Bull. Austral. Math. Soc. 05B15, 05B25, 51A45, 51B15, 51E15, 51E20
Vol. 49 (1994) [311–324]

A GEOMETRICAL REPRESENTATION THEORY FOR ORTHOGONAL ARRAYS

David G. Glynn

Every orthogonal array of strength s and of prime-power (or perhaps infinite) order q, has a well-defined collection of ranks r. Having rank r means that it can be constructed as a cone cut by q^s hyperplanes in projective space of dimension r over a field of order q.

Introduction to the Classical Representations

An *orthogonal array* k-$OA(q,s)$, is a $k \times q^s$ array $\mathfrak{A}$ containing elements from a set $S := S(\mathfrak{A})$ of size q such that every s rows of $\mathfrak{A}$ contain precisely once in their columns every possible ordered s-tuple of S. The parameter s is called the *strength* of the OA and q is called its *order*. We assume also that $k \geqslant s$.

A very important combinatorial problem (investigated, for example by R.C. Bose) is to construct an OA of given order and strength (both finite), but with a maximal number of rows k. The case of strength 1 is trivial, and strength 2 is well-known: a k-$OA(q,2)$ is equivalent to the following things.

(1) $k-2$ mutually orthogonal latin squares of order q;
(2) a k-net of order q;
(3) a transversal design of order q with k parallel classes.

Also, it is quite easy to show that the maximum value of k for a k-$OA(q,2)$ is $q+1$, and if that bound is attained the structure is equivalent to an affine plane of order q. The only finite planes presently constructed are of prime-power orders q.

For the reader who isn't conversant with these facts let us show how to construct a $(q+1)$-$OA(q,2)$ from a projective plane of finite order q. (Infinite arrays can be constructed similarly from infinite planes.) Fix any point V in the plane and associate the $q+1$ lines passing through V with the rows of the OA. Choose any set S of size q. For each of the $q+1$ lines through V associate with each point different from V and on that line a distinct element of S. Now every point of the plane except for V has an associated element of S such that no two points on a line through V have the same

Received 18th May, 1993
This research was supported by a grant from the University of Canterbury and by a von Humboldt Fellowship at the University of Tübingen.

https://doi.org/10.1017/S0004972700016373 Published online by Cambridge University Press

element. The columns of the OA are now associated with the q^2 lines of the plane not passing through V. Since in the plane two distinct lines intersect in a unique point, the element of the OA in a certain row and column is given by the associated element of the intersection of the pair of lines that correspond to that row and column.

The case of strength 3 is less well known, but if q is finite it is easy to see that a $(q+1)$-$OA(q,3)$ is equivalent to a *Laguerre plane* of order q. These have only been constructed for prime-power orders, and all known examples are embeddable in $PG(3,q)$ as a cone over an oval; see, for example [4]. When $q = 2^h$ it is possible to construct a $(q+2)$-$OA(q,3)$ as a cone over a planar hyperoval (complete oval or $(q+2)$-arc) in $PG(3,q)$.

This can be generalised to higher dimensions with the construction of an $\mathfrak{A} = k$-$OA(q,s)$, but we need q to be a prime-power. First, we have to define a k-arc of $PG(n,q)$, the n-dimensional projective space over $GF(q)$. It is a set of $k \geqslant n+1$ points, every $n+1$ of which are linearly independent. The classical examples of $(q+1)$-arcs are the normal rational curves, but there are several other examples; see [1] and [3].

To construct $\mathfrak{A}$ from a k-arc of $PG(n,q)$ we proceed as follows. We embed the $PG(n,q)$ as a hyperplane h of $PG(n+1,q)$, and consider the cone with the k-arc as base and having a vertex V which is any point not in h. Next we associate the rows of $\mathfrak{A}$ with the lines (or *generators*) of the cone through V. Let S be any set of size q. On each generator we label the points distinct from the vertex with the elements of S. The columns of $\mathfrak{A}$ are associated with the q^{n+1} hyperplanes of $PG(n+1,q)$, not passing through the vertex of the cone. Finally, the element of $\mathfrak{A}$ in a certain row and column is given by the element associated with the point of intersection of the corresponding generator and hyperplane. The strength of $\mathfrak{A}$ is $s = n+1$, because any $n+1$ points of the cone, on different generators, are contained in a unique hyperplane of $PG(n+1,q)$. If this were not the case, then the projection of these points from V to the base h would be a set of $n+1$ points of the k-arc which could not be independent.

The smallest non-trivial example of a k-arc is any set of k points of $PG(1,q)$. Then the above construction gives a k-$OA(q,2)$, which is equivalent to a sub-net of the affine plane $AG(2,q)$. In the plane $PG(2,q)$ it is quite hopeless to try to classify all the k-arcs, but if we restrict ourselves to the maximal cases

(1) $k = q+1$, for q odd, (an odd prime-power);
(2) $k = q+2$, for q even (and so $q = 2^h$, $h \in \mathbb{Z}$, $h \geqslant 1$);

then Segre's theorem (see [2]) implies in the first case that the arc is an irreducible conic, and so the corresponding $(q+1)$-$OA(q,3)$ is equivalent to the Miquelian Laguerre plane of order q. In the second case there are many examples of $(q+2)$-arcs, and so there are many examples of Laguerre planes that are embeddable in $PG(3,q)$.

We shall show that if the element set S is $GF(q)$ there is a way to label each of

https://doi.org/10.1017/S0004972700016373 Published online by Cambridge University Press

the generators in the above cone of $PG(n+1,q)$ such that the corresponding array has rank $n+1$. Furthermore, this array is equivalent (up to permutation of the columns) to the collection of all q^{n+1} vectors in the column space of the $k \times (n+1)$ matrix, each row of which forms the coordinates of a point of the k-arc. This set of vectors is actually an MDS code, but we shall not pursue this any further.

However, the above construction is not the main point of this paper. We shall show that there is a kind of *representation theory* of orthogonal arrays, similar to that of groups. Every orthogonal array of prime-power or infinite order can be represented as a cone in different ways. In the finite case there is certainly a cone of minimal dimension — it turns out that this dimension is greater than or equal to its strength, and that equality occurs if and only if the array has the above construction from a k-arc of $PG(n,q)$.

The Theory of General Representations

As some notation let $S_\lambda := \{1,\dots,\lambda\}$, for $1 \leqslant \lambda$, $\lambda \in \mathbb{Z}$.

Lemma 1. *Suppose A is a $k \times b$ matrix of rank $r \geqslant 1$ over a field F. Then A can be factorised into the product of two matrices over F*

$$A = XY,$$

where X is $k \times r$ and Y is $r \times b$, and where both X and Y have rank r.

Proof: Let the i'th column of A be $\mathbf{a}_i$, for $i \in S_b$. Now A has a set of r linearly independent columns: suppose that this set is $\{\mathbf{a}_{\phi(t)} \mid t \in S_r\}$, where ϕ is an injection from $S_r \to S_b$. Then define the matrix X so that its t'th column is $\mathbf{a}_{\phi(t)}$. Thus X also has rank r. Now the column space of X equals the column space of A, so that each column $\mathbf{a}_j$, ($j \in S_b$), of A may be written in the form $\mathbf{a}_j = \sum_{t=1}^{r} \mathbf{a}_{\phi(t)} y_{tj}$, where $y_{tj} \in F$. We let Y be the $r \times b$ matrix (y_{tj}). The $\phi(t)$'th column of Y is zero except for $y_{t\phi(t)} = 1$, so that Y contains an identity $r \times r$ submatrix. Hence Y also has rank r and $A = XY$. $\square$

Suppose from now on that $\mathfrak{A}$ is an OA of order $q = |S|$, which is also the size of some field F: that is, $q = p^h$, p is a prime, $h \in \mathbb{Z}$, $h \geqslant 1$; or q is infinite. Also suppose that $s \geqslant 2$.

To each row i of $\mathfrak{A}$ we can apply a bijection $\gamma_i \colon S \to F$, so that the elements of $\mathfrak{A}$ belong to F instead of S. Indeed, when q is finite, there are $(q!)^k$ ways of doing this. Let us call this sequence of mappings a *substitution*. Also, if $\Gamma := (\gamma_1, \dots, \gamma_k)$, the resulting matrix over F is $A := \mathfrak{A}(\Gamma)$.

https://doi.org/10.1017/S0004972700016373 Published online by Cambridge University Press

LEMMA 2. *If $\mathfrak{A}$ is a k-$OA(q,s)$, then for each substitution Γ, $A := \mathfrak{A}(\Gamma)$ is an OA isomorphic to $\mathfrak{A}$, and it has rank $r := r(A) \geqslant s$.*

PROOF: Two OA's, $\mathfrak{A}$ and $\mathfrak{A}'$ are considered to be isomorphic if they have the same sized arrays and element sets, and there exist permutations of the rows and of the columns of $\mathfrak{A}'$ to make an array $\mathfrak{A}''$ so that if we superpose $\mathfrak{A}$ onto $\mathfrak{A}''$ then for each row i a bijection β_i is induced that maps the element set $S(\mathfrak{A})$ onto the element set $S(\mathfrak{A}') = S(\mathfrak{A}'')$: if the element in position (i,j) of $\mathfrak{A}$ is x then the element in that position of $\mathfrak{A}''$ is $\beta_i(x)$. In the case of this Lemma, $A' = A''$ and $\beta_i = \gamma_i$, for all i, so that $\mathfrak{A} \cong A$. Also, $r(A) \geqslant s$, because every s rows of A are linearly independent, since every possible column from the field F appears in these rows. $\square$

DEFINITION 1: A substitution Γ acting on $\mathfrak{A}$ is associated with the rank of the subsequent matrix $A := \mathfrak{A}(\Gamma)$, which is called *the rank of the substitution.*

THEOREM 1. *A k-$OA(q,s)$, $\mathfrak{A}$, has a substitution of rank r over a field F if and only if $\mathfrak{A}$ can be represented in $\pi := PG(r,F)$ as a cone with point-vertex V, with k generators through V cut by a set H of q^s hyperplanes not passing through V. $\mathfrak{A}$ has strength s if and only if every set of s points of the cone, none equal to the vertex and on s different generators, is contained in a unique hyperplane of H.*

PROOF: Let $A = \mathfrak{A}(\Gamma)$ as above. From Lemma 1 we can write $A = XY$, where $r(X) = r(Y) = r(A) = r$, X is $k \times r$, Y is $r \times b$, $b = q^s$. Let the points of π be $(c, \mathbf{d})$, where $c \in F$, and $\mathbf{d} \in F^r$, and not both of c and $\mathbf{d}$ are zero. We construct a set of k points in the hyperplane with equation $c = 0$ by letting $P_i := (0, \mathbf{x}_i)$, where $\mathbf{x}_i$ is the i'th row of X. Let V be the point $(1,0)$ of π. It is the vertex of a cone with base $\{P_i \mid i \in S_k\}$: that is, the generators of the cone are the lines g_i joining P_i to V.

Now we must construct the hyperplanes that cut this cone. We use dual coordinates $[u, \mathbf{v}]$ for the hyperplanes of π, where $u \in F$, $\mathbf{v} \in F^r$, (not both zero). A point $(x, \mathbf{y})$ is on a hyperplane $[u, \mathbf{v}] \iff ux + \mathbf{v} \cdot \mathbf{y} = 0$. Let the hyperplane $h_j := [-1, \mathbf{y}_j]$, where $\mathbf{y}_j$ is the j'th column of Y. This gives $b = q^s$ hyperplanes.

We leave it as an exercise to show that if w is a $k \times 1$ vector, then $wX = 0 \iff wA = 0$. Hence a subset of rows of X is dependent if and only if the corresponding subset of rows of A is dependent. Thus one can check that all the points P_i and the hyperplanes h_j are different, because any $s \geqslant 2$ rows of A are independent implies that any s rows of X are also independent. And if two columns of Y were the same then the corresponding columns of A would be also the same. This would contradict the assumption that every possible column appears in the s rows precisely once.

In order to construct the matrix A from the cone and the set of q^s hyperplanes, one only has to note that the element in the (i,j)'th position of A is given by $\mathbf{x}_i \cdot \mathbf{y}_j$. This can be calculated directly from the intersection of the generator g_i with the hyperplane

https://doi.org/10.1017/S0004972700016373 Published online by Cambridge University Press

h_j — a general point of g_i is $(\lambda, \mathbf{x}_i)$ which is on $h_j = [-1, \mathbf{y}_j] \iff \lambda = \mathbf{x}_i \cdot \mathbf{y}_j$. What we are doing is labelling the point $(\lambda, \mathbf{x}_i)$ with λ. □

DEFINITION 2: The construction of Theorem 1 of an OA in r-dimensional space is called a *representation*.

It is important to note that the representation constructed from the substitution into the OA is essentially unique, (up to collineations of $PG(r, F)$). This is because every factorisation of A is of the type $XR.R^{-1}Y$, where R is $r \times r$ and non-singular over F. Then R really corresponds to a homography of $PG(r, F)$ which takes the cone and the set of hyperplanes corresponding to XY to the cone and hyperplanes corresponding to $XR.R^{-1}Y$.

Let us call the set of points defined by the rows of X the *base curve*, and the set of hyperplanes H corresponding to Y the *cutting hyperplanes*. The base curve and the set of cutting hyperplanes of the cone C defined by the base curve now become the objects of study.

From the exercise contained in the proof of Theorem 1 above, we know that every subset of s points of the base curve is independent. The case when r is minimal is $r = s$, and then H is the entire set of hyperplanes of π that do not pass through the vertex (when q is finite, at least). Then each set of r points (on different generators) of C are linearly independent, thus implying that the cone intersects any hyperplane of H in a k-arc (always pairwise isomorphic). We can define $m(\mathfrak{A})$ to be the minimal rank of a representation of $\mathfrak{A}$. Thus we have the following result.

THEOREM 2. *A k-$OA(q, s)$, $\mathfrak{A}$, of prime-power order q has $m(\mathfrak{A}) = s$ if and only if it is constructed from a cone C over a k-arc of $PG(s-1, q)$ intersected by all the hyperplanes not passing through the vertex of C.*

When $s = 2$ this implies that $m(\mathfrak{A}) = 2$ if and only if the OA is equivalent to a subnet of the affine plane $AG(2, q)$ of order q, which can be constructed from any subset of k points of $PG(1, q)$. When $s = 3$ it implies that $m(\mathfrak{A}) = 3$ if and only if the OA is constructed from a k-arc of $PG(2, q)$.

AN EXAMPLE: A REPRESENTATION OF CERTAIN DESARGUESIAN PLANES

Here we describe a non-trivial representation of the Desarguesian projective plane $PG(2, q)$ as a cone in $PG(4, q)$, (when 3 is not a factor of $q - 1$ or q, and $q \geqslant 5$). *This representation is also valid for the real projective plane.* From the classical examples we have to consider the $\mathfrak{A} = (q+1)$-$OA(q, 2)$ of rank 2 which has columns $(b, a + k_1 b, \dots, a + k_q b)^t$, where a, $b \in GF(q) = \{k_1, \dots, k_q\}$. Using the general representation theory on each row of this array we have to assign a permutation of $GF(q)$. In the case of finite fields a permutation can always be specified by a polynomial of degree

https://doi.org/10.1017/S0004972700016373 Published online by Cambridge University Press

less than $q-1$; see [5]. We want permutations that are not additive so that the rank of the array is increased slightly. The simplest possible case is when all the permutations on each row are equal. Then all permutation polynomials of degree less than three are additive, so that we should choose polynomials of degree at least three. If 3 is not a factor of $q-1$ or q, and if $q \geqslant 5$ the mapping $\chi\colon x \mapsto x^3$ is a good choice. (This is also valid for the real field.) Thus we are using the substitution $\Gamma := (\chi, \dots, \chi)$. We can check that the new array $A = \mathfrak{A}(\Gamma)$ is of rank 4. The four columns $(0,1,\dots,1)^t$, $(0,k_1,\dots,k_q)^t$, $(0,k_1{}^2,\dots,k_q{}^2)^t$, and $(1,k_1{}^3,\dots,k_q{}^3)^t$ generate the column space of A. Thus we have the decomposition $A = XY$ as follows:

$$\begin{pmatrix} \dots & b^3 & \dots \\ \dots & (a+k_1b)^3 & \dots \\ \vdots & \vdots & \vdots \\ \dots & (a+k_qb)^3 & \dots \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & k_1 & k_1{}^2 & k_1{}^3 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & k_q & k_q{}^2 & k_q{}^3 \end{pmatrix} \cdot \begin{pmatrix} \dots & a^3 & \dots \\ \dots & 3a^2b & \dots \\ \dots & 3ab^2 & \dots \\ \dots & b^3 & \dots \end{pmatrix}.$$

The base curve of the cone is the twisted cubic $\{(1,x,x^2,x^3) \mid x \in GF(q) \cup \{\infty\}\}$, (or an irreducible curve of degree 3, or normal rational curve) of $PG(3,q)$. The set of q^2 hyperplanes cutting this cone is given by

$$\{[-1, a^3, 3a^2b, 3ab^2, b^3] \mid a, b \in GF(q)\},$$

which, using the substitution $y := -a/b$ and $z := b^3$, may be re-written as

$$\{[-1, -zy^3, 3zy^2, -3zy, z] \mid y, z \in GF(q)\} \cup \{[-1, -z, 0, 0, 0] \mid z \in GF(q)\}$$

$$= \bigcup_{y \in GF(q) \cup \{\infty\}} \{[-1,0,0,0,0] + z[0, -y^3, 3y^2, -3y, 1] \mid z \in GF(q)\}.$$

Thus it is possible to construct all the cutting hyperplanes by the following method: in the base $PG(3,q)$ take the dual curve of $q+1$ planes $[-y^3, 3y^2, -3y, 1]$, ($y \in GF(q)$), and $[1,0,0,0]$, ($y = \infty$), and consider all the hyperplanes of $PG(4,q)$ passing through these planes but not passing through the vertex of the cone $V = (1,0,0,0,0)$. Note that we have omitted the first coordinate (which is zero) of the base curve, and also of the dual curve above. Then there is a symplectic polarity which takes the base curve to its dual curve. This is $(x_0, x_1, x_2, x_3) \leftrightarrow [-x_3, 3x_2, -3x_1, x_0]$. Each plane p of the dual curve intersects the curve only at its image P under the polarity — we call this plane the *tangent* at the point of the curve. And finally, any four distinct points P_1, P_2, P_3, and P_4 of the curve have the property that the line $p_1 \cap p_2$ is always skew to the line $P_3.P_4$. These things happen because the particular cone representation above inherits a certain group of the Desarguesian plane: this is the group of homologies with centre

V and axis a line not through V (or the base curve). The group is also isomorphic to the multiplicative group of a field that is the same order as the plane.

Many things can be deduced from the above example, but first let us note that it is not true that the base curve is always an arc. For if we replace the cubic substitution by a quintic substitution above, then we require the condition that $\chi\colon x \mapsto x^5$ is a permutation of the field, and not an automorphism. In particular let us consider fields of characteristic two; for example in the finite case we require that $5 \not| \; q-1$, and so $q = 2^h$, where $h \geqslant 3$, and $4 \not| \; h$. Since $(x+y)^5 = x^5 + x^4y + xy^4 + y^5$ in characteristic 2, we find that the base curve of the rank 4 representation is $(1, x, x^4, x^5)$, which is not an arc of 3-d space if $h \equiv 2 \pmod 4$; see [1]. One can generalise this even further by replacing 5 by $2^i + 1$, where the latter has no factors in common with $q - 1$, but let us omit these considerations, and proceed to the following section.

An Application to the Theory of Projective Planes of Lenz-Barlotti Class at Least I.2

Recall (see [2]) that a projective plane of Lenz-Barlotti Class at Least I.2 has a group G of homologies with a fixed point V as centre and a fixed line b as axis, such that V does not lie on b and G is sharply transitive on the points (not V nor on b) of any fixed line through V. In the case of a projective plane of finite order q, the group G has order $q-1$. The main examples are the Desarguesian planes over a skew field F, where G is isomorphic to the multiplicative group F^* of F (which is cyclic of order $q-1$ in the finite case, because $F \cong GF(q)$), or the planes over the proper near-fields, in which G is also isomorphic to the multiplicative group of the near-field, but not in general to that of a field of the same order.

Such a plane can have various representations as cones in $[r] := PG(r, F)$, where F is a field of the same order as the plane. However, in this section we are interested in representations with an extra property. Suppose the cone has a certain base (a distinguished cutting hyperplane). There is a unique group G of homologies of $PG(r, F)$ which fixes every point of the base (which is the axis of the group), and fixes every line through the vertex of the cone. It is isomorphic to F^*. Suppose the representation is preserved by G. This is equivalent to the statement that the set H of cutting hyperplanes ($[r-1]$'s) of the cone is fixed set-wise by G. In other words we can construct H from a certain collection H' of hyperplanes ($[r-2]$'s) of the base: we just take H to be all $[r-1]$'s passing through the $[r-2]$'s (excepting those through the vertex V of the cone). The dual coordinates for the $[r-2]$'s of H' are then given by any maximal subset of columns of Y that are not related by a constant factor k.

Conversely, one can see that any plane of type at least I.2, such that the group of homologies is isomorphic to the multiplicative group of a field (or perhaps skew-field)

https://doi.org/10.1017/S0004972700016373 Published online by Cambridge University Press

has a representation as above. This is because we have an orthogonal array representing the plane, which can be factorised $A = XY$, where one of the columns of Y can be assumed to be zero (corresponding to the base hyperplane), and if $\mathbf{y}$ is a column of Y, then so is $k\mathbf{y}$, for all $k \in F$. Let us shed light on the way to construct an array with this property. First, we have to label the points of the base line b with 0: this corresponds to the distinguished zero columns of A and of Y. Certain points P of the plane (not on b nor equal to V) are labelled 1; in fact there is one on each line through V. Since multiplying a row of A by a constant merely gives an equivalent OA, the actual points $P = P_i$ on each of the $q+1$ lines through V, that we choose to have the value 1, are irrelevant. Any line t, different from b, and not a generator through V, intersects b in a unique point (which is labelled 0). The other non-zero points on t are mapped by a homology $\lambda \in G$ to non-zero points on t^λ. If such a point Q were labelled k, then Q^λ would be labelled $k.\alpha(\lambda)$, where the column of A corresponding to t^λ is $\alpha(\lambda)$ times the column corresponding to t. Thus it follows that a general point P^λ $(\lambda \in G)$, (P has been labelled 1), is labelled $\alpha(\lambda)$, where α is a fixed isomorphism $G \to F^*$. For each isomorphism α we obtain a perhaps different representation of the plane. A general α is the composition of a fixed isomorphism $G \to F^*$ with a general automorphism of the group F^*. In the finite case, $F^* \cong \mathbb{Z}_{q-1}$. The automorphisms of a cyclic group map generators to generators, and so each automorphism is given (in $GF(q)$) by a power mapping $x \mapsto x^i$, where $(i, q-1) = 1$. Some of these automorphisms of F^* will give equivalent representations; certainly if they are related by an automorphism of F.

The set of hyperplanes H' must have some special properties which are given in the following.

THEOREM 3. *Consider a projective plane π with a group G of homologies with fixed centre V, with axis b, which is transitive on the set of points (not V nor on b) on any line through V. Suppose that G is isomorphic to the multiplicative group of some field F. Then π can be represented by a curve and a dual curve (of hyperplanes) of $PG(r-1, F)$. This curve and its dual satisfy the following properties, which are equivalent to the existence of such a plane.*

(1) *Each element of the dual curve is a hyperplane which is tangent at a unique point of the curve.*

(2) *The mapping induced between tangents and points of the curve is a bijection.*

(3) *Each point of any chord of the curve is contained in a unique hyperplane of the dual curve and this mapping is bijective.*

(4) *Each chord through two distinct points of the curve does not intersect the secundum that is the intersection of the tangent hyperplanes at a further two points of the curve.*

https://doi.org/10.1017/S0004972700016373 Published online by Cambridge University Press

The plane can be represented as a cone in $PG(r,F)$ over the curve, intersected by the hyperplanes of $PG(r,F)$, not passing through the vertex V but passing through the elements of the dual curve. The lines of the cone through V are also lines of the π.

PROOF: Most of the details have been shown before, but let us just see why the properties (1), (2), (3) and (4) should hold. (It is clear that third implies the last.) Now (1) holds because if a hyperplane h' of H' passed through two points of the base curve, then these two points would be in the two lines of the plane corresponding to the base hyperplane and any other hyperplane of H passing through h'. Next (2) holds because we must have pencils of lines of π passing through each point of the base line b. That (3) should hold comes from the consideration of two points x and y of the cone, not in the base, and on different lines of the cone through the vertex V. The line xy intersects the base hyperplane in a point z of the corresponding chord of the base curve that are on the lines Vx and Vy. There is a unique line of π passing through x and y, which implies that there is a unique hyperplane of H' passing through z. (The converse result follows from the same construction.) Through any point on the curve there is also a unique hyperplane of H'. □

In the finite case we can say even more.

THEOREM 4. *Let π be a plane of order q of type I.2 with a cyclic group of homologies G of order $q-1$, where q is a prime-power. Then the rank r of any representation preserving this group is even. (The group must have the vertex of the cone as centre and the base curve as axis.) There is also a symplectic polarity γ of the base $PG(r-1,q)$ which takes the curve (of $q+1$ points) to its dual curve of tangent hyperplanes. The plane π is self-dual. γ induces a duality of π, say σ, of order 4 if q is odd, and of order 2 (a polarity) if q is even. The group of dualities of π generated by G and σ is of order $2(q-1)$. It is dihedral in the q even case. In the odd order case it is isomorphic to the semi-direct product of G with the group of automorphisms of G of order 2 generated by $x \mapsto x^{-1}$.*

PROOF: Construct a $r \times (q+1)$ matrix Y', the i'th column of which gives the coordinates for the tangent hyperplane at the i'th point of the base curve. Let $Z := XY'$, where X is the $(q+1)\times r$ matrix defined before from the base curve. Because a point is incident with its tangent, this $(q+1)\times(q+1)$ matrix Z has a zero main diagonal. Also Theorem 3, part (3) implies that Z has the property that for any pair $i \neq j$ of rows every non-zero element of $GF(q)$ is given precisely once by a product $z_{it}{z_{jt}}^{-1}$, where neither z_{it} nor z_{jt} are zero. From this it follows quickly that the plane π is equivalent to a pair of matrices X and Y' over $F = GF(q)$, such that X is $(q+1)\times r$, Y' is $r \times (q+1)$, and every 2×2 subdeterminant of XY' is non-zero. Let i, j, and k now be integers representing distinct rows of Z. We have the following equations (where $F^* := GF(q)\setminus\{0\}$).

$$\begin{aligned}
&(1)\quad z_{ik}z_{jk}^{-1}\prod_{t\not\in\{i,j,k\}} z_{it}z_{jt}^{-1} = \prod_{f\in F^*} f;\\
&(2)\quad z_{ji}z_{ki}^{-1}\prod_{t\not\in\{i,j,k\}} z_{jt}z_{kt}^{-1} = \prod_{f\in F^*} f;\\
&(3)\quad z_{kj}z_{ij}^{-1}\prod_{t\not\in\{i,j,k\}} z_{kt}z_{it}^{-1} = \prod_{f\in F^*} f.
\end{aligned}$$

Multiplying these together gives us

$$z_{ik}z_{jk}^{-1}z_{ji}z_{ki}^{-1}z_{kj}z_{ij}^{-1} = \left(\prod_{f\in F^*} f\right)^3 = -1.$$

This implies that

$$z_{ij}z_{jk}z_{ki} + z_{ik}z_{kj}z_{ji} = 0.$$

By multiplying the rows of the matrix X by various non-zero constants, and by multiplying the columns of Y similarly, we may assume that the first column of Z contains all -1's and that the first row of Z contains all 1's (except for the zero in the top left position, of course). Then substituting $i = 1$ in the above gives $z_{jk} + z_{kj} = 0$. This, together with $z_{jj} = 0$, for all j, means that Z is skew-symmetric.

In order to show that the rank r of the representation is even we only need to note that a skew-symmetric matrix always has even rank. The rank of Z is r which must be even. Now let the rows of X be $\mathbf{x}_i$, (representing the points of the base curve); and let the columns of Y be $\mathbf{y}_j$, (representing the hyperplanes of the dual curve). From the skew-symmetric Z we have the equation $\mathbf{x}_i \cdot \mathbf{y}_j = -\mathbf{y}_i \cdot \mathbf{x}_j$, which implies that the subspace of dimension $r-1$ generated by the set of points

$$S := \{(\mathbf{x}_i, \mathbf{y}_i) \mid i = 1, \ldots, q+1\}$$

in $PG(2r-1, q)$ is totally isotropic with respect to the polarity

$$p : (\mathbf{x}, \mathbf{y}) \mapsto [\mathbf{y}, \mathbf{x}].$$

(Totally isotropic means that the subspace is fixed by p. Note that $\mathbf{x}_i\mathbf{y}_i = 0$, for all i.) But it is easy to see that every totally isotropic subspace containing no points of type $(\mathbf{x}, \mathbf{y})$ where either $\mathbf{x}$ or $\mathbf{y}$ is zero, is given by all points of type $(\mathbf{x}, D\mathbf{x})$, where D is a non-singular skew-symmetric $(r \times r)$ matrix. This implies that D corresponds to a symplectic polarity γ of $PG(r-1, q)$ which takes the base curve to its dual curve of tangent hyperplanes.

The duality d of π induced by γ can best be described after we have an algebraic formulation of the plane. Now the points of the cone are of the form $(\lambda, \mathbf{x}_i)$, where $\lambda \in GF(q)$ and $i = 1, \ldots, q+1$. The vertex is $V := (1, \mathbf{0})$. These are the points of π.

The lines of π are given by all the hyperplanes of the form $[-\mu, \mathbf{y}_i]$, where $\mu \in GF(q)$; there is also the base hyperplane $[1, \mathbf{0}]$. Incidence is given by inclusion. The duality of π is then given by

$$(\lambda, \mathbf{x}_i) \mapsto [-\lambda, \mathbf{y}_i], \quad (1, \mathbf{0}) \leftrightarrow [1, \mathbf{0}], \quad [\mu, \mathbf{y}_i] \mapsto (\mu, \mathbf{x}_i).$$

It is easy to check that this is a duality and that the order is 4 if q is odd, while the order is 2 if q is even. We leave the proof about the exact nature of the group of dualities to the reader. (It is elementary.) □

The case of q odd is analogous to the case of the real projective plane. An example of a group of dualities and homologies generated by one duality of order 4 and a transitive group of homologies is the following. Consider a circle with centre O in the Euclidean plane. The group of homologies of the plane with centre O and axis l_∞ is just the group of expansions (or blow-ups) by a non-zero factor k. A duality of order 4 can be constructed from the circle by composing the polarity associated with the circle with a rotation about the circle by $90°$. The square of this duality is the expansion by -1 ... in other words it is a reflection about O. (I am grateful to someone at the University of Kiel for this observation, and also to the hospitality shown during my visit there in early 1992.)

Let us conclude this section with some observations about the theory of curves and arcs. First, a rational curve in n-dimensional space usually has a well-defined invariant "tangent" subspace of each dimension at each of its points. For example, the curve described by the set of points $P_x := (1, f_1, \dots, f_n)$, where the f_i are polynomials in x, has a tangent line at the point P_x generated by P_x and $P'_x := (0, f'_1, \dots, f'_n)$; a tangent plane generated by P_x, P'_x, and $P''_x := (0, f''_1, \dots, f''_n)$; and so on up to the tangent hyperplane at x. (Some people use the word "osculating" to describe these spaces.) In the case of twisted cubic curves in 3-d space, and in some other examples, the mapping from point to tangent hyperplane is induced by a symplectic polarity, and indeed we have seen that if the correct conditions are satisfied, a projective plane can be constructed from the curve and its dual. It would be interesting to investigate these relationships further.

A generalisation of the case of the twisted cubics using the above theorems is given by any $(q+1)$-arc K of $PG(3, q)$, $q = 2^h$, h odd. Note that all these arcs are classified; see [1]. There is an associated symplectic polarity γ (and hyperbolic quadric) of such an arc. Let us show that the collection of tangents $\{P^\gamma \mid P \in K\}$ satisfies the conditions of Theorem 3. The arc can be given by

$$K := \{(1, x, x^\sigma, x^{\sigma+1}) \mid x \in GF(q) \cup \{\infty\}\},$$

where $\sigma = 2^i$, and $(i, h) = 1$; while the symplectic polarity is

$$(x_0, x_1, x_2, x_3) \mapsto [x_3, x_2, x_1, x_0].$$

https://doi.org/10.1017/S0004972700016373 Published online by Cambridge University Press

Using the fact that the group of homographies fixing the arc is sharply 3-transitive on its $q+1$ points we can assume that a general chord of the arc passes through $(1,0,0,0)$ and $(0,0,0,1)$. Then a general tangent plane $[x^{\sigma+1}, x^{\sigma}, x, 1]$ intersects this chord in a point $\left(1,0,0,x^{\sigma+1}\right)$. The condition must be that $x \mapsto x^{\sigma+1}$ is a permutation of $GF(q)$. We must evaluate $(\sigma+1, q-1)$. To do this we use the well-known fact that $\left(2^j-1, 2^h-1\right) = 2^{(j,h)}-1$, and so $\left(2^j-1, 2^h-1\right) = 1 \iff (j,h) = 1$; see [5]. Since $(\sigma-1, q-1) = 1$ because $(i,h) = 1$, we see that $(\sigma+1, q-1) = \left(\sigma^2-1, q-1\right) = 1 \iff (2i,h) = 1 \iff (2,h) = 1 \iff i$ is odd. We leave it as an exercise to show that there are exactly $\left(q^2+q\right)/2$ lines of $PG(3,q)$ that do not intersect any chord of K, being the images of the chords under the polarity. Perhaps we could call these "external lines". Suppose we wanted to construct a set of $q+1$ planes $\mathfrak{H}$ satisfying

(1) each plane of $\mathfrak{H}$ intersects K only at one point;

(2) each point on each chord of K is on precisely one plane of $\mathfrak{H}$.

Then each pair of planes of $\mathfrak{H}$ would have to intersect in an external line of K. On each of these lines there are two of the above tangent planes. It is not hard to see that on each tangent plane there are four distinct subsets of points.

(1) a unique point of K;

(2) $2q$ points on precisely 2 tangent planes (on the hyperbolic quadric associated with K);

(3) $\binom{q}{2}$ points on 3 tangent planes;

(4) $\binom{q}{2}$ points on 1 tangent plane, but not on K.

Thus any point, not on K, that is on only one tangent plane, is on a unique chord of K. Using the polarity of K (dualising) we see that any plane (not a tangent plane) that intersects K in only one point contains exactly one of the $\left(q^2+q\right)/2$ external lines. From this we see that there are only two possibilities for $\mathfrak{H}$. Either it is the set of $q+1$ tangent planes; or $\mathfrak{H}$ is the set of all the planes passing through one of the external lines (but this is a degenerate case). In both cases, however, the plane π constructed is isomorphic to $PG(2,q)$.

Note that the $(q+1)$-arcs in $PG(3,q)$, where $q \equiv -1 \pmod 3$, have also been used in the construction of both Hering planes (for q odd), and Schäffer planes (for q even). These are translation planes of order q^2, on which $SL(2,q)$ acts as a group of collineations. See [6] for further details.

Further Problems

Finally, let us present a list of problems, which may be a guide for a further development of this theory.

https://doi.org/10.1017/S0004972700016373 Published online by Cambridge University Press

(1) Classify all the representations of given OA's and develop a theory (in the same spirit as the theory of group representations). How should we define irreducible representations in this theory? Are *equivalent* representations those which are related by a collineation of the ambient projective space?

(2) Given an OA of prime-power or infinite order, what is its minimal rank?

(3) There are two methods which could be used to try to construct a representation of an OA. One could choose a certain cone C, then construct the set of hyperplanes H; or one could first choose the set H and find a maximal cone that satisfies the conditions of Theorem 1. (This latter method has the advantage of always giving an OA.)

(4) It is known that there are many OA's with a large group of automorphisms: for example, finite translation planes of order q give an OA with an elementary abelian group. If this group (or a subgroup) induces a group of collineations fixing the representation then it makes the construction of the C and H much easier. Then group representation theory can also be used.

(5) Is there an easy way to tell if two representations give the same OA?

(6) Theorem 2 has some interest in the theory of Laguerre planes, because of the association of embeddability in 3-dimensional space with the *bundle theorem*. It could be interesting to investigate this connection further.

(7) It is easy to see that given a representation of an OA it is usually possible to change the substitution on one of the generators (or rows of the matrix) so that the rank it increased by one. However, this new representation is somehow *degenerate*. Can this matter be clarified?

(8) In the case of k-arcs (when $r = s$), and their corresponding MDS codes there is a theory of orthogonal duality: from the matrix A of rank s that gives the k-$OA(q,s)$ one constructs the matrix $A^{\perp}$ of all columns which are orthogonal to every column of A — thus $r(A^{\perp}) = k - s$ and the dual orthogonal array has parameters k-$OA(q, k-s)$. Can this idea be extended to general representations?

(9) The representations of the OA corresponding to the affine plane over a field could be very interesting to classify.

(10) Theorems 3 and 4 about projective planes with special groups can be easily generalised to Laguerre planes. A Laguerre plane with a special circle and a "group of homologies" fixing this circle and being isomorphic to the multiplicative group of a field of the same order can be embedded in projective space as a cone C over a base curve K. In this case, however, K has a 2-dimensional set H'' of hyperplanes associated with it. The main condition is that every plane on three distinct points of K has the property that each of its points is on a unique hyperplane of H''. Since the known finite Laguerre planes have this type of group it would be also interesting to classify the curves and associated sets of hyperplanes that have this property. Infinite constructions

https://doi.org/10.1017/S0004972700016373 Published online by Cambridge University Press

would also be of interest.

References

[1] L.R.A. Casse and D.G. Glynn, 'The solution to Beniamino Segre's problem $I_{r,q}$, $r = 3$, $q = 2^h$', *Geom. Dedicata* **13** (1982), 157–164.

[2] P. Dembowski, *Finite geometries* (Springer-Verlag, Berlin, Heidelberg, New York, 1968).

[3] D.G. Glynn, 'The non-classical 10-arc of $PG(4,9)$', *Discrete Math.* **59** (1986), 43–51.

[4] D.G. Glynn and G.F. Steinke, 'Laguerre planes of even order and translation ovals', *Geom. Dedicata* (to appear).

[5] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and Its Applications **20** (Cambridge University Press, Cambridge, 1983).

[6] H. Lüneburg, *Translation planes* (Springer-Verlag, Berlin, Heidelberg, New York, 1980).

Department of Mathematics and Statistics
University of Canterbury
Christchurch
New Zealand
e-mail dgg@math.canterbury.ac.nz

https://doi.org/10.1017/S0004972700016373 Published online by Cambridge University Press