TRANSLATION PLANES AND DERIVATION SETS

By

E.F. Assmus, Jr.

and

J.D. Key

IMA Preprint Series # 481

February 1989

TRANSLATION PLANES AND DERIVATION SETS*

E.F. ASSMUS, JR.† AND J.D. KEY‡

Abstract. Using ideas from algebraic coding theory, a general notion of a *derivation set* for a projective plane is introduced. Certain geometric codes are used to locate such sets. These codes also lead to upper bounds for the p-ranks of incidence matrices of translation planes in terms of the dimensions of the associated codes.

1. Introduction. The main purpose of this paper is to place the notion of a derivation set for a finite projective plane in a coding-theoretic setting. In doing so, we expand on a remark made in [1] concerning "generalized derivations" for translation planes. Although the notion of a derivation set is of a general nature, applying to any projective plane, its most frequent use has been in the construction of translation planes. We choose, therefore, to link these two topics, thus naturally introducing certain geometric codes. These codes then yield an upper bound for the p-rank of an incidence matrix of a translation plane—of order a power of p—in terms of the dimension of the associated geometric code.

In [17, Theorem 5] Ostrom defined a very general notion of derivation for projective planes but, perhaps precisely because of this generality, not a great deal seems to have been made of it to produce new planes. Indeed, most of the instances that the authors are aware of involve choosing a Baer segment of a line of a projective plane as a possible derivation set. The theory of projective planes proposed in [1], involving codes associated with the plane and its affine parts, leads naturally to a notion of a derivation set that is, on the one hand, more general than the one in current use, but, on the other hand, not as general as the one proposed by Ostrom. In fact, from our definition it follows that for a plane of order p^2, p a prime, the only possible non-trivial derivation sets *are* the Baer segments and that for planes of prime order, there are no non-trivial derivation sets at all. We hope, therefore, that some progress will be made using this approach.

Concerning bounds, we showed in [1] that the incidence matrix of any affine translation plane of order $q = p^s$, where p is a prime, has rank over $\mathbf{F}_p$ bounded above by $q^2 + q - \dim(B(\mathbf{F}_q|\mathbf{F}_p))$, where $B(\mathbf{F}_q|\mathbf{F}_p)$ is the code over $\mathbf{F}_p$ of the design of points and s-flats of the affine geometry $AG_{2s}(p)$. We can write this upper bound as $q + \dim(B(\mathbf{F}_q|\mathbf{F}_p)^{\perp})$. We show here (see Section 3, Theorem 2) that $B(\mathbf{F}_q|\mathbf{F}_p)^{\perp}$ is the code spanned by all vectors of the form $v^X - v^Y$, where X and Y are parallel s-flats and v^Z denotes the characteristic

*This research was supported in part by the Institute for Mathematics and its Applications with funds provided by the National Science Foundation.

†Department of Mathematics, Lehigh University, Bethlehem, PA 18015, U.S.A.

‡Department of Mathematical Sciences, Martin Hall, Clemson University, Clemson, SC 29634–1907, U.S.A.

function of a subset Z of points. Denoting this latter code by $E(\mathbf{F}_q|\mathbf{F}_p)$, this bound has a refinement for translation planes with "kern" (see [15]) a subfield F of $\mathbf{F}_q$, namely

$$q + \dim(E(\mathbf{F}_q|F)),$$

where here the generating vectors, $v^X - v^Y$, must have X and Y parallel s-flats coming from a subspace of V viewed as a vector space over F, rather than $\mathbf{F}_p$: see Section 3, Theorem 1. Thus, for example, the bound for $q = 16$ is 101, rather than 109, when the translation plane is "2-dimensional". All translation planes of order 16 are known (see [7]), and all the 2-ranks have been determined (see [16], or Section 3). The (affine) ranks lie between 81 (the desarguesian) and 105 (the Lorimer and the derived semi-field planes), with the 2-dimensional planes having rank 97. We do not, unfortunately, have any instances of planes meeting these new bounds, but if there were any such planes, they would all be linearly equivalent (see Section 2), just as in the case of dimension equal to $q + \dim(B(\mathbf{F}_q|\mathbf{F}_p)^\perp)$.

The formulae for the dimension of the spaces $B(\mathbf{F}_q|F)$ and $E(\mathbf{F}_q|F)$ given by Delsarte [5] and Hamada [8] (see also [1, Appendix I]) are difficult to work with. We quote a formula, due to Key and Mackenzie [12], for $\dim(B(\mathbf{F}_q|\mathbf{F}_p))$ that is easy to use, but we do not have an easy-to-use formula for $\dim(E(\mathbf{F}_q|F))$ in the general case.

2. Preliminaries. We will adhere to the notation of [1] which we now briefly review. Let Π be an arbitrary projective plane of order n, p a prime dividing n. Set $N = n^2+n+1$ and view $\mathbf{F}_p^N$ as the vector space of all functions from the point set of Π to the field $\mathbf{F}_p$. Let $C_p(\Pi)$ be the subspace of $\mathbf{F}_p^N$ generated by the characteristic functions of the lines of Π, $C_p(\Pi)^\perp$ the orthogonal to $C_p(\Pi)$ under the standard inner product, and set $B_p(\Pi) = C_p(\Pi) + C_p(\Pi)^\perp$. It is shown in [1] that $B_p(\Pi)$ has minimum weight $n+1$ and that the minimal-weight vectors are precisely the scalar multiples of the characteristic functions of the lines of Π.

If π is an affine plane of order n, and p a prime dividing n, we make analogous definitions: $B_p(\pi) = C_p(\pi) + C_p(\pi)^\perp$ where $C_p(\pi)$ is that subspace of $\mathbf{F}_p^{n^2}$ generated by the characteristic functions of the lines of π. From [1], $B_p(\pi)$ has minimum weight n, and its minimal-weight vectors are scalar multiples of the characteristic functions of certain subsets of points of π. Now, however, subsets of points other than lines yielding minimal-weight vectors may, and usually do, appear. If Π is the projective completion of π with L the line at infinity, we will write $\pi = \Pi^L$, and then $B_p(\pi)$ is the image of $B_p(\Pi)$ under the projection map that ignores the points of L. In the affine case, $B_p(\pi)^\perp$, called the hull of π and denoted by $\mathrm{Hull}_p(\pi)$, plays a significant role. We have $\mathrm{Hull}_p(\pi) = C_p(\pi) \cap C_p(\pi)^\perp$, and it is shown in [1] that $\mathrm{Hull}_p(\pi)$ is generated by vectors of the form $v^l - v^m$ where l and m are parallel lines and v^X denotes the vector in $\mathbf{F}_p^{n^2}$ that is the characteristic function of X. Here again, of course, we are viewing $\mathbf{F}_p^{n^2}$ as the vector space of all functions from the points of π to the field $\mathbf{F}_p$. From [1], $\dim(\mathrm{Hull}_p(\pi)) = \dim(C_p(\pi)) - n$.

Next let $q = p^s$, set $K = \mathbf{F}_q$, and view $V = K \oplus K$ as a $2s$-dimensional vector space over $\mathbf{F}_p$. Then $|V| = q^2$, and $\mathbf{F}_p^V$, the vector space of all functions from V to $\mathbf{F}_p$, is a

q^2-dimensional vector space over $\mathbf{F}_p$. Now, for any subfield F of K one can view V as a vector space over F. An s-dimensional flat of V (i.e. a coset of an s-dimensional subspace of V viewed as a vector space over $\mathbf{F}_p$) that is a coset of an F-subspace of V will, for convenience, be called an *F-flat*. Let $B(K|F)$ be that subspace of $\mathbf{F}_p^V$ generated by all v^X, X an F-flat. It is shown in [5] that $B(K|F)$ has minimum weight q and that its minimal-weight vectors are precisely the scalar multiples of its generating vectors v^X. We have a Galois correspondence between the subfields of K and the codes $B(K|F)$. Here, $B(K|K)$ is the smallest code and can be viewed as $C_p(AG_2(q))$, where $AG_2(q)$ denotes the desarguesian affine plane of order $q = p^s$. In [1] we show that an affine plane π of order $q = p^s$ is a translation plane if and only if $C_p(\pi)$ is isomorphic to a subcode C of $B(K|\mathbf{F}_p)$ for which, viewing C as $C_p(\pi)$,

$$\mathrm{Hull}_p(\pi) \subset C_p(\pi) \subseteq B(K|\mathbf{F}_p) \subseteq B_p(\pi).$$

It can happen, of course, that C could be taken to be in $B(K|F)$ for a subfield F of K (in the literature on translation planes one would say that π had "kern" F); when this happens we say that π is *contained* in the code $B(K|F)$. Then we have

$$\mathrm{Hull}_p(\pi) \subset C_p(\pi) \subseteq B(K|F) \subseteq B(K|\mathbf{F}_p) \subseteq B_p(\ pi).$$

The final notion we need from [1] is that of *linear equivalence*: if π_1 and π_2 are two affine planes of order n and p is a prime dividing n, then π_1 and π_2 are linearly equivalent (at p) if $\mathrm{Hull}_p(\pi_1)$ and $\mathrm{Hull}_p(\pi_2)$ are code-isomorphic.

Notation new to the present paper: $E(K|F)$ is that subspace of $F_p^{q^2}$ generated by the vectors of the form $v^X - v^Y$ where X and Y are parallel F-flats of V. Clearly $E(K|F) \subseteq B(K|F)$.

Note: we will omit the subscript "p" that appears, for example, in $C_p(\pi), \mathrm{Hull}_p(\pi)$ and $B_p(\pi)$, writing simply $C(\pi), \mathrm{Hull}(\pi)$ and $B(\pi)$, where p is understood to be a fixed prime dividing the order n of the plane. For translation planes, certainly, n is a power of p.

3. Bounds. In [1] we proved that any translation plane π of order $q = p^s$ satisfies

$$\dim(C(\pi)) \leq q^2 + q - \dim(B(\mathbf{F}_q|\mathbf{F}_p)).$$

Put another way, the p-rank of an incidence matrix of π is bounded above by $q^2 + q - \dim(B(\mathbf{F}_q|\mathbf{F}_p))$. Moreover, any two translation planes meeting this bound are linearly equivalent.

We prove here the following analogous result.

THEOREM 1. *Suppose π is a translation plane contained in $B(\mathbf{F}_q|F)$, where F is a subfield of $\mathbf{F}_q$. Then*

$$\dim(C(\pi)) \leq q + \dim(E(\mathbf{F}_q|F)).$$

Moreover, any two translation planes contained in $B(\mathbf{F}_q|F)$ and meeting this bound are linearly equivalent.

Proof. If $C(\pi)$ is isomorphic to $C \subseteq B(\mathbf{F}_q|F)$, then $\mathrm{Hull}(\pi)$ is isomorphic to a subcode H of $E(\mathbf{F}_q|F)$; this follows since $\mathrm{Hull}(\pi)$ is generated by vectors of the form $v^l - v^m$, where l and m are parallel lines of π, and, under the isomorphism of $C(\pi)$ onto C, v^l will correspond to a vector v^X that is a generator of $B(\mathbf{F}_q|F)$, these being the only (up to scalar multiples) weight-q vectors of $B(\mathbf{F}_q|F)$. Since $\dim(H) = \dim(\mathrm{Hull}(\pi)) = \dim(C(\pi)) - q$, the required inequality follows. Moreover, equality implies that $H = E(\mathbf{F}_q|F)$, and hence any two affine translation planes contained in $B(\mathbf{F}_q|F)$ and meeting the bound have hulls isomorphic to $E(\mathbf{F}_q|F)$, and hence are linearly equivalent.

In order to show that the bound is, in fact, the same as that of [1] for $F = \mathbf{F}_p$, we first determine $B(\mathbf{F}_q|\mathbf{F}_p)^\perp$. The following result is implicit in the work of Delsarte [5], but, for the convenience of the reader, we include a proof. Note that a neat proof, via the modular algebra approach to Reed-Muller codes, can be found in [4, Chapter 3].

THEOREM 2. $B(\mathbf{F}_q|\mathbf{F}_p)^\perp = E(\mathbf{F}_q|\mathbf{F}_p)$.

Proof. First of all, it is clear that the generators of $E(\mathbf{F}_q|F)$, for any subfield F of $\mathbf{F}_q$, are in $B(\mathbf{F}_q|\mathbf{F}_p)^\perp$, since an s-flat of V meets any two parallel s-flats in the same number of points modulo p; i.e. in one point of each flat of the parallel class when the corresponding subspaces have intersection $\{0\}$, and in the empty set, or a power of p points, otherwise. Thus $E(\mathbf{F}_q|\mathbf{F}_p) \subseteq B(\mathbf{F}_q|\mathbf{F}_p)^\perp$. To prove equality we will prove that the two dimensions are equal. We use the radix-p form of the dimensions of $E(\mathbf{F}_q|\mathbf{F}_p) = E$ and $B(\mathbf{F}_q|\mathbf{F}_p) = B$ as given by Delsarte [5]. There it is shown that, for $q = p^s$, the dimension of B is equal to the number of integers z with $1 \le z < p^{2s}$ that "contain", in the sense of Delsarte, s multiples of $(p-1)$, and that the dimension of E is equal to the number of integers z with $1 \le z < p^{2s}$ that "properly contain" s multiples of $(p-1)$. (In Delsarte's notation B is $C_{p-1}(1,1,\ldots,1)$ with s ones and E is $C_1(1,1,\ldots,1)$ with $s+1$ ones.) More generally, for the moment, let z be a positive integer with p-ary expansion

$$z = \sum_{i=0}^{\infty} a_i p^i,$$

where, of course, $0 \le a_i < p$ and almost all a_i are 0. For z to contain $(p-1)$ k times we must be able to write $a_i = a_i^{(1)} + \cdots + a_i^{(k)}$ with $0 \le a_i^{(j)} < p$ for all i and j in such a manner that there are positive integers $m_1, \ldots, m_k$ with $m_j(p-1) = \sum_{i=0}^{\infty} b_i^{(j)} p^i$ and $b_i^{(j)} \le a_i^{(j)}$ for all i and j. Now, by a "casting out nines" argument, an integer $x = \sum_{i=0}^{\infty} x_i p^i$

is divisible by $(p-1)$ if and only if $\sum_{i=0}^{\infty} x_i$ is. Suppose that $z = \sum_{i=0}^{\infty} a_i p^i$ contains $(p-1)$ k times and that $\sum_{i=0}^{\infty} a_i = k(p-1)$. Then, however one writes $a_i = a_i^{(1)} + \cdots + a_i^{(k)}$ with $m_j(p-1) = \sum_{i=0}^{\infty} b_i^{(j)} p^i$ and $a_i^{(j)} \geq b_i^{(j)}$, we must have $\sum_{i=0}^{\infty} a_i^{(j)} \geq \sum_{i=0}^{\infty} b_i^{(j)} = n_j(p-1)$, with n_j a positive integer, and hence $\sum_{i=0}^{\infty} a_i^{(j)} \geq (p-1)$ for all j. Since $\sum_{i=0}^{\infty} a_i = k(p-1)$, we have thus $\sum_{i=0}^{\infty} a_i^{(j)} = (p-1)$ for $i \leq j \leq k$ and so $a_i^{(j)} = b_i^{(j)}$ for all i and j, where each $n_j = 1$. In this case z exactly contains $(p-1)$ k times and hence not properly.

Now let $\mathcal{B}$ and $\mathcal{E}$ be, respectively, the sets of integers giving the dimensions of B and E. Then, from what we have shown above, and writing $z = \sum_{i=0}^{2s-1} a_i p^i$, we have $z \in \mathcal{B}$ if and only if $\sum_{i=0}^{2s-1} a_i \geq s(p-1)$, and $z \in \mathcal{E}$ if and only if $\sum_{i=0}^{2s-1} a_i > s(p-1)$. Let $\overline{\mathcal{E}} = \{\overline{z} | z \in \mathcal{E}\}$ where, if $z = \sum_{i=0}^{\infty} a_i p^i$, $\overline{z} = \sum_{i=0}^{\infty} (p-1-a_i)p^i$. Since $\sum_{i=0}^{2s-1} (p-1-a_i) = 2s(p-1) - \sum_{i=0}^{2s-1} a_i$, it follows that $\mathcal{B}$ and $\overline{\mathcal{E}}$ are disjoint with $\mathcal{B} \cup \overline{\mathcal{E}} = \{z \in \mathbb{Z} \mid 0 \leq z < p^{2s}\}$. Hence $\dim(B) + \dim(E) = p^{2s} = q^2$ since, obviously, $|\mathcal{E}| = |\overline{\mathcal{E}}|$. This implies $\dim(E) = \dim(B^{\perp})$ and completes the proof.

REMARKS. 1) The Galois correspondence between subfields of $\mathbf{F}_q$ and the $E(\mathbf{F}_q|F)$ or $B(\mathbf{F}_q|F)$ yields a hierarchy of translation planes corresponding, in the language of the existing literature on translation planes, to the "kern" or "kernel" of the translation plane. Theorem 1 shows that this hierarchy reflects itself in the p-rank of the incidence matrix of the translation plane. Roughly speaking, the rank goes down as the kernel gets larger. Of course, Theorem 1 simply gives upper bounds that grow smaller as F gets larger; in practice the p-rank is rather sporadic: see [1, §7] and the Table of Ranks below. For a full description see [16].

q	dim(C(π))		$q^2+q-\dim(B(\mathbb{F}_q\|\mathbb{F}_p))$	$q+\dim(E(\mathbb{F}_q\|\mathbb{F}_{\sqrt{q}}))$
	$C(\pi)\subseteq B(\mathbb{F}_q\|\mathbb{F}_{\sqrt{q}})$	$C(\pi)\subseteq B(\mathbb{F}_q\|\mathbb{F}_p)$		
9	36*, 40	97, 99, 101, 105(×2)	40	40
16	81*, 97, 97		109	101
25	225*, 238, 250, 252, 254, 255, 256, 257(×4), 258(×4), 259(×2), 260(×2), 261(×3), 263(×2)		295	295

* The rank of the desarguesian plane

TABLE OF RANKS

The ranks of the affine translation planes of orders 9, 16, and 25.

2) We do not, unfortunately, have an easy-to-use formula for $\dim(E(\mathbf{F}_q|F))$ where F is an arbitrary subfield of $\mathbf{F}_q$: we have simply used the formulae given by Delsarte and Hamada. A formula for $\dim(B(\mathbf{F}_q|\mathbf{F}_p))$ that is very simple to use is derived in [12] from Hamada's general formula:

$$\dim(B(\mathbf{F}_q|\mathbf{F}_p)) = \sum_{i=0}^{s-1}(-1)^i \binom{2s}{i}\binom{p(s-1)+s}{2s}$$

where, as usual, $q=p^s$. Of course, by Theorem 2, $\dim(E(\mathbf{F}_q|\mathbf{F}_p)) = q^2 - \dim(B(\mathbf{F}_q|\mathbf{F}_p))$.

3) It would be useful to have a formula for $\dim(E(\mathbf{F}_q|\mathbf{F}_{\sqrt{q}}))$ for q an even power of p. We have computed the dimension of $E(\mathbf{F}_{16}|\mathbf{F}_4)$ using Delsarte's method; it is 85 and yields the bound 101 for 2-dimensional translation planes of order 16. There are precisely two such planes (see [13]); they both have 2-rank 97. It would be interesting to know whether or not they are linearly equivalent: had they both had 2-rank 101, they would have been, by Theorem 1. 4) Mackenzie [16] has also obtained, from Hamada's general formula, the following:

$$\dim(B(\mathbf{F}_{p^4}|\mathbf{F}_{p^2})) = \frac{1}{4}p^8 + \frac{7}{18}p^7 + \frac{2}{9}p^6 + \frac{1}{18}p^5 - \frac{1}{9}p^4 + \frac{1}{18}p^3 + \frac{5}{36}p^2.$$

4. Derivation Sets. Let Π be an arbitrary projective plane of order n, and p a prime dividing n. Let L be a line of Π. We want to explain when a subset D of L will be called a "derivation set" for Π.

Set $\pi = \Pi^L$. Then π is also of order n, and we have the natural projection of $B(\Pi)$ onto $B(\pi)$, where again we will omit the subscript "p" in what follows. If $\dim(B(\Pi)) = k$, then $B(\pi)$ is an $(n^2, k-1)$ code of minimum weight n. Besides the characteristic functions of the lines of π, there are, usually, other minimal-weight vectors in $B(\pi)$, all of which are of the form αv^X, where X is a subset of points of π, $|X| = n$, and $\alpha \in \mathbf{F}_p - \{0\}$. Lemma 1 of [1] describes the nature of such minimal-weight vectors of $B(\pi)$: if $b = \alpha v^X$ is a weight-n vector of $B(\pi)$, where X is not a line of π, normalized so that $\alpha = 1$, then lines in the same parallel class of π meet X constantly modulo p, and, if r is the number of classes whose lines meet X in 0 (mod p) points, then there is a unique vector $\underline{b} \in B(\Pi)$ with $\underline{b} \notin C(\Pi)^\perp$ such that $\underline{b} = v^{\underline{X}}$ for some subset $\underline{X}$ of points of Π, $\underline{b}$ projects to b, and $\text{weight}(\underline{b}) = |\underline{X}| = n + r$, with $1 < r < n$, $r \equiv 1 \pmod{p}$. The set $L \cap \underline{X}$ is, obviously, of cardinality r. For example (see [1]), if $\Pi = PG_2(q^2)$, $\underline{X}$ could be the points of a Baer subplane, with $L \cap \underline{X}$ a Baer segment of L. Then X would be an affine Baer subplane of $AG_2(q^2)$, furnishing a weight-q^2 vector of $B(AG_2(q^2))$ that does not come from a line. (Here, of course, q is a power of p, the order of Π being q^2.)

The above discussion should motivate our definition of "derivation set".

DEFINITION. Let D be a subset of points on a line L of a finite projective plane Π of order n. We say D is a *derivation set* for Π if there is a prime p dividing n and a collection $\mathcal{D}$ of vectors of $B(\Pi)$ satisfying the following conditions:

(i) $|\mathcal{D}| = n|D|$;

(ii) each vector $\underline{b} \in \mathcal{D}$ is of the form $v^{\underline{X}}$ where $D \subset \underline{X}$ and $\text{weight}\,(\underline{b}) = |\underline{X}| = n + |D|$;

(iii) for distinct $\underline{b}$ and $\underline{c}$ in $\mathcal{D}$, $\text{weight}\,(\underline{b} - \underline{c}) \geq 2n - 2$.

The point of the above definition is that, using Π and $\mathcal{D}$, it is easy to construct an affine plane, $\pi(\Pi, \mathcal{D})$, as follows: the points of $\pi(\Pi, \mathcal{D})$ are those of Π^L; the lines of $\pi(\Pi, \mathcal{D})$ are (i) those of π coming from the lines M of Π with $M \cap L \notin D$ and (ii) the subsets X of the points of π coming from $\{v^X | v^X = \text{image}(\underline{b}),\ \underline{b} \in \mathcal{D}\}$, where $\text{image}(\underline{b})$ denotes the image of $\underline{b}$ under the natural projection of $B(\Pi)$ to $B(\Pi^L)$.

The proof that this defines a plane follows from Lemma 1 of [1] (stated at the beginning of this section): first notice that the number of lines we have introduced is $n^2 + n$. A line m of π coming from a line M of Π with $M \cap L \notin D$ has $|m \cap X| = 1$ for each X with $v^X = \text{image}(\underline{b})$, where $\underline{b} \in \mathcal{D}$. Further, condition (iii) ensures that if P and Q are points of π with m the line through P and Q where m is a line of π coming from M of Π with $M \cap L \in D$, then P and Q are together in a unique subset X, as introduced.

It is an immediate consequence of the definition and [1, Lemma 1] that a derivation set has cardinality congruent to 1 modulo p. Those with cardinality equal to 1 have for $\mathcal{D}$ a parallel class of lines. Those with cardinality greater than 1 may admit various $\mathcal{D}$'s (see Section 5).

One could, of course, carry out the above construction using two or more disjoint derivation sets on the line L: for example, the Hall plane of order 16 can be obtained from $PG_2(16)$ by using two disjoint Baer segments. Perhaps a more exact term for the above notion would be "primitive derivation".

PROPOSITION 1. For a plane of prime order there do not exist non-trivial derivation sets. For a plane whose order is a square of a prime, the only possible non-trivial derivation sets are Baer segments.

Proof. This is an immediate consequence of [1, Lemma 2].

The "classical" derivation uses a Baer segment, D, of L and a collection of Baer subplanes having L as a line and D as the intersection of L with the Baer subplanes; this is, of course, one of our cases, but there are other cases as well. Our definition suggests looking for derivation sets under mild, algebraic-coding-theoretic constraints, whereas the broader definition of Ostrom [17] calls for a set-theoretic search.

Consider, therefore, $B(K|F)$, where $K = \mathsf{F}_q$ and $F = \mathsf{F}_p$. $B(K|F)$ is a code of length q^2 and minimum weight q, and we know all the minimal-weight vectors. If π is an affine translation plane of order q, we have $C(\pi) \subseteq B(K|F) \subseteq B(\pi)$. If we restrict the search to $B(K|F)$, then we would be very close to the methods of Ostrom [18]; searching in $B(\pi)$ would, of course, be superior, but more difficult, since a survey of the weight-q vectors in $B(K|F)$ is more tractable than a survey of those of $B(\pi)$.

We now show that the "classical" Baer subplane derivation, in the case of translation planes, takes place in $B(K|F)$—not in the usually larger $B(\pi)$.

PROPOSITION 2. If q is a square and π is an affine translation plane of order q, then every affine Baer subplane of π has point set X satisfying $v^X \in B(\mathsf{F}_q|\mathsf{F}_p)$.

Proof. The result is well-known [6, 14], but we sketch the proof for the convenience of the reader. First let Π be an arbitrary projective plane, Σ a Baer subplane of Π, and (P, L) a flag of Π that belongs to Σ. Let α be an elation of Π with centre P and axis L. Then, if Q and Q^α are points of Σ where $Q \notin L$, it follows that α is an elation of Σ; i.e. $\Sigma^\alpha = \Sigma$. For, if A is any point of Σ not on L and not on the line QQ^α, we have that AQ and PA are lines of Σ. The point $B = QA \cap L$ is on Σ, and hence $BQ^\alpha \cap PA$ is a point of Σ. But $A^\alpha = BQ^\alpha \cap PA$, and thus A^α is on Σ. We need only show now that every point C of Σ on QQ^α has C^α on Σ; but this follows if we reverse the roles of A and Q, since there must be an A in Σ not on L or QQ^α.

Now let $\pi = \Pi^L$ be an affine translation plane. All elations with axis L and centers on L exist. If $\underline{X}$ is the point set of a Baer subplane of Π and L is a line of this Baer subplane, $X = \underline{X} \cap \pi$ is an affine Baer subplane of π with $v^X \in B(\pi)$ [1]. We want to show that $v^X \in B(\mathsf{F}_q|\mathsf{F}_p)$. Without loss of generality, we can assume $O \in X$, O being the zero vector

of V. Suppose $Q \in X, Q \neq O$. The line QO meets L at a point P (at infinity) and there is an elation of Π with center P that moves O to Q. By the above, this elation fixes X setwise. It is defined by the vector (i.e. point) Q' going to $Q' + Q$ and hence X is closed under addition. Thus X is a subspace of V, and $v^X \in B(\mathsf{F}_q|\mathsf{F}_p)$.

REMARKS. 1) For an arbitrary affine plane π of order $n = m^2$, the Baer subplanes will correspond to minimal-weight vectors of $B_p(\pi)$ where p is *any* prime dividing n [1]. Notice that for affine planes we use "Baer subplane" to mean a subplane coming from the projective completion and having the line at infinity as a line.

2) For a translation plane of order $q = p^s$ given by the spread $\{S_0, S_1, \ldots, S_q\}$ (that is, $(q+1)$ s-dimensional subspaces of V with $S_i \cap S_j = \{0\}$ for $i \neq j$), a Baer subplane corresponds to a translate of an s-dimensional subspace T with $\dim(S_i \cap T) = s/2$ or 0 for all i.

3) Proposition 6 of [1] and its Corollary 5 assert that a translation plane of order p^2 has at least $p^3(p^2+1)(p+1)$ desarguesian Baer subplanes. It is possible for it to have more: $PG_2(p^2)$ does. The Proposition shows that if Π is a translation plane of order p^2 with translation line L, there are precisely $p^3(p^2+1)(p+1)$ Baer subplanes of Π that have L as a line, and all of these subplanes are desarguesian. For a 2-dimensional translation plane of order q^2 (i.e. for Π of order q^2 with $C(\Pi^L) \subseteq B(\mathsf{F}_{q^2}|\mathsf{F}_q)$), we know that there are at least $q^3(q^2+1)(q+1)$ desarguesian Baer subplanes that have L as a line, but there may be more: s-dimensional subspaces related to $B(\mathsf{F}_{q^2}|\mathsf{F}_p)$ may provide others.

5. Ovals and Derivation Sets. We next turn our attention to the case $p = 2$. With the notation of Remark 2 of Section 4, it may happen that a subspace T satisfies $\dim(S_i \cap T) = 0$ or 1 for all i. Such a T will have the property that v^T is a weight-q vector of $B(K|F)$ with $|T \cap l| = 0, 1$, or 2 for all lines l of the translation plane π. Now if $\pi = \Pi^L$ and $\underline{b}$ is the preimage of v^T given by [1, Lemma 1] (and stated in section 4), then $\underline{b} + v^L = v^{\underline{X}}$ where $\underline{X}$ is an oval ($q+2$ points with no three collinear) of Π. We show how a set of ovals in a translation plane coordinatized by a nearfield of even order can define the vectors in $\mathcal{D}$, yielding a derivation set D of cardinality $q-1$. The construction depends on the existence of a hyperbolic oval in the affine translation plane.

THEOREM 3. *Let Π be a projective plane of even order q. Suppose that*

(i) *Π has an oval $\underline{\mathcal{O}}_0$, and*

(ii) *there are two points, P_0 and Q_0 on $\underline{\mathcal{O}}_0$ for which Π is (P_0, Q_0)-transitive. Then, if L is the line through P_0 and Q_0, $D = L - \{P_0, Q_0\}$ is a derivation set for Π.*

Proof. The condition that Π is (P_0, Q_0)-transitive—that is, that every central collineation with centre P_0 and axis through Q_0 exists—is equivalent to the condition that Π is a translation plane coordinatized by a nearfield: see [6; §3.1.22(e)]. Thus $q = 2^s$, for some s.

We need to produce the set $\mathcal{D}$ of vectors $v^{\underline{X}}$ in the binary code $B(\Pi)$ with $|\underline{X}| = 2^{s+1}-1$, and with $\underline{X} \supset D$. Since any oval $\underline{\mathcal{O}}$ of Π provides a vector $v^{\underline{\mathcal{O}}}$ in $C(\Pi)^{\perp}$ of weight 2^s+2, the oval $\underline{\mathcal{O}}_0$ will yield $\underline{b} = v^L + v^{\underline{\mathcal{O}}}$ of weight $2^{s+1}-1$ with support containing D. Our goal is to extract a set of $2^s(2^s-1)$ of these ovals, with $v^{\underline{\mathcal{O}}} + v^{\underline{\mathcal{O}}^*}$ of weight at least $2^{s+1}-1$ for distinct $\underline{\mathcal{O}}$ and $\underline{\mathcal{O}}^*$. This we accomplish in a purely combinatorial manner.

Let H denote the group of all collineations of Π with center P_0 and axis passing through Q_0. Then H has order $2^s(2^s-1)$ (see [10, Chapter 6], for example) and no non-identity element of H can fix $\underline{\mathcal{O}}_0$. Thus the orbit Ω of $\underline{\mathcal{O}}_0$ under H has size $2^s(2^s-1)$. If we form the incidence structure $\mathcal{S}$ consisting of the points of Π not on L, and having for blocks the orbit Ω of ovals, together with the lines through P_0 and Q_0 other than L, then we can show that this structure is an affine plane of order 2^s. Now $\mathcal{S}$ has 2^{2s} points and $2^{2s}+2^s$ blocks, each of size 2^s. We show that any two points of $\mathcal{S}$ are on exactly one block of $\mathcal{S}$: let P and Q be distinct points of $\mathcal{S}$, not together on a line through P_0 or Q_0. The set of images of $\underline{\mathcal{O}}_0$ under the subgroup of elations of H forms a parallel class of blocks, so we can assume that P is on some $\underline{\mathcal{O}}^*$. If Q is also on $\underline{\mathcal{O}}^*$, then we have a block through P and Q; if Q is not on $\underline{\mathcal{O}}^*$ then form the lines PQ_0 and QP_0 and let them intersect at R. Let S be the point of intersection of QP_0 and $\underline{\mathcal{O}}^*$. Then there is a homology in H with center P_0 and axis PQ_0 that maps S to Q, and hence maps the oval $\underline{\mathcal{O}}^*$ to one through P and Q. Thus any two points of $\mathcal{S}$ are on at least one block, and now a count of (pairs of points, block)-intersections, in two ways, yields that any two points are together on exactly one block. The set Ω thus gives the required set of ovals.

REMARKS. 1) If one takes $\Pi = PG_2(2^s)$ and for the oval $\underline{\mathcal{O}}_0$ a conic plus nucleus, with the nucleus either P_0 or Q_0, then the derivation is taking place inside $B(\mathbf{F}_{2^s}|\mathbf{F}_2)$: for the conic given by $x^2 = yz$, with $\langle(0,0,1)'\rangle$ for the line L at infinity, contains the point $\langle(0,1,0)\rangle = P_0$ of L, and its nucleus is $Q_0 = \langle(1,0,0)\rangle$, which is again on L. In the affine plane with point set $\{(a,b,1)|a,b \in \mathbf{F}_{2^s}\}$, the conic consists of the points $\{(t,t^2,1)|t \in \mathbf{F}_{2^s}\}$. Since we are in characteristic $p=2$, this set is an s-dimensional subspace over $\mathbf{F}_2$.

It follows also (and the calculation is similar) that a conic plus nucleus will be furnished by a minimal-weight vector of $B(\mathbf{F}_{2^s}|\mathbf{F}_2)$ if and only if its nucleus is at infinity. Thus the derivation, even if we restrict to ovals coming from conics, may not be taking place in $B(\mathbf{F}_{2^s}|\mathbf{F}_2)$, but in $B(AG_2(2^s))$. Moreover, not all ovals come from conics when $s > 3$: see, for example, [9].

2) Another similarity with the derivation coming from Baer subplanes is that, in the new projective plane, one has the property that any line of Π^L that has been discarded, together with the points P_0 and Q_0 on the new line at infinity, becomes an oval of the new plane.

3) We do not know whether or not there is a $\mathcal{D}$ which, for our derivation set of cardinality 2^s-1, will yield a new non-desarguesian projective plane. Any $\mathcal{D}$ produced as in the proof of Theorem 3 will yield a translation plane coordinatized by a nearfield with multiplicative group isomorphic to that of the nearfield of the original plane, for the new projective

plane Σ with the new line M at infinity has, in its automorphism group G, all central collineations with center P_0 and axis through Q_0, and thus, by [6;§3.1.19, p.123], has all central collineations with center Q_0 and axis through P_0. It follows easily that Σ is a translation plane, with M a translation line: see, for example [10; Theorem 4.19, p. 100]. Thus by [6;§3.1.22(e) and §3.1.34], Σ^M can be coordinatized by a nearfield $\mathbf{D}$, and $\mathbf{D}$ is unique. By [6;§3.1.22(b)], the multiplicative group, $\mathbf{D}^\times$, is isomorphic to the group $G(P_0, L^*)$ of homologies with center P_0 and axis L^* through Q_0, and this, by our construction, is isomorphic to the multiplicative group of the original coordinatizing nearfield. Thus when the nearfield is a field, the new plane is desarguesian, however one chooses the oval. 4) In [11] Kelly has given a similar construction using even more conics.

6. Other Derivation Sets. We turn, finally, to other possible derivation sets that might arise from minimal-weight vectors of $B(K|F)$, where $K = \mathsf{F}_q$ and $F = \mathsf{F}_p$. Suppose Π is a translation plane with translation line L and $\pi = \Pi^L$. We have, as before,

$$C(\pi) \subset B(K|F) \subseteq B(\pi).$$

If $b \in B(K|F)$ has weight q but is not from a line of π, let $\underline{b} = v^{\underline{X}}$ be a pre-image of b with weight $q + r$, where $r \equiv 1 \pmod{p}$. We pointed out in [1] that $\underline{X}$ is a blocking set (see [3]) for Π, and hence $r \geq 1 + \sqrt{q}$. Without loss of generality, we may assume that $b = v^T$, where T is an s-dimensional subspace of V, and $q = p^s$. If $S_0, S_1, \ldots, S_q$ is the spread defining π, then $r = |\{S_i | S_i \cap T \neq \{0\}\}|$. In general it is difficult to count the number of T with given intersection properties, and all sorts of intersections can occur: for example, a "random" look at the possibilities for a spread of one of the 2-dimensional translation planes of order 16, i.e., the one defined by the coordinate set M_2 of [7], gave various intersection patterns for subspaces in $B(\mathsf{F}_{16}|\mathsf{F}_2)$. If we let the 4-tuple $[x_0, x_1, x_2, x_3]$ correspond to a subspace T meeting x_i members of the spread in subspaces of dimension i, for $i = 0, 1, 2, 3$, so that $r = x_1 + x_2 + x_3$, then we found instances of:

$[12, 0, 5, 0]$, $r = 5$ (Baer subplanes); $[10, 3, 4, 0]$, $r = 7$; $[8, 8, 0, 1]$, $r = 9$; $[8, 6, 3, 0]$, $r = 9$; $[6, 9, 2, 0]$, $r = 11$; $[4, 12, 1, 0]$, $r = 13$; $[12, 15, 0, 0]$, $r = 15$ (ovals).

There is one case for which the count is rather easy: if $S_i \cap T$ is of dimension $s - 1$ for one (and hence precisely one) S_i. Here we are assuming $s > 2$, since in the case $s = 2$, all T, except the $S_0, S_1, \ldots, S_q$, yield Baer subplanes. First observe that if $\dim(S_i \cap T) = s - 1$ and $\dim(S_j \cap T) \geq 2$ for some $j \neq i$, then, since $S_i \cap S_j = \{0\}$, $\dim(T) \geq s + 1 > s$, which is an impossibility. It follows that $\dim(T \cap S_i) = s - 1$ for exactly one S_i, $\dim(T \cap S_i) = 1$ for exactly p^{s-1} S_i, and $T \cap S_i = \{0\}$ for $p^{s-1}(p-1)$ of the S_i. Here $r = 1 + p^{s-1}$ and the $\underline{b}$ has weight $p^s + p^{s-1} + 1$. Choosing such a T is easy: simply take an $(s-1)$-dimensional subspace of one S_i and a 1-dimensional subspace of another and let T be the (necessarily direct) sum. An easy count gives the number of such subspace to be $p(p^s + 1)(p^s - 1)^2/(p - 1)^2$

and hence, counting translates, there are $p^{s+1}(p^s+1)(p^s-1)^2/(p-1)^2$ normalized weight-q vectors of $B(K|F)$ with $r = p^{s-1}+1$. Each of these produces a distinct blocking set of cardinality $p^s + p^{s-1} + 1$ in the projective translation plane

The following question arises: can there be a derivation set of cardinality $p^{s-1}+1$ in $PG_2(p^s)$? Recall that we must have $n|D|$ vectors in $\mathcal{D}$. Since $n = q$ for translation planes, the "n" is given by the translates of a T. Thus we must find $|D| = p^{s-1}+1$ subspaces, $T_0, T_1, \ldots, T_{p^{s-1}}$, with $T_m \cap S_i = \{0\}$ for any m implying $T_j \cap S_i = \{0\}$ for all j. Suppose we have found T_0 with $T_0 \cap S_0$ of dimension $s-1$ and $T_0 \cap S_i$ of dimension 1 for $1 \le i \le p^{s-1}$. Since a k-dimensional subspace of an n-dimensional space over F_q has $q^{k(n-k)}$ complementary $(n-k)$-dimensional subspaces, $T_0 \cap S_0$ has q^{s-1} complementary subspaces in S_0. Next, suppose there is an s-dimensional subspace T_1 with $T_1 \cap S_0$ complementary to $T_0 \cap S_0$, and $T_1 \cap S_1$ complementary to $T_0 \cap S_1$. Then $V = S_0 \oplus S_1 = (T_0 \cap S_0 \oplus T_1 \cap S_0) \oplus (T_0 \cap S_1 \oplus T_1 \cap S_1) = (T_0 \cap S_0 \oplus T_0 \cap S_1) \oplus (T_1 \cap S_0 \oplus T_1 \cap S_1) \subseteq T_0 + T_1$. Thus $T_0 \cap T_1 = \{0\}$ since both T_0 and T_1 are s-dimensional. It is thus conceivable that there could exist $T_0, T_1, \ldots, T_{p^s-1}$ with $T_j \cap S_i = \{0\}$ for $i > p^{s-1}$ and all j, and with $T_i \cap S_j$ of dimension $s-1$ for $0 \le i \le p^{s-1}$, and $T_i \cap T_j = \{0\}$ for $i \ne j$. These subspaces and their translates would yield the desired $q(p^{s-1}+1)$ vectors of $\mathcal{D}$. Put in the language of spreads, $T_0, T_1, \ldots, T_{p^{s-1}}$, as a partial spread, would replace $S_0, S_1, \ldots, S_{p^{s-1}}$.

For $q = 2^3$, the first case possible, we have $r = 5$ and, because of the peculiar homogeneity properties of $PTL_2(8)$ acting on L, any 5-set of L would be suitable if one such could be found. One computes easily that there are seven T's available for each 5-subset of L, but, unfortunately, five of these seven cannot be chosen properly. It follows, since $r \ge 1 + \sqrt{8}$, that the only non-trivial derivation sets have $r = 7$ and are given by ovals.

We have not investigated any other case. We end by remarking that one could work in $B(\mathsf{F}_{q^s}|\mathsf{F}_q)$, getting similar counts and possibilities.

REFERENCES

[1] E.F. Assmus, Jr. and J.D. Key, *Affine and projective planes*, Discrete Math., Special Coding Theory Issue (to appear).

[2] E.F. Assmus, Jr. and J.D. Key, *Baer subplanes, ovals and unitals*, Coding Theory, IMA Volumes in Mathematics and its Applications, ed. D. Ray-Chaudhuri, Springer, New York (1989).

[3] A.A. Bruen, *Blocking sets in finite projective planes*, SIAM J. Appl. Math., 21 (1971), 380–392.

[4] P. Charpin, *Thèse de Doctorat d'État*, Université de Paris VII (1987).

[5] P. Delsarte, *A geometric approach to a class of cyclic codes*, J. Combin. Theory, 6 (1969), 340–358.

[6] P. Dembowski, *Finite Geometries*, Springer (1968).

[7] U. Dempwolff and A. Reifart, *The classification of the translation planes of order 16, I*,, Geometriae Dedicata, 15 (1983), 137–153.

[8] N. Hamada, *On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error correcting codes*, Hiroshima Math. J., 3 (1973), 153-226.

[9] J.W.P. Hirschfeld, *Projective Geometries over Finite fields*, Oxford (1979).

[10] D.R. Hughes and F.C. Piper, *Projective Planes*, Springer Graduate Texts in Mathematics (1973).

[11] G. KELLY, *Symmetric designs with translation blocks*, Geometriae Dedicata, 15 (1984), 233–258.

[12] J.D. KEY AND K. MACKENZIE, *An upper bound for the p-rank of a translation plane (submitted).*

[13] E. KLEINFELD, *Techniques for enumerating Veblen-Wedderburn systems*, J. Assoc. Comput. Mach., 7 (1960), 330-337.

[14] H. LÜNEBURG, *Charakterisierungen der endlichen desarguesschen projektiven Ebenen*, Math. Z., 85 (1964), 419–450.

[15] H. LÜNEBURG, *Translation Planes*, Springer (1980).

[16] K. MACKENZIE, *Ph.D. thesis*, University of Birmingham (in preparation).

[17] T.G. OSTROM, *Semi-translation planes*, Trans. Amer. Math. Soc., 111 (1964), 1–18.

[18] T.G. OSTROM, *Vector spaces and construction of finite projective planes*, Archiv der Math., 14 (1968), 1–25.