell'}(\mathbb{F}_q))$ is a group homomorphism defined by $\theta\left((B, A)Z\right)(\mathbf{u}) := B\mathbf{u}A^{-1}$.*

Proof. It is easy to check that θ is well-defined and that it is a group homomorphism. Let $\eta : M_{\ell\times\ell'}(\mathbb{F}_q)\rtimes_\theta\Gamma(\ell, \ell') \to \mathfrak{H}(\ell, m)$ be the map given by $(\mathbf{u},\ (B, A)Z) \mapsto \psi_{\mathbf{u},A,B}$. Clearly, η is well-defined and surjective. Moreover, from (6) it is readily seen that η is a group homomorphism. Finally, suppose $(\mathbf{u},\ (B, A)Z)$ is in the kernel of η for some $B \in \mathrm{GL}_\ell(\mathbb{F}_q)$, $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$, and $\mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)$. Then

$$BPA^{-1} + \mathbf{u} = P \quad \text{ for all } P \in \mathbb{A}^\delta\left(\mathbb{F}_q\right). \tag{7}$$

Taking P to be the zero matrix in (7), we obtain $\mathbf{u} = \mathbf{0}$. Next, write $B = (b_{ij})$ and $A^{-1} = (a'_{ij})$ and let us fix any $r, s \in \mathbb{Z}$ with $1 \le r \le \ell$ and $1 \le s \le \ell'$. Taking P to be the $\ell \times \ell'$ matrix E_{rs}, with 1 in $(r, s)^{\text{th}}$ spot and 0 elsewhere, in (7), we obtain

$$b_{ir}\, a'_{sj} = \begin{cases} 1 & \text{if } (i, j) = (r, s), \\ 0 & \text{if } (i, j) \neq (r, s), \end{cases} \qquad \text{for } 1 \le i \le \ell \text{ and } 1 \le j \le \ell'. \tag{8}$$

In particular, $b_{rr} \neq 0$ and $a'_{ss} \neq 0$. Now taking $j = s$ in (8), we obtain $b_{ir} = 0$ for $i \neq r$. Likewise, $a'_{sj} = 0$ for $j \neq s$. It follows that B and A^{-1} are diagonal matrices. Furthermore, thanks to (8), we have $b_{11}a'_{11} = \cdots = b_{\ell\ell}a'_{11} = 1$ and $b_{11}a'_{11} = \cdots = b_{11}a'_{\ell'\ell'} = 1$, and therefore $B = \lambda I_\ell$ and $A^{-1} = \lambda^{-1}I_{\ell'}$ for some $\lambda \in \mathbb{F}_q^*$. This shows that the coset of (B, A) in G/Z is the identity element. Thus η is an isomorphism. □

It may be noted that $C^{\mathbb{A}}(\ell, m; 0)$ is a one-dimensional code of length $n = q^\delta$ spanned by $(1, 1, \ldots, 1)$ and thus its automorphism group is the full symmetric group S_n. For affine Grassmann codes of level $r \ge 1$, one has the following partial result, which extends Theorem 21 of [2].

Theorem 9. *Let r be a positive integer $\le \ell$. Then the automorphism group of $C^{\mathbb{A}}(\ell, m; r)$ contains a subgroup isomorphic to $\mathfrak{H}(\ell, m)$. In particular,*

$$\#\mathrm{Aut}\left(C^{\mathbb{A}}(\ell, m; r)\right) \ge \frac{q^\delta}{q-1}\left(\prod_{i=0}^{\ell-1}(q^\ell - q^i)\right)\left(\prod_{j=0}^{\ell'-1}(q^{\ell'} - q^j)\right). \tag{9}$$

Proof. In view of Lemma 7, $\psi_{\mathbf{u},A,B} \mapsto \sigma_{\mathbf{u},A,B}$ gives a natural map from $\mathfrak{H}(\ell, m)$ into $\mathrm{Aut}\left(C^{\mathbb{A}}(\ell, m; r)\right)$. 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 $\sigma_{\mathbf{u},A,B}$ is the identity permutation for some $B \in \mathrm{GL}_\ell(\mathbb{F}_q)$, $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$, and $\mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)$. Then $\sigma_{\mathbf{u},A,B}(\mathrm{Ev}(f)) = \mathrm{Ev}(f)$ for all $f \in \mathcal{F}(\ell, m)$, i.e.,

$$f(BPA^{-1} + \mathbf{u}) = f(P) \quad \text{ for all } f \in \mathcal{F}(\ell, m) \text{ and all } P \in \mathbb{A}^\delta\left(\mathbb{F}_q\right).$$

By letting f vary over all possible 1×1 minors, we see that (7) holds. Hence $\psi_{\mathbf{u},A,B}$ is the identity transformation of $\mathbb{A}^\delta$. Finally, (9) follows from Proposition 8. □

Remark 10. It may be tempting to believe that Aut $\left(C^{\mathbb{A}}(\ell,m;r)\right)$ is isomorphic to $\mathfrak{H}(\ell,m)$ for any $r\geq 1$. But already when $r=1$, we know from part (iii) of Proposition 4 that Aut $\left(C^{\mathbb{A}}(\ell,m;1)\right) = \mathrm{Aut}\left(\mathrm{RM}(1,\delta)\right) \simeq \mathrm{AGL}_\delta(\mathbb{F}_q) \simeq \mathbb{F}_q^\delta \rtimes \mathrm{GL}_\delta(\mathbb{F}_q)$, and the latter is, in general, much larger that $\mathfrak{H}(\ell,m)$. Even when $r=\ell=\ell'>1$, one can see as follows that Aut $\left(C^{\mathbb{A}}(\ell,m;r)\right) = \mathrm{Aut}\left(C^{\mathbb{A}}(\ell,m)\right)$ can be larger than $\mathfrak{H}(\ell,m)$. Consider the permutation σ of S_n induced by the transpose map, i.e., $\sigma\in S_n$ such that $(P_1^T,\dots,P_n^T) = \left(P_{\sigma(1)},\dots,P_{\sigma(n)}\right)$. It is clear that the minors of X^T are minors of X, and hence σ is an automorphism of $C^{\mathbb{A}}(\ell,m)$. If σ were equal to $\sigma_{\mathbf{u},A,B}$ for some $B\in\mathrm{GL}_\ell(\mathbb{F}_q)$, $A\in\mathrm{GL}_{\ell'}(\mathbb{F}_q)$, and $\mathbf{u}\in M_{\ell\times\ell'}(\mathbb{F}_q)$, then as in the proof of Theorem 9, we obtain

$$BPA^{-1}+\mathbf{u}=P^T \quad \text{ for all } P=(p_{ij})_{1\leq i\leq \ell,\, 1\leq j\leq \ell'}\in\mathbb{A}^\delta\left(\mathbb{F}_q\right).$$

Taking P to be the zero matrix, we conclude that $\mathbf{u}=\mathbf{0}$. Further, since linear polynomials are reduced and hence determined by the corresponding $\mathbb{F}_q$-valued function on $\mathbb{A}^\delta\left(\mathbb{F}_q\right)$, we see that $BXA^{-1}=X^T$. In particular, writing $B=(b_{ij})$ and $A^{-1}=\left(a'_{ij}\right)$, we see that

$$X_{ii}=\sum_{r=1}^{\ell}\sum_{s=1}^{\ell} b_{ir}X_{rs}a'_{si} \quad \text{ for } i=1,\dots,\ell.$$

Consequently, for any $i,r,s\in\{1,\dots,\ell\}$, we obtain $b_{ii}a'_{ii}=1$ and $b_{ir}a'_{si}=0$ if $(r,s)\neq(i,i)$. This, in turn, implies that B and A^{-1} are diagonal matrices. But then the $(i,j)^{\text{th}}$ entry of BXA^{-1} is $b_{ii}X_{ij}a'_{jj}$, which can not always be X_{ji} since $\ell>1$. This shows that σ does not belong the subgroup of Aut $\left(C^{\mathbb{A}}(\ell,m)\right)$ corresponding to $\mathfrak{H}(\ell,m)$. At any rate, the complete determination of $\mathrm{Aut}(C^{\mathbb{A}}(\ell,m))$ and more generally, Aut $\left(C^{\mathbb{A}}(\ell,m;r)\right)$ for $1<r\leq\ell$, remains an open question.

5. Duality

In this section we shall explicitly determine the dual of any affine Grassmann code and compute its minimum distance. Let us begin by observing that the monomial

$$\mathsf{F}:=\prod_{(i,j)\in\mathsf{R}}X_{ij}^{q-1}=\prod_{i=1}^{\ell}\prod_{j=1}^{\ell'}X_{ij}^{q-1}$$

is reduced and that $\mu\in\mathbb{M}(\ell,m)$ is a reduced monomial if and only if μ divides F. We may refer to F as the *full product*. Note that for $0\leq r\leq\ell$,

$$\dim\mathfrak{R}(\ell,m)=\#\,\overline{\mathbb{M}}(\ell,m)=\sum_{s=0}^{\ell}\binom{\delta}{s}(q-1)^s=q^\delta=\text{length}\left(C^{\mathbb{A}}(\ell,m;r)\right)$$

and also that

$$\dim C^{\mathbb{A}}(\ell,m;r)^\perp = n-\dim C^{\mathbb{A}}(\ell,m;r)=q^\delta-\sum_{i=0}^{r}\binom{\ell}{i}\binom{\ell'}{i}. \tag{10}$$

The usual "inner product" on $\mathbb{F}_q^{q^\delta}$ corresponds to the symmetric bilinear form $\langle\ ,\ \rangle$ on the $\mathbb{F}_q$-linear space $\mathfrak{R}(\ell,m)$ given by

$$\langle f,g\rangle:=\sum_{P\in\mathbb{A}^\delta}f(P)g(P)=\sum_{P\in\mathbb{A}^\delta}fg(P)=\sum_{P\in\mathbb{A}^\delta}\overline{fg}(P), \quad \text{ for } f,g\in\mathfrak{R}(\ell,m).$$

The dual of $C^{\mathbb{A}}(\ell,m;r)$ corresponds, via the $\mathbb{F}_q$-linear isomorphism $f\mapsto\mathrm{Ev}(f)$ of $\mathfrak{R}(\ell,m)\to\mathbb{F}_q^{q^\delta}$, to the subspace

$$\{f\in\mathfrak{R}(\ell,m):\langle f,\mathcal{M}\rangle=0 \text{ for all } \mathcal{M}\in\Delta(\ell,m;r)\} \tag{11}$$

of $\mathfrak{R}(\ell, m)$. We shall now proceed to determine an explicit $\mathbb{F}_q$-basis of this subspace. The first step is to recall the following well-known result (cf. [4, Lem. 1.6]).

Proposition 11. *Let $\mu \in \overline{\mathbb{M}}(\ell, m)$ be a reduced monomial. Then*

$$\sum_{P \in \mathbb{A}^\delta} \mu(P) = \begin{cases} 0 & \text{if } \mu \neq \mathsf{F}, \\ (-1)^\delta & \text{if } \mu = \mathsf{F}. \end{cases}$$

We have noted in Remark 1 that $\overline{fg}$ need not be equal to $\bar{f}\bar{g}$ for arbitrary $f, g \in \mathbb{F}_q[X]$. The following useful lemma shows what is the best that we can do in a special case.

Lemma 12. *Let $\mu, \nu \in \overline{\mathbb{M}}(\ell, m)$ be such that $\overline{\mu\nu} = \mathsf{F}$. Then there is a divisor ν' of ν such that $\mu\nu' = \mathsf{F}$. Moreover, if ν is squarefree and if $q > 2$, then $\mu\nu = \mathsf{F}$.*

Proof. For $(i, j) \in \mathsf{R}$, let $\alpha_{ij} = \deg_{X_{ij}} \mu$ and $\beta_{ij} = \deg_{X_{ij}} \nu$. Since μ and ν are reduced, it follows that

$$\deg_{X_{ij}} \overline{\mu\nu} = \begin{cases} \alpha_{ij} + \beta_{ij} & \text{if } \alpha_{ij} + \beta_{ij} \leq q - 1, \\ \alpha_{ij} + \beta_{ij} - q + 1 & \text{if } \alpha_{ij} + \beta_{ij} \geq q. \end{cases}$$

On the other hand, since $\overline{\mu\nu} = \mathsf{F}$, we see that $\alpha_{ij} + \beta_{ij} \geq q - 1$ for all $(i, j) \in \mathsf{R}$. Hence $\nu' := \prod_{(i,j) \in \mathsf{R}} X_{ij}^{q-1-\alpha_{ij}}$ is a divisor of ν and it clearly satisfies $\mu\nu' = \mathsf{F}$. Finally, suppose ν is squarefree and $q > 2$, but $\nu' \neq \nu$. Then there is a variable X_{ij} that divides ν, but not ν'. Now since $\mu\nu' = \mathsf{F}$, we see that $\deg_{X_{ij}} \mu = q - 1$. But then $\deg_{X_{ij}} \mu\nu = q$, which contradicts the assumption that $\overline{\mu\nu} = \mathsf{F}$, since $q > 2$. $\square$

Given any nonnegative integer $r \leq \ell$, define

$$\overline{\mathrm{FM}}(\ell, m; r) := \left\{ \frac{\mathsf{F}}{t} : t \in \mathrm{Term}(\mathcal{M}) \text{ for some } \mathcal{M} \in \Delta(\ell, m; r) \right\}.$$

It is clear that elements of $\overline{\mathrm{FM}}(\ell, m; r)$ are reduced monomials; we shall refer to them as *forbidden monomials* with respect to the affine Grassmann code of level r. This terminology is justified by the following result.

Lemma 13. *Let r be a nonnegative integer $\leq \ell$ and let $\mu \in \overline{\mathbb{M}}(\ell, m)$ be such that $\mu \notin \overline{\mathrm{FM}}(\ell, m; r)$. Then $\mathrm{Ev}(\mu) \in C^{\mathbb{A}}(\ell, m; r)^\perp$.*

Proof. Let $\mathcal{M} \in \Delta(\ell, m; r)$ and let $t \in \mathrm{Term}(\mathcal{M})$. Now $\overline{\mu t}$ is reduced and if it were equal to F, then by Lemma 12, $\mu = \mathsf{F}/t'$ for some divisor t' of t. But this contradicts the assumption that $\mu \notin \overline{\mathrm{FM}}(\ell, m; r)$ because the divisor of a term of a minor in $\Delta(\ell, m; r)$ is also a term of a minor in $\Delta(\ell, m; r)$. Thus, in view of Proposition 11, we obtain $\langle \mu, t \rangle = \sum_{P \in \mathbb{A}^\delta} \overline{\mu t}(P) = 0$. Consequently, μ is in the subspace of $\mathfrak{R}(\ell, m)$ given by (11), and so $\mathrm{Ev}(\mu) \in C^{\mathbb{A}}(\ell, m; r)^\perp$. $\square$

Already, we have enough information to show that affine Grassmann codes are almost always self-orthogonal. More precisely, we have the following.

Theorem 14. *Let r be a nonnegative integer $\leq \ell$. Then the affine Grassmann code $C^{\mathbb{A}}(\ell, m; r)$ of level r is self-orthogonal if and only if $(\ell, m; r; q)$ is different from $(1, 2; 1; 2)$, $(1, 2; 1; 3)$ and $(1, 3; 1; 2)$.*

Proof. First, if $r = 0$, then $C^{\mathbb{A}}(\ell, m; r)$ is the one-dimensional code spanned by the all 1-vector $(1, 1, \dots, 1)$ in $\mathbb{F}_q^{q^\delta}$ and this is clearly self-orthogonal. Now suppose $r \geq 1$. Observe that if $\mu \in \overline{\mathrm{FM}}(\ell, m; r)$ is any forbidden monomial, then

$$\deg \mu \geq \deg \mathsf{F} - r \geq \deg \mathsf{F} - \ell = [(q - 1)\ell' - 1]\,\ell \geq [(q - 1)\ell' - 1]\,r.$$

In particular, if $(q-1)\ell' > 2$, then no reduced monomial of degree $\le r$ is forbidden. On the other hand, $C^{\mathbb{A}}(\ell, m; r)$ is spanned by the evaluations of minors of size $\le r$, which, in turn, are $\mathbb{F}_q$-linear combinations of reduced monomials of degree $\le r$. Hence by Lemma 13, we can conclude that $C^{\mathbb{A}}(\ell, m; r) \subseteq C^{\mathbb{A}}(\ell, m; r)^{\perp}$ when $(q-1)\ell' > 2$. Now suppose $(q-1)\ell' \le 2$. Since $1 \le r \le \ell \le \ell'$, the only possible values of $(\ell, \ell'; r; q)$ are $(1,1;1;2)$, $(1,1;1;3)$, $(1,2;1;2)$, and $(2,2;2;2)$. For the first 3 values, one finds $\dim C^{\mathbb{A}}(\ell, m; r) > \dim C^{\mathbb{A}}(\ell, m; r)^{\perp}$, and hence $C^{\mathbb{A}}(\ell, m; r)$ is not self-orthogonal in these cases. When $r = \ell = \ell' = q = 2$, the code $C^{\mathbb{A}}(\ell, m; r)$ is spanned by the evaluations of $1, X_{11}, X_{12}, X_{21}, X_{22}$ and the minor $B := X_{11}X_{22} + X_{12}X_{21}$. The first 5 are non-forbidden reduced monomials; hence by Lemma 13, they are in $C^{\mathbb{A}}(\ell, m; r)^{\perp}$. A direct verification shows that $\langle B, B\rangle = 0$, since $q = 2$. Thus $C^{\mathbb{A}}(\ell, m; r)$ is self-orthogonal when $r = \ell = \ell' = q = 2$. □

Although the non-forbidden monomials give rise to linearly independent elements of the dual of an affine Grassmann code, they fail to span it. To extend these to a basis, one needs to add certain binomials such as the polynomial B in the proof of Theorem 14. A general definition of these binomials is given below.

First, let us introduce some notation, which will be useful in the sequel. For any nonnegative integer $r \le \ell$, denote, as usual, by S_r the set of all permutations of $\{1, \dots, r\}$. Further, given any $r \times r$ minor $\mathcal{M}$ of X and any $\sigma \in \mathrm{S}_r$, denote by $\mathsf{t}_\sigma(\mathcal{M})$ the *signed term* of $\mathcal{M}$ corresponding to the permutation σ. For example, $\mathsf{t}_\sigma(\mathcal{L}_r) = \mathrm{sgn}(\sigma) X_{1\sigma(1)} \cdots X_{r\sigma(r)}$, where $\mathcal{L}_r$ is the r^{th} leading principal minor of X. We will denote by ϵ the identity permutation and, by abuse of language, regard it as an element of S_r for every nonnegative integer r. In particular, for any minor $\mathcal{M}$ of X, the corresponding signed term $\mathsf{t}_\epsilon(\mathcal{M})$ is precisely the product of the variables on the principal diagonal of the submatrix corresponding to $\mathcal{M}$. Define

$$\mathsf{B}_{\mathcal{M},\sigma} := \frac{\mathsf{F}}{\mathsf{t}_\epsilon(\mathcal{M})} - \frac{\mathsf{F}}{\mathsf{t}_\sigma(\mathcal{M})} \quad \text{for } \mathcal{M} \in \Delta_r(\ell, m) \text{ and } \sigma \in \mathrm{S}_r.$$

Clearly, $\mathsf{B}_{\mathcal{M},\sigma} = 0$ if $\sigma = \epsilon$ and in particular, if $r \le 1$. If $r \ge 2$ and if σ is a non-identity permutation, then $\mathsf{B}_{\mathcal{M},\sigma}$ is a reduced polynomial with exactly two terms, each of which is a forbidden monomial up to a sign. We may refer to $\mathsf{B}_{\mathcal{M},\sigma}$ as the *binomial* corresponding to the minor $\mathcal{M}$ and the permutation σ.

Lemma 15. *Let i, r be integers such that $0 \le i \le r \le \ell$, and let $\mathcal{M} \in \Delta_i(\ell, m)$ and $\sigma \in \mathrm{S}_i$. Then $\mathrm{Ev}\,(\mathsf{B}_{\mathcal{M},\sigma}) \in C^{\mathbb{A}}(\ell, m; r)^{\perp}$.*

Proof. Clearly, it suffices to show that $\langle \mathsf{B}_{\mathcal{M},\sigma}, \mathcal{N}\rangle = 0$ for all $\mathcal{N} \in \Delta(\ell, m; r)$. So let us fix some $j \times j$ minor $\mathcal{N}$ of X, where $j \le r$. Also let π denote a permutation of $\{1, \dots, j\}$. We will distinguish two cases.

Case 1: $q > 2$. Since $\mathrm{sgn}(\pi)\mathsf{t}_\pi(\mathcal{N})$ is a squarefree monomial, it follows from Lemma 12 that $\overline{(\mathsf{F}/\mathsf{t}_\sigma(\mathcal{M}))\,\mathsf{t}_\pi(\mathcal{N})} = \pm\mathsf{F}$ only when $\mathsf{t}_\sigma(\mathcal{M}) = \pm\mathsf{t}_\pi(\mathcal{N})$, which, in turn, is possible only when $i = j$, $\mathcal{M} = \mathcal{N}$, and $\sigma = \pi$. Consequently, in view of Proposition 11, we see that $\langle \mathsf{B}_{\mathcal{M},\sigma}, \mathcal{N}\rangle = 0$ if $\mathcal{N} \ne \mathcal{M}$, whereas

$$\langle \mathsf{B}_{\mathcal{M},\sigma}, \mathcal{M}\rangle = \sum_{\pi \in \mathrm{S}_j} \langle \mathsf{B}_{\mathcal{M},\sigma}, \mathsf{t}_\pi(\mathcal{M})\rangle = \mathrm{sgn}(\epsilon)^2(-1)^\delta - \mathrm{sgn}(\sigma)^2(-1)^\delta = 0.$$

Case 2: $q = 2$. In this case it follows from Lemma 12 that $\overline{(\mathsf{F}/\mathsf{t}_\sigma(\mathcal{M}))\,\mathsf{t}_\pi(\mathcal{N})} = \mathsf{F}$ only when $\mathsf{t}_\sigma(\mathcal{M})$ divides $\mathsf{t}_\pi(\mathcal{N})$. Further, if Y denotes the $j \times j$ submatrix of X corresponding to the minor $\mathcal{N}$, then it is readily seen that $\mathsf{t}_\sigma(\mathcal{M})$ divides $\mathsf{t}_\pi(\mathcal{N})$ if and only if $i \le j$, $\mathcal{M} = \det Y'$, and $\sigma = \pi'$, where Y' is an $i \times i$ submatrix of Y and π' is the restriction to π to $\{1, \dots, i\}$. Consequently, in view of Proposition 11, we see that $\langle \mathsf{F}/\mathsf{t}_\sigma(\mathcal{M}), \mathsf{t}_\pi(\mathcal{N})\rangle = 1$ for precisely $(j-i)!$ permutations $\pi \in \mathrm{S}_j$ obtained by extending σ to $\{1,\dots,j\}$ by permuting $i+1,\dots,j$ randomly. It follows that

$$\langle \mathsf{B}_{\mathcal{M},\sigma},\, \mathcal{N}\rangle = 2(j-i)! = 0.$$

This completes the proof. Consequently, in view of Proposition 11, we obtain $\langle \mathsf{B}_{\mathcal{M},\sigma},\, \mathcal{N}\rangle = 0$ if $\mathcal{N} \neq \mathcal{M}$, while

$$\langle \mathsf{B}_{\mathcal{M},\sigma},\, \mathcal{M}\rangle = \sum_{\pi\in \mathrm{S}_j} \langle \mathsf{B}_{\mathcal{M},\sigma},\, \mathsf{t}_\pi(\mathcal{M})\rangle = \operatorname{sgn}(\epsilon)^2(-1)^\delta - \operatorname{sgn}(\sigma)^2(-1)^\delta = 0.$$

□

We are now ready to describe an explicit basis for $C^{\mathbb{A}}(\ell,m;r)^\perp$. In fact, this is given by the non-forbidden monomials and the binomials. More precisely, for a nonnegative integer $r \le \ell$, we let

$$\mathcal{B}(\ell,m;r) := \left(\overline{\mathbb{M}}(\ell,m)\setminus \overline{\mathrm{F}\mathbb{M}}(\ell,m;r)\right) \cup \left(\bigcup_{i=0}^{r} \{\mathsf{B}_{\mathcal{M},\sigma} : \mathcal{M}\in\Delta_i(\ell,m) \text{ and } \sigma\in \mathrm{S}_i^*\}\right),$$

where $\mathrm{S}_i^* := \mathrm{S}_i \setminus \{\epsilon\}$ is the set of non-identity permutations of $\{1,\dots,i\}$; also let

$$\mathcal{F}^*(\ell,m;r) := \mathbb{F}_q\text{-linear span of } \mathcal{B}(\ell,m;r).$$

Note that $\mathcal{F}^*(\ell,m;r)$ is a subspace of $\mathfrak{R}(\ell,m)$ and, in particular, it is $\mathbb{F}_q$-isomorphic to its image in $\mathbb{F}_q^{q^\delta}$ under the evaluation map. Now we have the following explicit description of the dual of an affine Grassmann code of any given level.

Theorem 16. *$C^{\mathbb{A}}(\ell,m;r)^\perp = \mathrm{Ev}\left(\mathcal{F}^*(\ell,m;r)\right)$ for $0 \le r \le \ell$.*

Proof. Fix a nonnegative integer $r \le \ell$. Let us first show that the elements of $\mathcal{B}(\ell,m;r)$ are linearly independent. Suppose

$$\sum_{\mu} a_\mu \mu + \sum_{i=0}^{r} \sum_{\mathcal{M}\in\Delta_i(\ell,m)} \sum_{\sigma\in \mathrm{S}_i^*} b_{i,\sigma,\mathcal{M}}\, \mathsf{B}_{\mathcal{M},\sigma} = 0,$$

for some $a_\mu,\, b_{i,\sigma,\mathcal{M}} \in \mathbb{F}_q$, where μ varies over $\overline{\mathbb{M}}(\ell,m)\setminus \overline{\mathrm{F}\mathbb{M}}(\ell,m;r)$. Then

$$\sum_{\mu} a_\mu \mu + \sum_{i=2}^{r} \sum_{\mathcal{M}\in\Delta_i(\ell,m)} \sum_{\sigma\in \mathrm{S}_i} b_{i,\sigma,\mathcal{M}}\, \frac{\mathsf{F}}{\mathsf{t}_\sigma(\mathcal{M})} = 0, \tag{12}$$

where, for $2 \le i \le r$ and $\mathcal{M}\in\Delta_i(\ell,m)$, we have put $b_{i,\epsilon,\mathcal{M}} := -\sum_{\sigma\in \mathrm{S}_i^*} b_{i,\sigma,\mathcal{M}}$. Now observe that (12) is a linear combination of distinct monomials. Hence we must have $a_\mu = 0$ and $b_{i,\sigma,\mathcal{M}} = 0$ for all relevant parameters μ, i, σ, and $\mathcal{M}$.

To complete the proof, it suffices to show that the cardinality of $\mathcal{B}(\ell,m;r)$ coincides with the dimension of the subspace of $\mathfrak{R}(\ell,m)$ given by (11). To this end, let us first note that a forbidden monomial is completely determined by an $i\times i$ minor of X and by one of its $i!$ terms. Since X has exactly $\binom{\ell}{i}\binom{\ell'}{i}$ minors, we see that

$$\#\overline{\mathbb{M}}(\ell,m)\setminus \overline{\mathrm{F}\mathbb{M}}(\ell,m;r) = q^\delta - \sum_{i=0}^{r} i!\binom{\ell}{i}\binom{\ell'}{i}.$$

On the other hand, the binomials are determined by an $i\times i$ minor of X and a non-identity permutation of $\{1,\dots,i\}$. Thus,

$$\#\bigcup_{i=0}^{r} \{\mathsf{B}_{\mathcal{M},\sigma} : \mathcal{M}\in\Delta_i(\ell,m) \text{ and } \sigma\in \mathrm{S}_i^*\} = \sum_{i=0}^{r} (i!-1)\binom{\ell}{i}\binom{\ell'}{i}.$$

Combining the last two equations, we see that $\#\mathcal{B}(\ell,m;r)$ is the expression on the right in (10), as desired. □

We shall now proceed to determine the minimum distance of the dual of an affine Grassmann code. As a warm-up, it may be noted that the Singleton bound shows already that for any nonnegative integer $r \le \ell$,

$$d\left(C^{\mathbb{A}}(\ell, m; r)^{\perp}\right) \le 1 + \sum_{i=0}^{r} \binom{\ell}{i}\binom{\ell'}{i} \le 1 + \binom{m}{\ell}.$$

This indicates that the minimum distance is rather small and it does not grow with q. In the trivial case $r = 0$, we obtain 2 as an upper bound, and it is readily seen that this is attained. Indeed, $C^{\mathbb{A}}(\ell, m; 0)$ is the one-dimensional code of length q^{δ} spanned by $(1, 1, \dots, 1)$ and its dual contains no codeword of weight 1. Another trivial case is when $q = 2$ and $r = \ell = \ell' = 1$. In this case, $C^{\mathbb{A}}(1, 2; 1) = \mathbb{F}_2^2$, while $C^{\mathbb{A}}(1, 2; 1)^{\perp} = \{\mathbf{0}\}$. Barring these, it will be seen below that the minimum distance is always 3 or 4.

Theorem 17. *Let r be a positive integer $\le \ell$. Then the minimum distance of the q-ary code $C^{\mathbb{A}}(\ell, m; r)^{\perp}$ is given by*

$$d\left(C^{\mathbb{A}}(\ell, m; r)^{\perp}\right) = \begin{cases} 3 & \text{if } q > 2, \\ 4 & \text{if } q = 2 \text{ and } \ell' > 1. \end{cases}$$

Moreover, if $q > 2$ and if a_1, a_2 are any distinct elements of $\mathbb{F}_q^*$, then $\mathrm{Ev}\left(g_{a_1,a_2}\right)$ *is a minimum-weight codeword of $C^{\mathbb{A}}(\ell, m; r)^{\perp}$, where*

$$g_{a_1,a_2} := \frac{1}{(X_{\ell\ell'} - a_1)(X_{\ell\ell'} - a_2)} \prod_{(i,j)\in \mathsf{R}} \left(X_{ij}^{q-1} - 1\right). \tag{13}$$

On the other hand, if $q = 2$ and $\ell' > 1$, then there are distinct $(i_1, j_1), (i_2, j_2) \in \mathsf{R}$ such that $i_1 = i_2$ or $j_1 = j_2$, and moreover for any such $(i_1, j_1), (i_2, j_2)$, if we let

$$h := \frac{\mathsf{F}}{X_{i_1 j_1} X_{i_2 j_2}}. \tag{14}$$

then $\mathrm{Ev}(h)$ *is a minimum-weight codeword of $C^{\mathbb{A}}(\ell, m; r)^{\perp}$.*

Proof. Let us assume that either $q > 2$ or that $q = 2$ and $\ell' > 1$. This ensures that $\delta(q-1) - 2 \ge 0$. Now, observe that every element of $\mathcal{B}(\ell, m; r)$ is either a reduced monomial of degree $\le \delta(q-1) - 2$ or a difference of two reduced monomials of degree $\le \delta(q-1) - 2$. Hence it follows from Theorem 16 that $C^{\mathbb{A}}(\ell, m; r)^{\perp}$ is a subcode of the generalized Reed-Muller code $\mathrm{RM}\left(\delta(q-1) - 2,\, \delta\right)$. Consequently, from part (ii) of Proposition 4, we see that

$$d\left(C^{\mathbb{A}}(\ell, m; r)^{\perp}\right) \ge d\left(\mathrm{RM}\left(\delta(q-1) - 2,\, \delta\right)\right) = \begin{cases} 3 & \text{if } q > 2, \\ 4 & \text{if } q = 2 \text{ and } \ell' > 1. \end{cases}$$

To complete the proof, it suffices to show that the evaluations of (13) and (14) give codewords of (Hamming) weight 3 and 4, respectively.

To begin with, suppose $q > 2$ and let a_1, a_2 be any distinct elements of $\mathbb{F}_q^*$. Since $X^{q-1} - 1 = \prod_{a \in \mathbb{F}_q^*}(X - a)$, it is clear that g_{a_1,a_2} defined by (13) is in $\mathbb{F}_q[X]$ and is, in fact, a reduced polynomial. Moreover, $\deg_{X_{\ell\ell'}} g_{a_1,a_2} \le q - 3$. On the other hand, since the terms of any minor are squarefree monomials, every forbidden monomial $\mu \in \overline{\mathrm{FM}}(\ell, m; r)$ must satisfy $\deg_{X_{ij}} \mu \ge q-2$ for all $i = 1, \dots, \ell$ and $j = 1, \dots, \ell'$. It follows that g_{a_1,a_2} is a $\mathbb{F}_q$-linear combination of non-forbidden reduced monomials and in particular, it is in $\mathcal{F}^*(\ell, m; r)$. Moreover, if $P = (p_{ij}) \in \mathbb{A}^{\delta}(\mathbb{F}_q)$, then $g_{a_1,a_2}(P) \ne 0$ if and only if $p_{ij} = 0$ for all $(i, j) \ne (\ell, \ell')$ and $p_{\ell\ell'} \in \{0, a_1, a_2\}$. Thus we conclude that $\mathrm{Ev}\left(g_{a_1,a_2}\right)$ is a codeword of $C^{\mathbb{A}}(\ell, m; r)^{\perp}$ of weight 3.

Next, suppose $q = 2$ and $\ell' > 1$. The existence of distinct $(i_1, j_1), (i_2, j_2) \in \mathsf{R}$ such that $i_1 = i_2$ or $j_1 = j_2$ is obvious; for example, we can take $i_1 = i_2 = \ell$, $j_1 = \ell' - 1$

and $j_2 = \ell'$. Moreover, for any such $(i_1, j_1), (i_2, j_2) \in \mathsf{R}$, the monomial $X_{i_1j_1}X_{i_2j_2}$ contains two variables from the same row or from the same column, and hence it can never be the term of any minor of X. Consequently, the reduced monomial h defined by (14) is non-forbidden and $\mathrm{Ev}(h)$ is a codeword of $C^{\mathbb{A}}(\ell, m; r)^{\perp}$. Furthermore, if $P = (p_{ij}) \in \mathbb{A}^{\delta}(\mathbb{F}_q)$, then $h(P) \neq 0$ if and only if $p_{ij} = 1$ for all $(i, j) \in \mathsf{R}$ different from (i_1, j_1) and (i_2, j_2). Thus we conclude that $\mathrm{Ev}(h)$ is of weight 4. □

6. Generation by Minimum-weight Codewords

In this section we will show that the affine Grassmann codes as well as their duals have the property that the codewords of minimum weight generate the code. The case of affine Grassmann codes is easy and in fact, it is shown below that the result holds more generally for affine Grassmann codes of any level.

Proposition 18. *Let r be a nonnegative integer $\leq \ell$. Then the minimum-weight codewords of $C^{\mathbb{A}}(\ell, m; r)$ generate $C^{\mathbb{A}}(\ell, m; r)$.*

Proof. The code $C^{\mathbb{A}}(\ell, m; r)$ is generated by $\mathrm{Ev}(\mathcal{M})$ as $\mathcal{M}$ varies over the $i \times i$ minors of X for $0 \leq i \leq r$. We proceed by decreasing induction on i $(0 \leq i \leq r)$ to show that $\mathrm{Ev}(\mathcal{M})$ is in the $\mathbb{F}_q$-linear span of minimum-weight codewords of $C^{\mathbb{A}}(\ell, m; r)$ for every $i \times i$ minor $\mathcal{M}$ of X. To begin with, if $i = r$, then $\mathcal{M}$ is the r^{th} leading principal minor of $Y := BXA$ for some permutation matrices $B \in \mathrm{GL}_{\ell}(\mathbb{F}_q)$ and $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$. Hence Lemma 7 shows that $\mathrm{Ev}(\mathcal{M})$ differs from $\mathrm{Ev}(\mathcal{L}_r)$ by an automorphism of $C^{\mathbb{A}}(\ell, m; r)$; consequently, by Theorem 5, $\mathrm{Ev}(\mathcal{M})$ is itself a minimum-weight codeword of $C^{\mathbb{A}}(\ell, m; r)$. Now, suppose $i < r$ and the result holds for the $(i+1) \times (i+1)$ minors of X. Let $a_1, \dots, a_i$ and $b_1, \dots, b_i$ denote, respectively, the row and column indices of X corresponding to the $i \times i$ minor $\mathcal{M}$. Since $i < r$, we can choose a row index α distinct from $a_1, \dots, a_i$ and a column index β distinct from $b_1, \dots, b_i$. Consider $X' = X + \mathbf{u}$, where $\mathbf{u}$ is the $\ell \times \ell'$ matrix whose $(\alpha, \beta)^{\text{th}}$ entry is 1 and all other entries are 0. Let $\mathcal{N}$ (resp: $\mathcal{N}'$) be the $(i+1) \times (i+1)$ minor of X (resp: X') corresponding to the row indices $a_1, \dots, a_i, \alpha$ and column indices $b_1, \dots, b_i, \beta$. Observe that $\mathcal{M} = \mathcal{N}' - \mathcal{N}$. From the induction hypothesis together with Lemma 7, it follows that both $\mathrm{Ev}(\mathcal{N})$ and $\mathrm{Ev}(\mathcal{N}')$ are in the $\mathbb{F}_q$-linear span of minimum-weight codewords of $C^{\mathbb{A}}(\ell, m; r)$ and therefore, so is $\mathrm{Ev}(\mathcal{M})$. □

Remark 19. Affine Grassmann codes are closely related to Grassmann codes, and this connection was explained in Section VII of [2]. We remark here that a result analogous to Proposition 18 holds for Grassmann codes as well. To see this, it suffices to note that by a result of Nogin (see, e.g., [6, Cor. 19]), the minimum-weight codewords of the Grassmann code $C(\ell, m)$ correspond precisely to the decomposable elements in the exterior power $\wedge^{m-\ell}\mathbb{F}_q^m$ and evidently, these decomposable elements span the corresponding function space $\mathcal{G}(\ell, m) = (\wedge^{\ell}\mathbb{F}_q^m)^* \simeq \wedge^{m-\ell}\mathbb{F}_q^m$.

As indicated in the Introduction, an analogous result for the dual of $C^{\mathbb{A}}(\ell, m; r)$ is not true, in general. However, the minimum-weight codewords of $C^{\mathbb{A}}(\ell, m)^{\perp}$ do generate $C^{\mathbb{A}}(\ell, m)^{\perp}$. In other words, a result analogous to Proposition 18 holds for the duals of affine Grassmann codes (of level ℓ). This, in fact, seems much harder to prove and we will need a number of auxiliary results, which will be spread over the next three subsections. The first subsection contains lemmas of a general nature concerning generating sets and bases for certain spaces of polynomials. Next, we show that the evaluations of certain non-forbidden monomials with respect to $C^{\mathbb{A}}(\ell, m; r)$ are generated by the minimum-weight codewords. Finally, the binomials in $\mathcal{B}(\ell, m; r)$ are dealt with in the last subsection, where we conclude with the main result of this section. Wherever possible, we will consider affine Grassmann codes of an arbitrary level so as to make it clear what works in general and what goes wrong when $r < \ell$ as opposed to $r = \ell$.

Before proceeding with generalities, and as a warm-up, let us consider the case of $r = 0$. Here $C^{\mathbb{A}}(\ell, m; 0)$ is the one-dimensional code of length $n := q^{\delta}$ spanned by $(1, 1, \ldots, 1)$ and $C^{\mathbb{A}}(\ell, m; 0)^{\perp} = \{(c_1, \ldots, c_n) \in \mathbb{F}_q^n : c_1 + \cdots + c_n = 0\}$. Thus, if $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ denotes the standard basis of $\mathbb{F}_q^n$, then $\mathbf{e}_1 - \mathbf{e}_2, \ldots, \mathbf{e}_1 - \mathbf{e}_n$ are minimum-weight codewords and these clearly generate $C^{\mathbb{A}}(\ell, m; 0)^{\perp}$.

6.1. **Generators and Bases.** Let T be an indeterminate over $\mathbb{F}_q$ and d a nonnegative integer. Denote by $\mathbb{F}_q[T]$ the space of polynomials in T with coefficients in $\mathbb{F}_q$, and by $\mathbb{F}_q[T]_{\le d}$ the subspace of polynomials in $\mathbb{F}_q[T]$ of degree $\le d$. Also, denote by $M_d[T]$ the set of monic polynomials in $\mathbb{F}_q[T]$ of degree d having d distinct roots in $\mathbb{F}_q$.

Lemma 20. *Assume that $d < q$. Then $M_d[T]$ spans $\mathbb{F}_q[T]_{\le d}$.*

Proof. Since $d < q$, we can choose distinct elements $a_1, \ldots, a_{d+1}$ from $\mathbb{F}_q$. The $d+1$ polynomials

$$p_i(T) := \prod_{\substack{1 \le j \le d+1 \\ j \ne i}} (T - a_j) \quad \text{for } i = 1, \ldots, d+1,$$

are elements of $M_d[T]$. Moreover, they are linearly independent, since a relation $\sum_j \beta_j p_j(T) = 0$ implies, after substituting a_i for T, that $\beta_i = 0$ for $i = 1, \ldots, d+1$. Since $M_d[T] \subset \mathbb{F}_q[T]_{\le d}$ and $\dim_{\mathbb{F}_q} \mathbb{F}_q[T]_{\le d} = d + 1$, the lemma follows. $\square$

Corollary 21. *$M_{q-1}[T] = \{(T - \alpha)^{q-1} - 1 : \alpha \in \mathbb{F}_q\}$ and moreover, $M_{q-1}[T]$ is a $\mathbb{F}_q$-basis of $\mathbb{F}_q[T]_{\le q-1}$.*

Proof. For each $\alpha \in \mathbb{F}_q$, the polynomial $(T - \alpha)^{q-1} - 1$ is clearly monic of degree $q - 1$ and its roots are precisely the elements $\beta \in \mathbb{F}_q$ with $\beta \ne \alpha$. It follows that $M_{q-1}[T] = \{(T - \alpha)^{q-1} - 1 : \alpha \in \mathbb{F}_q\}$. In particular, $\#M_{q-1}[T] = q = \dim \mathbb{F}_q[T]_{\le q-1}$. Hence by Lemma 20, $M_{q-1}[T]$ is a $\mathbb{F}_q$-basis of $\mathbb{F}_q[T]_{\le q-1}$. $\square$

Remark 22. For $0 \le d < q$, the set $M_d[T]$ is a basis of $\mathbb{F}_q[T]_{\le d}$ if and only if $d = 0$ or $d = q - 1$. The case $d = 0$ is trivial whereas $d = q - 1$ was noted above. For the converse, it suffices to observe that $\#M_d[T] = \binom{q}{d} \ge q > d + 1$ when $1 \le d < q - 1$. In general, for $0 \le d < q$, upon letting $e = q - 1 - d$, one can write

$$M_d[T] = \left\{ \frac{(T - \alpha)^{q-1} - 1}{(T - a_1) \cdots (T - a_e)} : \alpha, a_1, \ldots, a_e \text{ distinct elements of } \mathbb{F}_q \right\}. \tag{15}$$

This representation is particularly useful for large values of d. It may be noted, however, that for a given polynomial in $M_d[T]$, the corresponding $\alpha \in \mathbb{F}_q$ and the e-element subset $\{a_1, \ldots, a_e\}$ of $\mathbb{F}_q \setminus \{\alpha\}$ is not unique.

We now derive a multivariable analogue of Lemma 20. To this end, let s be a positive integer and $T_1, \ldots, T_s$ independent indeterminates over $\mathbb{F}_q$, and let $d_1, \ldots, d_s$ be nonnegative integers. Denote by $\mathbb{F}_q[T_1, \ldots, T_s]$ the space of polynomials in $T_1, \ldots, T_s$ with coefficients in $\mathbb{F}_q$ and by $\mathbb{F}_q[T_1, \ldots, T_s]_{\le (d_1, \ldots, d_s)}$ the subspace of polynomials $f \in \mathbb{F}_q[T_1, \ldots, T_s]$ with $\deg_{X_j} f \le d_j$ for $j = 1, \ldots, s$. Also, let

$$M_{(d_1, \ldots, d_s)}[T_1, \ldots, T_s] = \left\{ \prod_{i=1}^{s} f_i(T_i) \ : \ f_i(T_i) \in M_{d_i}[T_i] \text{ for } i = 1, \ldots, s \right\}.$$

Lemma 23. *Assume that $d_i < q$ for $i = 1, \ldots, s$. Then $M_{(d_1, \ldots, d_s)}[T_1, \ldots, T_s]$ spans $\mathbb{F}_q[T_1, \ldots, T_s]_{\le (d_1, \ldots, d_s)}$.*

Proof. $\mathbb{F}_q[T_1,\dots,T_s]_{\le(d_1,\dots,d_s)}$ is generated by monomials of the form $T_1^{e_1}\cdots T_s^{e_s}$ with $0\le e_i\le d_i$ for $i=1,\dots,s$, and by Lemma 20, each factor $T_i^{e_i}$ of such a monomial is a $\mathbb{F}_q$-linear combination of elements of $M_{d_i}[T_i]$. $\square$

As in Remark 22, it may be noted that $M_{(d_1,\dots,d_s)}[T_1,\dots,T_s]$ is a basis of $\mathbb{F}_q[T_1,\dots,T_s]_{\le(d_1,\dots,d_s)}$ if and only if $d_1=\cdots=d_s=0$ or $d_1=\cdots=d_s=q-1$. In particular, $M_{(q-1,\dots,q-1)}[T_1,\dots,T_s]$ is a basis of the space $\mathbb{F}_q[T_1,\dots,T_s]_{\le(q-1,\dots,q-1)}$ of all reduced polynomials in $T_1,\dots,T_s$ with coefficients in $\mathbb{F}_q$. The following lemma gives several other bases for this space. As in Section 2, for any $f\in\mathbb{F}_q[T_1,\dots,T_s]$, we denote by $\overline{f}$ the reduced polynomial in $\mathbb{F}_q[T_1,\dots,T_s]$ corresponding to f. Note that if $L\in\mathbb{F}_q[T_1,\dots,T_s]$ is a homogeneous linear polynomial, i.e., if $L=a_1T_1+\cdots+a_sT_s$ for some $a_1,\dots,a_s\in\mathbb{F}_q$, then $\overline{L}=L$. In particular, L can be identified with the functional $\mathbb{F}_q^s\to\mathbb{F}_q$ that maps $w=(w_1,\dots,w_s)\in\mathbb{F}_q^s$ to $L(w)=a_1w_1+\cdots+a_sw_s$.

Lemma 24. *Let $\{L_i : 1\le i\le s\}\subseteq\mathbb{F}_q[T_1,\dots,T_s]$ be a set of s linearly independent homogeneous linear polynomials. Then the set*

$$\mathfrak{L}:=\left\{\overline{L_1^{e_1}\cdots L_s^{e_s}} : 0\le e_i\le q-1 \text{ for } i=1,\dots,s\right\}$$

is a basis of $\mathbb{F}_q[T_1,\dots,T_s]_{\le(q-1,\dots,q-1)}$.

Proof. Since the linear polynomials $L_1,\dots,L_s$ are linearly independent, the map given by $w\mapsto(L_1(w),\dots,L_s(w))$ is a $\mathbb{F}_q$-linear isomorphism of $\mathbb{F}_q^s$ onto $\mathbb{F}_q^s$. Hence given any $v\in\mathbb{F}_q^s$, there exists $w_v\in\mathbb{F}_q^s$ such that $(L_1(w_v),\dots,L_s(w_v))=v$. Now let a relation $\sum_{e_1,\dots,e_s}\alpha_{e_1,\dots,e_s}\overline{L_1^{e_1}\cdots L_s^{e_s}}=0$ be given, where $\alpha_{e_1,\dots,e_s}\in F$ for all $e_1,\dots e_s$ (with $0\le e_i\le q-1$ for $i=1,\dots,s$). Evaluating the given relation at w_v, we find $\sum_{e_1,\dots,e_s}\alpha_{e_1,\dots,e_s}\alpha_{e_1,\dots,e_s}v_1^{e_1}\cdots v_s^{e_s}=0$. Consequently, the polynomial $\sum_{e_1,\dots,e_s}\alpha_{e_1,\dots,e_s}\alpha_{e_1,\dots,e_s}T_1^{e_1}\cdots T_s^{e_s}$ vanishes at all points of $\mathbb{F}_q^s$. Since $0\le e_i\le q-1$ for $i=1,\dots,s$, this is only possible if $\alpha_{e_1,\dots,e_s}=0$ for all $e_1,\dots,e_s$. Thus, $\mathfrak{L}$ is linearly independent. Finally, since $\#\,\mathfrak{L}=q^s=\dim_{\mathbb{F}_q}\mathbb{F}_q[T_1,\dots,T_s]_{\le(q-1,\dots,q-1)}$, the lemma is proved. $\square$

6.2. **Non-forbidden monomials.** Let us fix a positive integer $r\le\ell$. From Theorem 16, we know that $C^{\mathbb{A}}(\ell,m;r)^\perp=\mathrm{Ev}\left(\mathcal{F}^*(\ell,m;r)\right)$, where $\mathcal{F}^*(\ell,m;r)$ is the space spanned by the non-forbidden monomials and the binomials, or more precisely, by $\mathcal{B}(\ell,m;r)$. Let $\mathcal{F}^*_{\min}(\ell,m;r)$ denote the set of all $f\in\mathcal{F}^*(\ell,m;r)$ such that $\mathrm{Ev}(f)$ is a minimum-weight codeword of $C^{\mathbb{A}}(\ell,m;r)^\perp$, and let $\langle\mathcal{F}^*_{\min}(\ell,m;r)\rangle$ denote the subspace of $\mathcal{F}^*(\ell,m;r)$ spanned by $\mathcal{F}^*_{\min}(\ell,m;r)$.

We begin with a useful characterization of the non-forbidden monomials. To this end, let us first make a definition. We say that a reduced monomial $\mu\in\overline{\mathbb{M}}(\ell,m)$ is *maximal non-forbidden* with respect to $C^{\mathbb{A}}(\ell,m;r)$ if

$$\text{(i) } \mu=\frac{\mathsf{F}}{t}\quad\text{for some } t\in\mathrm{Term}\,(\mathcal{M})\ \text{ and } \mathcal{M}\in\Delta_{r+1}(\ell,m), \tag{16}$$

or if there are $(i_1,j_1),(i_2,j_2)\in\mathsf{R}$ such that

$$\text{(ii) } \mu=\frac{\mathsf{F}}{X_{i_1j_1}X_{i_2j_2}}\quad\text{with } i_1=i_2 \text{ or } j_1=j_2. \tag{17}$$

It may be noted that in (ii) above, the possibility $(i_1,j_1)=(i_2,j_2)$ is not excluded except when $q=2$, in which case it is automatically excluded since μ is a monomial to begin with. It may also be noted that when $r=\ell$, i.e., in the case of affine Grassmann codes, possibility (i) does not arise at all, whereas when $r=1$, we can combine (i) and (ii) to simply say that μ is a reduced monomial of degree $\delta(q-1)-2$. The terminology in the above definition is justified by the following.

Lemma 25. *A reduced monomial in $\overline{\mathbb{M}}(\ell,m)$ is non-forbidden with respect to $C^{\mathbb{A}}(\ell,m;r)$ if and only if it divides some maximal non-forbidden monomial with respect to $C^{\mathbb{A}}(\ell,m;r)$.*

Proof. For a monomial $\mu \in \mathbb{M}(\ell,m)$ and for $1 \le i \le \ell$ and $1 \le j \le \ell'$, let us denote by μ_i the i^{th} row-degree of μ (i.e., the number of variables, counting multiplicities, from the i^{th} row of X appearing in μ) and by μ^j the j^{th} column-degree of μ. Observe that a monomial $\mu \in \mathbb{M}(\ell,m)$ is a term of a minor of size $\le r$, i.e., $\mu \in \mathrm{Term}(\mathcal{M})$ for some $\mathcal{M} \in \Delta(\ell,m;r)$, if and only if $\deg(\mu) \le r$, $\mu_i \le 1$ for all $i = 1,\dots,\ell$ and $\mu^j \le 1$ for all $j = 1,\dots,\ell'$. Hence if $\mu \in \overline{\mathbb{M}}(\ell,m)$ is a reduced monomial, then

$$\mu \text{ is forbidden} \Leftrightarrow \deg(\mu) \ge \delta(q-1)-r,\ \mu_i \ge \delta(q-1)-1\ \forall\, i,\ \text{ and } \mu^j \ge \delta(q-1)-1\ \forall j.$$

In other words, a reduced monomial $\mu \in \overline{\mathbb{M}}(\ell,m)$ is non-forbidden with respect to $C^{\mathbb{A}}(\ell,m;r)$ if and only if (a) $\deg(\mu) \le \delta(q-1)-(r+1)$, or (b) $\mu_i \le \ell'(q-1)-2$ for some $i \in \{1,\dots,\ell\}$, or (c) $\mu^j \le \ell(q-1)-2$ for some $j \in \{1,\dots,\ell'\}$. To conclude, it suffices to observe that for any $\mu \in \overline{\mathbb{M}}(\ell,m)$, we have the following. If μ divides a monomial satisfying (16), then (a) holds. On the other hand, if (a) holds but neither (b) nor (c) holds, then μ divides a monomial satisfying (16). Finally, μ divides a monomial satisfying (17) if and only if (b) or (c) holds. $\square$

We will now proceed to show that non-forbidden monomials of type (ii), i.e., those that divide a maximal non-forbidden monomial given by (17), are generated by the minimum-weight codewords. In what follows we will tacitly use the obvious fact that the (permutation) automorphisms of a code and its dual are identical and that minimum-weight codewords are always preserved by an automorphism. Furthermore, we will make frequent use of the automorphisms of $C^{\mathbb{A}}(\ell,m;r)$ given by Lemma 7, i.e., the automorphisms induced by the transformation $X \mapsto BXA+\mathbf{u}$, where $B \in \mathrm{GL}_\ell(\mathbb{F}_q)$, $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ and $\mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)$. It is convenient to treat the binary and the non-binary cases separately.

Lemma 26. *Assume that $q=2$ and $\ell' > 1$. Suppose $\mu \in \overline{\mathbb{M}}(\ell,m)$ is as in* (17) *and $\nu \in \overline{\mathbb{M}}(\ell,m)$ divides μ. Then $\nu \in \langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle$.*

Proof. First, observe that $\mu \in \mathcal{F}^*_{\min}(\ell,m;r)$, thanks to Theorem 17. We use (finite) induction on $d := \deg(\mu/\nu) = \deg(\mu) - \deg(\nu)$ to show that $\nu \in \langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle$. If $d=0$, then $\nu=\mu$ and there is nothing to prove. Assume that $d>0$ and the result holds for smaller values of d. Since $d>0$, there is a variable X_{ij} that divides μ/ν. Write $\nu' = \nu X_{ij}$. By induction hypothesis $\nu' \in \langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle$. Hence the polynomial, say f', obtained from ν' when X is changed to $X+\mathbf{u}$ is in $\langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle$ for every $\mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)$. Now take $\mathbf{u}$ to be the $\ell\times\ell'$ matrix whose $(i,j)^{\text{th}}$ entry is 1 and all other entries are zero. Then $f' = \nu' + \nu$, and so $\nu \in \langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle$. $\square$

Lemma 27. *Assume that $q>2$. If $f \in \mathfrak{R}(\ell,m)$ is such that $\deg_{X_{ij}} f \le q-3$ for some $(i,j) \in \mathsf{R}$, then $f \in \langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle$.*

Proof. Applying an automorphism induced by $X \mapsto BXA$, where $B \in \mathrm{GL}_\ell(\mathbb{F}_q)$ and $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ are suitable permutation matrices, we may assume, without loss of generality, that $(i,j) = (\ell,\ell')$. In view of Corollary 21, Remark 22 and Lemma 23, we see that the space $\mathbb{F}_q[X]_{\le(q-1,q-1,\dots,q-1,q-3)}$ of all reduced polynomials of degree $\le q-3$ in the last variable $X_{\ell\ell'}$ is spanned by the products of the form

$$\frac{1}{(X_{\ell\ell'}-a_1)(X_{\ell\ell'}-a_2)} \prod_{(i,j)\in\mathsf{R}} (X_{ij}-\alpha_{ij})^{q-1} - 1,$$

where α_{ij} vary over $\mathbb{F}_q$ and a_1, a_2 vary over $\mathbb{F}_q \setminus \{\alpha_{\ell\ell'}\}$. But these products are precisely of the form (13) up to an automorphism induced by $X \mapsto X+\mathbf{u}$, where $\mathbf{u} \in M_{\ell\times\ell'}(\mathbb{F}_q)$. Hence from Theorem 17, we obtain the desired result. $\square$

The above lemma shows that if $q > 2$ and if a reduced monomial ν divides a maximal non-forbidden monomial of the form F/X_{ij}^2 for some $(i,j) \in \mathsf{R}$, then ν is generated by minimum-weight codewords of $C^{\mathbb{A}}(\ell,m;r)^{\perp}$. This covers, in particular, the case when $\ell' = 1$ (so that $r = \ell = 1$). It only remains to consider the case of reduced monomials dividing maximal non-forbidden monomials of the form $\mathsf{F}/X_{i_1j_1}X_{i_2j_2}$, where $(i_1,j_1),(i_2,j_2)$ are distinct elements of R and where $q > 2$.

Lemma 28. *Assume that $q > 2$ and $\ell' > 1$. Suppose μ is a maximal non-forbidden monomial of the form $\mathsf{F}/X_{i_1j_1}X_{i_2j_2}$, where $(i_1,j_1),(i_2,j_2)$ are distinct elements of R such that $i_1 = i_2$ or $j_1 = j_2$. Then every divisor of μ is in $\langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle$.*

Proof. First, suppose $i_1 = i_2$. Applying an automorphism induced by $X \mapsto BXA$, where $B \in \mathrm{GL}_\ell(\mathbb{F}_q)$ and $A \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ are suitable permutation matrices, we can and will assume that $\mu = \mathsf{F}/X_{\ell\ell'-1}X_{\ell\ell'}$. Let $\mathsf{R}' := \mathsf{R}\setminus\{(\ell,\ell'-1),(\ell,\ell')\}$ and let

$$\nu(X) = \prod_{(i,j)\in\mathsf{R}'} X_{ij}^{e_{ij}} \qquad (0 \le e_{ij} \le q-1)$$

be any reduced monomial in the $\ell\ell'-2$ variables $\{X_{ij} : (i,j)\in\mathsf{R}'\}$. By Lemma 27, $\nu(X)X_{\ell\ell'-1}^{q-3}X_{\ell\ell'}^{q-1} \in \langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle$. Consider the $\ell\times\ell'$ matrix $Y = (Y_{ij})$ obtained from X by adding the $(\ell'-1)^{\text{th}}$ column to the last column (so that for $1 \le i \le \ell$, $Y_{ij} = X_{ij}$ if $1 \le j < \ell'$ and $Y_{i\ell'} = X_{i\ell'-1} + X_{i\ell'}$). Clearly Y is obtained from X upon multiplication by an elementary matrix in $\mathrm{GL}_{\ell'}(\mathbb{F}_q)$ on the right, and hence $X \mapsto Y$ induces an automorphism of $C^{\mathbb{A}}(\ell,m;r)$. Consequently, the corresponding reduced polynomial is generated by the minimum-weight codewords, i.e.,

$$\overline{\nu(Y)X_{\ell\ell'-1}^{q-3}\left(X_{\ell\ell'-1}+X_{\ell\ell'}\right)^{q-1}} \in \langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle \quad \text{where} \quad \nu(Y) = \prod_{(i,j)\in\mathsf{R}'} Y_{ij}^{e_{ij}}.$$

Now since $\nu(Y)$ and $X_{\ell\ell'-1}^{q-3}\left(X_{\ell\ell'-1}+X_{\ell\ell'}\right)^{q-1}$ are polynomials in disjoint sets of variables, in view of Remark 1 and the binomial theorem, the polynomial

$$\sum_{t=0}^{q-1} \overline{\nu(Y)}\binom{q-1}{t}\overline{X_{\ell\ell'-1}^{q-3+t}X_{\ell\ell'}^{q-1-t}}$$

is in $\langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle$. Moreover, by Lemma 27, each term in the above expansion, except possibly the term corresponding to $t = 1$, is in $\langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle$. It follows therefore that the the term corresponding to $t = 1$ is also in $\langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle$. In other words, $\overline{\nu(Y)}X_{\ell\ell'-1}^{q-2}X_{\ell\ell'}^{q-2} \in \langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle$. Finally, since the Y_{ij}, $(i,j)\in\mathsf{R}'$, are clearly linearly independent, it follows from Lemma 24 that polynomials of the form $\overline{\nu(Y)}$ form a basis of the space of reduced polynomials in $\{X_{ij} : (i,j)\in\mathsf{R}'\}$. Hence we conclude that any divisor of μ is in $\langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle$. The case when $j_1 = j_2$ is proved similarly. □

Corollary 29. *Every non-forbidden monomial with respect to $C^{\mathbb{A}}(\ell,m)$ is in the $\mathbb{F}_q$-linear span of minimum-weight codewords of $C^{\mathbb{A}}(\ell,m)$.*

Proof. We have noted already that when $r = \ell$, the only maximal non-forbidden monomials with respect to $C^{\mathbb{A}}(\ell,m;r)$ are those of type (ii), i.e., those given by (17). Hence the desired result follows from Lemmas 25, 26, 27, and 28. □

6.3. **Binomials.** Fix a positive integer $r \le \ell$. Recall that the basis $\mathcal{B}(\ell,m;r)$ of $C^{\mathbb{A}}(\ell,m;r)^{\perp}$ consists of the non-forbidden monomials with respect to $C^{\mathbb{A}}(\ell,m;r)$ and the binomials

$$\mathsf{B}_{\mathcal{M},\sigma} := \frac{\mathsf{F}}{\mathsf{t}_\epsilon(\mathcal{M})} - \frac{\mathsf{F}}{\mathsf{t}_\sigma(\mathcal{M})},$$

where $\mathcal{M}$ varies over the minors of X with $\deg(\mathcal{M}) \le r$ and σ varies over the nonidentity permutations of $\{1,2,\ldots,\deg(\mathcal{M})\}$. The two monomials appearing in such a binomial are forbidden and therefore do not correspond to a codeword of $C^{\mathbb{A}}(\ell,m;r)^\perp$. However, the binomials themselves correspond to codewords of $C^{\mathbb{A}}(\ell,m;r)^\perp$, and we will show that they are generated by the minimum-weight codewords. We begin with an elementary algebraic observation, which will be useful in the sequel.

Lemma 30. *Let x,y,z,w be independent indeterminates over $\mathbb{F}_q$. Consider the polynomial $f=(zw)^{q-2}(x+z)^{q-1}(y+w)^{q-1}$. Also let*

$$\mathsf{F}_0 := (xyzw)^{q-1} \quad \text{and} \quad \mathsf{B}_0 := \frac{\mathsf{F}_0}{xw}+\frac{\mathsf{F}_0}{yz}. \tag{18}$$

Then the reduced polynomial corresponding to f is given by

$$\bar{f} = \frac{\mathsf{F}_0}{zw}+\frac{\mathsf{F}_0}{xy} - \mathsf{B}_0 + h,$$

where $h\in\mathbb{F}_q[x,y,z,w]$ is a reduced polynomial such that every $\mu\in\mathrm{Term}(h)$ satisfies $\deg_x \mu \le q-3$ or $\deg_y \mu \le q-3$.

Proof. Expanding $(x+z)^{q-1}$ and $(y+w)^{q-1}$ by the binomial theorem, we see that

$$\bar{f} = \sum_{s=0}^{q-1}\sum_{t=0}^{q-1}\binom{q-1}{s}\binom{q-1}{t}\overline{x^{q-1-s}z^{q-2+s}y^{q-1-t}w^{q-2+t}}.$$

Considering separately the terms in the double summation above corresponding to $(s,t)=(0,0),(1,0),(0,1)$ and $(1,1)$, and upon letting h denote the sum of the remaining terms, we readily obtain the desired result. $\square$

Lemma 31. *Assume that $r>1$. Let ρ be an integer such that $1<\rho\le r$ and let $\mathcal{M}\in\Delta_\rho(\ell,m)$. If $\sigma,\tau\in S_\rho$ are such that $\sigma^{-1}\tau$ is a transposition, then*

$$\frac{\mathsf{F}}{\mathsf{t}_\sigma(\mathcal{M})} - \frac{\mathsf{F}}{\mathsf{t}_\tau(\mathcal{M})} \in \langle \mathcal{F}^*_{\min}(\ell,m;r)\rangle .$$

Proof. Applying an automorphism induced by $X\mapsto BXA$, where $B\in \mathrm{GL}_\ell(\mathbb{F}_q)$ and $A\in\mathrm{GL}_{\ell'}(\mathbb{F}_q)$ are suitable permutation matrices, we may assume that $\mathcal{M}=\mathcal{L}_\rho$, i.e., $\mathcal{M}$ is the ρ^{th} leading principal minor of X. Next, by a similar trick, we may assume that σ is the identity permutation and τ is a transposition in S_ρ, say (st). Let us denote the indeterminates X_{ss}, X_{st}, X_{ts} and X_{tt} by x,y,z and w, respectively. Also let $\mathsf{R}' := \mathsf{R}\setminus\{(s,s),(s,t),(t,s),(t,t)\}$. With these simplifications and notations,

$$\frac{\mathsf{F}}{\mathsf{t}_\sigma(\mathcal{M})} - \frac{\mathsf{F}}{\mathsf{t}_\tau(\mathcal{M})} = \mathsf{B}_0 \prod_{(i,j)\in\mathsf{R}'} X_{ij}^{q-1}, \tag{19}$$

where B_0 is as in (18). On the other hand, by Lemmas 26 and 28, any divisor of F/zw is in $\langle\mathcal{F}^*_{\min}(\ell,m;r)\rangle$. In particular, $(zw)^{q-2}(xy)^{q-1}\nu(X)\in\langle\mathcal{F}^*_{\min}(\ell,m;r)\rangle$ for any reduced monomial $\nu(X)$ in the $\ell\ell'-4$ variables $\{X_{ij}:(i,j)\in\mathsf{R}'\}$. Now if $Z=(Z_{ij})$ is the $\ell\times\ell'$ matrix obtained from X by adding the t^{th} row to the s^{th} row, then $X\mapsto Z$ induces an automorphism of $C^{\mathbb{A}}(\ell,m;r)$ and therefore in view of Remark 1,

$$\overline{\left((zw)^{q-2}(x+z)^{q-1}(y+w)^{q-1}\right)}\,\overline{\nu(Z)} \in \langle\mathcal{F}^*_{\min}(\ell,m;r)\rangle .$$

Moreover, by Lemma 24, the reductions $\overline{\nu(Z)}$ form a basis of the space of reduced polynomials in $\{X_{ij}:(i,j)\in\mathsf{R}'\}$. Consequently, $\overline{\nu(Z)}$ can be replaced by an arbitrary reduced monomial in $\{X_{ij}:(i,j)\in\mathsf{R}'\}$, and, in particular, by $\prod_{(i,j)\in\mathsf{R}'}X_{ij}^{q-1}$.

This, in view of Lemma 30, shows that

$$\frac{\mathsf{F}}{zw} + \frac{\mathsf{F}}{xy} - \left(\mathsf{B}_0 \prod_{(i,j)\in \mathsf{R}'} X_{ij}^{q-1} \right) + H \in \langle \mathcal{F}^*_{\min}(\ell, m; r) \rangle \,, \tag{20}$$

where $H \in \mathbb{F}_q[X]$ is a reduced polynomial each of whose term has X_{ss}-degree or X_{st}-degree $\leq q-3$. By Lemmas 26 and 28, the first two terms in the above sum are in $\langle \mathcal{F}^*_{\min}(\ell, m; r) \rangle$ and moreover, so is H, thanks to Lemma 27. It is now clear that (19) and (20) yield the desired result. $\square$

An application of a classical result concerning permutations now yields the main result of this subsection.

Lemma 32. *Let ρ be a nonnegative integer $\leq r$ and let $\mathcal{M} \in \Delta_\rho(\ell, m)$ and $\sigma \in S_\rho$. Then the binomial $\mathsf{B}_{\mathcal{M},\sigma}$ is in $\langle \mathcal{F}^*_{\min}(\ell, m; r) \rangle$.*

Proof. If $\rho \leq 1$, then σ is necessarily the identity permutation ϵ and $\mathsf{B}_{\mathcal{M},\sigma} = 0$. Now assume that $\rho > 1$ and $\sigma \neq \epsilon$. Then σ is a nonempty product of transpositions in S_ρ, say $\sigma = \tau_1\tau_2\cdots\tau_t$. Define $\sigma_0 := \epsilon$ and $\sigma_i = \tau_1\tau_2\cdots\tau_i$ for $1 \leq i \leq t$. Then $\sigma_{i-1}^{-1}\sigma_i$ is a transposition for $1 \leq i \leq t$, and hence using Lemma 31, we see that

$$\mathsf{B}_{\mathcal{M},\sigma} = \frac{\mathsf{F}}{\mathsf{t}_\epsilon(\mathcal{M})} - \frac{\mathsf{F}}{\mathsf{t}_\sigma(\mathcal{M})} = \sum_{i=1}^{t} \frac{\mathsf{F}}{\mathsf{t}_{\sigma_{i-1}}(\mathcal{M})} - \frac{\mathsf{F}}{\mathsf{t}_{\sigma_i}(\mathcal{M})}$$

is in $\langle \mathcal{F}^*_{\min}(\ell, m; r) \rangle$. $\square$

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

Theorem 33. *$C^{\mathbb{A}}(\ell, m)^\perp$ is generated by its minimum-weight codewords.*

Proof. Follows from Corollary 29 and Lemma 32. $\square$

In the discussion before §6.1, we have noted that $C^{\mathbb{A}}(\ell, m; 0)^\perp$ is generated by its minimum-weight codewords. Moreover, analyzing the proofs of the results in this section, it can be seen that $C^{\mathbb{A}}(\ell, m; 1)^\perp$ is generated by its minimum-weight codewords. It is, however, easier to derive the result for $C^{\mathbb{A}}(\ell, m; 1)^\perp = \mathrm{RM}(1, \delta)^\perp = \mathrm{RM}(\delta(q-1)-2,\, \delta)$ directly from Theorem 33 as shown below.

Corollary 34. *For any positive integer d, the Reed-Muller codes $\mathrm{RM}(1, d)$ and $\mathrm{RM}(d(q-1)-2,\, d)$ are linear codes generated by their minimum-weight codewords.*

Proof. Taking $r = \ell = 1$ and $\ell' = d$ in Proposition 18, we see that $\mathrm{RM}(1, d)$ is generated by its minimum-weight codewords. Moreover taking $\ell = 1$ and $\ell' = d$ in Theorem 33, we see that $C^{\mathbb{A}}(1, d+1)^\perp = \mathrm{RM}(1, d)^\perp = \mathrm{RM}(d(q-1)-2,\, d)$ is generated by its minimum-weight codewords. $\square$

Remark 35. For the intermediate levels, generation by minimum-weight codewords is not true, in general. More precisely, if $1 < r < \ell$, then the minimum-weight codewords of $C^{\mathbb{A}}(\ell, m; r)^\perp$ need not generate $C^{\mathbb{A}}(\ell, m; r)^\perp$. For example, if $\ell = \ell' = 3$ and $q = r = 2$, then the affine Grassmann code $C^{\mathbb{A}}(3, 6; 2)$ is a $[512, 19, 192]$-code, while its dual is a $[512, 493, 4]$-code, and a computer verification shows that the number of codewords of weight 4 in $C^{\mathbb{A}}(3, 6; 2)^\perp$ and $C^{\mathbb{A}}(3, 6; 3)^\perp$ is the same! Hence the minimum-weight codewords of $C^{\mathbb{A}}(3, 6; 2)^\perp$ just generate $C^{\mathbb{A}}(3, 6; 3)^\perp$. In general, we have

$$C^{\mathbb{A}}(\ell, m)^\perp = C^{\mathbb{A}}(\ell, m; \ell)^\perp \subset C^{\mathbb{A}}(\ell, m; \ell-1)^\perp \subset \cdots \subset C^{\mathbb{A}}(\ell, m; 2)^\perp \subset C^{\mathbb{A}}(\ell, m; 1)^\perp$$

and it seems plausible that for $1 < r < \ell$, the minimum of weight codewords of $C^{\mathbb{A}}(\ell, m; r)^\perp$ generate the smallest of these codes, namely, $C^{\mathbb{A}}(\ell, m)^\perp$. In fact, the results of this section seem to show that the binomials and the non-forbidden monomials of type (ii) are generated by the minimum-weight codewords of $C^{\mathbb{A}}(\ell, m; r)^{\perp}$ for *any* $r = 1, \dots, \ell$. In particular, they are generated by the minimum-weight codewords of $C^{\mathbb{A}}(\ell, m)^{\perp}$. The difficulty arises due to maximal non-forbidden monomials of type (i), i.e., those given by (16). At any rate, a complete determination of the minimum-weight codewords of duals of affine Grassmann codes of any level and of the space generated by them could be an interesting problem.

Acknowledgments

We are grateful to the Otto Mønsted Foundation, which supported the visit of Sudhir Ghorpade to the Technical University of Denmark during May-July 2010 when some of this work was carried out.

References

[1] E. F. Assmus Jr. and J. D. Key, *Designs and their Codes*, Cambridge: Cambridge University Press, 1992.

[2] P. Beelen, S. R. Ghorpade, and T. Høholdt, "Affine Grassmann codes", *IEEE Trans. Information Theory*, vol. 56, pp. 3166–3176, 2010.

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

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

[5] P. Ding and J. D. Key, "Minimum-weight codewords as generators of generalized Reed-Muller codes", *IEEE Trans. Information Theory*, vol. 46, pp. 2152–2158, 2000.

[6] 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.

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

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

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

[10] V. Pless and W. C. Huffman (Eds.), *Handbook of Coding Theory*, Vols. I and II, Amsterdam: Elsevier, 1998.

Department of Mathematics, Technical University of Denmark,
DK 2800, Lyngby, Denmark.
E-mail address: p.beelen@mat.dtu.dk

Department of Mathematics, Indian Institute of Technology Bombay,
Powai, Mumbai 400076, India.
E-mail address: srg@math.iitb.ac.in

Department of Mathematics, Technical University of Denmark,
DK 2800, Lyngby, Denmark.
E-mail address: T.Hoeholdt@mat.dtu.dk