Twisted tensor product group embeddings and complete partial ovoids on quadrics in
\[ PG(2^t - 1, q) \]

Antonio Cossidente
Dipartimento di Matematica
Università della Basilicata
I-85100 Potenza - Italy
cossidente@unibas.it

Oliver H. King
Department of Mathematics
University of Newcastle
Newcastle Upon Tyne
NE1 7RU, U.K.
O.H.King@ncl.ac.uk
Proposed Running Head: Twisted tensor product group embeddings

Corresponding Author:
Antonio Cossidente
Dipartimento di Matematica
Università della Basilicata
Contrada Macchia Romana
I-85100 Potenza
Italy
cossidente@unibas.it
Abstract

We study the geometry of the groups $SL(2, q^t)$ and $Sp(2m, q^t)$, $m, t \geq 2$, $q$ even, in their twisted tensor product representation. We construct families of complete partial ovoids of hyperbolic quadrics in $PG(2^t - 1, q)$, all attaining the Blokhuis–Moorhouse bound. We identify the stabilizers of the complete partial ovoids.

Keywords: Twisted tensor product representation, complete partial ovoids, ovoids

1 Introduction

Let $G$ be a finite classical group with natural module $V_0$ of dimension $n \geq 2$ over the Galois field $GF(q^t)$. Let $V^\psi_i$ denote the $G$–module $V_0$ with group action given by $v \cdot g = vg^\psi_i$, where $g^\psi_i$ denotes the matrix $g$ with its entries raised to the $q^i$–th power, $i = 0, \ldots, t - 1$. Then one can form the tensor product module $V_0 \otimes V_0^\psi_0 \otimes \cdots \otimes V_0^\psi_{t-1}$, a module which can be realized over the field $GF(q)$. This gives rise to an embedding of the group $G$ in a classical group having an $n^t$–dimensional natural module over $GF(q)$, yielding an absolutely irreducible representation of the group $G$. Such representations are given by Steinberg ([17]) and further studied by Seitz ([16]). As Seitz observed, the normalizers of such “twisted tensor product groups” might easily be considered a ninth Aschbacher class [1].

In [4] we described the geometry of some twisted tensor product groups when $n = 3$ and $t = 2$. In this paper we study the geometry of two other classes of twisted tensor product groups: $PSL(2, q^t) \leq P\Omega^+(2^t, q)$, where $t \geq 2$ and $q$ is even; and $PSp(2m, q^t) \leq P\Omega^e((2m)^t, q)$ with $q$ even.

Let $PG(n, q)$ be the $n$–dimensional projective space over $GF(q)$. Throughout we shall assume that $q$ is even and that $t \geq 2$. An ovoid $\mathcal{O}$ in a classical polar space [10, Chapter 26] is a set of singular points such that every maximal totally singular subspace contains just one point of $\mathcal{O}$. The points of $\mathcal{O}$ are pairwise non-orthogonal. More generally a partial ovoid is a set of pairwise non-orthogonal singular points. A partial ovoid is said to be complete if it is maximal with respect to set–theoretic inclusion.
The possibility of the existence of ovoids in polar spaces of various dimensions has been studied extensively, for both odd and even $q$ (although the results referred to here are solely for even $q$). On the one hand there are known to be ovoids in $PG(7, q)$, both infinite families such as the unitary ovoids and the Desarguesian ovoids and individual ovoids such as Dye’s ovoid, and although the 2-transitive ovoids have been classified by Kleidman in [14], there is no general classification of ovoids. On the other hand Thas ([20]) has shown that quadrics in $PG(2n, q)$ and elliptic quadrics in $PG(2n + 1, q)$ have no ovoids if $n \geq 4$ and Kantor ([13]) has shown that hyperbolic quadrics in $PG(2n + 1, 2)$ have no ovoids if $n \geq 4$. Further, Blokhuis and Moorhouse ([2]) established an upper bound for the size of a partial ovoid of a polar space, a consequence of which is the non-existence of ovoids of hyperbolic quadrics in $PG(2n + 1, q)$ for $n \geq 4$ and $q$ even. A survey on ovoids in classical polar space is included by Thas in [22], and further information can be found in [20], [21], [10]. There are known to be examples of partial ovoids on quadrics in $PG(4n + 3, 8)$ whose size meets the Blokhuis-Moorhouse bound ([8]) for all values of $n$; also in [8] there are examples of complete partial ovoids on quadrics in $PG(4n + 1, 8)$ whose size falls just short of the Blokhuis-Moorhouse bound.

We find that our embedding of $PSL(2, q^t)$ is associated with an embedding of $PG(1, q^t)$ as a partial ovoid of a quadric in $PG(2^t - 1, q)$; if $t \geq 3$, then the quadric is hyperbolic. In $PG(2^t - 1, q)$ with $q$ even, the Blokhuis–Moorhouse bound is given by $q^t + 1$. We thus have a family of partial ovoids whose size attains the Blokhuis–Moorhouse bound. In particular when $t = 3$ and $q \geq 4$ the embedding yields a nice description of a Desarguesian ovoid of the hyperbolic quadric of $PG(7, q)$ ([11], [12]) as the image of a projective line in much the same way as an elliptic quadric of $PG(3, q)$ is the image of a projective line. Similarly our embedding of $PSp(2m, q^t)$ in $PΩ((2m)^t, q)$ has a particular application when $m = 2$ in the embedding of ovoids of $PG(3, q^t)$ as partial ovoids of $PG(4^t - 1, q)$ again with size attaining the Blokhuis–Moorhouse bound. The families of complete partial ovoids arising from Suzuki-Tits ovoids are not equivalent to those arising from elliptic quadrics or projective lines; the partial ovoids given by Dye in [8] are different again.
2 Embedding $Sp(2m, q^t)$ in $\Omega^\ell((2m)^t, q)$

Let $V_0$ now be a $2m$–dimensional vector space over $GF(q^t)$. Then $V = V_0 \otimes V_0 \otimes \cdots \otimes V_0$ ($t$ copies of $V_0$) is a vector space of dimension $(2m)^t$. If $f_0$ is a non–degenerate alternating form on $V_0$ then one can define a non–degenerate alternating form on $V$ by a linear extension from a basis of pure tensors as follows:

$$f(u_1 \otimes \cdots \otimes u_t, w_1 \otimes \cdots \otimes w_t) = \prod_{i=1}^t f_0(u_i, w_i).$$

Moreover there exists a unique quadratic form $Q$ on $V$ such that $Q(u_1 \otimes \cdots \otimes u_t) = 0$ for all $u_i \in V_0$ and such that $f$ is the bilinear form associated with $Q$ ([1, 9.1 (4)]). If $U$ is an $m$–dimensional totally isotropic subspace of $V_0$, then $U \otimes V_0 \otimes \cdots \otimes V_0$ is a totally singular subspace of $V$ of dimension $(2m)^t/2$, so $Q$ is a quadratic form of maximal Witt index.

Let $G$ be the group $Sp(2m, q^t)$ acting on $V_0$ and preserving $f_0$. Let $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m$ be a symplectic basis for $V_0$ (so $f_0(x_i, x_j) = f_0(y_i, y_j) = 0$ and $f_0(x_i, y_j) = \delta_{ij}$). The twisted action of $G$ on $V$, as described in the introduction third line, is given by $u_1 \otimes \cdots \otimes u_t \mapsto u_1 g \otimes u_2 g^\psi \otimes \cdots \otimes u_t g^{\psi t-1}$ with $g^{\psi t}$ preserving $f_0$ for each $i$. Thus $g$ preserves $Q$ on $V$. Taking note of the fact that $Sp(2m, q^t)$ is perfect, we thus have a representation $\rho : G \to \Omega^\ell((2m)^t, q^t)$.

In [4, Section 2] we introduced a semi–linear map $\phi$ on $V$ and the subset $W$ of $V$ consisting of all vectors fixed by $\phi$. Here we prove a number of properties of $\phi$ and $W$ that we shall need to refer to. We recall that $\phi(\lambda u_1 \otimes u_2 \otimes \cdots \otimes u_t) = \lambda^q u_1 \otimes u_2 \otimes \cdots \otimes u_{t-1}$, whenever each $u_i$ is one of $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m$ and $\lambda \in GF(q^t)$ and then $\phi$ is extended linearly over $GF(q)$. If we write $v^{\psi} = \sum (\lambda_i x_i + \mu_i y_i)$ when $v = \sum (\lambda_i x_i + \mu_i y_i) \in V_0$, then $\phi(v_1 \otimes v_2 \otimes \cdots \otimes v_t) = v_1^{\psi} \otimes v_2^{\psi} \otimes \cdots \otimes v_{t-1}^{\psi}$. We have not explicitly referred to the case: $m = 1$ here. However, given any basis $x_1, y_1$ for $V_0$ when $m = 1$ we can define an alternating form $f_0$ on $V_0$ such that $f_0(x_1, y_1) = 1$ and the symplectic group $Sp(2, q^t)$ is just $SL(2, q^t)$.

Lemma 2.1. (1) The semilinear map $\phi$ commutes with $\rho(G)$ on $V$;

(2) The set $W = \{w \in V : \phi(w) = w\}$ is a $GF(q)$–subspace of $V$, (globally) stabilized by $\rho(G)$;
(3) Any vectors in $W$ that are linearly independent over $GF(q)$ are linearly independent over $GF(q^t)$;

(4) $W$ has dimension $(2m)^t$ over $GF(q)$ and spans $V$ over $GF(q^t)$.

(5) $Q(w) \in GF(q)$ for each $w \in W$ and $Q$ is non–degenerate on restriction on $W$.

Proof.

(1) For any $x_1 \otimes x_2 \otimes \cdots \otimes x_t$ we have:

$$g(\phi(x_1 \otimes \cdots \otimes x_t)) = g(x_1^\psi \otimes x_2^\psi \otimes \cdots \otimes x_{t-1}^\psi)$$

$$= x_t^\psi \otimes x_1^\psi \otimes x_2^\psi g \otimes \cdots \otimes x_{t-1}^\psi.$$  

$$\phi(g(x_1 \otimes \cdots \otimes x_t)) = \phi(x_1^\psi \otimes x_2^\psi \otimes \cdots \otimes x_{t-1}^\psi)$$

$$= (x_t^\psi \otimes x_1^\psi \otimes x_2^\psi \otimes \cdots \otimes x_{t-1}^\psi)^\psi$$

$$= x_t^\psi \otimes x_1^\psi \otimes x_2^\psi g \otimes \cdots \otimes x_{t-1}^\psi.$$  

Any vector in $V$ is a $GF(q)$–linear combination of vectors of the type above, so $\rho(G)$ commutes with $\phi$ on the whole of $V$.

(2) If $w \in W$, then $\phi(g(w)) = g(\phi(w)) = g(w)$ so $g(w) \in W$.

(3) Suppose that $w_1, w_2, \ldots, w_r$ is a minimal counterexample (with, necessarily, $r \geq 2$. Then $\sum_{i=1}^r \mu_i w_i = 0$ for some $\mu_i \in GF(q^t)$, not all in $GF(q)$, and we may assume that $\mu_r = 1$. Under the map $\phi$ we find that $\sum_{i=1}^r \mu_i^q w_i = 0$ and so $\sum_{i=1}^{r-1} (\mu_i^q - \mu_i) w_i = 0$. As $w_1, \ldots, w_{r-1}$ are linearly independent over $GF(q)$ and $\mu_i^q - \mu_i$ are not all zero, we have a contradiction.

(4) It follows from (iii) that the $GF(q)$–dimension of $W$ is at most $2^t$. The $GF(q^t)$–subspace of $V$ spanned by $W$ is fixed by $\rho(G)$, but, by Steinberg’s Tensor Product Theorem [17], $\rho(G)$ is absolutely irreducible. Hence $W$ has dimension $(2m)^t$ as a vector space over $GF(q)$ and spans $V$ over $GF(q^t)$. 

6
(5) Consider the vectors $v \otimes v \otimes \cdots \otimes v^{t-1}$. All such vectors are fixed by $\phi$ so lie in $W$. Moreover they are preserved as a set by $\rho(G)$. This means that their $GF(q)$-span is preserved by $\rho(G)$. Given the irreducibility of $\rho(G)$ it follows that these vectors span $W$. Let $z_1, \ldots, z_{2m}$ be a basis for $W$ over $GF(q)$. The irreducibility of $\rho(G)$ means that the restriction of $Q$ to $W$ must be non-degenerate or trivial, but it suffices to consider $z_i$ and $z_j$ corresponding to non-orthogonal $x$ and $y$ to see that $Q$ is not trivial $Q(z_i + z_j) = f(z_i, z_j) = \prod f_0(x^{\psi_k}, y^{\psi_k}) \neq 0$.

Since $Sp(2m, q^t)$ is simple, $\rho$ is injective. Thus we may regard $Sp(2m, q^t)$ as a subgroup of $\Omega^t(2^m, q)$, and equivalently in the projective context, $PSp(2m, q^t)$ as a subgroup of $P\Omega^t((2m)^t, q)$.

3 The nature of the quadrics

In this section we show that the quadratic form on $W$ described in the previous section is usually hyperbolic.

We begin by describing a basis for the $GF(q)$-subspace $W$. Write $n = 2m$ and write $x_{m+1}, \ldots, x_n$ for $y_1, \ldots, y_m$. Let $\Delta = \{1, 2, \ldots, t\}$ and let $c = (1234 \ldots t)$, a cyclic permutation of $\Delta$. We define a pattern of length $t$ to be a sequence (row-vector) of length $t$ with entries coming from among the numbers $1, 2, \ldots, n$ and call it a $k$-pattern if exactly $k$ of the entries are between 1 and $m$. We say that a $k$-pattern $P$ is irreducible if $c^i P \neq P$ for all $1 \leq i < t$. Equivalently a pattern is a partition, $\{\Delta_1, \Delta_2, \ldots, \Delta_n\}$, of $\Delta$ with $\Delta_j$ corresponding to the positions having entry $j$; in this context the subgroup of $S_t$ generated by $c$ acts on the set of all partitions of $\Delta$ and an irreducible pattern corresponds to a partition lying in an orbit of length $t$. For any pattern $P$, the smallest $r \geq 1$ such that $c^r P = P$ is called the irreducible length of $P$; the first $r$ entries then form an irreducible pattern of length $r$. Equivalently, the partition of $\Delta$ corresponding to $P$ lies in an orbit of length $r$. Given a $k$-pattern $P$ of length $t$, the inverse pattern $P'$ is defined to be the $t-k$-pattern derived from $P$ by replacing each entry
j by \(j + m \pmod{n}\) for each \(j\). If \(t = 2s\) then a \(k\)-pattern \(P\) is said to be invertible if \(e^k P = P'\). Given a vector \(u\) corresponding to a pattern \(P\) irreducible length \(r\), the vectors \(\sum_{j=1}^{r} \phi^{j-1}(\lambda u)\), as \(\lambda\) ranges over \(GF(q')\), span a \(GF(q)\)-subspace \(V(P)\) of \(V\) of dimension \(r\), fixed by \(\phi\) vectorwise. The direct sum of such subspaces gives a \(GF(q)\)-subspace of dimension \(n^t\). A basis for \(GF(q')\) over \(GF(q)\) gives rise to a basis for \(V(P)\).

### 3.1 The case \(t\) odd

**Lemma 3.1.** If \(t\) is odd, then \(Q\) has maximal Witt index on \(W\).

**Proof.**

Suppose that \(t\) is odd. There are two possible approaches. One is via [15]. Using this approach we start from the position where we know that the image of \(Sp(2m, q^t)\) lies in \(\Omega^\epsilon((2m)^t, q^t)\) with \(\epsilon = +\) or \(-\). As Kleidman and Liebeck show, the value of \(\epsilon\) depends on whether a certain quadratic polynomial over \(GF(q)\) is reducible or not, and for \(t\) odd answer is the same over \(GF(q^t)\); given that \(\Omega^\epsilon((2m)^t, q^t)\) is here a subgroup of \(\Omega^+((2m)^t, q^t)\) we can see that \(\epsilon = +\). Notice that the arguments from [15] involved here concerning a classical group with a form do not actually use the classification of finite simple groups.

Alternatively, we can use notation set up above. Collect together the \(k\)-patterns \(P\) of length \(t\) for which \(k > t/2\). The sum of the corresponding \(V(P)\) is totally singular of dimension \((2m)^t/2\), so the quadric must be hyperbolic.

\(\square\)

### 3.2 The case \(t\) even

Assume that \(t = 2s\). In the \(GF(q)\)-subspace \(W\) of \(V\) consider the subspaces \(V(P)\) where \(P\) is a \(k\)-pattern of length \(t\). Let \(r\) be the irreducible length of \(P\) and let \(R\) be the irreducible pattern of length \(r\) that is repeated to give \(P\); if \(P\) is irreducible, then \(r = t\) and \(R = P\). The inverse pattern \(P'\) is obtained by repeating \(R'\). Suppose that \(u = \lambda u_1 \otimes u_2 \otimes \ldots \otimes u_t\) and \(v = \mu v_1 \otimes v_2 \otimes \ldots \otimes v_t\) are non-zero vectors corresponding to patterns \(P\) and \(S\) respectively. Then \(u\) and \(v\) are singular, and \(f(u, v) \neq 0\) if and only if \(S = P'\). Moreover if \(S = P'\), then \(f(\sum_{j=1}^{r} \phi^{j-1}u, \sum_{j=1}^{r} \phi^{j-1}v) = \sum_{j=1}^{r} (\lambda \mu)^{q^j-1} = Tr_{GF(q')/GF(q)}(\lambda \mu)\). It follows that if \(k \neq s\), then \(V(P)\) and \(V(P')\) are totally singular, \(V(P) \oplus V(P')\) is non-isotropic and \(V(P) \oplus V(P')\) is orthogonal to \(V(S)\) whenever \(S\) is
not derivable from \( P \) or \( P' \) (meaning that \( S \neq c'^i P \) or \( c'^i P' \) for any \( i \)). The same argument applies if \( k = s \) but \( R \) is not invertible. Thus in order to determine the Witt index of \( Q \) on \( W \) we need only consider the \( V(P) \) for which \( P \) is an \( s \)-pattern of length \( t \) and for which \( R \) is invertible. If \( R \) is indeed invertible, then \( r \) is even, the vectors of \( V(P) \) have the form \( \sum_{j=1}^{r} \phi_j^{-1} u \) where \( u = \lambda u_1 \otimes u_2 \otimes \ldots \otimes u_t \) corresponds to \( P \), and \( Q(\sum_{j=1}^{r} \phi_j^{-1} u) = Tr_{GF(q^{r/2})/GF(q)}(\lambda^{1+q^{r/2}}) \). Precisely this quadratic form is considered in [5] where it is shown to be elliptic. Hence we need to know the number of such subspaces. The same subspace arises from each of the patterns \( P, cP, \ldots, c^{r-1} P \). Thus if \( a(r) \) denotes the number of irreducible, invertible patterns of length \( r \), then \( a(r)/r \) is an integer denoting the number of corresponding subspaces \( V(P) \).

Let us write \( a(t) \) and \( d(t) \) for the number of irreducible, invertible \( s \)-patterns of length \( t \) and the number of reducible, invertible \( s \)-patterns of length \( t \) respectively. We can read these as 0 for odd \( t \).

**Lemma 3.2.**

1. \( a(t) + d(t) = n^s; \)
2. \( d(t) = \sum a(r) \), the sum taken over all \( r < t \) dividing \( t \) for which \( t/r \) is odd;
3. \( a(t)/t \) is an integer. It is even if \( m = n/2 \) is even, if \( t \) is divisible by 8 and if \( t \) is divisible by the square of an odd prime and odd otherwise;
4. If \( t > 2 \), then \( \sum_{r|t} a(r)/r \) is even. If \( t = 2 \), then \( \sum_{r|t} a(r)/r \) has the same parity as \( m = n/2 \).

Proof.

1. An invertible \( s \)-pattern of length \( t \) consists of an arbitrary pattern of length \( s \) (i.e., sequence of elements of \( \Delta \) of length \( s \)) followed by its inverse. There are \( n^s \) patterns of length \( s \).
2. Suppose that \( P \) is a reducible, invertible \( s \)-pattern of irreducible length \( r \) and let \( h = t/r \). If \( h \) is even, then \( r \) divides \( s \) and therefore \( c^r P = P \), contradicting \( c^r P = P' \). Hence \( h \) is odd. Let \( R \) be the irreducible pattern of length \( r \) that is repeated in order to obtain \( P \). Then \( R \) must be an \( r/2 \)-pattern and \( c^{(h+1)/2} P = P \) has in places \( s + 1 \) to \( s + r/2 \) the last \( r/2 \) entries from \( R \), but as \( P \) is invertible these entries are also
the inverse of the first \( r/2 \) entries of \( R \). Hence \( R \) is itself invertible. It follows that each reducible, invertible \( s \)-pattern corresponds to an irreducible invertible \( r/2 \)-pattern of length \( r \) for some divisor \( r \) of \( t \) such that \( t/r \) is odd. Conversely each irreducible invertible \( r/2 \)-pattern of such length \( r \) yields an invertible \( s \)-pattern of length \( t \) by repetition.

(3) Suppose that \( P \) is an irreducible invertible \( s \)-pattern. The \( t \) \( s \)-patterns \( P, cP, \ldots, c^{t-1}P \) are distinct since \( P \) is irreducible and all are invertible. Thus the \( a(t) \) irreducible invertible \( s \)-patterns fall into orbits of length \( t \) under the action of \( c \). Hence \( t \) divides \( a(t) \).

First we determine the parity of \( a(t)/t \) when \( t \) is a power of 2. In this case \( d(t) = 0 \) so \( a(t) = n^s \). If \( t = 2^{\alpha_1} \), then \( a(t)/t = n^{2^{\alpha_1}-1}/2^{\alpha_1} \) which is odd if \( \alpha_1 = 1 \) or 2 and \( m = n/2 \) is odd, and even otherwise.

We give a proof by induction on \( N \), the number of prime divisors of \( t \) (including repetition). If \( N = 1 \), then \( t = 2 \) and the result holds by the argument above. Now suppose that \( N \geq 2 \) and that the result holds whenever \( t \) has fewer than \( N \) prime divisors. Let us write \( t = 2^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k} \) where \( p_2, \ldots, p_k \) are distinct odd primes (so \( N = \alpha_1 + \alpha_2 + \ldots + \alpha_k \)). We can write

\[
d(t) = \sum_{r=2^{\alpha_1}p_2^{\beta_2}\ldots p_k^{\beta_k}, \beta_i \leq \alpha_i, r \neq t} a(r).
\]

Suppose that \( \alpha_1 \geq 3 \). Then for each term in this sum, \( a(r)/2^{\alpha_1} \) is even (by the induction hypothesis) so that \( d(t)/2^{\alpha_1} \) is even. Moreover \( t \) is sufficiently large that \( n^s/2^{\alpha_1} \) is even, so \( (n^s-d(t))/2^{\alpha_1} \) is even and hence \( a(t)/t \) is even. Now suppose that \( m = n/2 \) is even: by the induction hypothesis, for each term \( a(r) \) in the sum \( a(r)/2^{\alpha_1} \) is even so and then \( a(t)/t \) is even. Next suppose that \( m \) is odd, that \( \alpha_1 = 1 \) or 2 and that \( t \) is divisible by the square of an odd prime, i.e., \( \alpha_i \geq 2 \) for some \( i \geq 2 \). Looking at the expression for \( d(t) \), this time we find that \( a(r)/2^{\alpha_1} \) is even whenever \( \beta_i \geq 2 \) for some \( i \) and odd whenever each \( \beta_i \) is 0 or 1. There are \( 2^{k-1} \) occasions when \( a(r)/2^{\alpha_1} \) is odd (note that on no such occasion is \( r \) equal to \( t \)), so again \( d(t)/2^{\alpha_1} \) is even and then \( a(t)/t \) is even. Finally suppose that \( m \) is odd, that \( \alpha_1 = 1 \) or 2 and that \( t \) is divisible by at least one odd prime but not by the square of an odd prime. Then the expression for \( d(t) \) has \( 2^{k-1} - 1 \) terms, with \( a(r)/2^{\alpha_1} \) odd in each case (on this occasion the restriction \( r \neq t \) means that the
term where each $\beta_i$ is 1 is excluded); here then $d(t)/2^{\alpha_1}$ is odd and in turn $a(t)/t$ is odd.

(4) The terms in the sum $\sum_{r|t} a(r)/r$ are even unless: $m$ is odd and $r = 2^{\beta_1}p_2^{\beta_2} \cdots p_k^{\beta_k}$ with $\beta_1 = 1$ or 2 and $\beta_i$ is 0 or 1 for each $i \geq 2$ (and in such cases the terms are odd). Assume that $m$ is odd. If $t$ is not a power of 2, then there are an even number of terms with $\beta_1 = 1$ and $\beta_i$ is 0 or 1 for each $i \geq 2$. If $t = 2^{\alpha_1}$ with $\alpha_1 \geq 2$ then the terms are all even except for $a(4)/4$ and $a(2)/2$. If $t = 2$, then there is just one term: $a(2)/2 = 1$. Hence $\sum_{r|t} a(r)/r$ is even unless $m$ is odd and $t = 2$.

\[ \square \]

**Corollary 3.3.** The number of irreducible invertible $s$-patterns and reducible $s$-patterns that have invertible repeated subpatterns is even except when $t = 2$ and $m = n/2$ is odd. If $t$ is even, then $Q$ has maximal Witt index on $W$ except when $t = 2$ and $m = n/2$ is odd. In the exceptional case, $Q$ has non-maximal Witt index on $W$.

Proof. The number of subspaces $V(P)$ on which $Q$ is non-isotropic and elliptic is precisely $\sum_{r|t} a(r)/r$. This number is even with the single exception given.

\[ \square \]

4 Embedding $PG(2m - 1, q^t)$ in $PG((2m)^t - 1, q)$

4.1 Embedding the projective line and partial ovoids

Given $0 \neq v \in V_0$ let us denote by $\underline{v}$ the vector $v \otimes v^\psi \otimes \cdots \otimes v^{\psi^{t-1}} \in V$; recall that all such vectors lie in $W$ and are singular. Observe that for $0 \neq \lambda \in GF(q^t)$ we have $\lambda \underline{v} = (\lambda \lambda^q \cdots \lambda^{q^{t-1}}) \underline{v}$ with $\lambda \lambda^q \cdots \lambda^{q^{t-1}} \in GF(q)$.

Hence the injective map: $V_0 \to W, v \to \underline{v}$ leads to an injective map $\varphi : PG(2m - 1, q^t) \to PG((2m)^t - 1, q)$. Suppose that $x, y \in V_0$ such that $f_0(x, y) \neq 0$. Then

\[
\begin{align*}
f(x, y) & = f_0(x, y) \cdot f_0(x^\psi, y^\psi) \cdots \cdot f_0(x^{\psi^{t-1}}, y^{\psi^{t-1}}) \\
& = f_0(x, y) \cdot f_0(x, y)^q \cdots \cdot f_0(x, y)^{q^{t-1}} \\
& \neq 0.
\end{align*}
\]
We have now proved our first main theorem:

**Theorem 4.1.** Suppose that \( L \) is either the projective line \( \text{PG}(1,q^t) \) or a partial ovoid of a symplectic polarity of \( \text{PG}(2m-1,q^t) \) with \( m \geq 2 \), and that \( P = \varphi(L) \) in \( \text{PG}((2m)^t-1,q) \). Then \( P \) is a partial ovoid of a non-degenerate quadric in \( \text{PG}((2m)^t-1,q) \) having the same size as \( L \). The quadric is hyperbolic unless \( t = 2 \) and \( m = n/2 \) is odd, in which case it is elliptic.

\(\square\)

### 4.2 The Blokhuis-Moorhouse bound

In their 1995 paper [2] Blokhuis and Moorhouse give an upper bound for size of a partial ovoid of a classical polar space in \( \text{PG}(k,q) \). If \( q = p^e \) where \( p \) is prime, then the size of a partial ovoid is no greater than \( \left( \frac{k + p - 1}{k} \right)^e + 1 \). If \( p = 2 \), then this bound becomes simply \( (k + 1)^e + 1 \). If, in addition, \( k + 1 = 2^t \) for some \( t \), then the bound is \( 2^{te} + 1 = q^t + 1 \). In particular we get the same value for the bound in \( \text{PG}(2^a-1,2^{et}) \) and \( \text{PG}(2^{at}-1,2^e) \) for any \( a \geq 1 \).

The following theorem is a corollary to Theorem 4.1. It demonstrates that, for \( p = 2 \), the Blokhuis-Moorhouse bound is sharp for arbitrarily large dimension of the form \( 2^t - 1 \).

**Theorem 4.2.** If \( L \) is the projective line \( \text{PG}(1,q^t) \), then \( \varphi(L) \) is a partial ovoid of a non-degenerate quadric in \( \text{PG}(2^t-1,q) \) whose size attains the Blokhuis-Moorhouse bound. If \( L \) is a partial ovoid of a symplectic polarity of \( \text{PG}(2^a-1,q^t) \) (with \( a \geq 2 \) and \( q = 2^e \)) whose size attains the Blokhuis-Moorhouse bound, then \( \varphi(L) \) is a partial ovoid of a non-degenerate quadric in \( \text{PG}(2^{at}-1,q) \) whose size attains the Blokhuis-Moorhouse bound.

\(\square\)

**Remark 4.3.** When \( t = 2 \) and \( L \) is the projective line \( \text{PG}(1,q^t) \), the image \( P = \varphi(L) \) is an elliptic quadric. When \( t = 3 \) and \( L \) is the projective line \( \text{PG}(1,q^t) \), the image \( P \) has \( q^3 + 1 \) points and so is an ovoid of a hyperbolic quadric of \( \text{PG}(7,q) \) admitting \( \text{PSL}(2,q^3) \) as a 2–transitive automorphism group. By [12], [14] it is a Desarguesian ovoid if \( q > 2 \). If \( q = 2 \) and \( t = 3 \)
it is still true that $\mathcal{P}$ is an ovoid but it is now a polygon on admitting the alternating group $A_9$ as an automorphism group \cite{7}.

### 4.3 Complete partial ovoids from embeddings of $PG(1, q^t)$ and ovoids of $PG(3, q^t)$

In this section we consider complete partial ovoids in $PG(2t - 1, q)$ and $PG(4t - 1, q)$ arising as images of projective lines and of elliptic quadrics or Suzuki-Tits ovoids of $PG(3, q^t)$ respectively. We identify the stabilizers of these partial ovoids using the the classification of finite 2-transitive groups. In turn this relies on the Classification of Finite Simple Groups. Our source for the list of finite 2-transitive groups is \cite{3} where the groups are listed in Tables 7.3 and 7.4. Our interest is in groups having permutation degree $2^k + 1$ for some $k \geq 1$.

**Result 4.4.** A 2-transitive permutation group of degree $2^k + 1$ for some $k \geq 1$ is almost simple with unique minimal normal subgroup one of the following: $A_M$ with $M = 2^k + 1$, $SL(2, 2^k)$, $PSU(3, 2^{2k/3})$, $Sz(2^{k/2})$ where $k/2$ an odd integer.

Throughout this section we consider three possibilities:

- **Case PL:** $\mathcal{L}$ is the projective line $PG(1, q^t)$ with $t \geq 3$, $G = SL(2, q^t)$, $2^k = q^t$, we write $\Omega = \Omega^+(2^t, q)$ and $PW = PG(2^t - 1, q)$.

- **Case EQ:** $\mathcal{L}$ is an elliptic quadric of $PG(3, q^t)$, $G = \Omega^-(4, q^t)$, $2^k = q^{2t}$, we write $\Omega = \Omega^+(4^t, q)$ and $PW = PG(4^t - 1, q)$.

- **Case STO:** $\mathcal{L}$ is a Suzuki-Tits ovoid of $PG(3, q^t)$ with $q$ an odd power of 2 and $t$ odd, $G = Sz(q^t)$, $2^k = q^{2t}$, we write $\Omega = \Omega^+(4^t, q)$ and $PW = PG(4^t - 1, q)$.

We write $\mathcal{P} = \varphi(\mathcal{L})$, $\tilde{F} = \rho(F)$ for any subgroup $F$ of $G$ and let $\tilde{H}$ be the stabilizer of $\mathcal{P}$ in $\Omega$. Then $H$ contains $\tilde{G}$ and acts 2-transitively on $\mathcal{P}$. The action of $\tilde{G}$ on the vector space $W$ is irreducible by Steinberg’s Tensor Product Theorem ([17, Theorem 7.4, Theorem 12.2]) and so the points of $\mathcal{P}$ span the corresponding projective space. As the number of points exceeds the vector space dimension and $\tilde{G}$ acts 2-transitively, the only transformations fixing each point of $\mathcal{P}$ are scalar maps, here the identity is the only possibility. Thus the action of $\tilde{H}$ is faithful and we have:
Proposition 4.5. $\tilde{H}$ is almost simple with unique minimal normal subgroup $X$ being isomorphic to one of the following: $A_M$ with $M = 2^k + 1$, $SL(2, 2^k)$, $PSU(3, 2^{k/3})$, $Sz(2^{k/2})$ where $k/2$ is an odd integer.

The subgroup $X \cap \tilde{G}$ is normal in $\tilde{G}$, but $\tilde{G}$ is simple so either $X \cap \tilde{G} = 1$ or $\tilde{G} \leq X$.

Proposition 4.6. $\tilde{G} \leq X$.

Proof. Suppose that $X \cap \tilde{G} = 1$. Then $X\tilde{G}$ is a subgroup of $\tilde{H}$ of order $|X||\tilde{G}|$, but $\tilde{H}$ may be regarded as a subgroup of $Aut(X)$ and so $|\tilde{G}|$ divides $|Out(X)|$. The value of $|Out(X)|$ is well known for each possibility for $X$ (c.f. [15]): if $X \cong A_M$ with $M \geq 9$, then $|Out(X)| = 2$; if $X \cong SL(2, 2^k)$, then $|Out(X)| = k$; if $X \cong PSU(3, 2^{k/3})$, then $|Out(X)| = 2k/3$; if $X \cong Sz(2^{k/2})$, then $|Out(X)| = k/2$. On the other hand the order of $\tilde{G}$ is divisible by $2^k + 1$ with $k \geq 3$. The clear contradiction leads to the conclusion that $\tilde{G} \leq X$.

Proposition 4.7. $X = \tilde{G}$ except when $q = 2$, in which case $X = A_M$ with $M = 2^k + 1$.

Proof. We have established that $\tilde{G} \leq X$. We note that $|SL(2, 2^k)| = (2^k + 1)2^k(2^k - 1)$, $|Sz(2^{k/2})| = (2^k + 1)2^k(2^{k/2} - 1)$ and $|PSU(3, 2^{k/3})| = (2^k + 1)2^k(2^{k/3} - 1)/d$, where $d = hcf(3, 2^{k/3} + 1)$. We also note that $\Omega^{-}(4, q^t)$ is isomorphic to $SL(2, q^t)$. If $G = SL(2, 2^k)$, then simple arithmetic rules out all possibilities except $X \cong SL(2, 2^k)$ and $X \cong A_M$. If $G = Sz(2^{k/2})$, then similarly all possibilities are ruled out except $X \cong Sz(2^{k/2})$, $X \cong SL(2, 2^k)$ and $X \cong A_M$, but here $\tilde{G}$ cannot be embedded in $SL(2, 2^k)$ because $SL(2, 2^k)$ has minimal degree $2^k + 1$. Thus we have $\tilde{G} \leq X \leq \Omega$ with $X$ either $\tilde{G}$ or isomorphic to $A_M$. Suppose that $X \cong A_M$ with $M = 2^k + 1$. It is known (c.f. [15, Proposition 5.3.7]) that if $A_M$ is embedded in $PGL(r, q)$, then $r \geq M - 2$. This leads to $q^t - 1 \leq 2^t$, $q^{2t} - 1 \leq 4^t$ and $q^{2t} - 1 \leq 4^t$ in the cases $PL$, $EQ$ and $STO$ respectively. In other words $q = 2$ is the only possibility. In Remark 4.3 we observed that $PSL(2, 2^3)$ fixes an ovoid which is also a polygon admitting $A_9$ as an automorphism group, so that $PSL(2, 2^3) < A_9 < P\Omega^{+}(8, 2)$. More generally in the three cases here being considered for $L$, if $q = 2$, the partial ovoid $P$ is a polygon. Such a polygon admits the alternating group $A_{2^k + 1}$ as an automorphism group inside $\Omega$; a transposition corresponds to a symmetry of $O^{+}(2^k, 2)$, and, as such elements do not lie in $\Omega$, the alternating group is the
full stabilizer. The representation here of the alternating group is precisely
the fully deleted permutation module.

\[ \text{Proposition 4.8. The normalizer of } X \text{ stabilizes } P. \]

Proof. We first consider the case \( q = 2 \). Here it is possible to discern
that \( P \) is the only orbit of \( A_M \) of length \( 2^k + 1 \). If \( h \in N(\Omega) \), then \( Ph \) is
also an orbit of length \( 2^k + 1 \). Hence \( Ph = P \).

Now assume that \( q > 2 \). The following applies to all three cases. Let \( F \)
be the stabilizer in \( G \) of a point of \( L \). Then \( F \) can also be described as the
normalizer in \( G \) of a Sylow 2-subgroup \( S \) of \( G \) and there is a cyclic subgroup
\( C \) of \( F \) such that \( C \cap S = 1 \) and \( F = CS \). Exactly one point of \( L \) is fixed
by \( F \) and exactly one point of \( \tilde{P} \) is fixed by \( \tilde{F} \). Suppose that \( \tilde{F} \)
fixes exactly one point \( \tilde{P} \) of \( \tilde{P} \) (necessarily \( \tilde{P} \) will be in \( \tilde{P} \)). If \( h \in N(\tilde{G}) \), then \( h^{-1}Fh \)
fixes \( Ph \), but \( h^{-1}Fh \) is the normalizer in \( \tilde{G} \) of a Sylow 2-subgroup so fixes a
point of \( \tilde{P} \). Hence \( Ph \in \tilde{P} \). It follows that \( Ph = P \).

Consider first the case \( PL \). We can take \( F \) to be the stabilizer of \( < v_1 > \),
so it consists of upper-triangular matrices, and we can take \( C \) to be the
diagonal subgroup of order \( 2^t - 1 \) fixing both \( < v_1 > \) and \( < v_2 > \). A generator
for \( C \) is given by

\[ g = \begin{bmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{bmatrix}, \]

where \( \xi \) is a generator for \( GF(q^t)^* \) (the multiplicative group of \( GF(q^t) \)). The
eigenvalues of \( \rho(g) \) are \( \prod_{j=1}^{t} \xi_{\epsilon_j q^j - 1} \) where each \( \epsilon_j = \pm 1 \). The elements of
\( GF(q)^* \) are given by powers of \( \xi^{k(q)} \), where \( k(q) = 1 + q + q^2 + \ldots + q^{t-1} \). Hence
the only two eigenvalues of \( \rho(g) \) that lie in \( GF(q) \) are \( \xi^{k(q)} \) and \( \xi^{-k(q)} \), and
these correspond to eigenvectors \( v_1 \) and \( v_2 \) respectively, both corresponding
to points of \( \tilde{P} \). Hence \( P \) has only two fixed points in \( PW \) and \( \tilde{F} \) has only one.

Now consider the case \( EQ \). We may assume that the points \( (\lambda_1, \lambda_2, \lambda_3, \lambda_4) \)
of the elliptic quadric in \( PG(3, q^t) \) satisfy \( \lambda_1 \lambda_3 + \lambda_2^2 + \lambda_4^3 + a\lambda_2 \lambda_3 = 0 \) (where
the polynomial \( x^2 + ax + 1 \) is irreducible over \( GF(q^t) \)). Again we can take \( F \)
to be the stabilizer of \( < v_1 > \). We can take \( C \) to be the stabilizer of points
corresponding to \( v_1 \) and \( v_3 \); this time \( C \) has order \( q^{2t} - 1 \). The eigenvalues for
a generator \( g \) for \( C \) are \( \xi^{\pm 1+q^j} \) where \( \xi \) is a generator for \( GF(q^{2t})^* \). The eigen-
values for \( \rho(g) \) are \( \prod_{j=1}^{t} \xi_{\epsilon_j q^{j-1} + \nu_j q^{j-1}} \) where each \( \epsilon_j = \pm 1 \) and each \( \nu_j = \pm 1 \).
Of these only two lie in $GF(q^t): \xi^{1+q+q^2+\ldots+q^{2t-1}}$ and $\xi^{-(1+q+q^2+\ldots+q^{2t-1})}$, and these correspond to eigenvectors $v_1$ and $v_2$ respectively, both corresponding to points of $\mathcal{P}$. Hence $\tilde{C}$ has only two fixed points in $PW$ and $\tilde{F}$ has only one.

Finally consider the case $STO$. We take $\xi$ to be a generator for $GF(q^t)$. If we write $q^t = 2^{2l+1}$ (so if $q = 2^e$ then $te = 2l + 1$), then there is an automorphism $\sigma$ of $GF(q^t)$ given by $\sigma(\xi) = \xi^{2^{l+1}}$. With respect to the symplectic basis $v_1, v_2, v_3, v_4$ for $V_0$, the points of $\mathcal{L}$ correspond to vectors $v_1$ and $\alpha v_1 + \beta v_2 + \gamma v_3 + \delta v_4$ where $\alpha + \beta \gamma + \sigma(\beta) + \gamma^2 \sigma(\gamma) = 0$ (c.f. [19]). Again we can take $F$ to be the stabilizer of $<v_1>$ and it will consist of upper-triangular matrices. This time we take $C$ to be the diagonal subgroup (of order $q^t - 1$) with generator $g$ given by

$$
\begin{bmatrix}
\sigma(\xi)\xi & 0 & 0 & 0 \\
0 & \xi & 0 & 0 \\
0 & 0 & \sigma(\xi)^{-1} & \xi^{-1} \\
0 & 0 & 0 & \xi^{-1}
\end{bmatrix}.
$$

The eigenvalues of $g$ are distinct and so $C$ fixes four points of $PG(3, q^t)$ corresponding to $v_1, v_2, v_3$ and $v_4$, only one of which lies on $\mathcal{L}$. The eigenvalues of $\rho(g)$ have the form $\xi^{A(q)}$ where $A(q) = A_0 + A_1q + \ldots + A_{t-1}q^{t-1}$ and each $A_i$ is one of $\pm 1, \pm (2^{l+1} + 1)$. We can write $A(q) = B(q) + 2^{l+1}C(q)$, where $B(q) = B_0 + B_1q + \ldots + B_{t-1}q^{t-1}$, $C(q) = C_0 + C_1q + \ldots + C_{t-1}q^{t-1}$ with each $B_i$ being $\pm 1$ and each $C_i$ being $B_i$ or $0$; since $q$ is a power of 2, the value of $B(q)$ is always non-zero, and $C(q)$ can only be 0 if each $C_i$ is 0. Suppose first that $C_0, C_1, \ldots, C_{t-1}$ are all non-zero. Then $A(q) = (1 + 2^{l+1})B(q)$ and the hcf of $2^{l+1} + 1$ and $k(q) = 1 + q + q^2 + \ldots + q^{t-1}$ is 1. If $\xi^{A(q)} \in GF(q)$, then $k(q)$ divides $A(q)$, i.e., $k(q)$ divides $B(q)$. This is only possible when $B(q) = \pm k(q)$. Thus in this case $g$ has eigenvalues $\xi^{\pm (1+2^{l+1})k(q)}$. Now suppose that at least one of the coefficients $C_i$ is zero. Observe that $q^{(t-1)/2} < 2^{l+1} < q^{(t+1)/2}$ so we can write $2^{l+1} = q^{(t-1)/2}2^d$ for some $0 < d < e$. Indeed $2^{2l+2} = q^{l-1}2^d$ becomes $2q = 2^d$, i.e., $e + 1 = 2d$. Hence $A(q) = B(q) + 2^{l+1}C(q) = B(q) + 2^d q^{(l-1)/2} C(q)$. Suppose that $\xi^{A(q)} \in GF(q)$, then $\xi^{A(q)} = \xi^{A(q)q^j}$ for any $j \geq 0$ and $k(q)$ divides $A(q)q^j$. Suppose that $C_i = 0$ and let $j = (t - 1)/2 - i$. We have $A(q)q^j = B(q)q^j + 2^d q^{t-1-i} C(q) = D_1(q) + D_2(q)(q^t - 1) + 2^d (E_1(q) + E_2(q)(q^t - 1))$ where $D_1(q)$ has degree $t - 1$ in $q$ with coefficients $\pm 1$, and $E_1(q)$ has degree $t - 2$ in $q$ with coefficients 0 or $\pm 1$. We have supposed that $\xi^{A(q)} \in GF(q)$
so \( k(q) \) divides \( A(q)q^j \) and hence \( k(q) \) divides \( D_1(q) + 2^dE_1(q) \). Let \( U \) be the coefficient of \( q^{t-1} \) in \( D_1(q) \), then \( D_1(q) - Uk(q) = 2D_3(q) \), where \( D_3(q) \) has degree at most \( t - 2 \) in \( q \) and coefficients 0 or \( \pm 1 \), and \( k(q) \) divides \( 2D_3(q) + 2^dE_1(q) \). Let \( h(q) = 1 + q + q^2 + \ldots + q^{t-2} \), then \( qh(q) = k(q) - 1 \). Therefore \( |2D_3(q) + 2^dE_1(q)| < 2h(q) + 2^d h(q) < qh(q) < k(q) \). From this we deduce that \( 2D_3(q) + 2^dE_1(q) = 0 \), but each term in the expression \( 2D_3(q) + 2^dE_1(q) \) has the form \( \pm 2q^j \) or \( \pm 2^d q^j \) and so represent different powers of 2, and the sum of such terms can only be 0 if there are no terms, i.e., \( D_3(q) = 0 \) and \( E_1(q) = 0 \). It follows that \( A(q) = \pm k(q) \) (modulo \( q^t - 1 \)) and in this case \( g \) has eigenvalues \( \xi \pm k(q) \). Hence there are four eigenvalues of \( \rho \) lying in \( GF(q) \) so \( C \) has four fixed points in \( PW \), corresponding to \( v_1, v_2, v_3 \) and \( v_4 \). Only the first of these lies in \( P \) but it is nevertheless true that the other three are not fixed by \( \bar{F} \). Hence \( \bar{F} \) has a single fixed point in \( PW \).

In summary, the results above give:

**Theorem 4.9.** (1) Suppose that \( q > 2 \) is even and that \( t \geq 3 \). If \( \mathcal{L} = \text{PG}(1, q^t) \), then the stabilizer of \( \mathcal{P} \) in \( \Omega^+(2^t, q) \) is the normalizer of \( \rho(\text{SL}(2, q^t)) \).

(2) Suppose that \( q > 2 \) is even and that \( t \geq 2 \). If \( \mathcal{L} \) is an elliptic quadric in \( \text{PG}(3, q^t) \), then the stabilizer of \( \mathcal{P} \) in \( \Omega^+(4^t, q) \) is the normalizer of \( \rho(\Omega^{-}(4, q^t)) \).

(3) Suppose that \( q > 2 \) is an odd power of 2 and that \( t \geq 3 \) is odd. If \( \mathcal{L} \) is a Suzuki-Tits ovoid in \( \text{PG}(3, q^t) \), then the stabilizer of \( \mathcal{P} \) in \( \Omega^+(4^t, q) \) is the normalizer of \( \rho(\text{Sz}(q^t)) \).

(4) If \( q = 2 \), then in all three cases \( \mathcal{P} \) is a polygon whose stabilizer is the alternating group on the points.

**Remark 4.10.** Comparing the partial ovoids arising as images of Suzuki-Tits ovoids with those arising as the images of elliptic quadrics, the difference in the structure of the stabilizers shows that the two families of partial ovoids are not equivalent. The cases where \( \mathcal{L} = \text{PG}(1, q^t) \) (with \( t > 2 \) even) and where \( \mathcal{L} \) is an elliptic quadric of \( \text{PG}(3, q^t) \) lead to stabilizers with the same structure, but it is not clear whether or not the partial ovoids are equivalent. Indeed,
the embedding procedure allows for the possibility of a stepped embedding of $PG(1,q^{abcd...})$ as a partial ovoid in $PG(2^a - 1, q^{bcd...})$ that is then embedded in $PG(2^{ab} - 1, q^{cd...})$ and so on, and it is not clear that the resulting partial ovoid is necessarily equivalent to that obtained from a single step embedding of $PG(1,q^{abcd...})$ in $PG(2^{abcd...} - 1, q)$.

4.4 Dye’s partial ovoids

In [6], R.H. Dye constructed new ovoids on a hyperbolic quadric in $PG(7,8)$. Later, in [8], he constructed partial ovoids on quadrics (sometimes elliptic, sometimes hyperbolic) in $PG(2^{m+1},8)$ whose size attains the Blokhuis–Moorhouse bound. The construction of ovoids in $PG(7,8)$ involved an initial construction of nine points of a polygon, followed by the addition of points lying on conics formed by the intersection of various planes with the quadric. This approach formed the basis of the constructions of partial ovoids in the later paper. We are led to ask whether the partial ovoids we have constructed in $PG(2^t - 1,8)$ could be those constructed by Dye. The answer is no for the reason that Dye’s partial ovoids, by construction, meet some planes in conics, whereas our partial ovoids never meet a plane in a conic, as is proved in the following Proposition.

**Proposition 4.11.** Suppose that $P$ is a partial ovoid on a quadric in $PG((2^m)^t-1,q)$ arising as the embedding of a projective line $PG(1,q^t)$ or of a partial ovoid of a symplectic polarity of $PG(2^m - 1, q^t)$ with $m \geq 2$. Then any plane of $PG((2^m)^t-1,q)$ meets $P$ in at most three points.

**Proof.** Let us suppose that $L$ is either the projective line $PG(1,q^t)$ or a partial ovoid of a symplectic polarity of $PG(2^m - 1, q^t)$ with $m \geq 2$, and that $P$ is the image of $L$ in $PG((2^m)^t-1,q)$. We show that the images of four points of $L$ cannot lie in a plane of $PG((2^m)^t-1,q)$. Note that the statement of the theorem is true for $P$ precisely when it is true for $Ph$ whenever $h \in O((2m)^t,q)$ (the orthogonal group associated with the quadric). In particular we may replace $L$ by $Lg$ for any $g \in Sp(2m,q^t)$ and $P$ by $Ph$ where $h = \rho(g)$. Thus we may assume that two of our four points are represented by vectors $x_1$ and $y_1$; we denote the remaining two vectors by $x$ and $y$. We write $y_i = x_{m+i}$ for each $1 \leq i \leq m$ and $x = \sum_{i=1}^m \alpha_i x_i$, $y = \sum_{i=1}^m \beta_i x_i$: in all cases $\alpha_1, \beta_1 \neq 0$, $\alpha_{m+1}, \beta_{m+1} \neq 0$; moreover we may assume that $\alpha_1 = \beta_1 = 1$. 

18
We can see that $x_1 = x_1 \otimes x_1 \otimes x_1 \ldots \otimes x_1 \otimes x_1$ and $y_1 = x_{m+1} \otimes x_{m+1} \otimes x_{m+1} \ldots \otimes x_{m+1} \otimes x_{m+1}$. The expression for $x$ has a component in each subspace $V(P)$ and we can observe that:

- if $i \neq 1$, the component corresponding to pattern $(i1\ldots1)$ is $\sum_{j=1}^{t} \phi^{j-1}(\alpha_i x_i \otimes x_1 \otimes x_1 \ldots \otimes x_1 \otimes x_1)$;

- if $i, j \neq 1$ and either or both of $i \neq j$, $t \geq 3$, the component corresponding to pattern $(ij1\ldots1)$ is $\sum_{j=1}^{t} \phi^{j-1}(\alpha_i \alpha_j x_i \otimes x_j \otimes x_1 \otimes x_1 \ldots \otimes x_1 \otimes x_1)$.

Similarly the expression for $y$ has a component in each subspace $V(P)$ and for components corresponding to $(i1\ldots1)$ ($i \neq 1$) and $(ij1\ldots1)$ ($i, j \neq 1$; and either or both of $i \neq j$, $t \geq 3$) we may simply replace $\alpha$ by $\beta$ in the expressions above.

Suppose that $x_1$, $y_1$, $x$, and $y$ lie in a plane, then $y = ax_1 + by_1 + cx$ for some $a, b, c \in GF(q)$. Then

- if $i \neq 1$, then $\beta_i = c\alpha_i$;

- if $i, j \neq 1$ and either or both of $i \neq j$, $t \geq 3$, then $\beta_i \beta_j = c\alpha_i \alpha_j$.

Note that, since $\alpha_1 = \beta_1 = 1$ and $x \neq y$, the first property tells us that $c \neq 1$. Moreover $\beta_{m+1} = c\alpha_{m+1}$ with $\alpha_{m+1}, \beta_{m+1} = 0$ so $\alpha_{m+1} = \beta_{m+1}$.

Suppose first that $L$ is a projective line. Then $t \geq 3$ and we have equations: $c \neq 0, 1; \beta_{m+1} = c\alpha_{m+1}; \beta_{m+1}\beta_{m+1} = c\alpha_{m+1}\alpha_{m+1}$ that are inconsistent. Hence $x_1, y_1, x, y$ cannot lie in a plane.

Now suppose that $L$ is a partial ovoid. Then $m \geq 2$ and the equations: $c \neq 0, 1; \beta_i = c\alpha_i; \beta_{m+1}\beta_{m+1} = c\alpha_{m+1}\alpha_{m+1}$ (for $i \neq m + 1$) lead to the conclusion that $\alpha_i = \beta_i = 0$ for all $i \neq 1, m + 1$. However this can only happen if $x_1, y_1, x, y$ are collinear, which they are not. Hence in this case also $x_1, y_1, x, y$ cannot lie in a plane.

\[\Box\]

**Acknowledgements:** The first author acknowledges the support of the London Mathematical Society. The second author acknowledges the support
of the Royal Society and the Department of Mathematics of the University of Basilicata.

References


