On ovoids of parabolic quadrics

S. Ball * P. Govaerts L. Storme†

12 January 2005

Abstract

It is known that every ovoid of the parabolic quadric $Q(4,q)$, $q = p^h$, p prime, intersects every three-dimensional elliptic quadric in 1 mod p points. We present a new approach which gives us a second proof of this result and, in the case when $p = 2$, allows us to prove that every ovoid of $Q(4,q)$ either intersects all the three-dimensional elliptic quadrics in 1 mod 4 points or intersects all the three-dimensional elliptic quadrics in 3 mod 4 points.

We also prove that every ovoid of $Q(4,q)$, q prime, is an elliptic quadric. This theorem has several applications, one of which is the non-existence of ovoids of $Q(6,q)$, q prime, $q > 3$.

We conclude with a 1 mod p result for ovoids of $Q(6,q)$.

1 Definitions

Let $PG(n,q)$ denote the n-dimensional projective space over the finite field of order q. The non-singular quadrics in finite projective space are: the non-singular parabolic quadrics $Q(2m,q)$ in $PG(2m,q)$, the non-singular elliptic quadrics $Q^-(2m+1,q)$ in $PG(2m+1,q)$, and the non-singular hyperbolic quadrics $Q^+(2m-1,q)$ in $PG(2m-1,q)$. For $m \geq 2$, they are finite classical polar spaces of rank m, see [8] or [17].

Let $\mathcal{P}$ be a finite classical polar space of rank k. A *generator* of $\mathcal{P}$ is a $(k-1)$-dimensional subspace on $\mathcal{P}$. An *ovoid* (respectively a *partial ovoid*) O of $\mathcal{P}$ is a set of points of $\mathcal{P}$ such that every generator of $\mathcal{P}$ contains exactly (respectively at most) one point of O. A table that lists the known (non-)existence results on ovoids of finite classical polar spaces can be found in [29]. The tangent hyperplane to $\mathcal{P}$ at a point $P \in \mathcal{P}$ is denoted by $T_P(\mathcal{P})$ or $P^\perp$, where $\perp$ is the polarity corresponding to $\mathcal{P}$.

*The first author acknowledges the support of the Ministerio de Ciencia y Tecnología, España.
†The third author thanks the Fund for Scientific Research - Flanders (Belgium) for a Research Grant.

For a definition of the split Cayley hexagon $\mathrm{H}(q)$ and more information on generalised polygons, see [32]. A *partial ovoid* of $\mathrm{H}(q)$ is a set of mutually opposite points on $\mathrm{H}(q)$. It is called an *ovoid* if it has size q^3+1.

2 Ovoids of $\mathrm{Q}(4,q)$

In the theory of minimal t-fold blocking sets in finite projective spaces, *t mod p results* [19, 25, 26] have proven to be very useful. Such results tell "how" a hyperplane intersects the minimal t-fold blocking sets: *in t mod p points*. They make the blocking sets easier to handle and have made several classification theorems possible.

There is hope that similar results for other objects will prove to be equally fruitful. The following 1 mod p result on ovoids of the quadric $\mathrm{Q}(4,q)$, was proven for $p=2$ by Bagchi and Narasimha Sastry [1], and for all primes by Ball [2].

Theorem 1 *Let O be an ovoid of $\mathrm{Q}(4,q)$, $q=p^h$, p prime. Every elliptic quadric $\mathrm{Q}^-(3,q)$ on $\mathrm{Q}(4,q)$ intersects O in 1 mod p points.*

In this paper, we use this theorem to prove that every ovoid of $\mathrm{Q}(4,q)$, q prime, is an elliptic quadric. We also provide a new proof of Theorem 1, using a different approach to that used in [2], which allows us to extend Theorem 1 to a stronger result in the case when q is even, namely Theorem 4.

For the purpose of this paper, $\mathrm{Q}(4,q)$ is defined by the quadratic form

$$X_0X_4+X_1X_3+X_2^2=0.$$

If O is an ovoid of $\mathrm{Q}(4,q)$ that contains the point $(0,0,0,0,1)$, then O is necessarily of the form

$$\{(0,0,0,0,1)\}\cup\{(1,x,y,g(x,y),-y^2-xg(x,y)) : x,y\in \mathrm{GF}(q)\} \tag{1}$$

for some polynomial $g(x,y)$.

Lemma 1 *The set* (1) *is an ovoid of* $\mathrm{Q}(4,q)$ *iff for all $a\in\mathrm{GF}(q)$*

$$\{(ax+y,g(x,y)-ay) : x,y\in\mathrm{GF}(q)\}=\mathrm{GF}(q)^2.$$

Proof. If $y'+ax'=y+ax$ and $g(x',y')-ay'=g(x,y)-ay$, then

$$(1,x',y',g(x',y'),-y'^2-x'g(x',y'))\in(1,x,y,g(x,y),-y^2-xg(x,y))^{\perp}.$$

Hence the condition is necessary. It is not hard to check that it is sufficient. □

If O is an ovoid of $\mathrm{Q}(4,q)$ that does not contain the point $(0,0,0,0,1)$, but does contain the point $(0,0,0,1,0)$, then O is necessarily of the form

$$\{(0,0,0,1,0)\} \cup \{(0,1,z,-z^2,-f(z)) : z \in \mathrm{GF}(q)\}$$
$$\cup \{(1,x,y,h(x,y),-y^2-xh(x,y)) : x,y \in \mathrm{GF}(q),\ x \neq 0\} \quad (2)$$

for some polynomials $h(x,y)$ and $f(z)$.

Lemma 2 *The set* (2) *is an ovoid of* $\mathrm{Q}(4,q)$ *iff for all* $a \in \mathrm{GF}(q)$

$$\{(ax+y,h(x,y)-ay) : x,y \in \mathrm{GF}(q), x \neq 0\} \cup \{(z,az+f(-a)) : z \in \mathrm{GF}(q)\} = \mathrm{GF}(q)^2.$$

Proof. If $y'+ax' = y+ax$ and $h(x',y')-ay' = h(x,y)-ay$, then

$$(1,x',y',h(x',y'),-y'^2-x'h(x',y')) \in (1,x,y,h(x,y),-y^2-xh(x,y))^{\perp}.$$

If $z = ax+y$ and $az+f(-a) = h(x,y)-ay$, then

$$(0,1,-a,-a^2,-f(-a)) \in (1,x,y,h(x,y),-y^2-xh(x,y))^{\perp}.$$

As in the proof of Lemma 1, it now suffices to check that the condition is sufficient. □

We will need the following lemma to prove Lemma 4.

Lemma 3

$$\prod_{u,v \in \mathrm{GF}(q)} (T+uX+vY) = T^{q^2} - (Y^{q^2-q} + (X^q - XY^{q-1})^{q-1})T^q + (YX^q - XY^q)^{q-1}T.$$

Proof. Apply the equality $\prod_{a \in \mathrm{GF}(q)} (U+aV) = U^q - UV^{q-1}$ twice. □

Lemma 4 *Let O be an ovoid of* $\mathrm{Q}(4,q)$, *$q = p^h$, p prime. Every hyperplane intersects O in* $1 \bmod p$ *or zero points.*

Proof. Let O be an ovoid of $\mathrm{Q}(4,q)$ defined according to (1) by the polynomial $g(x,y)$ and define a Rédei polynomial G in three variables as

$$G(T,X,Y) = \prod_{u,v \in \mathrm{GF}(q)} (T+uX+vY+g(u,v)) = \sum_{j=0}^{q^2} \sigma_j(X,Y)T^{q^2-j}.$$

Considering the terms of degree q^2 in G and applying Lemma 3, the degree of the polynomial σ_j is at most $j-1$ whenever $0 < j < q^2-q$.

By Lemma 1, we have that for all $a \in \mathrm{GF}(q)$

$$G(T,aZ,Z-a) = \prod_{u,v\in \mathrm{GF}(q)} (T+(au+v)Z+g(u,v)-av) = \prod_{u,v\in \mathrm{GF}(q)} (T+uZ+v)$$

and then by Lemma 3 (with $X=Z$ and $Y=1$) that

$$G(T,aZ,Z-a) = T^{q^2} - ((Z^q-Z)^{q-1}+1)T^q + (Z^q-Z)^{q-1}T.$$

Hence the polynomial $\sigma_j(aZ,Z-a) \equiv 0$ whenever $0<j<q^2-q$.

Let $f_j(X,Y)$ be the homogeneous polynomial of terms of highest degree of $\sigma_j(X,Y)$. Then $f_j(aZ,Z-a)\equiv 0$ for all $a \in GF(q)$ and so the degree of f_j is either at least q or $f_j(X,Y)\equiv 0$. Hence for $0<j\leq q$, since the degree of f_j is equal to the degree of σ_j which is less than q, we have that $f_j(X,Y)\equiv 0$ and therefore $\sigma_j(X,Y)\equiv 0$.

So

$$G(T,X,Y) = T^{q^2} + \sum_{j=0}^{q^2-q-1} \sigma_{q^2-j}(X,Y)T^j. \tag{3}$$

Differentiate the Rédei polynomial with respect to T

$$\frac{\partial G}{\partial T} = \sum_{u,v\in \mathrm{GF}(q)} \frac{G(T,X,Y)}{T+uX+vY+g(u,v)}.$$

Evaluate at $X=x$ and $Y=y$, and multiply through by T^q-T. Then we have a polynomial identity and the divisibility

$$G(T,x,y) \mid (T^q-T)\frac{\partial G}{\partial T}(T,x,y).$$

The left-hand side has degree q^2 and the right-hand side has degree less than q^2. Hence, the right-hand side is zero and so $\sigma_j(x,y)=0$ for all $(x,y)\in \mathrm{GF}(q)^2$ whenever $j \not\equiv 0 \bmod p$. But then $G(T,x,y)$ is a p-th power. This implies that there are 0 mod p pairs $(u,v)\in \mathrm{GF}(q)^2$ such that

$$ux+vy+g(u,v) = -c$$

for any given $(x,y,c)\in \mathrm{GF}(q)^3$. Hence, the hyperplane

$$cX_0+xX_1+yX_2+X_3 = 0$$

is incident with $(0,0,0,0,1)$ and 0 mod p other points of the ovoid. The other hyperplanes incident with $(0,0,0,0,1)$, of the form

$$cX_0+xX_1+yX_2 = 0,$$

are trivially incident with 1 mod q points of the ovoid. The point $(0,0,0,0,1)$ was chosen arbitrarily from the ovoid; so we have shown that if a hyperplane is incident with a point of the ovoid, then it is incident with 1 mod p points of the ovoid. $\square$

Let B be a multiset of points in $\mathrm{AG}(n,q)$ with weight function μ. The *support* S of B is the set of points P of $\mathrm{AG}(n,q)$ with multiplicity $\mu(P)$ greater than zero. The size of the intersection of B with a subspace Π of $\mathrm{AG}(n,q)$ equals $\sum_{P\in S\cap\Pi}\mu(P)$. The following result of Blokhuis and Wilbrink is unpublished. We thank them for giving us the permission to include the proof.

Theorem 2 *Let B be a multiset of points in $\mathrm{AG}(n,q)$, $n>1$, $q=p^h$, p prime, such that every hyperplane intersects B in $1 \bmod p$ or in zero points. Then the support of B has at most $q-p+1$ elements and every non-zero weight is $1 \bmod p$.*

Proof. (Blokhuis and Wilbrink [4]) For $n=2$, the proof is essentialy due to Blokhuis and Mazzocca [3]. Denote the support of B by S. Identify $\mathrm{AG}(2,q)$ in a natural way with $\mathrm{GF}(q^2)$ and consider the polynomial

$$F(X)=\sum_{b\in S}\mu(b)(X-b)^{q-1}.$$

Counting the points of B by looking at the lines through a point of B, we deduce that $\sum_{b\in S}\mu(b)\equiv 1 \bmod p$. As $\sum_{b\in S}\mu(b)$ is the coefficient of X^{q-1} in $F(X)$, the polynomial $F(X)$ has degree $q-1$. Since for all $d,e\in\mathrm{GF}(q^2)$, the number $(d-e)^{q-1}$ is a $q+1$-st root of unity denoting the direction of the line joining d and e, and since $\sum_{a^{q+1}=1}a=0$, it follows that $F(b)=0$ for each $b\in B$. This shows that the support of B has at most $q-1$ points.

If some point of B has multiplicity different from $1 \bmod p$, then each of the $q+1$ lines through that point must contain at least one further point of B, a contradiction. It follows that $|B|$ equals the size of its support $\bmod p$, whence $|\mathrm{support}(B)|\le q-p+1$.

Now we use induction on n. Let B be a multiset in $\mathrm{AG}(n,q)$ satisfying the conditions of the theorem and let P be a point at infinity. In the quotient space of P, B forms a $1 \bmod p$ or zero multiset. Therefore the support of B is contained in $q-p+1$ lines through P. Suppose that the support of B has more than $q-p+1$ points and take any subset of size $q-p+2$ of the support. This subset determines at most $q^2/2$ directions, hence in the quotient space of some point Q at infinity, B forms a multiset with at least $q-p+2$ points in its support, a contradiction. □

Lemma 5 *Let O be an ovoid of $\mathrm{Q}(4,q)$, $q=p^h$, p prime. Every hyperplane intersects O in at least one point.*

Proof. If there would exist a hyperplane H missing O, then Theorem 2 could be used on O in $\mathrm{AG}(4,q)=\mathrm{PG}(4,q)\setminus H$ to show that $|O|\le q-p+1$. □

Remark 1 *It is possible to prove Lemma 5 without using Theorem 2. This can be done in a way similar to the proof of Lemma 7.*

Theorem 1 now follows from Lemma 4 and Lemma 5.

Theorem 3 *Let O be an ovoid of* $\mathrm{Q}(4,q)$ *and suppose that every hyperplane intersects O in* $1 \bmod q$ *points, then O is an elliptic quadric.*

Proof. This proof is based on the proof of [14, Theorem 4.2].

Let O be an ovoid of $\mathrm{Q}(4,q)$ and let x_i denote the number of hyperplanes incident with exactly i points of O. By counting in two ways hyperplanes, incident pairs (P,E), triples (P,Q,E), and 4-tuples (P,Q,R,E), where P, Q and R are distinct points of O and E is a hyperplane, we can compute the numbers $\sum x_i$, $\sum ix_i$, $\sum i(i-1)x_i$ and $\sum i(i-1)(i-2)x_i$. These numbers will be independent of the ovoid. Hence we can compute (again, independent from the ovoid) the number $\sum(i-1)(i-q-1)(q^2+1-i)x_i$. As this number is zero for the elliptic quadric, it is zero for any ovoid O.

Using the assumption that every hyperplane intersects O in $1 \bmod q$ points, it follows that every term in $\sum(i-1)(i-q-1)(q^2+1-i)x_i$ is non-negative and therefore zero and so every hyperplane is incident with either 1, $q+1$, or q^2+1 points of O.

Now suppose that there does not exist a hyperplane containing q^2+1 points of O. Then all hyperplanes intersect O in either 1 or $q+1$ points. Let π be any plane containing more than two points of O, say $|\pi \cap O| = x > 2$, and count the points of O by looking at the hyperplanes through π. This results in

$$q^2+1 = x + (q+1)(q+1-x),$$

hence $x = 2$, a contradiction. So, there exists a hyperplane intersecting O in q^2+1 points. This hyperplane intersects $\mathrm{Q}(4,q)$ in an elliptic quadric $\mathrm{Q}^-(3,q)$, all of whose points are elements of O. □

Corollary 1 *If q is prime, then every ovoid of* $\mathrm{Q}(4,q)$ *is an elliptic quadric.*

Remark 2

1. *This result was already known for $q \in \{2,3,5,7\}$, see [7, 9, 10, 11, 20, 21].*
2. *There are ovoids of $Q(4,q)$ that are not elliptic quadrics. There are examples due to Kantor [18] one of which exists for every q odd and not a prime, and another which exists for all $q = 3^{2h+1} \geq 27$. There is an example due to Tits [31] which exists for every $q > 2$ even and not a square. The only other known examples are the example due to Thas and Payne [30], which exists when $q = 3^h \geq 27$, and the example due to Penttila and Williams [24], which exists when $q = 3^5$.*

Lemma 6 *Let $q > 2$ be even and suppose that there is a hyperplane E incident with* $3 \bmod 4$ *points of an ovoid O of* $\mathrm{Q}(4,q)$*. Let $P \in O \cap E$ and let $\pi = E \cap T_P(\mathrm{Q}(4,q))$. Then, apart from $T_P(\mathrm{Q}(4,q))$, every hyperplane containing π is incident with* $3 \bmod 4$ *points of O.*

Proof. Let P be the point $(0,0,0,0,1)$ and let E be the hyperplane

$$cX_0 + xX_1 + yX_2 + X_3 = 0.$$

The hyperplane $T_P(\mathrm{Q}(4,q))$ is the hyperplane $X_0 = 0$, so we wish to show that for each $a \in \mathrm{GF}(q)$, the hyperplane

$$aX_0 + xX_1 + yX_2 + X_3 = 0$$

is incident with 3 mod 4 points of O.

Let O be an ovoid defined by a function $g(x,y)$ as in (1) and let $G(T,X,Y)$ be the associated Rédei polynomial as in the proof of Lemma 4. The hyperplane E is incident with P and 2 mod 4 other points of the ovoid O, by hypothesis. Arguing as in the proof of Lemma 4, this implies that the linear factor $T-c$ occurs with multiplicity 2 mod 4 in the polynomial $G(T,x,y)$. Hence

$$G(T,x,y) \in \mathrm{GF}(q)[T^2] \setminus \mathrm{GF}(q)[T^4].$$

We can write

$$G(T,x,y) = (T^{q^2/2} + L(T))^2,$$

where L', the derivative of L, is not zero and the degree of $L(T)$ is at most $q^2/2 - q/2 - 1$, according to (3). The polynomial $T^{q^2/2} + L(T)$ is the product of linear factors in $\mathrm{GF}(q)[T]$, so the product of its distinct linear factors divides $T^q + T$. The repeated factors divide its derivative and so we have the divisibility

$$T^{q^2/2} + L(T) \mid (T^q + T)L'(T).$$

The right-hand side is not zero and the quotient $M(T)$ has degree at most $q/2 - 2$. If we differentiate the identity

$$(T^{q^2/2} + L(T))M(T) = (T^q + T)L'(T),$$

then we see that

$$M'(T)T^{q^2/2} + (L(T)M(T))' = L'(T).$$

The degree of $(L(T)M(T))'$ is at most $q^2/2 - 4$, so $M'(T) = 0$ and $M(T) = 1$. Hence

$$G(T,x,y) = (T^q + T)^2 R(T)^4,$$

where $L'(T) = R(T)^2$. For all $a \in \mathrm{GF}(q)$, the linear factor $T + a$ is a factor of $G(T,x,y)$ with multiplicity 2 mod 4. So there are 2 mod 4 pairs (u,v) such that

$$ux + vy + g(u,v) = a$$

and hence the hyperplane

$$aX_0 + xX_1 + yX_2 + X_3 = 0$$

is incident with 2 mod 4 points of $O \setminus \{(0,0,0,0,1)\}$. □

Lemma 7 *Let $q > 2$ be even and suppose that there is a hyperplane E incident with* 3 mod 4 *points of an ovoid O of* $\mathrm{Q}(4,q)$*. Let $P \in (E \cap \mathrm{Q}(4,q)) \setminus O$ and let $\pi = E \cap T_P(\mathrm{Q}(4,q))$. Then, apart from $T_P(\mathrm{Q}(4,q))$, every hyperplane containing π is incident with* 3 mod 4 *points of O.*

Proof. Let P be the point $(0,0,0,0,1)$, not a point of O, and let E be the hyperplane

$$cX_0 + xX_1 + yX_2 + X_3 = 0.$$

The hyperplane $T_P(\mathrm{Q}(4,q))$ is the hyperplane $X_0 = 0$. Let O be an ovoid defined by the functions $h(x,y)$ and $f(z)$ as in (2). The points of O in the hyperplane $X_0 = 0$ are the $q+1$ points $\{(0,0,0,1,0)\} \cup \{(0,1,z,z^2,f(z)) : z \in \mathrm{GF}(q)\}$.

Since E is incident with 3 mod 4 points of O, it must meet $\mathrm{Q}(4,q)$ in a three-dimensional elliptic quadric, so the quadratic equation $Z^2 + yZ + x = 0$ has no solutions in $\mathrm{GF}(q)$ and E is therefore skew to the points of O that lie in the hyperplane $X_0 = 0$.

So we wish to show that the hyperplanes $aX_0 + xX_1 + yX_2 + X_3 = 0$, where a is any element of $\mathrm{GF}(q)$, are incident with 3 mod 4 points of the set

$$\{(1,x,y,h(x,y),y^2 + xh(x,y)) : x,y \in \mathrm{GF}(q),\ x \neq 0\}.$$

Define a Rédei polynomial H in three variables as

$$H(T,X,Y) = \prod_{u,v \in \mathrm{GF}(q),\ u \neq 0} (T + uX + vY + h(u,v)) = \sum_{j=0}^{q^2-q} \psi_j(X,Y) T^{q^2-q-j}.$$

The degree of H is $q^2 - q$, so the degree of the polynomial ψ_j is at most j. Similarly to Lemma 3,

$$\prod_{z \in \mathrm{GF}(q)} (T + zZ + (az + f(-a))) = T^q - (Z+a)^{q-1}T + f(-a)(1 - (Z+a)^{q-1}).$$

By Lemma 2, we have that for all $a \in \mathrm{GF}(q)$

$$H(T,aZ,Z-a) = \prod_{u,v \in \mathrm{GF}(q), u \neq 0} (T + (au+v)Z + h(u,v) - av)$$

$$= \left(\prod_{u,v \in \mathrm{GF}(q)} (T + uZ + v) \right) / (T^q - (Z+a)^{q-1}T + f(-a)(1 - (Z+a)^{q-1})),$$

and then by Lemma 3 again that

$$H(T,aZ,Z-a)(T^q - (Z+a)^{q-1}T + f(-a)(1 - (Z+a)^{q-1}))$$

$$= T^{q^2} + (-(Z^q - Z)^{q-1} - 1)T^q + (Z^q - Z)^{q-1}T.$$

Hence, for all $a \in \mathrm{GF}(q)$, the polynomial $\psi_j(aZ, Z-a) \equiv 0$ whenever $0 < j < q-1$ and following the argument in Lemma 4, $\psi_j(X,Y) \equiv 0$ for $0 < j < q-1$.

So we have

$$H(T,X,Y) = T^{q^2-q} + \sum_{j=0}^{q^2-2q+1} \psi_{q^2-q-j}(X,Y)T^j. \tag{4}$$

As in Lemma 4, for all $(x,y) \in \mathrm{GF}(q)^2$, we have the divisibility

$$H(T,x,y) \mid (T^q - T)\frac{\partial H}{\partial T}(T,x,y).$$

The left-hand side has degree q^2-q and the right-hand side has degree less than or equal to q^2-q.

As, by hypothesis, the hyperplane E is incident with 3 mod 4 points of the ovoid O, the linear factor $T+c$ occurs with multiplicity 3 mod 4 in the polynomial $H(T,x,y)$. So either $T+c$ occurs with multiplicity 2 mod 4 in the polynomial

$$H_1(T) := \frac{\partial H}{\partial T}(T,x,y),$$

or $H_1(T)=0$. If $H_1(T)=0$, then $H(T,x,y)$ would be a square such that the linear factor $T+c$ would occur with even multiplicity in $H(T,x,y)$, a contradiction. Hence the linear factor $T+c$ occurs with multiplicity 2 mod 4 in the polynomial $H_1(T) := \frac{\partial H}{\partial T}(T,x,y)$.

The polynomial $H_1(T)$ is a constant multiple of $H(T,x,y)/(T^q+T)$ and so by (4) it has degree q^2-2q, is a square and we can write

$$H_1(T) = (T^{q^2/2-q} + H_2(T))^2$$

where the degree of $H_2(T)$ is at most $q^2/2-3q/2$. The hypothesis implies that the polynomial $T^{q^2/2-q}+H_2(T)$ has a factor that occurs an odd number of times and so $H_2'(T) \not\equiv 0$. Moreover it splits completely into linear factors in $\mathrm{GF}(q)[T]$. So, as in the proof of Lemma 6, we have the divisibility

$$T^{q^2/2-q} + H_2(T) | (T^q+T)H_2'(T).$$

Let the quotient of this division be $M_1(T)$ and note that it has degree at most $q/2-2$. Differentiate the corresponding equality to see that

$$M_1'(T)T^{q^2/2-q} + (H_2(T)M_1(T))' = H_2'(T).$$

The degree of $(H_2(T)M_1(T))'$ is at most $q^2/2-q-4$ and so $M_1'=0$ and $M_1=1$. This implies that $H(T,x,y)$ is a constant multiple of

$$(T^q+T)^3R(T)^4,$$

where $H_2'(T) = R(T)^2$. So for all $a \in \mathrm{GF}(q)$, there are 3 mod 4 pairs (u, v) such that

$$ux + vy + h(u, v) = a,$$

and hence the hyperplane

$$aX_0 + xX_1 + yX_2 + X_3 = 0$$

is incident with 3 mod 4 points of $O \setminus T_P(\mathrm{Q}(4,q))$. $\square$

Remark 3 *Lemma 5 can be proven similarly to Lemma 7.*

Theorem 4 *Let O be an ovoid of $\mathrm{Q}(4,q)$, q even. Either every elliptic quadric on $\mathrm{Q}(4,q)$ intersects O in 3 mod 4 points or every elliptic quadric on $\mathrm{Q}(4,q)$ intersects O in 1 mod 4 points.*

Proof. Suppose that there is a hyperplane E intersecting O in 3 mod 4 points. By Lemma 6 and Lemma 7, every non-tangent hyperplane that contains a tangent plane of the elliptic quadric $E \cap \mathrm{Q}(4,q)$ is incident with 3 mod 4 points of O. Let E_1 be any other hyperplane that meets $\mathrm{Q}(4,q)$ in an elliptic quadric. Consider its intersection with the $q+1$ hyperplanes that contain a given tangent plane of $E \cap \mathrm{Q}(4,q)$. Then E_1 intersects at least one of these hyperplanes, call it E_2, in a plane that is a tangent plane to the elliptic quadric $E_2 \cap \mathrm{Q}(4,q)$. Now apply Lemma 6 and Lemma 7 to E_2 to conclude that E_1 is incident with 3 mod 4 points of O. $\square$

3 Applications when q is prime

The fact that every ovoid of $\mathrm{Q}(4,q)$, q prime, is an elliptic quadric is not unexpected and a number of results have already appeared assuming exactly this. They yield immediate corollaries to Corollary 1.

As a first application of Corollary 1, non-existence results on (partial) ovoids of $\mathrm{Q}(6,q)$ and the generalised hexagon $\mathrm{H}(q)$ are presented.

Theorem 5 ([22]) *If for some q, $q > 3$, every ovoid of $\mathrm{Q}(4,q)$ is an elliptic quadric, then $\mathrm{Q}(6,q)$ has no ovoid.*

Corollary 2 *For $q > 3$ prime, $\mathrm{Q}(6,q)$ has no ovoid.*

Corollary 3 *For $q > 3$ prime, $\mathrm{H}(q)$ has no ovoid.*

Proof. Thas [28] proves that a (partial) ovoid of $\mathrm{Q}(6,q)$ is a (partial) ovoid of $\mathrm{H}(q)$ and vice versa. $\square$

Corollary 4 *For $q > 3$ prime, a partial ovoid of $\mathrm{H}(q)$ has size at most $q^3 - 1$.*

Proof. In [15], it is proven that a partial ovoid of size q^3 of $\mathrm{H}(q)$ can be extended to an ovoid of $\mathrm{H}(q)$. $\square$

Corollary 5 *For $q > 3$ prime, a partial ovoid of $\mathrm{Q}(6,q)$ has size at most $q^3 - 1$.*

Proof. See the proof of Corollary 3. $\square$

Since the non-existence of ovoids of $\mathrm{Q}(6,q)$, $q > 3$ prime, is now known, the problem arises of determining the *smallest blocking sets* of $\mathrm{Q}(2n,q)$, $n \geq 3$, $q > 3$ prime. A *blocking set* of $\mathrm{Q}(2n,q)$ is a set of points of $\mathrm{Q}(2n,q)$ intersecting every generator of $\mathrm{Q}(2n,q)$ in at least one point. The following result on the smallest blocking sets of $\mathrm{Q}(2n,q)$, $n \geq 3$, $q > 3$ prime, was first proven for $n = 3$ and $q = 5,7$ by De Beule and Storme [13]; the proof dealing with all prime values $q > 3$ was given by De Beule and Metsch [12]. The result for $n > 3$ follows from the arguments of De Beule and Storme [13].

Theorem 6 ([12], [13]) *The smallest blocking sets of $\mathrm{Q}(2n,q)$, $q > 3$ prime, $n \geq 3$, are the truncated cones $\Pi_{n-3}\mathrm{Q}^-(3,q) \setminus \Pi_{n-3}$ contained in $\mathrm{Q}(2n,q)$, where Π_{n-3} is an $(n-3)$-dimensional space contained in $\mathrm{Q}(2n,q)$ and where $\mathrm{Q}^-(3,q)$ is a 3-dimensional elliptic quadric of $\mathrm{Q}(2n,q)$ in a 3-space skew to Π_{n-3}.*

A second application is a characterisation of the generalised quadrangle $\mathrm{Q}^-(5,q)$. In the statement of this theorem, a *subtended ovoid* in Δ is an ovoid of Δ obtained by taking the intersection of Δ with the q^2+1 lines of Γ through a point of $\Gamma \setminus \Delta$.

Theorem 7 ([5], [6]) *Let Γ be a generalised quadrangle of order (q,q^2) with a subquadrangle Δ isomorphic to $Q(4,q)$. If all subtended ovoids in Δ are elliptic quadrics, then Γ is isomorphic to $Q^-(5,q)$.*

Corollary 6 *If Γ is a generalised quadrangle of order (q,q^2), q prime, that has a subquadrangle isomorphic to $Q(4,q)$, then Γ is isomorphic to $Q^-(5,q)$.*

To conclude this section, we state the dual result of Corollary 1.

Theorem 8 *Every spread of $\mathrm{W}_3(q)$, q prime, is a regular spread of $\mathrm{PG}(3,q)$.*

Proof. The generalised quadrangle $\mathrm{Q}(4,q)$ is the point-line dual of the generalised quadrangle $\mathrm{W}_3(q)$ [23]. $\square$

4 Ovoids of $\mathrm{Q}(6,q)$

A 1 mod p property also holds for ovoids of $\mathrm{Q}(6,q)$.

Theorem 9 *An ovoid O of $\mathrm{Q}(6,q)$, $q = p^h$, p prime, intersects every elliptic quadric $\mathrm{Q}^-(5,q)$ on $\mathrm{Q}(6,q)$ in 1 mod p points.*

Proof. Let $P \in \mathrm{Q}(6,q) \setminus O$ and let π_4 be a 4-space in $T_P(\mathrm{Q}(6,q))$ that does not contain P. Then π_4 intersects $\mathrm{Q}(6,q)$ in a parabolic quadric Q_4 isomorphic to $Q(4,q)$ and $T_P(\mathrm{Q}(6,q)) \cap O$ is projected from P onto an ovoid O^* of Q_4. By Theorem 1, every elliptic quadric $\mathrm{Q}^-(3,q)$ of Q_4 contains 1 mod p points of O^*. Hence, for each point $P \in \mathrm{Q}(6,q) \setminus O$, every cone $P\mathrm{Q}^-(3,q)$ on $\mathrm{Q}(6,q)$ is incident with 1 mod p points of O.

Let Q_5^- be any elliptic quadric $\mathrm{Q}^-(5,q)$ on $\mathrm{Q}(6,q)$ and denote the hyperplane of $\mathrm{PG}(6,q)$ containing it by H. Consider a line l of Q_5^- skew to O. Such a line exists since Q_5^- has no ovoids [28]. Denote the points on l by $P_0, P_1, \ldots, P_q$. The tangent hyperplanes $T_{P_i}(\mathrm{Q}(6,q))$ intersect H in 4-spaces $T_{P_i}(\mathrm{Q}_5^-)$ for each $i \in \{0,1,\ldots,q\}$. Let

$$\begin{aligned} \pi_3 &= T_{P_0}(\mathrm{Q}_5^-) \cap T_{P_1}(\mathrm{Q}_5^-) \\ &= T_{P_0}(\mathrm{Q}(6,q)) \cap T_{P_1}(\mathrm{Q}(6,q)) \cap H. \end{aligned}$$

Suppose that $|\pi_3 \cap O| = x$. The 4-spaces $T_{P_i}(\mathrm{Q}_5^-) \subseteq T_{P_i}(\mathrm{Q}(6,q))$, $i = 0,1,\ldots,q$, define a pencil of 4-spaces through π_3 in H. Since $|T_{P_i}(\mathrm{Q}_5^-) \cap O| \equiv 1 \bmod p$, counting the number of points of O in this pencil of 4-spaces yields

$$\begin{aligned} |\mathrm{Q}_5^- \cap O| &\equiv (q+1)\cdot 1 - qx \pmod{p} \\ &\equiv 1 \pmod{p}. \end{aligned}$$

Since Q_5^- was chosen arbitrarily, the theorem is proven. □

Remark 4

1. *If $q = 3^h$, then $\mathrm{Q}(6,q)$ has ovoids [18, 27, 28].*
2. *It is not necessary to prove a similar result on higher-dimensional parabolic quadrics since Gunawardena and Moorhouse [16] (for q odd), and Thas [28] (for q even) have proven that such quadrics have no ovoids.*

Acknowledgements The suggestions of the referee have simplified several proofs in this paper. In particular, we want to thank the referee for reminding us of the existence of the previously unpublished Theorem 2 of Blokhuis and Wilbrink. We are grateful for their permission to include the proof of this theorem. We would like to thank Dr. Michel Lavrauw for his careful reading of the original manuscript.

References

[1] B. Bagchi and N. S. Narasimha Sastry, 'Even order inversive planes, generalized quadrangles and codes', *Geom. Dedicata*, 22 (1987) 137–147.

[2] S. Ball, 'On ovoids of $O(5,q)$', *Adv. Geom.*, 4 (2004) 1–7.

[3] A. Blokhuis and F. Mazzocca, 'On maximal sets of nuclei in $PG(2,q)$ and quasi-odd sets in $AG(2,q)$', in: *Advances in finite geometries and designs (Chelwood Gate, 1990)* (Oxford Univ. Press, New York, 1991), pp. 27–34.

[4] A. Blokhuis and H. Wilbrink, unpublished manuscript.

[5] L. Brouns, J. A. Thas and H. Van Maldeghem, 'A characterization of $Q(5,q)$ using one subquadrangle $Q(4,q)$', *European J. Combin.*, 23 (2002) 163–177.

[6] M. R. Brown, 'A characterisation of the generalized quadrangle $Q(5,q)$ using cohomology', *J. Algebraic Combin.*, 15 (2002) 107–125.

[7] R. H. Bruck, 'Construction problems of finite projective planes', in: *Combinatorial Mathematics and its Applications (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967)* (Univ. North Carolina Press, Chapel Hill, N.C., 1969), pp. 426–514.

[8] P. J. Cameron, *Projective and Polar Spaces* (QMW Maths Notes 13, 1991), http://www.maths.qmw.ac.uk/∼pjc/pps.

[9] T. Czerwinski, 'The collineation groups of the translation planes of order 25', *Geom. Dedicata*, 39 (1991) 125–137.

[10] T. Czerwinski and D. Oakden, 'The translation planes of order twenty-five', *J. Combin. Theory Ser. A*, 59 (1992) 193–217.

[11] E. H. Davis, 'Translation planes of order 25 with nontrivial $X-OY$ perspectivities', in: *Proceedings of the Tenth Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1979)* (Winnipeg, Man., 1979. Utilitas Math.), pp. 341–348.

[12] J. De Beule and K. Metsch, 'The smallest minimal blocking sets of $Q(2n,q)$, q prime', *J. Combin. Theory Ser. A*, 106 (204), 327–333.

[13] J. De Beule and L. Storme, 'The smallest minimal blocking sets of $Q(2n,q)$ for small odd q', *Discrete Math.*, to appear.

[14] J. Eisfeld, L. Storme and P. Sziklai, 'Minimal covers of the Klein quadric', *J. Combin. Theory Ser. A*, 95 (2001) 145–157.

[15] P. Govaerts, L. Storme and H. Van Maldeghem, 'On a particular class of minihypers and its applications. III. Applications', *European J. Combin.*, 23 (2002) 659–672.

[16] A. Gunawardena and G. E. Moorhouse, 'The non-existence of ovoids in $O_9(q)$', *European J. Combin.*, 18 (1997) 171–173.

[17] J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries* (The Clarendon Press, Oxford University Press, New York, 1991).

[18] W. M. Kantor, 'Ovoids and translation planes', *Canad. J. Math.*, 34 (1982) 1195–1207.

[19] L. Lovász and T. Szőnyi, 'Multiple blocking sets and algebraic curves', abstract from *Finite Geometry and Combinatorics* (Third International Conference at Deinze (Belgium), May 18–24, 1997).

[20] R. Mathon and G. F. Royle, 'The translation planes of order 49', *Des. Codes Cryptogr.*, 5 (1995) 57–72.

[21] D. J. Oakden, 'Spreads in three-dimensional projective space'. Doctoral thesis, University of Toronto, 1973.

[22] C. M. O'Keefe and J. A. Thas, 'Ovoids of the quadric $Q(2n,q)$', *European J. Combin.*, 16 (1995) 87–92.

[23] S. E. Payne and J. A. Thas, *Finite Generalized Quadrangles* (Pitman, Boston, Mass., 1984).

[24] T. Penttila and B. Williams, 'Ovoids of parabolic spaces', *Geom. Dedicata*, 82 (2000) 1–19.

[25] T. Szőnyi, 'Blocking sets in Desarguesian affine and projective planes', *Finite Fields Appl.*, 3 (1997) 187–202.

[26] T. Szőnyi and Zs. Weiner, 'Small blocking sets in higher dimensions', *J. Combin. Theory Ser. A*, 95 (2001) 88–101.

[27] J. A. Thas, 'Polar spaces, generalized hexagons and perfect codes', *J. Combin. Theory Ser. A*, 29 (1980) 87–93.

[28] J. A. Thas, 'Ovoids and spreads of finite classical polar spaces', *Geom. Dedicata*, 10 (1981) 135–143.

[29] J. A. Thas, 'Ovoids, spreads and m-systems of finite classical polar spaces', in: *Surveys in combinatorics, 2001 (Sussex)* (Cambridge Univ. Press, Cambridge, 2001), pp. 241–267.

[30] J. A. Thas and S. E. Payne, 'Spreads and ovoids in finite generalized quadrangles', *Geom. Dedicata*, 52 (1994) 227–253.

[31] J. Tits, 'Ovoides et Groupes de Suzuki', *Arch. Math.*, Vol. XIII (1962) 187–198.

[32] H. Van Maldeghem, *Generalized Polygons* (Birkhäuser Verlag, Basel, 1998).

Simeon Ball,
Departament de Matemàtica Applicada IV, Universitat Politècnica de Catalunya, Jordi Girona 1–3, Mòdul C3, 08034 Barcelona, Spain
simeon@mat.upc.es

Patrick Govaerts and Leo Storme,
Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281, S22, 9000 Gent, Belgium
pg@cage.ugent.be
ls@cage.ugent.be