Some p-ranks Related to Finite Geometric Structures

G. ERIC MOORHOUSE[†] Dept. of Mathematics, University of Wyoming, Laramie WY 82071–3036, U.S.A. moorhous@UWyo.edu

Dedicated to Professor T. G. Ostrom

Abstract The p-rank of the point-hyperplane incidence matrix A of $PG(n, p^e)$ is well-known. Let A_S be the submatrix formed by the rows of A indexed by an arbitrary subset S of the points. We show that the p-rank of A_S is related to the Hilbert function (or a modification thereof) for $\mathcal{I}(S)$, the ideal of $F[X_0, X_1, \ldots, X_n]$ generated by all homogeneous polynomials vanishing on S. This leads to a determination of $\operatorname{rank}_p(A_S)$ in case S is a naturally embedded Grassmann variety. The cases when S is a quadric or a Hermitian variety have been treated by Blokhuis and the author [2] and the author [10] respectively.

1 HILBERT FUNCTIONS AND p-RANKS

Let $F = GF(q)$, $q = p^e$, and let A be the incidence matrix of points versus hyperplanes of $PG(n, F)$. Thus A is a square matrix of size $N = (q^{n+1} - 1)/(q - 1)$ having entries 1 and 0 corresponding to incident and non-incident point-hyperplane pairs. Now let A_S be an $s \times N$ submatrix of A, whose rows are indexed by an s-subset S of the points of $PG(n, F)$. The intent of Theorem 1 is to describe a general approach to finding the p-rank of A_S. This approach makes use of a modification of the Hilbert function of $\mathcal{I}(S)$, the ideal in the polynomial ring $R := F[X_0, X_1, \ldots, X_n]$ generated by all homogeneous polynomials which vanish on S. Much of our terminology and background results are standard in algebraic geometry; see eg. [7].

For each integer $k \geq 0$, let R_k be the F-subspace of R consisting of all homogeneous polynomials of degree k. The natural action of $G := GL(n + 1, F)$ on

† The author is grateful to David Wagner and Andries Brouwer for useful discussions, and to the Fields Institute for Research in Mathematical Sciences where part of this research was conducted.

$R_1 \cong F^{n+1}$ extends uniquely to an action of G on the algebra $R = \bigoplus_{k\geq 0} R_k$, and each R_k is an FG-submodule. Let $\mathfrak{I} \subseteq R$ be a homogeneous ideal, i.e. the ideal $\mathfrak{I}$ is generated by homogeneous polynomials. The *Hilbert function* of $\mathfrak{I}$ is defined by

$$h_{\mathfrak{I}}(k) = \dim\bigl(R_k \;/\; \mathfrak{I} \cap R_k\bigr) = \binom{n+k}{n} - \dim(\mathfrak{I} \cap R_k)\,.$$

It is known that for all sufficiently large k, the function $h_{\mathfrak{I}}(k)$ agrees with a polynomial $P_{\mathfrak{I}}(k)$, called the *Hilbert polynomial of* $\mathfrak{I}$. Over algebraically closed fields, Hilbert polynomials provide a precise algebraic definition of the degree and dimension of projective varieties.

Denote by $R_k^{\dagger}$ the subspace of R_k spanned by all monomials $X_0^{\alpha_0} X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ where $\alpha_0, \alpha_1, \ldots, \alpha_n$ are non-negative integers summing to k such that the multinomial coefficient $\binom{k}{\alpha_0,\, \alpha_1,\, \cdots,\, \alpha_n}$ is not divisible by p. This is more than an F-subspace; as shown in [2], it is an FG-submodule of R_k. Note that the inclusion $R_k^{\dagger} \subseteq R_k$ is proper iff $k \geq p$. By Lucas' Theorem (see Section 2) we have

$$dim(R_k^{\dagger}) = \prod_{\ell=0}^{e-1} \binom{n+k_\ell}{n}$$

where the p-adic expansion of k is given by $k = \sum_{\ell=0}^{e-1} k_\ell p^\ell$, $0 \leq k_\ell \leq p-1$. In particular, $\dim(R_{q-1}^{\dagger}) = \binom{p+n-1}{n}^e = (\dim R_{p-1})^e$. We modify the Hilbert function of $\mathfrak{I}$ by defining

$$h_{\mathfrak{I}}^{\dagger}(k) = dim\bigl(R_k^{\dagger} \;/\; \mathfrak{I} \cap R_k^{\dagger}\bigr)\,.$$

In general, the values of $h_{\mathfrak{I}}^{\dagger}(k)$ for $k \gg 0$ are not given by any polynomial.

Let G_S be the subgroup of $G = GL(n+1, F)$ preserving the point set S in $PG(n, F)$. As explained in Section 5, the row and column spaces of A_S over F are naturally contragredient FG_S-modules. Similarly, the row and column spaces of $J - A_S$ are naturally contragredient FG_S-modules, where J is an $s \times N$ matrix of 1's. In Section 3 we prove

THEOREM 1

(i) $\mathrm{rank}_p(J - A_S) = h_{\mathcal{I}(S)}^{\dagger}(q-1)$. Moreover, the column space $Col(J - A_S)$ is isomorphic to $R_{q-1}^{\dagger} \;/\; \mathcal{I}(S) \cap R_{q-1}^{\dagger}$ as an FG_S-module.

(ii) $\mathrm{rank}_p A_S$ differs from $\mathrm{rank}_p(J - A_S)$ by at most one. If $|H \cap S| \equiv 1 \mod p$ for every hyperplane H of $PG(n, F)$, then $\mathrm{rank}_p A_S = 1 + \mathrm{rank}_p(J - A_S)$, and $Col(A_S) \cong \langle \mathbf{1} \rangle \oplus Col(J - A_S)$ where $\langle \mathbf{1} \rangle$ is a trivial FG_S-module of dimension one.

We are most interested in the case S is a 'discrete variety' of the form $\mathcal{Z}(\mathfrak{I})$, i.e. the set of points of $PG(n, F)$ where a given homogeneous ideal $\mathfrak{I}$ vanishes. Although the Hilbert function of $\mathfrak{I}$ is often readily available, care is required in applying Theorem 1 since in general, the inclusion $\mathcal{I}(S) \supseteq \mathfrak{I}$ may be proper. The *radical* of $\mathfrak{I}$ is the ideal $\sqrt{\mathfrak{I}} := \{f \in R : f^k \in \mathfrak{I}$ for some positive integer $k\} \subseteq R$. Clearly

$$\mathcal{I}(S) = \mathcal{I}(\mathcal{Z}(\mathfrak{I})) \supseteq \sqrt{\mathfrak{I}} \supseteq \mathfrak{I}\,.$$

Since F is not algebraically closed, $\mathcal{I}(\mathcal{Z}(\mathfrak{I}))$ is typically larger than $\sqrt{\mathfrak{I}}$ (considering that for all $\mathfrak{I}$, $X_i^q X_j - X_i X_j^q$ vanishes on $PG(n, F)$ for all $i \neq j$).

DEFINITION $\mathfrak{I}$ satisfies FFN(k) (Finite Field Nullstellensatz of degree k) if every $f \in R_k$ which vanishes on $\mathcal{Z}(\mathfrak{I})$, belongs to $\mathfrak{I}$.

In many cases $\mathfrak{I}$ satisfies FFN$(q-1)$, which implies that $h^{\dagger}_{\mathcal{I}(\mathcal{Z}(\mathfrak{I}))}(q-1) = h^{\dagger}_{\mathfrak{I}}(q-1)$ and Theorem 1 applies. Moreover, $h^{\dagger}_{\mathfrak{I}}(q-1) \le (h_{\mathfrak{I}}(p-1))^e$ (see Lemma 2) with equality in many cases, including Examples 1.1, 1.2, 1.4 below.

1.1 Example: Projective Spaces

Let $\mathfrak{I} = (0)$, $S = \mathcal{Z}(0) = PG(n, p^e)$. Then

$$\operatorname{rank}_p A_S = \operatorname{rank}_p A = h^{\dagger}_{(0)}(q-1) + 1 = (h_{(0)}(p-1))^e + 1 = \tbinom{p+n-1}{n}^e + 1.$$

This is the well-known result of Goethals and Delsarte [6], MacWilliams and Mann [9], and Smith [11]; see also [3]. In this case, $Col(A) \cong R^{\dagger}_{q-1} \oplus \langle \mathbf{1} \rangle$ as FG-modules.

1.2 Example: Quadrics

Let $Q(X) = Q(X_0, X_1, \ldots, X_n)$ be a quadratic form, i.e. $Q(X) \in R_2$. We will assume that the corresponding bilinear form $f(X,Y) := Q(X+Y) - Q(X) - Q(Y)$ is nondegenerate. Thus the quadric $S := \mathcal{Z}(Q)$ is nondegenerate, and if $p = 2$ then n is odd. Homogeneous polynomials of degree $k \ge 2$ belonging to the principal ideal $\mathfrak{I} = (Q)$ are precisely those polynomials of the form $Q(X)f(X)$ where $f \in R_{k-2}$, so

$$h_{(Q)}(k) = \dim(R_k) - \dim(R_{k-2}) = \tbinom{n+k}{n} - \tbinom{n+k-2}{n}.$$

In [2] it is also shown that (Q) satisfies FFN(q) for $n \ge 4$, and FFN$(q-1)$ for $n = 3$, and that consequently

$$\operatorname{rank}_p A_{\mathcal{Z}(Q)} = \left[\tbinom{n+p-1}{n} - \tbinom{n+p-3}{n}\right]^e + 1$$

for $n \ge 3$. This statement fails for $n \le 2$, as does FFN$(q-1)$.

1.3 Example: Hermitian Varieties

Suppose $q = p^{2d}$ and let $U(X) = \sum_{i=0}^{n} \sum_{j=0}^{n} a_{ij} X_i X_j^{p^d}$ be a nondegenerate unitary form; thus $a_{ji} = a_{ij}^{p^d}$ and $\det\big[a_{ij}\big] \ne 0$. Then $S := \mathcal{Z}(U)$ is a nondegenerate Hermitian variety. In [10] it is shown that the principal ideal (U) satisfies FFN(q) for $n \ne 3$, and

$$\operatorname{rank}_p A_{\mathcal{Z}(U)} \;=\; h^{\dagger}_{(U)}(q-1) + 1 \;=\; \left[\tbinom{n+p-1}{n}^2 - \tbinom{n+p-2}{n}^2\right]^d + 1$$

for all $n \ge 1$.

1.4 Example: Grassmann Varieties

Let $V = F^{\nu+1}$. Every subspace $U \le V$ of dimension $r+1$ gives rise to a one-dimensional subspace $\bigwedge^{r+1} U \le \bigwedge^{r+1} V$. This defines an injective mapping from the collection of projective r-subspaces of $PG(\nu, F)$ to points of $PG(\bigwedge^{r+1} V) = PG(n, F)$ where $n = \tbinom{\nu+1}{r+1} - 1$. The image of this mapping is the *Grassmann variety* $S = G_{r,\nu}(F)$, a discrete variety of the form $S = \mathcal{Z}(\mathfrak{I})$ where $\mathfrak{I}$ is the ideal generated by a certain collection of homogeneous quadratic polynomials known as van der Waerden syzygies. In Section 4, we show that $\mathfrak{I}$ satisfies FFN$(q-1)$, and consequently

THEOREM 2 If $S = \mathcal{Z}(\mathfrak{I})$ is the Grassmann variety $G_{r,\nu}(p^e)$ naturally embedded in $PG(n, p^e)$ where $n = \binom{\nu+1}{r+1} - 1$, then $\operatorname{rank}_p A_S = \delta^e + 1$ where $\delta = h_{\mathfrak{I}}(p-1)$ is given by the formula

$$h_{\mathfrak{I}}(k) = \prod_{j=0}^{r} \frac{(\nu + k - r + j)!\, j!}{(\nu - r + j)!\,(k+j)!}\,.$$

For example, the Grassmann variety $G_{0,n}(p^e)$ coincides with $PG(n, p^e)$, and the p-rank value from Theorem 2 agrees with that obtained in Example 1.1. Also, the Grassmann variety $G_{1,3}(p^e)$ coincides with the Klein quadric in $PG(5, p^e)$, and the value $\operatorname{rank}_p A_S = [p(p+1)^2(p+2)/12]^e + 1$ from Theorem 2 agrees with the value given in Example 1.2.

2 STANDARD MONOMIALS

The goal of this section is to provide combinatorial interpretations of the Hilbert function values $h_{\mathfrak{I}}(k)$ and $h^{\dagger}_{\mathfrak{I}}(k)$ as the cardinalities of certain sets of monomials. In many cases, including Examples 1.2–1.4 above, this leads to explicit computation of $h^{\dagger}_{\mathfrak{I}}(q-1)$ and hence the desired p-rank values; in other cases, they may at least provide useful bounds for p-ranks. We require only a few notions from the theory of Gröbner bases, as introduced in [12], [13]; several broader texts on the subject are now available, including [5].

Let $X = (X_0, X_1, \ldots, X_n)$ be an $(n+1)$-tuple of indeterminates, and let $R = K[X] = K[X_0, X_1, \ldots, X_n]$ be the polynomial ring over a fixed arbitrary field K. A *monomial* is a polynomial of the form $X_0^{\alpha_0} X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in R$ for some non-negative integers $\alpha_0, \alpha_1, \ldots, \alpha_n$ (note that we require coefficient 1). The set of monomials is a multiplicative submonoid $\mathcal{M} \subset R$. A *monomial ordering* is a total ordering $<$ on $\mathcal{M}$ such that

(i) $(\mathcal{M}, <)$ is well-ordered with least element 1, and
(ii) for all $m, m', m'' \in \mathcal{M}$, $m < m' \Rightarrow m''m < m''m'$.

The most well-known monomial ordering, and the only one we shall require, is the *lexicographical ordering* defined by

$$X_0^{\alpha_0} X_1^{\alpha_1} \cdots X_n^{\alpha_n} < X_0^{\beta_0} X_1^{\beta_1} \cdots X_n^{\beta_n} \iff \begin{array}{r} \text{there exists } i_0 \text{ such that } \alpha_{i_0} < \beta_{i_0} \\ \text{and } \alpha_i = \beta_i \text{ whenever } i < i_0\,. \end{array}$$

For any nonzero polynomial $f \in R$, let $\operatorname{Init}(f)$ denote the *initial monomial* of f, i.e. the largest monomial with respect to $<$ which appears in f. For any subset $B \subseteq R$, define $\operatorname{Init}(B) := \{\operatorname{Init}(f) : 0 \neq f \in B\}$.

Now let $\mathfrak{I} \subseteq R$ be an ideal. A monomial $m \in \mathcal{M}$ is *standard* (with respect to $\mathfrak{I}$) if $m \notin \operatorname{Init}(\mathfrak{I})$. Let $k \geq 0$, and let R_k be the k-homogeneous component of R. We immediately have

LEMMA 1 $R_k = (\mathfrak{I} \cap R_k) \oplus \langle \mathcal{SM}_{\mathfrak{I}}(k) \rangle$ where $\mathcal{SM}_{\mathfrak{I}}(k)$ is the set of standard monomials of degree k. In particular, $h_{\mathfrak{I}}(k) = \left|\mathcal{SM}_{\mathfrak{I}}(k)\right|$.

Now suppose the field K (not necessarily finite) has prime characteristic p. Given an integer $k \geq 0$, choose $e \geq 0$ such that $p^e > k$. Then k has a unique p-adic expansion of the form $k = k_0 + k_1 p + k_2 p^2 + \cdots + k_{e-1} p^{e-1}$ where $0 \leq k_\ell \leq p-1$. As before, let $R_k^\dagger$ be the subspace of R_k spanned by all monomials $m(X) = X_0^{\alpha_0} X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ such that the multinomial coefficient

$$\binom{k}{\alpha_0,\ \alpha_1,\ \cdots,\ \alpha_n} := \begin{cases} \dfrac{k!}{\alpha_0!\alpha_1!\cdots\alpha_n!}, & \alpha_\ell \geq 0,\ \sum \alpha_\ell = k; \\ 0, & \text{otherwise} \end{cases}$$

is not divisible by p (and so in particular, $\deg(m) = \alpha_0 + \alpha_1 + \cdots + \alpha_n = k$). Lucas' Theorem (see [3], [2]) states that

$$\binom{k}{\alpha_0,\ \alpha_1,\ \cdots,\ \alpha_n} \equiv \prod_{\ell=0}^{e-1} \binom{k_\ell}{\alpha_{0\ell}\,,\ \alpha_{1\ell}\,,\ \cdots,\ \alpha_{n\ell}} \mod p$$

where $\alpha_i = \sum_\ell \alpha_{i\ell} p^\ell$, $0 \leq \alpha_{i,\ell} \leq p-1$. It follows that the monomial $m(X)$ belongs to $R_k^\dagger$ if and only if it is expressible in the form

$$m(X) = \textstyle\prod_{\ell=0}^{e-1} m_\ell(X)^{p^\ell}$$

where $m_\ell(X)$ is a monomial of degree k_ℓ. In particular,

$$dim(R_k^\dagger) = \prod_{\ell=0}^{e-1} \binom{n+k_\ell}{n}.$$

We say the monomial $m(X)$ is *p-standard* if each of the monomials m_ℓ (as above) is standard.

LEMMA 2 Let $k \geq 0$ be an integer, with p-adic coefficients k_ℓ as above. Then

(i) $R_k^\dagger = (\mathfrak{I} \cap R_k^\dagger) + \langle \mathcal{SM}_\mathfrak{I}^{(p)}(k) \rangle$ where $\mathcal{SM}_\mathfrak{I}^{(p)}(k)$ is the set of p-standard monomials of degree k.

(ii) $h_\mathfrak{I}^\dagger(k) \leq \left|\mathcal{SM}_\mathfrak{I}^{(p)}(k)\right| = \prod_{\ell=0}^{e-1} h_\mathfrak{I}(k_\ell)$.

(iii) $h_\mathfrak{I}^\dagger(q-1) \leq (h_\mathfrak{I}(p-1))^e$.

Proof: We must show that every monomial in $R_k^\dagger$, but not in $\mathfrak{I}$, is p-standard. Accordingly, suppose $m(X) = \prod_{\ell=0}^{e-1} m_\ell(X)^{p^\ell}$ for some monomials $m_\ell \in R_{k_\ell}$. If m is not p-standard, then for some ℓ_0 and some $f \in R_{k_{\ell_0}}$ we have $m_{\ell_0} = \mathrm{Init}(f)$. But then since $\mathrm{char}(K) = p$, the polynomial

$$f(X)^{p^{\ell_0}} \textstyle\prod_{\ell \neq \ell_0} m_\ell(X)^{p^\ell}$$

lies in $\mathfrak{I} \cap R_k^\dagger$, with initial monomial $m \in \mathrm{Init}(\mathfrak{I} \cap R_k^\dagger)$. This proves (i), and the remaining conclusions clearly follow as well. $\square$

LEMMA 3 Let $k \geq 0$. Then

(i) $h_{\mathcal{I}(\mathcal{Z}(\mathfrak{I}))}(k) \leq h_\mathfrak{I}(k)$ and $h_{\mathcal{I}(\mathcal{Z}(\mathfrak{I}))}^\dagger(k) \leq h_\mathfrak{I}^\dagger(k)$.

(ii) If $\mathfrak{I}$ satisfies FFN(k), then equality holds in (i).

(iii) Suppose the ideal $\mathfrak{I}$ is prime. Then $\mathfrak{I}$ satisfies FFN(k) iff $\mathfrak{I}$ satisfies FFN(ℓ) for all $\ell \leq k$, iff $h_{\mathcal{I}(\mathcal{Z}(\mathfrak{I}))}(k) = h_\mathfrak{I}(k)$, iff $h_{\mathcal{I}(\mathcal{Z}(\mathfrak{I}))}(\ell) = h_\mathfrak{I}(\ell)$ for all $\ell \leq k$.

Proof: (i) and (ii) are clear. Suppose $\mathfrak{I}$ is a prime ideal satisfying FFN(k), and let $0 \le \ell < k$. For $i = 0, 1, 2, \ldots, n$, the polynomial $X_i^{k-\ell} f(X_0, \ldots, X_n) \in R_k$ vanishes on $\mathcal{Z}(\mathfrak{I})$. If $f \notin \mathfrak{I}$ then $X_0, X_1, \ldots, X_n \in \mathfrak{I}$ and $\mathfrak{I} \supset R_k \ni f$, a contradiction. Hence $\mathfrak{I}$ satisfies FFN(ℓ), and (iii) follows. $\square$

The following is well-known.

LEMMA 4 Suppose $f \in R$ has degree $\le q-1$ in each of $X_0, X_1, \ldots, X_n$. If f vanishes on F^{n+1} then $f = 0$.

Proof: If $\sum_\alpha a_{\alpha_0\alpha_1\cdots\alpha_n} x_0^{\alpha_0} x_1^{\alpha_1} \cdots x_n^{\alpha_n} = 0$ (sum over $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_n) \in \{0, 1, 2, \ldots, q-1\}^{n+1}$) for all $x = (x_0, x_1, \ldots, x_n) \in F^{n+1}$, then the vector $\big(a_\alpha\big)_\alpha$ lies in the left null space of the $q^{n+1} \times q^{n+1}$ matrix with (α, x)-entry equal to $x_0^{\alpha_0} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. By [2, Lemma 2.3], the latter matrix is nonsingular, and so $\big(a_\alpha\big) = 0$. $\square$

3 INCIDENCE MATRICES

Most of this section can be found in [2] and [10], either directly or implicitly. In particular, the following is shown in [2]. Let $F^{k\times\ell}$ denote the vector space of $k \times \ell$ matrices over $F = GF(q)$, and let A be the incidence matrix of $PG(n, F)$ as in Section 1.

LEMMA 5 $Col(J_{N,N} - A) \cong R_{q-1}^\dagger$ as FG-modules, where $G = GL(n+1, F)$.

We sketch the proof of Lemma 5, describing the natural isomorphism $R_{q-1}^\dagger \to Col(J_{N,N} - A)$, since this is useful in verifying Theorem 1. For each $f(X) = f(X_0, X_1, \ldots, X_n) \in R_{q-1}^\dagger$ and $x \in F^{n+1}$, the value of $f(x) \in F$ clearly depends only on the subspace $\langle x\rangle$. So we have a well-defined FG-homomorphism $\varphi : R_{q-1}^\dagger \to F^{N\times 1}$ which maps f to the column vector having values $f(x)$ as $\langle x\rangle$ ranges over the one-dimensional subspaces of F^{n+1} (i.e. the points of $PG(n, F)$). For any nonzero $\ell(X) \in R_1$, $\varphi(\ell^{q-1})$ is the column of $J_{N,N} - A$ corresponding to the hyperplane $\mathcal{Z}(\ell)$. However, $Col(J_{N,N} - A)$ and $R_{q-1}^\dagger$ both have dimension $\binom{p+n-1}{n}^e$. Therefore $R_{q-1}^\dagger = \big\langle \ell(X)^{q-1} : \ell \in R_1 \big\rangle$ and $\varphi : R_{q-1}^\dagger \to Col(J_{N,N} - A)$ is the required isomorphism. $\square$

Now let $\pi_S : F^{N\times 1} \to F^{s\times 1}$ be the projection onto the coordinates corresponding to the points of S. This gives rise to an exact sequence of FG_S-modules:

$$0 \longrightarrow \mathcal{I}(S) \cap R_{q-1}^\dagger \longrightarrow R_{q-1}^\dagger \stackrel{\pi_S\circ\varphi}{\longrightarrow} Col(J_{s,N} - A_S) \longrightarrow 0\,.$$

This proves Theorem 1(i).

Since $\mathrm{rank}_p(J_{s,N}) = 1$, it is clear that $\mathrm{rank}_p A_S$ differs from $\mathrm{rank}_p(J_{s,N} - A_S)$ by at most 1. Now suppose that $|H \cap S| \equiv 1 \mod p$ for every hyperplane H of $PG(n, F)$. Then the sum of the rows of A_S (modulo p) equals $\mathbf{1} = (1, 1, \ldots, 1) \in F^{1\times N}$, so that $Row(A_S) = Row(J_{s,N} - A_S) + \langle \mathbf{1}\rangle$. To see that the latter sum is direct, observe that every row of $J_{s,N} - A_S$ has sum $q^n \equiv 0 \mod p$, whereas every row of A_S has sum $\equiv 1 \mod p$. The proof of Theorem 1 follows by taking contragredients (Section 5).

4 GRASSMANN VARIETIES

For terminology and basic properties on Grassmann varieties, we follow [12], [13]; see also [4] for a more general approach.

We develop further the description of Example 1.4, this time over an arbitrary field K, and using explicit coordinates. Consider the vector space $V = K^{\nu+1}$, with standard basis $\{e_0, e_1, \ldots, e_\nu\}$. Fix an integer r, $0 \le r \le \nu$. By $\bigwedge^{r+1} V$, we mean the K-vector space of dimension $n+1 := \binom{\nu+1}{r+1}$ with basis consisting of the symbols

$$e_{\tau_0\tau_1\cdots\tau_r} := e_{\tau_0} \wedge e_{\tau_1} \wedge \cdots \wedge e_{\tau_r}\,, \quad 0 \le \tau_0 < \tau_1 < \cdots < \tau_r \le \nu\,.$$

Given an $(r+1)$-dimensional subspace $U \le V$, let $x = \left[x_{ij}\right]$ be an $(r+1) \times (\nu+1)$ matrix whose rows form a basis for U. Then $\bigwedge^{r+1} U$ is the point (one-dimensional subspace) of $\bigwedge^{r+1} V$ spanned by the vector

$$\Phi(x) := \sum_{[\tau_0\tau_1\cdots\tau_r]\in\Lambda} \det \begin{bmatrix} x_{0,\tau_0} & x_{0,\tau_1} & \cdots & x_{0,\tau_r} \\ x_{1,\tau_0} & x_{1,\tau_1} & \cdots & x_{1,\tau_r} \\ \vdots & \vdots & \ddots & \vdots \\ x_{r,\tau_0} & x_{r,\tau_1} & \cdots & x_{r,\tau_r} \end{bmatrix} e_{\tau_0\tau_1\cdots\tau_r}\ .$$

The Grassmann variety $G_{r,\nu}(K) \subseteq PG\big(\bigwedge^{r+1} V\big) = PG(n, K)$ is the set of all such points. To justify the term 'variety', we must find an ideal $\mathfrak{I}$ whose zero set coincides with $G_{r,\nu}(K)$.

Let $X = [X_{ij}]_{0\le i\le r,\ 0\le j\le\nu}$ be an $(r+1) \times (\nu+1)$ matrix of indeterminates, and let $K[X] = K[X_{00}, X_{01}, \ldots, X_{r\nu}]$ be the corresponding polynomial algebra over K. As coordinate functions for $\bigwedge^{r+1} V$, we require $\binom{\nu+1}{r+1}$ additional indeterminates, for which purpose we adopt the set Λ consisting of the $\binom{\nu+1}{r+1}$ *bracket symbols*

$$[\tau_0\ \tau_1\ \cdots\ \tau_r], \qquad 0 \le \tau_0 < \tau_1 < \cdots < \tau_r \le \nu.$$

Let $K[\Lambda]$ denote the polynomial algebra in these new indeterminates. Let φ : $K[\Lambda] \to K[X]$ be the unique algebra homomorphism such that

$$\varphi([\tau_0\ \tau_1\ \cdots\ \tau_r]) = \det \begin{bmatrix} X_{0\tau_0} & X_{0\tau_1} & \cdots & X_{0\tau_r} \\ X_{1\tau_0} & X_{1\tau_1} & \cdots & X_{1\tau_r} \\ \vdots & \vdots & \ddots & \vdots \\ X_{r\tau_0} & X_{r\tau_1} & \cdots & X_{r\tau_r} \end{bmatrix}.$$

As described above, the Grassmann variety $G_{r,n}(K) \subseteq PG\big(\bigwedge^{r+1} V\big) = PG(n, K)$ is obtained by evaluating the expression

$$\Phi(X) := \sum_{[\tau_0\tau_1\cdots\tau_r]\in\Lambda} \varphi([\tau_0\,\tau_1 \cdots \tau_r])\, e_{\tau_0\tau_1\cdots\tau_r}$$

at constant matrices $\left[x_{ij}\right]$ of full rank. Moreover, $G_{r,n}(K) = \mathcal{Z}(\mathfrak{I})$ where $\mathfrak{I} \subseteq K[\Lambda]$ is the *syzygy ideal* generated by certain homogeneous quadratic polynomials known as *van der Waerden syzygies,* as described in [13], [12]; the exact form of these generators will not be required here.

Let $<$ denote the lexicographical order on monomials for each of our sets X, Λ of indeterminates; thus

$$X_{00} < X_{01} < \cdots < X_{0\nu} < X_{10} < \cdots < X_{1\nu} < \cdots < X_{r0} < \cdots < X_{r\nu}\,;$$

$$\prod_{i,j} X_{ij}^{\alpha_{ij}} < \prod_{i,j} X_{ij}^{\beta_{ij}} \iff \begin{array}{c}\text{there exists } (i_0, j_0) \text{ such that } \alpha_{i_0 j_0} < \beta_{i_0 j_0} \\ \text{and } \alpha_{ij} = \beta_{ij} \text{ whenever } X_{ij} < X_{i_0 j_0}\,;\end{array}$$

$$[\tau_0\, \tau_1\, \cdots\, \tau_r] < [\rho_0\, \rho_1\, \cdots\, \rho_r] \iff \begin{array}{c}\text{there exists } j_0 \text{ such that } \tau_{j_0} < \rho_{j_0} \\ \text{and } \tau_j = \rho_j \text{ for all } j < j_0.\end{array}$$

Products of indeterminates in Λ are represented by *tableaux,* which are arrays having the indeterminates as rows: thus the monomial $T = \prod_{i=1}^{k} [\tau_{i0}\, \tau_{i1}\, \cdots\, \tau_{ir}]$ of degree k may be expressed as

$$T = \begin{bmatrix} \tau_{10} & \tau_{11} & \cdots & \tau_{1r} \\ \tau_{20} & \tau_{21} & \cdots & \tau_{2r} \\ \vdots & \vdots & & \vdots \\ \tau_{k0} & \tau_{k1} & \cdots & \tau_{kr} \end{bmatrix}.$$

The *degree* of this tableau is k, the number of rows. We may assume that the rows have been listed in weakly increasing order:

$$[\tau_{10}\, \tau_{11}\, \cdots\, \tau_{1r}] \le [\tau_{20}\, \tau_{21}\, \cdots\, \tau_{2r}] \le \cdots \le [\tau_{k0}\, \tau_{k1}\, \cdots\, \tau_{kr}].$$

Let

$$T = \big[\tau_{ij} : 1 \le i \le k,\ 0 \le j \le r\big], \qquad T' = \big[\tau'_{ij} : 1 \le i \le k',\ 0 \le j \le r\big]$$

be two tableaux. Then $T < T'$ iff either $k < k'$, or $k = k'$ and there exists $i \le k$ such that $[\tau_{i0}\, \tau_{i1}\, \cdots\, \tau_{ir}] < [\tau'_{i0}\, \tau'_{i1}\, \cdots\, \tau'_{ir}]$ and the first $i-1$ rows of T' coincide with those of T. By [12], [13] we have

LEMMA 6 Let T be an arbitrary tableau, as above. Then T is standard ($T \notin \mathrm{Init}(\mathfrak{I})$) if and only if every column of T is weakly increasing, i.e. $\tau_{1j} \le \tau_{2j} \le \cdots \le \tau_{kj}$.

The number of standard tableaux of degree k is given by [8, p.387] in slightly different language:

$$h_{\mathfrak{I}}(k) = \det \begin{bmatrix} \binom{\nu+k}{k} & \binom{\nu+k-1}{k-1} & \cdots & \binom{\nu+k-r}{k-r} \\ \binom{\nu+k}{k+1} & \binom{\nu+k-1}{k} & \cdots & \binom{\nu+k-r}{k-r+1} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{\nu+k}{k+r} & \binom{\nu+k-1}{k+r-1} & \cdots & \binom{\nu+k-r}{k} \end{bmatrix}.$$

Although it was assumed in [8] that $\mathrm{char}(K) = 0$, it is clear that the number of standard tableaux with k rows cannot depend on the choice of K. By [1, p.95], the $(r+1) \times (r+1)$ determinant above can be evaluated in closed form, whereby we obtain

LEMMA 7 $h_{\mathfrak{I}}(k) = \displaystyle\prod_{j=0}^{r} \frac{(\nu+k-r+j)!\, j!}{(\nu-r+j)!\,(k+j)!}$, independent of the choice of field K.

Case (i) of the following is found in [12, pp.81–82].

LEMMA 8   Let T, T' be tableaux such that either
 (i) T, T' are both standard; or
 (ii) T, T' are both p-standard where $p = \mathrm{char}(K)$ is prime.
If $\varphi(T)$ and $\varphi(T')$ have the same initial monomial, then $T = T'$.

Proof: We may assume that T, T' are of the same degree k. First suppose that the monomial $T = [\tau_{ij}]_{1\le i\le k,\ 0\le j\le r}$ is standard. Clearly $\mathrm{Init}(\varphi([\tau_{i0}\,\tau_{i1}\cdots\tau_{ir}])) = X_{0,\tau_{i0}}X_{1,\tau_{i1}}\cdots X_{r,\tau_{ir}}$, and so

$$\mathrm{Init}(\varphi(T)) = \prod_{i=1}^{k} X_{0,\tau_{i0}}X_{1,\tau_{i1}}\cdots X_{r,\tau_{ir}}\ .$$

The number of times an integer τ appears in column j of T equals the exponent of $X_{j,\tau}$ in $\mathrm{Init}(\varphi(T))$, and since the jth column of T is weakly increasing, this means we can recover the jth column of T from $\mathrm{Init}(\varphi(T))$, for each $j = 0, 1, 2, \ldots, r$. This verifies the Lemma in Case (i).

Now suppose $T = \prod_{\ell=0}^{e-1} T_\ell^{p^\ell}$ is p-standard, i.e. T_ℓ is a standard tableau of degree $k_\ell \le p-1$. Then

$$\mathrm{Init}(\varphi(T)) = \prod_{\ell=0}^{e-1}\big(\mathrm{Init}\ \varphi(T_\ell)\big)^{p^\ell}.$$

The degree of this polynomial with respect to X_{ij} is given by

$$\deg_{X_{ij}}\big(\mathrm{Init}\ \varphi(T)\big) = \sum_{\ell=0}^{e-1}\deg_{X_{ij}}\big(\mathrm{Init}\ \varphi(T_\ell)\big)p^\ell$$

where $\deg_{X_{ij}}\big(\mathrm{Init}\ \varphi(T_\ell)\big) \le k_\ell \le p-1$. By the uniqueness of p-adic expansions, the monomial $\mathrm{Init}(\varphi(T))$ uniquely determines each of the monomials $\mathrm{Init}(\varphi(T_\ell))$ ($\ell = 0, 1, 2, \ldots, e-1$), which in turn (by case (i)) uniquely determines each of the tableaux $T_0, T_1, \ldots, T_{e-1}$ and hence also T. This proves the Lemma in Case (ii). $\square$

For the remainder of Section 4, we replace K by the finite field F of order $q = p^e$.

LEMMA 9   (i) The syzygy ideal $\mathfrak{I} \subseteq F[\Lambda]$ satisfies $\mathrm{FFN}(q-1)$.
 (ii) $h^\dagger_{\mathfrak{I}}(q-1) = (h_{\mathfrak{I}}(p-1))^e$.

Proof: Let $R = F[\Lambda]$, and suppose $f(\Lambda) \in R_{q-1}$ vanishes on $G_{r,\nu}(F)$. Since $R_{q-1} = (\mathfrak{I}\cap R_{q-1}) \oplus \langle\mathcal{T}\rangle$ where $\langle\mathcal{T}\rangle$ is the F-span of $\mathcal{T}$, the set of standard tableaux of degree $q-1$, we may assume that $f \in \langle\mathcal{T}\rangle$ vanishes on $G_{r,\nu}(F)$. We must show that $f = 0$. By hypothesis, the polynomial $\widehat{f}(X) := f(\Phi(X)) \in F[X]$ vanishes on $F^{(r+1)\times(\nu+1)}$. Clearly $\deg_{X_{ij}}(\widehat{f}) \le \deg(f) = q-1$, and so by Lemma 4, $\widehat{f}(X)$ is the zero polynomial. If $f(\Lambda) \ne 0$, then let $T = \mathrm{Init}(f) \in \mathcal{T}$; then by Lemma 8(i) we have $\mathrm{Init}(\widehat{f}) = \mathrm{Init}\,\varphi(T) \ne 0$, a contradiction. Thus $f(\Lambda) = 0$ as required, and (i) follows.

By Lemma 2, we have $R^\dagger_{q-1} = (\mathfrak{I}\cap R^\dagger_{q-1}) + \langle\mathcal{T}'\rangle$ where $\mathcal{T}'$ is the set of all p-standard tableaux of degree $q-1$. We must show that this sum is direct. Accordingly, suppose $0 \ne f(\Lambda) \in \mathfrak{I}\cap\langle\mathcal{T}'\rangle$. By hypothesis, the polynomial

$\widehat{f}(X) := f(\Phi(X)) \in F[X]$ vanishes on $F^{(r+1)\times(\nu+1)}$. As above, this implies that $\widehat{f}(X) = 0$ and $f(\Lambda) = 0$, a contradiction. Thus $R^{\dagger}_{q-1} = (\mathfrak{I} \cap R^{\dagger}_{q-1}) \oplus \langle \mathcal{T}' \rangle$ and conclusion (ii) follows from Lemma 2. $\square$

LEMMA 10 Let $S = G_{r,\nu}(F) \subseteq PG(n, F)$ and let H be any hyperplane of $PG(n, F)$, $F = GF(q)$. Then $|H \cap S| \equiv 1 \mod q$.

Proof: (Due to A. E. Brouwer.) Let N_H be the number of incident point-line pairs (P, ℓ) such that $P \in S \smallsetminus H$ and $\ell \subseteq S$. For every point $P \in S$, the number of lines contained in S passing through P, equals $[(q^{r+1}-1)/(q-1)][(q^{\nu-r}-1)/(q-1)] \equiv 1 \mod q$. Thus $N_H \equiv |S \smallsetminus H| \mod q$. However, every line $\ell \subseteq S$ not contained in H, contains exactly q points of $S \smallsetminus H$, so that $N_H \equiv 0 \mod q$. Furthermore, $|S| = \prod_{i=0}^{r}[(q^{\nu-i+1}-1)/(q^{r-i+1}-1)] \equiv 1 \mod q$, so that $|S \cap H| = |S| - |S \smallsetminus H| \equiv 1 \mod q$. $\square$

Now Theorem 2 follows from Theorem 1 and Lemmas 3, 7, 8 and 10.

5 AUTOMORPHISMS OF MATRICES

Let $B \in K^{k\times\ell}$, the vector space of all $k \times \ell$ matrices over a field K. Let G be a group, and let $Perm(k)$ denote the group of all $k \times k$ permutation matrices. Consider a *permutation action* of G on B, i.e. a homomorphism $G \to Perm(k) \times Perm(\ell)$, $g \mapsto (\Pi_1(g), \Pi_2(g))$ such that

$$\Pi_1(g)B = B\Pi_2(g)$$

for all $g \in G$. In the special case that B is square and invertible, it is well known that Π_1 and Π_2 are equivalent linear representations (although not necessarily equivalent permutation representations). In this section we prove a natural generalisation of this fact, which was alluded to in [2], but not proven there.

Our intent is to show that the row and column spaces of B over K are naturally contragredient KG-modules (in general not isomorphic, as this author erroneously stated in [2]). In order to deal just with left KG-modules, we consider instead the column spaces

$$Col(B) = \{Bx : x \in K^{\ell\times 1}\} \le K^{k\times 1}, \qquad Col(B^\top) = \{B^\top y : y \in K^{k\times 1}\} \le K^{\ell\times 1}.$$

Since $\Pi_1(g)(Bx) = B(\Pi_2(g)x) \in Col(B)$, we see that $Col(B)$ is indeed a left KG-module via $v \mapsto \Pi_1(g)v$. Similarly, since $B^\top\Pi_1(g) = \Pi_2(g)B^\top$, $Col(B^\top)$ is a left KG-module via $w \mapsto \Pi_2(g)w$.

LEMMA 11 $Col(B^\top) \cong Col(B)^*$ as left KG-modules.

Proof: Choose $M_1 \in GL(k,K),\ M_2 \in GL(\ell,K)$ such that

$$M_1BM_2 = \begin{bmatrix} I_r & O_{r,\ell-r} \\ O_{k-r,r} & O_{k-r,\ell-r} \end{bmatrix}$$

where I_r is an identity matrix of size $r = \operatorname{rank}_K B$ and the O's consist of zeroes. Now

$$\big(M_1\Pi_1(g)M_1^{-1}\big)\big(M_1BM_2\big) = \big(M_1BM_2\big)\big(M_2^{-1}\Pi_2(g)M_2\big)$$

for all $g \in G$. From this it is easy to see that

$$M_1\Pi_1(g)M_1^{-1} = \begin{bmatrix} Q(g) & * \\ O & * \end{bmatrix}, \qquad M_2^{-1}\Pi_2(g)M_2 = \begin{bmatrix} Q(g) & O \\ * & * \end{bmatrix}$$

where $Q : G \to GL(r,K)$ is a homomorphism. Via $v \mapsto (M_1\Pi_1(g)M_1^{-1})v$, we have a left KG-module $Col(M_1B)$ isomorphic to $Col(B)$, and since

$$Col(M_1B) = Col(M_1BM_2) = \{(\underbrace{*,*,\cdots,*}_{r\ \text{times}},\underbrace{0,0,\cdots,0}_{k-r\ \text{times}})^\top\},$$

the associated matrix representation of degree r is explicitly given by Q. Similarly, via

$$w \;\mapsto\; (M_2^{-\top}\Pi_2(g)M_2^\top)w \;=\; (M_2\Pi_2(g)M_2^{-1})^{-\top}w \;=\; \begin{bmatrix} Q(g)^{-\top} & * \\ O & * \end{bmatrix} w\,,$$

$Col(M_2^\top B^\top)$ becomes a left KG-module isomorphic to $Col(B^\top)$. Again, $Col(M_2^\top B^\top) = Col(M_2^\top B^\top M_1^\top) = \{(*,*,\ldots,*,0,0,\ldots,0)^\top\}$ and so the associated matrix representation of degree r is given by $Q^{-\top}$. $\square$

REFERENCES

1. E. Arbarello, M. Cornalba, P. A. Griffiths and J. Harris, *Geometry of Algebraic Curves, Volume I,* Springer-Verlag, New York (1985).
2. A. Blokhuis and G. E. Moorhouse, Some p-ranks related to orthogonal spaces, *J. Algeb. Comb., 4:* 295–316 (1995).
3. A. E. Brouwer and H. A. Wilbrink, Block Designs, in *Handbook of Incidence Geometry, Buildings and Foundations,* ed. F. Buekenhout, pp.349–382, North-Holland, Amsterdam and New York (1995).
4. A. M. Cohen and R. H. Cushman, Gröbner bases and standard monomial theory, in *Computational Algebraic Geometry,* ed. F. Eyssette and A. Galligo, pp.41–60, Birkhäuser Boston (1993).
5. D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms,* Springer-Verlag, New York (1992).
6. J. M. Goethals and P. Delsarte, On a class of majority-logic decodable cyclic codes, *IEEE Trans. Inform. Theory, 14:* 182–188 (1968).
7. R. Hartshorne, *Algebraic Geometry,* Springer-Verlag, New York (1977).

8. W. V. D. Hodge and D. Pedoe, *Methods of Algebraic Geometry, Volume II*, Camb. Univ. Press, Cambridge (1952).
9. F. J. MacWilliams and H. B. Mann, On the p-rank of the design matrix of a difference set, *Inform. and Control, 12:* 474–489 (1968).
10. G. E. Moorhouse, Some p-ranks related to Hermitian varieties, to appear in *J. Stat. Plan. Inf.*
11. 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:* 122–129 (1969).
12. B. Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, Vienna (1993).
13. B. Sturmfels and N. White, Gröbner bases and invariant theory, *Adv. Math., 76:* 245–259 (1989).