# On minimum size blocking sets of the outer tangents to a hyperbolic quadric in PG(3, q)

Bart De Bruyn        Binod Kumar Sahoo

August 6, 2018

### Abstract

Let $Q^+(3, q)$ be a hyperbolic quadric in $\mathrm{PG}(3, q)$ and $\mathcal{T}_1$ be the set of all lines of $\mathrm{PG}(3, q)$ meeting $Q^+(3, q)$ in singletons (the so-called outer tangents). If $k$ is the minimum size of a $\mathcal{T}_1$-blocking set in $\mathrm{PG}(3, q)$, then we prove that $k \geq q^2 - 1$. It is known that there is no $\mathcal{T}_1$-blocking set of size $q^2 - 1$ for $q > 2$ even and that there is a unique (up to isomorphism) $\mathcal{T}_1$-blocking set of size 3 for $q = 2$. For $q = 3$, we prove as well that there is a unique $\mathcal{T}_1$-blocking set of size 8. Using a computer, we also classify all $\mathcal{T}_1$-blocking sets of size $q^2 - 1$ for each prime power $q \leq 13$. On basis of some structural similarities we are subsequently able to recognize three families of blocking sets whose further study shows that they can be constructed from certain objects related to finite fields (like nice subsets or permutations of the latter). This connection with finite fields allows us to obtain some computer free descriptions.

**Keywords:** Projective space, Blocking set, Conic, Ovoid, Hyperbolic quadric

**AMS 2010 subject classification:** 05B25, 51E21

## 1   Introduction

### 1.1   On the hyperbolic quadric $Q^+(3, q)$ in $\mathrm{PG}(3, q)$

Let $Q^+(3, q)$ be a hyperbolic quadric in $\mathrm{PG}(3, q)$. We denote by $\mathcal{E}$, $\mathcal{T}_1$, $\mathcal{S}$ and $\mathcal{T}_0$ the set of lines of $\mathrm{PG}(3, q)$ that intersect $Q^+(3, q)$ in respectively 0, 1, 2 and $q + 1$ points. The elements of $\mathcal{E}$ are called *external lines*, those of $\mathcal{S}$ *secant lines* and those of $\mathcal{T} := \mathcal{T}_0 \cup \mathcal{T}_1$ *tangent lines*. The tangent lines belonging to $\mathcal{T}_0$ are called the *inner tangents* and those of $\mathcal{T}_1$ the *outer tangents*. The inner tangents are precisely the lines contained in $Q^+(3, q)$, and so we have $|\mathcal{T}_0| = 2(q + 1)$. As every point of $Q^+(3, q)$ is contained in $q - 1$ outer tangents, we have $|\mathcal{T}_1| = (q + 1)^2(q - 1)$ and hence $|\mathcal{T}| = (q + 1)(q^2 + 1)$. We also have $|\mathcal{S}| = \frac{1}{2}q^2(q+1)^2$ and $|\mathcal{E}| = (q^2+1)(q^2+q+1) - \frac{1}{2}q^2(q+1)^2 - (q+1)(q^2+1) = \frac{1}{2}q^2(q-1)^2$.

With the quadric $Q^+(3, q)$, there is naturally associated a polarity $\zeta$ which is symplectic if $q$ is even and orthogonal if $q$ is odd. For every point $x$ of $Q^+(3, q)$, $x^\zeta$ is a plane which is

1

*tangent to* $Q^+(3,q)$ *at the point* $x$ and intersects $Q^+(3,q)$ in the union of two lines through $x$. The $q + 1$ tangent lines through $x$ are precisely the lines through $x$ contained in $x^\zeta$.

Suppose $q$ is even. With the symplectic polarity $\zeta$, there is associated a symplectic generalized quadrangle $W(q)$, whose points are the points of $\mathrm{PG}(3,q)$ and whose lines are the lines of $\mathrm{PG}(3,q)$ that are totally isotropic with respect to $\zeta$, with incidence being containment. The lines of $W(q)$ are precisely the elements of $\mathcal{T}$.

For every point $x$ of $\mathrm{PG}(3,q) \setminus Q^+(3,q)$, $x^\zeta$ is a plane through the point $x$, and the tangent lines contained in $x^\zeta$ are precisely the lines of $x^\zeta$ through $x$. The plane $x^\zeta$ intersects $Q^+(3,q)$ in a conic $O_x$ with kernel $x$. This conic $O_x$ is also an ovoid[1] of $Q^+(3,q)$ as it intersects each inner tangent in a unique point. The map $x \mapsto O_x$ defines a bijection between $\mathrm{PG}(3,q) \setminus Q^+(3,q)$ and the set of conics contained in $Q^+(3,q)$.

Suppose $q$ is odd. For every point $x$ of $\mathrm{PG}(3,q) \setminus Q^+(3,q)$, $x^\zeta$ is a nontangent plane with $x \notin x^\zeta$ and it meets $Q^+(3,q)$ in a conic $O_x$ of $x^\zeta$. The tangent lines through $x$ are precisely the lines through $x$ meeting the conic $O_x$. Again, the conic $O_x$ is an ovoid of $Q^+(3,q)$ and the map $x \mapsto O_x$ defines a bijection between $\mathrm{PG}(3,q) \setminus Q^+(3,q)$ and the set of conics contained in $Q^+(3,q)$.

## 1.2   Blocking sets in $\mathrm{PG}(3,q)$

For a given nonempty set $\mathcal{L}$ of lines of $\mathrm{PG}(3,q)$, a set $X$ of points of $\mathrm{PG}(3,q)$ is called an $\mathcal{L}$-*blocking set* if each line of $\mathcal{L}$ meets $X$. Continuing with the notation of Section 1.1, we call two $\mathcal{L}$-blocking sets $X_1$ and $X_2$ with $\mathcal{L} \in \{\mathcal{E}, \mathcal{S}, \mathcal{T}, \mathcal{T}_0, \mathcal{T}_1\}$ *isomorphic* if there exists an automorphism of $\mathrm{PG}(3,q)$ stabilizing $Q^+(3,q)$ and mapping $X_1$ to $X_2$.

The first step in the study of blocking sets has been to determine the smallest cardinality of a blocking set and to characterize, if possible, all blocking sets of that cardinality.

If $\mathcal{L}$ is the set of all lines of $\mathrm{PG}(3,q)$ and $X$ is an $\mathcal{L}$-blocking set, then $|X| \geq q^2 + q + 1$ and equality holds if and only if $X$ is a plane of $\mathrm{PG}(3,q)$. This follows from a more general result by Bose and Burton [4, Theorem 1]. Biondi et al. characterized the minimum size $\mathcal{E}$-blocking sets in [3, Theorem 2.4] for $q \geq 9$ odd and in [2, Theorem 1.1] for $q \geq 8$ even (also see [14, Section 3] and [11, Section 2] for a different proof which works for all $q$). When $q > 2$ is even, the minimum size $(\mathcal{E} \cup \mathcal{S})$-blocking sets were determined in [16, Theorem 1.3] using properties of generalized quadrangles. For $\mathcal{L} \in \{\mathcal{S}, \mathcal{T} \cup \mathcal{S}, \mathcal{E} \cup \mathcal{S}\}$, the minimum size $\mathcal{L}$-blocking sets are described in [15, Theorems 1.7, 1.8, 1.9] for all $q$. The minimum size $(\mathcal{E} \cup \mathcal{T})$-blocking sets are characterized in [14, Proposition 1.5] for $q$ even and in [11, Theorem 1.1] for all $q \geq 3$.

If $k$ is the minimum size of a $\mathcal{T}$-blocking set in $\mathrm{PG}(3,q)$, then $q^2 + 1 \leq k \leq q^2 + q$ by [10, Lemmas 2.1, 2.2]. If $q$ is even, then the $\mathcal{T}$-blocking sets of size $q^2 + 1$ are precisely the ovoids of the generalized quadrangle $W(q)$ associated with $Q^+(3,q)$. There are two known types of such ovoids: ovoids which are *elliptic quadrics* of the ambient projective space $\mathrm{PG}(3,q)$ and the so-called *Suzuki-Tits ovoids*. The former ovoids exist for each power of 2 and the latter only for the prime powers of the form $2^{2e+1}$ with $e \in \mathbb{N} \setminus \{0\}$.

---

[1]An *ovoid* of a point-line geometry is a set of points meeting each line in a singleton.

For $q \leq 32$, it has been proved that every ovoid of $W(q)$, $q$ even, is either an elliptic quadric or a Suzuki-Tits ovoid. In the $q$ odd case, not much is known for the minimum size $\mathcal{T}$-blocking sets. In $\mathrm{PG}(3,3)$, by [10, Theorem 1.1], there is no $\mathcal{T}$-blocking set of size 10 and there are exactly two $\mathcal{T}$-blocking sets of size 11 up to isomorphism. By means of the computer algebra systems GAP [18] and Sage [13], it was proved that there exist no $\mathcal{T}$-blocking sets of size $q^2 + 1$ for each odd prime power $q \leq 13$, see [10, Theorem 1.2].

## 1.3 $\mathcal{T}_1$-blocking sets

The minimum size $\mathcal{T}_0$-blocking sets are well known as these are precisely the ovoids of $Q^+(3,q)$. In this paper, we shall study the minimum size $\mathcal{T}_1$-blocking sets. In the following lemma, we derive a lower bound for the size of such blocking sets.

**Lemma 1.1** *If $X$ is a $\mathcal{T}_1$-blocking set, then $|X| \geq q^2 - 1$, with equality if and only if $X \cap Q^+(3,q) = \emptyset$ and every outer tangent contains a unique point of $X$.*

**Proof.** We count in two ways the number of pairs $(x, L)$, where $x \in X$ and $L$ is an outer tangent containing $x$. The number $N$ of such pairs is equal to $|X \cap Q^+(3,q)| \cdot (q-1) + |X \setminus Q^+(3,q)| \cdot (q+1)$. We thus have $N \leq |X| \cdot (q+1)$, with equality if and only if $X \cap Q^+(3,q) = \emptyset$. As each of the $(q+1)^2(q-1)$ outer tangents contains at least one point of $X$, we have $(q+1)^2(q-1) \leq N$ with equality if and only if every outer tangent contains a unique point of $X$. Combining both inequalities for $N$, we find $(q+1)^2(q-1) \leq |X| \cdot (q+1)$, that is, $q^2 - 1 \leq |X|$. By the above, the necessary and sufficient conditions for equality are as stated in the lemma. ∎

The following lemma is proved in the same way as Lemma 1.1.

**Lemma 1.2** *Let $\Omega$ be a set of points of $\mathrm{PG}(3,q)$ disjoint from $Q^+(3,q)$ such that every outer tangent meets $\Omega$ in at most one point. Then $|\Omega| \leq q^2 - 1$, with equality if and only if every outer tangent meets $\Omega$ in precisely one point.*

Suppose now that $q$ is even. As said before, the lines of $W(q)$ are then the elements of $\mathcal{T} = \mathcal{T}_0 \cup \mathcal{T}_1$. So, every ovoid of $W(q)$ is a $\mathcal{T}_1$-blocking set, showing that the minimum size $k$ of a $\mathcal{T}_1$-blocking set satisfies $q^2 - 1 \leq k \leq q^2 + 1$. $\mathcal{T}_1$-blocking sets of size $q^2 - 1$ are maximal partial ovoids of $W(q)$. Indeed, by Lemma 1.1 we know that every $\mathcal{T}_1$-blocking set of size $q^2 - 1$ is disjoint from each $\mathcal{T}_0$-line and meets each $\mathcal{T}_1$-line in a singleton; the maximality as partial ovoid follows from the fact that each point of $\mathrm{PG}(3,q)$ is contained in an outer tangent. By [5, Corollary 1], maximal partial ovoids of size $q^2 - 1$ of $W(q)$, $q$ even, cannot exist if $q > 2$. For $q = 2$, there is up to isomorphism a unique partial ovoid of size 3 of $W(2)$ that is also a $\mathcal{T}_1$-blocking set, see e.g. [17, Theorem 3.9]. Nothing seems to be known about $\mathcal{T}_1$-blocking sets of size $q^2$. It is also not known whether $\mathcal{T}_1$-blocking sets of size $q^2 + 1$ are always ovoids of $W(q)$.

Let us therefore consider the case where $q$ is odd. Francesco Pavese pointed out to the authors that $\mathcal{T}_1$-blocking sets of size $q^2 - 1$ are related to maximal partial ovoids of size $q^2 - 1$ of the generalized quadrangle $Q(4,q)$, see Section 2. This connection allows to prove the following.

3

**Theorem 1.3** $\mathcal{T}_1$-blocking sets of size $q^2 - 1$, $q$ odd, can only exist if $q$ is a prime.

For $q \in \{3, 5, 7, 11\}$, we are able to construct a number of $\mathcal{T}_1$-blocking sets of size $q^2 - 1$. We have also used the computer algebra systems GAP [18] and Sage [13] to classify all $\mathcal{T}_1$-blocking sets of minimum size $q^2 - 1$ for each odd prime $q \leq 13$, see [9]. Our results are as follows.

**Theorem 1.4** There are no $\mathcal{T}_1$-blocking sets of size $q^2 - 1$ for $q = 13$. The number of nonisomorphic $\mathcal{T}_1$-blocking sets of size $q^2 - 1$ is equal to 1 if $q = 3$, equal to 3 if $q = 5$ and equal to 4 if $q \in \{7, 11\}$.

In the following table, we provide some information about these $\mathcal{T}_1$-blocking sets. Also this information was obtained by means of computer computations.

| Set | $q$ | Number | IP secants | IP externals | $\mathcal{T}$-block. sets |
|---|---|---|---|---|---|
| $B_1$ | 3 | 9 | $0^{32}1^{32}2^8$ | $0^8 2^8 4^2$ | 1 |
| $B_2$ | 5 | 200 | $0^{198}1^{144}2^{108}$ | $0^{64}1^{72}2^{36}3^{24}6^4$ | 1 |
| $B_3$ | 5 | 400 | $0^{180}1^{198}2^{54}3^{18}$ | $0^{60}1^{90}2^{18}3^{14}4^{18}$ | 2 |
| $B_4$ | 5 | 25 | $0^{144}1^{288}4^{18}$ | $0^{96}2^{72}3^{32}$ | 1 |
| $B_5$ | 7 | 3528 | $0^{576}1^{736}2^{192}3^{32}4^{32}$ | $0^{294}1^{320}2^{168}3^{64}4^{28}6^8$ | 2 |
| $B_6$ | 7 | 784 | $0^{576}1^{720}2^{216}3^{48}6^8$ | $0^{306}1^{288}2^{216}4^{72}$ | 1 |
| $B_7$ | 7 | 4704 | $0^{592}1^{696}2^{216}3^{40}4^{24}$ | $0^{276}1^{360}2^{156}3^{48}4^{18}5^{24}$ | 2 |
| $B_8$ | 7 | 588 | $0^{640}1^{576}2^{288}3^{64}$ | $0^{324}1^{192}2^{336}4^{24}8^6$ | 1 |
| $B_9$ | 11 | 2904 | $0^{2880}1^{4200}2^{1500}5^{120}10^{12}$ | $0^{2500}1^{1200}2^{1800}3^{400}4^{150}$ | 1 |
| $B_{10}$ | 11 | 29040 | $0^{2928}1^{4140}2^{1500}5^{84}6^{60}$ | $0^{2140}1^{2100}2^{1200}3^{400}4^{150}5^{60}$ | 2 |
| $B_{11}$ | 11 | 24200 | $0^{2880}1^{4248}2^{1440}5^{72}6^{72}$ | $0^{2112}1^{2304}2^{792}3^{672}4^{162}6^8$ | 2 |
| $B_{12}$ | 11 | 2420 | $0^{3168}1^{3600}2^{1800}5^{144}$ | $0^{2040}1^{2160}2^{1440}3^{240}4^{90}6^{80}$ | 1 |

Given a particular $\mathcal{T}_1$-blocking set $B$ and a set $\mathcal{L} \in \{\mathcal{S}, \mathcal{E}\}$, the *intersection pattern (IP)* of $B$ with respect to the lines of $\mathcal{L}$ is defined as the sequence $n_1^{e_1} n_2^{e_2} \cdots n_k^{e_k}$, where

- $k \in \mathbb{N} \setminus \{0\}$;
- $n_1, n_2, \ldots, n_k \in \mathbb{N}$ with $n_1 < n_2 < \cdots < n_k$;
- $e_1, e_2, \ldots, e_k \in \mathbb{N} \setminus \{0\}$;
- for every $i \in \{1, \ldots, k\}$, there are $e_i$ lines in $\mathcal{L}$ that intersect $B$ in $n_i$ points.

The intersection pattern of the various blocking sets with respect to $\mathcal{S}$ and $\mathcal{E}$ have been mentioned in columns 4 and 5 of the above table. The number of $\mathcal{T}_1$-blocking sets isomorphic to a given blocking set $B_i$ is given in the third column. On basis of computer data of the various blocking sets, we have been able to describe three families of blocking sets. These will respectively be studied in Sections 3, 4 and 5.

The blocking sets $B_1$, $B_2$, $B_8$ belong to the first family, all whose members $B$ have the special property that they can be partitioned by $q - 1$ external lines. These external lines are moreover contained in a regular spread together with one of the two reguli of $Q^+(3, q)$.

We show in Section 3 that these blocking sets arise from subsets $\{\alpha_1, \alpha_2, \ldots, \alpha_{q-1}\}$ of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ that satisfy the following properties:

(a) $\alpha_i - \alpha_j \notin \mathbb{F}_q$ for all $i, j \in \{1, 2, \ldots, q-1\}$ with $i \neq j$;

(b) $\frac{1}{\alpha_i + l} - \frac{1}{\alpha_j + l} \notin \mathbb{F}_q$ for all $l \in \mathbb{F}_q$ and all $i, j \in \{1, 2, \ldots, q-1\}$ with $i \neq j$.

The blocking sets $B_1$, $B_4$, $B_6$ and $B_9$ belong to the second family, all whose members $B$ have the special property that there exist two disjoint lines $L_1$ and $L_2$ of $Q^+(3, q)$ and $q + 1$ mutually disjoint lines $K_1, K_2, \ldots, K_{q+1}$ meeting $L_1$ and $L_2$ such that $B = (K_1 \cup K_2 \cup \cdots \cup K_{q+1}) \setminus (L_1 \cup L_2)$. We show in Section 4 that these blocking sets arise from permutations $\sigma$ of $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ that satisfy the following properties:

(P1) $\sigma$ has no fixed points;

(P2) $\sigma^2 = 1$;

(P3) $(x - x^\sigma)x$ is a nonsquare for all $x \in \mathbb{F}_q^*$;

(P4) $(x^\sigma - x)(y^\sigma - y)(y - x)(y^\sigma - x^\sigma)$ is a nonsquare for all $x, y \in \mathbb{F}_q^*$ with $y \notin \{x, x^\sigma\}$.

The blocking sets $B_1$, $B_3$ and $B_5$ belong to the third family, all whose members $B$ have the special property that there exist two mutually disjoint external lines $L_1$ and $L_2$ and $q + 1$ mutually disjoint external lines $K_1, K_2, \ldots, K_{q+1}$ meeting $L_1$ and $L_2$ such that $B = (K_1 \cup K_2 \cup \cdots \cup K_{q+1}) \setminus (L_1 \cup L_2)$.

The following proposition says that every $\mathcal{T}_1$-blocking set of size $q^2 - 1$ will give rise to a $\mathcal{T}$-blocking set of size $q^2 + q - 1$.

**Proposition 1.5** *Suppose $X$ is a $\mathcal{T}_1$-blocking set of size $q^2 - 1$ in $\mathrm{PG}(3, q)$. Let $x$ be a point of $X$ and let $Y$ be the set of $q + 1$ points of $Q^+(3, q)$ that are the tangency points of the outer tangents through $x$. Then $(X \setminus \{x\}) \cup Y$ is a $\mathcal{T}$-blocking set of size $q^2 + q - 1$.*

**Proof.** Note that $X \cap Q^+(3, q) = \emptyset$ by Lemma 1.1. As $Y$ is an ovoid of $Q^+(3, q)$, every inner tangent meets $Y$. Suppose $L$ is an outer tangent. Then $L$ meets $X$. If $L$ would not meet $X \setminus \{x\}$, then it contains $x$ and hence must contain a point of $Y$. So, $(X \setminus \{x\}) \cup Y$ is a $\mathcal{T}$-blocking set of size $q^2 + q - 1$. ∎

Note that it is possible that a $\mathcal{T}_1$-blocking set of size $q^2 - 1$ gives rise to several non-isomorphic $\mathcal{T}$-blocking sets of size $q^2 + q - 1$. The last column of the table mentions how many nonisomorphic $\mathcal{T}$-blocking sets of size $q^2 + q - 1$ arise from the $\mathcal{T}_1$-blocking set $B_i$, $i \in \{1, \ldots, 12\}$. Using Theorem 1.4 and Proposition 1.5, we can thus construct $\mathcal{T}$-blocking sets whose size is strictly smaller than $q^2 + q$ for $q \in \{3, 5, 7, 11\}$. The number of nonisomorphic $\mathcal{T}$-blocking sets of size $q^2 + q - 1$ that arise in this fashion is one if $q = 3$, four if $q = 5$ and six if $q \in \{7, 11\}$. Besides these seventeen $\mathcal{T}$-blocking sets, one additional $\mathcal{T}$-blocking set is known whose size is strictly smaller than $q^2 + q$, namely a particular $\mathcal{T}$-blocking set of size 11 in $\mathrm{PG}(3, 3)$, see [10, Section 3]. Note that $\mathcal{T}$-blocking sets of size $q^2 + q$ always exist, namely tangent planes minus their tangency points.

5

# 2 Proof of Theorem 1.3

The result stated in Theorem 1.3 was communicated to the authors by Francesco Pavese after submission of this paper. The authors wish to thank him for his permission to include this result in the final version. The following chain of results is in fact an expansion of his arguments as communicated to one of us in an email.

**Lemma 2.1** *Consider a parabolic quadric $Q(4,q)$ in $\mathrm{PG}(4,q)$, $q$ odd, and let $\zeta$ be the orthogonal polarity of $\mathrm{PG}(4,q)$ associated with $Q(4,q)$. Let $L$ be a secant line of $Q(4,q)$, put $\alpha = L^\zeta$ and let $a, b \in L \setminus Q(4,q)$ such that $b \in a^\zeta$. Then:*

   (1) *If $q \equiv 1 \pmod 4$, then $\langle a, \alpha \rangle$ and $\langle b, \alpha \rangle$ intersect $Q(4,q)$ in nonsingular quadrics of the same type (i.e. both hyperbolic or elliptic).*

   (2) *If $q \equiv 3 \pmod 4$, then $\langle a, \alpha \rangle$ and $\langle b, \alpha \rangle$ intersect $Q(4,q)$ in nonsingular quadrics of different types.*

**Proof.** We introduce coordinates $(X_0, X_1, X_2, X_3, X_4)$ such that $Q(4,q)$ has equation $X_0^2 + X_1 X_2 + X_3 X_4 = 0$ and $L$ has equation $X_0 = X_1 = X_2 = 0$. Then $a = (0,0,0,1,t)$ and $b = (0,0,0,-1,t)$ for some $t \in \mathbb{F}_q^*$. The plane $\alpha$ has equation $X_3 = X_4 = 0$. The hyperplane $\langle a, \alpha \rangle$ has equation $tX_3 - X_4 = 0$ and intersects $Q(4,q)$ in a nonsingular quadric with equation $X_0^2 + X_1 X_2 + tX_3^2 = 0$. This is a hyperbolic quadric if and only if $-t$ is a square. The hyperplane $\langle b, \alpha \rangle$ has equation $tX_3 + X_4 = 0$ and intersects $Q(4,q)$ in a nonsingular quadric with equation $X_0^2 + X_1 X_2 - tX_3^2 = 0$. This is a hyperbolic quadric if and only if $t$ is a square. So, both intersections have the same type if and only if $-1$ is a square, i.e. $q \equiv 1 \pmod 4$. ∎

Let $Q^+(3,q)$, $q$ odd, be embedded as a hyperplane section in $Q(4,q)$, and let $\zeta$ be the polarity of $\mathrm{PG}(4,q)$ associated with $Q(4,q)$. Let $\pi$ be the hyperplane of $\mathrm{PG}(4,q)$ such that $\pi \cap Q(4,q) = Q^+(3,q)$, and put $x^* := \pi^\zeta$. Let $H$, respectively $E$, denote the set of all points $y$ of $\mathrm{PG}(4,q) \setminus Q(4,q)$ for which $y^\zeta \cap Q(4,q)$ is a hyperbolic quadric, respectively an elliptic quadric. Put $U := H \cap \pi$ if $q \equiv 1 \pmod 4$ and $U := E \cap \pi$ if $q \equiv -1 \pmod 4$. The following three properties are known and easily follow from counting the points of $Q(4,q)$ with respect to the $q+1$ hyperplanes through the plane $L^\zeta$:

   (A) If $L$ is a line of $\pi$ exterior to $Q^+(3,q)$, then $|L \cap H| = |L \cap E| = |L \cap U| = \frac{q+1}{2}$.

   (B) If $L$ is a line of $\pi$ secant to $Q^+(3,q)$, then $|L \cap H| = |L \cap E| = |L \cap U| = \frac{q-1}{2}$.

   (C) If $L$ is an outer tangent to $Q^+(3,q)$ (in $\pi$), then $(|L \cap H|, |L \cap E|)$ is either $(q, 0)$ or $(0, q)$. In particular, every outer tangent to $Q^+(3,q)$ meets $U$ in either $0$ or $q$ points.

**Lemma 2.2** *The number of outer tangents to $Q^+(3,q)$ that meet $U$ in precisely $q$ points is half the number of outer tangents to $Q^+(3,q)$.*

6

**Proof.** As every outer tangent to $Q^+(3,q)$ is contained in a unique tangent plane to $Q^+(3,q)$ (in $\pi$), it suffices to prove this claim for the outer tangents contained in a particular tangent plane $\alpha \subseteq \pi$. But this follows from (B) and (C) by considering a secant line contained in $\alpha$. ∎

**Lemma 2.3** *If $X \subseteq \pi$ is a $\mathcal{T}_1$-blocking set of size $q^2 - 1$ (with respect to $Q^+(3,q)$), then $|X \cap U| = \frac{|X|}{2} = \frac{q^2-1}{2}$.*

**Proof.** Every outer tangent intersects $X$ in precisely one point. The claim then follows from Lemma 2.2 taking into account that every point of $X$ is contained in a constant number of outer tangents (namely $q + 1$). ∎

Note that $(x^*)^\zeta \cap Q(4,q) = Q^+(3,q)$ is a hyperbolic quadric. By Lemma 2.1 and the definition of the set $U$, we thus have:

**Lemma 2.4** *If $L$ is a secant line (to $Q(4,q)$) through $x^*$, then the unique point in $L \cap \pi$ belongs to $U$.*

**Lemma 2.5** *If $L$ is an external line (to $Q(4,q)$) through $x^*$, then the unique point of $L \cap \pi$ does not belong to $U$.*

**Proof.** Let $L'$ be a secant line through $x^*$ and consider the plane $\alpha = \langle L, L' \rangle$. As $\alpha$ contains an external line, it cannot be a tangent plane[2] and so intersects $\pi$ in an external or secant line $M$. By (A) and (B), the number of points of $|M \cap U|$ is equal to $\frac{|M \setminus Q^+(3,q)|}{2} = \frac{q+1-|M \cap Q^+(3,q)|}{2}$. As $|\alpha \cap Q(4,q)| = q + 1$ and $M \subseteq (x^*)^\zeta$, also the number of secant lines through $x^*$ contained in $\alpha$ is equal to $\frac{(q+1)-|M \cap Q^+(3,q)|}{2}$. These facts in combination with Lemma 2.4 imply that the unique point in the intersection $L \cap \pi$ does not belong to $U$. ∎

**Lemma 2.6** *Suppose $u_1$ and $u_2$ are two distinct points of $U$ such that $u_1 u_2$ is not an outer tangent to $Q^+(3,q)$. Then the plane $\langle x^*, u_1, u_2 \rangle$ is not a tangent plane.*

**Proof.** If this plane were a tangent plane, then its tangency point would belong to $(x^*)^\zeta = \pi$ and so $\langle x^*, u_1, u_2 \rangle \cap \pi = u_1 u_2$ would be an outer tangent, a contradiction. ∎

Theorem 1.3 is a consequence of the following proposition.

**Proposition 2.7** *Suppose $X \subseteq \pi$ is a blocking set of size $q^2 - 1$ with respect to the outer tangents to $Q^+(3,q)$. For every point $x \in X \cap U$, let $O_x$ be the set of two points of $Q(4,q)$ on the secant line $x^* x$ (see Lemmas 2.4 and 2.5). Then $O := \bigcup_{x \in X \cap U} O_x$ is a maximal partial ovoid of size $q^2 - 1$ of $Q(4,q)$. Moreover, $q$ must be prime.*

**Proof.** By Lemma 2.3, we know that $|X \cap U| = \frac{q^2-1}{2}$ and so $|O| = q^2 - 1$. The two points in each $O_x$, $x \in X \cap U$, are noncollinear in $Q(4,q)$. Suppose now that $x_1$ and $x_2$ are two

---

[2]With a tangent plane, we mean here a plane intersecting $Q(4,q)$ in the union of two lines.

distinct points of $X \cap U$ and that $y_1 \in O_{x_1}$, $y_2 \in O_{x_2}$ are collinear in $Q(4, q)$. Then the plane $\langle x^*, x_1, x_2 \rangle$ would be a tangent plane, in contradiction with Lemma 2.6.

So, $O$ is a partial ovoid of size $q^2 - 1$ of $Q(4, q)$. We now show that $O$ is a maximal partial ovoid of $Q(4, q)$. Suppose to the contrary that there exists a point $v$ of $Q(4, q)$ not belonging to $O$ for which $O \cup \{v\}$ is also a partial ovoid. We distinguish two cases.

Suppose $v \in Q^+(3, q)$. Let $L \subseteq \pi$ be an outer tangent to $Q^+(3, q)$ through $v$ containing $q$ points of $U$. Let $u$ be the unique point of $L \cap X$. Then $\langle L, x^* \rangle$ is a tangent plane to $Q(4, q)$ which intersects $Q(4, q)$ in the union of two lines, namely $\langle L, x^* \rangle \cap Q(4, q) = vy_1 \cup vy_2$, where $O_u = \{y_1, y_2\} \subseteq O$. This is in contradiction with the fact that $v$ is not collinear in $Q(4, q)$ with any point of $O$.

Suppose $v \notin Q^+(3, q)$. Then $x^*v$ is a secant line meeting $\pi$ in a point $u \in U \setminus X$. There exists an outer tangent $L$ to $Q^+(3, q)$ containing $u$ and this outer tangent contains a unique point $u' \in X$. The pair $\{u, u'\}$ is a subset of either $H$ or $E$. So, $u' \in X \cap U$. Putting $L \cap Q^+(3, q) = \{w\}$ and $O_{u'} = \{y_1, y_2\} \subseteq O$, we again see that $\langle x^*, L \rangle$ is a tangent plane intersecting $Q(4, q)$ in $wy_1 \cup wy_2$. As $v \in wy_1 \cup wy_2$, the point $v$ is collinear in $Q(4, q)$ with either $y_1$ or $y_2$, again a contradiction.

So, $O$ is a maximal partial ovoid of size $q^2 - 1$ of $Q(4, q)$. By Theorem 3 of [8], we know that maximal partial ovoids of $Q(4, q)$ of size $q^2 - 1$ can only exist if $q$ is a prime. ∎

# 3 A first family of $\mathcal{T}_1$-blocking sets

The first family of $\mathcal{T}_1$-blocking sets that we are going to define and investigate is related to regular spreads of $\mathrm{PG}(3, q)$.

## 3.1 Regular spreads of $\mathrm{PG}(3, q)$

Let $\widetilde{V}$ be a 4-dimensional vector space over $\mathbb{F}_{q^2}$ with basis $\{\bar{v}_1, \bar{v}_2, \bar{v}_3, \bar{v}_4\}$. The set $V$ consisting of all linear combinations of $\bar{v}_1, \bar{v}_2, \bar{v}_3, \bar{v}_4$ with coefficients in $\mathbb{F}_q$ can naturally be given the structure of a 4-dimensional vector space over $\mathbb{F}_q$. We denote by $\mathrm{PG}(3, q^2) = \mathrm{PG}(\widetilde{V})$ and $\mathrm{PG}(3, q) = \mathrm{PG}(V)$ the projective spaces associated with the respective vector spaces $\widetilde{V}$ and $V$. Since every 1-dimensional subspace of $V$ is contained in a unique 1-dimensional subspace of $\widetilde{V}$, we can and will regard the points of $\mathrm{PG}(V)$ as points of $\mathrm{PG}(\widetilde{V})$.

For every vector $\bar{v} = \alpha_1 \bar{v}_1 + \alpha_2 \bar{v}_2 + \alpha_3 \bar{v}_3 + \alpha_4 \bar{v}_4$ of $\widetilde{V}$ with all $\alpha_i$'s belonging to $\mathbb{F}_{q^2}$, we define $\bar{v}^q := \alpha_1^q \bar{v}_1 + \alpha_2^q \bar{v}_2 + \alpha_3^q \bar{v}_3 + \alpha_4^q \bar{v}_4$, for every point $x = \langle \bar{v} \rangle$ of $\mathrm{PG}(\widetilde{V})$, we define $x^q := \langle \bar{v}^q \rangle$, and for every subspace $\Sigma$ of $\mathrm{PG}(\widetilde{V})$ we define $\Sigma^q := \{x^q \mid x \in \Sigma\}$. The vectors $\bar{v} \in \widetilde{V}$ for which $\bar{v}^q = \bar{v}$ are precisely the vectors of $V$, and the points $x$ of $\mathrm{PG}(\widetilde{V})$ satisfying $x^q = x$ are precisely the points of $\mathrm{PG}(V)$.

Now, let $L^*$ be a line of $\mathrm{PG}(\widetilde{V})$ for which $L^* \cap (L^*)^q = \emptyset$. For every point $x$ of $L^*$, the line $xx^q$ of $\mathrm{PG}(\widetilde{V})$ intersects $\mathrm{PG}(V)$ in a line $L_x$ of $\mathrm{PG}(V)$. In this way, we get a

collection $S = \{L_x \mid x \in L^*\}$ of $q^2 + 1$ mutually disjoint lines of PG($V$) forming a *regular spread* of PG($3, q$). The following fact is known, see e.g. Theorem 5.3 of Bruck [6].

> Suppose $x_1, x_2, x_3$ are three mutually distinct points of $L^*$ and let $B$ be the unique Baer subline of $L^*$ containing $\{x_1, x_2, x_3\}$. Then the set $\mathcal{R}_B := \{L_x \mid x \in B\}$ is the unique regulus of PG($3, q$) containing the lines $L_{x_1}$, $L_{x_2}$ and $L_{x_3}$.

Now, let $B^*$ be a fixed Baer subline of $L^*$ and put $\mathcal{R}^* := \mathcal{R}_{B^*}$. Then the union of all lines of $\mathcal{R}^*$ is a hyperbolic quadric $Q^+(3, q)$ of PG($3, q$).

If $L$ is a line of PG($3, q$) not belonging to $S$, then the set of lines of $S$ meeting $L$ is a regulus $\mathcal{R}_L$ of PG($3, q$). We denote by $B_L$ the unique Baer subline $B$ of $L^*$ for which $\mathcal{R}_B = \mathcal{R}_L$.

## 3.2 Description and investigation of the family

**Lemma 3.1** *If $L$ is an outer tangent to $Q^+(3, q)$, then $B_L$ intersects $B^*$ in a singleton. Conversely, every Baer subline of $L^*$ intersecting $B^*$ in a singleton is of the form $B_L$ for some outer tangent line $L$.*

**Proof.** Suppose $L$ is an outer tangent. Let $x$ denote the unique point of $L \cap Q^+(3, q)$, let $U$ denote the unique line of $S$ through $x$ and let $y$ denote the unique point of $L^*$ for which $L_y = U$. Since $L \cap Q^+(3, q) = \{x\}$, we have $\mathcal{R}_L \cap \mathcal{R}^* = \{U\}$ and $B_L \cap B^* = \{y\}$.

Conversely, suppose that $B$ is a Baer subline of $L^*$ intersecting $B^*$ in a singleton $\{y\}$. Then $\mathcal{R}_B \cap \mathcal{R}^* = \mathcal{R}_B \cap \mathcal{R}_{B^*} = \{L_y\}$. Let $x$ be an arbitrary point of $L_y$ and let $L$ be the unique line through $x$ meeting each line of $\mathcal{R}_B$. As $\mathcal{R}_B \cap \mathcal{R}_{B^*} = \{L_y\}$, $L_y$ is the only line of $\mathcal{R}_{B^*}$ that meets $L$, implying that $\{x\} = L_y \cap L$ is the only point of $Q^+(3, q)$ contained in $L$. So, $L$ is an outer tangent. Obviously, we have $\mathcal{R}_L = \mathcal{R}_B$ and so $B_L = B$. ∎

Now, suppose that $X'$ is a set of points of $L^*$ which is disjoint from $B^*$. Put $S' = \{L_x \mid x \in X'\} \subseteq S \setminus \mathcal{R}^*$, and $\Omega := \bigcup_{L \in S'} L$.

**Lemma 3.2** *Let $L$ be an outer tangent. Then $|L \cap \Omega|$ equals the number of points of $X'$ that are contained in $B_L$.*

**Proof.** As $L$ intersects one of the lines of $\mathcal{R}^* \subseteq S$ in a unique point, it will intersect each line of $S$ in at most one point. So, $|L \cap \Omega|$ equals the number of lines of $S'$ that $L$ meets, that is, $|L \cap \Omega| = |\mathcal{R}_L \cap S'|$. The latter number is also equal to $|B_L \cap X'|$. ∎

The following is an immediate consequence of Lemmas 1.2, 3.1 and 3.2.

**Proposition 3.3** *Suppose $X'$ is a set of $q - 1$ points. Then $\Omega$ is a $\mathcal{T}_1$-blocking set of size $q^2 - 1$ if and only if one of the following two equivalent conditions hold:*

(1) *Every Baer subline of $L^*$ meeting $B^*$ in a singleton contains a unique point of $X'$.*

(2) *Every Baer subline of $L^*$ meeting $B^*$ in a singleton contains at most one point of $X'$.*

Now, we choose a reference system $\{\bar{e}_1, \bar{e}_2\}$ for $L^*$ in such a way that $B^*$ consists of all points $\langle k_1\bar{e}_1 + k_2\bar{e}_2 \rangle$, where $k_1, k_2 \in \mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\}$. Suppose $X' = \{x_1, x_2, \dots, x_{q-1}\}$ is a set of $q-1$ points of $L^* \setminus B^*$. Then there exists unique $\alpha_1, \alpha_2, \dots, \alpha_{q-1} \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $x_i = \langle \alpha_i \bar{e}_1 + \bar{e}_2 \rangle$ for every $i \in \{1, 2, \dots, q-1\}$. We now determine necessary and sufficient conditions that must be satisfied by $\alpha_1, \alpha_2, \dots, \alpha_{q-1}$ such that every Baer subline of $L^*$ meeting $B^*$ in a singleton contains at most one point of $X'$. The following observation will be useful to that end.

**Lemma 3.4** *For every $x \in B^*$ and every $y \in L^* \setminus B^*$, there exists a unique Baer subline of $L^*$ through $y$ intersecting $B^*$ in the singleton $\{x\}$.*

**Proof.** Since any three distinct points of $L^*$ are contained in a unique Baer subline, the number of Baer sublines containing $\{x, y\}$ is equal to $\frac{|L^* \setminus \{x,y\}|}{q-1} = \frac{q^2-1}{q-1} = q+1$, and any of these Baer sublines intersects $B^*$ in either 1 or 2 points. In fact, the number of these Baer sublines intersecting $B^*$ in two points is equal to $|B^* \setminus \{x\}| = q$, showing that there exists a unique such Baer subline intersecting $B^*$ in the singleton $\{x\}$.

Another proof goes as follows. Let $\kappa$ be the Klein correspondence from the set of lines of $\mathrm{PG}(3, q)$ to the points of the hyperbolic quadric $Q^+(5, q)$ of $\mathrm{PG}(5, q)$. The regular spread $S$ is then mapped by $\kappa$ to an elliptic quadric $Q^-(3, q) \subseteq Q^+(5, q)$ and the reguli contained in $S$ are mapped to conics contained in $Q^-(3, q)$, see e.g. [12, §15.4 and Lemma 17.1.2]. Let $C^*$ denote the conic corresponding to $B^*$, denote by $\tilde{x} \in C^*$ the point of $\mathrm{PG}(5, q)$ corresponding to the line $L_x$ and by $\tilde{y} \in Q^-(3, q) \setminus C^*$ the point of $\mathrm{PG}(5, q)$ corresponding to the line $L_y$. The Baer sublines through $y$ meeting $B^*$ in the singleton $\{x\}$ correspond (via their associated reguli) to conics in $Q^-(3, q)$ through $\tilde{y}$ meeting $C^*$ in the singleton $\{\tilde{x}\}$. There is a unique conic like that. Its carrying plane is $\langle \tilde{y}, \tilde{L} \rangle$, where $\tilde{L}$ is the line of the plane $\langle C^* \rangle$ that is tangent to $C^*$ at the point $\tilde{x}$. ∎

Now, let $i, j \in \{1, 2, \dots, q-1\}$ with $i \neq j$, and let $p \in B^*$. We determine necessary and sufficient conditions to be satisfied by $\alpha_i$ and $\alpha_j$ in order that the unique Baer subline $B_p$ through $x_i$ intersecting $B^*$ in $\{p\}$ would not contain $x_j$.

Consider first the case that $p = \langle \bar{e}_1 \rangle$. Then $B_p$ contains the point $\langle \bar{e}_1 \rangle$ as well as all points of the form $\langle (\alpha_i + k)\bar{e}_1 + \bar{e}_2 \rangle$, where $k \in \mathbb{F}_q$. So, a necessary and sufficient condition is that $\alpha_i - \alpha_j \notin \mathbb{F}_q$.

Consider next the case where $p = \langle \bar{e}_2 - l\bar{e}_1 \rangle$ for some $l \in \mathbb{F}_q$. We have $x_i = \left\langle \frac{\bar{e}_2 - l\bar{e}_1}{\alpha_i + l} + \bar{e}_1 \right\rangle$ and $x_j = \left\langle \frac{\bar{e}_2 - l\bar{e}_1}{\alpha_j + l} + \bar{e}_1 \right\rangle$. The unique Baer subline through $x_i$ intersecting $B^*$ in $p = \langle \bar{e}_2 - l\bar{e}_1 \rangle$ consists of the point $p$ together with all points of the form $\left\langle \left(k + \frac{1}{\alpha_i + l}\right)(\bar{e}_2 - l\bar{e}_1) + \bar{e}_1 \right\rangle$, where $k \in \mathbb{F}_q$. So, a necessary and sufficient condition is that $\frac{1}{\alpha_i + l} - \frac{1}{\alpha_j + l} \notin \mathbb{F}_q$.

So, we can conclude the following:

10

**Proposition 3.5** *Suppose* $A = \{\alpha_1, \alpha_2, \ldots, \alpha_{q-1}\}$ *is a set of* $q-1$ *elements of* $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, *and put* $X' = \{\langle \alpha_i \bar{e}_1 + \bar{e}_2 \rangle \mid i \in \{1, 2, \ldots, q-1\}\}$. *Then every Baer subline of* $L^*$ *meeting* $B^*$ *in a singleton contains a unique point of* $X'$ *if and only if the following properties are satisfied:*

(a) $\alpha_i - \alpha_j \notin \mathbb{F}_q$ *for all* $i, j \in \{1, 2, \ldots, q-1\}$ *with* $i \neq j$;

(b) $\frac{1}{\alpha_i + l} - \frac{1}{\alpha_j + l} \notin \mathbb{F}_q$ *for all* $l \in \mathbb{F}_q$ *and all* $i, j \in \{1, 2, \ldots, q-1\}$ *with* $i \neq j$.

We call a subset $A = \{\alpha_1, \alpha_2, \ldots, \alpha_{q-1}\}$ of size $q-1$ of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfying the properties (a) and (b) of Proposition 3.5 a *subset of blocking type* of $\mathbb{F}_{q^2}$. By Propositions 3.3 and 3.5, we then have

**Proposition 3.6** *The set* $\Omega$ *is a* $\mathcal{T}_1$-*blocking set if and only if the set* $\{\alpha_1, \alpha_2, \ldots, \alpha_{q-1}\}$ *is a subset of blocking type of* $\mathbb{F}_{q^2}$.

A $\mathcal{T}_1$-blocking set of size $q^2 - 1$ that is obtained from a subset of blocking type of $\mathbb{F}_{q^2}$ has the property that it contains at least $q - 1$ external lines. In our computer classification of all $\mathcal{T}_1$-blocking sets of size $q^2 - 1$ with $q \leq 13$, there are three blocking sets that have this property, namely $B_1$, $B_2$ and $B_8$ (see the table in Section 1). For each $q \in \{3, 5, 7\}$, we now show that there exist subsets of blocking type of $\mathbb{F}_{q^2}$. This then shows that the blocking sets $B_1$, $B_2$ and $B_8$ belong to the family of blocking sets under consideration in this section.

**Lemma 3.7** *Let* $a, b, c, d \in \mathbb{F}_q$ *with* $ad - bc \neq 0$ *and let* $\tau$ *be an automorphism of* $\mathbb{F}_{q^2}$. *Then* $\phi : \mathbb{F}_{q^2} \setminus \mathbb{F}_q \to \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *defined by* $x \mapsto \frac{ax^\tau + b}{cx^\tau + d}$ *is a bijection which maps every subset of blocking type of* $\mathbb{F}_{q^2}$ *to a subset of blocking type of* $\mathbb{F}_{q^2}$.

**Proof.** Let $A_1$ be a subset of blocking type of $\mathbb{F}_{q^2}$ and let $X_1$ denote the corresponding set of points of $L^* \setminus B^*$ (see Proposition 3.5). Let $\theta$ be the automorphism of $L^*$ determined by $\langle u\bar{e}_1 + v\bar{e}_2 \rangle \mapsto \langle (au^\tau + bv^\tau)\bar{e}_1 + (cu^\tau + dv^\tau)\bar{e}_2 \rangle$, and put $X_2 = X_1^\theta$. Note that $(B^*)^\theta = B^*$. Since every Baer subline meeting $B^*$ in a singleton contains a unique point of $X_1$, the same property holds for $X_2$. So, the subset $A_2$ of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ corresponding to $X_2$ (in the sense of Proposition 3.5) is a subset of blocking type of $\mathbb{F}_{q^2}$. Obviously, $A_2 = A_1^\phi$. ∎

Let $A_1$ and $A_2$ be two subsets of blocking type of $\mathbb{F}_{q^2}$. Then $A_1$ and $A_2$ are called *equivalent* if there exist $a, b, c, d \in \mathbb{F}_q$ with $ad - bc \neq 0$ and an automorphism $\tau$ of $\mathbb{F}_{q^2}$ such that $A_2 = A_1^\phi$, were $\phi : \mathbb{F}_{q^2} \setminus \mathbb{F}_q \to \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ is the map defined by $x \mapsto \frac{ax^\tau + b}{cx^\tau + d}$.

In view of Proposition 3.6, the following proposition would also follow from the nonexistence of $\mathcal{T}_1$-blocking sets of size $q^2 - 1$ for even $q > 2$. However, we want to add a proof since it is short and independent of the results on maximal partial ovoids of $W(q)$ obtained in [5].

**Proposition 3.8** *If* $q > 2$ *is even, then no subsets of blocking type of* $\mathbb{F}_{q^2}$ *do exist.*

**Proof.** By Proposition 3.5, it suffices to prove that there does not exist a set $X$ of $q - 1$ points in $L^* \setminus B^*$ such that every Baer subline intersecting $B^*$ in a singleton contains a unique point of $X$. Suppose to the contrary that $X$ is such a set. Since $q > 2$, we can take two distinct points $x_1, x_2 \in X$. For every point $y \in B^*$, the unique Baer subline of $L^*$ containing $x_1$, $x_2$ and $y$ cannot intersect $B^*$ in 1 or more than 2 points and so must intersect in precisely 2 points. So, the Baer sublines containing $x_1, x_2$ determine a partition of $B^*$ in pairs, proving that $q + 1$ is even, that is, $q$ is odd. ∎

**Proposition 3.9** *Up to equivalence, $\mathbb{F}_4$ has a unique subset of blocking type.*

**Proof.** Suppose $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2$ is a root of $x^2 + x + 1$. Then both $\{\alpha\}$ and $\{\alpha + 1\}$ are subsets of blocking type. The map $\phi : x \mapsto x + 1$ shows that they are equivalent. ∎

**Proposition 3.10** *Up to equivalence, $\mathbb{F}_9$ has a unique subset of blocking type.*

**Proof.** Suppose $\beta \in \mathbb{F}_9 \setminus \mathbb{F}_3$ is a root of $x^2 + 1$. Suppose $A$ is a subset of blocking type of $\mathbb{F}_9$. Then property (a) of Proposition 3.5 implies that $A$ has the form $\{\beta + \epsilon_1, -\beta + \epsilon_2\}$, where $\epsilon_1, \epsilon_2 \in \mathbb{F}_3$. By considering the map $\phi : x \mapsto x - \epsilon_1$, we may suppose that $\epsilon_1 = 0$ and $\epsilon := \epsilon_2 \in \mathbb{F}_3$. Since $\frac{1}{\beta} - \frac{1}{-\beta+1} = -\beta - (-\beta - 1) = 1 \in \mathbb{F}_3$ and $\frac{1}{\beta} - \frac{1}{-\beta-1} = -\beta - (-\beta+1) = -1 \in \mathbb{F}_3$, we must have $\epsilon = 0$ by property (b) of Proposition 3.5. Then the facts that

- $\frac{1}{\beta} - \frac{1}{-\beta} = (-\beta) - \beta = \beta \notin \mathbb{F}_3$,
- $\frac{1}{\beta+1} - \frac{1}{-\beta+1} = (\beta - 1) - (-\beta - 1) = -\beta \notin \mathbb{F}_3$,
- $\frac{1}{\beta-1} - \frac{1}{-\beta-1} = (\beta + 1) - (-\beta + 1) = -\beta \notin \mathbb{F}_3$,

imply that $\{\beta, -\beta\}$ is indeed a subset of blocking type of $\mathbb{F}_9$. ∎

We have verified the following with GAP and Sage, see [9].

**Proposition 3.11**
- *Up to equivalence, $\mathbb{F}_{25}$ has a unique subset of blocking type. If $\beta \in \mathbb{F}_{25} \setminus \mathbb{F}_5$ is a root of $x^2 - x + 2$, then $\{\beta, \beta^8, \beta^9, \beta^{14}\}$ is a subset of blocking type.*

- *Up to equivalence, $\mathbb{F}_{49}$ has a unique subset of blocking type. If $\beta \in \mathbb{F}_{49} \setminus \mathbb{F}_7$ is a root of $x^2 - x + 3$, then $\{\beta, \beta^4, \beta^7, \beta^{19}, \beta^{28}, \beta^{37}\}$ is a subset of blocking type.*

- *Suppose $q$ is an odd prime power for which $9 \le q \le 49$. Then $\mathbb{F}_{q^2}$ has no subsets of blocking type.*

The following lemma might be well known, but we found no suitable reference. Therefore a proof has been added.

**Lemma 3.12** (1) *For every automorphism $\theta$ of the projective line $L^*$, there exists an automorphism $\theta'$ of $\mathrm{PG}(3, q)$ stabilizing the spread $S$ such that $L_x^{\theta'} = L_{x^\theta}$ for every point $x$ of $L^*$.*

(2) *Suppose $\theta'$ is an automorphism of $\mathrm{PG}(3, q)$ stabilizing the spread $S$. Then there exists an automorphism $\theta$ of $L^*$ such that $(L_x)^{\theta'} = L_{x^\theta}$ for every point $x$ of $L^*$.*

12

**Proof.** (1) Let $W$ denote the 2-dimensional subspace of $\widetilde{V}$ such that $L^* = \mathrm{PG}(W)$. The $q^4$ vectors of $V$ are precisely the $q^4$ vectors of the form $\bar{w} + \bar{w}^q$, where $\bar{w} \in W$. Let $\phi$ be the semi-linear map of $W$ that induces the automorphism $\theta$ of $\mathrm{PG}(W) = L^*$. Then the map $V \to V : \bar{w} + \bar{w}^q \mapsto \bar{w}^\phi + (\bar{w}^\phi)^q$ is a semi-linear map inducing an automorphism $\theta'$ of $\mathrm{PG}(3, q)$. The automorphism $\theta'$ stabilizes the spread $S$ and satisfies $L_x^{\theta'} = L_{x^\theta}$ for every point $x$ of $L^*$.

(2) Suppose that $\theta'$ is an automorphism of $\mathrm{PG}(3, q)$ stabilizing the spread $S$. The automorphism $\theta'$ is induced by an automorphism $\overline{\theta'}$ of $\mathrm{PG}(3, q^2)$. Every line $L \in S$ is contained in a unique line $\overline{L}$ of $\mathrm{PG}(3, q^2)$, and we define $\overline{S} := \{\overline{L} \mid L \in S\}$. It is known, see e.g. Theorem 3.9 of Beutelspacher and Ueberberg [1], that there are two lines in $\mathrm{PG}(3, q^2)$ meeting every line of $\overline{S}$. These are the lines $L^*$ and $(L^*)^q$. As $\theta'$ stabilizes the spread $S$, we must have $(L^*)^{\overline{\theta'}} \in \{L^*, (L^*)^q\}$. If $\theta^*$ is the automorphism of $\mathrm{PG}(3, q^2)$ induced by the map $\bar{v} \mapsto \bar{v}^q$, then both $\overline{\theta'}$ and $\overline{\theta'} \circ \theta^*$ induce $\theta'$. So, without loss of generality, we may suppose that $(L^*)^{\overline{\theta'}} = L^*$. Then $\overline{\theta'}$ induces an automorphism $\theta$ of $L^*$. Obviously, $L_x^{\theta'} = L_{x^\theta}$ for every point $x$ of $L^*$. ∎

**Proposition 3.13** *Suppose $A_1$ and $A_2$ are two subsets of blocking type of $\mathbb{F}_{q^2}$. Let $X_i'$, $i \in \{1, 2\}$, denote the set of points of $L^*$ corresponding to $A_i$ (as in Proposition 3.5). If $A_1$ and $A_2$ are equivalent, then there exists an automorphism of $\mathrm{PG}(3, q)$ stabilising $Q^+(3, q)$ and mapping $\Omega_1 = \bigcup_{x \in X_1'} L_x$ to $\Omega_2 = \bigcup_{x \in X_2'} L_x$.*

**Proof.** Since $A_1$ and $A_2$ are equivalent, there exist $a, b, c, d \in \mathbb{F}_q$ with $ad - bc \neq 0$ and an automorphism $\tau$ of $\mathbb{F}_{q^2}$ such that $A_2 = A_1^\phi$, where $\phi$ is the permutation of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ determined by $x \mapsto \frac{ax^\tau + b}{cx^\tau + d}$. Let $\theta$ be the automorphism of $L^*$ determined by the map $\langle u\bar{e}_1 + v\bar{e}_2 \rangle \mapsto \langle (au^\tau + bv^\tau)\bar{e}_1 + (cu^\tau + dv^\tau)\bar{e}_2 \rangle$. Then $(X_1')^\theta = X_2'$ and $(B^*)^\theta = B^*$. If $\theta'$ is the automorphism of $\mathrm{PG}(3, q)$ as in Lemma 3.12(1), then $\Omega_1^{\theta'} = \Omega_2$ and $\mathcal{R}_{B^*}^{\theta'} = \mathcal{R}_{B^*}$. The latter implies that $\theta'$ stabilizes the hyperbolic quadric $Q^+(3, q)$ of $\mathrm{PG}(3, q)$. ∎

Our intention is now to prove the converse of Proposition 3.13. To that end the following lemma will be useful.

**Lemma 3.14** *Suppose $S' \subseteq S$ is a set of $q - 1$ lines disjoint from $Q^+(3, q)$ such that $\Omega = \bigcup_{L \in S'} L$ is a $\mathcal{T}_1$-blocking set of size $q^2 - 1$. If $q > 5$, then $S$ is the unique regular spread containing the lines of $S'$.*

**Proof.** By Propositions 3.6 and 3.8, we know that $q \geq 7$ is odd. Suppose by way of contradiction that $S$ is not the unique regular spread containing the lines of $S'$. Then $S'$ is contained[3] in a regulus $\mathcal{R} \subset S$. We denote by $Q'$ the unique hyperbolic quadric containing the lines of $\mathcal{R}$.

The quadrics $Q'$ and $Q^+(3, q)$ have at most $2(q + 1)$ common points (the union of 0, 1 or 2 lines of $S$). Let $x \in Q^+(3, q) \setminus Q'$ and denote by $\pi$ the plane of $\mathrm{PG}(3, q)$ that is tangent to $Q^+(3, q)$ in the point $x$. Let $L_1 \subseteq S$ and $L_2$ be the two lines of $Q^+(3, q)$

---

[3]This follows for instance from the Klein correspondence which maps reguli to conics and regular spreads to elliptic quadrics.

through $x$. As $x \notin Q'$, the line $L_1$ is not contained in $\mathcal{R}$. As any two lines of $\pi$ meet, $L_1$ is the unique line of $S$ in $\pi$. In particular, no line of $\mathcal{R}$ is contained in $\pi$. The plane $\pi$ can therefore not be tangent to the quadric $Q'$.

The intersection $\pi \cap Q'$ is thus a conic of $\pi$ containing $q + 1$ points. The set $\Omega \cap \pi$ is a set of $q - 1$ points. Since $\Omega$ is a $\mathcal{T}_1$-blocking set of size $q^2 - 1$, each line of $\pi$ through $x$ distinct from $L_1$ and $L_2$ contains a unique point of $\Omega \cap \pi$. So there are at least $q - 3 > 2$ tangent lines to $Q' \cap \pi$ among the $q - 1$ lines of $\pi$ through $x$ distinct from $L_1$ and $L_2$. This is impossible. Since $q$ is odd, there are at most 2 such tangent lines through $x$. ■

We now prove the converse of Proposition 3.13.

**Proposition 3.15** *Suppose $A_1$ and $A_2$ are two subsets of blocking type of $\mathbb{F}_{q^2}$. Let $X'_i$, $i \in \{1, 2\}$, denote the set of points of $L^*$ corresponding to $A_i$ (as in Proposition 3.5). If there exists an automorphism of $\mathrm{PG}(3, q)$ stabilising $Q^+(3, q)$ and mapping $\Omega_1 = \bigcup_{x \in X'_1} L_x$ to $\Omega_2 = \bigcup_{x \in X'_2} L_x$, then $A_1$ and $A_2$ are equivalent.*

**Proof.** By Propositions 3.8, 3.9, 3.10 and 3.11, we may assume $q > 5$. Let $\theta'$ denote the automorphism of $\mathrm{PG}(3, q)$ mentioned in the statement of the proposition. For every $i \in \{1, 2\}$, $S'_i := \{L_x \mid x \in X'_i\}$ is the set of lines contained in $\Omega_i$. As $\Omega_1^{\theta'} = \Omega_2$, we have $S_1^{\theta'} = S_2$. By Lemma 3.14, we then know that $\theta'$ stabilizes the spread $S$. By Lemma 3.12(2) and its proof, we know that $\theta'$ is induced by an automorphism $\overline{\theta'}$ of $\mathrm{PG}(3, q^2)$ such that $(L^*)^{\overline{\theta'}} = L^*$. Let $\theta$ be the restriction of $\overline{\theta'}$ to $L^*$. Since $\theta'$ stabilizes $Q^+(3, q)$, we have $(B^*)^\theta = B^*$. Since $\Omega_1^\theta = \Omega_2$, we have $(X'_1)^\theta = X'_2$. If the automorphism $\theta$ of $L^*$ is described by $\langle u\bar{e}_1 + v\bar{e}_2 \rangle \mapsto \langle (au^\tau + bv^\tau)\bar{e}_1 + (cu^\tau + dv^\tau)\bar{e}_2 \rangle$, where $\tau$ is an automorphism of $\mathbb{F}_{q^2}$ and $a, b, c, d \in \mathbb{F}_q$ such that $ad - bc \neq 0$, then $A_2 = A_1^\phi$ where $\phi$ is the permutation $x \mapsto \frac{ax^\tau + b}{cx^\tau + d}$ of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. So, $A_1$ and $A_2$ are equivalent. ■

By Propositions 3.13 and 3.15, the classification of the isomorphism classes of $\mathcal{T}_1$-blocking sets arising from subsets of blocking type of $\mathbb{F}_{q^2}$ is thus equivalent with the classification, up to equivalence, of these subsets of blocking type.

## 4 A second family of $\mathcal{T}_1$-blocking sets

Suppose that $L_1$ and $L_2$ are two disjoint lines of $Q^+(3, q)$ and let $\mathcal{L}$ denote a set of $q + 1$ secant lines meeting $L_1$ and $L_2$. Put $X := \left( \bigcup_{L \in \mathcal{L}} L \right) \setminus (L_1 \cup L_2)$.

**Lemma 4.1** *We have $|X| = q^2 - 1$.*

**Proof.** For every point $x \in \mathrm{PG}(3, q) \setminus Q^+(3, q)$, there is a unique (secant) line through $x$ meeting both $L_1$ and $L_2$. It follows that any two distinct lines of $\mathcal{L}$ cannot meet at a point of $\mathrm{PG}(3, q) \setminus Q^+(3, q)$. As $|\mathcal{L}| = q + 1$, we have $|X| = (q + 1)(q - 1) = q^2 - 1$. ■

We now investigate when $X$ is a $\mathcal{T}_1$-blocking set of size $q^2 - 1$.

**Lemma 4.2** *If $X$ is a $\mathcal{T}_1$-blocking set of size $q^2 - 1$, then any two lines of $\mathcal{L}$ are disjoint.*

**Proof.** Suppose $K_1$ and $K_2$ are two distinct lines of $\mathcal{L}$ sharing a common point $x$, necessarily contained in $L_1 \cup L_2$. Without loss of generality, we may suppose that $x \in L_1$. The plane $\langle x, L_2 \rangle$ is then a tangent plane. If $y \in L_2$ is the tangency point of this plane, then any outer tangent through $y$ contained in $\langle x, L_2 \rangle$ meets $K_1$ and $K_2$ (and hence $X$) in two points, in contradiction with Lemma 1.1. ∎

We now show that with each $\mathcal{T}_1$-blocking set $X$ of size $q^2 - 1$ that is of the above form, there is associated a permutation of $\mathbb{F}_q^*$ satisfying the properties (P1), (P2), (P3), (P4) of Section 1.3, and conversely, that with each such permutation there is an associated $\mathcal{T}_1$-blocking set of that size.

We take a reference system $\{\bar{e}_1, \bar{e}_2, \bar{e}_3, \bar{e}_4\}$ for $\mathrm{PG}(3, q)$ such that $Q^+(3, q)$ has equation $X_1 X_4 = X_2 X_3$, $L_1 = \mathrm{PG}(\langle \bar{e}_1, \bar{e}_2 \rangle)$ and $L_2 = \mathrm{PG}(\langle \bar{e}_3, \bar{e}_4 \rangle)$.

Now, take two distinct lines $P$ and $R$ of $\mathcal{L}$, and for every $i \in \{1, 2\}$, put $P \cap L_i = \{p_i\}$ and $R \cap L_i = \{r_i\}$. By Lemma 4.2, we may suppose that $p_1 \neq r_1$ and $p_2 \neq r_2$. Put

$$p_1 = (a, b, 0, 0), \quad p_2 = (0, 0, c, d), \quad r_1 = (\alpha, \beta, 0, 0), \quad r_2 = (0, 0, \gamma, \delta),$$

where $a, b, c, d, \alpha, \beta, \gamma, \delta \in \mathbb{F}_q$. The fact that the lines $P = p_1 p_2$ and $R = r_1 r_2$ are not contained in $Q^+(3, q)$ implies that $ad - bc \neq 0$ and $\alpha\delta - \beta\gamma \neq 0$.

Now, let $p$ be an arbitrary point of $P \setminus \{p_1, p_2\}$ and let $r$ be an arbitrary point of $R \setminus \{r_1, r_2\}$. Then

$$p = (a, b, cs, ds), \quad r = (\alpha, \beta, \gamma t, \delta t),$$

for certain $s, t \in \mathbb{F}_q^*$. An arbitrary point of $pr \setminus \{r\}$ has the form

$$(a + \alpha x, b + \beta x, cs + \gamma t x, ds + \delta t x),$$

with $x \in \mathbb{F}_q$. The intersection of $pr \setminus \{r\}$ with $Q^+(3, q)$ is determined by the equation

$$(ad - bc)s + \Big( (a\delta - b\gamma)t + (\alpha d - \beta c)s \Big)x + (\alpha\delta - \beta\gamma)tx^2 = 0.$$

By Lemma 1.2, $X$ will be a $\mathcal{T}_1$-blocking set if and only if $pr$ is not a tangent line for all possibilities for $P, R \in \mathcal{L}$ with $P \neq R$, $p \in P \setminus \{p_1, p_2\}$ and $r \in R \setminus \{r_1, r_2\}$. Now, the line $pr$ is not a tangent line if and only if

$$\Big( (a\delta - b\gamma)t + (\alpha d - \beta c)s \Big)^2 - 4(ad - bc)(\alpha\delta - \beta\gamma)st \neq 0,$$

that is,

$$(a\delta - b\gamma)^2 t^2 + (\alpha d - \beta c)^2 s^2 + 2(a\delta - b\gamma)(\alpha d - \beta c)st - 4(ad - bc)(\alpha\delta - \beta\gamma)st \neq 0. \quad (*)$$

The fact that $(*)$ holds for all $s, t \in \mathbb{F}_q^*$ implies that $a\delta - b\gamma = 0$ if and only if $\alpha d - \beta c = 0$, or equivalently, $p_2 r_1$ is a line of $Q^+(3, q)$ if and only if $p_1 r_2$ is a line of $Q^+(3, q)$. So, we

may suppose that we have chosen the reference system in such a way that $\mathrm{PG}(\langle \bar{e}_1, \bar{e}_4 \rangle)$ and $\mathrm{PG}(\langle \bar{e}_2, \bar{e}_3 \rangle)$ are lines of $\mathcal{L}$.

If $a\delta - b\gamma = \alpha d - \beta c = 0$, then $(*)$ holds for all $s, t \in \mathbb{F}_q^*$. Suppose therefore that $a\delta - b\gamma \neq 0 \neq \alpha d - \beta c$. The fact that $(*)$ holds for all $s, t \in \mathbb{F}_q^*$ is equivalent with the fact that

$$\Delta := \Big( (a\delta - b\gamma)(\alpha d - \beta c) - 2(ad - bc)(\alpha\delta - \beta\gamma) \Big)^2 - (a\delta - b\gamma)^2 (\alpha d - \beta c)^2$$

is a nonsquare. One computes that

$$
\begin{aligned}
\Delta &= 4(ad - bc)(\alpha\delta - \beta\gamma)\Big( (ad - bc)(\alpha\delta - \beta\gamma) - (a\delta - b\gamma)(\alpha d - \beta c) \Big) \\
&= 4(ad - bc)(\alpha\delta - \beta\gamma)(a\beta - b\alpha)(c\delta - d\gamma).
\end{aligned}
$$

The affine coordinates of $p_1$, $p_2$, $r_1$ and $r_2$ are as follows:

$$x = \frac{b}{a} \in \mathbb{F}_q \cup \{\infty\}, \qquad x' = \frac{d}{c} \in \mathbb{F}_q \cup \{\infty\}, \qquad y = \frac{\beta}{\alpha} \in \mathbb{F}_q \cup \{\infty\}, \qquad y' = \frac{\delta}{\gamma} \in \mathbb{F}_q \cup \{\infty\}.$$

Since $p_1 \neq r_1$ and $p_2 \neq r_2$, we have $x \neq y$ and $x' \neq y'$. The facts that $ad - bc \neq 0$ and $\alpha\delta - \beta\gamma \neq 0$ imply that $x \neq x'$ and $y \neq y'$. The facts that $a\delta - b\gamma \neq 0 \neq \alpha d - \beta c$ imply that $x \neq y'$ and $y \neq x'$. So, $x$, $x'$, $y$ and $y'$ are mutually distinct. Since $\mathrm{PG}(\langle \bar{e}_1, \bar{e}_4 \rangle)$ and $\mathrm{PG}(\langle \bar{e}_2, \bar{e}_3 \rangle)$ are lines of $\mathcal{L}$, we have $0' = \infty$ and $\infty' = 0$.

If $a = 0$, then $x = \infty$, $x' = 0$ and $d = 0$. So, $y, y' \notin \{0, \infty\}$ and the fact that $\frac{\Delta}{4} = -bc(\alpha\delta - \beta\gamma)(-b\alpha)(c\delta)$ is a nonsquare implies that $(y' - y)y'$ is a nonsquare.

If $c = 0$, then $x' = \infty$, $x = 0$ and $b = 0$. So, $y, y' \notin \{0, \infty\}$ and the fact that $\frac{\Delta}{4} = ad(\alpha\delta - \beta\gamma)a\beta(-d\gamma)$ is a nonsquare implies that $(y - y')y$ is a nonsquare.

By supposing that one of $\alpha, \gamma$ is zero, we find by symmetry that $x, x' \notin \{0, \infty\}$ and that also $(x' - x)x'$ and $(x - x')x$ are nonsquares.

If $a, c, \alpha, \gamma$ are distinct from $0$, then $x, x', y, y' \notin \{0, \infty\}$ and the fact that $\Delta$ is a nonsquare implies that $(x' - x)(y' - y)(y - x)(y' - x')$ is a nonsquare.

As $0' = \infty$ and $\infty' = 0$, Lemma 4.2 implies that the map $x \mapsto x'$ defines a permutation $\sigma$ of the set $\mathbb{F}_q^*$. The fact that $a\delta - b\gamma = 0$ if and only if $\alpha d - \beta c = 0$ implies that $x = y' \Leftrightarrow y = x'$ for $x, y \in \mathbb{F}_q^*$, i.e. that $\sigma^2 = 1$. The fact that $x \neq x'$ implies that $\sigma$ has no fixed points.

Notice also that the set $\mathcal{L}$ of lines is completely determined by the map $\sigma : \mathbb{F}_q^* \to \mathbb{F}_q^*$. Summarizing, we thus have:

**Proposition 4.3** $X$ is a $\mathcal{T}_1$-blocking set of size $q^2 - 1$ if and only if the permutation $\sigma$ of $\mathbb{F}_q^*$ satisfies the following properties:

$(P1)$ $\sigma$ has no fixed points;

$(P2)$ $\sigma^2 = 1$;

$(P3)$ $(x - x^\sigma)x$ is a nonsquare for all $x \in \mathbb{F}_q^*$;

16

(P4) $(x^\sigma - x)(y^\sigma - y)(y - x)(y^\sigma - x^\sigma)$ *is a nonsquare for all* $x, y \in \mathbb{F}_q^*$ *with* $y \notin \{x, x^\sigma\}$.

Note that the property that $(x^\sigma - x)x^\sigma$ is a nonsquare for all $x \in \mathbb{F}_q^*$ is implied by properties (P2) and (P3). Indeed, it is obtained from (P3) be replacing $x$ by $x^\sigma$ and using the fact that $\sigma^2 = 1$. In fact, also Property (P1) is implied by (P3), but we have decided to keep it for clarity reasons. The facts that $(x - x^\sigma)x$ and $(x^\sigma - x)x^\sigma$ are nonsquares imply that $-xx^\sigma$ itself should be a square. So, we have:

**Proposition 4.4** *If a permutation* $\sigma$ *of* $\mathbb{F}_q^*$ *satisfies the properties* (P2) *and* (P3) *of Proposition 4.3, then* $(x^\sigma - x)x^\sigma$ *is a nonsquare and* $-xx^\sigma$ *is a square for every* $x \in \mathbb{F}_q^*$.

A $\mathcal{T}_1$-blocking set of size $q^2 - 1$ that is obtained from a permutation $\sigma$ of $\mathbb{F}_q^*$ that satisfies the properties (P1), (P2), (P3) and (P4) has the property that there are $q + 1$ secant lines meeting the blocking set in exactly $q - 1$ points. In our computer classification of all $\mathcal{T}_1$-blocking sets of size $q^2 - 1$ with $q \leq 13$, there are four blocking sets that have this property, namely $B_1$, $B_4$, $B_6$ and $B_9$ (see the table in Section 1). For each $q \in \{3, 5, 7, 11\}$, we now prove that there exists a permutation $\sigma$ satisfying (P1), (P2), (P3) and (P4). This then shows that the blocking sets $B_1$, $B_4$, $B_6$ and $B_9$ belong to the family of blocking sets under consideration in this section.

**Proposition 4.5** *Let* $\tau$ *be the permutation of* $\mathbb{F}_q^*$ *mapping* $x \in \mathbb{F}_q^*$ *to* $x^{-1}$. *If* $\sigma$ *is a permutation of* $\mathbb{F}_q^*$ *satisfying the properties* (P1), (P2), (P3) *and* (P4), *then* $\tau^{-1}\sigma\tau$ *also satisfies the same properties. Moreover, the associated* $\mathcal{T}_1$-*blocking sets of size* $q^2 - 1$ *are isomorphic.*

**Proof.** The verification that $\tau^{-1}\sigma\tau$ satisfies the properties (P1), (P2), (P3) and (P4) is straightforward, but also follows from the discussion below.

Let $V$ be the 4-dimensional vector space over $\mathbb{F}_q$ for which $\mathrm{PG}(3, q) = \mathrm{PG}(V)$. The linear map of $V$ mapping $(\bar{e}_1, \bar{e}_2, \bar{e}_3, \bar{e}_4)$ to $(\bar{e}_2, \bar{e}_1, \bar{e}_4, \bar{e}_3)$ defines an automorphism of $\mathrm{PG}(3, q)$ stabilizing $Q^+(3, q)$, $L_1$ and $L_2$. The set $\mathcal{L}$ is transformed into another set $\mathcal{L}'$ of $q + 1$ secant lines. The affine coordinates of the images of points of $L_1 \cup L_2$ are the multiplicative inverses of the original affine coordinates. The involution of $\mathbb{F}_q^*$ corresponding to $\mathcal{L}'$ must thus be the map $\tau^{-1}\sigma\tau$. ∎

**Proposition 4.6** *Let* $\sigma$ *be a permutation of* $\mathbb{F}_q^*$ *satisfying the properties* (P1), (P2), (P3) *and* (P4). *The following hold:*

- *For* $q = 3$, *there is only one possibility for* $\sigma$, *namely* $(1, 2)$.

- *For* $q = 5$, *there is only one possibility for* $\sigma$, *namely* $(1, 4)(2, 3)$.

- *For* $q = 7$, *there are two possibilities for* $\sigma$, *namely* $(1, 3)(2, 6)(4, 5)$ *and* $(1, 5)(4, 6)(2, 3)$. *They are conjugate under the permutation* $\tau$.

- *For* $q = 11$, *there are two possibilities for* $\sigma$, *namely* $(1, 2)(4, 8)(3, 6)(5, 10)(9, 7)$ *and* $(1, 6)(4, 2)(3, 7)(5, 8)(9, 10)$. *They are conjugate under the permutation* $\tau$.

17

**Proof.** We only work out the case $q = 11$. The other (easier) cases can be treated with a similar reasoning. If $q = 11$, then $-1$ is a nonsquare. Since $xx^\sigma$ and $(x - x^\sigma)x$ are nonsquares for all $x \in \mathbb{F}_{11}^*$, we have that $1^\sigma \in \{2, 6, 10\}$, $3^\sigma \in \{6, 7, 8\}$, $4^\sigma \in \{2, 7, 8\}$, $5^\sigma \in \{6, 8, 10\}$ and $9^\sigma \in \{2, 7, 10\}$. This leads to the following 13 possibilities for the involution $\sigma$:

$(1, 2)(4, 7)(9, 10)(3, 8)(5, 6)$; $(1, 2)(4, 7)(9, 10)(3, 6)(5, 8)$; $(1, 2)(4, 8)(3, 6)(5, 10)(9, 7)$;
$(1, 2)(4, 8)(3, 7)(5, 6)(9, 10)$; $(1, 6)(4, 2)(3, 7)(5, 8)(9, 10)$; $(1, 6)(4, 2)(3, 8)(5, 10)(9, 7)$;
$(1, 6)(9, 2)(5, 10)(3, 7)(4, 8)$; $(1, 6)(9, 2)(5, 10)(3, 8)(4, 7)$; $(1, 10)(4, 2)(9, 7)(3, 6)(5, 8)$;
$(1, 10)(4, 2)(9, 7)(3, 8)(5, 6)$; $(1, 10)(9, 2)(4, 7)(3, 6)(5, 8)$; $(1, 10)(9, 2)(4, 7)(3, 8)(5, 6)$;
$(1, 10)(9, 2)(4, 8)(5, 6)(3, 7)$.

Only the involutions $(1, 2)(4, 8)(3, 6)(5, 10)(9, 7)$ and $(1, 6)(4, 2)(3, 7)(5, 8)(9, 10)$ satisfy the required properties. ∎

We have verified the following with GAP and Sage, see [9].

**Proposition 4.7** *If $q \leq 25$ is an odd prime power, and $\sigma$ is a permutation of $\mathbb{F}_q^*$ satisfying the properties (P1), (P2), (P3) and (P4), then $q \in \{3, 5, 7, 11\}$.*

**Proposition 4.8** *Suppose $q \equiv 3 \pmod 4$. Let $\alpha, \beta \in \mathbb{F}_q^*$ and suppose $\sigma : \mathbb{F}_q^* \to \mathbb{F}_q^*$ is defined as follows: $x^\sigma = \alpha x$ if $x \in \mathbb{F}_q^*$ is a square and $x^\sigma = \beta x$ if $x \in \mathbb{F}_q^*$ is a nonsquare. Then $\sigma$ satisfies the properties (P1), (P2), (P3) and (P4) if and only if*

(i) $\beta = \alpha^{-1}$;

(ii) $\alpha$ *is a nonsquare;*

(iii) $\alpha - 1$ *is a square;*

(iv) *for every nonsquare $y \in \mathbb{F}_q^*$ distinct from $\alpha$, $(y - 1)(y - \alpha^2)$ is a nonsquare.*

**Proof.** As $q \equiv 3 \pmod 4$, we know that $-1$ is not a square. As $1^\sigma = \alpha$ and $-xx^\sigma$ is a square for all $x \in \mathbb{F}_q^*$, we see that $\alpha$ is a nonsquare. Property (P1) implies that $\alpha \neq 1 \neq \beta$. Property (P2) implies that $\beta = \alpha^{-1}$ (evaluate $\sigma^2$ at 1). Property (P3) applied to the case where $x$ is a square yields that $(1 - \alpha)x^2$ is a nonsquare, that is, $\alpha - 1$ is a square. Property (P3) applied to the case where $x$ is a nonsquare yields that $x^2(1 - \frac{1}{\alpha})$ is a nonsquare, which is certainly the case since $\alpha - 1$ is a square and $\alpha$ is a nonsquare. So, properties (P1), (P2) and (P3) hold if and only if $\beta = \alpha^{-1}$, $\alpha$ is a nonsquare and $\alpha - 1$ is a square.

We now determine when property (P4) holds, under the assumption that (i), (ii) and (iii) already hold.

If $x$ and $y$ are distinct nonzero squares, then $f(x, y) := (x^\sigma - x)(y^\sigma - y)(y - x)(y^\sigma - x^\sigma) = (\alpha - 1)^2 xy\alpha(y - x)^2$ is a nonsquare.

If $x$ and $y$ are distinct nonsquares, then $f(x, y) = (\frac{1}{\alpha} - 1)^2 xy\frac{1}{\alpha}(y - x)^2$ is a nonsquare.

As $f(x, y) = f(y, x)$, the only remaining case to examine is the case where $x$ is a square and $y$ is a nonsquare. In this case, $f(x, y) = (\alpha - 1)(\frac{1}{\alpha} - 1)xyx^2(\frac{y}{x} - 1)(\frac{y}{x} \cdot \frac{1}{\alpha} - \alpha) =$

18

$-\frac{1}{\alpha^2}(\alpha-1)^2 xyx^2(\frac{y}{x}-1)(\frac{y}{x}-\alpha^2)$. So, $f(x,y)$ is a nonsquare if and only if $(\frac{y}{x}-1)(\frac{y}{x}-\alpha^2)$ is a nonsquare. As $y \neq x^\sigma = \alpha x$, $\frac{y}{x}$ can reach all nonsquares distinct from $\alpha$. So, besides (i), (ii) and (iii), we should also require that (iv) holds. ∎

By Proposition 4.6, we know that if $q \in \{3,7,11\}$, then all known examples of permutations $\sigma$ satisfying the properties (P1), (P2), (P3) and (P4) are obtained as in Proposition 4.8, with $\alpha = 2$ if $q = 3$, $\alpha \in \{3,5\}$ if $q = 7$ and $\alpha \in \{2,6\}$ if $q = 11$. This led us to the question whether more examples of elements $\alpha \in \mathbb{F}_q^*$ with $q$ congruent to 3 modulo 4 exist that satisfy the conditions (ii), (iii) and (iv) of Proposition 4.8. This is however not the case as a combination of theoretical arguments and computer computations show. The following proposition was provided to us by one of the anonymous referees of this paper.

**Proposition 4.9** *If $q \geq 59$, then there are no $\alpha \in \mathbb{F}_q^*$ satisfying the conditions (ii), (iii) and (iv) of Proposition 4.8.*

**Proof.** For $e \in \mathbb{N} \setminus \{0,1\}$, denote by $C_0^{e,q}$ the group of nonzero $e$th powers of $\mathbb{F}_q$. Observe that $|C_0^{e,q}| = \frac{q-1}{e}$ if $q \equiv 1 \pmod{e}$. Denote by $\omega$ a primitive element of $\mathbb{F}_q$, and by $C_i^{e,q} := \omega^i C_0^{e,q}$, $i \in \{0,1,\ldots,e-1\}$, the $e$ cosets of $C_0^{e,q}$ in the multiplicative group of $\mathbb{F}_q$. We take the following result from [7, Theorem 2.2]:

Let $q \equiv 1 \pmod{e}$, let $B = \{b_0, b_1, \ldots, b_{m-1}\}$ be an arbitrary subset of size $m \geq 1$ of $\mathbb{F}_q$ and let $(\beta_0, \beta_1, \ldots, \beta_{m-1})$ be an arbitrary element of $\mathbb{Z}_e^m$. Set $Y = \{y \in \mathbb{F}_q \mid y - b_i \in C_{\beta_i}^{e,q}$ for every $i \in \{0,1,\ldots,m-1\}\}$. Then $|Y| > n$ for integers $n \geq 0$ if $q > Q(e,m,n) := \frac{1}{4}\left(U + \sqrt{U^2 + 4e^{m-1}(m+en)}\right)^2$, where $U = \sum_{h=1}^{m} \binom{m}{h}(e-1)^h(h-1)$.

Now, suppose $\alpha$ is a given nonsquare of $\mathbb{F}_q^*$ for which $\alpha - 1$ is a square. Put $e := 2$, $m := 3$, $n := 1$, and suppose $q > Q(2,3,1) = 58.117....$ By the above, there exists a $y \neq \alpha$ such that
$$y \in C_1^{2,q}, \quad y - 1 \in C_0^{2,q}, \quad y - \alpha^2 \in C_0^{2,q}.$$
Then $y \in \mathbb{F}_q^* \setminus \{\alpha\}$ is a nonsquare for which $(y-1)(y-\alpha^2)$ is a square. So, condition (iv) of Proposition 4.8 cannot be satisfied. ∎

We have verified the following by computer, see [9].

**Proposition 4.10** *If $q < 59$ is a prime power which is congruent to 3 modulo 4 and $\alpha \in \mathbb{F}_q^*$ satisfies the conditions (ii), (iii) and (iv) of Proposition 4.8, then $q \in \{3,7,11\}$. Moreover, $\alpha = 2$ if $q = 3$, $\alpha \in \{3,5\}$ if $q = 7$ and $\alpha \in \{2,6\}$ if $q = 11$.*

# 5 A third family of $\mathcal{T}_1$-blocking sets

Let $Q^+(3,q)$ with $q$ odd be a hyperbolic quadric in $\mathrm{PG}(3,q)$. Let $\mathcal{L}_1$ and $\mathcal{L}_2$ denote the two reguli of $\mathrm{PG}(3,q)$ defined by $Q^+(3,q)$. Let $\kappa$ be the Klein correspondence between the

set of lines of $\mathrm{PG}(3,q)$ and the Klein quadric $Q^+(5,q)$ of $\mathrm{PG}(5,q)$. Let $\zeta$ be the orthogonal polarity of $\mathrm{PG}(5,q)$ associated with $Q^+(5,q)$. For every $i \in \{1,2\}$, $\mathcal{C}_i := \kappa(\mathcal{L}_i)$ is then a nondegenerate conic of the plane $\pi_i := \langle \mathcal{C}_i \rangle$ of $\mathrm{PG}(5,q)$, see e.g. [12, Section 15.4]. The lines of $\mathcal{L}_2$ are precisely those lines that meet each line of $\mathcal{L}_1$, implying that $\pi_2 = \pi_1^\zeta$. Let $L_1$ and $L_2$ be two disjoint lines of $\mathrm{PG}(3,q)$ which themselves are also disjoint from $Q^+(3,q)$. Put $p_i := \kappa(L_i)$, $i \in \{1,2\}$. Then $p_1$ and $p_2$ do not belong to $\mathcal{C}_1 \cup \mathcal{C}_2$ (and hence also not to $\pi_1 \cup \pi_2$) and are not $Q^+(5,q)$-collinear. Suppose that the following conditions hold:

(a) $\Pi := \langle p_1, p_2, \pi_1 \rangle$ is a 3-dimensional subspace of $\mathrm{PG}(5,q)$ meeting $Q^+(5,q)$ in an elliptic quadric $Q^-(3,q)$;

(b) if $p_3$ is the unique point in $p_1 p_2 \cap \pi_1$, then $p_3$ is an internal point to the conic $\mathcal{C}_1$.

Note that the 3-dimensional space $(p_1 p_2)^\zeta$ intersects $Q^+(5,q)$ in a $(q+1) \times (q+1)$-grid $\mathcal{G}$.

Now, let $K_1, K_2, \ldots, K_{q+1}$ be a collection of $q+1$ mutually disjoint lines meeting $L_1$ and $L_2$, and put $k_i := \kappa(K_i)$, $i \in \{1, 2, \ldots, q+1\}$.

**Lemma 5.1** *The set $\{k_1, k_2, \ldots, k_{q+1}\}$ is an ovoid of $\mathcal{G}$. Conversely, every ovoid of $\mathcal{G}$ is the image under the Klein correspondence of a set of $q+1$ mutually disjoint lines meeting $L_1$ and $L_2$.*

**Proof.** Since $K_i$ with $i \in \{1, 2, \ldots, q+1\}$ meets $L_1$ and $L_2$, the point $k_i = \kappa(K_i)$ is $Q^+(5,q)$-collinear with both $p_1 = \kappa(L_1)$ and $p_2 = \kappa(L_2)$, that is, $k_i$ is a point of $\mathcal{G}$. Since no two lines of the collection $K_1, K_2, \ldots, K_{q+1}$ meet, no two points of the collection $k_1, k_2, \ldots, k_{q+1}$ are $Q^+(5,q)$-collinear, and so $\{k_1, k_2, \ldots, k_{q+1}\}$ is an ovoid of $\mathcal{G}$.

Conversely, if $O$ is an ovoid of $\mathcal{G}$, then $\kappa^{-1}(O)$ is a set of $q+1$ lines meeting $L_1$ and $L_2$ (as $O \subseteq (p_1 p_2)^\zeta$). As no two points of $O$ are $Q^+(5,q)$-collinear, these $q+1$ lines are mutually disjoint. ∎

Let $P$ denote the set of all points $p$ contained in a (unique) set $u_1 u_2 \setminus \{u_1, u_2\}$, where $u_1 \in \mathcal{C}_1$ and $u_2 \in \mathcal{C}_2$.

**Lemma 5.2** *The set $P$ is precisely the image under the Klein correspondence of the set of outer tangents.*

**Proof.** For every incident point-plane pair $(p, \pi)$ of $\mathrm{PG}(3,q)$, let $\mathcal{L}(p, \pi)$ denote the set of lines of $\pi$ through $p$. The images of these sets under the Klein correspondence are precisely the lines of $Q^+(5,q)$. The outer tangents are precisely the lines contained in a set $\mathcal{L}(p, \pi) \setminus \{M_1, M_2\}$, where $p = M_1 \cap M_2$ and $\pi = \langle M_1, M_2 \rangle$ for some $M_1 \in \mathcal{L}_1$ and $M_2 \in \mathcal{L}_2$. Using the Klein correspondence $\kappa$, we see that the image of the set of outer tangents under $\kappa$ coincides with the set $P$. ∎

**Lemma 5.3** *No point of $P$ can be $Q^+(5,q)$-collinear with both $p_1$ and $p_2$.*

**Proof.** Suppose $p \in P$ is $Q^+(5,q)$-collinear with both $p_1$ and $p_2$. Also assume that $p \in u_1u_2 \setminus \{u_1, u_2\}$, where $u_1 \in \mathcal{C}_1$ and $u_2 \in \mathcal{C}_2$. The planes $\langle p_1, p_2, u_1 \rangle$ and $\pi_1$ of the 3-space $\Pi$ meet in a line $U$. As $p_3 \in U$ is an internal point to $\mathcal{C}_1$, this line $U$ contains besides $u_1$ still one other point $u_1'$ of $\mathcal{C}_1$. The point $p$ is $Q^+(5,q)$-collinear with $p_1, p_2, u_1$ and hence with every point of the set $\langle p_1, p_2, u_1 \rangle \cap Q^+(5,q)$. In particular, $p$ is $Q^+(5,q)$-collinear with $u_1'$. Since also $u_2 \in \mathcal{C}_2$ is $Q^+(5,q)$-collinear with $u_1' \in \mathcal{C}_1$, we have that $u_1 \in pu_2$ is $Q^+(5,q)$-collinear with $u_1'$, a contradiction. ∎

**Proposition 5.4** *The set $(K_1 \cup K_2 \cup \cdots \cup K_{q+1}) \setminus (L_1 \cup L_2)$ is a $\mathcal{T}_1$-blocking set of size $q^2 - 1$ if and only if the following holds for every point $p \in P$:*

> *The number of points in the collection $k_1, k_2, \ldots, k_{q+1}$ that are $Q^+(5,q)$-collinear with $p$ is equal to 1 if $p$ is $Q^+(5,q)$-collinear with neither of $p_1, p_2$ and equal to 2 if $p$ is $Q^+(5,q)$-collinear with (precisely) one of $p_1, p_2$.*

**Proof.** By Lemmas 5.2 and 5.3, an outer tangent can never meet both $L_1$ and $L_2$. In particular, none of the lines $K_1, K_2, \ldots, K_{q+1}$ is an outer tangent. For the set $(K_1 \cup K_2 \cup \cdots \cup K_{q+1}) \setminus (L_1 \cup L_2)$ to be a $\mathcal{T}_1$-blocking set (of size $q^2 - 1$), the following should hold for an arbitrary outer tangent line $U$.

> The number of $i \in \{1, 2, \ldots, q+1\}$ such that $U$ and $K_i$ meet is equal to 1 if $U$ is disjoint from $L_1 \cup L_2$, and equal to 2 if $U$ meets (precisely) one of $L_1, L_2$.

Translating this condition via the Klein correspondence and taking into account Lemma 5.2, we see that $(K_1 \cup K_2 \cup \cdots \cup K_{q+1}) \setminus (L_1 \cup L_2)$ is a $\mathcal{T}_1$-blocking set if and only if the condition mentioned in the proposition is satisfied. ∎

A $\mathcal{T}_1$-blocking set of size $q^2 - 1$ that is obtained as described in Proposition 5.4 must have (at least) $q + 1$ external lines, each of which meets the blocking set in $q - 1$ points. In our computer classification of all $\mathcal{T}_1$-blocking sets of size $q^2 - 1$ with $q \leq 13$, there are only three blocking sets that have this property, namely $B_1$, $B_3$ and $B_5$ (see the table in Section 1). Using the criterion mentioned in Proposition 5.4, we have constructed (with the aid of a computer) a $\mathcal{T}_1$-blocking set for each $q \in \{3, 5, 7\}$. This then shows that the blocking sets $B_1$, $B_3$ and $B_5$ indeed belong to the family of $\mathcal{T}_1$-blocking sets given by Proposition 5.4. Moreover, they are the unique members of this family with $q$ respectively equal to 3, 5 and 7.

In order to use the criterion mentioned in Proposition 5.4, we shall introduce coordinates. We can choose a reference system in $PG(5,q)$ such that $p_1 = (1,0,0,0,0,0)$, $p_2 = (0,1,0,0,0,0)$ and the Klein quadric $Q^+(5,q)$ has equation $X_1X_2 + X_3X_4 + X_5X_6 = 0$. The grid $\mathcal{G}$ determined by the points of $(p_1p_2)^\varsigma \cap Q^+(5,q)$ is then described by the equations $X_1 = X_2 = 0$, $X_3X_4 + X_5X_6 = 0$. The points of $\mathcal{G}$ are

- $M(\alpha, \beta) := (0,0,1,-\alpha\beta,\alpha,\beta)$, $\alpha, \beta \in \mathbb{F}_q$;
- $M(\alpha, \infty) := (0,0,0,-\alpha,0,1)$, $\alpha \in \mathbb{F}_q$;
- $M(\infty, \beta) := (0,0,0,-\beta,1,0)$, $\beta \in \mathbb{F}_q$;
- $M(\infty, \infty) := (0,0,0,1,0,0)$.

The lines of $\mathcal{G}$ are

- $K_\infty := \{(0,0,0,1,0,0)\} \cup \{(0,0,0,-\beta,1,0) \mid \beta \in \mathbb{F}_q\}$;
- $K_\alpha := \{(0,0,0,-\alpha,0,1)\} \cup \{(0,0,1,-\alpha\beta,\alpha,\beta) \mid \beta \in \mathbb{F}_q\}$, $\alpha \in \mathbb{F}_q$;
- $L_\infty := \{(0,0,0,1,0,0)\} \cup \{(0,0,0,-\alpha,0,1) \mid \alpha \in \mathbb{F}_q\}$;
- $L_\beta := \{(0,0,0,-\beta,1,0)\} \cup \{(0,0,1,-\alpha\beta,\alpha,\beta) \mid \alpha \in \mathbb{F}_q\}$, $\beta \in \mathbb{F}_q$.

Then $K_x \cap L_y = M(x,y)$ for all $x, y \in \overline{\mathbb{F}_q} := \mathbb{F}_q \cup \{\infty\}$. There is a one-to-one correspondence between the permutations $\tau$ of $\overline{\mathbb{F}_q}$ and the ovoids $O_\tau$ of $\mathcal{G}$, where

$$O_\tau := \{M(x, x^\tau) \mid x \in \overline{\mathbb{F}_q}\}.$$

We suppose that $\Pi$ is the subspace of co-dimension 2 of $\mathrm{PG}(5,q)$ having equations $X_4 = X_3$ and $X_6 = -\alpha X_5$, with $\alpha$ a given nonsquare. Then $\Pi \cap Q^+(5,q)$ is an elliptic quadric $Q^-(3,q)$ with equations

$$X_4 = X_3, \quad X_6 = -\alpha X_5, \quad X_1 X_2 + X_3^2 - \alpha X_5^2 = 0.$$

Note that $p_1, p_2 \in Q^-(3,q)$.

Now, consider a plane $\pi_1 \subseteq \Pi$ with equation $X_1 + c_2 X_2 + c_3 X_3 + c_5 X_5 = 0$, where $c_2 \neq 0$. Then $p_1$ and $p_2$ do not belong to $\pi_1$. Put $\mathcal{C}_1 := \pi_1 \cap Q^+(5,q)$.

**Lemma 5.5** $\mathcal{C}_1$ *is a nondegenerate conic of* $\pi_1$ *if and only if* $\alpha(4c_2 + c_3^2) \neq c_5^2$.

**Proof.** Replacing $X_1$ by $-c_2 X_2 - c_3 X_3 - c_5 X_5$ in the quadratic equation $X_1 X_2 + X_3^2 - \alpha X_5^2 = 0$, we find $-c_2 X_2^2 - c_3 X_2 X_3 - c_5 X_2 X_5 + X_3^2 - \alpha X_5^2 = 0$. This determines a nondegenerate conic if and only if

$$\begin{vmatrix} -c_2 & -\frac{c_3}{2} & -\frac{c_5}{2} \\ -\frac{c_3}{2} & 1 & 0 \\ -\frac{c_5}{2} & 0 & -\alpha \end{vmatrix} \neq 0,$$

that is, $\alpha(c_2 + \frac{c_3^2}{4}) - \frac{c_5^2}{4} \neq 0$. ∎

Now, suppose $\mathcal{C}_1$ is a nondegenerate conic of $\pi_1$. Then $\mathcal{C}_2 := \mathcal{C}_1^\zeta \cap Q^+(5,q)$ is a nondegenerate conic of $\pi_2 := \pi_1^\zeta$ as well. Put $p_3 := p_1 p_2 \cap \pi_1 = (-c_2, 1, 0, 0, 0, 0)$.

**Lemma 5.6** *The point* $p_3 \in \pi_1$ *is an internal point to the conic* $\mathcal{C}_1$ *if and only if* $c_2(\alpha c_3^2 - c_5^2 + 4\alpha c_2)$ *is a nonsquare in* $\mathbb{F}_q$.

**Proof.** In order for the point $p_3$ to be internal, we need to show that the line $p_3^\zeta \cap \pi_1$ has no points in common with $\mathcal{C}_1 \subset \pi_1$. The hyperplane $p_3^\zeta$ has equation $X_1 = c_2 X_2$. So, if $p = (X_1, X_2, X_3, X_4, X_5, X_6)$ belongs to $\mathcal{C}_1 \cap p_3^\zeta$, then the conditions $X_1 = c_2 X_2$ and $X_1 + c_2 X_2 + c_3 X_3 + c_5 X_5 = 0$ imply that

$$X_1 = -\frac{c_3 X_3 + c_5 X_5}{2}, \qquad X_2 = -\frac{c_3 X_3 + c_5 X_5}{2c_2},$$

22

and the condition $X_1X_2 + X_3^2 - \alpha X_5^2 = 0$ implies that

$$\frac{(c_3X_3 + c_5X_5)^2}{4c_2} + X_3^2 - \alpha X_5^2 = 0,$$

that is,

$$(c_3^2 + 4c_2)X_3^2 + (c_5^2 - 4\alpha c_2)X_5^2 + 2c_3c_5X_3X_5 = 0.$$

For the point $p_3$ to be internal, the latter equation should only have $(X_3, X_5) = (0, 0)$ as solution. So, $p_3$ is an internal point if and only if $(c_3c_5)^2 - (c_3^2 + 4c_2) \cdot (c_5^2 - 4\alpha c_2)$ is a nonsquare, that is, $c_2(\alpha c_3^2 - c_5^2 + 4\alpha c_2)$ is a nonsquare in $\mathbb{F}_q$. ∎

**Remark.** The conditions mentioned in Lemmas 5.5 and 5.6 are always satisfied when $c_3 = c_5 = 0$. In this case, the line $p_1p_2$ not only meets $\pi_1$ in an internal point of $\mathcal{C}_1$, but also $\pi_2$ in an internal point of $\mathcal{C}_2$. This follows from a similar reasoning as in the proof of Lemma 5.6 using the fact that the plane $\pi_2$ is described by the equations $X_1 = c_2X_2$, $X_4 = -X_3$, $X_6 = \alpha X_5$.

We have written a computer program in GAP (see [9]) to verify for each ovoid $\{k_1, k_2, \ldots, k_{q+1}\}$ of $\mathcal{G}$ (determined by a permutation $\tau$ of $\overline{\mathbb{F}_q}$) whether the condition mentioned in Proposition 5.4 is satisfied. We have found solutions for $q \in \{3, 5, 7\}$. For each of these values of $q$, we mention one solution.

- If $q = 3$, then $\overline{\mathbb{F}_q} = \{\infty, 0, 1, 2\}$, $\alpha = 2$, $c_2 = 2$, $c_3 = 0$, $c_5 = 0$ and $\tau$ is trivial.

- If $q = 5$, then $\overline{\mathbb{F}_q} = \{\infty, 0, 1, 2, 3, 4\}$, $\alpha = 2$, $c_2 = 2$, $c_3 = 1$, $c_5 = 2$ and $\tau = (031)(24)$.

- If $q = 7$, then $\overline{\mathbb{F}_q} = \{\infty, 0, 1, 2, 3, 4, 5, 6\}$, $\alpha = 3$, $c_2 = 3$, $c_3 = 0$, $c_5 = 0$ and $\tau = (2453)$.

In fact, for each $q \in \{3, 5, 7\}$, we have found several solutions for $(\alpha, c_2, c_3, c_5, \tau)$, but by our earlier remark, they should all give rise to isomorphic $\mathcal{T}_1$-blocking sets. We have thus given explicit constructions for the blocking sets $B_1$, $B_3$ and $B_5$.

# 6 $\mathcal{T}_1$-blocking sets of size 8 in $\mathrm{PG}(3, 3)$

From Sections 3, 4 and 5, we know that there exist $\mathcal{T}_1$-blocking sets of size 8 in $\mathrm{PG}(3, 3)$. All these $\mathcal{T}_1$-blocking sets are isomorphic as the following proposition shows.

**Proposition 6.1** *Suppose $q = 3$. Then up to isomorphism there is a unique $\mathcal{T}_1$-blocking set of size 8 in $\mathrm{PG}(3, 3)$.*

**Proof.** Suppose $B$ is such a set of points. By Lemma 1.1, $B \cap Q^+(3, 3) = \emptyset$ and every outer tangent contains a unique point of $B$. We prove a number of additional properties for such $\mathcal{T}_1$-blocking sets. These properties occur in a number of claims directly followed by their proofs.

CLAIM 1: *Every tangent plane to $Q^+(3,3)$ contains precisely two points of $B$.*

Suppose $\pi$ is a tangent plane with tangent point $x$. The two lines of $\pi$ through $x$ contained in $Q^+(3,3)$ are disjoint from $B$, and the other two lines of $\pi$ through $x$ are outer tangents and so each contains a unique point of $B$. (qed)

CLAIM 2: *Every nontangent plane to $Q^+(3,3)$ contains 2, 3, 4 or 5 points of $B$.*

Let $\pi$ be a nontangent plane. Put $\pi \cap Q^+(3,3) = \{x_1, x_2, x_3, x_4\}$ and let $y_1, y_2, y_3$ denote the three points of $\pi$ that are internal to the conic $\pi \cap Q^+(3,3)$. For every $i \in \{1, 2, 3, 4\}$, let $L_i$ denote the unique tangent line through $x_i$ contained in $\pi$. Let $a$ denote the unique point of $L_1 \cap B$. Through $a$ there are two tangents to the conic $\pi \cap Q^+(3,3)$. Without loss of generality, we may suppose that the second tangent line through $a$ is $L_2$. The tangent line $L_3$ does not contain $a$ and so there exists a unique point $b$ on $L_3$ distinct from $x_3$, $L_3 \cap L_1$ and $L_3 \cap L_2$. The points $L_3 \cap L_1$ and $L_3 \cap L_2$ are not contained in $B$, implying that $b \in B$. The two lines through $b$ that are tangent to $\pi \cap Q^+(3,3)$ are the lines $L_3$ and $L_4$. So, the points of $B$ contained in $L_1 \cup L_2 \cup L_3 \cup L_4$ are the points $a$ and $b$. Every other point of $B$ must be an internal point, and so equal to $y_1$, $y_2$ or $y_3$. (qed)

Suppose $L$ is a secant line to $Q^+(3,3)$. Let $\pi_1$ and $\pi_2$ denote the two nontangent planes through $L$ and denote by $E_i$, $i \in \{1, 2\}$, the set of three points of $K_i \setminus L$, where $K_i$ is the unique external line of $\pi_i$ intersecting $L$ in a point that is external to the conic $\pi_i \cap Q^+(3,3)$. Put $B_L := (L \setminus Q^+(3,3)) \cup E_1 \cup E_2$. Then $|B_L| = 8$.

CLAIM 3: *Suppose $(L \setminus Q^+(3,3)) \subseteq B$ for a certain secant line $L$. Then $B = B_L$.*

By Claim 1, each of the two tangent planes through $L$ does not contain extra points of $B$ besides those of $L \setminus Q^+(3,3)$. By Claim 2, each of the two secant planes through $L$ contains at most 3 extra points of $B$ besides those of $L \setminus Q^+(3,3)$. Since $8 = |B| \leq |L \setminus Q^+(3,3)| + 3 \cdot 2 = 2 + 6 = 8$, we necessarily have $B = B_L$. Indeed, suppose $\pi$ is a nontangent plane through $L$, and $x$ is the unique point of $L$ that is external to the conic $\pi \cap Q^+(3,3)$ of $\pi$. The two tangent lines through $x$ contained in $\pi$ cannot contain extra points of $B$ (besides $x$). So, the unique external line through $x$ contained in $\pi$ must contain three extra points of $B$ (besides $x$). (qed)

In the sequel we will assume that $L \setminus Q^+(3,3)$ is not contained in $B$ for every secant line $L$, and derive a contradiction.

Let $x \in B$. The point $x$ is contained in four tangent lines, six secant lines and three external lines. None of the four tangent lines through $x$ can contain extra points of $B$ besides $x$. The same holds for the secant lines (by our assumption). Since $|B| = 8$, at least one of the external lines through $x$, say $K$, is completely contained in $B$. Let $y$ be a point of $B \setminus K$. As $K$ is an external line, the plane $\pi = \langle K, y \rangle$ is a nontangent plane. In $\pi$, there is a secant line $S$ through $y$ containing two points of $B$, namely $y$ and $S \cap K$, and this is impossible.

In conclusion, we can say that $B = B_L$ for a certain secant line $L$. As the automorphism group of $\mathrm{PG}(3,3)$ stabilising $Q^+(3,3)$ acts transitively on the set of secant lines, there is up to isomorphism at most one (and hence precisely one) set of 8 points that is a $\mathcal{T}_1$-blocking set. ∎

# Acknowledgements

# References

[1] A. Beutelspacher and J. Ueberberg, Bruck's vision of regular spreads or What is the use of a Baer superspace?, Abh. Math. Sem. Univ. Hamburg 63 (1993), 37–54.

[2] P. Biondi and P. M. Lo Re, On blocking sets of external lines to a hyperbolic quadric in PG$(3, q)$, $q$ even, J. Geom. 92 (2009), 23–27.

[3] P. Biondi, P. M. Lo Re and L. Storme, On minimum size blocking sets of external lines to a quadric in PG$(3, q)$, Beiträge Algebra Geom. 48 (2007), 209–215.

[4] R. C. Bose and R. C. Burton, A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes, J. Combinatorial Theory 1 (1966), 96–104.

[5] M. R. Brown, J. De Beule and L. Storme, Maximal partial spreads of $T_2(O)$ and $T_3(O)$, European J. Combin. 24 (2003), 73–84.

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

[7] M. Buratti and A. Pasotti. Combinatorial designs and the theorem of Weil on multiplicative character sums. *Finite Fields Appl.* 15 (2009), 332–344.

[8] J. De Beule and A. Gács. Complete arcs on the parabolic quadric $Q(4, q)$. *Finite Fields Appl.* 14 (2008), 14–21.

[9] B. De Bruyn and B. K. Sahoo. Computer computations for "On minimum size blocking sets of the outer tangents to a hyperbolic quadric in PG$(3, q)$", available online at `https://cage.ugent.be/geometry/preprints.php`.

[10] B. De Bruyn, B. K. Sahoo and B. Sahu, Blocking sets of tangent lines to a hyperbolic quadric in PG$(3, 3)$, communicated.

[11] B. De Bruyn, B. K. Sahoo and B. Sahu, Blocking sets of tangent and external lines to a hyperbolic quadric in PG$(3, q)$, Discrete Math. 341 (2018), 2820–2826.

[12] J. W. P. Hirschfeld, Finite projective spaces of three dimensions, Oxford University Press, 1985.

[13] *Sage Mathematics Software (Version 6.3)*, The Sage Developers, 2014. (http://www.sagemath.org).

[14] B. K. Sahoo and B. Sahu, Blocking sets of tangent and external lines to a hyperbolic quadric in PG$(3, q)$, $q$ even, Proc. Indian Acad. Sci. Math. Sci., to appear.

[15] B. K. Sahoo and B. Sahu, Blocking sets of certain line sets to a hyperbolic quadric in PG$(3, q)$, Adv. Geom., DOI: 10.1515/advgeom-2018-0009 (in press).

[16] B. K. Sahoo and N. S. N. Sastry, Binary codes of the symplectic generalized quadrangle of even order, Des. Codes Cryptogr. 79 (2016), 163–170.

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

[18] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.7.5, 2014. (http://www.gap-system.org)

**Addresses**:

**Bart De Bruyn**
Department of Mathematics, Ghent University
Krijgslaan 281 (S25), B-9000 Gent, Belgium
Email: Bart.DeBruyn@Ugent.be

**Binod Kumar Sahoo**
1) School of Mathematical Sciences
National Institute of Science Education and Research (NISER), Bhubaneswar
P.O. - Jatni, District- Khurda, Odisha - 752050, India

2) Homi Bhabha National Institute (HBNI)
Training School Complex, Anushakti Nagar
Mumbai - 400094, India

Email: bksahoo@niser.ac.in