The known maximal partial ovoids of size q^2-1 of $\mathrm{Q}(4,q)$

Kris Coolsaet, Jan De Beule*, and Alessandro Siciliano

Abstract

We present a description of maximal partial ovoids of size q^2-1 of the parabolic quadric $\mathrm{Q}(4,q)$ as sharply transitive subsets of $\mathrm{SL}(2,q)$ and show their connection with spread sets. This representation leads to an elegant explicit description of all known examples. We also give an alternative representation of these examples which is related to root systems.

Keywords: maximal partial ovoid, generalized quadrangle, parabolic quadric, special linear group, $\mathrm{SL}(2,q)$, transitive subset, spread set

1 Introduction

A (finite) *generalized quadrangle* (GQ) is an incidence structure $\mathcal{S}=(\mathcal{P},\mathcal{B},\mathrm{I})$ in which $\mathcal{P}$ and $\mathcal{B}$ are disjoint non-empty sets of objects called points and lines (respectively), and for which $\mathrm{I}\subseteq(\mathcal{P}\times\mathcal{B})\cup(\mathcal{B}\times\mathcal{P})$ is a symmetric point-line incidence relation satisfying the following axioms:

(i) each point is incident with $1+t$ lines ($t\geqslant 1$) and two distinct points are incident with at most one line;

(ii) each line is incident with $1+s$ points ($s\geqslant 1$) and two distinct lines are incident with at most one point;

(iii) if x is a point and L is a line not incident with x, then there is a unique pair $(y,M)\in\mathcal{P}\times\mathcal{B}$ for which $x\ \mathrm{I}\ M\ \mathrm{I}\ y\ \mathrm{I}\ L$.

*The author is a postdoctoral research fellow of the Research Foundation Flanders – Belgium (FWO).

The integers s and t are the parameters of the GQ and $\mathcal{S}$ is said to have order (s,t). If $s=t$, then $\mathcal{S}$ is said to have order s. If $\mathcal{S}$ has order (s,t), then $|\mathcal{P}|=(s+1)(st+1)$ and $|\mathcal{B}|=(t+1)(st+1)$ (see e.g. [11]).

If we interchange the roles of points and lines in a GQ we obtain a new GQ $(\mathcal{B},\mathcal{P},\mathrm{I})$ which is called the *dual* of the original.

An *ovoid* of a GQ $\mathcal{S}$ is a set $\mathcal{O}$ of points of $\mathcal{S}$ such that every line is incident with exactly one point of the ovoid. An ovoid of a GQ of order (s,t) has necessarily size $1+st$. A *partial ovoid* of a GQ is a set $\mathcal{K}$ of points such that every line contains *at most* one point of $\mathcal{K}$. The difference $\rho=st+1-|\mathcal{K}|$ between the size of an ovoid and the size of a particular partial ovoid $\mathcal{K}$, is called the *deficiency* of $\mathcal{K}$. (Hence $\rho=0$ if and only if $\mathcal{K}$ is an ovoid.)

A partial ovoid $\mathcal{K}$ is called *maximal* if and only if $\mathcal{K}\cup\{p\}$ is not a partial ovoid for any point $p\in\mathcal{P}\setminus\mathcal{K}$, in other words, if $\mathcal{K}$ cannot be extended to a larger partial ovoid.

It is a natural question to study *extendability* of partial ovoids, i.e., for what values of ρ can a partial ovoid of deficiency ρ be guaranteed to extend to a full ovoid? The following theorem is a typical result in this context.

Theorem 1 ([11, 2.7.1]) *Let $\mathcal{S}=(\mathcal{P},\mathcal{B},\mathrm{I})$ be a GQ of order (s,t). Any partial ovoid of size $st-\rho$, $0\le\rho<\frac{t}{s}$ is contained in a uniquely defined ovoid of $\mathcal{S}$.*

Remark that if no ovoids of a particular GQ exist, then Theorem 1 implies an upper bound on the size of partial ovoids. The following theorem deals with the limit situation, and will be of use in Section 2.

Theorem 2 ([11, 2.7.2]) *Let $\mathcal{S}=(\mathcal{P},\mathcal{B},\mathrm{I})$ be a GQ of order (s,t). Let $\mathcal{K}$ be a maximal partial ovoid of size $st-t/s$ of $\mathcal{S}$. Let $\mathcal{B}'$ be the set of lines incident with no point of $\mathcal{K}$, and let $\mathcal{P}'$ be the set of points on at least one line of $\mathcal{B}'$ and let I' be the restriction of I to points of $\mathcal{P}'$ and lines of $\mathcal{B}'$. Then $\mathcal{S}'=(\mathcal{P}',\mathcal{B}',\mathrm{I}')$ is a subquadrangle of order $(s,t/s)$.*

Consider the parabolic quadric $\mathrm{Q}(4,q)$ in the 4-dimensional projective space $\mathrm{PG}(4,q)$. This quadric consists of points of $\mathrm{PG}(4,q)$ that are singular with respect to a non-degenerate quadratic form on $\mathrm{PG}(4,q)$, which is, up to a coordinate transformation, unique.

The points and totally isotropic lines of $\mathrm{Q}(4,q)$ constitute an example of a generalized quadrangle of order q. Any elliptic quadric contained in $\mathrm{Q}(4,q)$, obtained from a hyperplane section, is an example of an ovoid of $\mathrm{Q}(4,q)$. These are the only ovoids when q is a prime, [2]. When $q=p^h$, $h>1$, other examples are known, see e.g. [7] for a list of references.

Applying Theorem 1 to the GQ $\mathrm{Q}(4,q)$ implies that a partial ovoid of size q^2 cannot be maximal. In this paper we shall be concerned with the next case, that of maximal partial ovoids of size q^2-1. It is shown in [6] that maximal partial ovoids of $\mathrm{Q}(4,q)$ of size q^2-1 do not exist when q is odd and not prime. When q is odd and prime, examples of maximal partial ovoids of this size are known for $q=3,5,7$ and 11, but none for $q>11$, [12]. In this paper we will give detailed descriptions of exactly these examples. It was also shown in [9] that $q=3,5,7$ and 11 are the only values permitted under the additional assumption that $(q^2-1)^2$ divides the automorphism group of the maximal partial ovoid.

For the sake of completeness, we mention that for q even and $q>2$, maximal partial ovoids of size q^2-1 are excluded, and more is known, by the following theorem.

Theorem 3 ([4, Corollary 1]) *Let $\mathcal{K}$ be a maximal partial ovoid of $\mathrm{Q}(4,q)$, q even. Then $|\mathcal{K}| \leq q^2-q+1$.*

For the case $q=2$ it is easily seen that here exist maximal partial ovoids of size $q^2-1=3$, see e.g. [14].

In Section 2 we shall restrict ourselves to q odd, and show that maximal partial ovoids of size q^2-1 can be represented as sharply transitive subsets of the special linear group $\mathrm{SL}(2,q)$ and show how this representation naturally leads to a uniform description of the known examples (cf. Theorem 5). In Section 3 we illustrate the connection between these partial ovoids and spread sets, and hence with partial spreads of the symplectic geometry $\mathrm{W}(3,q)$. Finally, in Section 4 we present another (and quite different) way to construct the known examples, in terms of root systems.

2 The geometry of Q(4,q) and SL(2,q)

From now on we shall assume that q is odd.

If a maximal partial ovoid $\mathcal{O}$ of $\mathrm{Q}(4,q)$ has size q^2-1, it follows from Theorem 2 that the lines of $\mathrm{Q}(4,q)$ not meeting $\mathcal{O}$ constitute a subGQ of order $(q,1)$, which is necessarily a hyperbolic quadric $\mathrm{Q}^+(3,q)$ contained in the intersection of a hyperplane π_∞ and $\mathrm{Q}(4,q)$.

It is therefore natural to consider the geometry $\mathrm{Q}^*(4,q)$ that consists of the points of $\mathrm{Q}(4,q)$ that do not belong to π_∞ (the 'affine points') together with the lines of $\mathrm{Q}(4,q)$ that do not lie entirely inside π_∞ and therefore intersect π_∞ in exactly one point (the 'affine lines'). There are $q(q^2-1)$ affine points and $(q+1)(q^2-1)$ affine lines. Each affine line contains q affine points and each affine point lies on $q+1$ affine lines.

A maximal partial ovoid $\mathcal{O}$ of $\mathrm{Q}(4,q)$ of size q^2-1 is then precisely a set of affine points such that each affine line contains exactly one point of $\mathcal{O}$. Such a set may as well be dubbed an 'affine ovoid'.

Without loss of generality we may choose the equation of $\mathrm{Q}(4,q)$ to be $X_0^2 = X_1X_4 - X_2X_3$ and the equation of π_∞ to be $X_0 = 0$. With this notation, the affine points can all be given normalized coordinates with $X_0 = 1$, and hence are in one–one correspondence with the quadruples (X_1, X_2, X_3, X_4) such that $X_1X_4 - X_2X_3 = 1$. In other words, the points of $\mathrm{Q}^*(4,q)$ are in one–one correspondence with the 2×2 matrices of determinant one, i.e., with the elements of $\mathrm{SL}(2,q)$. It is this correspondence and the group structure of $\mathrm{SL}(2,q)$ which can be exploited to better understand the 'affine ovoids'.

We are certainly not the first to identify the points of $\mathrm{Q}^*(4,q)$ with group elements of $\mathrm{SL}(2,q)$. Indeed, this representation is related to the much more general interpretation of so-called span-symmetric GQs as group coset geometries [11, Theorem 10.7.8]. Fortunately, for the particular case of $\mathrm{Q}^*(4,q)$ we can derive the necessary properties in a much simpler setting.

The following lemma shows that there is a wide variety of ways to express collinearity in $\mathrm{Q}^*(4,q)$. We write I for the 2×2 identity matrix.

Lemma 4 *Let $q = p^h$, p prime, p odd. Let $X, Y \in \mathrm{SL}(2,q)$ such that $X \neq Y$. Then the following are equivalent*

(i) *X and Y are collinear in $\mathrm{Q}^*(4,q)$,*
(ii) *$(1-k)X + kY \in \mathrm{SL}(2,q)$ for all $k \in \mathrm{GF}(q)$,*
(iii) *$(1-k)X + kY \in \mathrm{SL}(2,q)$ for at least one $k \in \mathrm{GF}(q) - \{0,1\}$,*
(iv) *$Y - X$ is singular, i.e., $\det(Y-X) = 0$,*
(v) *$\mathrm{Tr}\, XY^{-1} = \mathrm{Tr}\, Y^{-1}X = 2$,*
(vi) *$\mathrm{Tr}\, YX^{-1} = \mathrm{Tr}\, X^{-1}Y = 2$,*
(vii) *XY^{-1} (and hence YX^{-1}) has multiplicative order p,*
(viii) *$Y^{-1}X$ (and hence $X^{-1}Y$) has multiplicative order p.*

Proof. Write $X = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$. Because $\det X = 1$, the inverse X^{-1} of X is the same as the adjoint $X^\#$, hence $X^{-1} = X^\# = \begin{pmatrix} X_4 & -X_2 \\ -X_3 & X_1 \end{pmatrix}$.

Note that the adjoint operator is linear on 2×2 matrices. Also the trace of the adjoint of a matrix is the same as the trace of the original. As a consequence $\mathrm{Tr}\, M = \mathrm{Tr}\, M^{-1}$ for all $M \in \mathrm{SL}(2,q)$, and in particular $\mathrm{Tr}\, XY^{-1} = \mathrm{Tr}\, YX^{-1}$ and this again is equal to $\mathrm{Tr}\, Y^{-1}X = \mathrm{Tr}\, X^{-1}Y$.

Consider $Z = (1-k)X + kY$ for some $k \in \mathrm{GF}(q)$. We have $Z^\# =$

$(1-k)X^{\#} + kY^{\#} = (1-k)X^{-1} + kY^{-1}$ and therefore

$$\begin{aligned}(\det Z)I = ZZ^{\#} &= [(1-k)X + kY][(1-k)X^{-1} + kY^{-1}] \\ &= (1-k)^2 I + k(1-k)XY^{-1} + k(1-k)YX^{-1} + k^2 I \\ &= (1-2k+2k^2)I + k(1-k)(XY^{-1} + YX^{-1}).\end{aligned}$$

Taking the trace of both sides of this equation and dividing by 2, yields $\det Z = 1 - 2k + 2k^2 + k(1-k)\mathrm{Tr}\, XY^{-1}$. Hence $\det Z = 1$ if and only if $k(1-k)(\mathrm{Tr}\, XY^{-1} - 2) = 0$.

The matrix $Y - X$ is singular if and only if $YX^{-1} - 1$ is singular. Write $U = YX^{-1}$, $t = \mathrm{Tr}\, U$. Note that $\det U = 1$. U satisfies its own characteristic equation, and therefore $U^2 - tU + 1 = 0$. If $t = 2$, this means $(U-1)^2 = 0$ and hence $U - 1$ is singular. Conversely, $U - 1$ is singular if and only if 1 is an eigenvalue of U. Because $\det U = 1$, this means that also the other eigenvalue of U is 1 and hence $\mathrm{Tr}\, U$ equals the sum of the eigenvalues, which is 2.

Finally, for any $M \in \mathrm{SL}(2,q)$ we have $(M-I)^p = M^p - I$. Hence, if $M^p = I$, then the minimal polynomial of M must divide $(x-1)^p$ and be either $x - 1$, in which case $M = I$, or $(x-1)^2 = x^2 - 2x + 1$, and then $\mathrm{Tr}\, M = 2$. Conversely, if $\mathrm{Tr}\, M = 2$, then $(M-I)^2 = 0$ and hence also $(M-I)^p = 0$. □

The interpretation of the combinatorial problem of partial ovoids as subsets of group elements immediately provides us with natural examples of affine ovoids in the following theorem.

Theorem 5 *Let G denote a subgroup of $\mathrm{SL}(2,q)$ of order $q^2 - 1$. Then G is an affine ovoid of $\mathrm{Q}^*(4,q)$.*

Proof. Let $X, Y \in G$, $X \neq Y$. Because p does not divide the order of G, no element of G can have order p. In particular XY^{-1} cannot have order p and therefore by Lemma 4 X and Y cannot be collinear. □

The subgroup structure of $\mathrm{SL}(2,q)$ is well known [13, Chapter 3,§6]. When q is odd, $\mathrm{SL}(2,q)$ contains a subgroup of order $q^2 - 1$ if and only if q=3, 5, 7 or 11, as listed in the following table

Group	Subgroup
SL(2,3)	Q_8
SL(2,5)	$\mathrm{SL}(2,3) = 2 \cdot A_4$
SL(2,7)	$\mathrm{GL}(2,3) = 2 \cdot S_4$
SL(2,11)	SL(2,5)

As mentioned before, these are the only known examples of affine ovoids to date (up to equivalence, cf. below).

We conjecture that also the converse of Theorem 5 is true — that every affine ovoid must be (equivalent to) a subgroup of $\mathrm{SL}(2,q)$, and hence that all affine ovoids are already known.

Two subsets of $\mathrm{Q}(4,q)$ are called equivalent if there exists an automorphism of the generalized quadrangle $\mathrm{Q}(4,q)$ that maps the one set to the other. The following lemma describes some of these automorphisms that also leave the hyperplane π_∞ invariant.

Lemma 6 *Consider $M, N \in \mathrm{GL}(2,q)$ such that $\det M = \det N$. Let σ be a field automorphism of $\mathrm{GF}(q)$. Then the following maps are automorphisms of the geometry $\mathrm{Q}^*(4,q)$.*

$$X \mapsto MX^\sigma N^{-1}, \quad X \mapsto M(X^{-1})^\sigma N^{-1} \tag{1}$$

Proof. For each of the maps in (1) the image of a matrix X of determinant 1 again has determinant 1. Each map therefore preserves the point set of $Q^*(4,q)$. Also, $\mathrm{Tr}\, XY^{-1}$ is mapped to either $(\mathrm{Tr}\, XY^{-1})^\sigma$ or $(\mathrm{Tr}\, YX^{-1})^\sigma$, and hence by Lemma 4 (*v–vi*), collinearity is preserved. □

In particular, multiplication on the left or right by a fixed element of $\mathrm{SL}(2,q)$ is an automorphism of the geometry. And hence, from Theorem 5 it follows that not only every subgroup G of the appropriate size, but also every coset of that group, is an affine ovoid of $\mathrm{Q}^*(4,q)$, be it equivalent to G.

If we are only interested in point subsets $\mathcal{O}$ up to equivalence, then it follows from Lemma 6 that we may as well assume that $I \in \mathcal{O}$. Moreover, if $X \in \mathcal{O} \setminus \{I, -I\}$ has $\mathrm{Tr}\, X = t$, then we may always find an automorphism of type (1) with $M = N$ that leaves I invariant, and maps X to a chosen matrix of trace t (and determinant 1) different from $\pm I$.

This technique can be used to describe the (affine) lines in an elegant way.

Lemma 7 *The lines of $\mathrm{Q}^*(4,q)$ are precisely the cosets of the Sylow p-subgroups of $\mathrm{SL}(2,q)$.*

Proof. By the above, it is sufficient to prove that a line that contains I is a Sylow p-subgroup of $\mathrm{SL}(2,q)$. Moreover, without loss of generality we may assume that the line contains the matrix $M(1) \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. It follows that the points of the line are of the form $M(k) \stackrel{\text{def}}{=} (1-k)I + kM(1)$ with

$k \in \mathrm{GF}(q)$. We have $M(k) = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ and the set $\{M(k)|k \in \mathrm{GF}(q)\}$ is a Sylow p-subgroup of $\mathrm{SL}(2,q)$, isomorphic to the additive group of the field $\mathrm{GF}(q)$. □

The next result shows that affine ovoids are connected to so-called transitive subsets of $\mathrm{SL}(2,q)$. A subset S of $\mathrm{SL}(2,q)$ is called *transitive* if and only if for any two non-zero vectors $u, v \in \mathrm{GF}(q)^2$ there exist an element $X \in S$ such that $uX = v$. S is *sharply transitive* if and only if the element X is always unique.

Theorem 8 *Let q be odd. Let $\mathcal{O} \subseteq \mathrm{SL}(2,q)$. Then $\mathcal{O}$ is an affine ovoid of $\mathrm{Q}^*(4,q)$ if and only if $\mathcal{O}$ is a sharply transitive subset of $\mathrm{SL}(2,q)$.*

Proof. Let $\mathcal{O}$ be sharply transitive and take $X, Y \in \mathcal{O}$, $X \neq Y$. Then, for any $u \in \mathrm{GF}(q)^2$, uX and uY must differ, and hence $u(X-Y) \neq 0$, for all $u \neq (0,0)$. It follows that $X - Y$ is non-singular, and hence X, Y are never collinear, by Lemma 4, making $\mathcal{O}$ an affine ovoid.

Conversely, let $\mathcal{O}$ be an affine ovoid. For every $X, Y \in \mathcal{O}$, $X - Y$ is non-singular, and hence the set $V = \{uX|X \in \mathcal{O}\}$ has size $|\mathcal{O}|$. Because $|\mathcal{O}| \geq q^2 - 1$ the set V must contain every non-zero vector of $\mathrm{GF}(q)^2$. Therefore $\mathcal{O}$ is transitive, and because $|\mathcal{O}|$ is exactly $q^2 - 1$, it is even sharply transitive. □

For $t \in \mathrm{GF}(q)$ we define the *discriminant* $\delta(t)$, as follows:

$$\delta(t) = \begin{cases} -1, & \text{when } t^2 - 4 \text{ is not a square in } \mathrm{GF}(q), \\ 0, & \text{when } t^2 - 4 = 0, \\ 1, & \text{when } t^2 - 4 \text{ is a non-zero square in } \mathrm{GF}(q). \end{cases}$$

The quadratic equation $\lambda^2 - t\lambda + 1 = 0$ has exactly $1 + \delta(t)$ solutions for $\lambda \in \mathrm{GF}(q)$. (This is the characteristic equation of a matrix $X \in \mathrm{SL}(2,q)$ with $\mathrm{Tr}\, X = t$.)

Proposition 9 *Let $t \in \mathrm{GF}(q)$. Let S_t denote the set of all elements X of $\mathrm{SL}(2,q)$ such that $\mathrm{Tr}\, X = t$. Then $S_t = H_t \setminus \pi_\infty$ where H_t is a hyperplane section of $\mathrm{Q}(4,q)$ whose type depends on $\delta(t)$ as follows:*

(i) *If $\delta(t) = -1$, then H_t is an elliptic quadric of type $Q^-(3,q)$.*
(ii) *If $\delta(t) = 1$, then H_t is a hyperbolic quadric of type $Q^+(3,q)$.*
(iii) *If $\delta(t) = 0$, then H_t is a quadratic cone.*

In all cases $|S_t| = q(q + \delta(t))$.

Proof. Let $X = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$ as before. The condition $\mathrm{Tr}\, X = t$ translates to $X_1 + X_4 = t$, or in projective coordinates, $X_1 + X_4 = tX_0$ which is the equation of a hyperplane H_t of $\mathrm{PG}(4, q)$. Such a hyperplane intersects $\mathrm{Q}(4, q)$ in either a cone, an elliptic or a hyperbolic quadric. It remains to determine which values of t lead to which type of intersection.

Combining the equation of H_t with the equation of $\mathrm{Q}(4, q)$ yields

$$X_1(tX_0 - X_1) - X_2X_3 - X_0^2 = 0.$$

The corresponding quadratic form has the following associated determinant :

$$\begin{vmatrix} -1 & t/2 & 0 & 0 \\ t/2 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1/2 \\ 0 & 0 & -1/2 & 0 \end{vmatrix} = (1 - t^2/4)(1/4) = \frac{1}{16}\delta(t).$$

The type of the hyperplane section is determined by whether this determinant is a square, a non-square or zero, yielding the classification in the statement of this theorem.

It remains to determine the value of $|S_t|$. Note that the size of the hyperplane section is equal to q^2+1, q^2+q+1 or $(q+1)^2$ depending on the type of the hyperplane section, i.e., equal to $q^2+q+1+\delta(t)q$. From this size we need to subtract the size of the intersection $S_t \cap \pi_\infty$. This intersection consists of the points satisfying $X_0 = 0$ and $-X_1^2 - X_2X_3 = 0$, i.e., a non-degenerate conic. A conic has $q+1$ points, and therefore $|S_t| = q^2+q+1+\delta(t)q-(q+1) = q(q + \delta(t))$. □

Lemma 10 *Let $\mathcal{O}$ denote an affine ovoid of $\mathcal{Q}^*(4, q)$. Then*

(i) *$\mathcal{O}$ either contains I or else exactly $q + 1$ elements of trace 2 different from I,*

(ii) *$\mathcal{O}$ either contains $-I$ or else exactly $q+1$ elements of trace -2 different from $-I$,*

(iii) *$\mathcal{O}$ contains exactly $q+1$ points of trace t, for every t such that $\delta(t) > 0$.*

Every point of $\mathcal{Q}^*(4, q)$ outside $\mathcal{O}$ is collinear with exactly $q + 1$ points of $\mathcal{O}$.

Proof. By Proposition 9 (iii), the points of trace 2 consist of $q + 1$ (affine) lines through the common point I. Because $\mathcal{O}$ is an affine ovoid, each of these lines must contain exactly one point of $\mathcal{O}$. Either this is the point common to all these lines, i.e., I, or else a different point for each line. This proves the first part of this lemma. The second part is proved in the same way, by considering the points of trace -2 instead of 2.

Now, let t be such that $\delta(t) > 0$. By Proposition 9 (i) H_t is a hyperboloid and its point can therefore be partitioned into $q+1$ lines (in two different ways). Each of these lines must contain exactly one point of $\mathcal{O}$.

Finally, consider a point outside $\mathcal{O}$. Without loss of generality we may assume this point to be I. The first part of this lemma then proves that this point is collinear to exactly $q+1$ points of $\mathcal{O}$. □

Lemma 11 *Let $A, B \in \mathrm{SL}(2,q)$ such that $A \neq B$. Then A and B are collinear to the same points of π_∞ if and only if $A = -B$.*

Proof. Let $A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$, $B = \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix}$. The points $(X_0, X_1, \ldots, X_4)$ of π_∞ that are collinear to A (resp. B) are the points of the 3-dimensional subspace of π_∞ with equation $X_0 = 0$ and $A_2X_1 + A_1X_2 - A_4X_3 - A_3X_4 = 0$ (resp. $B_2X_1 + B_1X_2 - B_4X_3 - B_3X_4 = 0$). These two 3-spaces are the same if and only if the corresponding quadruples $(A_2, A_1, -A_4, -A_3)$ and $(B_2, B_1, -B_4, -B_3)$ are equal up to a multiplicative factor. In other words, if the matrices A and B are equal up to a multiplicative factor. From $\det A = \det B = 1$ it follows that this factor can only be 1 or -1. □

Pairs of points $A, -A$ that satisfy the conditions of Lemma 11, shall be called *antipodal*. Note that antipodality is preserved by the automorphisms of Lemma 6.

Theorem 12 *If the affine ovoid $\mathcal{O}$ is a subgroup of $\mathrm{SL}(2,q)$ then it is the disjoint union of $\frac{1}{2}(q^2-1)$ antipodal pairs.*

Proof. Assume the contrary, and let $A \in \mathcal{O}$ such that $-A \notin \mathcal{O}$. Without loss of generality we may set $A = I$. By Lemma 10 (ii) $\mathcal{O}$ must contain at least one element X with $\mathrm{Tr}\, X = -2$ but $X \neq -I$. Such X must satisfy its characteristic equation $X^2 + 2X + 1 = 0$. Hence $(X+1)^2 = 0$ and then $X^p + 1 = 0$ (see the proof of Lemma 4). It follows that X has order $2p$, and hence that $2p$ must divide the order $q^2 - 1$ of the group $\mathcal{O}$. This is a contradiction. □

(In [9] this theorem was proved for the special case $q = 5$.)

3 Spreads of W(3,q) and spread sets

In this section we shall describe an interesting correspondence between the points of $\mathrm{Q}^*(4,q)$ and certain lines of the 3-dimensional projective space $\mathrm{PG}(3,q)$.

A *spread* $\mathcal{S}$ of $\mathrm{PG}(3,q)$ is a set of lines which partition the point set of $\mathrm{PG}(3,q)$. A spread necessarily contains q^2+1 lines. A *partial spread* of $\mathrm{PG}(3,q)$ is a set of mutually non-intersecting lines. It follows that a partial spread is a spread if and only if it has size q^2+1. A partial spread is *maximal* if it cannot be extended to a larger partial spread.

Every partial spread that is sufficiently large can always be made into a full spread by adding appropriate lines, as stated in the following theorem.

Theorem 13 ([5]) *Let $\mathcal{S}$ be a partial spread of $\mathrm{PG}(3,q)$ of size $q^2+1-\delta$. If $\delta \leq \epsilon$, such that $q+\epsilon$ is smaller than the smallest non-trivial blocking set of $\mathrm{PG}(2,q)$, then $\mathcal{S}$ is extendable to a spread.*

(A lower bound for ϵ is $\sqrt{q}$, and this lower bound is sharp when q is a square.)

One way to construct spreads is by means of so-called spread sets (see [8] for more information). A *spread set* is a collection $\mathcal{C}$ of 2×2-matrices over $\mathrm{GF}(q)$ which satisfies the following three conditions:

(i) $|\mathcal{C}| = q^2$;
(ii) $\mathcal{C}$ contains the zero matrix and the identity matrix;
(iii) If $X, Y \in \mathcal{C}$, $X \neq Y$, then $\det(X-Y) \neq 0$.

Let $X = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$ denote a general 2×2 matrix (not necessarily of determinant 1) and define $L(X)$ to be the line of $\mathrm{PG}(3,q)$ that connects the points with coordinates $(1,0,X_1,X_2)$ and $(0,1,X_3,X_4)$. Recall that the line L through the points (x_1,x_2,x_3,x_4) and (y_1,y_2,y_3,y_4) can also be represented by its *Plücker coordinates* $p(L) = (p_{01},p_{02},p_{03},p_{23},p_{31},p_{12})$, satisfying $p_{01}p_{23}+p_{02}p_{31}+p_{03}p_{12}=0$, where $p_{ij} \stackrel{\text{def}}{=} \begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix}$. The Plücker coordinates of $L(X)$ are easily computed to be

$$p(L(X)) = (1, X_3, X_4, \det X, -X_1, X_2). \tag{2}$$

It is not so difficult to prove that the lines $L(X)$ and $L(Y)$ have a non-empty intersection if and only if $\det(X-Y)=0$. Hence, if $\mathcal{C}$ is a spread set, then the set of lines $L(\mathcal{C}) \stackrel{\text{def}}{=} \{L(X) \mid X \in \mathcal{C}\}$ is a partial spread of $\mathrm{PG}(3,q)$ of size q^2.

Theorem 13 guarantees that we can find one more line L' such that $L(\mathcal{C}) \cup \{L'\}$ is a full spread of $\mathrm{PG}(3,q)$, and indeed, in this case it is easily verified that the line connecting the points with coordinates $(0,0,1,0)$ and $(0,0,0,1)$ satisfies this role. In fact, every spread of $\mathrm{PG}(3,q)$ is equivalent to a spread which is obtained from a spread set in this way.

Now, affine ovoids of $\mathrm{SL}(2,q)$ yield a natural way to construct spread sets. Indeed, it follows immediately from Lemma 4 that extending an affine

ovoid $\mathcal{O}$ with the zero matrix yields a spread set $\mathcal{C} \stackrel{\text{def}}{=} \mathcal{O} \cup \{0\}$. The fact that every $X \in \mathcal{O}$ has $\det X = 1$ makes this spread set (and the associated spread) rather special. Indeed, by (2), every line of the partial spread $L(\mathcal{O})$ (i.e., every line of the full spread, except two) satisfies the identity $p_{01} = p_{23}$. In other words, every such line is an isotropic line for the symplectic form

$$\begin{vmatrix} x_0 & x_1 \\ y_0 & y_1 \end{vmatrix} - \begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix}. \tag{3}$$

If we denote by $\mathrm{W}(3,q)$ the geometry where the points are the points of $\mathrm{PG}(3,q)$ and the lines are those lines of $\mathrm{PG}(3,q)$ that are isotropic with regard to the symplectic form (3), then it follows that $L(\mathcal{O})$ is a partial spread of $\mathrm{W}(3,q)$

It is well known, see e.g. [11], that $\mathrm{W}(3,q)$ is a GQ which is equivalent to the dual of $\mathrm{Q}(4,q)$. Hence, (maximal) partial ovoids of $\mathrm{Q}(4,q)$ are equivalent to (maximal) partial spreads of $\mathrm{W}(3,q)$. The Plücker coordinates in (2) demonstrate the explicit correspondence between $L(X)$ and X for our representation of $\mathrm{Q}^*(4,q)$. (This correspondence is linear because $\det X = 1$.)

We could equally well choose to present the theory developed in Section 2 in the framework of partial spreads of $\mathrm{W}(3,q)$ and spread sets. The extra condition that $I \in \mathcal{C}$ is not really a restriction, and is related to the fact that by Lemma 6 we can also require $I \in \mathcal{O}$ without loss of generality.

4 Another explicit description

In this section we give another explicit description of the known examples of affine ovoids of $\mathrm{Q}^*(4,q)$, although it is not directly related to $\mathrm{SL}(2,q)$.

We now choose a different representation of the parabolic quadric $\mathrm{Q}(4,q)$, i.e., as the quadric with equation $X_1^2+X_2^2+X_3^2+X_4^2 = X_0^2$. Two points X, Y on this quadric are collinear if and only if $X_1Y_1+X_2Y_2+X_3Y_3+X_4Y_4 = X_0Y_0$.

For π_∞ we again take the hyperplane with equation $X_0 = 0$. The affine points of the quadric then satisfy the property $X_0 \neq 0$, and again we may normalize their coordinates by setting $X_0 = 1$.

We shall consider several sets of vectors of norm 1 in a 4-dimensional real Euclidean space with the property that the number of mutual inner products among the vectors is relatively small. As a first example, consider the following set of 8 vectors :

$$\mathcal{K}_8 \stackrel{\text{def}}{=} \{(\pm 1,0,0,0),(0,\pm 1,0,0),(0,0,\pm 1,0),(0,0,0,\pm 1)\}.$$

Each vector in this set has norm 1 and inner products between different elements of $\mathcal{K}_8$ can only take the values 0 and -1, i.e., never 1. It fol-

lows that the set $\mathcal{O}$ of points with coordinates $(1, X_1, X_2, X_3, X_4)$, where $(X_1, X_2, X_3, X_4) \in \mathcal{K}_8$, is a set of 8 points of the (real) parabolic quadric where no two points are collinear. Hence, if we reduce this set modulo 3, we obtain an affine ovoid for the case $q = 3$.

The set $\mathcal{K}_8$ is a root system of rank 4 of type A_1^4. Root systems have the property that they allow only few different values for inner products. It is therefore natural to investigate whether they can lead to affine ovoids also for other values of q.

Indeed, consider the following root system (of type D_4) :

$$\mathcal{K}_{24} \stackrel{\text{def}}{=} \mathcal{K}_8 \cup \{(\pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2})\}.$$

Possible values for inner products of different elements are now $\frac{1}{2}$, 0, $-\frac{1}{2}$ and -1. Hence, reducing modulo 5 yields an affine ovoid (of size 24) for $q = 5$.

The same root system has an alternative representation.

$$\mathcal{K}'_{24} \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}\{(\pm1, \pm1, 0, 0), (\pm1, 0, \pm1, 0), \\ (\pm1, 0, 0, \pm1), (0, \pm1, \pm1, 0), (0, \pm1, 0, \pm1), (0, 0, \pm1, \pm1)\}.$$

This representation cannot be used in GF(5) because 2 is not a square modulo 5. However, in GF(7) we may write $\sqrt{2} = 3$.

It turns out that there are also only a small number of possibilities for inner products between elements of $\mathcal{K}_{24}$ and $\mathcal{K}'_{24}$, viz. $\pm1/\sqrt{2}$ and 0. As a consequence, the set $\mathcal{K}_{48} \stackrel{\text{def}}{=} \mathcal{K}_{24} \cup \mathcal{K}'_{24}$ only admits the inner products -1, $\pm1/2$, $\pm1/\sqrt{2}$ and 0. Modulo 7 all of these are different from 1, and hence we may use $\mathcal{K}_{48}$ to obtain an affine ovoid when $q = 7$.

Note that $\mathcal{K}_{48}$ can be obtained from the root system of type F_4 by normalizing the short and long vectors to become the same length. This is the largest root system of rank 4, hence for the case $q = 11$ we shall have to look elsewhere.

In that case the 600-cell, a 4-dimensional polytope of type H_4, comes to the rescue. The set $\mathcal{K}_{120}$ of coordinates of the 120 vertices of this polytope can be constructed by extending $\mathcal{K}_{24}$ with the 96 coordinates of the form $\frac{1}{2}(\pm1, \pm\varphi, \pm1/\varphi, 0)$, with $\varphi = \frac{1}{2}(1+\sqrt{5})$ (the golden ratio), where we allow all *even* permutations of the coordinates. Inner products among these vertices have values -1, $-\varphi/2$, $-1/2$, $-1/(2\varphi)$, 0, $1/(2\varphi)$, $1/2$, $\varphi/2$ or 1, where the latter value only occurs when both vectors are the same. In GF(11), $\sqrt{5} = 4$ and hence φ reduces to 8. In other words, $\mathcal{K}_{120}$ provides an example of an affine ovoid for $q = 11$.

Root systems have been used in the past for constructing other types of combinatorial object, e.g., (partial) flocks of hyperbolic quadrics by Bader et al. [1].

5 Concluding remarks

It was already mentioned that we are convinced that the four affine ovoids discussed in this paper constitute the full set of existing examples when q is odd, although so far a proof of this result has completely eluded us. We think that the representation of affine ovoids within $\mathrm{SL}(2,q)$ provides the most natural setting for such a proof, as it allows the use of both group theoretical and combinatorial techniques for tackling the problem. On the other hand, the setting of Section 4 is probably the best way to look for counterexamples.

By Theorem 8 our conjecture is equivalent to the statement that every sharply transitive subset of $\mathrm{SL}(2,q)$ is a coset of a subgroup. The analogous statement for $\mathrm{PGL}(2,q)$ is true, cf. [10], and equivalent to the classification of flocks of the hyperbolic quadric of $\mathrm{PG}(3,q)$, as was first observed by Bonisoli [3]. Unfortunately, the techniques used to prove this statement do not readily carry over to our case.

If our conjecture turns out to be too strong, then at least we expect all affine ovoids to consist of antipodal pairs (although again, we had no success in proving this weaker result). In that case, the problem of classifying all affine ovoids of $\mathrm{SL}(2,q)$ can be reduced to the same problem for the smaller group $\mathrm{PSL}(2,q)$, an affine ovoid then being defined as a set of size $\frac{1}{2}(q^2-1)$ of elements X, Y of $\mathrm{PSL}(2,q)$ such that $\mathrm{Tr}\, XY^{-1} \neq \pm 2$.

The problem can also be approached through the theory of association schemes. With $\mathrm{SL}(2,q)$ we may associate a scheme that consists of the relation of antipodality ($X = -Y$) together with q relations R_t for $t \in \mathrm{GF}(q)$, where $X\, R_t\, Y$ if and only if $\mathrm{Tr}\, XY^{-1} = t$ (and $X \neq \pm Y$). It is not so difficult to compute the various intersection numbers for this association scheme. The use of standard methods from the theory of association schemes is however somewhat hindered by the fact that the number of classes varies with q.

This setting is closely related to the group representation theory of $\mathrm{SL}(2,q)$. Indeed, the conjugacy classes of $\mathrm{SL}(2,q)$ correspond to the sets of matrices of given trace, where extra provision should be made for the singleton classes $\{I\}$ and $\{-I\}$. In this context it would also be nice to extend Lemma 10 with a non-trivial result for $\delta(t) < 0$.

Yet another alternative is to employ a computer to at least tackle the smaller cases. We have proved by computer that for $q = 3$, 5, 7 and 11

the affine ovoids are indeed unique and that for $q = 9$ none exist (which confirms the result of [6]). For $q = 9$ our program takes only a few minutes of CPU time while for $q = 11$ already three weeks were needed. We fear that for larger values of q the problem may already be intractable by standard methods. Again a stronger version of Lemma 10 might be of help.

References

[1] L. Bader, N. Durante, M. Law, G. Lunardon, and T. Penttila. Flocks and partial flocks of hyperbolic quadrics via root systems. *J. Algebraic Combin.*, 16(1):21–30, 2002.

[2] S. Ball, P. Govaerts, and L. Storme. On ovoids of parabolic quadrics. *Des. Codes Cryptogr.*, 38(1):131–145, 2006.

[3] A. Bonisoli. On the sharply 1-transitive subsets of $\mathrm{PGL}(2, p^m)$. *J. Geom.*, 31(1-2):32–41, 1988.

[4] M. R. Brown, J. De Beule, and L. Storme. Maximal partial spreads of $T_2(\mathcal{O})$ and $T_3(\mathcal{O})$. *European J. Combin.*, 24(1):73–84, 2003.

[5] A. Bruen. Partial spreads and replaceable nets. *Canad. J. Math.*, 23:381–391, 1971.

[6] J. De Beule and A. Gács. Complete arcs on the parabolic quadratic $\mathrm{Q}(4, q)$. *Finite Fields Appl.*, 14(1):14–21, 2008.

[7] J. De Beule, A. Klein, and K. Metsch. Substructures of finite classical polar spaces. In *Current research topics in Galois geometry*, chapter 2, pages 35–61. Nova Sci. Publ., New York, 2012.

[8] P. Dembowski. *Finite geometries*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Springer-Verlag, Berlin, 1968.

[9] S. De Winter and K. Thas. Bounds on partial ovoids and spreads in classical generalized quadrangles. *Innov. Incidence Geom.*, 11:19–33, 2010.

[10] N. Durante and A. Siciliano. (B)-geometries and flocks of hyperbolic quadrics. *J. Combin. Theory Ser. A*, 102(2):425–431, 2003.

[11] S. E. Payne and J. A. Thas. *Finite generalized quadrangles*. EMS Series of Lectures in Mathematics. European Mathematical Society (EMS), Zürich, second edition, 2009.

[12] T. Penttila. Private communication.

[13] M. Suzuki. *Group theory. I*, volume 247 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1982. Translated from the Japanese by the author.

[14] K. Thas. Nonexistence of complete $(st - t/s)$-arcs in generalized quadrangles of order (s, t). I. *J. Combin. Theory Ser. A*, 97(2):394–402, 2002.