Adv. Geom. **4** (2004), 1–7

Advances in Geometry

On ovoids of O(5, q)

Simeon Ball*

(Communicated by T. Penttila)

Abstract. This article is about ovoids of the generalised quadrangle $\mathrm{O}(5, q)$ and, equivalently, spreads of the generalised quadrangle $\mathrm{Sp}(4, q)$. In a less than conventional way the quadrangles are represented in the field $\mathrm{GF}(q^4)$ which allows some amount of computation to be done. It is shown that an ovoid of $\mathrm{O}(5, q)$ meets an elliptic quadric in 1 modulo p points.

1 Introduction

A *generalised quadrangle* is a polar space of rank 2 and consists of points and lines which have the following properties.

(Q1) Two points lie on at most one line.

(Q2) If L is a line, and p a point not on L, then there is a unique point of L collinear with p.

(Q3) No point is collinear with all others.

The axioms (Q1)–(Q3) are self-dual; the dual of a generalised quadrangle is a generalised quadrangle.

Let $\mathcal{Q}$ be a finite generalised quadrangle. Each line is incident with $1 + s$ points and each point is incident with $1 + t$ lines, for some s and t, and we say $\mathcal{Q}$ is a generalised quadrangle of order (s, t). If $s = t$ then $\mathcal{Q}$ is said to have order s. An *ovoid* of a generalised quadrangle is a set of points $\mathcal{O}$ such that each line contains exactly one point of $\mathcal{O}$. A *spread* of a generalised quadrangle is a set $\mathcal{S}$ of lines such that each point is incident with exactly one line of $\mathcal{S}$. An ovoid $\mathcal{O}$ and a spread $\mathcal{S}$ of $\mathcal{Q}$ satisfy

$$|\mathcal{O}| = |\mathcal{S}| = st + 1.$$

The set of lines dual to the ovoid $\mathcal{O}$ form a spread in the generalised quadrangle dual to $\mathcal{Q}$. The set of points dual to the spread $\mathcal{S}$ forms an ovoid in the generalised quadrangle dual to $\mathcal{Q}$.

*The author is supported by British EPSRC Fellowship No. AF/990-480.

Let $q = p^h$ for some prime p and integer h. Let $\mathrm{Sp}(4,q)$ denote the symplectic generalised quadrangle of order q. The points of $\mathrm{Sp}(4,q)$ are the points of $\mathrm{PG}(3,q)$ and the lines are the totally isotropic lines of a symplectic polarity. Recall that a symplectic polarity is induced by an alternating bilinear form b. An alternating bilinear form on a vector space V satisfies $b(\mathbf{v},\mathbf{v}) = 0$ for all $\mathbf{v}$ in V. This implies

$$b(\mathbf{v},\mathbf{w}) = -b(\mathbf{w},\mathbf{v})$$

for all $\mathbf{v},\mathbf{w}$ in V. (Expand $b(\mathbf{v}+\mathbf{w},\mathbf{v}+\mathbf{w}) = 0$.) Hence if the characteristic is 2 then any alternating form is symmetric.

Let $\mathrm{O}(5,q)$ denote the generalised quadrangle of order q whose points are the points of a non-singular quadric in $\mathrm{PG}(4,q)$ and whose lines are the lines contained in that quadric. The generalised quadrangle $\mathrm{O}(5,q)$ is also denoted $Q(4,q)$ elsewhere.

These notes are concerned with ovoids in $\mathrm{O}(5,q)$. To give the known ovoids explicitly we use the quadratic form $Q(\mathbf{x}) = x_0x_4 + x_1x_3 + x_2^2$ on $V(5,q)$ and note that any ovoid containing $(0,0,0,0,1)$ may be written in the form

$$\mathcal{O}(f) = \{(0,0,0,0,1)\} \cup \{(1,x,y,f(x,y),-y^2 - xf(x,y)) : x,y \in \mathrm{GF}(q)\}.$$

The only known ovoids in $\mathrm{O}(5,q)$ are listed in the following table which comes from [3] where they also calculate the stabilisers. In the table n is a non-square of $\mathrm{GF}(q)$ and α is an automorphism of $\mathrm{GF}(q)$.

name	$f(x,y)$	q	restrictions
elliptic quadrics	$-nx$	all	
Kantor I [2]	$-nx^\alpha$	p^h, $h>1$, p odd	$\alpha^2 = 1$
Kantor II [2]	$''$	$''$	$\alpha^2 \neq 1$
Penttila–Williams [3]	$-x^9 - y^{81}$	3^5	
Ree–Tits slice [2]	$-x^{2\alpha+3} - y^\alpha$	3^{2h+1}, $h>0$	$\alpha = \sqrt{3q}$
Thas–Payne [4]	$-nx - \left(\frac{1}{n}x\right)^{1/9} - y^{1/3}$	3^h, $h>2$	
Tits [5]	$x^{\alpha+1} + y^\alpha$	2^{2h+1}	$\alpha = \sqrt{2q}$

In fact, due to the following lemma, ovoids in $\mathrm{O}(5,q)$ are dual to spreads in $\mathrm{Sp}(4,q)$.

Lemma. $\mathrm{O}(5,q)$ *is the dual of* $\mathrm{Sp}(4,q)$.

Proof. Let $O^+(6,q)$ be the Klein quadric of lines of $\mathrm{PG}(3,q)$. The image of the lines of $\mathrm{Sp}(4,q)$ is the intersection of $O^+(6,q)$ with a hyperplane $\mathrm{PG}(4,q)$, which is $\mathrm{O}(5,q)$. The lines of $\mathrm{Sp}(4,q)$ incident with a given point form a pencil of lines in a plane and therefore their images on $\mathrm{O}(5,q)$ lie on a line. □

This article contains a proof of the following.

Theorem. *An ovoid in* $O(5, q)$ *meets an elliptic quadric in* 1 *modulo* p *points.*

This result was proved for q even in [1] where they prove that an ovoid meets not only an elliptic quadric but also a Tits ovoid in an odd number of points.

2 The geometry PG(3, q) in GF(q^4)

Let $V(4, q)$ be the 4-dimensional vector space over $GF(q)$ (from now on we shall refer to vector space dimension as *rank*), and let $PG(3, q)$ be the 3-dimensional projective space whose k-dimensional subspaces are the subspaces of $V(4, q)$ of rank $k + 1$; for example a point of $PG(3, q)$ is a 0-dimensional subspace which is a subspace of rank 1 in $V(4, q)$. The finite field $GF(q^4)$ can be viewed as a 4-dimensional vector space over $GF(q)$ and we shall begin by examining the link between this field and the geometry $PG(3, q)$.

Given a set of indeterminates $\{X_i \mid i = 0, \ldots, 3\}$ the planes (hyperplanes) of $PG(3, q)$ are given by linear homogeneous equations of the form

$$\sum_{i=0}^{3} c_i X_i = c_0 X_0 + c_1 X_1 + c_2 X_2 + c_3 X_3 = 0, \qquad (*)$$

where (c_0, c_1, c_2, c_3) is a point of $PG(3, q)$. The points of $PG(3, q)$ are subspaces of rank 1 in $V(4, q)$ which in $GF(q^4)$ are given by the sets of zeros of equations of the form

$$X^q = uX$$

where $u^{q^3+q^2+q+1} = 1$. This is a necessary and sufficient condition on u for the polynomial $X^q - uX$ to divide $X^{q^4} - X$ and hence to be a polynomial that splits completely into distinct linear factors over $GF(q^4)$. Hence it makes sense to refer to the points of $PG(3, q)$ as $(q^3 + q^2 + q + 1)$-st roots of unity in $GF(q^4)$.

Let Tr be the trace function from $GF(q^4)$ to $GF(q)$. In $GF(q^4)$ the polynomial

$$\mathrm{Tr}(a^{q^i} X) = a^{q^i} X + a^{q^{i+1}} X^q + a^{q^{i+2}} X^{q^2} + a^{q^{i+3}} X^{q^3}$$

splits completely into distinct linear factors over $GF(q^4)$, has degree q^3 and is linear over $GF(q)$. Hence we choose a to be a fixed primitive element of $GF(q^4)$ and consider the hyperplane (plane) of $PG(3, q)$ (subspace of $V(4, q)$ of rank 3)

$$X_i = 0 \quad \text{as the equation} \quad \mathrm{Tr}(a^{q^i} X) = 0,$$

over $GF(q^4)$, and in general the hyperplane $(*)$ as the equation

$$\mathrm{Tr}\left(\left(\sum_{i=0}^{3} c_i a^{q^i}\right) X\right) = 0.$$

The lines of $\mathrm{PG}(3,q)$ in $\mathrm{GF}(q^4)$ are obtained by looking at the set of zeros of polynomials whose zeros are zeros of two such hyperplane polynomials and we conclude that these have the form

$$L(X) := X^{q^2} + cX^q + eX$$

for some c and e in $\mathrm{GF}(q^4)$. These polynomials must have q^2 distinct zeros in $\mathrm{GF}(q^4)$ and hence divide $X^{q^4} - X$. The polynomial

$$L^{q^2} - c^{q^2}L^q - (e^{q^2} - c^{q^2+q})L \pmod{X^{q^4} - X}$$

has degree q and q^2 zeros and is therefore identically zero. Equating coefficients gives the following necessary and sufficient conditions that

$$c^{q+1} = e^q - e^{q^2+q+1} \quad \text{and} \quad e^{q^3+q^2+q+1} = 1. \tag{$**$}$$

3 The geometry Sp(4, q) in GF(q^4)

Let Γ be an element of $\mathrm{GF}(q^4)$ satisfying $\Gamma^{q^2-1} = -1$. Let b be the alternating bilinear form defined by

$$b(X,Y) := \mathrm{Tr}(\Gamma Y^{q^2}X) = \Gamma Y^{q^2}X + \Gamma^q Y^{q^3}X^q - \Gamma YX^{q^2} - \Gamma^q Y^q X^{q^3}$$

and note that

$$b(X,Y) = -b(Y,X).$$

The map

$$y \to b(X,y) = \mathrm{Tr}(\Gamma y^{q^2}X) = 0$$

maps y to its symplectic hyperplane and defines a symplectic polarity. Let x and y be two orthogonal elements of $\mathrm{GF}(q^4)$, $b(x,y) = 0$, and let $L(X) = X^{q^2} + cX^q + eX$ be the line that joins them. By elimination from the equations $L(x) = 0$ and $L(y) = 0$ we can deduce that

$$(x^qy - y^qx)e = x^{q^2}y^q - y^{q^2}x^q \quad \text{and} \quad (x^qy - y^qx)c = -(x^{q^2}y - y^{q^2}x)$$

and

$$(\Gamma c + \Gamma^q ec^q)(x^qy - y^qx) = b(x,y) = 0.$$

The totally isotropic lines of the polarity defined by $b(X,Y)$ have $-\gamma c = ec^q$ where $\gamma = \Gamma^{1-q}$, as well as the restrictions $(**)$. In the case when $c = 0$ there are $q^2 + 1$ lines where each line is given by the set of zeros of an equation of the form

$$X^{q^2} + eX = 0$$

where $e^{q^2+1} = 1$. In the case c is non-zero let $d = c^{-1}$ and we find that $e = -\gamma d^{q-1}$ and

$$\gamma d^{q^3+q} - \gamma^{-1} d^{q^2+1} + 1 = 0. \qquad (\dagger)$$

For each d satisfying this equation there is a totally isotropic line which is given by the set of zeros of an equation of the form

$$dX^{q^2} + X^q - \gamma d^q X = 0.$$

The points of $Sp(4, q)$ are the points of $PG(3, q)$ and for this reason we take as before the points to be the $(q^3 + q^2 + q + 1)$-st roots of unity (alternatively the non-zero $(q - 1)$-st powers) in $GF(q^4)$. Therefore we replace the indeterminate X by U where $U = X^{q-1}$. It now follows that the lines of $Sp(4, q)$ are given by the zeros (all $(q^3 + q^2 + q + 1)$-st roots of unity) of equations

$$U^{q+1} + e = 0,$$

for each e satisfying $e^{q^2+1} = 1$ and

$$dU^{q+1} + U - \gamma d^q = 0 \qquad (\dagger\dagger)$$

for each d satisfying $(\dagger)$.

Remark. The geometry $PG(1, q^2)$ has as points the subspaces of rank 1 in $V(2, q^2)$. In $GF(q^4)$ they are the given by sets of zeros of equations of the form

$$X^{q^2} + eX = 0$$

where $e^{q^2+1} = 1$. Hence the lines defined by the sets of zeros of equations of the form $U^{q+1} + e = 0$ are skew and together they form a Desarguesian spread $\mathscr{R}$ of $Sp(4, q)$. A Desarguesian spread is equivalent to a regular spread. The set of points in the generalised quadrangle $O(5, q)$ dual to a regular spread of $Sp(4, q)$ is an elliptic quadric. Hence we need to prove that a spread of $Sp(4, q)$ meets the spread $\mathscr{R}$ in 1 modulo p lines.

Remark. The equations $(**)$ and $-\gamma c = ec^q$ imply that

$$c^2 = \gamma^{-1} e^{q+1} (e^{q^2+1} - 1).$$

When q is even we can take square roots and parameterize the lines using $(q^3 + q^2 + q + 1)$-st roots of unity. Moreover when q is even we can assume that $\gamma = 1$ since the

alternating form is also symmetric. Thus we have that the totally isotropic lines of $\mathrm{Sp}(4,q)$ are given by the zeros of equations of the form

$$U^{q+1} + (e^{(q^2+q+2)/2} + e^{(q+1)/2})U + e = 0$$

and one can check that if the point x lies on the line parameterized by e then e lies on the line parameterized by x^{2q}. Hence we see that $\mathrm{Sp}(4,q)$ is self-dual when q is even, a fact first noted in [5].

4 An ovoid of O(5, q) meets an elliptic quadric in 1 modulo p points

Recall that $q = p^h$ for some prime p and integer h. In this section we prove that a spread of $\mathrm{Sp}(4,q)$ has 1 modulo p lines in common with the regular spread $\mathscr{R}$. This regular spread is entirely arbitrary.

Proof of the theorem. Let $\mathscr{S}$ be a spread of $\mathrm{Sp}(4,q)$ and let the sets $\mathscr{D}$ and $\mathscr{E}$ be such that for $d \in \mathscr{D}$ the line

$$dU^{q+1} + U - \gamma d^q = 0$$

is in $\mathscr{S}$ and for $e \in \mathscr{E}$ the line

$$U^{q+1} + e = 0$$

is in $\mathscr{S}$. Clearly

$$|\mathscr{D}| + |\mathscr{E}| = q^2 + 1.$$

The aim will be to show that $|\mathscr{D}| = 0$ modulo p and then the result will follow.

The bilinear form $b(X, Y)$ can be rewritten for the points of $\mathrm{PG}(3,q)$ by replacing X^{q-1} by U and Y^{q-1} by V. Hence for a fixed point u in $\mathrm{PG}(3,q)$ the zeros of the polynomial

$$(u, V) := \gamma u^{q+1} - \gamma V^{q+1} + u^{q^2+q+1}V - uV^{q^2+q+1}$$

are the points that are orthogonal to u, i.e. lie on the symplectic hyperplane through u. Let v be the point of $\mathrm{Sp}(4,q)$ (i.e. $\mathrm{PG}(3,q)$) that is the intersection of the line of $\mathrm{Sp}(4,q)$ of the form

$$dV^{q+1} + V - \gamma d^q = 0$$

with the plane $(u, V) = 0$, assuming that the line is not contained in the plane. We can calculate directly or check by substitution that

$$v^q = -u(du^{q+1} + u - \gamma d^q)^{q-1}.$$

Similarly if v is the point of intersection of the line of $\mathrm{Sp}(4,q)$ of the form

$$V^{q+1}+e=0$$

with the plane $(u,V)=0$ then

$$v^q=\gamma^{-1}ue(u^{q+1}+e)^{q-1}.$$

The coefficient of V^{q^2+q} in (u,V) is minus the sum of all the points in the plane $(u,V)=0$ and is zero. Likewise the sum of all the points on any line is minus the coefficient of V^q in the equation of this line which is also zero. Hence the sum of all points lying in an affine plane is also zero. Thus the sum of all the points of intersection of the spread $\mathscr{S}$ with the plane $(u,V)=0$ is zero and we have

$$0=\sum v=\sum v^q=-\sum_{d\in\mathscr{D}}u(du^{q+1}+u-\gamma d^q)^{q-1}+\sum_{e\in\mathscr{E}}\gamma^{-1}ue(u^{q+1}+e)^{q-1}.$$

Note that of course one of the lines of the spread contains the point u and the term in the sum corresponding to this line will be zero. The polynomial

$$\sum_{d\in\mathscr{D}}U(dU^{q+1}+U-\gamma d^q)^{q-1}-\sum_{e\in\mathscr{E}}\gamma^{-1}Ue(U^{q+1}+e)^{q-1}$$

is zero for all points of $\mathrm{PG}(3,q)$ and since it's degree is only q^2 it is identically zero. However the coefficient of U^q is $|\mathscr{D}|$ and hence $|\mathscr{D}|=0$ modulo p. □

References

[1] B. Bagchi, N. S. Narasimha Sastry, Even order inversive planes, generalized quadrangles and codes. *Geom. Dedicata* **22** (1987), 137–147. MR 88b:51006 Zbl 0609.51011

[2] W. M. Kantor, Ovoids and translation planes. *Canad. J. Math.* **34** (1982), 1195–1207. MR 84b:51019 Zbl 0467.51004

[3] T. Penttila, B. Williams, Ovoids of parabolic spaces. *Geom. Dedicata* **82** (2000), 1–19. MR 2001i:51005

[4] J. A. Thas, S. E. Payne, Spreads and ovoids in finite generalized quadrangles. *Geom. Dedicata* **52** (1994), 227–253. MR 95m:51005 Zbl 0804.51007

[5] J. Tits, Ovoïdes et groupes de Suzuki. *Arch. Math.* **13** (1962), 187–198. MR 25 #3990 Zbl 0109.39402

Received 13 April, 2001; revised 2 October, 2002

S. Ball, School of Mathematical Sciences, Queen Mary and Westfield College, University of London, Mile End Road, London E1 4NS, United Kingdom
Email: s.ball@qmul.ac.uk