

# Approaching Some Problems in Finite Geometry through Algebraic Geometry

G. Eric Moorhouse, University of Wyoming

**Abstract.** In the study of finite geometries one often requires knowledge the ranks of related (0,1)-incidence matrices. We describe some of the combinatorial questions in finite geometry for which formulas for these ranks are useful; and we describe methods from algebraic geometry that are useful in obtaining such rank formulas.

## 1. Motivation and Background

Here we recall the definitions of a few standard notions from finite geometry. Considering the audience for this presentation, many of whom are coding theorists, the coding-theoretic interpretations of our objects of study, and of our results, will occasionally be explicitly mentioned. For a more extensive summary description of the relevant definitions from finite geometry, see e.g. [9], [17], [32].

We denote by  $P^n(\mathbb{F}_q)$  the classical projective  $n$ -space over the finite field  $\mathbb{F}_q$  of order  $q$ , i.e. the incidence system formed by the subspaces of  $\mathbb{F}_q^{n+1}$ : the points, lines, planes, etc. being the subspaces of dimension 1, 2, 3, etc.; thus the vector  $(k+1)$ -subspaces of  $\mathbb{F}_q^{n+1}$  are the projective  $k$ -subspaces. In particular  $P^2(\mathbb{F}_q)$  denotes the classical (i.e. Desarguesian) projective plane of order  $q$ . Non-classical projective planes exist, but all projective spaces of dimension  $n \geq 3$  are classical.

An *ovoid in projective 3-space*  $P^3(\mathbb{F}_q)$  is a set of  $q^2 + 1$  points with no three collinear. Alternatively, one may consider a linear  $[n, 4]$ -code  $\mathcal{C}$  over  $\mathbb{F}_q$  such that the dual code  $\mathcal{C}^\perp$  has minimum weight  $\geq 4$ ; in this case  $n \leq q^2 + 1$ , and equality holds iff a generator matrix for  $\mathcal{C}$  has as its columns the points of an ovoid in  $P^3(\mathbb{F}_q)$ . For  $q$  odd, every ovoid is an elliptic quadric (Barlotti [2]; Panella [28]). For  $q$  even, the *known ovoids* are the elliptic quadrics and (for  $q = 2^{2e+1}$ ) the Suzuki-Tits ovoids.

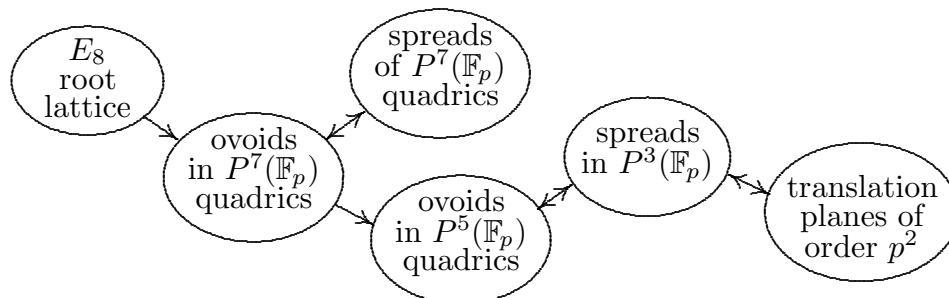
A *spread in*  $P^{2n-1}(\mathbb{F}_q)$  is a set  $\mathcal{S}$  consisting of  $q^n + 1$  projective  $(n-1)$ -subspaces which partition the points. These exist for all  $n \geq 1$  and prime powers  $q$ , and every such spread gives a plane (affine or projective) of order  $q^n$  known as a *translation plane*. This construction is responsible for most of the explicitly known finite projective planes.

An *orthogonal* (resp. *unitary*) *polar space* is the incidence system formed by the subspaces of projective space which lie on a given nondegenerate quadric (resp., Hermitian variety). A *symplectic polar space* is the incidence system formed by the totally isotropic subspaces of a projective space with respect to a nondegenerate alternating form. Let  $\mathcal{P}$  be

any *finite classical polar space* (i.e. a finite orthogonal, unitary or symplectic polar space). An *ovoid in  $\mathcal{P}$*  is a set  $\mathcal{O}$  consisting of points of  $\mathcal{O}$  such that every maximal subspace of  $\mathcal{P}$  contains exactly one point of  $\mathcal{O}$ . A *spread in  $\mathcal{P}$*  is a set  $\mathcal{S}$  consisting of maximal subspaces of  $\mathcal{P}$ , such that every point of  $\mathcal{P}$  lies in exactly one member of  $\mathcal{S}$ . These notions of ovoid and spread are distinct from (albeit related to) the notions of ovoid and spread for projective spaces. In the polar space setting, one has a bipartite incidence graph formed by incidences between points and maximal subspaces. Whenever one has a bipartite graph with partition  $A \cup B$  of the vertices (and every edge of the graph has one end in  $A$  and the other in  $B$ ) then one may ask for a subset  $\mathcal{O} \subseteq A$  such that every vertex in  $B$  is adjacent to exactly one member of  $\mathcal{O}$ ; or a subset  $\mathcal{S} \subseteq B$  such that every vertex in  $A$  is adjacent to exactly one member of  $\mathcal{S}$ . At this level of abstraction we see that ovoids and spreads are very similar notions.

Questions of existence and possible constructions of ovoids and spreads in the finite classical polar spaces are in many cases open; for an almost-current survey see [18, pp.345–348]. Ovoids of polar spaces are most intensively studied in the orthogonal case. If  $\mathcal{Q}$  is a nondegenerate quadric in  $P^{2n-1}(\mathbb{F}_q)$  then  $\mathcal{Q}$  is *hyperbolic* or *elliptic* according as maximal subspaces lying in the quadric have projective dimension  $n-1$  or  $n-2$ . In the hyperbolic case an ovoid in  $\mathcal{Q}$  (defined as above) is simply a set  $\mathcal{O}$  consisting of  $q^{n-1}+1$  points of  $\mathcal{Q}$ , no two on a line of the quadric. It is known [33] that ovoids do not exist in the elliptic case for  $n \geq 5$ ; and [15] that no ovoids exist in nondegenerate quadrics of  $P^{2n}(\mathbb{F}_q)$  (the *parabolic* case) for  $n \geq 4$ .

There are many connections between the various notions of spreads, ovoids, and other objects. The following sample of such connections is not exhaustive but is intended to hint at the central role played by these notions in finite geometry: Spreads of projective 3-space are equivalent to ovoids in the Klein quadric (i.e. the hyperbolic quadric in projective 5-space) via the Klein correspondence (the Plücker map). Ovoids and spreads in higher-dimensional spaces often give ovoids and spreads in lower-dimensional spaces, by a simple process of ‘slicing’. The  $E_8$  root lattice gives rise to numerous constructions (see [12], [23], [24], [26]) of ovoids in the hyperbolic quadric in projective 7-space, and these are in turn equivalent to spreads of the same quadric. In particular the following connections arise:



The most significant open question in this area is the question of whether there exist ovoids in nondegenerate quadrics in  $P^n(\mathbb{F}_q)$  for  $n > 7$ . Ovoids in higher dimensions would give rise to significant numbers of ovoids in dimensions 5 and 7, which seems unlikely; yet no proof of impossibility is known. One may be tempted to mimic the construction of ovoids from the  $E_8$  root lattice, using the Leech lattice to produce ovoids in quadrics in  $P^{23}(\mathbb{F}_p)$ ; however this approach cannot succeed for primes  $p < 59$  by virtue of Corollary 4.2 below. Such nonexistence results for ovoids motivated our interest in the  $p$ -rank formulas of Section 4.

Another motivation for our work is the desire to better understand the following striking parallel between different spaces admitting ovoids.

**1.1 Ovoids in  $P^3(\mathbb{F}_q)$ ,  $q = 2^r$ .** Here the known ovoids belong to two infinite families, each admitting a doubly transitive subgroup of  $PGL(4, q)$ : the elliptic quadrics (for all  $q$  even, stabilized by  $PSL(3, q)$ ) and the Suzuki-Tits ovoids (for  $q = 2^{2e+1}$  only, admitting the Suzuki group  ${}^2B_2(q)$ ). The binary code spanned by the (characteristic vectors of the) planes of  $P^3(\mathbb{F}_q)$  has dimension  $q^2+1$  (only for  $q$  even), and the tangent planes to any ovoid form a basis for the code.

**1.2 Ovoids in hyperbolic quadrics in  $P^7(\mathbb{F}_q)$ ,  $q = 2^r$ .** Aside from one known sporadic example for  $q = 8$  (Dye's ovoid; see [19]) just two infinite families of ovoids are known, each admitting a doubly transitive subgroup of  $P\Omega^+(8, q)$ : one family (for all  $q$  even) stabilized by  $PSL(3, q)$ , and the other (for  $q = 2^{2e+1}$  only) admitting  $PSU(3, q)$ . The binary code spanned by the (characteristic vectors of the) tangent hyperplanes to the quadric has dimension  $q^3+1$  (only for  $q$  even), and the tangent hyperplanes to any ovoid form a basis for the code.

**1.3 Ovoids in nondegenerate (parabolic) quadrics in  $P^6(\mathbb{F}_q)$ ,  $q = 3^r$ .** Here the known ovoids belong to two infinite families, each admitting a doubly transitive subgroup of  $P\Omega(7, q)$ : one family (for all  $q = 3^r$ ) stabilized by  $PSU(3, q)$ , and the Ree-Tits ovoids (for  $q = 3^{2e+1}$  only) admitting the Ree group  ${}^2G_2(q)$ . The ternary code spanned by the (characteristic vectors of the) tangent hyperplanes to the quadric has dimension  $q^3+1$  (only for  $q = 3^r$ ), and the tangent hyperplanes to any ovoid form a basis for the code.

Without the  $p$ -rank formulas of Section 4 this analogy is not complete. One may hope to use the tightness of the  $p$ -rank bound in each case to classify ovoids in each situation, or to look to the recent literature on case 1.1 (for example Brown [6], [7]) in the hopes of finding techniques that may apply also to cases 1.2 and 1.3.

## 2. $p$ -Ranks Related to Projective Spaces

Let  $A$  be the  $(0, 1)$ -incidence matrix of a finite point-block incidence structure, i.e. the matrix having rows indexed by points and columns indexed by blocks, and with entries 0

and 1 corresponding to non-incident and incident point-block pairs, respectively. By the  $p$ -rank of the incidence structure, we mean the rank of  $A$  over a field of characteristic  $p$ . It has long been known (see [13], [20], [31]) that the symmetric design of points and hyperplanes of  $P^n(\mathbb{F}_q)$  has  $p$ -rank equal to

$$\binom{p+n-1}{n}^r + 1$$

where  $q = p^r$ . The binomial coefficient appearing in the latter formula is in fact the coefficient of  $t^{p-1}$  in the binomial series

$$\frac{1}{(1-t)^{n+1}} = 1 + \binom{n+1}{1}t + \binom{n+2}{2}t^2 + \dots + \binom{n+p-1}{p-1}t^{p-1} + \dots$$

which arises as the Hilbert series for projective  $n$ -space. More explanation of the connection between  $p$ -ranks and Hilbert series is given in Section 3. Stronger information is in fact available: Black and List [3] give the Smith normal form of the point-hyperplane incidence matrix, although here we omit the details.

More generally, one may ask for the  $p$ -rank the design of points versus projective  $(n-k)$ -subspaces of  $P^n(\mathbb{F}_q)$  where  $q = p^r$ ; that is, the dimension of the linear code  $\mathcal{C} = \mathcal{C}(n, k, p^r)$  spanned over  $\mathbb{F}_p$  by the (characteristic vectors) of the projective subspaces of  $P^n(\mathbb{F}_q)$  of codimension  $k$ . The first formula available for this is that of Hamada [16]; see also [5, p.366]. Unfortunately the computational time required to evaluate Hamada's formula can be prohibitive, even for rather modest values of the input parameters. Fortunately however,  $\dim \mathcal{C}$  can be computed quite easily using the information implicit in [1], where the structure of the code as an  $\mathbb{F}_q G$ -module for the group  $G = PGL(n+1, \mathbb{F}_q)$  is given. We have

$$\dim \mathcal{C}(n, k, p^r) = 1 + (\text{coeff. of } t^r \text{ in } \text{tr}[(I - tM)^{-1}])$$

where  $M$  is the  $k \times k$  matrix with  $(i, j)$ -entry equal to the coefficient of  $t^{p^i-j}$  in  $(1+t+t^2+\dots+t^{p-1})^{n+1}$ . For example the following Maple<sup>TM</sup> code [21] determines the dimension of the  $\mathbb{F}_5$ -code spanned by lines of  $P^3(\mathbb{F}_{5^r})$ :

```
> with(linalg):
> p:=5: n:=3: k:=2:
> S:=simplify(((1-t^p)/(1-t))^(n+1)):
> M:=array(1..k,1..k):
> for i from 1 to k do
>   for j from 1 to k do
>     M[i,j]:=coeff(S,t,p*j-i):
>   od:
> od:
> print(M);
```

$$\begin{bmatrix} 35 & 80 \\ 20 & 85 \end{bmatrix}$$

```
> simplify(trace(inverse(&*(t)-t*M)));
```

$$-\frac{2(60t - 1)}{1375t^2 - 120t + 1}$$

```
> series(%,t=0,6);
```

$$2 + 120t + 11650t^2 + 1233000t^3 + 131941250t^4 + 14137575000t^5 + O(t^6)$$

Thus the dimension of the code spanned by the lines of  $P^3(\mathbb{F}_{5^r})$  is

$$120, 11650, 1233000, 131941250, 14137575000, \dots$$

for  $r = 1, 2, 3, \dots$

Again, even stronger information is available [10] from the Smith normal form of the incidence matrix of points versus projective  $(n-k)$ -subspaces.

### 3. $p$ -Ranks Via the Hilbert Function

Consider the  $\mathbb{F}_q$ -linear code  $\hat{\mathcal{C}}$  of length  $N = (q^{n+1}-1)/(q-1)$  spanned by the (characteristic vectors of the) hyperplanes of  $P^n(\mathbb{F}_q)$  where  $q = p^r$ . The subcode  $\mathcal{C} \subset \hat{\mathcal{C}}$  spanned by the *complements* of the hyperplanes has dimension  $\binom{p+n-1}{n}^r$ , while  $\hat{\mathcal{C}}$  itself has dimension  $\binom{p+n-1}{n}^r + 1$ . Now let  $\mathcal{V}$  be a subset of the points of  $P^n(\mathbb{F}_q)$ . Denote by  $\hat{\mathcal{C}}_{\mathcal{V}}$  and  $\mathcal{C}_{\mathcal{V}}$  the punctured codes of length  $|\mathcal{V}|$  obtained by simply restricting  $\hat{\mathcal{C}}$  and  $\mathcal{C}$  (respectively) to the coordinate positions indexed by  $\mathcal{V}$ . We are interested in general methods for determining the dimensions of  $\hat{\mathcal{C}}_{\mathcal{V}}$  and  $\mathcal{C}_{\mathcal{V}}$ . We note that  $\mathcal{C}_{\mathcal{V}} \subseteq \hat{\mathcal{C}}_{\mathcal{V}}$  is a subcode of codimension at most 1, and in many cases of interest (see Theorem 3.5 below) the exact codimension is 1. So for now we focus attention on  $\mathcal{C}_{\mathcal{V}}$ . We are most interested in the case of a point set  $\mathcal{V}$  arising as the set of  $\mathbb{F}_q$ -rational points of a projective variety. We establish notation to describe this case.

Consider the polynomial ring  $R = \mathbb{F}_q[X_0, X_1, \dots, X_n] = \bigoplus_{d \geq 0} R_d$  where  $R_d$  is the  $d$ -homogeneous part of  $R$  with respect to the standard degree grading. Let  $I \subseteq R$  be a homogeneous ideal, and let  $\mathcal{V}$  be the set of  $\mathbb{F}_q$ -rational points of projective  $n$ -space where  $I$  vanishes; thus  $\mathcal{V} = \mathcal{V}(I + J)$  is the zero set of the ideal  $I + J$  where  $J$  is generated by the polynomials  $X_i^q X_j - X_i X_j^q$  for  $0 \leq i < j \leq n$ . Let  $\mathcal{I} = \mathcal{I}(\mathcal{V}) \subseteq R$  be the ideal generated by all homogeneous polynomials vanishing on  $\mathcal{V}$ ; this is just the radical ideal  $\mathcal{I} = \sqrt{I + J}$ . We denote the Hilbert function of  $\mathcal{I}$  by  $h_{\mathcal{I}}(d) = \dim(R_d/\mathcal{I}_d)$  where  $\mathcal{I}_d = \mathcal{I} \cap R_d$ . Denote by  $LM(\mathcal{I})$  the set of leading monomials in  $\mathcal{I}$  with respect to some fixed monomial ordering. A monomial in  $R$  is *standard* if it is *not* in  $\mathcal{I}$ . Then  $h_{\mathcal{I}}(d)$  is the number of standard monomials of degree  $d$ . For simplicity we consider first the special case  $q = p$ .

**3.1 Theorem** [27]. *If  $q = p$  then  $\dim(\mathcal{C}_V) = h_{\mathcal{I}}(p - 1)$ .*

**3.2 Computational Example.** Consider the incidence system of points of the cubic surface  $x^3 + y^3 + z^2w = 0$  in  $P^3(\mathbb{F}_{11})$  versus all hyperplanes of the projective space. Using Macaulay 2 [14] we compute

```

i1 : p = 13;
i2 : F = ZZ/(p);
i3 : R = F[x,y,z,w];
i4 : S = (s,t)->s^p*t-s*t^p;
i5 : J = ideal(S(x,y),S(x,z),S(x,w),S(y,z),S(y,w),S(z,w));
o5 : Ideal of R
i6 : I = ideal(x^3+y^3+z^2*w)+J;
o6 : Ideal of R
i7 : II = radical(I);
o7 : Ideal of R
i8 : hilbertSeries(I)
o8 = 
$$\frac{1 - T^3 - 6T^{14} + 4T^{15} - T^{16} + 6T^{17} - 4T^{18} + T^{19} + 2T^{26} + \dots + 2T^{33}}{(1 - T)^4}$$

o8 : Divide
i9 : hilbertSeries(II)
o9 = 
$$\frac{1 - T^3 - 2T^{10} - 4T^{11} + T^{12} + 9T^{13} - 3T^{14} + 2T^{15} - T^{16} - 2T^{17}}{(1 - T)^4}$$

o9 : Divide
i10 : hilbertSeries(II, Order=>p)
o10 = 
$$1 + 4T + 10T^2 + 19T^3 + 31T^4 + 46T^5 + 64T^6 + \dots + 187T^{11} + 200T^{12}$$

o10 : ZZ [T, MonomialOrder => RevLex, Inverses => true]

```

From the coefficient of  $T^{p-1}$  we see that  $\dim(\mathcal{C}_V) = 200$ , and so  $\dim(\hat{\mathcal{C}}_V) = 201$  by Theorem 3.5 below. The most time-consuming step in this example (the computation of the radical ideal) requires at most a few seconds on a typical personal computer, but in other examples this step may overwhelm the computational resources of the machine. In such cases one might try to explicitly determine the radical by other means; or it may be necessary to determine the required  $p$ -rank by Gaussian elimination. For example we check independently that the above cubic surface has 209 points, and that the  $209 \times 2380$  incidence matrix of points versus hyperplanes has 13-rank equal to 201.

Now consider the general case  $q = p^r$ ,  $r \geq 1$ . We define a  $p$ -standard monomial to be a monomial of the form  $m_0 m_1^p m_2^{p^2} \dots$ , a finite product in which each  $m_i$  is a standard monomial of degree less than  $p$ . (This definition is not standard; sorry, no pun intended!) Denote by  $h_{\mathcal{I}}^{\dagger}(d)$  the number of  $p$ -standard monomials of degree  $d$ .

**3.3 Theorem** [27].  $\dim(\mathcal{C}_{\mathcal{V}}) = h_{\mathcal{I}}^{\dagger}(q-1)$ .

This requires us to count the number of monomials of the form  $m_0 m_1^p m_2^{p^2} \cdots m_{r-1}^{p^{r-1}}$  where each  $m_i$  is a standard monomial of degree  $p-1$ .

**3.4 Example: Projective  $n$ -Space.** Let  $I = 0$ , so that  $\mathcal{I} = 0$  and  $\mathcal{V}$  consists of all  $(q^{n+1} - 1)/(q - 1)$  points of  $P^n(\mathbb{F}_q)$ . Every monomial is standard, and the  $p$ -standard monomials are those of the form  $m_0 m_1^p m_2^{p^2} \cdots m_{r-1}^{p^{r-1}}$  where each monomial  $m_i$  has degree  $p-1$ . There are  $\binom{p+n-1}{n}$  choices for each  $m_i$ , and hence the number of  $p$ -standard monomials of degree  $q-1$  is  $h_{\mathcal{I}}^{\dagger}(q-1) = \binom{p+n-1}{n}^r$ . This gives the well-known value for  $\dim(\mathcal{C}_{\mathcal{V}})$ ; and the value  $\dim(\hat{\mathcal{C}}_{\mathcal{V}}) = 1 + \dim(\mathcal{C}_{\mathcal{V}})$  may be seen as a special case of the following (for a vacuous set of  $k = 0$  polynomials).

**3.5 Theorem.** Let  $f_1, \dots, f_k \in R$  be nonconstant homogeneous polynomials of total degree  $\sum_i \deg(f_i) \leq n - 2$ , and let  $\mathcal{V}$  be the set of all points in  $P^n(\mathbb{F}_q)$  where every  $f_i$  vanishes. Then  $\dim(\hat{\mathcal{C}}_{\mathcal{V}}/\mathcal{C}_{\mathcal{V}}) = 1$ .

*Proof.* Let  $M$  be the number of vectors in  $\mathbb{F}_q^{n+1}$  where all  $f_1, \dots, f_k$  vanish. Since the total degree  $\sum_i \deg(f_i) < n$ , the Chevalley-Warning Theorem [30, p.5] shows that  $p$  divides  $M$ . But the homogeneity of  $f_1, \dots, f_k$  means that  $q-1$  divides  $M-1$ , so in fact  $M = mp(q-1) + q$  for some  $m \geq 0$ . Thus  $|\mathcal{V}| = (M-1)/(q-1) = mp + 1 \equiv 1 \pmod{p}$ .

Now let  $h \in R_1$  be a nonzero homogeneous linear polynomial, and let  $M_h$  be the number of vectors in  $\mathbb{F}_q^{n+1}$  where all  $k+1$  of the polynomials  $f_1, f_2, \dots, f_k, h$  vanish. Since the total degree again satisfies  $1 + \sum_i \deg(f_i) \leq n-1$ , the previous argument also shows that  $M_h = m_h p(q-1) + q$  for some  $m_h \geq 0$ . Thus  $|H \cap \mathcal{V}| = m_h p + 1 \equiv 1 \pmod{p}$  where  $H$  is the hyperplane of  $P^n(\mathbb{F}_q)$  consisting of all points where  $h$  vanishes.

Since  $\dim(\hat{\mathcal{C}}/\mathcal{C}) = 1$ , it suffices to find a nonzero linear functional  $\phi : \hat{\mathcal{C}}_{\mathcal{V}} \rightarrow \mathbb{F}_p$  vanishing on  $\mathcal{C}_{\mathcal{V}}$ . For  $v \in \hat{\mathcal{C}}_{\mathcal{V}}$ , define  $\phi(v)$  to be simply the sum of the coordinate entries of  $v$ . In case  $v$  is the characteristic vector of a hyperplane  $H$  (restricted to  $\mathcal{V}$ ), we have  $\phi(v) = |H \cap \mathcal{V}| \equiv 1 \pmod{p}$ . Similarly if  $v$  is the characteristic vector of the complement of a hyperplane  $H$ , then  $\phi(v) = |\mathcal{V}| - |H \cap \mathcal{V}| \equiv 1 - 1 \equiv 0 \pmod{p}$ . Since we have considered typical generators for the codes  $\hat{\mathcal{C}}_{\mathcal{V}}$  and  $\mathcal{C}_{\mathcal{V}}$ , our  $\phi$  has the required properties and the conclusion follows.  $\square$

## 4. $p$ -Ranks Related to Polar Spaces and Grassmannians

We survey some interesting  $p$ -rank formulas and some applications to bounds for ovoids. Each  $p$ -rank formula listed here is derived either by the approach described in Section 3, or from the theory of group representations. Our notation  $q, p, n, R, J, \mathcal{C}_{\mathcal{V}}$ , etc. is the same as in Section 3.

**4.1 Theorem** [4]. *Let  $I = (Q)$  where  $Q(X_0, X_1, \dots, X_n) \in R_2$  is an irreducible quadratic form, and let  $\mathcal{Q} = \mathcal{V}(I + J)$  be the resulting quadric in  $P^n(\mathbb{F}_q)$ . Let  $\hat{\mathcal{C}}_{\mathcal{Q}}$  be the  $\mathbb{F}_q$ -linear code of length  $|\mathcal{Q}|$  spanned by the hyperplane sections of the quadric. Then*

$$\dim(\hat{\mathcal{C}}(\mathcal{Q})) = \left[ \binom{p+n-1}{n} - \binom{p+n-3}{n} \right]^r + 1.$$

If a nondegenerate quadric  $\mathcal{Q}$  in  $P^n(\mathbb{F}_q)$  admits an ovoid  $\mathcal{O}$  then the tangent hyperplanes to  $\mathcal{Q}$  at the points of  $\mathcal{O}$  span a subcode of  $\hat{\mathcal{C}}_{\mathcal{Q}}$  of dimension  $p^{\lfloor n/2 \rfloor r} + 1$ . This gives

**4.2 Corollary** [4]. *There do not exist ovoids in  $\mathcal{Q}$  (using the notation of Theorem 4.1) if*

$$p^{\lfloor n/2 \rfloor} > \binom{p+n-1}{n} - \binom{p+n-3}{n}.$$

*In particular ovoids do not exist in  $\mathcal{Q}$  for  $n = 9$  and  $p = 2, 3$ ; or for  $n = 11$  and  $p = 2, 3, 5, 7$ .*

In studying finite projective planes, it is often useful to have an explicit basis for the  $\mathbb{F}_p$ -linear code spanned by the lines. In the case of classical (Desarguesian) planes  $P^2(\mathbb{F}_p)$ , this code has dimension  $\binom{p+1}{2} + 1$  and so it had long been speculated that an explicit basis could be formed from any conic (which has  $p + 1$  points). This follows also from our approach to  $p$ -ranks:

**4.3 Corollary** [4]. *Let  $\hat{\mathcal{C}}$  be the  $\mathbb{F}_p$ -linear code spanned by the lines of  $P^2(\mathbb{F}_p)$ , so that  $\dim(\hat{\mathcal{C}}) = \binom{p+1}{2} + 1$ . Let  $\mathcal{C} \subset \hat{\mathcal{C}}$  be the subcode of dimension  $\binom{p+1}{2}$  spanned by the complements of the lines. Let  $\mathcal{Q}$  be any conic in the plane, so that  $\mathcal{Q}$  has  $p+1$  tangent lines,  $\binom{p+1}{2}$  secant lines, and  $\binom{p}{2}$  passant lines (i.e. lines not meeting  $\mathcal{Q}$ ). Then the complements to the secants form a basis for  $\mathcal{C}$ . Moreover the tangents and the passants together form a basis for  $\hat{\mathcal{C}}$ .*

We remark in passing that another choice of explicit basis is found in [22].

**4.4 Theorem** [25]. *Suppose  $q = q_0^2 = p^r$  ( $r$  even) and let  $I = (U)$  where  $U \in R_{q_0+1}$  is a nondegenerate unitary form; we may choose coordinates so that  $U(X_0, X_1, \dots, X_n) = X_0^{q_0+1} + X_1^{q_0+1} + \dots + X_n^{q_0+1}$ . Let  $\mathcal{H} = \mathcal{V}(I + J)$  be the resulting hermitian variety in  $P^n(\mathbb{F}_q)$ . Let  $\hat{\mathcal{C}}_{\mathcal{H}}$  be the  $\mathbb{F}_q$ -linear code of length  $|\mathcal{H}|$  spanned by the hyperplane sections of  $\mathcal{H}$ . Then*

$$\dim(\hat{\mathcal{C}}_{\mathcal{H}}) = \left[ \binom{p+n-1}{n}^2 - \binom{p+n-2}{n}^2 \right]^{r/2} + 1.$$

Bounds for ovoids in unitary polar spaces, similar to those of Theorem 4.1 and Corollary 4.2, are obtained [25] using Theorem 4.4.

**4.5 Theorem.** *Let  $\mathcal{Q}$  be a nondegenerate (parabolic) quadric in  $P^4(\mathbb{F}_q)$ , and consider the incidence system of points of  $P^4(\mathbb{F}_q)$  versus lines of  $\mathcal{Q}$ . The  $p$ -rank of this incidence system is*

- (a) (for  $q = 2^r$ )  $1 + \left(\frac{1+\sqrt{17}}{2}\right)^{2r} + \left(\frac{1-\sqrt{17}}{2}\right)^{2r}$ ;
- (b) (for  $q = p$ )  $1 + \frac{p(p+1)^2}{2}$ ;
- (c) (for  $q = p^r$ )  $1 + \alpha_+^r + \alpha_-^r$  where  $\alpha_{\pm} = \frac{p(p+1)^2}{4} \pm \frac{p(p^2-1)}{12}\sqrt{17}$ .

The incidence system of Theorem 4.5 is a classical generalized quadrangle of order  $(q, q)$ ; and it immediately follows that the dual generalized quadrangle also has  $p$ -rank as given by Theorem 4.5. This dual generalized quadrangle is the symplectic polar space in  $P^3(\mathbb{F}_q)$  formed by a nondegenerate alternating form. Proofs of (a) and (c), using representation theory, appear in [29] and [11]; and in the prime case (b) a proof appears in [8] using methods from Section 3.

In the following, we embed the collection of all projective  $s$ -subspaces of  $P^m(\mathbb{F}_q)$  in  $P^n(\mathbb{F}_q)$  via the Plücker embedding, where  $n = \binom{m+1}{s+1} - 1$ . The image of this embedding is the set  $\mathcal{G}_s^n(\mathbb{F}_q)$  of  $\mathbb{F}_q$ -rational points of the Grassmann variety  $\mathcal{G}_s^n$ . Recall that  $\mathcal{G}_s^n = \mathcal{V}(I)$  where the ideal  $I \subset R$  is generated by certain homogeneous polynomials of degree 2 (the van der Waerden syzygies). The Hilbert function for this variety is known:

$$h_I(d) = \prod_{0 \leq j \leq s} \frac{(m+d-s+j)! j!}{(m-s+j)! (d+j)!}.$$

**4.6 Theorem.** *Let  $\mathcal{G} = \mathcal{G}_s^n(\mathbb{F}_q) = \mathcal{V}(I + J)$  be the set of  $\mathbb{F}_q$ -rational points of the Grassmann variety, with  $n, I, h_I$  as above, and let  $\hat{\mathcal{C}}_{\mathcal{G}}$  be the  $\mathbb{F}_q$ -linear code of length  $|\mathcal{G}| = \binom{n+1}{s+1}_q$  spanned by the hyperplane sections of  $\mathcal{G}$ . Then*

$$\dim(\hat{\mathcal{C}}_{\mathcal{G}}) = h_I(p-1)^r + 1$$

with  $h_I(d)$  as above.

Note that the Grassmann variety  $\mathcal{G}_1^3(\mathbb{F}_q)$  is in fact the Klein quadric, i.e. the hyperbolic quadric in  $P^5(\mathbb{F}_q)$ ; in this case the dimension of the code  $\hat{\mathcal{C}}_{\mathcal{G}}$  is

$$\left[ \frac{1}{12} p(p+1)^2(p+2) \right]^r + 1,$$

as given by either Theorem 4.1 or 4.6.

## 5. References

- [1] M. Bardoe and P. Sin, ‘The permutation modules for  $\mathrm{GL}(n+1, \mathbb{F}_q)$  acting on  $P^n(\mathbb{F}_q)$  and  $\mathbb{F}_q^{n+1}$ ’, *J. London Math. Soc.* **61** (2000), 58–80.

- [2] A. Barlotti, ‘Un’estensione del teorema di Segre-Kustaanheimo’, *Bull. Un. Mat. Ital.* **10** (1955), 498–506.
- [3] S.C. Black and R.J. List, ‘On certain abelian groups associated with finite projective geometries’, *Geom. Dedicata* **33** (1990), 13–19.
- [4] A. Blokhuis and G.E. Moorhouse, ‘Some  $p$ -ranks related to orthogonal spaces’, *J. Algebraic Combinatorics* **4** (1995), 295–316.
- [5] A.E. Brouwer and H.E. Wilbrink, ‘Block Designs’, in *Handbook of Incidence Geometry*, ed. F. Buekenhout, Elsevier, Amsterdam, 1995, pp.349–382.
- [6] M.R. Brown, ‘Ovoids of  $PG(3, q)$ ,  $q$  even, with a conic section’, *J. London Math. Soc.* **62** (2000), 569–582.
- [7] M.R. Brown, ‘The determination of ovoids of  $PG(3, q)$  containing a pointed conic’, *J. Geom.* **67** (2000), 61–72.
- [8] D. de Caen and G.E. Moorhouse, ‘The  $p$ -rank of the  $Sp(4, p)$  Generalized Quadrangle’, preprint, 2000. Available at <http://www.uwo.edu/moorhouse/pub/sp4p.pdf>
- [9] P.J. Cameron, ‘Finite Geometries’, in *Handbook of Combinatorics*, ed. R. Graham et. al., Elsevier, Amsterdam, 1995, pp.647–691.
- [10] D.B. Chandler, P. Sin and Q. Xiang, ‘The invariant factors of the incidence matrices of points and subspaces in  $PG(n, q)$  and  $AG(n, q)$ ’, *Trans. Amer. Math. Soc.* **358** (2006), 4935–4957.
- [11] D.B. Chandler, P. Sin and Q. Xiang, ‘The permutation action of finite symplectic groups of odd characteristic on their standard modules’ preprint, 2006.
- [12] J.H. Conway, P.B. Kleidman and R.A. Wilson, ‘New families of ovoids in  $O_8^+$ ’, *Geom. Dedicata* **26** (1988), 157–170.
- [13] J.M. Goethals and P. Delsarte, ‘On a class of majority-logic decodable cyclic codes’, *IEEE Trans. Inform. Theory* **14** (1968), 182–188.
- [14] D.R. Grayson and M.E. Stillman, *Macaulay 2, a software system for research in algebraic geometry*. Available at <http://www.math.uiuc.edu/Macaulay2/>
- [15] A. Gunawardena and G.E. Moorhouse, ‘The non-existence of ovoids in  $O_9(q)$ ’, *Europ. J. Combinatorics* **18** (1997), 171–173.
- [16] N. Hamada, ‘The rank of the incidence matrix of points and  $d$ -flats in finite geometries’, *J. Sci. Hiroshima Univ. Ser. A-I Math.* **32** (1968), 381–396.
- [17] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd ed., Oxford Univ. Press, Oxford, 1998.
- [18] J.W.P. Hirschfeld and J.A. Thas, *General Galois Geometries*, Oxford Univ. Press, Oxford, 1991.
- [19] W.M Kantor, ‘Ovoids and translation planes’, *Canad. J. Math.* **24** (1982), 1195–1207.
- [20] 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.

- [21] M.B. Monagan et. al., *Maple 10 Programming Guide*, Maplesoft, Waterloo, Canada, 2005.
- [22] G.E. Moorhouse, ‘Bruck nets, codes, and characters of loops’, *Designs, Codes and Cryptography* **1** (1991), 7–29.
- [23] G.E. Moorhouse, ‘Ovoids from the  $E_8$  root lattice’, *Geom. Dedicata* **46** (1993), 287–297.
- [24] G.E. Moorhouse, ‘Root lattice constructions of ovoids’, in *Finite Geometry and Combinatorics*, ed. F. De Clerck et. al., pp.269–275, Camb. Univ. Press, Cambridge (1993).
- [25] G.E. Moorhouse, ‘Some  $p$ -ranks related to Hermitian varieties’, *J. Stat. Plan. Inf.* **56** (1996), 229–241.
- [26] G.E. Moorhouse, ‘Ovoids and translation planes from lattices’, in *Mostly Finite Geometries*, ed. N.L. Johnson; Marcel Dekker Inc., 1997, pp.123–134.
- [27] G.E. Moorhouse, ‘Some  $p$ -ranks related to finite geometric structures’, in *Mostly Finite Geometries*, ed. N. L. Johnson; Marcel Dekker Inc., 1997, pp.353–364.
- [28] G. Panella, ‘Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito’, *Bull. Un. Mat. Ital.* **10** (1955), 507–513.
- [29] N. Sastry and P. Sin, ‘The codes of generalized quadrangles of even order’, *Proceedings of the AMS Summer Research Institute on Group actions and Cohomology*, Seattle, 1996.
- [30] J.P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973.
- [31] K.J.C. Smith, ‘On the  $p$ -rank of the incidence matrix of points and hyperplanes in a finite projective geometry’, *J. Combin. Theory* **1** (1969), 122–129.
- [32] J.A. Thas, ‘Projective geometry over a finite field’, in *Handbook of Incidence Geometry*, ed. F. Buekenhout, Elsevier, Amsterdam, 1995, pp.295–347.
- [33] J.A. Thas, ‘Ovoids and spreads of finite classical polar spaces’, *Geom. Dedicata* **10** (1981), 135–144.