Journal of Statistical Planning and Inference **56** (1996), 229–241

Some p-ranks Related to Hermitian Varieties

G. Eric Moorhouse
Dept. of Mathematics, University of Wyoming, Laramie WY, U.S.A.

Abstract. We determine the p-rank of the incidence matrix of hyperplanes of $PG(n, p^e)$ and points of a nondegenerate Hermitian variety. As a corollary, we obtain new bounds for the size of caps and the existence of ovoids in finite unitary spaces. This paper is a companion to [2], in which Blokhuis and this author derive the analogous p-ranks for quadrics.

Keywords: p-rank, Hermitian variety, ovoid

1. Introduction

Let $F \supseteq K$ be finite fields of order q^2 and $q = p^e$ respectively, where p is prime. Choose a nondegenerate Hermitian variety of $PG(n, F)$, denoted by $\mathcal{Z}(U)$, the zero set of a nondegenerate unitary form U, as defined in Section 2. The number of points and of hyperplanes in $PG(n, F)$ is $m = \left[{n+1 \atop 1}\right]_{q^2} = (q^{2(n+1)} - 1)/(q^2 - 1)$. Let $P_1, P_2, \ldots, P_s$ denote the points of $\mathcal{Z}(U)$, where s is given by Lemma 2.1 below, and let $P_{s+1}, \ldots, P_m$ be the remaining points of $PG(n, F)$. Name the hyperplanes as $H_i = P_i^\delta$ for $i = 1, 2, \ldots, m$, where δ is the unitary polarity associated to U; thus H_1, H_2, $\ldots$, H_s are the hyperplanes tangent to the Hermitian variety. Then we have a symmetric 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 $A_1 = \big(A_{11}\ A_{12}\big)$ consists of the first s rows of A; A_{11} consists of the first s columns of A_1, etc. Our main result is the determination of the rank of A_1 in characteristic p, as will be proven in Section 5:

1.1 Theorem. $\operatorname{rank}_p A_1 = \left[\binom{p+n-1}{n}^2 - \binom{p+n-2}{n}^2\right]^e + 1\,.$

For comparison, we state the corresponding result for quadrics as found in [2]: for $n \geq 2$, the incidence matrix of hyperplanes of $PG(n, p^e)$ and points of a nondegenerate quadric, has p-rank equal to $\left[\binom{p+n-1}{n}-\binom{p+n-3}{n}\right]^e+1$. All these results are related to the following, which is well known.

1.2 Theorem. $\operatorname{rank}_p A = \binom{p+n-1}{n}^{2e}+1\,.$

The latter result has numerous independent sources, such as Goethals and Delsarte [4], MacWilliams and Mann [6], and Smith [8]. See also [3] for a treatment closer in spirit to ours, or [1] for more details and related results and discussion.

The following new bounds for caps and ovoids on Hermitian varieties, are improvements of those given in [2]. Recall that a *cap* in $\mathcal{Z}(U)$ is a set of points in $\mathcal{Z}(U)$, no two of which lie on a line of $\mathcal{Z}(U)$. An *ovoid* in $\mathcal{Z}(U)$ is a cap of size $q^{2\lfloor n/2\rfloor+1}+1$ (see [5], [9]).

1.3 Corollary. *Let $\mathcal{Z}(U)$ be a nondegenerate Hermitian variety in $PG(n,q^2)$, $q=p^e$.*

(i) If $\mathcal{S}$ is a cap in $\mathcal{Z}(U)$, then $|\mathcal{S}| \le \left[\binom{p+n-1}{n}^2-\binom{p+n-2}{n}^2\right]^e+1\,.$

(ii) If $n=2m+1$ and $\mathcal{Z}(U)$ contains an ovoid, then $p^n \le \binom{p+n-1}{n}^2-\binom{p+n-2}{n}^2.$

The latter follows directly from Theorem 1.1, since if $\mathcal{S}=\{P_1,\dots,P_k\}$ is a cap in $\mathcal{Z}(U)$, then the upper left $k\times k$ submatrix of A_{11} is an identity matrix, whence $k\le \operatorname{rank}_p A_{11}\le \operatorname{rank}_p A_1$ (cf. [2]).

We remark that ovoids in $\mathcal{Z}(U)$ are trivial for $n=2$; exist for $n=3$ (see [10], [7]); are nonexistent for $n=2m\ge 4$ (see [9]); and are unknown to exist for $n=2m+1\ge 5$. As an application of Corollary 1.3, we see that there do not exist ovoids in $\mathcal{Z}(U)\subset PG(2m+1,p^{2e})$ for $p\in\{2,3\}$ and $2m+1\ge 7$; for $p\in\{5,7\}$ and $2m+1\ge 9$; or for $p\in\{11,13\}$ and $2m+1\ge 11$. The case of $PG(11,13^{2e})$ was not excluded, however, by the weaker bounds given in [2].

Our proof of Theorem 1.1 depends on some rather technical arguments involving polynomials. However, this approach yields, as a bonus, a natural interpretation of the row or column space of A_1 over F, as a module for the unitary group; see Theorem 5.5 below. It remains an open problem to determine $\operatorname{rank}_p A_{11}$, which might *conceivably* yield a slight improvement of Corollary 1.3.

We wish to thank the referee for suggestions which were useful in revising the original manuscript.

2. Preliminaries

We suppose that Hermitian forms are familiar to the reader. However, we define our terms and establish notation for forms in a polynomial setting.

Let $V = F^{n+1} = \{\mathbf{x} = (x_0, x_1, \ldots, x_n) : x_i \in F\}$, considered as a vector space over $F = GF(q^2)$. Let $F[\mathbf{X}] := F[X_0, X_1, \ldots, X_n]$, the ring of polynomials in the $n+1$ indeterminates $\mathbf{X} := (X_0, X_1, \ldots, X_n)$, and let $F_d[\mathbf{X}]$ be the subspace consisting of all homogeneous polynomials of degree d within $F[\mathbf{X}]$, together with the zero polynomial. The zero set of each nonzero $f(\mathbf{X}) \in F_d[\mathbf{X}]$, considered projectively, becomes a *variety of degree d* in $PG(V) = PG(n, F)$, denoted by $\mathcal{Z}(f)$. A *Hermitian form* on V is a polynomial of the form

$$h(\mathbf{X}, \mathbf{Y}) = \sum_{0 \le i,j \le n} a_{ij} X_i Y_j^q \in F_{q+1}[\mathbf{X}, \mathbf{Y}]$$

where $a_{ij} \in F$, $a_{ji}^q = a_{ij}$ for all $i, j \in \{0, 1, \ldots, n\}$. We will suppose that $h(\mathbf{X}, \mathbf{Y})$ is *nondegenerate,* i.e. $\det\big(a_{ij}\big) \neq 0$. The corresponding *Hermitian polarity* δ of $PG(V)$ is determined by

$$\text{(point of } PG(V)) \quad \langle \mathbf{y} \rangle \overset{\delta}{\longleftrightarrow} \mathcal{Z}(\ell_{\mathbf{y}}) \quad \text{(hyperplane of } PG(V))$$

where $\mathbf{0} \neq \mathbf{y} \in V$ and $\ell_{\mathbf{y}}(\mathbf{X}) := h(\mathbf{X}, \mathbf{y}) \in F_1[\mathbf{X}]$. (Observe the use of upper case letters for indeterminates, as in $\mathbf{Y} = (Y_0, \ldots, Y_n)$, and lower case letters for constants, as in $\mathbf{y} = (y_0, \ldots, y_n)$.) The *unitary form* corresponding to $h(\mathbf{X}, \mathbf{Y})$ is

$$U(\mathbf{X}) := h(\mathbf{X}, \mathbf{X}) \in F_{q+1}[\mathbf{X}]\,.$$

It is well known that any member of the triple $\big(h(\mathbf{X}, \mathbf{Y}),\, \delta,\, U(\mathbf{X})\big)$ determines the other two (although h and U are determined only to within nonzero K-multiples). A point $\langle \mathbf{x} \rangle$ (respectively, hyperplane H) is *absolute* with respect to δ, if $\langle \mathbf{x} \rangle \in \langle \mathbf{x} \rangle^\delta$ (resp., $H^\delta \in H$). If $n \ge 2$ and $U(\mathbf{X})$ is nondegenerate (i.e. $h(\mathbf{X}, \mathbf{Y})$ is nondegenerate), then the polynomial $U(\mathbf{X})$ is absolutely irreducible.

The *standard* Hermitian form is given by $\sum X_i Y_i^q$. It is well known that any nondegenerate Hermitian form is equivalent to the standard form, under a linear change of coördinates. A *nondegenerate Hermitian variety* in $PG(V)$ is a variety of the form $\mathcal{Z}(U)$, where $U(\mathbf{X})$ is a nondegenerate unitary form. This is exactly the set of absolute points with respect to the corresponding Hermitian polarity δ. A hyperplane H is said to be *tangent* to the variety $\mathcal{Z}(U)$ if H is absolute with respect to δ. The following may be found in Theorem 23.2.4 of [5].

2.1 Lemma. *$PG(n,F)$ contains $s = (q^{n+1}+(-1)^n)(q^n-(-1)^n)/(q^2-1)$ absolute points (or hyperplanes), and $m-s = q^n(q^{n+1}+(-1)^n)/(q+1)$ nonabsolute points (or hyperplanes).*

A projective subspace W of $PG(V)$ is said to be *nondegenerate* if $\mathcal{Z}(U)\cap W$ is a nondegenerate Hermitian variety in W. For example, the nondegenerate hyperplanes of $PG(V)$ are precisely the nonabsolute hyperplanes of $PG(V)$ with respect to δ.

3. Hermitian Curves

Consider the case $n=2$, so that $\mathcal{Z}(U)$ is a Hermitian curve in $PG(2,F)$. Recall that there are many homogeneous polynomials in $\mathbf{X}=(X,Y,Z):=(X_0,X_1,X_2)$ of degree $\geq q^2+1$ which vanish on $PG(2,F)$. We will determine all homogeneous polynomials of degree $\leq q^2$ which vanish on $\mathcal{Z}(U)$. First, observe that these are not necessarily multiples of $U(\mathbf{X})$. For, given a nonabsolute line $\mathcal{Z}(\ell)$ of $PG(2,F)$, where $0\neq \ell(\mathbf{X})\in F_1[\mathbf{X}]$, define

$$f_\ell(\mathbf{X}) := \ell(\mathbf{X})\prod_{i=1}^{q^2-q} h(\mathbf{X},\mathbf{a}_i)$$

where $\{\langle\mathbf{a}_i\rangle : 1\leq i\leq q^2-q\}$ is the set of all nonabsolute points of $\mathcal{Z}(\ell)$, and $h(\mathbf{X},\mathbf{Y})$ is the Hermitian form corresponding to $U(\mathbf{X})$. Note that $\deg f_\ell(\mathbf{X}) = q^2-q+1$, and that the nonabsolute line $\mathcal{Z}(\ell)$ determines $f_\ell(\mathbf{X})$ only to within a nonzero scalar multiple. Now let $\langle\mathbf{v}\rangle$ be a point of $\mathcal{Z}(U)$. If $\langle\mathbf{v}\rangle$ lies on $\mathcal{Z}(\ell)$, then $\ell(\mathbf{v})=0$. Otherwise $\langle\mathbf{v}\rangle$ is an absolute point not on $\mathcal{Z}(\ell)$, in which case the absolute line $\langle\mathbf{v}\rangle^\delta$ meets $\mathcal{Z}(\ell)$ in a nonabsolute point $\langle\mathbf{a}_i\rangle$, and $h(\mathbf{v},\mathbf{a}_i)=0$. In any case, $f_\ell(\mathbf{v})=0$; that is, $f_\ell(\mathbf{X})$ vanishes on $\mathcal{Z}(U)$.

To see that $f_\ell(\mathbf{X})$ is not divisible by $U(\mathbf{X})$, we may suppose that $U(\mathbf{X}) = X^{q+1}+Y^{q+1}+Z^{q+1}$, the standard unitary form, and that $\ell(\mathbf{X})=X$. Then $\mathcal{Z}(\ell)=\{(0,0,1)\}\cup\{(0,1,\alpha) : \alpha\in F\}$, and the absolute points of $\mathcal{Z}(\ell)$ are $\{(0,1,\alpha) : \alpha\in F,\ \alpha^{q+1}=-1\}$. Thus

$$\begin{aligned} f_\ell(\mathbf{X}) &= \lambda XZ\prod_{\alpha\in F} h\big(\mathbf{X},(0,1,\alpha)\big)\Big/\prod_{\alpha^{q+1}=-1} h\big(\mathbf{X},(0,1,\alpha)\big)\\ &= \lambda XZ\prod_{\alpha\in F}(Y+\alpha^q Z)\Big/\prod_{\alpha^{q+1}=-1}(Y+\alpha^q Z)\\ &= \lambda X(Y^{q^2}Z - YZ^{q^2})\,/\,(Y^{q+1}+Z^{q+1}) \end{aligned}$$

for some $\lambda\in F\smallsetminus\{0\}$. By comparing degrees with respect to X, we see that $f_\ell(\mathbf{X})$ is not divisible by $U(\mathbf{X})$.

Now $U(\mathbf{X})$ and $f_\ell(\mathbf{X})$ generate a nonprincipal ideal $(f_\ell(\mathbf{X}), U(\mathbf{X})) \subset F[\mathbf{X}]$, any member of which vanishes on $\mathcal{Z}(U)$.

3.1 Lemma. *The ideal $(f_\ell(\mathbf{X}), U(\mathbf{X}))$ is independent of the choice of nonabsolute line $\mathcal{Z}(\ell)$.*

Proof. Clearly the verity of the lemma is not affected by the choice of nondegenerate unitary form $U(\mathbf{X})$, although the ideal $\mathcal{I} = (f_\ell(\mathbf{X}), U(\mathbf{X}))$ itself certainly depends on the choice of $U(\mathbf{X})$. For convenience we choose the somewhat less standard form $U(\mathbf{X}) = X^qY + XY^q + Z^{q+1}$. Let $\mathcal{Z}(\ell)$ and $\mathcal{Z}(\ell^*)$ be two nonabsolute lines of $PG(2,F)$. We first assume that the intersection point $\mathcal{Z}(\ell) \cap \mathcal{Z}(\ell^*)$ is absolute. Since the isometry group of $U(\mathbf{X})$ acts transitively on the set of ordered pairs of nonabsolute lines whose intersection is an absolute point, we may assume that $\ell(\mathbf{X}) = Z,\ \ell^*(\mathbf{X}) = Y - Z,\ \mathcal{Z}(\ell) = \{\langle(1,0,0)\rangle\} \cup \{\langle(\alpha,1,0)\rangle : \alpha \in F,\ \alpha^q + \alpha = 0\},\ \mathcal{Z}(\ell^*) = \{\langle(1,0,0)\rangle\} \cup \{\langle(\alpha,1,1)\rangle : \alpha \in F,\ \alpha^q + \alpha + 1 = 0\}$. As above, we obtain (to within a nonzero scalar multiple)

$$f_\ell(\mathbf{X}) = Z \prod_{\alpha^q+\alpha\neq 0} (X + \alpha Y) = Z(X^{q^2-1} - Y^{q^2-1})/(X^{q-1} + Y^{q-1})$$

and

$$\begin{aligned} f_{\ell^*}(\mathbf{X}) &= (Y - Z) \prod_{\alpha^q+\alpha+1\neq 0} (X + \alpha Y + Z) \\ &= (Y - Z)[X^{q^2} + Z^{q^2} - (X + Z)Y^{q^2-1}] \,/\, [X^q + Z^q + (X + Z)Y^{q-1} - Y^q]. \end{aligned}$$

Some algebraic manipulation shows that

$$f_\ell(\mathbf{X}) + f_{\ell^*}(\mathbf{X}) = \frac{\begin{array}{r}(X^{q^2-1} - Y^{q^2-1})(X^qY + XY^q + Z^{q+1}) \\ + Z(Y - Z)(X^{q-1} + Y^{q-1})[Z^{q^2-1} - (X^qY + XY^q)^{q-1}]\end{array}}{(X^{q-1} + Y^{q-1})[X^q + Z^q + (X + Z)Y^{q-1} - Y^q]} .$$

Let us denote the numerator and denominator of the latter expression by $Numer(\mathbf{X})$ and $Denom(\mathbf{X})$. Of course, $Denom(\mathbf{X})$ divides $Numer(\mathbf{X})$ since $f_\ell(\mathbf{X})$ and $f_{\ell^*}(\mathbf{X})$ are polynomials. Also, $U(\mathbf{X})$ divides $Numer(\mathbf{X})$, since

$$\begin{aligned} \frac{Numer(\mathbf{X})}{U(\mathbf{X})} &= X^{q^2-1} - Y^{q^2-1} + Z(Y - Z)(X^{q-1} + Y^{q-1}) \frac{Z^{q^2-1} - (X^qY + XY^q)^{q-1}}{Z^{q+1} + X^qY + XY^q} \\ &= X^{q^2-1} - Y^{q^2-1} + Z(Y - Z)(X^{q-1} + Y^{q-1}) \sum_{i=0}^{q-2} Z^{(q+1)(q-2-i)}(-X^qY - XY^q)^i \\ &\in F_{q^2-1}[\mathbf{X}] . \end{aligned}$$

Since $Denom(\mathbf{X})$ is a product of factors of degree $\leq q$, it is coprime to the irreducible polynomial $U(\mathbf{X})$. It follows that $U(\mathbf{X})$ divides $Numer(\mathbf{X})/Denom(\mathbf{X}) = f_\ell(\mathbf{X}) + f_{\ell^*}(\mathbf{X})$. Therefore $(f_\ell(\mathbf{X}), U(\mathbf{X})) = (f_{\ell^*}(\mathbf{X}), U(\mathbf{X}))$.

Now suppose that $\mathcal{Z}(\ell)$ and $\mathcal{Z}(\ell^{**})$ are two nonabsolute lines of $PG(2, F)$ which intersect in a nonabsolute point. Let $\langle \mathbf{v} \rangle$ and $\langle \mathbf{v}^{**} \rangle$ be absolute points on $\mathcal{Z}(\ell)$ and $\mathcal{Z}(\ell^{**})$ respectively. Then $\langle \mathbf{v}, \mathbf{v}^{**} \rangle$ is a nonabsolute line, which we may call $\mathcal{Z}(\ell^*)$. The previous argument shows that $(f_\ell(\mathbf{X}), U(\mathbf{X})) = (f_{\ell^*}(\mathbf{X}), U(\mathbf{X})) = (f_{\ell^{**}}(\mathbf{X}), U(\mathbf{X}))$. Therefore the ideal $(f_\ell(\mathbf{X}), U(\mathbf{X}))$ is independent of the choice of nonabsolute line $\mathcal{Z}(\ell)$. $\square$

We denote $\mathcal{I} = \mathcal{I}(U) := (f_\ell(\mathbf{X}), U(\mathbf{X}))$. We will show (Lemma 3.3) that *any* homogeneous polynomial of degree $\leq q^2$ which vanishes on $\mathcal{Z}(U)$, lies in $\mathcal{I}$. But first, we prove the following, valid for arbitrary $n \geq 2$. (We follow the convention that $0^0 = 1$, and $F_d[\mathbf{X}] = 0$ whenever $d < 0$. Also, we abbreviate $\mathbf{X}' = (X_1, X_2, \ldots, X_n)$.)

3.2 Lemma. *Let $U(\mathbf{X}) = \sum_{i=0}^n X_i^{q+1}$ where $n \geq 2$. Suppose that $f(\mathbf{X}) \in F_d[\mathbf{X}]$ vanishes on $\mathcal{Z}(U)$. Use the division algorithm to write $f(\mathbf{X}) = g(\mathbf{X})U(\mathbf{X}) + \sum_{i=0}^q f_i(\mathbf{X}')X_0^i$ for uniquely determined polynomials $g(\mathbf{X}) \in F_{d-q-1}[\mathbf{X}]$ and $f_i(\mathbf{X}') \in F_{d-i}[\mathbf{X}'] = F_{d-i}[X_1, X_2, \ldots, X_n]$. Then $f_i(\mathbf{x}')x_0^i = 0$ for every absolute point $\langle \mathbf{x} \rangle = \langle (x_0, \mathbf{x}') \rangle = \langle (x_0, x_1, \ldots, x_n) \rangle$.*

(Note: The conclusion says that $f_i(\mathbf{x}') = 0$ for $i = 0, 1, \ldots, q$ if $x_0 \neq 0$; or $f_0(\mathbf{x}') = 0$ if $x_0 = 0$.)

Proof. Let $\omega \in F$ be a primitive $(q+1)$-st root of unity. Suppose that a given point $\langle \mathbf{x} \rangle$ is absolute, i.e. $U(\mathbf{x}) = \sum_{i=0}^n x_i^{q+1} = 0$. Clearly, all the points $\langle (\omega^j x_0, \mathbf{x}') \rangle$ are absolute, for $j = 0, 1, \ldots, q$. By hypothesis, we have

$$0 = f(\omega^j x_0, \mathbf{x}') = \sum_{i=0}^q \omega^{ij} f_i(\mathbf{x}') x_0^i$$

for $j = 0, 1, \ldots, q$. We may regard this as a system of $q+1$ linear equations in the unknowns $f_i(\mathbf{x}')x_0^i$, having a Vandermonde coefficient matrix whose determinant is $\prod_{0 \leq i < j \leq q}(\omega^j - \omega^i) \neq 0$. This implies that $f_i(\mathbf{x}')x_0^i = 0$ for $i = 0, 1, \ldots, q$. $\square$

3.3 Lemma. *Let $f(\mathbf{X}) \in F_d[\mathbf{X}]$ where $d \le q^2$. Then $f(\mathbf{X})$ vanishes on $\mathcal{Z}(U)$ if and only if $f(\mathbf{X}) \in \mathcal{I}(U)$.*

Proof. We have seen that every polynomial in $\mathcal{I}$ vanishes on $\mathcal{Z}(U)$. Conversely, suppose that $f(\mathbf{X})$ vanishes on $\mathcal{Z}(U)$. We may assume that $U(\mathbf{X}) = X^{q+1} + Y^{q+1} + Z^{q+1}$. The line $\mathcal{Z}(X)$ is nonabsolute, and so $\mathcal{I} = (f_X(\mathbf{X}), U(\mathbf{X}))$ where $f_X(\mathbf{X}) = f_X(X,Y,Z) = X(Y^{q^2}Z - YZ^{q^2})/(Y^{q+1} + Z^{q+1}) = XY\prod_{\alpha^{q+1} \ne -1}(\alpha Y + Z)$. As in Lemma 3.2, we may write $f(\mathbf{X}) = g(\mathbf{X})U(\mathbf{X}) + \sum_{i=0}^{q} f_i(Y,Z)X^i$ for certain polynomials $g(\mathbf{X}) \in F_{d-q-1}[\mathbf{X}]$, $f_i(Y,Z) \in F_{d-i}[Y,Z]$. It suffices now to show that $f_X(X,Y,Z)$ divides each of the terms $f_i(Y,Z)X^i$.

It is clear that X divides $f_i(Y,Z)X^i$ for $i = 1, 2, \ldots, q$. We must show that $f_0(Y,Z) = 0 \in F_d[Y,Z]$. For any $y, z \in F$, there exists $x \in F$ such that $x^{q+1} + y^{q+1} + z^{q+1} = 0$. By Lemma 3.2, $f_0(y,z) = 0$. Therefore $Y^{q^2}Z - YZ^{q^2}$ divides $f_0(Y,Z)$. However, $\deg f_0(Y,Z) = d \le q^2$, so $f_0(Y,Z) = 0$ as claimed.

The remaining linear factors of $f_X(X,Y,Z)$ are of the form $\alpha Y + \beta Z$ where $\alpha^{q+1} + \beta^{q+1} \ne 0$. Given such α and β, there exists $x \ne 0$ such that $x^{q+1} + \alpha^{q+1} + \beta^{q+1} = 0$. Thus $\langle(x, \beta, -\alpha)\rangle$ is an absolute point. By Lemma 3.2, $f_i(\beta, -\alpha)x^i = 0$, and so $\alpha Y + \beta Z$ divides $f_i(Y,Z)$.

Thus $f_X(X,Y,Z)$ divides $f_i(Y,Z)X^i$ for $i = 0, 1, \ldots, q$, and so $f(\mathbf{X}) \in \mathcal{I}$. $\square$

The following will be used in Section 4.

3.4 Lemma. *Let $U(\mathbf{X}) = X^{q+1} + Y^{q+1} + Z^{q+1}$, and $f(\mathbf{X}) = f(X,Y,Z) \in F_d[\mathbf{X}]$ where $d \le q^2$. Suppose that $f(\mathbf{X})$ vanishes at every* nonabsolute *point of $PG(2,F)$, and at every point of the nonabsolute line $\mathcal{Z}(X)$. Then*

$$f(\mathbf{X}) = \lambda X \prod_{\substack{\alpha \in GF(q) \\ \alpha \ne 1}} (\alpha X^{q+1} + Y^{q+1} + Z^{q+1})$$

for some $\lambda \in F$.

Proof. Since $f(\mathbf{X})$ vanishes at all $q^2 + 1$ points of $\mathcal{Z}(X)$, and $\deg f(\mathbf{X}) \le q^2$, we have $f(\mathbf{X}) = Xg(\mathbf{X})$ for some $g(\mathbf{X}) \in F_{d-1}[\mathbf{X}]$.

Consider an absolute line of the form $\mathcal{Z}(Y + cZ)$, where $c^{q+1} = -1$. This line has q^2 nonabsolute points $\langle(1, \lambda c, -\lambda)\rangle$, $\lambda \in F$, and $g(\mathbf{X})$ vanishes at each of these q^2 points. Since

$\deg g(\mathbf{X}) \le q^2-1$, we have $(Y+cZ) \mid g(\mathbf{X})$. Thus $f(\mathbf{X}) = Xr(\mathbf{X})\prod_{c^{q+1}=-1}(Y+cZ) = X(Y^{q+1}+Z^{q+1})r(\mathbf{X})$ for some $r(\mathbf{X}) \in F_{d-q-2}[\mathbf{X}]$.

For all $\alpha \in GF(q)\smallsetminus\{0,1\}$, the polynomial $Xr(\mathbf{X})$ of degree $\le q^2-q-1$ vanishes at every point of the nondegenerate Hermitian curve $\mathcal{Z}(\alpha X^{q+1}+Y^{q+1}+Z^{q+1})$. By Lemma 3.3, we have $(\alpha X^{q+1}+Y^{q+1}+Z^{q+1}) \mid Xr(\mathbf{X})$, and so $(\alpha X^{q+1}+Y^{q+1}+Z^{q+1}) \mid r(\mathbf{X})$. The result now follows. $\square$

4. A Nullstellensatz

Our goal in this section is to prove the following extension of Lemma 3.3.

4.1 Theorem. *Suppose that $f(\mathbf{X}) \in F_d[\mathbf{X}]$ vanishes at every point of a nondegenerate Hermitian variety $\mathcal{Z}(U)$ of $PG(n,q^2)$.*

(i) If $n=1$, then U divides f.

(ii) If $n=2$ and $d \le q^2$, then $f \in \mathcal{I}(U)$.

(iii) If $n \ge 3$ and $d \le q^2$, then U divides f.

Proof. Suppose first that $n=1$, and that $U(X_0,X_1) = X_0^qX_1 - X_0X_1^q$. Then $\mathcal{Z}(U) = \{\langle(1,0)\rangle\} \cup \{\langle(\alpha,1)\rangle : \alpha \in K\} = PG(1,K)$, embedded as a Baer subline of $PG(1,F)$. If $f(\alpha,\beta)=0$, where $(\alpha,\beta) \ne (0,0)$, then $f(\mathbf{X})$ is divisible by $\beta X_0 - \alpha X_1$. Thus if $f(\mathbf{X})$ vanishes on $\mathcal{Z}(U)$, then $f(\mathbf{X})$ is divisible by $X_0\prod_{\alpha\in K}(\alpha X_0 - X_1) = U(\mathbf{X})$, as required.

For $n=2$, conclusion (ii) follows from Lemma 3.3. We proceed to prove conclusion (iii) by induction on n. In the remainder of the proof, we will always assume the standard Hermitian form $U(\mathbf{X}) = \sum_{i=0}^n X_i^{q+1}$. Also, we may assume without loss of generality that $d=q^2$; otherwise replace $f(\mathbf{X}) \in F_d[\mathbf{X}]$ by $X_0^{q^2-d}f(\mathbf{X}) \in F_{q^2}[\mathbf{X}]$.

Suppose first that $n=3$. We may assume without loss of generality (see Lemma 3.2) that $f(\mathbf{X}) = \sum_{i=0}^q f_i(\mathbf{X}')X_0^i$ where $f_i(\mathbf{X}') \in F_{q^2-i}[\mathbf{X}'] = F_{q^2-i}[X_1,X_2,X_3]$, and we must show that each $f_i(\mathbf{X}')=0$. We first show that $f_0(\mathbf{X}') = 0 \in F_{q^2}[\mathbf{X}']$. Given any $x_1,x_2,x_3 \in F$, there exists $x_0 \in F$ such that $\sum_{i=0}^3 x_i^{q+1} = 0$. By Lemma 3.2, we have $f_0(x_1,x_2,x_3)=0$. Since $f_0(\mathbf{X}') \in F_{q^2}[\mathbf{X}']$ vanishes everywhere, we have $f_0 = 0$ as claimed.

Now suppose that $1 \le i \le q$, and we show that $f_i(\mathbf{X}')=0$. We use $\mathbf{X}' = (X_1,X_2,X_3)$ as coördinates for the nondegenerate hyperplane $H = \mathcal{Z}(X_0)$, with the standard unitary form $U_H(\mathbf{X}') = \sum_{i=1}^{3} X_i^{q+1}$. Let $\langle(0, x_1, x_2, x_3)\rangle$ be any nonabsolute point of H. If $x_1 \neq 0$, then there exists $\alpha \in F \smallsetminus \{0\}$ such that $\langle(\alpha x_1, x_1, x_2, x_3)\rangle$ is an absolute point of $PG(3, F)$; by Lemma 3.2, we have $f_i(x_1, x_2, x_3)(\alpha x_1)^i = 0$. Since $\alpha \neq 0$, we have $f_i(x_1, x_2, x_3)x_1^i = 0$. Clearly, $f_i(\mathbf{X}')X_1^i$ also vanishes at every point of the nonabsolute line $\mathcal{Z}_H(X_1)$ of H. By Lemma 3.4, we have $f_i(\mathbf{X}')X_1^i = \lambda X_1 \prod_{1 \neq \beta \in GF(q)} (\beta X_1^{q+1} + X_2^{q+1} + X_2^{q+1})$. Thus $f_2 = f_3 = \ldots = f_q = 0$ and $f_1(\mathbf{X}') = \lambda \prod_\beta (\beta X_1^{q+1} + X_2^{q+1} + X_2^{q+1})$ for some $\lambda \in F$. However, a similar argument shows that $f_1(\mathbf{X}') = \mu X_2 \prod_\beta (X_1^{q+1} + \beta X_2^{q+1} + X_3^{q+1})$. Thus $f_1 = 0$. This completes the proof in the case $n = 3$.

Now suppose that $n \geq 4$. Let $\varepsilon \in F$ such that $\varepsilon^{q+1} = -1$. For each $c \in F$, consider the hyperplane $H_c = \mathcal{Z}(X_0 - \varepsilon X_1 - c X_2)$. The restriction of $U(\mathbf{X})$ to H_c is given by $U_c(\mathbf{X}') = c^q \varepsilon X_1^q X_2 + c \varepsilon^q X_1 X_2^q + (1 + c^{q+1}) X_2^{q+1} + \sum_{i=3}^{n} X_i^{q+1}$. We see that $U_c(\mathbf{X}')$ (and so also H_c) is nondegenerate whenever $c \neq 0$. Furthermore, if $c \neq d$ are nonzero elements of F, then clearly the polynomials $U_c(\mathbf{X}')$ and $U_d(\mathbf{X}')$ have no common factor. As before, we may suppose that $f(\mathbf{X}) = \sum_{i=0}^{q} f_i(\mathbf{X}') X_0^i$ where $f_i(\mathbf{X}') \in F_{q^2 - i}[\mathbf{X}'] = F_{q^2-i}[X_1, \ldots, X_n]$. Suppose that $U_c(\mathbf{x}') = U_c(x_1, \ldots, x_n) = 0$. Then $U(\varepsilon x_1 + c x_2, \mathbf{x}') = 0$, so by Lemma 3.2, we have $f_i(\mathbf{x}')(\varepsilon x_1 + c x_2)^i = 0$. By induction, $U_c(\mathbf{X}')$ divides $f_i(\mathbf{X}')(\varepsilon X_1 + c X_2)^i \in F_{q^2}[\mathbf{X}']$. Since $U_c(\mathbf{X}')$ has no linear factors, this implies that $U_c(\mathbf{X}') \mid f_i(\mathbf{X}')$. Thus $\prod_{0 \neq c \in F} U_c(\mathbf{X}')$ divides $f_i(\mathbf{X}')$. Comparing degrees gives $f_i(\mathbf{X}') = 0$. $\square$

5. Determining the p-ranks

Define $F_d^\dagger[\mathbf{X}]$ to be the subspace of $F_d[\mathbf{X}]$ spanned by all monomials of the form $\mathbf{X}^{\mathbf{i}} := X_0^{i_0} X_1^{i_1} \cdots X_n^{i_n}$ such that $i_0 + \cdots + i_n = d$ and p does not divide the multinomial coefficient $\binom{d}{\mathbf{i}} := \binom{d}{i_0,\, i_1,\, \cdots,\, i_n} = \frac{d!}{i_0! i_1! \cdots i_n!}$. We state a few properties of $F_{q^2-1}^\dagger[\mathbf{X}]$ without proof; for proofs and details, see [2]. The group $G = GL(n+1, F)$ acts naturally on $F_1[\mathbf{X}]$ with respect to the basis $\mathbf{X} = (X_0, X_1, \ldots, X_n)$. This action extends uniquely to an action on the algebra $F[\mathbf{X}]$, for which each homogeneous part $F_d[\mathbf{X}]$ is an FG-submodule. The space $F_d^\dagger[\mathbf{X}]$ is invariant under linear changes of coördinates; that is, $F_d^\dagger[\mathbf{X}]$ is an FG-submodule of $F_d[\mathbf{X}]$.

Let $\mathcal{V}_{p-1} := F_{p-1}[\mathbf{X}]$, considered as an FG-module in the usual way, i.e. $T \in G$ acts on $f(\mathbf{X}) \in \mathcal{V}_{p-1}$ via $f(\mathbf{X}) \mapsto f(T\mathbf{X}) := f(TX_0, \ldots, TX_n)$. Let $\sigma : F \to F$ be the Frobenius automorphism $x \mapsto x^p$, and 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 $k = 0, 1, \ldots, 2e-1$, a new FG-module $\mathcal{V}_{p-1}^{(k)}$ is obtained by twisting $\mathcal{V}_{p-1}$ by the automorphism σ^k. That is, $\mathcal{V}_{p-1}^{(k)}$ has the same elements as $\mathcal{V}_{p-1}$, but the action of $T \in G$ on $\mathcal{V}_{p-1}^{(k)}$ is given by

$$f(\mathbf{X}) \mapsto f(T^{\sigma^{-k}}\mathbf{X}) := f(T^{\sigma^{-k}}X_0, \ldots, T^{\sigma^{-k}}X_n), \qquad f(\mathbf{X}) \in \mathcal{V}_{p-1}^{(k)}.$$

Then we have an isomorphism of FG-modules

$$\bigotimes_{k=0}^{e-1} (\mathcal{V}_{p-1}^{(k)} \otimes \mathcal{V}_{p-1}^{(e+k)}) \to F_{q^2-1}^{\dagger}[\mathbf{X}]$$

determined by

$$\begin{aligned}\big(f_0(\mathbf{X}) \otimes f_e(\mathbf{X})\big) \otimes \big(f_1(\mathbf{X}) \otimes f_{e+1}(\mathbf{X})\big) \otimes \cdots \otimes \big(f_{e-1}(\mathbf{X}) \otimes f_{2e-1}(\mathbf{X})\big)& \\ \mapsto \prod_{k=0}^{e-1} f_k(\mathbf{X}^{p^k}) f_{e+k}(\mathbf{X}^{p^{e+k}}) = \prod_{k=0}^{e-1} \big(f_k^{\sigma^{-k}}(\mathbf{X})\big)^{p^k} \big(f_{e+k}^{\sigma^{-e-k}}(\mathbf{X})\big)^{p^{e+k}}&\end{aligned}$$

where $\mathbf{X}^{p^k} := (X_0^{p^k}, \ldots, X_n^{p^k})$. (The advantage of pairing $\mathcal{V}_{p-1}^{(k)}$ with $\mathcal{V}_{p-1}^{(e+k)}$ will become apparent later.) In particular, $\dim F_{q^2-1}^{\dagger}[\mathbf{X}] = \binom{p+n-1}{n}^{2e}$. The following is an analogue of Lemma 2.7 of [2], and so we provide here only the outline of a proof.

5.1 Lemma. $\operatorname{rank}_p A_1 = 1 + \binom{p+n-1}{n}^{2e} - \dim\{f(\mathbf{X}) \in F_{q^2-1}^{\dagger}[\mathbf{X}] : f$ vanishes *at every point* of $\mathcal{Z}(U)\}$.

Sketch of Proof. Let $M_1 = \big(\mathbf{x}\mathbf{y}^{\top}\big)^{q^2-1}$ be the $((q^2-1)s+1) \times q^{2(n+1)}$ matrix having rows indexed by the row vectors $\mathbf{x} \in F^{n+1}$ such that $U(\mathbf{x}) = 0$, and columns indexed by all the row vectors $\mathbf{y} \in F^{n+1}$. Then $\operatorname{rank}_p M_1 = \operatorname{rank}_p(J - A_1)$, since $J - A_1$ is obtained from M_1 by deleting duplicate rows and columns, and deleting the all-zero row and column.

The number of absolute points on a given hyperplane H is $(q^n + (-1)^{n-1})(q^{n-1} - (-1)^{n-1})/(q^2-1) \equiv 1 \mod p$ if H is nonabsolute, or $1 + q(q^{n-1} + (-1)^{n-2})(q^{n-2} - (-1)^{n-2})/(q^2-1) \equiv 1 \mod p$ if H is absolute. So the sum (modulo p) of the rows of A_1 is $\mathbf{1} = (1, 1, \ldots, 1)$. Furthermore, every point lies on $m \equiv 1 \mod p$ hyperplanes, so the row space of $J - A_1$ lies in $\mathbf{1}^{\perp}$. It follows that $Row(A_1) = \langle \mathbf{1} \rangle \oplus Row(J - A_1)$, and so $\operatorname{rank}_p A_1 = 1 + \operatorname{rank}_p(J - A_1) = 1 + \operatorname{rank}_p M_1$.

Now we have $\operatorname{rank}_p M_1 = q^{2(n+1)} - \dim \mathcal{N}$, where $\mathcal{N}$ is the right null space of M_1. Let $\mathbf{a} = \big(a_{\mathbf{y}} : \mathbf{y} \in F^{n+1}\big)$. Then $M_1 \mathbf{a}^\top = \mathbf{b}^\top = \big(b_{\mathbf{x}} : \mathbf{x} \in F^{n+1},\ U(\mathbf{x}) = 0\big)^\top$ where

$$\begin{aligned}
b_{\mathbf{x}} &= \sum_{\mathbf{y}\in F^{n+1}} a_{\mathbf{y}} (\mathbf{x}\mathbf{y}^\top)^{q^2-1} \\
&= \sum_{\mathbf{y}\in F^{n+1}} a_{\mathbf{y}} \sum_{\Sigma \mathbf{i} = q^2-1} \binom{q^2-1}{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \mathbf{y}^{\mathbf{i}} \\
&= \sum_{\Sigma \mathbf{i} = q^2-1} \binom{q^2-1}{\mathbf{i}} \Bigg[\sum_{\mathbf{y}\in F^{n+1}} a_{\mathbf{y}} \mathbf{y}^{\mathbf{i}} \Bigg] \mathbf{x}^{\mathbf{i}}.
\end{aligned}$$

Thus $\mathbf{a}^\top \in \mathcal{N}$ if and only if the polynomial $f_{\mathbf{a}}(\mathbf{X}) := \sum_{\Sigma \mathbf{i} = q^2-1} \binom{q^2-1}{\mathbf{i}} \big[\sum_{\mathbf{y}\in F^{n+1}} a_{\mathbf{y}} \mathbf{y}^{\mathbf{i}}\big] \mathbf{X}^{\mathbf{i}} \in F^{\dagger}_{q^2-1}[\mathbf{X}]$ vanishes at every point of $\mathcal{Z}(U)$. It follows from Lemma 2.3 of [2] that $\dim \mathcal{N} = \dim F^{\dagger}_{q^2-1}[\mathbf{X}] - \dim \{f(\mathbf{X}) \in F^{\dagger}_{q^2-1}[\mathbf{X}] \ :\ f \text{ vanishes at every point of } \mathcal{Z}(U)\}$. Since $\dim F^{\dagger}_{q^2-1}[\mathbf{X}] = \binom{p+n-1}{n}^{2e}$, the result follows. $\square$

For convenience, we henceforth assume the following.

5.2 Assumption. *$U(\mathbf{X})$ is a nondegenerate unitary form, of the form $X_0^{q+1} + \sum_{i=1}^n \sum_{j=1}^n a_{ij} X_i X_j^q$ where $a_{ji}^q = a_{ij}$ and $\det\big(a_{ij} \ :\ 1 \le i,j \le n\big) \ne 0$.*

We produce a convenient basis of $F^{\dagger}_{q^2-1}[\mathbf{X}]$, by first producing a basis for each of the factors $\mathcal{V}^{(k)}_{p-1} \otimes \mathcal{V}^{(e+k)}_{p-1}$, $k = 0, 1, \ldots, e-1$. We abbreviate the degree of a monomial $\mathbf{X}^{\mathbf{i}} = X_0^{i_0} \cdots X_n^{i_n}$ by $\sum \mathbf{i} := i_0 + \cdots + i_n$; of course, $i_0, \ldots, i_n$ are non-negative integers. If $\mathbf{X}^{\mathbf{j}} = X_0^{j_0} \cdots X_n^{j_n}$ is another such monomial, we abbreviate $\mathbf{X}^{\mathbf{i}+p^e\mathbf{j}} = \mathbf{X}^{\mathbf{i}+q\mathbf{j}} = X_0^{i_0+qj_0} \cdots X_n^{i_n+qj_n}$. Let $\{g_1(\mathbf{X}), \ldots, g_{b'}(\mathbf{X})\}$ be the set of polynomials of the form $U(\mathbf{X})\mathbf{X}^{\mathbf{i}+q\mathbf{j}}$ such that $\sum \mathbf{i} = \sum \mathbf{j} = p-2$; here $b' = \binom{p+n-2}{n}^2$. Also let $\{g_{b'+1}(\mathbf{X}), \ldots, g_b(\mathbf{X})\}$ be the set of monomials of the form $\mathbf{X}^{\mathbf{i}+q\mathbf{j}}$ such that $\sum \mathbf{i} = \sum \mathbf{j} = p-1$ and $i_0 j_0 = 0$; here $b = \binom{p+n-1}{n}^2$. Define $\mathcal{B} := \big\{\prod_{k=0}^{e-1} g_{r_k}(\mathbf{X})^{p^k} \ :\ 1 \le r_0, r_1, \ldots, r_{e-1} \le b\big\}$. Observe that $g_{r_k}(\mathbf{X})^{p^k} = g_{r_k}^{\sigma^k}(\mathbf{X}^{p^k})$. It follows directly from earlier discussion that $\mathcal{B}$ is a basis for $F^{\dagger}_{q^2-1}[\mathbf{X}]$. We also define $\mathcal{B}' := \big\{\prod_{k=0}^{e-1} g_{r_k}(\mathbf{X})^{p^k} \in \mathcal{B} \ :\ \text{at least one } r_k \le b'\big\}$. Let $\mathcal{E}_{U,\mathbf{X}}$ be the span of $\mathcal{B}'$. The following is immediate.

5.3 Lemma. *$\mathcal{E}_{U,\mathbf{X}}$ is a subspace of $F^{\dagger}_{q^2-1}[\mathbf{X}]$ of dimension $b^e - (b-b')^e = \binom{p+n-1}{n}^{2e} - \big[\binom{p+n-1}{n}^2 - \binom{p+n-2}{n}^2\big]^e$. Moreover, every member of $\mathcal{E}_{U,\mathbf{X}}$ is divisible by $U(\mathbf{X})$.*

Each $\prod_{k=0}^{e-1} g_{r_k}(\mathbf{X})^{p^k} \in \mathcal{B}$, 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 $\theta : \mathcal{B} \to \{\mathbf{X}^{\mathbf{i}} : \Sigma\mathbf{i} = q^2-1$ and $p \nmid \binom{q^2-1}{\mathbf{i}}\}$ from the basis $\mathcal{B}$ to the standard basis of $F^{\dagger}_{q^2-1}[\mathbf{X}]$. Furthermore, $\theta(\mathcal{B}')$ is the set of all monomials $\mathbf{X}^{\mathbf{i}} = X_0^{i_0} \cdots X_n^{i_n}$ of degree q^2-1 such that in the p-ary expansion $i_0 = \sum_{k=0}^{2e-1} i_{0,k} p^k$, we have $i_{0,k} i_{0,e+k} > 0$ for some $k \in \{0, 1, \ldots, e-1\}$; for by definition, $i_{0,j} i_{0,e+j} > 0 \Leftrightarrow U(\mathbf{X}) \mid g_{r_j}(\mathbf{X})^{p^j} \Leftrightarrow U(\mathbf{X}) \mid g_{r_j}(\mathbf{X}) \Leftrightarrow r_j \le b'$.

5.4 Lemma. *Let $n \ge 2$, and let $U(\mathbf{X})$ be as in Assumption 5.2. Define $\mathcal{E}_{U,\mathbf{X}}$ as above. Then the following three statements are equivalent.*

(i) $\operatorname{rank}_p A_1 = \left[\binom{p+n-1}{n}^2 - \binom{p+n-2}{n}^2\right]^e + 1$.

(ii) $\mathcal{E}_{U,\mathbf{X}} = F^{\dagger}_{q^2-1}[\mathbf{X}] \cap U(\mathbf{X}) F_{q^2-q-2}[\mathbf{X}]$.

(iii) If $f(\mathbf{X}) \in F^{\dagger}_{q^2-1}[\mathbf{X}]$ contains no monomials in $\theta(\mathcal{B}')$, and $U(\mathbf{X}) \mid f(\mathbf{X})$, then $f(\mathbf{X}) = 0$.

Moreover, these conditions hold for $n = 2$.

Before proving Lemma 5.4, we observe that condition (i) is independent of the choice of $U(\mathbf{X})$ satisfying Assumption 5.2; hence Lemma 5.4 implies that (ii) and (iii) are likewise independent of the choice of $U(\mathbf{X})$.

Proof of Lemma 5.4. We first verify conditions (i) and (ii) when $n = 2$. In this case, A_{11} is an identity matrix of size q^3+1, so that $\operatorname{rank}_p A_1 = q^3+1$, and (i) holds. By Lemma 5.1, this gives

$$\begin{aligned} &\dim\{f(\mathbf{X}) \in F^{\dagger}_{q^2-1}[\mathbf{X}] : f \text{ vanishes at } P_1, P_2, \ldots, P_s\} \\ &\quad = \binom{p+1}{2}^{2e} - p^{3e} = \binom{p+1}{2}^{2e} - \left[\binom{p+1}{2}^2 - \binom{p}{2}^2\right]^e = \dim \mathcal{E}_{U,\mathbf{X}}\,, \end{aligned}$$

so that (ii) holds as well.

Next we show that (i) $\Leftrightarrow$ (ii). We may suppose that $n \ge 3$. Combining Theorem 4.1 and Lemmas 5.1 and 5.3, we have

$$\begin{aligned} \operatorname{rank}_p A_1 &= 1 + \binom{p+n-1}{n}^{2e} - \dim\bigl(F^{\dagger}_{q^2-1}[\mathbf{X}] \cap U(\mathbf{X}) F_{q^2-q-2}[\mathbf{X}]\bigr) \\ &\le 1 + \binom{p+n-1}{n}^{2e} - \dim \mathcal{E}_{U,\mathbf{X}} \\ &= 1 + \left[\binom{p+n-1}{n}^2 - \binom{p+n-2}{n}^2\right]^e, \end{aligned}$$

and equality holds iff $\mathcal{E}_{U,\mathbf{X}} = F^{\dagger}_{q^2-1}[\mathbf{X}] \cap U(\mathbf{X}) F_{q^2-q-2}[\mathbf{X}]$. Thus (i) $\Leftrightarrow$ (ii).

Assume that (ii) holds, and suppose $f(\mathbf{X}) \in F^{\dagger}_{q^2-1}[\mathbf{X}]$ contains no monomials in $\theta(\mathcal{B}')$, and $U(\mathbf{X}) \mid f(\mathbf{X})$. If $f(\mathbf{X}) \ne 0$, then expand $f(\mathbf{X})$ in terms of the basis $\mathcal{B}'$, and let $\prod_{k=0}^{e-1} g_{r_k}(\mathbf{X})^{p^k} \in \mathcal{B}'$ be a basis element appearing (with nonzero coefficient) in this expansion of $f(\mathbf{X})$, for which the degree in X_0 is maximal. By our choice of $\prod_k g_{r_k}(\mathbf{X})^{p^k}$, no other elements of the basis $\mathcal{B}'$ contribute the same monomial $\theta\big(\prod_k g_{r_k}(\mathbf{X})^{p^k}\big)$, and so $f(\mathbf{X})$ contains a monomial in $\theta(\mathcal{B}')$, contrary to the hypothesis. Thus (ii) $\Rightarrow$ (iii).

Conversely, assume (iii) holds, and suppose that $f(\mathbf{X}) \in F^{\dagger}_{q^2-1}[\mathbf{X}]$ is divisible by $U(\mathbf{X})$. We must show that $f(\mathbf{X}) \in \mathcal{E}_{U,\mathbf{X}}$. If $f(\mathbf{X})$ contains no monomials in $\theta(\mathcal{B}')$, then $f(\mathbf{X}) = 0$ and we are done. Otherwise, choose a monomial $\mathbf{X}^{\mathbf{i}} = X_0^{i_0} \cdots X_n^{i_n} = \theta\big(\prod_{k=0}^{e-1} g_{r_k}(\mathbf{X})^{p^k}\big) \in \theta(\mathcal{B}')$ appearing in $f(\mathbf{X})$ (with coefficient $c \neq 0$, say) for which i_0 is maximal. Then $f(\mathbf{X}) - c\prod_k g_{r_k}(\mathbf{X})^{p^k} \in F^{\dagger}_{q^2-1}[\mathbf{X}]$ is also divisible by $U(\mathbf{X})$, and has one fewer monomial of degree i_0 in X_0, than does $f(\mathbf{X})$. After a finite number of iterations, we obtain $f(\mathbf{X}) - g(\mathbf{X}) \in F^{\dagger}_{q^2-1}[\mathbf{X}]$ having no monomials in $\theta(\mathcal{B}')$, where $g(\mathbf{X}) \in \mathcal{E}_{U,\mathbf{X}}$; then by assumption, $f(\mathbf{X}) - g(\mathbf{X}) = 0$, and so (iii) $\Rightarrow$ (ii). $\square$

Proof of Theorem 1.1. We must show that the conditions of Lemma 5.4 hold for all $n \geq 2$. The case $n = 2$ is already settled. Hence we assume $n \geq 3$ and proceed by induction on n.

Suppose that $f(\mathbf{X}) \in F^{\dagger}_{q^2-1}[\mathbf{X}]$ contains no monomials in $\theta(\mathcal{B}')$, and $U(\mathbf{X}) \mid f(\mathbf{X})$. We must show that $f(\mathbf{X}) = 0$. Let $H := \mathcal{Z}(X_0)$, and as before, abbreviate $\mathbf{X}' = (X_1, X_2, \ldots, X_n)$. Let W be any nondegenerate hyperplane of H (so that W has codimension 2 in $PG(V)$). Then $W = H \cap \mathcal{Z}(\ell)$ for some nonzero $\ell(\mathbf{X}') \in F_1[\mathbf{X}']$ which depends on the choice of W only to within a nonzero scalar multiple. Choose this nonzero scalar multiple so that the last of $X_1, \ldots, X_n$ appearing in $\ell(\mathbf{X}')$ (with nonzero coefficient), appears with coefficient 1. For the sake of argument, we assume that $\ell(\mathbf{X}') = X_n - \sum_{i=1}^{n-1} c_i X_i$. (The argument is similar if $\ell(\mathbf{X}') = X_k - \sum_{i=1}^{k-1} c_i X_i$, $1 \leq k < n$.) Now $\mathcal{Z}(\ell) = W \oplus \langle(1,0,0,0,\ldots,0)\rangle$ is a nondegenerate hyperplane of $PG(V)$. Thus $U_W(X_0, \ldots, X_{n-1}) := U(X_0, \ldots, X_{n-1}, \sum c_i X_i)$ is a nondegenerate unitary form in $(X_0, \ldots, X_{n-1})$, and U_W divides $f_W(X_0, \ldots, X_{n-1}) := f(X_0, \ldots, X_{n-1}, \sum c_i X_i)$. Observe that U_W satisfies Assumption 5.2 for $n-1$ in place of n. Every monomial appearing in $f(\mathbf{X})$ is of the form $\mathbf{X}^{\mathbf{i}} = X_0^{i_0} X_1^{i_1} \cdots X_n^{i_n}$ where $i_{0,0} i_{0,e} = i_{0,1} i_{0,e+1} = \cdots = i_{0,e-1} i_{0,2e-1} = 0$ for the digits in the p-ary expansion $i_0 = \sum_{k=0}^{2e-1} i_{0,k} p^k$. Hence every monomial appearing in $f_W(X_0, \ldots, X_{n-1})$ is of the form $X_0^{i_0} X_1^{i'_1} \cdots X_{n-1}^{i'_{n-1}}$ where i_0 is as before. Furthermore, $f_W(X_0, \ldots, X_{n-1}) \in F^{\dagger}_{q^2-1}[\mathbf{X}]$ by Lemma 2.5(i) of [2]. By induction, we have $f_W(X_0, \ldots, X_{n-1}) = 0$, i.e. $\ell(\mathbf{X}') \mid f(\mathbf{X})$. The number of distinct linear factors of $f(\mathbf{X})$

obtained in this way, equals the number of nondegenerate hyperplanes of H, which by Lemma 2.1, equals $(q^n-(-1)^n)(q^{n-1}+(-1)^n)/(q^2-1) \geq q^2(q^2-q+1)$, and this exceeds q^2-1. Thus $f(\mathbf{X})=0$ as required. $\square$

Finally, we identify the row space of A_1 over F, as a module for H, the isometry group of $U(\mathbf{X})$ (i.e. $H=\{T\in GL(n+1,F) : U(T\mathbf{X})=U(\mathbf{X})\}$, the unitary group). First recall (cf. [2]) that

$$Row(A) \cong \langle \mathbf{1}\rangle \oplus F^{\dagger}_{q^2-1}[\mathbf{X}]$$

as FG-modules where $G=GL(n+1,F)$; '*Row*' denotes row space over F; and $\langle\mathbf{1}\rangle$ is the one-dimensional trivial module. Also recall that $F^{\dagger}_{q^2-1}[\mathbf{X}]$ is the subspace of $F_{q^2-1}[\mathbf{X}]$ spanned by all polynomials of the form $\ell(\mathbf{X})^{q^2-1}$ where $\ell(\mathbf{X})\in F_1[\mathbf{X}]$. The following may be shown by arguments similar to those found in [2].

5.5 Theorem. *Let $\mathcal{L}_{U,\mathbf{X}}$ be the subspace of $F_{q^2-1}[\mathbf{X}]$ spanned by all polynomials of the form $\ell(\mathbf{X})^{q^2-1}$, where $\ell(\mathbf{X})\in F_1[\mathbf{X}]$ such that $\mathcal{Z}(\ell)$ is a hyperplane tangent to the Hermitian variety $\mathcal{Z}(U)$. Then*

$$Row(A_1) \cong \langle\mathbf{1}\rangle \oplus \mathcal{L}_{U,\mathbf{X}} \cong \langle\mathbf{1}\rangle \oplus \left(F^{\dagger}_{q^2-1}[\mathbf{X}]\,/\,\mathcal{E}_{U,\mathbf{X}}\right)$$

as FH-modules.

References

1. E. F. Assmus, Jr. and J. D. Key, *Designs and their Codes,* Cambridge Univ. Press, Cambridge, 1992.
2. A. Blokhuis and G. E. Moorhouse, 'Some p-ranks related to orthogonal spaces', submitted to *J. Algeb. Comb.*
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, 1993(?).
4. J. M. Goethals and P. Delsarte, "On a class of majority-logic decodable cyclic codes", *IEEE Trans. Inform. Theory* **14** (1968), 182–188.
5. J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries*, Oxford Univ. Press, Oxford and New York, 1991.

6. 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.
7. S. E. Payne and J. A. Thas, *Finite Generalized Quadrangles,* Pitman, Boston and London, 1984.
8. 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.
9. J. A. Thas, "Ovoids and spreads of finite classical polar spaces", *Geom. Ded.* **10** (1981), 135–144.
10. J. A. Thas, "Semi-partial geometries and spreads of classical polar spaces", *J. Comb. Theory Ser. A* **35** (1983), 58–66.