Orthogonal arrays from Hermitian varieties

A. Aguglia * L. Giuzzi *

Abstract

A simple orthogonal array $OA(q^{2n-1}, q^{2n-2}, q, 2)$ is constructed by using the action of a large subgroup of $PGL(n+1, q^2)$ on a set of non–degenerate Hermitian varieties in $PG(n, q^2)$.

Keywords: Orthogonal array; Hermitian variety; collineation.

1 Introduction

Let $\mathcal{Q} = \{0, 1, \ldots, q-1\}$ be a set of q symbols and consider a $(k \times N)$–matrix A with entries in $\mathcal{Q}$. The matrix A is an *orthogonal array* with q levels and strength t, in short an $OA(N, k, q, t)$, if any $(t \times N)$–subarray of A contains each $t \times 1$–column with entries in $\mathcal{Q}$, exactly $\mu = N/q^t$ times. The number μ is called the *index* of the array A. An orthogonal array is *simple* when it does not contain any repeated column.

Orthogonal arrays were first considered in the early Forties, see Rao [9, 10], and have been intensively studied ever since, see [13]. They have been widely used in statistic, computer science and cryptography.

There are also remarkable links between these arrays and affine designs, see [12, 14]. In particular, an $OA(q\mu_1, k, q, 1)$ exists if and only if there is a resolvable $1-(q\mu_1, \mu_1, k)$ design. Similarly, the existence of an $OA(q^2\mu_2, k, q, 2)$, is equivalent to that of an affine $1-(q^2\mu_2, q\mu_2, k)$ design, see [12]

A general procedure for constructing an orthogonal array depends on homogeneous forms $f_1, \ldots, f_k$, defined over a subset $\mathcal{W} \subseteq \mathrm{GF}(q)^{n+1}$. The array

$$A(f_1, \ldots, f_k; \mathcal{W}) = \left\{ \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_k(x) \end{pmatrix} : x \in \mathcal{W} \right\},$$

*Research supported by the Italian Ministry MIUR, Strutture geometriche, combinatoria e loro applicazioni.

with an arbitrary order of columns, provides an orthogonal array if the size of the intersection $V(f_i) \cap V(f_j) \cap \mathcal{W}$ for distinct varieties $V(f_i)$ and $V(f_j)$, is independent of the choice of i, j. Here $V(f)$ denotes the algebraic variety associated to f. This procedure was applied for linear functions by Bose [3], and for quadratic functions by Fuji-Hara and Miyamoto [5, 6].

In this paper, we construct a simple orthogonal array $\mathcal{A}_0 = OA(q^{2n-1}, q^{2n-2}, q, 2)$ by using the above procedure for Hermitian forms. To do this we look into the action of a large subgroup of $PGL(n+1, q^2)$ on a set of non–degenerate Hermitian varieties in $PG(n, q^2)$. The resulting orthogonal array $\mathcal{A}_0$ is closely related to an affine $2-(q^{(2n-1)}, q^{2(n-1)}, q^{(2n-3)} + \ldots + q + 1)$ design $\mathcal{S}$, that for $q \geq 2$, provides a non–classical model of the $(2n-1)$–dimensional affine space $AG(2n-1, q)$. Precisely, the points of $\mathcal{S}$ are labelled by the columns of $\mathcal{A}_0$, some parallel classes of $\mathcal{S}$ correspond to the rows of $\mathcal{A}_0$ and each of the q parallel blocks associated to a given row of $\mathcal{A}_0$ is labelled by one of the q different symbols in that row.

2 Preliminary results on Hermitian varieties

Let $\Sigma = PG(n, q^2)$ be the desarguesian projective space of dimension n over $\mathrm{GF}(q^2)$ and denote by $X = (x_1, x_2, \ldots, x_{n+1})$ homogeneous coordinates for its points. The hyperplane $\Sigma_\infty : X_{n+1} = 0$ will be taken as the hyperplane at infinity.

We use σ to write the involutory automorphism of $\mathrm{GF}(q^2)$ which leaves all the elements of the subfield $\mathrm{GF}(q)$ invariant. A Hermitian variety $\mathcal{H}(n, q^2)$ is the set of all points X of Σ which are self conjugate under a Hermitian polarity h. If H is the Hermitian $(n+1) \times (n+1)$–matrix associated to h, then the Hermitian variety $\mathcal{H}(n, q^2)$ has equation

$$XH(X^\sigma)^T = 0.$$

When A is non–singular, the corresponding Hermitian variety is *non–degenerate*, whereas if A has rank n, the related variety is a *Hermitian cone*. The radical of a Hermitian cone, that is the set $\{Y \in \Sigma |\ YH(X^\sigma)^T = 0\ \forall X \in \Sigma\}$, consists of one point, the *vertex* of the cone.

All non–degenerate Hermitian varieties are projectively equivalent; a possible canonical equation is

$$X_1^{q+1} + \ldots + X_{n-1}^{q+1} + X_n^q X_{n+1} + X_n X_{n+1}^q = 0, \tag{1}$$

where the polynomial on the left side of (1) is a *Hermitian form*. All Hermitian cones of Σ are also projectively equivalent.

A non–degenerate Hermitian variety $\mathcal{H}(n, q^2)$ of Σ has several remarkable properties, see [11, 7]; here we just recall the following.

(1) The number of points on $\mathcal{H}(n, q^2)$ is

$$\mu_n(q) = q^{2n-1} + q(q^{n-\epsilon} + \ldots + q^{2n-4}) + q^{n+\epsilon-2} + \ldots + q^2 + 1,$$

where $\epsilon = 0$ or 1, according as n is even or odd.

(2) A maximal subspace of Σ included in $\mathcal{H}(n, q^2)$ has dimension

$$\left\lfloor \frac{n-1}{2} \right\rfloor .$$

These maximal subspaces are called *generators* of $\mathcal{H}(n, q^2)$.

(3) Any line of Σ meets $\mathcal{H}(n, q^2)$ in 1, $q+1$ or q^2+1 points. The lines meeting $\mathcal{H}$ in one point are called *tangent lines.*

(4) The polar hyperplane π_P with respect to h of a point P on $\mathcal{H}(n, q^2)$ is the locus of the lines through P either contained in $\mathcal{H}(n, q^2)$ or tangent to it at P. This hyperplane π_P is also called the *tangent hyperplane* at P of $\mathcal{H}(n, q^2)$. Furthermore,

$$|\mathcal{H}(n, q^2) \cap \pi_P| = 1 + q^2 \mu_{n-2}(q).$$

(5) Every hyperplane π of Σ which is not a tangent hyperplane of $\mathcal{H}(n, q^2)$ meets $\mathcal{H}(n, q^2)$ in a non–degenerate Hermitian variety $\mathcal{H}(n-1, q^2)$ of π.

In Section 4 we shall make extensive use of non–degenerate Hermitian varieties, together with Hermitian cones of vertex the point $P_\infty(0, 0, \ldots, 1, 0)$. Let $AG(n, q^2) = \Sigma \setminus \Sigma_\infty$ be the affine space embedded in Σ. We may provide an affine representation for the Hermitian cones with vertex at P_∞ as follows.

Let ε be a primitive element of $\mathrm{GF}(q^2)$. Take a point $(a_1, \ldots, a_{n-1}, 0)$ on the affine hyperplane $\Pi : X_n = 0$ of $AG(n, q^2)$. We can always write $a_i = a_i^1 + \varepsilon a_i^2$ for any $i = 1, \ldots, n-1$. There is thus a bijective correspondence ϑ between the points of Π and those of $AG(2n-2, q)$,

$$\vartheta(a_1, \ldots, a_{n-1}, 0) = (a_1^1, a_1^2, \ldots, a_{n-1}^1, a_{n-1}^2).$$

Pick now a hyperplane π' in $AG(2n-2, q)$ and consider its pre–image $\pi = \vartheta^{-1}(\pi')$ in Π. The set of all the lines $P_\infty X$ with $X \in \pi$ is a Hermitian cone of vertex P_∞. The set π is a basis of this cone.

Let $T_0 = \{t \in \mathrm{GF}(q^2) : \mathrm{tr}(t) = 0\}$, where $\mathrm{tr} : x \in \mathrm{GF}(q^2) \mapsto x^q + x \in \mathrm{GF}(q)$ is the trace function. Then, such an Hermitian cone $\mathcal{H}_{\omega,v}$ is represented by

$$\omega_1^q X_1 - \omega_1 X_1 + \omega_2^q X_2^q - \omega_2 X_2 + \ldots + \omega_{n-1}^q X_{n-1}^q - \omega_{n-1} X_{n-1} = v, \qquad (2)$$

where $\omega_i \in \mathrm{GF}(q^2)$, $v \in T_0$ and there exists at least one $i \in \{1, \ldots, n-1\}$ such that $\omega_i \neq 0$.

3 Construction

In this section we provide a family of simple orthogonal arrays $OA(q^{2n-1}, q^{2n-2}, q, 2)$, where n is a positive integer and q is any prime power. Several constructions based on finite fields of orthogonal arrays are known, see for instance [3, 5, 6]. The construction of [3] is based upon linear transformations over finite fields. Non–linear functions are used in [5, 6]. In [6], the authors dealt with a subgroup of $PGL(4, q)$, in order to obtain suitable quadratic functions in 4 variables; then, the domain $\mathcal{W}$ of these functions was appropriately restricted, thus producing an orthogonal array $OA(q^3, q^2, q, 2)$. The construction used in the aforementioned papers starts from k distinct multivariate functions $f_1, \ldots, f_k$, all with a common domain $\mathcal{W} \subseteq \mathrm{GF}(q)^{n+1}$, which provide an array

$$A(f_1, \ldots, f_k; \mathcal{W}) = \left\{ \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_k(x) \end{pmatrix} : x \in \mathcal{W} \right\},$$

with an arbitrary order of columns.

In general, it is possible to generate functions f_i starting from homogeneous polynomials in $n+1$ variables and considering the action of a subgroup of the projective group $PGL(n+1, q)$. Indeed, any given homogeneous polynomial f is associated to a variety $V(f)$ in Σ of equation

$$f(x_1, \ldots, x_{n+1}) = 0.$$

The image $V(f)^g$ of $V(f)$ under the action of an element $g \in PGL(n+1, q)$ is a variety $V(f^g)$ of Σ, associated to the polynomial f^g.

A necessary condition for $A(f_1, \ldots, f_k; \mathcal{W})$ to be an orthogonal array, when all the f_i's are homogeneous, is that $|V(f_i) \cap V(f_k) \cap \mathcal{W}|$ is independent of the choice of i, j, whenever $i \neq j$.

Here, we consider homogeneous polynomials which are Hermitian forms of $\mathrm{GF}(q^2)[X_1, \ldots, X_n, X_{n+1}]$. Denote by G the subgroup of $PGL(n+1, q^2)$ consisting of all collineations represented by

$$\alpha(X'_1, \ldots, X'_{n+1}) = (X_1, \ldots, X_{n+1})M$$

where $\alpha \in GF(q^2) \setminus \{0\}$, and

$$M = \begin{pmatrix} 1 & 0 & \dots & 0 & j_1 & 0 \\ 0 & 1 & \dots & 0 & j_2 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & & 1 & j_{n-1} & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 \\ i_1 & i_2 & \dots & i_{n-1} & i_n & 1 \end{pmatrix}^{-1}, \tag{3}$$

with $i_s,\ j_m \in \mathrm{GF}(q^2)$. The group G has order $q^{2(2n-1)}$. It stabilises the hyperplane Σ_∞, fixes the point $P_\infty(0,\dots,0,1,0)$ and acts transitively on $AG(n,q^2)$.

Let $\mathcal{H}$ be the non–degenerate Hermitian variety associated to the Hermitian form

$$F = X_1^{q+1} + \dots + X_{n-1}^{q+1} + X_n^q X_{n+1} + X_n X_{n+1}^q.$$

The hyperplane Σ_∞ is the tangent hyperplane at P_∞ of $\mathcal{H}$. The Hermitian form associated to the variety $\mathcal{H}^g$, as g varies in G, is

$$\begin{aligned} F^g = X_1^{q+1} + \dots + X_{n-1}^{q+1} + X_n^q X_{n+1} + X_n X_{n+1}^q + X_{n+1}^{q+1}(i_1^{q+1} + \dots + i_{n-1}^{q+1} + i_n^q + i_n) \\ + \operatorname{tr}\left(X_{n+1}^q(X_1(i_1^q + j_1) + \dots + X_{n-1}(i_{n-1}^q + j_{n-1}))\right) \end{aligned} \tag{4}$$

The subgroup Ψ of G preserving $\mathcal{H}$ consists of all collineations whose matrices satisfy the condition

$$\begin{cases} j_1 = -i_1^q \\ \vdots \\ j_{n-1} = -i_{n-1}^q \\ i_1^{q+1} + \dots + i_{n-1}^{q+1} + i_n^q + i_n = 0 \end{cases}.$$

Thus, Ψ contains $q^{(2n-1)}$ collineations and acts on the affine points of $\mathcal{H}$ as a sharply transitive permutation group. Let $C = \{a_1 = 0, \dots, a_q\}$ be a system of representatives for the cosets of T_0, viewed as an additive subgroup of $\mathrm{GF}(q^2)$. Furthermore, let $\mathcal{R}$ denote the subset of G whose collineations are induced by

$$M' = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 \\ i_1 & i_2 & \dots & i_{n-1} & i_n & 1 \end{pmatrix}^{-1}, \tag{5}$$

where $i_1, \ldots, i_{n-1} \in GF(q^2)$, and for each tuple $(i_1, \ldots, i_{n-1})$, the element i_n is the unique solution in C of equation

$$i_1^{q+1} + \ldots + i_{n-1}^{q+1} + i_n^q + i_n = 0. \tag{6}$$

The set $\mathcal{R}$ has cardinality q^{2n-2} and can be used to construct a set of Hermitian form $\{F^g | g \in \mathcal{R}\}$ whose related varieties are pairwise distinct.

Theorem 3.1. *For any given prime power q, the matrix $\mathcal{A} = A(F^g, g \in \mathcal{R}; \mathcal{W})$, where*

$$\mathcal{W} = \{(x_1, \ldots, x_{n+1}) \in \mathrm{GF}(q^2)^{n+1} : x_{n+1} = 1\},$$

is an $OA(q^{2n}, q^{2n-2}, q, 2)$ of index $\mu = q^{2n-2}$.

Proof. It is sufficient to show that the number of solutions in $\mathcal{W}$ to the system

$$\begin{cases} F(X_1, X_2, \ldots, X_n, X_{n+1}) = \alpha \\ F^g(X_1, X_2, \ldots, X_n, X_{n+1}) = \beta \end{cases} \tag{7}$$

is q^{2n-2} for any α, $\beta \in \mathrm{GF}(q)$, $g \in \mathcal{R} \setminus \{id\}$. By definition of $\mathcal{W}$, this system is equivalent to

$$\begin{cases} X_1^{q+1} + \ldots + X_{n-1}^{q+1} + X_n^q + X_n = \alpha \\ X_1^{q+1} + \ldots + X_{n-1}^{q+1} + X_n^q + X_n + \mathrm{tr}\left(X_1 i_1^q + \ldots + X_{n-1} i_{n-1}^q\right) = \beta \end{cases} \tag{8}$$

Subtracting the first equation from the second we get

$$\mathrm{tr}(X_1 i_1^q + \ldots + X_{n-1} i_{n-1}^q) = \gamma, \tag{9}$$

where $\gamma = \beta - \alpha$. Since g in not the identity then, $(i_1^q, \ldots, i_{n-1}^q) \neq (0, \ldots, 0)$, and hence Equation (9) is equivalent to the union of q linear equations over $\mathrm{GF}(q^2)$ in $X_1, \ldots, X_{n-1}$. Thus, there are q^{2n-3} tuples $(X_1, \ldots, X_{n-1})$ satisfying (9). For each such a tuple, (8) has q solutions in X_n that provide a coset of T_0 in $\mathrm{GF}(q^2)$. Therefore, the system (7) has q^{2n-2} solutions in $\mathcal{W}$ and the result follows. $\square$

The array $\mathcal{A}$ of Theorem 3.1 is not simple since

$$F^g(x_1, \ldots, x_n, 1) = F^g(x_1, \ldots, x_n + r, 1) \tag{10}$$

for any $g \in \mathcal{R}$, and $r \in T_0$.

We now investigate how to extract a subarray $\mathcal{A}_0$ of $\mathcal{A}$ which is simple. We shall need a preliminary lemma.

Lemma 3.2. *Let $x \in \mathrm{GF}(q^2)$ and suppose $\mathrm{tr}(\alpha x) = 0$ for any $\alpha \in \mathrm{GF}(q^2)$. Then, $x = 0$.*

Proof. Consider $\mathrm{GF}(q^2)$ as a 2–dimensional vector space over $\mathrm{GF}(q)$. By [8, Theorem 2.24], for any linear mapping $\Xi : \mathrm{GF}(q^2) \to \mathrm{GF}(q)$, there exists exactly one $\alpha \in \mathrm{GF}(q^2)$ such that $\Xi(x) = \mathrm{tr}(\alpha x)$. In particular, if $\mathrm{tr}(\alpha x) = 0$ for any $\alpha \in \mathrm{GF}(q^2)$, then x, is in the kernel of all linear mappings Ξ. It follows that $x = 0$. $\square$

Theorem 3.3. *For any prime power q, the matrix $\mathcal{A}_0 = A(F^g, g \in \mathcal{R}, \mathcal{W}_0)$, where*

$$\mathcal{W}_0 = \{(x_1, \ldots, x_{n+1}) \in \mathcal{W} : x_n \in C\}$$

is a simple $OA(q^{2n-1}, q^{2n-2}, q, 2)$ of index $\mu = q^{2n-3}$.

Proof. We first show that $\mathcal{A}_0$ does not contain any repeated column. Let $\mathcal{A}$ be the array introduced in Theorem 3.1, and index its columns by the corresponding elements in $\mathcal{W}$. Observe that the column $(x_1, \ldots, x_n, 1)$ is the same as $(y_1, \ldots, y_n, 1)$ in A if, and only if,

$$F^g(x_1, \ldots, x_n, 1) = F^g(y_1, \ldots, y_n, 1),$$

for any $g \in \mathcal{R}$. We thus obtain a system of q^{2n-2} equations in the $2n$ indeterminates $x_1, \ldots x_n, y_1, \ldots, y_n$. Each equation is of the form

$$\mathrm{tr}(x_n - y_n) = \sum_{t=1}^{n-1} \left(y_t^{q+1} - x_t^{q+1} + \mathrm{tr}(a_t(y_t - x_t))\right), \tag{11}$$

where the elements $a_t = i_t^q$ vary in $\mathrm{GF}(q^2)$ in all possible ways. The left hand side of the equations in (11) does not depend on the elements a_t; in particular, for $a_1 = a_2 = \ldots = a_t = 0$ we have,

$$\mathrm{tr}(x_n - y_n) = \sum_{t=1}^{n-1} (y_t^{q+1} - x_t^{q+1});$$

hence,

$$\sum_{t=1}^{n-1} (y_t^{q+1} - x_t^{q+1}) = \sum_{t=1}^{n-1} \left(y_t^{q+1} - x_t^{q+1} + \mathrm{tr}(a_t(y_t - x_t))\right)$$

Thus, $\sum_{t=1}^{n-1} \mathrm{tr}(a_t(y_t - x_t)) = 0$. By the arbitrariness of the coefficients $a_t \in \mathrm{GF}(q^2)$, we obtain that for any $t = 1, \ldots n-1$, and any $\alpha \in \mathrm{GF}(q^2)$,

$$\mathrm{tr}(\alpha(y_t - x_t)) = 0.$$

Lemma 3.2 now yields $x_t = y_t$ for any $t = 1, \ldots, n-1$ and we also get from (11)

$$\mathrm{tr}(x_n - y_n) = 0.$$

Thus, x_n and y_n are in the same coset of T_0. It follows that two columns of $\mathcal{A}$ are the same if and only if the difference of their indexes in $\mathcal{W}$ is a vector of the form $(0,0,0,\ldots,0,r,0)$ with $r \in T_0$. By construction, there are no two distinct vectors in $\mathcal{W}_0$ whose difference is of the required form; thus, $\mathcal{A}_0$ does not contain repeated columns.

The preceding argument shows that the columns of $\mathcal{A}$ are partitioned into q^{2n-1} classes, each consisting of q repeated columns. Since $\mathcal{A}_0$ is obtained from $\mathcal{A}$ by deletion of $q-1$ columns in each class, it follows that $\mathcal{A}_0$ is an $OA(q^{2n-1}, q^{2n-2}, q, 2)$ of index q^{2n-3}. □

4 A non–classical model of $AG(2n-1,q)$

We keep the notation introduced in the previous sections. We are going to construct an affine $2-\left(q^{2n-1}, q^{2n-2}, q^{(2n-3)}+\ldots+q+1\right)$ design $\mathcal{S}$ that, as we will see, is related to the array A_0 defined in Theorem 3.3. Our construction is a generalisation of [1].

Let again consider the subgroup G of $PGL(n+1,q^2)$ whose collineations are induced by matrices (3). The group G acts on the set of all Hermitian cones of the form (2) as a permutation group. In this action, G has $q^{(2n-3)}+\ldots+1$ orbits, each of size q. In particular the $q^{(2n-3)}+\ldots+1$ Hermitian cones $\mathcal{H}_{\omega,0}$ of affine equation

$$\omega_1^q X_1 - \omega_1 X_1 + \omega_2^q X_2^q - \omega_2 X_2 + \ldots + \omega_{n-1}^q X_{n-1}^q - \omega_{n-1} X_{n-1} = 0, \qquad (12)$$

with $(\omega_1,\ldots,\omega_{n-1}) \in GF(q^2)^{n-1} \setminus \{(0,\ldots,0)\}$, constitute a system of representatives for these orbits.

The stabiliser in G of the origin $O(0,\ldots,0,1)$ fixes the line OP_∞ point–wise, while is transitive on the points of each other line passing through P_∞. Furthermore, the centre of G comprises all collineations induced by

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & & 1 & 0 & 0 \\ 0 & 0 & \ldots & 0 & 1 & 0 \\ 0 & 0 & \ldots & 0 & i_n & 1 \end{pmatrix}^{-1}, \qquad (13)$$

with $i_n \in GF(q^2)$. The subset of (13) with $i_n \in T_0$ induces a normal subgroup N of G acting semiregularly on the affine points of $AG(n,q^2)$ and preserving each line parallel to the X_n-axis. Furthermore, N is contained in Ψ and also preserves every affine Hermitian cone $\mathcal{H}_{\omega,v}$.

We may now define an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$ as follows. The set $\mathcal{P}$ consists of all the point–orbits of $AG(n, q^2)$ under the action of N. Write $N(x_1, \ldots, x_n)$ for the orbit of the point $(x_1, \ldots, x_n)$ in $AG(n, q^2)$under the action of N.

The elements of $\mathcal{B}$ are the images of the Hermitian variety $\mathcal{H}$ of affine equation

$$X_1^{q+1} + \ldots + X_{n-1}^{q+1} + X_n^q + X_n = 0, \tag{14}$$

together with the images of the Hermitian cones (12) under the action of G. If a block $B \in \mathcal{B}$ arises from (14), then it will be called *Hermitian–type*, whereas if B arises from (12), it will be *cone–type*. Incidence is given by inclusion.

Theorem 4.1. *The aforementioned incidence structure $\mathcal{S}$ is an affine*

$$2 - (q^{(2n-1)}, q^{2(n-1)}, q^{(2n-3)} + \ldots + q + 1)$$

design, isomorphic, for $q > 2$, to the point–hyperplane design of the affine space $AG(2n-1, q)$.

Proof. By construction, $\mathcal{S}$ has q^{2n-1} points and $q^{(2n-1)} + q^{2(n-1)} \ldots + q$ blocks, each block consisting of $q^{2(n-1)}$ points.

We first prove that the number of blocks through any two given points is $q^{(2n-3)} + \ldots + q + 1$. Since $\mathcal{S}$ has a point–transitive automorphism group, we may assume, without loss of generality, one of these points to be $O = N(0, \ldots, 0)$. Let $A = N(x_1, x_2, \ldots, x_n)$ be the other point. We distinguish two cases, according as the points lie on the same line through P_∞ or not.

We begin by considering the case $(0, 0, \ldots, 0) \neq (x_1, x_2, \ldots, x_{n-1})$. The line ℓ represented by $X_1 = x_1, \ldots, X_{n-1} = x_{n-1}$, is a secant to the Hermitian variety $\mathcal{H}$. Since the stabiliser of the origin is transitive on the points of ℓ, we may assume that $A \subseteq \mathcal{H}$; in particular, $(x_1, x_2, \ldots, x_n) \in \mathcal{H}$ and

$$x_1^{q+1} + \ldots + x_{n-1}^{q+1} + x_n^q + x_n = 0. \tag{15}$$

Observe that this condition is satisfied by every possible representative of A. Another Hermitian type block arising from the variety $\mathcal{H}^g$ associated to the form (4), contains the points O and A if and only if

$$i_1^{q+1} + \ldots + i_{n-1}^{q+1} + i_n^q + i_n = 0 \tag{16}$$

and

$$\begin{gathered} x_1^{q+1} + \ldots + x_{n-1}^{q+1} + x_n^q + x_n + x_1^q(i_1 + j_1^q) + \ldots + x_{n-1}^q(i_{n-1} + j_{n-1}^q) + \\ + x_1(i_1^q + j_1) + \ldots + x_{n-1}(i_{n-1}^q + j_{n-1}) + i_1^{q+1} + \ldots + i_{n-1}^{q+1} + i_n^q + i_n = 0. \end{gathered} \tag{17}$$

Given (15) and (16), Equation (17) becomes

$$\mathrm{tr}(x_1(i_1^q + j_1) + \ldots + x_{n-1}(i_{n-1}^q + j_{n-1})) = 0 \tag{18}$$

Condition (16) shows that there are q^{2n-1} possible choices for the tuples $\mathbf{i} = (i_1, \ldots, i_n)$; for any such a tuple, because of (18), we get q^{2n-3} values for $\mathbf{j} = (j_1, \ldots, j_{n-1})$. Therefore, the total number of Hermitian–type blocks through the points O and A is exactly

$$\frac{q^{4(n-1)}}{q^{2n-1}} = q^{2n-3}.$$

On the other hand, cone–type blocks containing O and A are just cones with basis a hyperplane of $AG(2n-2, q)$, through the line joining the affine points $(0, \ldots, 0)$ and $\theta(x_1, \ldots, x_{n-1}, 0)$; hence, there are precisely $q^{2n-4} + \ldots + q + 1$ of them.

We now deal with the case $(x_1, x_2, \ldots, x_{n-1}) = (0, 0, \ldots, 0)$. A Hermitian–type block through $(0, \ldots, 0)$ meets the X_n-axis at points of the form $(0, \ldots, 0, r)$ with $r \in T_0$. Since $x_n \notin T_0$, no Hermitian–type block may contain both O and A. On the other hand, there are $q^{2n-3} + \ldots + q + 1$ cone-type blocks through the two given points that is, all cones with basis a hyperplane in $AG(2n-2, q)$ containing the origin of the reference system in $AG(2n-2, q)$. It follows that $\mathcal{S}$ is a $2 - (q^{(2n-1)}, q^{2(n-1)}, q^{(2n-3)} + \ldots + q + 1)$ design.

Now we recall that two blocks of a design may be defined parallel if they are either coincident or disjoint. In order to show that $\mathcal{S}$ is indeed an affine design we need to check the following two properties, see [4, Section 2.2, page 72]:

(a) any two distinct blocks either are disjoint or have q^{2n-3} points in common;

(b) given a point $N(x_1, \ldots, x_n) \in \mathcal{P}$ and a block $B \in \mathcal{B}$ such that $N(x_1, \ldots, x_n) \notin B$, there exists a unique block $B' \in \mathcal{B}$ satisfying both $N(x_1, \ldots, x_n) \in B'$ and $B \cap B' = \emptyset$.

We start by showing that (a) holds for any two distinct Hermitian–type blocks. As before, we may suppose one of them to be $\mathcal{H}$ and denote by $\mathcal{H}^g$ the other one, associated to the form (4). We need to solve the system of equations given by (15) and (17). Subtracting (15) from (17),

$$\mathrm{tr}(x_1(i_1^q + j_1) + \ldots + x_{n-1}(i_{n-1}^q + j_{n-1})) = \gamma, \tag{19}$$

where $\gamma = -(i_1^{q+1} + \ldots + i_{n-1}^{q+1} + i_n^q + i_n)$.

Suppose that $(i_1^q + j_1, \ldots, i_{n-1}^q + j_{n-1}) \neq (0, \ldots, 0)$. Arguing as in the proof of Theorem 3.1, we see that there are q^{2n-3} tuples $(x_1, \ldots, x_{n-1})$ satisfying (19) and, for each such a tuple, (15) has q solutions in x_1. Thus, the system given by (15) and (17) has q^{2n-2} solutions; taking into account the definition of a point of $\mathcal{S}$, it follows that the number of the common points of the two blocks under consideration is indeed q^{2n-3}.

In the case $(i_1^q + j_1, \ldots, i_{n-1}^q + j_{n-1}) = (0, \ldots, 0)$, either $\gamma \neq 0$ and the two blocks are disjoint, or $\gamma = 0$ and the two blocks are the same.

We now move to consider the case wherein both blocks are cone–type. The bases of these blocks are either disjoint or share $q^{2(n-2)}$ affine points; in the former case, the blocks are disjoint; in the latter, they have $q^{2(n-2)}$ lines in common. Since each line of $AG(n, q^2)$ consists of q points of $\mathcal{S}$, the intersection of the two blocks has size q^{2n-3}.

We finally study the intersection of two blocks of different type. We may assume again the Hermitian–type block to be $\mathcal{H}$. Let then $\mathcal{C}$ be cone–type. Each generator of $\mathcal{C}$ meets the Hermitian variety $\mathcal{H}$ in q points which form an orbit of N. Therefore, the number of common points between the two blocks is, as before, q^{2n-3}; this completes the proof of (a).

We are going to show that property (b) is also satisfied. By construction, any cone–type block meets every Hermitian–type block. Assume first B to be the Hermitian variety $\mathcal{H}$ and $P = N(x_1, x_2, \ldots, x_n) \not\subseteq \mathcal{H}$. Since we are looking for a block B' through P, disjoint from $\mathcal{H}$, also B' must be Hermitian–type. Let β be the collineation induced by

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & & 1 & 0 & 0 \\ 0 & 0 & \ldots & 0 & 1 & 0 \\ 0 & 0 & \ldots & 0 & i_n & 1 \end{pmatrix}^{-1},$$

with $i_n^q + i_n + x_1^{q+1} + \ldots + x_{n-1}^{q+1} + x_n^q + x_n = 0$. Then, the image B' of $\mathcal{H}$ under β is disjoint from $\mathcal{H}$ and contains the set P. To prove the uniqueness of the block satisfying condition (b), assume that there is another block $\widetilde{B}$, which is the image of $\mathcal{H}$ under the collineation ω induced by

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & b_1 & 0 \\ 0 & 1 & \ldots & 0 & b_2 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & & 1 & b_{n-1} & 0 \\ 0 & 0 & \ldots & 0 & 1 & 0 \\ a_1 & a_2 & \ldots & a_{n-1} & a_n & 1 \end{pmatrix}^{-1},$$

and such that $\widetilde{B} \cap \mathcal{H} = \emptyset$ and $P \subseteq \widetilde{B}$. As $\widetilde{B}$ and $\mathcal{H}$ are disjoint, the system given by (15) and

$$\begin{aligned} x_1^{q+1}+\ldots+x_{n-1}^{q+1}+x_n^q+x_n+x_1^q(a_1+b_1^q)+\ldots+x_{n-1}^q(a_{n-1}+b_{n-1}^q)+\\ +x_1(a_1^q+b_1)+\ldots+x_{n-1}(a_{n-1}^q+b_{n-1})+a_1^{q+1}+\ldots+a_{n-1}^{q+1}+a_n^q+a_n=0. \end{aligned} \tag{20}$$

must have no solution. Arguing as in the proof of (a), we see that this implies that $(a_1^q+b_1,\ldots,a_{n-1}^q+b_{n-1})=(0,\ldots,0)$. On the other hand, $P\in\widetilde{B}\cap B'$ yields $i_n^q+i_n+a_1^{q+1}+\ldots+a_{n-1}^{q+1}+a_n^q+a_n=0$, that is $\omega^{-1}\beta$ is in the stabiliser Ψ of $\mathcal{H}$ in G; hence, $B'=\widetilde{B}$.

Now, assume B to be a cone-type block. Denote by π its basis and let $P'=(x_1^1,x_1^2,\ldots,x_{n-1}^1,x_{n-1}^2)$ be the image $\vartheta(x_1,\ldots,x_{n-1},0)$ on the affine space $AG(2n-2,q)$ identified, via ϑ, with the affine hyperplane $X_n=0$. In $AG(2n-2,q)$ there is a unique hyperplane π' passing trough the point P' and disjoint from π. This hyperplane π' uniquely determines the block B' with property (b).

In order to conclude the proof of the current theorem we shall require a deep characterisation of the high–dimensional affine space, namely that an affine design $\mathcal{S}$ such that $q>2$, is an affine space if and only if every line consists of exactly q points, see [4, Theorem 12, p. 74].

Recall that the line of a design $\mathcal{D}$ through two given points L,M is defined as the set of all points of $\mathcal{D}$ incident to every block containing both L and M. Thus, choose two distinct points in $\mathcal{S}$. As before, we may assume that one of them is $O=N(0,\ldots,0)$ and let $A=N(x_1,\ldots,x_n)$ be the other one.

Suppose first that A lies on the X_n-axis. In this case, as we have seen before, there are exactly $q^{2n-3}+\ldots+q+1$ blocks incident to both O and A, each of them cone–type. Their intersection consists of q points of $\mathcal{S}$ on the X_n-axis.

We now examine the case where A is not on the X_n-axis. As before, we may assume that $A\subseteq\mathcal{H}$, hence (15) holds. Exactly $q^{2n-3}+\ldots+q+1$ blocks are incident to both O and A: q^{2n-2} are Hermitian–type, the remaining $q^{2n-4}+\ldots+q+1$ being cone–type. Hermitian–type blocks passing through O and A are represented by

$$\begin{aligned} X_1^{q+1}+\ldots+X_{n-1}^{q+1}+X_n^q+X_n+X_1^q(i_1+j_1^q)+\ldots+\\ X_{n-1}^q(i_{n-1}+j_{n-1}^q)+X_1(i_1^q+j_1)+\ldots+X_{n-1}(i_{n-1}^q+j_{n-1})=0, \end{aligned} \tag{21}$$

with (18) satisfied. Set $x_s=x_s^1+\varepsilon x_s^2$ for any $s=1,\ldots,n$, with $x_s^1,x_s^2\in\mathrm{GF}(q)$. The cone–type blocks incident to both O and A are exactly those with basis a hyperplane of $AG(2n-2,q)$ containing the line through the points $(0,\ldots,0)$ and $(x_1^1,x_1^2,\ldots,x_{n-1}^1,x_{n-1}^2)$. Hence, these blocks share q generators, say r_t, with affine equations of the form

$$r_t\begin{cases} X_1=tx_1\\ \vdots\\ X_{n-1}=tx_{n-1}\end{cases}$$

as t ranges over GF(q). Each generator r_t meets the intersection of the Hermitian–type blocks through O and A at those points $(tx_1, tx_2, \ldots, tx_{n-1}, \overline{x}_n)$ satisfying each of the (21), that is

$$\begin{gathered} t^2 x_1^{q+1} + \ldots + t^2 x_{n-1}^{q+1} + \overline{x}_n^q + \overline{x}_n + t x_1^q (i_1 + j_1^q) + \ldots + t x_{n-1}^q (i_{n-1} + j_{n-1}^q) + \\ + t x_1 (i_1^q + j_1) + \ldots + t x_{n-1} (i_{n-1}^q + j_{n-1}) = 0. \end{gathered} \tag{22}$$

Given (15), (18), Equations (22) become

$$\overline{x}_n^q + \overline{x}_n - t^2 (x_n^q + x_n) = 0. \tag{23}$$

Since $t^2(x_n^q + x_n) \in \mathrm{GF}(q)$, (23) has q solutions, all of the form $\{\overline{x}_n + r | r \in T_0\}$. The point-set $\{(tx_1, tx_2, \ldots, tx_{n-1}, \overline{x}_n + r) | r \in T_0\}$ coincides with the point $N(tx_1, tx_2, \ldots, tx_{n-1}, \overline{x}_n) \in \mathcal{P}$ and as t varies in $GF(q)$, we get that the intersection of all blocks containing O and A consists, also in this case, of q points of $\mathcal{S}$. $\square$

Remark 4.2. The array A_0 defined in Theorem 3.3 is closely related to the affine design $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$. Precisely, $\mathcal{W}_0$ is a set of representatives for $\mathcal{P}$. The rows of $\mathcal{A}_0$ are generated by the forms F^g for g varying in $\mathcal{R}$, whose associated Hermitian varieties provide a set of representatives for the q^{2n-2} parallel classes of Hermitian–type blocks in $\mathcal{B}$.

References

[1] Aguglia, A. *Designs arising from Buekenhout-Metz unitals* J. Combin. Des. **11** (2003), 79–88.

[2] Beth, T. Jungnickel, D., Lenz, H. " Design Theory ", Vol. I, II, Cambridge University Press, Cambridge, (1999).

[3] Bose, R. C., *Mathematical theory of the symmetrical factorial design*, Sankhya **8**, (1947), 107–166.

[4] Dembowski, P., *Finite Geometries*, Springer–Verlag, Berlin, Heidelberg, New York, 1968.

[5] Fuji-Hara, R. and Miyamoto, N., *Balanced arrays from quadratic functions*, J. Statist. Plann. Inference **84** (2000), 285–293.

[6] Fuji-Hara and R., Miyamoto, N., *A construction of combinatorial arrays from non-linear functions* Util. Math. **52** (1997), 183–192.

[7] Hirschfeld, J.P.W. "Projective Geometries Over Finite Fields," Oxford University Press, Oxford, 1998.

[8] Lidl, R. and Niederreiter, H., "Finite fields", Addison–Wesley, 1983.

[9] Rao, C. R., *On Hypercubes of strength d and a system of confounding in factorial experiments* Bull. Cal. Math. Soc. **38** (1946) 67–68.

[10] Rao, C. R., *Factorial experiments derivable from combinatorial arrangements of arrays*, J. Roy. Stat. Soc. (Suppl.) **9**, (1947), 128-139.

[11] Segre, B., *Forme e geometrie hermitiane, con particolare riguardo al caso finito*, Ann. Mat. Pura Appl. **70** (1965) 1–201.

[12] Shrikhande, S.S. and Bhagwandas,D.,*On embedding of orthogonal arrays of strength two*, Combinatorial Mathematica and its Applications, University of North Carolina Press (1969), $256 - 273$.

[13] Hedayat, A. S., Sloane, N. J. A. and Stufken, J. "Orthogonal arrays: theory and applications", Springer Verlag (1999).

[14] Tonchev, V.D., *Affine designs and linear orthogonal arrays*, Discrete Mathematics **294** (2005), 219–222.

Angela Aguglia
Dipartimento di Matematica
Politecnico di Bari
Via G. Amendola 126/B
70126 Bari
Italy
a.aguglia@poliba.it

Luca Giuzzi
Dipartimento di Matematica
Politecnico di Bari
Via G. Amendola 126/B
70126 Bari
Italy
l.giuzzi@poliba.it