J. Algeb. Combinatorics **4** (1995), 295–316

Some p-ranks Related to Orthogonal Spaces

Aart Blokhuis[1] and G. Eric Moorhouse[2]

Abstract. We determine the p-rank of the incidence matrix of hyperplanes of $PG(n, p^e)$ and points of a nondegenerate quadric. This yields new bounds for ovoids and the size of caps in finite orthogonal spaces. In particular, we show the nonexistence of ovoids in $O^+_{10}(2^e)$, $O^+_{10}(3^e)$, $O_9(5^e)$, $O^+_{12}(5^e)$ and $O^+_{12}(7^e)$. We also give slightly weaker bounds for more general finite classical polar spaces. Another application is the determination of certain explicit bases for the code of $PG(2, p)$ using secants, or tangents and passants, of a nondegenerate conic.

Keywords: p-rank, quadric, ovoid, code

1. Introduction

Let F be a finite field of order $q = p^e$ where p is prime. Choose a nondegenerate quadric of $PG(n, F)$, denoted by $\mathcal{Z}(Q)$, the zero set of a nondegenerate quadratic form Q, as defined in Section 2. Let $P_1, P_2, \ldots, P_s$ denote the points of $\mathcal{Z}(Q)$, where $s = s(Q)$ is given by Lemma 2.2 below; and let $P_{s+1}, \ldots, P_m$ be the remaining points of $PG(n, F)$, where $m = \left[{n+1 \atop 1}\right]_q = (q^{n+1} - 1)/(q - 1)$. Denote the tangent hyperplanes to the quadric by $H_i = P_i^\perp$ for $i = 1, 2, \ldots, s$, where $\perp$ denotes orthogonal 'perp' relative to Q, and denote the remaining hyperplanes by $H_{s+1}, \ldots, H_m$. Then we have a partition of the point-hyperplane incidence matrix for $PG(n, F)$ given by

$$A = \big(a_{ij} \,:\, 1 \le i, j \le m\big) = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

where $a_{ij} = 0$ or 1 according as $P_i \notin H_j$ or $P_i \in H_j$. Here, for example, $A_1 = \big(A_{11}\ A_{12}\big)$ consists of the first s rows of A, and the upper-left $s \times s$ submatrix A_{11} is symmetric. The following result, which by today is well-known, originates from numerous independent sources; see Goethals and Delsarte [5], MacWilliams and Mann [9], and Smith [12]. See

[1] Dept. of Mathematics and Computing Science, Eindhoven University of Technology, Eindhoven, The Netherlands.

[2] Dept. of Mathematics, University of Wyoming, Laramie WY, U.S.A. The second author gratefully acknowledges the hospitality of the Eindhoven University of Technology where this research was conducted.

also [3] for a treatment closer in spirit to ours, or [1] for more details and related results and discussion.

1.1 Theorem. $\operatorname{rank}_p A = \binom{p+n-1}{n}^e + 1\,.$

Here rank_p denotes the rank in characteristic p. In Section 2 we prove the following related result.

1.2 Theorem. *Let $n \geq 2$. Then*

(i) $\operatorname{rank}_p A_1 = \left[\binom{p+n-1}{n} - \binom{p+n-3}{n}\right]^e + 1\,.$

(ii) If q and n are both even, then $\operatorname{rank}_p A_{11} = n^e + 1$.

Note that for n odd, conclusion (i) is remarkably independent of whether the quadric $\mathcal{Z}(Q)$ is of hyperbolic or elliptic type. Also note that the binomial coefficient $\binom{p+n-3}{n}$ vanishes when $p=2$, so that if q is even and n is odd, we have $\operatorname{rank}_2 A_1 = (n+1)^e + 1$. Theorem 1.2(ii) is a trivial consequence of Theorem 1.1; see Lemma 2.1. Our proof of Theorem 1.2(i) relies on the following Nullstellensatz: If f is a homogeneous polynomial of degree at most $q-1$ in $n+1$ indeterminates, where $n \geq 3$, and if f vanishes on a nondegenerate quadric $\mathcal{Z}(Q)$, then Q divides f. Actually we prove a slightly stronger form of this statement; see Theorem 2.11.

In Section 3 we make some remarks concerning the representations of the orthogonal group on the codes of A_1 and A_{11}.

An application of these results to caps and ovoids is given in Section 4. Recall (cf. [7], [8], [14]) that a *cap* on a quadric $\mathcal{Z}(Q)$ is a set of points on $\mathcal{Z}(Q)$, no two of which lie on a line of $\mathcal{Z}(Q)$. A *generator* of $\mathcal{Z}(Q)$ is a projective subspace of $PG(n, F)$ contained in $\mathcal{Z}(Q)$, which is maximal among such subspaces. An *ovoid* on $\mathcal{Z}(Q)$ is a cap $\mathcal{O}$ such that every generator of the quadric contains a (necessarily unique) point of $\mathcal{O}$. Examples of such ovoids are known for $n \leq 7$, and they abound for $n \leq 5$. The question of whether such ovoids can exist for $n \geq 8$ remains unsettled. An elementary consequence of Theorem 1.2 is that for any p, there exists an upper bound on n such that a nondegenerate quadric $\mathcal{Z}(Q) \subset PG(n, q)$ may admit an ovoid. We stress the remarkable fact that this bound depends only on p, the characteristic of the field. This we see immediately from the following results.

1.3 Theorem. *If $\mathcal{S}$ is any cap on a nondegenerate quadric in $PG(n,q)$, where $q=p^e$, then $|\mathcal{S}| \le \left[\binom{p+n-1}{n} - \binom{p+n-3}{n}\right]^e + 1$. Moreover, if n and q are both even, then the stronger inequality $|\mathcal{S}| \le n^e + 1$ holds.*

1.4 Corollary. *Suppose a nondegenerate quadric in $PG(n,q)$ admits an ovoid. If q is odd, then $p^{\lfloor n/2 \rfloor} \le \binom{p+n-1}{n} - \binom{p+n-3}{n}$. If q is even, then $n \le 5$ or $n=7$.*

1.5 Corollary. *There are no ovoids in $O_7(2^e)$, $O_{10}^+(2^e)$, $O_{10}^+(3^e)$, $O_9(5^e)$, $O_{12}^+(5^e)$ or $O_{12}^+(7^e)$.*

Most of Corollary 1.5 is new, although it was previously known (see [8], [11], [14]) that no ovoids exist in $O_7(2^e)$, $O_{10}^+(2)$ or $O_{10}^+(3)$. Here $O_{2m+1}(q)$ denotes a $(2m+1)$-dimensional vector space over F equipped with a nondegenerate quadratic form Q, so that $\mathcal{Z}(Q)$ is a nondegenerate quadric in $PG(2m,q)$. Also $O_{2m}^+(q)$ is a $2m$-dimensional vector space together with a nondegenerate form Q of Witt index m, so that $\mathcal{Z}(Q)$ is a (nondegenerate) hyperbolic quadric in $PG(2m-1,q)$.

As a measure of the strength of Theorem 1.3 in cases where ovoids cannot exist, the second author has constructed caps of size 55 in $O_{10}^+(3)$, thus attaining the upper bound of Theorem 1.3.

In Section 4 we prove the following, which is slightly weaker than Corollary 1.4 in the case of orthogonal spaces, but applies also to symplectic and unitary spaces. All terminology will be defined in Section 4.

1.6 Theorem. *Let $\mathcal{P}$ be any finite classical polar space, naturally embedded in $PG(n,q)$. If $\mathcal{S}$ is any cap in $\mathcal{P}$, then $|\mathcal{S}| \le \binom{p+n-1}{n}^e + 1$.*

This shows that for any classical family of finite polar spaces over $F=GF(p^e)$, ovoids cannot exist when the rank of the polar space exceeds some bound depending on p (but not on e). Inasmuch as Theorem 1.6 is an elementary consequence of the known Theorem 1.1, it is surprising that this bound has until now remained unnoticed. The question of which finite polar spaces admit ovoids has been settled in the symplectic case [7] but not completely in the unitary case, as we now describe. The polar space $\mathcal{U}(n,q^2)$ of unitary type is defined as the set of all projective subspaces of $PG(n,q^2)$ which lie on a given nondegenerate Hermitian variety. Ovoids of $\mathcal{U}(n,q^2)$ are defined just as for quadrics; see also Section 4. Ovoids of $\mathcal{U}(3,q^2)$ exist trivially, but $\mathcal{U}(2m,q^2)$ has no ovoids for $m \geq 2$. The situation in $\mathcal{U}(2m-1,q^2)$ is open for $m \geq 3$, and the following bound applies.

1.7 Corollary. *If $\mathcal{U}(2m-1,q^2)$ contains an ovoid, where $q=p^e$, then $p^{2m-1} \leq \binom{p+2m-2}{2m-1}^2$.*

1.8 Corollary. *No ovoids exist in $\mathcal{U}(7,2^{2e})$, $\mathcal{U}(7,3^{2e})$, $\mathcal{U}(9,5^{2e})$ or $\mathcal{U}(9,7^{2e})$.*

The proof, given in Section 4, depends ultimately on Theorem 1.1. Also in Section 4 we prove the following.

1.9 Theorem. *(i) (Bagchi and Sastry [2]) Let $\mathcal{O}$ be an ovoid in $PG(3,2^e)$. Then the tangent planes to $\mathcal{O}$ form a basis for the code spanned by (the characteristic vectors of) the planes of $PG(3,2^e)$.*

(ii) Let $\mathcal{O}$ be an ovoid in $O_7(3^e)$ or in $O_8^+(2^e)$. Then the tangent hyperplanes to $\mathcal{O}$ (i.e. the planes $x^\perp$ for $x \in \mathcal{O}$) form a basis for the code spanned by (the characteristic vectors of) the tangent hyperplanes to the quadric.

Finally, in Section 5 we give an application of this work to codes of projective planes. The *code* $\mathcal{C}$ of $PG(2,q)$ is the space spanned by the (characteristic vectors of the) lines, over $F=GF(q)$. It is well known that the complements of the lines span the code $\mathcal{C} \cap \mathbf{1}^\perp$ (which coincides with $\mathcal{C}^\perp$ if $q=p$), and that $\dim(\mathcal{C} \cap \mathbf{1}^\perp) = \dim \mathcal{C} - 1 = \binom{p+1}{2}^e$ (cf. Theorem 1.1). Let $\mathcal{Z}(Q)$ be an irreducible conic in the plane. We shall prove the following.

1.10 Theorem. *(i) $\mathcal{C} \cap \mathbf{1}^\perp$ is spanned by the complements of the secants of $\mathcal{Z}(Q)$; also by the complements of the nonsecants (i.e. tangents and passants) of $\mathcal{Z}(Q)$. Furthermore, the nonsecants span $\mathcal{C}$ itself.*

(ii) In case q is prime, the complements of the secants form a basis of $\mathcal{C}^\perp = \mathcal{C} \cap \mathbf{1}^\perp$, and the nonsecants form a basis of $\mathcal{C}$.

The authors are pleased to acknowledge that these investigations have been guided by stimulating conversations with Ruud Pelikaan, Andries Brouwer, Ron Baker and Robert Liebler.

2. Polynomials and p-ranks

Let $F = GF(q)$, with $q = p^e$ as in Section 1. The vector space $V = F^{n+1} = \{\mathbf{x} = (x_0, x_1, \ldots, x_n) : x_i \in F\}$, considered projectively, becomes the n-dimensional projective space $PG(n, F)$. Points of $PG(n, F)$ (or of V) are one-dimensional subspaces of V. Let $F_d[X_0, X_1, \ldots, X_n]$ denote the vector space of homogeneous polynomials of degree d in $F[X_0, X_1, \ldots, X_n]$, together with 0, and for $f(X_0, \ldots, X_n) \in F_d[X_0, \ldots, X_n]$, let $\mathcal{Z}(f)$ denote the zero set of f, considered as a variety of degree d in $PG(n, F)$. We use the abbreviations $\mathbf{X} = (X_0, X_1, \ldots, X_n)$, $f(\mathbf{X}) = f(X_0, \ldots, X_n)$, $F[\mathbf{X}] = F[X_0, \ldots, X_n]$, and $F_d[\mathbf{X}] = F_d[X_0, \ldots, X_n]$. Note that we use lower case $\mathbf{x} \in V$ for vectors, but upper case $\mathbf{X}$ for an $(n+1)$-tuple of indeterminates. The hyperplanes of $PG(n, F)$ are the varieties of the form $\mathcal{Z}(\ell)$ such that $0 \neq \ell(\mathbf{X}) \in F_1[\mathbf{X}]$. If H is a projective subspace of $PG(n, F)$, we shall write $\mathcal{Z}_H(f) = H \cap \mathcal{Z}(f)$, considered as a variety in H.

A *quadratic form on* V is a polynomial $Q(\mathbf{X}) \in F_2[\mathbf{X}]$. The corresponding *quadric* is $\mathcal{Z}(Q)$. The *bilinear form associated to* $Q(\mathbf{X})$ is the polynomial $(\mathbf{X}, \mathbf{Y}) := Q(\mathbf{X}+\mathbf{Y}) - Q(\mathbf{X}) - Q(\mathbf{Y}) \in F[\mathbf{X}, \mathbf{Y}]$. For each subspace $U \leq V$, define $U^\perp = \{\mathbf{v} \in V : (\mathbf{v}, \mathbf{u}) = 0 \ \forall \mathbf{u} \in U\}$. A *singular point* is a point of the quadric $\mathcal{Z}(Q)$, i.e. a one-dimensional subspace $\langle \mathbf{x} \rangle$ of V such that $Q(\mathbf{x}) = 0$. We shall only consider the case that $Q(\mathbf{X})$ (or $\mathcal{Z}(Q)$) is *nondegenerate;* by definition, this means that $V^\perp$ contains no singular points. Equivalently, $V^\perp = \{\mathbf{0}\}$ (i.e. the bilinear form is nondegenerate) unless q and n are both even; if q and n are both even, then $V^\perp$ is a nonsingular point, called the *radical point* of V. More details concerning quadrics may be found in [7].

If n and q are not both even, then the bilinear form $(\ ,\ )$ is nondegenerate, and $\perp$ is a polarity (orthogonal or symplectic according as q is odd or even), in which case we may suppose moreover that $H_i = P_i^\perp$ for all $i = 1, 2, \ldots, m$, whence A is symmetric. But if n and q are both even, then $\perp$ fails to be a polarity. In the latter case, however, Theorem 1.2(ii) holds, by the following.

2.1 Lemma. *Suppose that n and q are both even. Then A_{11} is a point-hyperplane incidence matrix of $PG(n-1, q)$. Thus $\mathrm{rank}_2 A_{11} = n^e + 1$.*

Proof. Let $\langle \mathbf{x} \rangle = V^\perp$ be the radical point of $V = F^{n+1}$. We show that A_{11} is a point-hyperplane incidence matrix for $V/\langle \mathbf{x} \rangle$. Points of $V/\langle \mathbf{x} \rangle$ are the same as the lines (two-dimensional subspaces) of V which pass through $\langle \mathbf{x} \rangle$. Each such line is of the form $P_i + \langle \mathbf{x} \rangle$, $1 \leq i \leq s$. The hyperplanes of $V/\langle \mathbf{x} \rangle$ are just the hyperplanes of V which pass through $\langle \mathbf{x} \rangle$, and these are just the tangent hyperplanes $H_1,\ H_2,\ \ldots,\ H_s$ to the quadric. Moreover, $P_i + \langle \mathbf{x} \rangle$ lies in H_j iff $P_i \in H_j$, and A_{11} is the incidence matrix for this relation. Now $\mathrm{rank}_2 A_{11} = n^e + 1$ by Theorem 1.1. $\square$

For reference, we record here the well-known formula for the number of points on a quadric; see Theorem 22.5.1(b) of [7] for details.

2.2 Lemma. *The number of points of $PG(n,q)$ on a nondegenerate quadric $\mathcal{Z}(Q)$, is $(q^n-1)/(q-1)+\varepsilon q^{(n-1)/2}$, where $\varepsilon = \varepsilon(Q) = +1, -1$ or 0, according as $\mathcal{Z}(Q)$ is hyperbolic or elliptic (n odd), or n is even. The number of nonsingular points is $q^n - \varepsilon q^{(n-1)/2}$.*

The standard basis of $F_d[X_0,\ldots,X_n]$ is the set of $\binom{n+d}{n}$ monomials $X_0^{i_0}X_1^{i_1}\ldots X_n^{i_n}$ such that $i_0, i_1, \ldots, i_n \geq 0$, $i_0{+}i_1{+}\ldots{+}i_n = d$. We use the abbreviations $\mathbf{i} := (i_0, i_1, \ldots, i_n)$, $\mathbf{X}^{\mathbf{i}} := X_0^{i_0}X_1^{i_1}\ldots X_n^{i_n}$. We define the *degree* of the $(n+1)$-tuple $\mathbf{i}$ to be the degree of the monomial which it represents, i.e. $\deg \mathbf{i} = \deg \mathbf{X}^{\mathbf{i}} = i_0{+}i_1{+}\ldots{+}i_n$. Likewise for $\mathbf{y} = (y_0, \ldots, y_n) \in F^{n+1}$, define $\mathbf{y}^{\mathbf{i}} = y_0^{i_0}y_1^{i_1}\ldots y_n^{i_n}$, using the convention $0^0 = 1$. We shall frequently use the abbreviation $\mathbf{X}' := (X_1, X_2, \ldots, X_n)$ for coördinates of the hyperplane $\mathcal{Z}(X_0)$.

Consider the $q^{n+1} \times q^{n+1}$ matrix $B = \left(\mathbf{x}^{\mathbf{i}}\right)$ with rows indexed by vectors $\mathbf{x} \in F^{n+1}$ and columns indexed by $\mathbf{i}$ such that $0 \leq i_0, i_1, \ldots, i_n \leq q{-}1$.

2.3 Lemma. *B is nonsingular.*

Proof. If $n = 0$ then B is a Vandermonde matrix B_0 of size $q \times q$, and the result is well known. In general, $B = B_0 \otimes B_0 \otimes \cdots \otimes B_0$, an $(n+1)$-fold Kronecker product, and again the result follows. $\square$

Now define $F_d^\dagger[\mathbf{X}] = F_d^\dagger[X_0,\ldots,X_n]$ to be the subspace of $F_d[\mathbf{X}]$ spanned by all monomials $\mathbf{X}^{\mathbf{i}}$ such that p does not divide

$$\binom{d}{\mathbf{i}} := \binom{d}{i_0,\ i_1,\ \cdots,\ i_n} = \frac{d\,!}{i_0!\,i_1!\,\cdots\,i_n!}\,.$$

Note that $F_d^\dagger[\mathbf{X}] = F_d[\mathbf{X}]$ if and only if $d \leq p-1$.

2.4 Lemma. *Let $d = d_0 + d_1 p + \ldots + d_r p^r$ be the p-ary expansion of d, with $0 \le d_0, d_1, \ldots, d_r \le p-1$. Then the monomials $\mathbf{X}^{\mathbf{i}_0 + p\mathbf{i}_1 + \ldots + p^r \mathbf{i}_r}$ for which $\mathbf{i}_0, \ldots, \mathbf{i}_r$ are $(n+1)$-tuples of degree $d_0, \ldots, d_r$ respectively, form a basis of $F_d^\dagger[\mathbf{X}]$. In particular, $\dim F_d^\dagger[\mathbf{X}] = \prod_{j=0}^{r} \binom{n+d_j}{n}$ and $\dim F_{q-1}^\dagger[\mathbf{X}] = \binom{p+n-1}{n}^e$.*

Proof. See, for example, [3] for the essence of a proof using Lucas' Theorem. □

Let $\mathcal{V}_1$ be $F_1[\mathbf{X}]$, endowed with the natural representation of $G = GL(n+1, F)$ with respect to the ordered basis $\mathbf{X} = (X_0, X_1, \ldots, X_n)$; for $T \in G$ we write $T\mathbf{X} = (TX_0, TX_1, \ldots, TX_n)$. This action extends uniquely to a faithful action of G on the algebra $F[\mathbf{X}]$, given by $Tf(\mathbf{X}) = f(T\mathbf{X})$. It is well known that each homogeneous part $\mathcal{V}_d = F_d[\mathbf{X}]$ is invariant under this action of G. Here $\mathcal{V}_d$ is regarded as an FG-module, isomorphic to the space of homogeneous symmetric tensors of order d on $\mathcal{V}_1$.

Consider the Frobenius automorphism σ defined by $x \mapsto x^p$, so that $\mathrm{Aut}(F) = \{1, \sigma, \sigma^2, \ldots, \sigma^{e-1}\}$. Allow σ to act naturally on G and on $F[\mathbf{X}]$ by applying σ to each matrix entry and to each polynomial coefficient. For each $i = 0, 1, \ldots, e-1$, a new FG-module $\mathcal{V}_d^{(i)}$ is obtained by twisting $\mathcal{V}_d$ by the automorphism σ^i. That is, the elements of $\mathcal{V}_d^{(i)}$ coincide with those of $\mathcal{V}_d = F_d[\mathbf{X}]$, but the new action of $T \in G$ is given by

$$f(\mathbf{X}) \mapsto f(T^{\sigma^{-i}}\mathbf{X}), \qquad f(\mathbf{X}) \in \mathcal{V}_d^{(i)}.$$

We require the following.

2.5 Lemma. *(i) $F_d^\dagger[\mathbf{X}]$ is invariant under $G = GL(n+1, F)$ for every $d \ge 0$. More generally, $F_d^\dagger[\mathbf{X}]$ is invariant under the ring R of $(n+1) \times (n+1)$ matrices over F.*

(ii) We have an isomorphism of FG-modules given by

$$F_{q-1}^\dagger[\mathbf{X}] \cong \bigotimes_{j=0}^{e-1} \mathcal{V}_{p-1}^{(j)}.$$

Proof. (i) A typical generator T of G is of the form $TX_0 = \alpha X_0 + \beta X_1$, $\alpha \ne 0$; $TX_j = X_j$ for $j \ge 1$. Then for a typical monomial $\mathbf{X}^{\mathbf{i}} \in F_d^\dagger[\mathbf{X}]$, we have

$$T\mathbf{X}^{\mathbf{i}} = \sum_{0 \le j \le i_0;\ p \nmid \binom{i_0}{j}} \alpha^{i_0 - j} \beta^j \binom{i_0}{j} X_0^{i_0 - j} X_1^{i_1 + j} X_2^{i_2} \ldots X_n^{i_n}.$$

The only monomials which appear on the right are those in $F_d^\dagger[\mathbf{X}]$; this follows directly from the identity

$$\binom{i_1+j}{i_1}\binom{d}{i_0-j,\ \ i_1+j,\ \ i_2,\ \ \cdots,\ i_n} = \binom{i_0}{j}\binom{d}{\mathbf{i}}$$

and the hypothesis that $\binom{d}{\mathbf{i}}$ is not divisible by p. Thus $F_d^\dagger[\mathbf{X}]$ is invariant under G. If we remove the above restriction that $\alpha \neq 0$, then T ranges over generators of the multiplicative monoid of R, and the above argument suffices to show that $F_d^\dagger[\mathbf{X}]$ is invariant under R. (Remark: Although $F_d^\dagger[\mathbf{X}]$ is an FG-module, it is not an R-module, since in general $f((A+B)\mathbf{X}) \neq f(A\mathbf{X}) + f(B\mathbf{X})$ where $A+B$ denotes addition in the ring R.)

(ii) By Lemma 2.4, we have a vector space isomorphism

$$\varphi : \mathcal{V}_{p-1}^{(0)} \otimes \mathcal{V}_{p-1}^{(1)} \otimes \cdots \otimes \mathcal{V}_{p-1}^{(e-1)} \to F_{q-1}^\dagger[\mathbf{X}]$$

determined by

$$g_0(\mathbf{X}) \otimes g_1(\mathbf{X}) \otimes \cdots \otimes g_{e-1}(\mathbf{X}) \mapsto \prod_{j=0}^{e-1} g_j(\mathbf{X}^{p^j}) = \prod_{j=0}^{e-1} \big(g_j^{\sigma^{-j}}(\mathbf{X})\big)^{p^j}$$

where $\mathbf{X}^{p^j} = (X_0^{p^j}, X_1^{p^j}, \ldots, X_n^{p^j})$. To see that this is in fact an isomorphism of FG-modules, let $T \in G$; then

$$\begin{aligned} T\big(g_0(\mathbf{X}) \otimes g_1(\mathbf{X}) \otimes \cdots \otimes g_{e-1}(\mathbf{X})\big) &= g_0(T\mathbf{X}) \otimes g_1(T^{\sigma^{-1}}\mathbf{X}) \otimes \cdots \otimes g_{e-1}(T^{\sigma^{-e+1}}\mathbf{X}) \\ &\xmapsto{\varphi} \prod_{j=0}^{e-1} g_j(T\mathbf{X}^{p^j}) = T \prod_{j=0}^{e-1} g_j(\mathbf{X}^{p^j})\,, \end{aligned}$$

i.e. $\varphi T = T\varphi$ as required. $\square$

Remark. We shall require Lemma 2.5 only for $d \le q$, in which case one may show that $F_d^\dagger[\mathbf{X}]$ is the subspace of $F_d[\mathbf{X}]$ spanned by all $\ell(\mathbf{X})^d$, $\ell(\mathbf{X}) \in F_1[\mathbf{X}]$; see Corollary 3.2.

We may coördinatise the points and hyperplanes using one-dimensional subspaces spanned by row and column vectors of length $n+1$, namely, $P_i = \langle \mathbf{x}_i \rangle$, $H_j = \langle \mathbf{y}_j^\top \rangle$. As usual, we have $P_i \in H_j$ iff $\mathbf{x}_i \mathbf{y}_j^\top = 0$. Here we use the standard bilinear form $\mathbf{x}\mathbf{y}^\top$ rather than $(\mathbf{x},\mathbf{y})$, since the latter form is sometimes degenerate. Thus the entries of A are given by

$$a_{ij} = 1 - (\mathbf{x}_i\mathbf{y}_j^\top)^{q-1} = \begin{cases} 1, & \mathbf{x}_i\mathbf{y}_j^\top = 0; \\ 0, & \text{otherwise.} \end{cases}$$

Now let $M = \big((\mathbf{x}\mathbf{y}^\top)^{q-1}\big)$ be the $q^{n+1}\times q^{n+1}$ matrix with rows and columns indexed by the row vectors $\mathbf{x},\mathbf{y}\in F^{n+1}$. Assume that the first $(q-1)s+1$ rows of M are indexed by those vectors $\mathbf{x}$ such that $Q(\mathbf{x})=0$, and the remaining $q^{n+1}-(q-1)s-1$ columns are indexed by the remaining vectors $\mathbf{x}\in F^{n+1}$. This induces on M a partition of the form $M = \binom{M_1}{M_2}$ where M_1 consists of the first $(q-1)s+1$ rows of M.

2.6 Lemma. *(i)* $\operatorname{rank}_p M = \operatorname{rank}_p A - 1$.
(ii) $\operatorname{rank}_p M_1 = \operatorname{rank}_p A_1 - 1$ *for* $n \geq 3$.
(iii) For $n=2$, *we have* $\operatorname{rank}_p M_1 = \operatorname{rank}_p A_1 = q+1$.

Proof. Observe that $\mathbf{x}$ and $\lambda\mathbf{x}$ index identical rows of M whenever $\lambda\in F\smallsetminus\{0\}$; similar duplications occur among the columns. Deleting from M duplicates of rows, and of columns, and deleting the zero row and column, gives the matrix

$$J - A = \begin{pmatrix} J-A_1 \\ J-A_2 \end{pmatrix},$$

assuming (as we may) that vectors in F^{n+1} and points of $PG(n,F)$ have been ordered consistently; here each J is a matrix of all 1's of the appropriate size. Thus $\operatorname{rank}_p M = \operatorname{rank}_p(J-A)$, and similarly, $\operatorname{rank}_p M_1 = \operatorname{rank}_p(J-A_1)$.

Each row and column of A has q^n zeroes and $m-q^n$ ones, where $m\equiv 1 \mod p$, which gives $Row(A) = \langle\mathbf{1}\rangle \oplus Row(J-A)$, where $\mathbf{1}=(1,1,\ldots,1)$ of length m, and *'Row'* denotes the row space over F. Together with the preceding remarks, this proves (i).

Conclusion (ii) follows by the same arguments as in the previous paragraph, if only we can show that each column of A_1 has 1 (mod p) ones and 0 (mod p) zeroes. A typical column of A_1 is indexed by a hyperplane $H\subset PG(n,F)$. If $\mathcal{Z}_H(Q)$ is a nondegenerate quadric in H, then the number of points in $\mathcal{Z}_H(Q)$ is 1 mod p by Lemma 2.2, since H has projective dimension $n-1\geq 2$. Otherwise $\mathcal{Z}_H(Q)$ is a cone over a radical point $\langle\mathbf{x}\rangle$, and the number of points on this degenerate quadric in H is $1+qs'\equiv 1 \mod p$, where '1' counts the point $\langle\mathbf{x}\rangle$, and s' is the number of points on the nondegenerate quadric induced on $H/\langle\mathbf{x}\rangle$. Thus (ii) holds as before.

Finally, suppose $n=2$. Then A_{11} is an identity matrix of size $q+1$. Thus $\operatorname{rank}_p A_1 = \operatorname{rank}_p A_{11} = q+1$. The column space $Col(J-A_{11})$ is the set of all column vectors $(v_1,\ldots,v_{q+1})^\top$ such that $\sum_i v_i = 0$. For each passant of the conic $\mathcal{Z}(Q)$, the corresponding column of M_1 is $(1,1,\ldots,1)^\top \notin Col(J-A_{11})$, so that $\operatorname{rank}_p M_1 = q+1$. □

2.7 Lemma. *We have*

$$\operatorname{rank}_p M_1 = \binom{p+n-1}{n}^e - \dim\left\{ f(\mathbf{X}) \in F^\dagger_{q-1}[\mathbf{X}] \;:\; f(\mathbf{X}) \text{ vanishes on } \mathcal{Z}(Q) \right\}.$$

Proof. For each vector $\mathbf{a} = \left(a_{\mathbf{y}} \;:\; \mathbf{y} \in F^{n+1}\right)$, define

$$\begin{aligned} f_{\mathbf{a}}(\mathbf{X}) &= \sum_{\mathbf{y}\in F^{n+1}} a_{\mathbf{y}} (\mathbf{X}\mathbf{y}^\top)^{q-1} \\ &= \sum_{\mathbf{y}\in F^{n+1}} a_{\mathbf{y}} \sum_{\deg(\mathbf{i})=q-1} \binom{q-1}{\mathbf{i}} \mathbf{X}^{\mathbf{i}}\mathbf{y}^{\mathbf{i}} \\ &= \sum_{\deg(\mathbf{i})=q-1} \binom{q-1}{\mathbf{i}} \left[\sum_{\mathbf{y}\in F^{n+1}} a_{\mathbf{y}}\mathbf{y}^{\mathbf{i}} \right] \mathbf{X}^{\mathbf{i}} \;\in\; F^\dagger_{q-1}[\mathbf{X}]\,. \end{aligned}$$

Then $\mathbf{a} \mapsto f_{\mathbf{a}}(\mathbf{X})$ defines a linear map $F^{F^{n+1}} \to F^\dagger_{q-1}[\mathbf{X}]$, and it follows from Lemma 2.3 that this map is surjective. Also $f_{\mathbf{a}}(\mathbf{X})$ vanishes on $\mathcal{Z}(Q)$ if and only if $\mathbf{a}^\top$ is in the right null space of M_1. Thus

$$\begin{aligned} \dim F^\dagger_{q-1}[\mathbf{X}] - \dim\big\{ f(\mathbf{X}) \in F^\dagger_{q-1}[\mathbf{X}] \;:\; f(\mathbf{X}) \text{ vanishes on } \mathcal{Z}(Q) \big\} \\ = q^{n+1} - \dim\Big(\text{right null space of } M_1\Big) \\ = \operatorname{rank}_p M_1. \end{aligned}$$

Applying Lemmas 2.4 and 2.6(ii) gives the result. □

Note that $f(\mathbf{X})^{p^j} = f^{\sigma^j}(\mathbf{X}^{p^j})$, where σ is the Frobenius automorphism of F, extended to $F[\mathbf{X}]$. Observe from Lemma 2.5 that $F^\dagger_{q-1}[\mathbf{X}]$ is spanned by the products $\prod_{j=0}^{e-1} g_j(\mathbf{X})^{p^j}$ such that $g_j(\mathbf{X}) \in F_{p-1}[\mathbf{X}]$. Define $\mathcal{E}_{Q,\mathbf{X}}$ to be the subspace of $F^\dagger_{q-1}[\mathbf{X}]$ spanned by all polynomials of the form $\prod_{j=0}^{e-1} g_j(\mathbf{X})^{p^j}$ such that $Q(\mathbf{X})$ divides at least one of the factors $g_j(\mathbf{X}) \in F_{p-1}[\mathbf{X}]$. By construction, $\mathcal{E}_{Q,\mathbf{X}} \le Q(\mathbf{X})F_{q-3}[\mathbf{X}] \cap F^\dagger_{q-1}[\mathbf{X}]$; and we will see (Lemma 2.14) that equality holds when $n \ge 3$. Note that $\mathcal{E}_{Q,\mathbf{X}} = 0$ when q is even. The following is immediate.

2.8 Lemma. *Let $\{g_1(\mathbf{X}), \ldots, g_{b'}(\mathbf{X})\}$ be a basis for the subspace $Q(\mathbf{X})F_{p-3}[\mathbf{X}] < F_{p-1}[\mathbf{X}]$, and extend this to a basis $\{g_1(\mathbf{X}), \ldots, g_b(\mathbf{X})\}$ for $F_{p-1}[\mathbf{X}]$, where $b = \binom{p+n-1}{n}$ and $b' = \binom{p+n-3}{n}$. Then*

(i) $\mathcal{B} = \left\{\prod_{j=0}^{e-1} g_{r_j}(\mathbf{X})^{p^j} \,:\, 1 \le r_0, r_1, \ldots, r_{e-1} \le b\right\}$ is a basis for $F^\dagger_{q-1}[\mathbf{X}]$, and

(ii) $\mathcal{B}' = \left\{\prod_{j=0}^{e-1} g_{r_j}(\mathbf{X})^{p^j} \in \mathcal{B} \,:\, \text{at least one } r_j \le b'\right\}$ is a basis for $\mathcal{E}_{Q,\mathbf{X}}$; in particular, $\dim \mathcal{E}_{Q,\mathbf{X}} = b^e - (b-b')^e$.

2.9 Lemma. *Suppose that $n = 3$. Then $\mathcal{E}_{Q,\mathbf{X}}$ is the set of all $f(\mathbf{X}) \in F^\dagger_{q-1}[\mathbf{X}]$ vanishing on $\mathcal{Z}(Q)$. Furthermore, any polynomial in $F_{q-1}[\mathbf{X}]$ vanishing on $\mathcal{Z}(Q)$, is divisible by $Q(\mathbf{X})$.*

Proof of Lemma 2.9. Consider first the case that $\mathcal{Z}(Q)$ is an elliptic quadric of $PG(3,q)$. Then A_{11} is an $s \times s$ identity matrix where $s = q^2+1$, so that $\operatorname{rank}_p A_1 = \operatorname{rank}_p A_{11} = s = q^2+1$. Now by Lemmas 2.6, 2.7 and 2.8,

$$
\begin{aligned}
q^2 &= \operatorname{rank}_p A_1 - 1 \\
&= \binom{p+2}{3}^e - \dim\left\{f(\mathbf{X}) \in F^\dagger_{q-1}[\mathbf{X}] \,:\, f(\mathbf{X}) \text{ vanishes on } \mathcal{Z}(Q)\right\} \\
&\le \binom{p+2}{3}^e - \dim\left\{f(\mathbf{X}) \in F^\dagger_{q-1}[\mathbf{X}] \,:\, Q(\mathbf{X}) \,\middle|\, f(\mathbf{X})\right\} \\
&\le \binom{p+2}{3}^e - \dim \mathcal{E}_{Q,\mathbf{X}} \\
&= \left[\binom{p+2}{3} - \binom{p}{3}\right]^e = p^{2e} = q^2.
\end{aligned}
$$

Hence equality holds throughout, and $\mathcal{E}_{Q,\mathbf{X}} = \left\{f(\mathbf{X}) \in F^\dagger_{q-1}[\mathbf{X}] : f(\mathbf{X}) \text{ vanishes on } \mathcal{Z}(Q)\right\}$. Now by Lemma 2.4 and the above, we have

$$
\begin{aligned}
\dim F_{q-1}[\mathbf{X}] - \dim&\left\{f(\mathbf{X}) \in F_{q-1}[\mathbf{X}] \,:\, Q(\mathbf{X}) \,\middle|\, f(\mathbf{X})\right\} \\
&= \binom{q+2}{3} - \binom{q}{3} = q^2 \\
&= \dim F^\dagger_{q-1}[\mathbf{X}] - \dim\left\{f(\mathbf{X}) \in F^\dagger_{q-1}[\mathbf{X}] \,:\, Q(\mathbf{X}) \,\middle|\, f(\mathbf{X})\right\}.
\end{aligned}
$$

Consequently, $F_{q-1}[\mathbf{X}] = F^\dagger_{q-1}[\mathbf{X}] + \left\{f(\mathbf{X}) \in F_{q-1}[\mathbf{X}] \,:\, Q(\mathbf{X}) \,\middle|\, f(\mathbf{X})\right\}$. Suppose now that $f(\mathbf{X}) \in F_{q-1}[\mathbf{X}]$ vanishes on $\mathcal{Z}(Q)$. We may write $f(\mathbf{X}) = f^\dagger(\mathbf{X}) + Q(\mathbf{X})g(\mathbf{X})$ for some $g(\mathbf{X}) \in F_{q-3}[\mathbf{X}]$, where $f^\dagger(\mathbf{X}) \in F^\dagger_{q-1}[\mathbf{X}]$ vanishes on $\mathcal{Z}(Q)$. We have seen that this implies that $Q(\mathbf{X}) \mid f^\dagger(\mathbf{X})$, and so $Q(\mathbf{X}) \mid f(\mathbf{X})$ as required.

The same proof works for a hyperbolic quadric $\mathcal{Z}(Q)$ in $PG(3,q)$, if only we can show that $\operatorname{rank}_p A_1 \ge q^2+1$, or equivalently, that $\operatorname{rank}_p(J - A_1) \ge q^2$. In this case $\mathcal{Z}(Q)$ is a $(q+1)\times(q+1)$ grid. For each point $\langle \mathbf{x}\rangle$ of $\mathcal{Z}(Q)$, let $v_{\mathbf{x}}$ be the column of $J-A_1$ indexed by the tangent plane $\mathbf{x}^\perp$; that is, $v_{\mathbf{x}}$ is the column vector of length $(q+1)^2$ with entries indexed by the points of $\mathcal{Z}(Q)$, having entry 1 at each of the q^2 points of $\mathcal{Z}(Q)$ not perpendicular with $\langle \mathbf{x}\rangle$, and 0 otherwise. Fix a point $\langle \mathbf{u}\rangle$ of $\mathcal{Z}(Q)$, as in Figure 1.

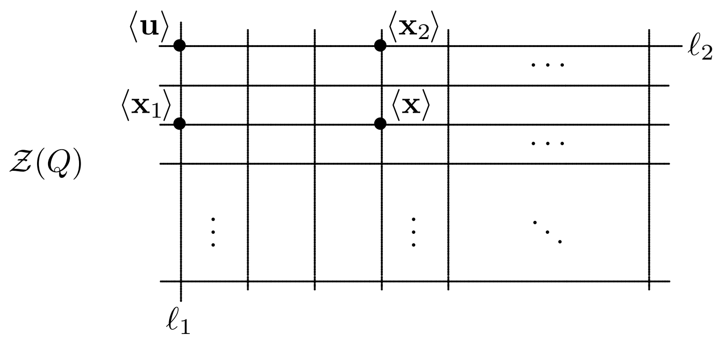

Figure 1.

Let ℓ_1,ℓ_2 be the two lines of $\mathcal{Z}(Q)$ through $\langle \mathbf{u}\rangle$, and denote the tangent plane $H=\mathbf{u}^\perp=\langle \ell_1,\ell_2\rangle$. For any point $\langle \mathbf{x}\rangle$ of $\mathcal{Z}(Q)$ not on H, let $\langle \mathbf{x}_i\rangle$ be the unique point of ℓ_i perpendicular to $\mathbf{x}$; then $v_{\mathbf{x}}-v_{\mathbf{x}_1}-v_{\mathbf{x}_2}+v_{\mathbf{u}}$ has value 1 at $\langle \mathbf{x}\rangle$, and vanishes at all other points of $\mathcal{Z}(Q)$ outside H. Thus $\operatorname{rank}_p(J-A_1)\ge \dim\big\langle v_{\mathbf{x}} : \langle \mathbf{x}\rangle\in\mathcal{Z}(Q)\big\rangle \ge q^2$ as required. $\square$

The following lemma will be required in the proof of Theorem 2.11.

2.10 Lemma. *For any point $\langle \mathbf{u}\rangle$ of $PG(n,F)$, where $n\ge 4$, there are more than q nondegenerate hyperplanes of $PG(n,F)$ not passing through $\langle \mathbf{u}\rangle$. Moreover if $n=4$, there are more than q hyperbolic hyperplanes not passing through $\langle \mathbf{u}\rangle$.*

Proof. Suppose first that n is odd, $n\ge 5$. We may assume that $Q(\mathbf{X})=\alpha X_0^2+X_0X_1+X_1^2+X_2X_3+X_4X_5+\cdots+X_{n-1}X_n$. As usual, we denote the standard basis of V by $\{\mathbf{e}_0,\dots,\mathbf{e}_n\}$. By Witt's Theorem, there is no loss of generality in assuming that $\mathbf{u}\in\{\mathbf{e}_0+\mathbf{e}_2+\alpha\mathbf{e}_3,\ \mathbf{e}_0+\mathbf{e}_2+(\alpha{+}1)\mathbf{e}_3\}$ if q is even; or if q is odd, $\mathbf{u}\in\{\mathbf{e}_0+\mathbf{e}_2-\alpha\mathbf{e}_3,\ \mathbf{e}_0+\mathbf{e}_2+(1{-}\alpha)\mathbf{e}_3,\ \mathbf{e}_0+\mathbf{e}_2+(\epsilon{-}\alpha)\mathbf{e}_3\}$, where $\epsilon\in F$ is a fixed nonsquare. It is straightforward to check that for $\lambda\in F$, the hyperplanes $\mathcal{Z}(X_0+\lambda X_4)$ and $\mathcal{Z}(X_0+\lambda X_5)$ are nondegenerate. Moreover, there are $2q-1>q$ hyperplanes of this form, none of which contain $\langle \mathbf{u}\rangle$, as required.

Now suppose that n is even, $n\ge 4$. We may assume that $Q(\mathbf{X})=X_0^2+X_1X_2+X_3X_4+\cdots+X_{n-1}X_n$, and that $\mathbf{u}\in\{\mathbf{e}_0,\ \mathbf{e}_0+\mathbf{e}_1-\mathbf{e}_2,\ \mathbf{e}_0+\mathbf{e}_1+(\epsilon{-}1)\mathbf{e}_2\}$ where $\epsilon=1$ if

q is even; ϵ is a fixed nonsquare if q is odd. For $\lambda \in F$, we have $2q-1 > q$ nondegenerate (and in fact, hyperbolic) hyperplanes of the form $\mathcal{Z}(X_0+\lambda X_3)$ and $\mathcal{Z}(X_0+\lambda X_4)$, none of which contain $\langle \mathbf{u} \rangle$. $\square$

2.11 Theorem. *Suppose that $f(\mathbf{X}) \in F_d[\mathbf{X}]$ vanishes at every point of a nondegenerate quadric $\mathcal{Z}(Q)$ of $PG(n,F)$.*

(i) If $n=3$, $d \le q-1$ and $\mathcal{Z}(Q)$ is an elliptic quadric, then Q divides f.

(ii) If $n=3$, $d \le q$ and $\mathcal{Z}(Q)$ is a hyperbolic quadric, then Q divides f.

(iii) If $n \ge 4$ and $d \le q$ then Q divides f.

Remarks. For $n=2$ there exist homogeneous polynomials of degree $\lfloor q/2 \rfloor + 1$ vanishing on a nondegenerate conic $\mathcal{Z}(Q)$ of $PG(2,q)$, but not divisible by Q. An example of this is $\prod_i \ell_i(X_0,X_1,X_2)$ where for $0 \le i \le \lfloor q/2 \rfloor$ we choose $\ell_i(X_0,X_1,X_2) = a_iX_0 + b_iX_1 + c_iX_2 \in F_1[X_0,X_1,X_2]$ such that the lines $\mathcal{Z}(\ell_i)$ are secants of the conic which together cover the $q+1$ points of the conic.

It is clear that the degree restriction $d \le q$ is necessary since $PG(n,q)$ may be covered by $q+1$ hyperplanes and hence there exist many homogeneous polynomials of degree $q+1$ vanishing at every point of $PG(n,q)$. Furthermore an elliptic quadric in $PG(3,q)$ may be covered by q planes, which explains why the stronger hypothesis $d \le q-1$ is required in (i).

Proof of Theorem 2.11. Conclusion (i) follows from Lemma 2.9. This is immediate for $d=q-1$, but also clear for $d<q-1$ by applying Lemma 2.9 to $\widetilde{f}(\mathbf{X}) = X_0^{q-1-d} f(\mathbf{X}) \in F_{q-1}[\mathbf{X}]$.

We proceed to prove (ii), assuming first that q is odd. There is no loss of generality in assuming that $Q(\mathbf{X}) = X_0^2 + X_1X_2 - X_3^2 = X_0^2 - Q_1(\mathbf{X}')$ where $Q_1(\mathbf{X}') = X_3^2 - X_1X_2$ is a nondegenerate quadratic form in the plane $H = \mathcal{Z}(X_0)$ with coördinates $\mathbf{X}' := (X_1,X_2,X_3)$. Suppose that $f(\mathbf{X}) \in F_d[\mathbf{X}]$ vanishes on $\mathcal{Z}(Q)$. Also we may assume that $f(\mathbf{X})$ has degree at most 1 in X_0; otherwise subtract the appropriate multiple of $Q(\mathbf{X})$ from $f(\mathbf{X})$. Thus $f(\mathbf{X}) = X_0 g(\mathbf{X}') + h(\mathbf{X}')$ for some $g(\mathbf{X}') \in F_{d-1}[\mathbf{X}']$ and $h(\mathbf{X}') \in F_d[\mathbf{X}']$. We must show that $g(\mathbf{X}') = h(\mathbf{X}') = 0$.

The exterior points with respect to the conic $\mathcal{Z}_H(Q_1)$ in $H = \mathcal{Z}(X_0)$ are those points $\langle (x,y,z) \rangle$ such that $Q_1(x,y,z) \in F$ is a nonzero square (see Theorem 8.3.3 of [6]). For such a point $\langle(x,y,z)\rangle$ with $Q_1(x,y,z)=w^2\neq 0$, we find that $\langle(w,x,y,z)\rangle$ and $\langle(-w,x,y,z)\rangle$ both lie on the quadric $\mathcal{Z}(Q)$. By hypothesis, $f(\mathbf{X})$ vanishes at these two points, and we solve $0=wg(x,y,z)+h(x,y,z)=-wg(x,y,z)+h(x,y,z)$ to obtain $g(x,y,z)=h(x,y,z)=0$. Similarly, for points $\langle(0,x,y,z)\rangle$ with $Q_1(x,y,z)=0$, we obtain $h(x,y,z)=0$. Now let $\ell_0(\mathbf{X}'),\ell_1(\mathbf{X}'),\ldots,\ell_q(\mathbf{X}')\in F_1[\mathbf{X}']$ such that the lines $\mathcal{Z}(\ell_i)$ are the $q+1$ tangents to the conic $\mathcal{Z}_H(Q_1)$. Since $h(\mathbf{X}')$ vanishes at all $q+1$ points of $\mathcal{Z}_H(\ell_i)$ and $\deg h(\mathbf{X}')\leq q$, we must have $\ell_i(\mathbf{X}')\,\big|\,h(\mathbf{X}')$. Since $\ell_0(\mathbf{X}')\ell_1(\mathbf{X}')\ldots\ell_q(\mathbf{X}')$ divides $h(\mathbf{X}')$, the degree restriction implies that $h(\mathbf{X}')=0$. Similarly, $g(\mathbf{X}')$ is of degree at most $q-1$ and vanishes at q points of every tangent (namely, the q exterior points on such a tangent) and so $g(\mathbf{X}')=0$. Thus $f(\mathbf{X})=0$ as required.

Next we prove (ii) supposing that q is even. There is no loss in assuming that $Q(\mathbf{X})=X_0^2+X_0X_1+X_2X_3$, $f(\mathbf{X})=X_0g(\mathbf{X}')+h(\mathbf{X}')$, $g(\mathbf{X}')\in F_{d-1}[\mathbf{X}']$, $h(\mathbf{X}')\in F_d[\mathbf{X}']$, and we must show that $g(\mathbf{X}')=h(\mathbf{X}')=0$. The restriction of $Q(\mathbf{X})$ to the plane $H=\mathcal{Z}(X_0)$ is degenerate. The $q+1$ lines $\mathcal{Z}_H(X_2)$ and $\mathcal{Z}_H(\alpha X_1+\alpha^2X_2+X_3)$ for $\alpha\in F$ form a dual conic in H, and together with the nuclear line $\mathcal{Z}_H(X_1)$ these give a classical dual hyperoval. The $q+1$ points of $\mathcal{Z}_H(\alpha X_1+\alpha^2X_2+X_3)\smallsetminus\mathcal{Z}_H(X_1)$ are of the form $\langle(0,1,y,\alpha^2y+\alpha)\rangle$ for $y\in F$. For each such point we have two points $\langle(\alpha y,1,y,\alpha^2y+\alpha)\rangle$, $\langle(\alpha y+1,1,y,\alpha^2y+\alpha)\rangle\in\mathcal{Z}(Q)$ at which $X_0g(\mathbf{X}')+h(\mathbf{X}')$ must vanish. As before we obtain $0=g(1,y,\alpha^2y+\alpha)=h(1,y,\alpha^2y+\alpha)$. Since $g(\mathbf{X}')$ vanishes at q points of $\mathcal{Z}_H(\alpha X_1+\alpha^2X_2+X_3)$, we have $(\alpha X_1+\alpha^2X_2+X_3)\,\big|\,g(\mathbf{X}')$ for all $\alpha\in F$. Since $g(\mathbf{X}')\in F_{d-1}[\mathbf{X}']$, this forces $g(\mathbf{X}')=0$. Now the fact that $f(\mathbf{X})$ vanishes at $\langle(\alpha,0,1,\alpha^2)\rangle\in\mathcal{Z}(Q)$ implies similarly that $h(0,1,\alpha^2)=0$. Thus $h(\mathbf{X}')$ vanishes at all $q+1$ points of $\mathcal{Z}_H(\alpha X_1+\alpha^2X_2+X_3)$ and so $(\alpha X_1+\alpha^2X_2+X_3)\,\big|\,h(\mathbf{X}')$ for all $\alpha\in F$. Similarly $X_2\,\big|\,h(\mathbf{X}')$, and so degree considerations yield $h(\mathbf{X}')=0$ as required.

We now prove (iii) of Theorem 2.11 assuming that q is odd. By Lemma 2.5(i), we may assume that $Q(\mathbf{X})=X_0^2+Q'(\mathbf{X}')$ where $Q'(\mathbf{X}')$ is a nondegenerate quadratic form in $\mathbf{X}'=(X_1,X_2,\ldots,X_n)$. By adding to $f(\mathbf{X})$ a multiple of $Q(\mathbf{X})$ if necessary, we may assume that $f(\mathbf{X})=X_0g(\mathbf{X}')+h(\mathbf{X}')$ where $g(\mathbf{X}')\in F_{d-1}[\mathbf{X}']$ and $h(\mathbf{X}')\in F_d[\mathbf{X}']$. Every hyperplane of $PG(n,F)$ which does not pass through $\langle(1,0,0,\ldots,0)\rangle$ is of the form $\mathcal{Z}\big(X_0-\ell(\mathbf{X}')\big)$ for some $\ell(\mathbf{X}')\in F_1[\mathbf{X}']$, and such a hyperplane is nondegenerate if and only if $Q_\ell(\mathbf{X}')=Q(\ell(\mathbf{X}'),X_1,\ldots,X_n)$ defines a nondegenerate quadratic form in $\mathbf{X}'$. Suppose that $Q_\ell(\mathbf{X}')$ is nondegenerate; and if $n=4$, assume in addition that $Q_\ell(\mathbf{X}')$ is of hyperbolic type. Observe that $-\ell(\mathbf{X}')$ satisfies the same requirements as $\ell(\mathbf{X}')$. If Q_ℓ vanishes at $\mathbf{x}=(x_1,\ldots,x_n)$, then $Q\big(\ell(\mathbf{x}),\mathbf{x}\big)=Q\big(-\ell(\mathbf{x}),\mathbf{x}\big)=0$, so by hypothesis,

$\pm\ell(\mathbf{x})g(\mathbf{x})+h(\mathbf{x})=0$, which implies that $\ell(\mathbf{x})g(\mathbf{x})=h(\mathbf{x})=0$. By induction, $Q_\ell(\mathbf{X}')=Q_{-\ell}(\mathbf{X}')$ divides both $\ell(\mathbf{X}')g(\mathbf{X}')$ and $h(\mathbf{X}')$. Now let N be the number of functions $\ell(\mathbf{X}')$ satisfying the above hypotheses; then $g(\mathbf{X}')$ and $h(\mathbf{X}')$ are each divisible by at least $(N+1)/2$ distinct quadratic factors $Q_\ell(\mathbf{X}')=Q_{-\ell}(\mathbf{X}')$, including $Q_0(\mathbf{X}')$. (It is easy to check that two such polynomials $Q_\ell(\mathbf{X}')$ and $Q_{\ell^*}(\mathbf{X}')$ have no nontrivial common factor unless $\ell^*(\mathbf{X}')\in\{\ell(\mathbf{X}'),\,-\ell(\mathbf{X}')\}$.) However, $N>q$ by Lemma 2.10, and g and h have degree at most q, so $g=h=0$ as required.

For the remainder of the proof of (iii), q is even. By Lemma 2.5(i), we may assume that $Q(\mathbf{X})=X_0^2+X_0X_1+Q'(X_2,\dots,X_n)$ where Q' is a nondegenerate quadratic form in $(X_2,\dots,X_n)$. As before we may assume that $f(\mathbf{X})=X_0g(\mathbf{X}')+h(\mathbf{X}')$, $g(\mathbf{X}')\in F_{d-1}[\mathbf{X}']$, $h(\mathbf{X}')\in F_d[\mathbf{X}']$ where $\mathbf{X}'=(X_1,\dots,X_n)$, and we must show that $g=h=0$. Every hyperplane of $PG(n,F)$ which does not pass through $\langle(1,0,0,\dots,0)\rangle$ is of the form $\mathcal{Z}\big(X_0+\ell(\mathbf{X}')\big)$ for some $\ell(\mathbf{X}')\in F_1[\mathbf{X}']$, and such a hyperplane is nondegenerate if and only if $Q_\ell(\mathbf{X}')=Q(\ell(\mathbf{X}'),X_1,\dots,X_n)$ defines a nondegenerate quadratic form in $\mathbf{X}'$. Suppose that $Q_\ell(\mathbf{X}')$ is nondegenerate; and if $n=4$, assume in addition that $Q_\ell(\mathbf{X}')$ is of hyperbolic type. Notice that $X_1+\ell(\mathbf{X}')$ satisfies the same requirements as $\ell(\mathbf{X}')$. If Q_ℓ vanishes at $\mathbf{x}=(x_1,\dots,x_n)$, then $Q\big(\ell(\mathbf{x}),\mathbf{x}\big)=Q\big(x_1+\ell(\mathbf{x}),\mathbf{x}\big)=0$, so by hypothesis, $\ell(\mathbf{x})g(\mathbf{x})+h(\mathbf{x})=\big(x_1+\ell(\mathbf{x})\big)g(\mathbf{x})+h(\mathbf{x})=0$, which implies that $x_1g(\mathbf{x})=0$. By induction, $Q_\ell(\mathbf{X}')=Q_{X_1+\ell}(\mathbf{X}')$ divides both $X_1g(\mathbf{X}')$ and $\ell(\mathbf{X}')g(\mathbf{X}')+h(\mathbf{X}')$. Now let N be the number of functions $\ell(\mathbf{X}')$ satisfying the above hypotheses; then $g(\mathbf{X}')$ is divisible by at least $N/2$ distinct quadratic factors $Q_\ell(\mathbf{X}')=Q_{X_1+\ell}(\mathbf{X}')$. (Again, it is easy to check that two such polynomials $Q_\ell(\mathbf{X}')$ and $Q_{\ell^*}(\mathbf{X}')$ have no nontrivial common factor, unless $\ell^*(\mathbf{X}')\in\{\ell(\mathbf{X}'),\,X_1+\ell(\mathbf{X}')\}$.) By Lemma 2.10, we have $N>q$, which forces $g(\mathbf{X}')=0$. Thus $h(\mathbf{X}')$ is also divisible by at least $N/2>q/2$ quadratic factors, so $h(\mathbf{X}')=0$, which completes the proof of Theorem 2.11. $\square$

For convenience, we shall henceforth assume the following.

2.12 Assumption. $Q(\mathbf{X})$ *is a nondegenerate quadratic form in which the coefficient of* X_0^2 *is 1.*

We choose bases $\mathcal{B}$ and $\mathcal{B}'$ for $F^\dagger_{q-1}[\mathbf{X}]$ and $\mathcal{E}_{Q,\mathbf{X}}$ in accordance with Lemma 2.8, starting with a basis of $F_{p-1}[\mathbf{X}]$, starting with a basis of $F_{p-1}[\mathbf{X}]$. Namely, let $\{g_1(\mathbf{X}),\dots,g_{b'}(\mathbf{X})\}=\{Q(\mathbf{X})\mathbf{X}^{\mathbf{i}}\,:\,\mathbf{i}$ is an $(n{+}1)$-tuple of degree $p{-}3\}$ and $\{g_{b'+1}(\mathbf{X}),\dots,g_b(\mathbf{X})\}=$

$\{\mathbf{X}^{\mathbf{i}} \,:\, \mathbf{i}$ is an $(n{+}1)$-tuple of degree $p{-}1,\ 0 \le i_0 \le 1\}$ where $b = \binom{p+n-1}{n},\ b' = \binom{p+n-3}{n}$. Thus $\mathcal{B} = \left\{\prod_{j=0}^{e-1} g_{r_j}(\mathbf{X})^{p^j} \,:\, 1 \le r_0, r_1, \ldots, r_{e-1} \le b\right\}$ is a basis of $F_{q-1}^{\dagger}[\mathbf{X}]$ containing a basis $\mathcal{B}' = \left\{\prod_{j=0}^{e-1} g_{r_j}(\mathbf{X})^{p^j} \in \mathcal{B} \,:\, \text{at least one } r_j \le b'\right\}$ of $\mathcal{E}_{Q,\mathbf{X}}$. Each $\prod_j g_{r_j}(\mathbf{X})^{p^j} \in \mathcal{B}$, when expanded into monomials in $\mathbf{X}$, contains a unique monomial $\mathbf{X}^{\mathbf{i}}$ of highest degree in X_0. This defines a bijection $\theta : \mathcal{B} \to \left\{\mathbf{X}^{\mathbf{i}} \,:\, \mathbf{i} \text{ is an } (n{+}1)\text{-tuple of degree } q{-}1 \text{ such that } p \nmid \binom{q-1}{\mathbf{i}}\right\}$ between two bases of $F_{q-1}^{\dagger}[\mathbf{X}]$. Furthermore, $\theta(\mathcal{B}')$ is the set of all monomials $\mathbf{X}^{\mathbf{i}} = X_0^{i_0} X_1^{i_1} \ldots X_n^{i_n}$ of degree $q-1$ with $p \nmid \binom{q-1}{\mathbf{i}}$, such that the p-ary expansion $i_0 = i_{0,0} + i_{0,1}p + \ldots + i_{0,e-1}p^{e-1}$ contains at least one digit satisfying $i_{0,k} \ge 2$; for by definition, $i_{0,j} \ge 2$ if and only if $Q(\mathbf{X}) \mid g_{r_j}(\mathbf{X})$, if and only if $r_j \le b'$.

2.13 Lemma. *Let $n \ge 3$, and let $Q(\mathbf{X})$ be as in Assumption 2.12. Define $\mathcal{E}_{Q,\mathbf{X}}$ as above. Then the following three statements are equivalent.*

(i) $\operatorname{rank}_p A_1 = \left[\binom{p+n-1}{n} - \binom{p+n-3}{n}\right]^e + 1\,.$

(ii) $\mathcal{E}_{Q,\mathbf{X}} = F_{q-1}^{\dagger}[\mathbf{X}] \cap Q(\mathbf{X}) F_{q-3}[\mathbf{X}]$.

(iii) If $f(\mathbf{X}) \in F_{q-1}^{\dagger}[\mathbf{X}]$ contains no monomials in $\theta(\mathcal{B}')$, and $Q(\mathbf{X}) \mid f(\mathbf{X})$, then $f(\mathbf{X}) = 0$.

Before proving Lemma 2.13, we observe that $\operatorname{rank}_p A_1$ depends only on n and (possibly) on $\varepsilon(Q)$, in the notation of Lemma 2.2. Hence Lemma 2.13 implies that the validity of (ii), or of (iii), likewise only depends on n and (possibly) on $\varepsilon(Q)$.

Proof of Lemma 2.13. Combining Theorem 2.11 and Lemmas 2.6(ii) and 2.7, we have

$$\begin{aligned}
\operatorname{rank}_p A_1 &= 1 + \tbinom{p+n-1}{n}^e - \dim\left\{f(\mathbf{X}) \in F_{q-1}^{\dagger}[\mathbf{X}] \,:\, f \text{ vanishes on } \mathcal{Z}(Q)\right\} \\
&= 1 + \tbinom{p+n-1}{n}^e - \dim\left\{f(\mathbf{X}) \in F_{q-1}^{\dagger}[\mathbf{X}] \,:\, Q(\mathbf{X}) \mid f(\mathbf{X})\right\} \\
&\le 1 + \tbinom{p+n-1}{n}^e - \dim \mathcal{E}_{Q,\mathbf{X}} \\
&= 1 + \left[\tbinom{p+n-1}{n} - \tbinom{p+n-3}{n}\right]^e,
\end{aligned}$$

and equality holds iff $\mathcal{E}_{Q,\mathbf{X}} = F_{q-1}^{\dagger}[\mathbf{X}] \cap Q(\mathbf{X}) F_{q-3}[\mathbf{X}]$. Thus (i) $\Leftrightarrow$ (ii).

Assume that (ii) holds, and suppose $f(\mathbf{X}) \in F_{q-1}^{\dagger}[\mathbf{X}]$ contains no monomials in $\theta(\mathcal{B}')$, and $Q(\mathbf{X}) \mid f(\mathbf{X})$. If $f(\mathbf{X}) \ne 0$, then expressing $f(\mathbf{X})$ as a linear combination of polynomials in $\mathcal{B}'$, we may choose $\prod_j g_{r_j}(\mathbf{X})^{p^j} \in \mathcal{B}'$ appearing in $f(\mathbf{X})$ with maximal degree in X_0. By our choice of $\prod_j g_{r_j}(\mathbf{X})^{p^j} \in \mathcal{B}'$, no other elements of the basis $\mathcal{B}'$ appearing in $f(\mathbf{X})$ contribute the same monomial $\theta\left(\prod_j g_{r_j}(\mathbf{X})^{p^j}\right)$, and so $f(\mathbf{X})$ contains a monomial in $\theta(\mathcal{B}')$, contrary to hypothesis. Thus (ii) $\Rightarrow$ (iii).

Conversely, assume (iii) holds, and suppose that $f(\mathbf{X}) \in F^{\dagger}_{q-1}[\mathbf{X}]$ is divisible by $Q(\mathbf{X})$. It is easy to see that there exists $h(\mathbf{X}) \in \mathcal{E}_{Q,\mathbf{X}}$ such that none of the monomials in $\theta(\mathcal{B}')$ appear in $f(\mathbf{X})-h(\mathbf{X})$. For suppose that $f(\mathbf{X})$ contains monomials of the form $\mathbf{X}^{\mathbf{i}} = \theta(g(\mathbf{X}))$, $g(\mathbf{X}) \in \mathcal{B}'$, and among all such monomials, choose $\mathbf{X}^{\mathbf{i}} = X_0^{i_0}X_1^{i_1}\cdots X_n^{i_n} = \theta\big(g(\mathbf{X})\big)$ appearing in $f(\mathbf{X})$ for which i_0 is maximal. Let $c_{\mathbf{i}}$ be the coefficient of $\mathbf{X}^{\mathbf{i}}$ in $f(\mathbf{X})$; then $f(\mathbf{X})-c_{\mathbf{i}}g(\mathbf{X}) \in F^{\dagger}_{q-1}[\mathbf{X}]$ has one fewer monomial of degree i_0 in X_0, than does $f(\mathbf{X})$. Repeat this process with $f(\mathbf{X})-c_{\mathbf{i}}g(\mathbf{X})$ in place of $f(\mathbf{X})$. After a finite number of iterations, we obtain $f(\mathbf{X})-h(\mathbf{X}) \in F^{\dagger}_{q-1}[\mathbf{X}]$ having no monomials in $\theta(\mathcal{B}')$, where $h(\mathbf{X}) \in \mathcal{E}_{Q,\mathbf{X}}$. Then by assumption, $f(\mathbf{X})-h(\mathbf{X}) = 0$, and so (iii) $\Rightarrow$ (ii). □

Proof of Theorem 1.2. Theorem 1.2(ii) follows from Lemma 2.1. Theorem 1.2(i) holds for $n=2$ by Lemma 2.6(iii), and for $n \geq 3$ by the following.

2.14 Lemma. *The equivalent conditions of Lemma 2.13 hold whenever $n \geq 3$.*

Proof. For $n=3$, this follows from Lemma 2.9. Hence assume that $n \geq 4$, and proceed by induction on n. Suppose $f(\mathbf{X}) \in F^{\dagger}_{q-1}[\mathbf{X}]$ contains no monomials in $\theta(\mathcal{B}')$, and $Q(\mathbf{X}) \mid f(\mathbf{X})$. We must show that $f(\mathbf{X}) = 0$.

First consider the case that n is even (q even or odd). We may assume that $Q(\mathbf{X}) = X_0(X_0+X_1) + X_1X_2 + X_3X_4 + \cdots + X_{n-1}X_n$, in accordance with Assumption 2.12. Let $\ell(\mathbf{X}) = X_n - aX_2$, where $0 \neq a \in F$, so that the hyperplane $\mathcal{Z}(\ell)$ is nondegenerate. Then $Q_\ell(X_0,\ldots,X_{n-1}) := Q(X_0,\ldots,X_{n-1},\, aX_2)$ is a nondegenerate quadratic form in $(X_0,\ldots,X_{n-1})$, and Q_ℓ divides $f_\ell(X_0,\ldots,X_{n-1}) := f(X_0,\ldots,X_{n-1},\, aX_2)$. Observe that Q_ℓ satisfies Assumption 2.12 for $n-1$ in place of n. Every monomial appearing in $f(\mathbf{X})$ is of the form $\mathbf{X}^{\mathbf{i}} = X_0^{i_0}\cdots X_n^{i_n}$ such that each of the digits in the p-ary expansion $i_0 = \sum_{k=0}^{e-1} i_{0,k}p^k$ satisfies $0 \leq i_{0,k} \leq 1$. Hence every monomial appearing in $f_\ell(\mathbf{X})$ is of the form $X_0^{i_0}X_1^{i_1}X_2^{i_2'}X_3^{i_3}\cdots X_{n-1}^{i_{n-1}}$ where i_0 is as before. Also $f_\ell(X_0,\ldots,X_{n-1}) \in F^{\dagger}_{q-1}[X_0,\ldots,X_{n-1}]$ by Lemma 2.5(i). By induction, we have $f_\ell(X_0,\ldots,X_{n-1}) = 0$, i.e. $\ell(\mathbf{X}) \mid f(\mathbf{X})$. Thus $f(\mathbf{X})$ is divisible by $\prod_{a\neq 0}(X_n - aX_2) = X_n^{q-1} - X_2^{q-1}$. Similarly, $f(\mathbf{X})$ is divisible by $X_{n-1}^{q-1} - X_2^{q-1}$, so that $f(\mathbf{X}) = 0$.

Now suppose that n is odd, $n \geq 5$. We may suppose that $Q(\mathbf{X}) = X_0^2 + X_0X_1 + \alpha X_1^2 + X_2X_3 + \cdots + X_{n-1}X_n$, where the choice of $\alpha \in F$ depends on whether $\mathcal{Z}(Q)$ is hyperbolic or elliptic. Let $\ell(\mathbf{X}) = X_n - aX_1 - bX_{n-1}$, where $a, b \in F$ are chosen such that the hyperplane $\mathcal{Z}(\ell)$ is nondegenerate. This means that $a^2 \neq (4\alpha - 1)b$, and since $4\alpha \neq 1$ (otherwise $Q(\mathbf{X})$ would be degenerate), there are $q(q-1)$ such choices for $\ell(\mathbf{X})$. As before, we obtain $\ell(\mathbf{X}) \mid f(\mathbf{X})$. This gives $q(q-1) > q-1$ linear factors for $f(\mathbf{X})$, and so $f(\mathbf{X}) = 0$. $\square$

3. Representations of the Orthogonal Group

Let $G = GL(n+1, F)$, and let H be the isometry group of the quadratic form Q, otherwise known as the orthogonal group. That is, H is the set of all $T \in G$ such that $Q(T\mathbf{X}) = Q(\mathbf{X})$. Our goal is to determine, as far as possible, the row and column and row spaces of A_1 and A_{11} as FH-modules. We begin, however, with some general remarks.

Let $\mathrm{Perm}(r)$ denote the group of $r \times r$ permutation matrices. Let B be any $k \times \ell$ matrix over F, and let Γ be any group. An *action* of Γ on B is a homomorphism $\Gamma \to \mathrm{Perm}(k) \times \mathrm{Perm}(\ell)$, $g \mapsto (L(g), R(g))$ such that $L(g)^\top B R(g) = B$ for all $g \in \Gamma$. In the special case that B is square and invertible, then L and R are equivalent linear representations (although not necessarily equivalent permutation representations) of degree $k = \ell$. We may generalize this well-known fact by saying that the column and row spaces of B are isomorphic $F\Gamma$-modules. Here, the column space of B means the F-span of the columns of B; this is invariant under left-multiplication by every $L(g)^\top$, and so forms an $F\Gamma$-submodule of $F^k = \{k \times 1 \text{ vectors over } F\}$. The row space of B is described dually. We loosely refer to either the row space or column space of B as the *code* of B, since these are isomorphic $F\Gamma$-modules, even though they are not isomorphic as codes, in the usual sense of code isomorphism; indeed in general, they have different lengths.

Now we see that the code of A is a natural FG-module of dimension $\binom{p+n-1}{n}^e + 1$. Likewise, the code of A_1 (or of A_{11}) is an FH-module of dimension given by Theorem 1.2. We proceed to investigate these modules.

3.1 Theorem. *The code of A is an FG-module isomorphic to $\langle \mathbf{1} \rangle \oplus F^\dagger_{q-1}[\mathbf{X}] \cong \langle \mathbf{1} \rangle \oplus \left(\bigotimes_{j=0}^{e-1} \mathcal{V}_{p-1}^{(j)} \right)$, where $\langle \mathbf{1} \rangle$ is the (one-dimensional) trivial FG-module.*

Proof. Let $T \mapsto (L(T), R(T))$ denote the action of G on A, as above. The column space of A satisfies $\mathit{Col}(A) = \langle \mathbf{1} \rangle \oplus \mathit{Col}(J - A)$ as a direct sum of FG-modules, where $\mathbf{1} = (1, 1, \ldots, 1)^\top$ of length m, which is fixed by G.

Choose coördinates $P_i = \langle(x_{i0}, x_{i1}, \ldots, x_{in})\rangle$ for the points of $PG(n,F)$, $i = 1, 2, \ldots, m$. For each $f(\mathbf{X}) \in F^{\dagger}_{q-1}[\mathbf{X}]$, the value of $f(P_i) \in F$ is well-defined since $\lambda^{q-1} = 1$ for all nonzero $\lambda \in F$. The map $\phi : F^{\dagger}_{q-1}[\mathbf{X}] \to F^m$, $f(\mathbf{X}) \mapsto (f(P_1), f(P_2), \ldots, f(P_m))^\top$ is F-linear, and for all $T \in G$,

$$\begin{aligned}\phi(Tf(\mathbf{X})) &= \phi f(T\mathbf{X}) = (f(TP_1), \ldots, f(TP_m))^\top \\ &= L(T)^\top (f(P_1), \ldots, f(P_m))^\top = L(T)^\top \phi f(\mathbf{X}) \,.\end{aligned}$$

Thus ϕ is an FG-homomorphism. Every hyperplane of $PG(n,F)$ is of the form $H_j = \mathcal{Z}(\ell_j)$ for some $\ell_j \in F_1[\mathbf{X}]$, and the j-th column of $J - A$ is $\phi(\ell_j(\mathbf{X})^{q-1})$. So $\phi(U) = \mathit{Col}(J-A)$ where $U \le F^{\dagger}_{q-1}[\mathbf{X}]$ is the subspace spanned by all polynomials $\ell(\mathbf{X})^{q-1}$ such that $\ell \in F_1[\mathbf{X}]$. Comparing dimensions by Theorem 1.1 and Lemma 2.4, we see that in fact $U = F^{\dagger}_{q-1}[\mathbf{X}]$ and ϕ is an FG-isomorphism from $F^{\dagger}_{q-1}[\mathbf{X}]$ to $\mathit{Col}(J-A)$. $\square$

The following is evident from the proof of Theorem 3.1.

3.2 Corollary. *$F^{\dagger}_{q-1}[\mathbf{X}]$ is spanned by the polynomials $\ell(\mathbf{X})^{q-1}$ for which $\ell(\mathbf{X}) \in F_1[\mathbf{X}]$.*

Suppose now that n and q are both even, and let $\langle \mathbf{x} \rangle = V^\perp$, the radical point of $V = F^{n+1}$. Recall, from Lemma 2.1, that A_{11} is the incidence matrix of points and hyperplanes of $V/\langle \mathbf{x} \rangle$. Furthermore, $(\mathbf{X}, \mathbf{Y})$ induces a nondegenerate H-invariant symplectic form on $V/\langle \mathbf{x} \rangle$, so that H acts on A_{11} as $Sp(n,q)$ (see Theorem 11.9 of [13]). This yields the following.

3.3 Theorem. *Suppose that $n = 2m$ and $q = 2^e$. Then the code of A_{11} is an FH-module of dimension $n^e + 1$. This is the usual permutation module for $Sp(2m,q)$ acting on the points (or hyperplanes) of $PG(2m-1,q)$.*

For $n = 2$, we have $H \cong SL(2,q)$ or $\langle -I \rangle \times SL(2,q)$ according as q is even or odd, and it is clear that the code of A_1 is the usual permutation module for H of degree $q+1$. Therefore in what follows, we shall consider only the case $n \ge 3$, in which case we have seen (Lemma 2.14) that $\mathcal{E}_{Q,\mathbf{X}} = Q(\mathbf{X}) F_{q-3}[\mathbf{X}] \cap F^{\dagger}_{q-1}[\mathbf{X}]$.

There are two obvious FH-submodules of $F^{\dagger}_{q-1}[\mathbf{X}]$ of interest. One is $\mathcal{E}_{Q,\mathbf{X}}$. The other, which we denote $\mathcal{L}_{Q,\mathbf{X}}$, is the subspace of $F^{\dagger}_{q-1}[\mathbf{X}]$ spanned by all polynomials $\ell(\mathbf{X})^{q-1}$ where $\ell(\mathbf{X}) \in F_1[\mathbf{X}]$ such that $\mathcal{Z}(\ell)$ is a tangent hyperplane to the quadric $\mathcal{Z}(Q)$, i.e. one of the hyperplanes $P_1^\perp, \ldots, P_s^\perp$. Equivalently, $\mathcal{L}_{Q,\mathbf{X}}$ is the span of the polynomials $(\mathbf{X},\mathbf{x})^{q-1}$ such that $\langle\mathbf{x}\rangle$ is a point of the quadric $\mathcal{Z}(Q)$.

3.4 Theorem. *Suppose that $n\geq 3$. Then the code of A_1 is an FH-module isomorphic to $\langle\mathbf{1}\rangle \oplus \left(F_{q-1}^\dagger[\mathbf{X}]/\mathcal{E}_{Q,\mathbf{X}}\right)$. Moreover, the latter is isomorphic to $\langle\mathbf{1}\rangle \oplus \mathcal{L}_{Q,\mathbf{X}}$ if q and n are not both even.*

Proof. As in the proof of Theorem 3.1, we have $Col(A_1) = \langle\mathbf{1}\rangle \oplus Col(J - A_1)$ where the $s\times 1$ vector $\mathbf{1}$ spans a trivial module. Imitating the proof of Theorem 3.1, we truncate the map ϕ to obtain an FH-homomorphism $\psi : F_{q-1}^\dagger[\mathbf{X}] \to F^s,\ f(\mathbf{X}) \mapsto ((f(P_1),\ldots,f(P_s))^\top$. The j-th column of A_1 is $\psi(\ell_j(\mathbf{X})^{q-1})$, so by Corollary 3.2, $\psi(F_{q-1}^\dagger[\mathbf{X}]) = Col(J - A_1)$. Also, $\psi(f(\mathbf{X})) = \mathbf{0}$ if and only if $f(\mathbf{X})$ vanishes on $\mathcal{Z}(Q)$, so by Theorem 2.11 and Lemma 2.14, $\ker\psi = \mathcal{E}_{Q,\mathbf{X}}$. It follows that $Col(J - A_1) \cong F_{q-1}^\dagger[\mathbf{X}]/\mathcal{E}_{Q,\mathbf{X}}$.

Now suppose that q and n are not both even, so that $\perp$ is a polarity (orthogonal or symplectic, according as q is odd or even). We may assume that A is symmetric, so that $A_1^\top = \binom{A_{11}}{A_{21}}$, whose code is isomorphic to that of A_1. Now if $H_j = \mathcal{Z}(\ell_j)$ is a tangent hyperplane to the quadric $(1\leq j\leq s)$, then $\phi(\ell_j(\mathbf{X})^{q-1})$ is the j-th column of $J - A_1^\top$, where ϕ and $\ell_j(\mathbf{X})$ are as in the proof of Theorem 3.1. So the restriction of ϕ to $\mathcal{L}_{Q,\mathbf{X}}$ is an isomorphism $\mathcal{L}_{Q,\mathbf{X}} \to Col(J - A_1^\top)$. $\square$

By considering the restriction of ψ (as above) to $\mathcal{L}_{Q,\mathbf{X}}$, we also obtain

3.5 Theorem. *Suppose that $n \geq 3$. Then the code of A_{11} is an FH-module isomorphic to $\langle\mathbf{1}\rangle \oplus Col(J - A_{11})$, where*

$$Col(J - A_{11}) \cong (\mathcal{L}_{Q,\mathbf{X}} + \mathcal{E}_{Q,\mathbf{X}})/\mathcal{E}_{Q,\mathbf{X}} \cong \mathcal{L}_{Q,\mathbf{X}}/(\mathcal{L}_{Q,\mathbf{X}} \cap \mathcal{E}_{Q,\mathbf{X}})\,.$$

However, we have not determined the dimension of the latter module in general.

4. Bounds for Caps and Ovoids

We proceed to define terms and to prove Results 1.3 through 1.9.

Let $\mathcal{S}$ be a cap on a nondegenerate quadric $\mathcal{Z}(Q)$ in $PG(n,F)$. As in Section 1, we may suppose that $\mathcal{S} = \{P_1, P_2, \ldots, P_k\}$, $\mathcal{Z}(Q) = \{P_1,\ldots,P_k,\ldots,P_s\}$ and that the hyperplanes $H_1, H_2, \ldots, H_m$ of $PG(n,F)$ are ordered such that $H_i = P_i^\perp$ for $1\leq i\leq s$. By definition of a cap, for $1 \leq i,j \leq k$ we have $P_i \in P_j^\perp$ if and only if $i=j$. Thus the upper-left $k\times k$

submatrix of A_{11} is a $k \times k$ identity matrix. It follows that $\operatorname{rank}_p A_1 \geq \operatorname{rank}_p A_{11} \geq k$, and so Theorem 1.3 follows from Theorem 1.2.

If $n = 2m$ then by the general theory (see [7], [14]), $|\mathcal{S}| \leq q^m + 1$, and equality occurs if and only if $\mathcal{S}$ is an ovoid. If $n = 2m-1$ then $|\mathcal{S}| \leq q^{m-1}+1$ or $|\mathcal{S}| \leq q^m + 1$ according as $\mathcal{Z}(Q)$ is hyperbolic or elliptic; again, equality occurs if and only if $\mathcal{S}$ is an ovoid. Thus Corollary 1.4 follows from Theorem 1.3, and Corollary 1.5 follows easily. Actually, we see that the inequality in Corollary 1.4 may be improved slightly when $n = 2m-1$ and $\mathcal{Z}(Q)$ is elliptic; however this case does not concern us greatly since it is known [14] that elliptic quadrics in $PG(2m-1, q)$ do not have ovoids for $m \geq 3$.

The simplicity of our bounds for ovoids, Corollaries 1.3 and 1.7, is a consequence of a seeming coincidence, for which we have no satisfying explanation: namely, the p-ranks given by Theorems 1.1 and 1.2 are both of the form $\left(\text{integer}\right)^e + 1$, and it is also true that the size of an ovoid in any finite classical polar space is an integer of this form.

Now let $\perp$ be a symplectic or unitary polarity of $PG(n, q)$, where n is odd in the symplectic case, and q is a square in the unitary case. The set of all projective subspaces U of $PG(n, q)$ such that $U \subseteq U^\perp$, together with the natural incidence relation of inclusion, is a polar space of symplectic or unitary type, according to $\perp$.

Finite orthogonal polar spaces can be defined similarly using an orthogonal polarity, in the case of odd characteristic. But to allow arbitrary finite characteristic, we instead define a finite orthogonal polar space as the set of projective subspaces of $PG(n, q)$ which lie on a nondegenerate quadric $\mathcal{Z}(Q)$, again with inclusion as the incidence relation. We denote by $U^\perp$ the orthogonal 'perp' of U with respect to the bilinear form associated to Q. Recall that if q is even, then $\perp$ is a symplectic polarity when n is odd, and not a polarity at all when n is even.

Let $\mathcal{P}$ be a *finite classical polar space,* i.e. a finite polar space of orthogonal, symplectic or unitary type as defined above, naturally embedded in $PG(n, q)$. A *cap* in $\mathcal{P}$ is a set $\mathcal{S}$ consisting of points of $\mathcal{P}$, such that $X \notin Y^\perp$ whenever $X \neq Y$ are in $\mathcal{S}$. An *ovoid* of $\mathcal{P}$ is a cap $\mathcal{O}$ such that every *generator* (i.e. maximal member) of $\mathcal{P}$ contains a (unique) point of $\mathcal{O}$. Let A be the point-hyperplane incidence matrix of $PG(n, q)$, with respect to some ordering of points as $P_1, P_2, \ldots, P_m$ and hyperplanes as $H_1, H_2, \ldots, H_m$. Just as in Section 1, we may suppose that $P_1, \ldots, P_s$ are the points of $\mathcal{P}$, and that $H_i = P_i^\perp$ for $1 \leq i \leq s$. Again, this gives a matrix partition

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

where A_{11} is $s\times s$, A_{12} is $s\times(m-s)$, etc. (In the symplectic case, every point is absolute, so $s=m$ and $A_{11}=A$.) Except in the case of orthogonal polar spaces in $PG(2m,2^e)$, we may suppose moreover that $H_i=P_i^\perp$ for $1\le i\le m$ and A is symmetric. Clearly, Theorem 1.6 is a consequence of the following, together with Theorem 1.1.

4.1 Proposition. *Let $\mathcal{P}$ be a finite classical polar space naturally embedded in $PG(n,q)$.*

(i) If $\mathcal{S}$ is a cap in $\mathcal{P}$, then $|\mathcal{S}|\le \operatorname{rank}_p A_{11}$.

(ii) If $\mathcal{P}$ is not of orthogonal type in $PG(2m,2^e)$, then $2\operatorname{rank}_p\big(A_{11}\ A_{12}\big)-\operatorname{rank}_p A\le \operatorname{rank}_p A_{11}\le \operatorname{rank}_p\big(A_{11}\ A_{12}\big)\le \operatorname{rank}_p A$.

Proof. Let $\mathcal{S}=\{P_1,P_2,\ldots,P_k\}$ be a cap in $\mathcal{P}$. Then the upper-left $k\times k$ submatrix of A_{11} is a $k\times k$ identity matrix, which proves (i).

Suppose that $\mathcal{P}$ is not of orthogonal type in $PG(2m,2^e)$. By the remarks above, we may suppose that A is symmetric. Let U be the space consisting of all row vectors $\mathbf{u}$ of length $m-s$ such that $\mathbf{u}\big(A_{21}\ A_{22}\big)$ is in the row space of $\big(A_{11}\ A_{12}\big)$; then $\dim U=m-s-\operatorname{rank}_p A+\operatorname{rank}_p\big(A_{11}\ A_{12}\big)$. Similarly, let U' be the space of all row vectors $\mathbf{u}$ of length $m-s$ such that $\mathbf{u}A_{21}$ is in the row space of A_{11}; then $\dim U'=m-s-\operatorname{rank}_p\binom{A_{11}}{A_{21}}+\operatorname{rank}_p A_{11}$. Clearly $U\le U'$. Also $\operatorname{rank}_p\big(A_{11}\ A_{12}\big)=\operatorname{rank}_p\binom{A_{11}}{A_{21}}$ by duality. Together this gives $2\operatorname{rank}_p\big(A_{11}\ A_{12}\big)-\operatorname{rank}_p A\le\operatorname{rank}_p A_{11}$, and the remaining inequalities in (ii) are trivial. $\square$

Further insight into the above bounds for the p-rank of A_{11} is provided by the following, which follows directly from Theorems 3.1, 3.4 and 3.5, and Lemma 2.8.

4.2 Corollary. *Suppose that $\mathcal{P}$ is an orthogonal polar space arising from a nondegenerate quadric in $PG(n,q)$, $q=p^e$, where n and q are not both even. Then in the notation of Section 3, we have* $\operatorname{rank}_p A_{11}=\left[\binom{p+n-1}{n}-\binom{p+n-3}{n}\right]^e+1-r$*, where*

$$0\le r=\dim\left(\mathcal{E}_{Q,\mathbf{X}}\cap\mathcal{L}_{Q,\mathbf{X}}\right)\le\dim\mathcal{E}_{Q,\mathbf{X}}=\binom{p+n-1}{n}^e-\left[\binom{p+n-1}{n}-\binom{p+n-3}{n}\right]^e.$$

The upper bound for $\operatorname{rank}_p A_{11}$ occurs if and only if $\mathcal{E}_{Q,\mathbf{X}}\cap\mathcal{L}_{Q,\mathbf{X}}=0$, if and only if $\mathcal{E}_{Q,\mathbf{X}}+\mathcal{L}_{Q,\mathbf{X}}=F_{q-1}^\dagger[\mathbf{X}]$; it is not known how often this occurs. An explicit determination of $\operatorname{rank}_p A_{11}$ may yield a slight improvement to our bounds for caps and ovoids, but not enough to eliminate all orthogonal ovoids in $O^+_{10}(q)$, in light of the lower bound for $\operatorname{rank}_p A_{11}$.

For a unitary polar space embedded naturally in $PG(2m-1, q^2)$, an ovoid is equivalent [7] to a cap of size $q^{2m-1}+1$, and so Corollary 1.7 follows from Corollary 1.6; also Corollary 1.8 follows.

Finally, we prove Theorem 1.9, which highlights a very interesting parallel between orthogonal ovoids in $O_7(3^e)$ and $O^+_8(2^e)$, and ordinary ovoids of $PG(3, 2^e)$.

Only two families of ovoids in $O_7(q)$ are known, and both occur in characteristic 3: the *unitary ovoids* in $O_7(3^e)$ for all $e \geq 1$, so-called because they admit $PSU_3(3^e)$ as an automorphism group; and the *Ree-Tits ovoids* for e odd, which admit ${}^2G_2(3^e)$. (These two constructions coincide for $O_7(3)$.) No argument currently exists to show that these are the only ovoids in $O_7(q)$, although Corollary 1.5 excludes characteristic 2. Observe that for a nondegenerate quadric in $PG(6, 3^e)$, we have $\operatorname{rank}_3 A_1 = \left[\binom{8}{6} - \binom{6}{6}\right]^e + 1 = 27^e + 1 = q^3 + 1$, which is exactly the size of an ovoid. This means that for any ovoid $\mathcal{O}$ in $O_7(3^e)$, the rows of A_1 indexed by points $P \in \mathcal{O}$, form a basis for the row space of A_1. The dual of this statement verifies Theorem 1.9(ii) in the case of $O_7(3^e)$.

Exactly the same situation arises for ovoids in $O^+_8(2^e)$, where $\operatorname{rank}_2 A_1 = \left[\binom{8}{7} - \binom{6}{7}\right]^e + 1 = 8^e + 1 = q^3 + 1 = |\mathcal{O}|$, which completes the proof of Theorem 1.9(ii). In this case just two infinite families of ovoids and one sporadic example are known [8]: the Desarguesian ovoids in $O^+_8(2^e)$ for all $e \geq 1$; the unitary ovoids for e odd, and Dye's ovoid in $O^+_8(2^3)$.

Recall [4] that an *ovoid* of $PG(3, q)$ is a set of $q^2 + 1$ points, no three of which are collinear. For q odd, such ovoids are necessarily elliptic quadrics; however for q even, no classification is known. The known ovoids in $PG(3, 2^e)$ are the elliptic quadrics (for all $e \geq 1$) and the *Suzuki-Tits ovoids* (for e odd). By Theorem 1.1, the point-plane incidence matrix A of $PG(3, 2^e)$ has 2-rank equal to $\binom{4}{3}^e + 1 = q^2 + 1$, exactly the number of points in an ovoid. This proves Theorem 1.9(i). Considerably more effort has been expended in attempts to classify ovoids in $PG(3, 2^e)$ than in the orthogonal spaces $O_7(3^e)$ and $O^+_8(2^e)$, but our observations suggest that a greater use of coding theory may be helpful in each of these problems.

5. Codes of Projective Planes

It is well known that the code of $PG(2,p)$ spanned by the lines, in the natural characteristic p, has dimension $\frac{1}{2}p(p+1)+1$. Since a nondegenerate conic has $\frac{1}{2}p(p+1)$ secants and $\frac{1}{2}p(p+1)+1$ nonsecants, it is tempting to use these to form explicit bases for the code, and with this motivation we prove the more general Theorem 1.10. (See [10] for a construction of other such explicit bases.) Curiously, this is accomplished by our study in Section 2 of quadrics in $PG(3,q)$, beginning with the following, in odd characteristic.

5.1 Lemma. *Let $f(\mathbf{X}) \in F_d[\mathbf{X}]$, $d \le q-1$ where $q=|F|$ is odd, $\mathbf{X} = (X_0, X_1, X_2)$, and define $Q(\mathbf{X}) = X_0^2 - X_1X_2$.*

(i) $\mathcal{Z}(Q)$ is a nondegenerate conic in $PG(2,F)$. For each $\mathbf{x} \in F^3 \smallsetminus \{\mathbf{0}\}$, the corresponding point $\langle \mathbf{x} \rangle$ is absolute, exterior or interior with respect to this conic, according as $Q(\mathbf{x})$ is zero, a nonzero square or a nonsquare.

(ii) If $f(\mathbf{x})=0$ whenever $Q(\mathbf{x}) \in F$ is a nonzero square, then $f=0$.

(iii) If $f(\mathbf{x})=0$ whenever $Q(\mathbf{x}) \in F$ is zero or a nonsquare, then $f=0$.

Proof. (i) See Theorem 8.3.3 of [6].
(ii) Define $\widetilde{Q}(X_0,X_1,X_2,X_3) = X_0^2 - X_1X_2 - X_3^2$. Then $\mathcal{Z}(\widetilde{Q})$ is a hyperbolic quadric in $PG(3,F)$. Given $f(\mathbf{X})$ satisfying the hypotheses, define $\widetilde{f}(X_0,X_1,X_2,X_3) = X_3 f(X_0, X_1,X_2) \in F_{d+1}[X_0,X_1,X_2,X_3]$. For any point (x_0,x_1,x_2,x_3) on the quadric $\mathcal{Z}(\widetilde{Q})$, we have $Q(x_0,x_1,x_2) = x_3^2$. Then either $x_3 \ne 0$ so $f(x_0,x_1,x_2)=0$ by hypothesis and $\widetilde{f}(x_0,x_1,x_2,x_3)=0$, or $x_3=0$ and again $\widetilde{f}(x_0,x_1,x_2,x_3)=0$. Thus $\widetilde{f}$ vanishes on $\mathcal{Z}(\widetilde{Q})$. By Theorem 2.11, $\widetilde{f}=0$ and so $f=0$.
(iii) Let $\epsilon \in F$ be a given nonsquare, and define $\widetilde{Q}(X_0,X_1,X_2,X_3) = X_0^2 - X_1X_2 - \epsilon X_3^2$. Then $\mathcal{Z}(\widetilde{Q})$ is an elliptic quadric in $PG(3,F)$. Given $f(\mathbf{X})$ satisfying the hypotheses, define $\widetilde{f}(X_0,X_1,X_2,X_3) = f(X_0,X_1,X_2) \in F_d[X_0,X_1,X_2,X_3]$. For any point (x_0,x_1,x_2,x_3) on the quadric $\mathcal{Z}(\widetilde{Q})$, we have $Q(x_0,x_1,x_2) = \epsilon x_3^2$, which is either zero or a nonsquare. Thus $\widetilde{f}(x_0,x_1,x_2,x_3) = f(x_0,x_1,x_2)=0$ by hypothesis. Again $\widetilde{f}=0$ by Theorem 2.11, and so $f=0$. □

Let $\mathcal{Z}(Q)$ be an irreducible conic in $PG(2,q)$, where $q=p^e$ is odd. Let A be the point-line incidence matrix of $PG(2,q)$, partitioned as

$$A = \begin{pmatrix} A_{\text{ext}} \\ A_{\text{nonext}} \end{pmatrix}$$

where A_{ext} consists of the first $\frac{1}{2}q(q+1)$ rows of A, indexed by the exterior points with respect to the conic $\mathcal{Z}(Q)$, and A_{nonext} consists of the remaining rows, indexed by the $\frac{1}{2}q(q-1)$ interior points and the $q+1$ absolute points of the conic. We may suppose that $Q(\mathbf{X}) = X_0^2 - X_1X_2$ where $\mathbf{X} = (X_0, X_1, X_2)$. As in Section 2, let $M = \big((\mathbf{x}\mathbf{y}^\top)^{q-1}\big)$, which is a $q^3 \times q^3$ matrix with rows and columns indexed by the row vectors $\mathbf{x}, \mathbf{y} \in F^3$. We may assume that

$$M = \begin{pmatrix} M_{\text{sq}} \\ M_{\text{nonsq}} \end{pmatrix}$$

where M_{sq} consists of the first $\frac{1}{2}q(q^2-1)$ rows of M, indexed by those vectors $\mathbf{x}$ such that $Q(\mathbf{x}) \in F$ is a nonzero square, and M_{nonsq} consists of the remaining $\frac{1}{2}q(q^2+1)$ rows of M, indexed by those $\mathbf{x}$ such that $Q(\mathbf{x})$ is zero or a nonsquare. Clearly, in the case q is odd, Theorem 1.10 is a consequence of (the dual of) the following, in which each J denotes an all-1's matrix of the appropriate size.

5.2 Lemma. *For q odd,*

(i) $\operatorname{rank}_p A_{\text{ext}} = \operatorname{rank}_p(J - A_{\text{ext}}) = \operatorname{rank}_p M_{\text{sq}} = \binom{p+1}{2}^e$.

(ii) $\operatorname{rank}_p A_{\text{nonext}} = \operatorname{rank}_p(J - A_{\text{nonext}}) + 1 = \operatorname{rank}_p M_{\text{nonsq}} + 1 = \binom{p+1}{2}^e + 1$.

Proof. As in the proof of Lemma 2.6, permuting as necessary the rows and columns of M_{sq} (respectively, M_{nonsq}), and deleting duplicate rows and columns as well as all-zero rows and columns, yields $J - A_{\text{ext}}$ (respectively, $J - A_{\text{nonext}}$). Thus $\operatorname{rank}_p M_{\text{sq}} = \operatorname{rank}_p(J - A_{\text{ext}})$ and $\operatorname{rank}_p M_{\text{nonsq}} = \operatorname{rank}_p(J - A_{\text{nonext}})$.

To show that A_{ext} and $J - A_{\text{ext}}$ have the same column space, and hence the same p-rank, it suffices to show that the column vector $\mathbf{1}^\top = (1, 1, \ldots, 1)^\top$ of length $\frac{1}{2}q(q+1)$ lies in the column space of both matrices. But the sum of the columns of A_{ext} over F is $\mathbf{1}^\top$. And adding together those columns of $J - A_{\text{ext}}$ indexed by tangent lines, gives $-\mathbf{1}^\top$, which suffices.

Now let $\mathbf{1}^\top = (1, 1, \ldots, 1)^\top$ of length $\frac{1}{2}q(q+1)+1$, the sum of the columns of A_{nonext}, and let $\mathbf{v}^\top$ be the column vector of length $\frac{1}{2}q(q+1)+1$ having entries '2' and '1' in those positions indexed by interior points and absolute points of $\mathcal{Z}(Q)$, respectively. Using the fact that each secant line has $(q-1)/2$ interior points, and each passant has $(q+1)/2$ interior points, we have $\mathbf{v}(J - A_{\text{nonext}}) = \mathbf{0}$, whereas $\mathbf{v}\mathbf{1}^\top = 1$. This shows that $\mathit{Col}(J - A_{\text{nonext}}) = \mathit{Col}(A_{\text{nonext}}) \cap (\mathbf{v}^\top)^\perp \subsetneq \mathit{Col}(A_{\text{nonext}})$ where *'Col'* denotes column space. Thus $\operatorname{rank}_p(J - A_{\text{nonext}}) = \operatorname{rank}_p A_{\text{nonext}} - 1$.

Combining the technique of proof of Lemma 2.7 with the results of Lemmas 2.4 and 5.1, we have

$$\begin{aligned}\operatorname{rank}_p M_{\rm sq} &= q^3 - \dim\Big(\text{right null space of } M_{\rm sq}\Big)\\ &= \dim F^{\dagger}_{q-1}[\mathbf{X}] - \dim\big\{f(\mathbf{X})\in F^{\dagger}_{q-1}[\mathbf{X}] \,:\, f(\mathbf{x})=0\\ &\qquad\qquad\qquad\qquad\qquad\qquad \text{whenever } Q(\mathbf{x})\in F \text{ is a square}\big\}\\ &= \tbinom{p+1}{2}^e - 0 \;=\; \operatorname{rank}_p M,\end{aligned}$$

and similarly for $M_{\rm nonsq}$. □

Henceforth q is even, and it remains to prove Theorem 1.10 in this case. Define $S = \big\{x^2+x \,:\, x\in F\big\} \subset F$. Then S is closed under addition, $|S| = q/2$ and S will play a rôle analogous to that of the squares in the case of odd characteristic. (It is well known, although not important here, that S consists of all elements of F which have trace zero over the prime field.) An analogue of Lemma 5.1 is the following.

5.3 Lemma. *Let $f(\mathbf{X}) \in F_d[\mathbf{X}]$, $d\le q-1$ where $\mathbf{X} = (X_0, X_1, X_2)$ and $q=|F|$ is even, and define $Q(\mathbf{X}) = X_0^2 + X_1X_2$.*

(i) $\mathcal{Z}(Q)$ is a nondegenerate conic in $PG(n,F)$ with nucleus $\langle(1,0,0)\rangle$. For each $(\beta,\gamma)\neq(0,0)$, the line $\mathcal{Z}(\beta X_1+\gamma X_2)$ is a tangent; the line $\mathcal{Z}(X_0+\beta X_1+\gamma X_2)$ is a secant or passant, according as $\beta\gamma\in S$ or $\beta\gamma\in F\smallsetminus S$.

(ii) If $f(1,\beta,\gamma)=0$ whenever $\beta\gamma\in S$, then $f=0$.

(iii) If $f(\alpha,\beta,\gamma)=0$ whenever $\alpha=0$, and $f(1,\beta,\gamma)=0$ whenever $\beta\gamma\in F\smallsetminus S$, then $f=0$.

Proof. (i) Each line of the form $\mathcal{Z}(X_0+\beta X_1)$ contains two points $\langle(0,0,1)\rangle$, $\langle(\beta,1,\beta^2)\rangle$ of the conic $\mathcal{Z}(Q)$. If $\gamma\neq 0$ and $\beta\gamma\in S$, say $\beta\gamma = x^2+x$, then $\mathcal{Z}(X_0+\beta X_1+\gamma X_2)$ contains two points $\big\langle\big(\gamma x,\gamma^2,x^2\big)\big\rangle$, $\big\langle\big(\gamma(x{+}1),\gamma^2,x^2{+}1\big)\big\rangle$ of the conic. We have produced $q(q+1)/2$ lines of the form $\mathcal{Z}(X_0+\beta X_1+\gamma X_2)$, each of which we have shown to be a secant; hence these constitute all the $q(q+1)/2$ secants. The remaining assertions are left as an exercise. (ii) Define $\widetilde{Q}(X_0,X_1,X_2,X_3) = X_0^2+X_1X_2+X_0X_3$. Then $\mathcal{Z}(\widetilde{Q})$ is a hyperbolic quadric in $PG(3,F)$. Given $f(\mathbf{X})$ satisfying the hypotheses, define $\widetilde{f}(X_0,X_1,X_2,X_3) = X_3 f(X_3, X_2, X_1) \in F_{d+1}[X_0,X_1,X_2,X_3]$. Let (x_0,x_1,x_2,x_3) be any point on the quadric $\mathcal{Z}(\widetilde{Q})$. If $x_3=0$ then $\widetilde{f}(x_0,x_1,x_2,x_3)=0$. Otherwise $x_3\neq 0$ and

$$\Big(\frac{x_1}{x_3}\Big)\Big(\frac{x_2}{x_3}\Big) \;=\; \Big(\frac{x_0}{x_3}\Big)^2 + \Big(\frac{x_0}{x_3}\Big) \;\in\; S,$$

so that $f\big(1,\frac{x_2}{x_3},\frac{x_1}{x_3}\big) = 0$ by hypothesis, whence $\widetilde{f}(x_0,x_1,x_2,x_3) = x_3 f(x_3,x_2,x_1) = 0$. Thus $\widetilde{f}$ vanishes on $\mathcal{Z}(\widetilde{Q})$. By Theorem 2.11, $\widetilde{f}=0$ and so $f=0$.

(iii) Fix $\epsilon \in F \smallsetminus S$, and define $\widetilde{Q}(X_0,X_1,X_2,X_3) = X_0^2+X_1X_2+X_0X_3+\epsilon X_3^2$. Then $\mathcal{Z}(\widetilde{Q})$ is an elliptic quadric in $PG(3,F)$. Given $f(\mathbf{X})$ satisfying the hypotheses, define $\widetilde{f}(X_0,X_1,X_2,X_3) = f(X_3,X_2,X_1) \in F_d[X_0,X_1,X_2,X_3]$. Let (x_0,x_1,x_2,x_3) be any point on the quadric $\mathcal{Z}(\widetilde{Q})$. If $x_3=0$ then $\widetilde{f}(x_0,x_1,x_2,x_3) = f(0,x_2,x_1) = 0$ by hypothesis. Otherwise $x_3 \neq 0$ and

$$\Big(\frac{x_1}{x_3}\Big)\Big(\frac{x_2}{x_3}\Big) = \Big(\frac{x_0}{x_3}\Big)^2 + \Big(\frac{x_0}{x_3}\Big) + \epsilon \in F \smallsetminus S$$

since S is closed under addition. Thus $f\big(1,\frac{x_2}{x_3},\frac{x_1}{x_3}\big) = 0$ by hypothesis, whence $\widetilde{f}(x_0,x_1,x_2,x_3) = f(x_3,x_2,x_1) = 0$. Again $\widetilde{f}=0$ by Theorem 2.11, and so $f=0$. $\square$

To complete the proof of Theorem 1.10 in the case of even characteristic, duality does not apply. Let $\mathcal{Z}(Q)$ be an irreducible conic in $PG(2,q)$ where $q=2^e$. Let A be the point-line incidence matrix of the plane, partitioned as

$$A = \big(A_{\text{sec}} \;\; A_{\text{nonsec}}\big)$$

where A_{sec} consists of the first $\frac{1}{2}q(q+1)$ columns of A, indexed by the secant lines with respect to $\mathcal{Z}(Q)$, and A_{nonsec} consists of the remaining columns, indexed by the $\frac{1}{2}q(q-1)$ passants and the $q+1$ tangents. We may suppose that $Q(\mathbf{X}) = X_0^2+X_1X_2$ where $\mathbf{X} = (X_0,X_1,X_2)$. Let $M = \big((\mathbf{x}\mathbf{y}^\top)^{q-1}\big)$ be as before, and we may assume that

$$M = \big(M_S \;\; M_{F\smallsetminus S}\big)$$

where M_S consists of the first $\frac{1}{2}q(q^2-1)$ columns of M, indexed by those row vectors $\mathbf{y}$ such that $y_0 \neq 0$, $y_1y_2/y_0^2 \in S$, and $M_{F\smallsetminus S}$ consists of the remaining $\frac{1}{2}q(q^2+1)$ columns of M. The proof of Theorem 1.10 is completed by the following lemma.

5.4 Lemma. *For q even,*

(i) $\operatorname{rank}_2 A_{\text{sec}} = \operatorname{rank}_2(J+A_{\text{sec}}) = \operatorname{rank}_2 M_S = 3^e$.

(ii) $\operatorname{rank}_2 A_{\text{nonsec}} = \operatorname{rank}_2(J+A_{\text{nonsec}})+1 = \operatorname{rank}_2 M_{F\smallsetminus S}+1 = 3^e+1$.

Proof. As in the proof of Lemma 5.2, we have $\operatorname{rank}_2 M_S = \operatorname{rank}_2(J+A_{\text{sec}})$ and $\operatorname{rank}_2 M_{F\smallsetminus S} = \operatorname{rank}_2(J+A_{\text{nonsec}})$.

The sum of the rows of A_{sec} over F is the row vector $\mathbf{1} = (1,1,\ldots,1)$ of length $\frac{1}{2}q(q+1)$. Also $\mathbf{1}$ is the row of $J+A_{\text{sec}}$ indexed by the nucleus. Since $\mathbf{1}$ lies in the row space of both A_{sec} and $J+A_{\text{sec}}$, these two matrices have the same row space, and hence the same 2-rank.

Now let $\mathbf{1} = (1,1,\ldots,1)$ of length $\frac{1}{2}q(q+1)+1$, the sum of the columns of A_{nonsec}, and let $\mathbf{v}$ be the row vector of length $\frac{1}{2}q(q+1)+1$ having entries '1' and '0' in those positions indexed by tangent lines and passants, respectively. Then $\mathbf{v}(J+A_{\text{nonsec}}) = 0$, whereas $\mathbf{v}\mathbf{1}^\top = 1$. This shows that $\mathit{Row}(J+A_{\text{nonsec}}) = \mathit{Row}(A_{\text{nonsec}}) \cap \mathbf{v}^\perp \subsetneq \mathit{Row}(A_{\text{nonsec}})$. Thus $\operatorname{rank}_2(J+A_{\text{nonsec}}) = \operatorname{rank}_2 A_{\text{nonsec}} - 1$.

Imitating the proof of Lemma 2.7, together with the results of Lemmas 2.4 and 5.3, we have

$$\begin{aligned}
\operatorname{rank}_2 M_S &= q^3 - \dim\Big(\text{left null space of } M_S\Big)\\
&= \dim F^\dagger_{q-1}[\mathbf{X}] - \dim\big\{f(\mathbf{X})\in F^\dagger_{q-1}[\mathbf{X}] \,:\, f(1,\beta,\gamma)=0 \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{whenever } \beta\gamma\in S\,\big\}\\
&= 3^e - 0 \;=\; \operatorname{rank}_2 M,
\end{aligned}$$

and similarly for $M_{F\smallsetminus S}$. □

References

1. E. F. Assmus, Jr. and J. D. Key, *Designs and their Codes*, Cambridge Univ. Press, Cambridge, 1992.
2. B. Bagchi and N. S. N. Sastry, "Even order inversive planes, generalized quadrangles and codes", *Geom. Ded.* **22** (1987), 137–147.
3. A. E. Brouwer and H. A. Wilbrink, "Block Designs", in *Handbook of Incidence Geometry. Foundations and Buildings*, ed. F. Buekenhout, North-Holland, Amsterdam and New York, 1994.
4. P. Dembowski, *Finite Geometries*, Springer, Berlin and New York, 1968.
5. J. M. Goethals and P. Delsarte, "On a class of majority-logic decodable cyclic codes", *IEEE Trans. Inform. Theory* **14** (1968), 182–188.

6. J. W. P. Hirschfeld, *Projective Geometries over Finite Fields,* Oxford Univ. Press, New York, 1979.
7. J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries,* Oxford Univ. Press, Oxford and New York, 1991.
8. W. M. Kantor, “Ovoids and translation planes”, *Canad. J. Math.* **34** (1982), 1195–1207.
9. F. J. MacWilliams and H. B. Mann, “On the p-rank of the design matrix of a difference set”, *Inform. and Control* **12** (1968), 474–489.
10. G. E. Moorhouse, “Bruck nets, codes and characters of loops”, *Des. Codes and Crypt.* **1** (1991), 7–29.
11. E. Shult, “Nonexistence of ovoids in $\Omega^+(10,3)$”, *J. Comb. Theory, Ser. A* **51** (1989), 250–257.
12. K. J. C. Smith, “On the p-rank of the incidence matrix of points and hyperplanes in a finite projective geometry”, *J. Comb. Theory* **1** (1969), 122–129.
13. D. E. Taylor, *The Geometry of the Classical Groups,* Heldermann Verlag, Berlin, 1992.
14. J. A. Thas, “Ovoids and spreads of finite classical polar spaces”, *Geom. Ded.* **10** (1981), 135–144.