Minimal blocking sets of size $q^2 + 2$ of $Q(4, q)$, q an odd prime, do not exist

J. De Beule [a]

[a] *Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281, B-9000 Gent, Belgium*

K. Metsch [b]

[b] *Mathematisches Institut, Universität Giessen, Arndtstrasse 2, D-35392 Giessen, Germany*

Abstract

It is known that every blocking set of $Q(4, q)$, $q > 2$ even, with less than $q^2 + 1 + \sqrt{q}$ points contains an ovoid, and hence $Q(4, q)$ has no minimal blocking set $\mathcal{B}$ with $q^2 + 1 < |\mathcal{B}| < q^2 + 1 + \sqrt{q}$. In contrast to this, it is even not known whether or not $Q(4, q)$, q odd, has minimal blocking sets of size $q^2 + 2$. In this paper, the non-existence of a minimal blocking set of size $q^2 + 2$ of $Q(4, q)$, q an odd prime, is shown. Strong geometrical information is obtained using an algebraic description of $W(3, q)$. Geometrical and combinatorial arguments complete the proof.

Key words: ovoid, blocking set, polar space, parabolic quadric
1991 MSC: 05B25, 51E12, 51E20, 51E21

1 Introduction

Consider the non-singular parabolic quadric $Q(4, q)$ in the 4-dimensional projective space $\mathrm{PG}(4, q)$. It is known that $(q^2 + 1)(q + 1)$ points and the same number of lines of $\mathrm{PG}(4, q)$ are contained in $Q(4, q)$, and that no higher dimensional subspaces of $\mathrm{PG}(4, q)$ are completely contained in it. This quadric is also an example of a finite classical generalized quadrangle if we consider it as a pure point-line geometry.

Email addresses: `jdebeule@cage.ugent.be` (J. De Beule), `klaus.metsch@math.uni-giessen.de` (K. Metsch).

An *ovoid* of $Q(4,q)$ is a set $\mathcal{O}$ of points of $Q(4,q)$, such that every line of $Q(4,q)$ meets $\mathcal{O}$ in exactly one point, necessarily, $|\mathcal{O}| = q^2+1$. A *blocking set* is a set $\mathcal{B}$ of points of $Q(4,q)$, such that every line of $Q(4,q)$ meets $\mathcal{B}$ in at least one point, necessarily $|\mathcal{B}| \geq q^2+1$ with equality if and only if $\mathcal{B}$ is an ovoid. A blocking set $\mathcal{B}$ is called *minimal* if $\mathcal{B} \setminus \{p\}$ is not a blocking set for any point $p \in \mathcal{B}$. A *multiple line* of $\mathcal{B}$ is a line of $Q(4,q)$ meeting $\mathcal{B}$ in at least two points.

It is a well known fact that the dual of the generalized quadrangle $Q(4,q)$, i.e., the point-line geometry obtained by interchanging the role of the points and the lines, is isomorphic to the generalized quadrangle $W(3,q)$, which is the generalized quadrangle with as pointset the points of $\mathrm{PG}(3,q)$, and as lineset the totally isotropic lines with respect to a symplectic polarity of $\mathrm{PG}(3,q)$. For more details we refer to [6].

An ovoid of $Q(4,q)$ translates under the duality to a *spread* of $W(3,q)$, this is a set of lines of $W(3,q)$ partitioning the pointset. A blocking set of $Q(4,q)$ translates to a *cover* of $W(3,q)$, this is a set of lines $\mathcal{C}$, such that every point of $W(3,q)$ lies on at least one line of $\mathcal{C}$. A *multiple point* of $\mathcal{C}$ is a point of $W(3,q)$ lying on at least two lines of $\mathcal{C}$.

It is known that $Q(4,q)$ has always an ovoid. Every elliptic quadric $Q^-(3,q)$ contained in $Q(4,q)$ is an example. Considering minimal blocking sets of $Q(4,q)$, q even, the following result is known.

Result 1 (Eisfeld et al. [5]) *Let $\mathcal{B}$ be a blocking set of the quadric $Q(4,q)$, q even. If $q \geq 32$ and $|\mathcal{B}| \leq q^2+1+\sqrt{q}$, then $\mathcal{B}$ contains an ovoid of $Q(4,q)$. If $q = 4, 8, 16$ and $|\mathcal{B}| \leq q^2+1+\frac{q+4}{6}$, then $\mathcal{B}$ contains an ovoid of $Q(4,q)$.*

No analogue theorem is known for q odd. It is even not known whether or not $Q(4,q)$, q odd, has a minimal blocking set of cardinality q^2+2, that is a blocking set of size q^2+2 that does not contain an ovoid. It is probably a bit unexpected but this problem seems to be quite hard. Using a combination of geometrical and algebraic methods we are able to solve the problem when q is an odd prime. Our result is as follows.

Theorem 2 *If q is an odd prime, then $Q(4,q)$ does not have a minimal blocking set of size q^2+2.*

We remark that this was proved earlier for $q = 5$ and $q = 7$, see [3].

Recently, it was proved that all ovoids of $Q(4,q)$, q odd prime, are elliptic quadrics $Q^-(3,q)$, [2]. In the proof, one considers an ovoid $\mathcal{O}$ of $Q(4,q)$, $q = p^h$, p an odd prime. Then it is proved that all hyperplanes of $\mathrm{PG}(4,q)$ intersect $\mathcal{O}$ in $1 \mod p$ points. When $q = p$, combinatorial arguments prove that $\mathcal{O}$ is necessarily an elliptic quadric. The $1 \mod p$ result is proved using polynomial techniques. In an earlier paper, [1], the $1 \mod p$ result is obtained using an algebraic description of the generalized quadrangle $W(3,q)$ in the field $\mathrm{GF}(q^4)$. Using this description of $W(3,q)$ and the structure of the multiple points, we obtain comparable results for minimal blocking sets of $Q(4,q)$, q odd, of size q^2+2. When q is a prime, these results, together with geometrical and combinatorial arguments, exclude the existence of such a blocking set.

In Section 2, we will adapt the algebraic approach from [1] to obtain a $t \mod p$ result. In Section 3 we will derive some combinatorial properties of a blocking set of size q^2+2 of $Q(4,q)$. In the last section, we will exclude the existence of a minimal blocking set of size q^2+2 of $Q(4,q)$, q an odd prime, using again geometrical and combinatorial arguments.

2 The intersection numbers

We make use of the fact that $Q(4,q)$ and $W(3,q)$ are dually isomorphic. Under this duality blocking sets of $Q(4,q)$ translates to covers of $W(3,q)$. In this section we prove a theorem on covers of $W(3,q)$ that have the property that the multiple points (the points covered more than once) form a sum of symplectic lines, see the next section for more details. By assigning the weight $w(L)=-1$ to these lines one is in the situation of the following theorem.

Theorem 3 *Consider $W(3,q)$ in $\mathrm{PG}(3,q)$, $q=p^h$, p a prime. Suppose that w is a function from the lineset $\mathcal{L}$ of $W(3,q)$ to $\mathrm{GF}(p)$ such that for every point v we have*

$$\sum_{L\in\mathcal{L}:\ L\ni v} w(L) = 1 \tag{1}$$

Let $\mathcal{F}$ be a regular spread of $\mathrm{PG}(3,q)$ consisting of lines of $W(3,q)$. Then

$$\sum_{L\in\mathcal{F}} w(L) = 1.$$

Before we start with the proof we summarize a description of $W(3,q)$ in $\mathrm{GF}(q^4)$ that was used in [1]. The points of $W(3,q)$ are the points of $\mathrm{PG}(3,q)$ and are represented by the solutions $u \in \mathrm{GF}(q^4)$ of the equation $u^{q^3+q^2+q+1} = 1$. The symplectic space is described using an alternating bilinear form $b: V(4,q)\times V(4,q) \to \mathrm{GF}(q)$. Therefore a constant $\Gamma \in \mathrm{GF}(q^4)$ is chosen such that $\Gamma^{q^2-1} = -1$. The bilinear form is defined as

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

We emphasize that X, Y are not points of $\mathrm{PG}(3,q)$ here, but vectors of $V(4,q)$. From this it can be derived that two points that are represented by u and v are perpendicular if and only if

$$\gamma u^{q+1} - \gamma v^{q+1} + q^{q^2+q+1} v - u v^{q^2+q+1} = 0 \tag{2}$$

Here $\gamma := \Gamma^{1-q}$.

The lines of $W(3,q)$, identified with their pointsets, are represented by two types of equations; the $q+1$ solutions of such an equation are exactly the representants of the points constituting the pointset of the line. Type (i) lines are represented by the equation

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

where $d \in \mathcal{D} := \{x \in \mathrm{GF}(q^4) \mid x^{q^3+q} - \gamma^{-1} x^{q^2+1} + 1 = 0\}$. Type (ii) lines are represented by the equation

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

where $e \in \mathcal{E} := \{x \in \mathrm{GF}(q^4) \mid x^{q^2+1} = 1\}$. It is also proved in [1] that the q^2+1 lines of type (ii) constitute a regular spread of $W(3,q)$.

Remark. Since the coefficient of U^q in the equation of a symplectic line is zero, we find $\sum_{v \in L} v = 0$ for any symplectic line L. This implies that $\sum_{v \in \pi} v = 0$ for every plane π, since the π is the union of the $q+1$ symplectic lines on the point $u := \pi^\perp$.

Proof of Theorem 3. The lines $L \in \mathcal{L}$ are represented by elements $d \in \mathcal{D}$ or $e \in \mathcal{E}$ and we denote by w_d or w_e the weight $w(L)$ of L. Without loss of generality we may assume that the regular spread $\mathcal{F}$ consists of the symplectic lines represented by the elements of $\mathcal{E}$. Consider a point of $u \in W(3,q)$. All symplectic lines on u lie in $u^\perp$ and all symplectic lines in $u^\perp$ pass through u. Consider a symplectic line not passing through u. Then L meets $u^\perp$ in a point v. If L has type (i), represented by $d \in \mathcal{D}$, then, using equation (2), one can prove

$$v^q = -u(du^{q+1} + u - \gamma d^q)^{q-1}. \tag{3}$$

If L has type (ii), represented with parameter $e \in \mathrm{GF}(q^4)$, then, using equation (2) it is proved that

$$v^q = \gamma^{-1} u e (u^{q+1} + e)^{q-1}. \tag{4}$$

This was also used in [1]. It follows that

$$-\sum_{L \in \mathcal{L}} w_L \sum_{v \in L \cap u^\perp} v^q = \sum_{d \in \mathcal{D}} w_d u (du^{q+1} + u - \gamma d^q)^{q-1} - \sum_{e \in \mathcal{E}} w_e \gamma^{-1} u e (u^{q+1} + e)^{q-1}.$$

In fact, every symplectic line appears on the left and the right hand side. We show that the contribution on both sides is equal for every line L of F. If L is not contained in $u^\perp$, so that L meets $u^\perp$ in a unique point v, then this follows from (3) and (4). Now consider the case when L is contained in $u^\perp$. Then the contribution on the left hand side is $w_L(\sum_{v\in L} v)^q$, which is zero by the remark of this section. The contribution on the right side is also zero, because then L is a symplectic line on u, so u satisfies the equation of L.

The left hand side of the equation is zero, since

$$\sum_{L\in\mathcal{L}}\sum_{v\in L\cap u^\perp} w_L v^q = \sum_{v\in u^\perp} v^q = \left(\sum_{v\in u^\perp} v\right)^q = 0^q = 0.$$

The first equality sign follows from the hypothesis in Theorem 3, and the third equality sign follows from the remark in this section. Consider the polynomial

$$f(U) := \sum_{d\in D} w_d U(dU^{q+1} + U - \gamma d^q)^{q-1} - \sum_{e\in\mathcal{E}} w_e \gamma^{-1} Ue(U^{q+1} + e)^{q-1}.$$

This polynomial has degree at most q^2 and by the previous arguments, $f(u) = 0$ for all points u. As there are $q^3 + q^2 + q + 1$ points, it follows that $f(U)$ is identically zero. Looking at the coefficient of U^q in $f(U)$, we conclude that

$$\sum_{d\in\mathcal{D}} w_d = 0.$$

Hypothesis (1) shows that

$$(q+1)\sum_{L\in\mathcal{L}} w(L) = \sum_u \sum_{L\in\mathcal{L}:L\ni u} w(L) = \sum_u 1 = q^3 + q^2 + q + 1.$$

As this is a calculation in GF(p), then $\sum_{L\in\mathcal{L}} w(L) = 1$. Hence the sum of $\sum_{d\in\mathcal{D}} w_d$ and $\sum_{e\in\mathcal{E}} w_e$ is also one, so $\sum_{e\in\mathcal{E}} w_e = 1$. Because the $e \in \mathcal{E}$ represent the lines of the spread $\mathcal{F}$, this proves the theorem. $\square$

3 The structure of the multiple points

Suppose that $\mathcal{B}$ is a blocking set of size $q^2 + 1 + r$ of $Q(4, q)$. A line of $Q(4, q)$ is called a *multiple line* or an *excess line* of $\mathcal{B}$ when it contains at least two points of $\mathcal{B}$. The *excess* e_L of a line L of $Q(4, q)$ is by definition $|L \cap \mathcal{B}| - 1$. Counting pairs (u, L) with lines $L \in B$ and points $u \in Q(4, q)$ with $u \in L$, one finds that the sum of the excesses over all lines of $Q(4, q)$ is $r(q + 1)$. Consider a line L of $Q(4, q)$. Every point of $L \cap \mathcal{B}$ lies on $q + 1$ lines of $Q(4, q)$ while the points of $\mathcal{B}$ that are not on L lie on a unique line of $Q(4, q)$ that meets L.

Hence, if $\mathcal{M}$ is the set consisting of the q^2+q+1 lines of $Q(4,q)$ that meet L, then

$$\sum_{M\in\mathcal{M}}(1+e_M)=(1+e_L)\cdot(q+1)+(|\mathcal{B}|-1-e_L)\cdot 1.$$

As $|\mathcal{M}|=q^2+q+1$, this gives

$$\sum_{M\in\mathcal{M}}e_M=|\mathcal{B}|-q^2-1+e_Lq.$$

Now suppose that $|\mathcal{B}|=q^2+2$. Then the right hand side is equal to e_Lq+1. As the sum of the excesses over all lines of $Q(4,q)$ is $r(q+1)=q+1$, it follows that $e_L\leq 1$. Furthermore, if L is a multiple line, then $e_L=1$ and L meets every other multiple line. It follows that there exist $q+1$ multiple lines and that they mutually meet. Hence, for $|\mathcal{B}|=q^2+2$, there exists a point $m\in Q(4,q)$ with the property that the $q+1$ lines of $Q(4,q)$ on m are the multiple lines; they meet B in two points while every other line of $Q(4,q)$ meets $\mathcal{B}$ in a unique point. We remark that this property can also be derived from a general theorem in [5].

Consider a solid (3-space) of the ambient projective space $\mathrm{PG}(4,q)$ of $Q(4,q)$. Then $S\cap Q(4,q)$ is either a quadric $Q^+(3,q)$, a quadric $Q^-(3,q)$ or a cone with a point vertex over a $Q(2,q)$; we say that S has *hyperbolic*, *elliptic* or *parabolic* type in the respective cases.

If S is a hyperbolic solid, then the existence of m shows that $|S\cap\mathcal{B}|=q+2$ if $m\in S$, and $|S\cap\mathcal{B}|=q+1$, if $m\notin S$. If S is a parabolic solid, then similarly $m\in S$ implies that $|S\cap B|\in\{2,q+2\}$ if $m\in S$, and $|S\cap B|\in\{1,q+1\}$ if $m\notin S$. Hence, for hyperbolic and parabolic solids S we have that

$$|S\cap\mathcal{B}|\equiv\begin{cases}2 \mod q, \text{ if } m\in S,\\ 1 \mod q, \text{ if } m\notin S.\end{cases}\tag{5}$$

In the forth section we shall see that if (5) also holds for the elliptic solids, then $\mathcal{B}$ is the union of a point and an elliptic quadric. For odd primes we can show that this always holds:

Lemma 4 *Suppose that $\mathcal{B}$ is a blocking set of size q^2+2 of $Q(4,q)$, q an odd prime. Then (5) holds for the elliptic solids.*

Proof. We recall that exactly $q+2$ lines are blocked twice by $\mathcal{B}$ and that all these lines pass through a point m of $Q(4,q)$. We now use that $Q(4,q)$ and $W(3,q)$ are dual. Under the duality the blocking set $\mathcal{B}$ corresponds to a cover $\mathcal{C}$ of $W(3,q)$, and the point m translates to a symplectic line M. Every point of $W(3,q)$ is covered by exactly one line of $\mathcal{C}$, except for the points of M which are covered by two lines of $\mathcal{C}$. Define a function w from the set consisting of the lines of $W(3,q)$ to the field $\mathrm{GF}(q)$ as follows. If $M \notin \mathcal{C}$ put $w(L) = 1$ for $L \in \mathcal{C}$, $w(M) := -1$, and $w(L) = 0$ for the remaining symplectic lines. If $M \in \mathcal{C}$ put $w(L) = 1$ for $L \in C \setminus \{M\}$ and $w(L) = 0$ for the remaining symplectic lines. Then hypothesis (1) of Theorem 3 is satisfied.

As the regular spreads of $\mathrm{PG}(3,q)$ consisting of symplectic lines correspond under the duality to solids of $\mathrm{PG}(4,q)$ meeting $Q(4,q)$ in an elliptic quadric $Q^-(3,q)$, the assertion follows from Theorem 3. $\square$

Remarks. (1) If $|\mathcal{B}| = q^2 + 2$, then we have proved above the existence of a point m lying on all multiple lines. We mention that $m \in \mathcal{B}$ if and only if $\mathcal{B} \setminus \{m\}$ is an ovoid of $Q(4,q)$.

(2) Consider a blocking set $\mathcal{B}$ of $Q(4,q)$ with $|\mathcal{B}| = q^2+1+r$. We also consider the corresponding cover $\mathcal{C}$ of $W(3,q) \subseteq \mathrm{PG}(3,q)$. If r is not too large, then it was shown in [5], then there exists r lines $M_1, \ldots, M_r$ of $\mathrm{PG}(3,q)$ (repeated lines are allowed) with the following property. The number of lines of $\mathcal{C}$ on a point v of $W(3,q)$ is one plus the number of lines M_i on v. Here the lines M_i can be symplectic but need not to be symplectic. However, if they are all symplectic, then the technique of Section 2 can be applied. In that case, going back to $\mathcal{B}$ in $Q(4,q)$ one obtains points $m_1, \ldots, m_r$ of $Q(4,q)$ corresponding to $M_1, \ldots, M_r$, and the intersection of a solid with $\mathcal{B}$ is modulo p congruent to one plus the number of points M_i in such a solid.

If a line M_i is not symplectic, then the translation to $Q(4,q)$ gives a regulus consisting of multiple lines, and then the opposite regulus will also have only multiple lines.

(3) S. De Winter [4] has constructed a minimal blocking set of $Q(4,q)$ of size $q^2 + 3$ for $q = 5$. If one analyzes the structure of the multiple lines in his example, one sees that the multiple lines are the $2(q+1)$ lines of a hyperbolic quadric $Q^+(3,q)$.

4 The final step

In this section, $\mathcal{B}$ denotes a blocking set of $Q(4,q)$ of size $q^2 + 2$. It has been shown in Section 3 that there exists a point m of $Q(4,q)$ with the property that the $q+1$ lines of $Q(4,q)$ on m meet $\mathcal{B}$ in two points while every other line of $Q(4,q)$ meets $\mathcal{B}$ in a unique point. If q is a prime, we have also seen that for every solid S we have

$$|S \cap \mathcal{B}| \equiv \begin{cases} 2 \mod q, \text{ if } m \in S, \\ 1 \mod q, \text{ if } m \notin S. \end{cases} \tag{6}$$

We shall not assume in this section that q is a prime, but we shall assume that (6) holds for all solids. We also assume that q is odd. Our goal is to show that $\mathcal{B}$ is not minimal. This will also prove Theorem 2.

We proceed in an indirect way and assume for the rest of the section that $\mathcal{B}$ is minimal. This implies that $m \notin \mathcal{B}$, since the special properties of m imply otherwise that $B \setminus \{m\}$ is also a blocking set. We shall derive a contradiction in a series of lemmas.

Lemma 5 *If t_i is the number of solids meeting $\mathcal{B}$ in precisely i points, then $t_{q+2} \geq \frac{1}{2}q(q^2+q)$ and $t_2 \leq \frac{1}{2}(q^2+q+2)(q-1)$.*

Proof. Only solids through m can meet $\mathcal{B}$ in two or $q+2$ points. The solid $m^\perp$ meets $\mathcal{B}$ in $2q+2$ points. Every other solid S on m meets $m^\perp$ in a plane. Note that $m^\perp \cap Q(4,q)$ is a cone with vertex m over a $Q(2,q)$.

There are $(q^2+q)/2$ planes π of $m^\perp$ on m that meet $Q(4,q)$ in the union of two lines; these meet $\mathcal{B}$ in four points. From (6) it follows that every solid S with $S \neq m^\perp$ on such a plane π contains at least $q-2$ more points of $\mathcal{B}$. As $|\mathcal{B}| = q^2+2 = (2q+2)+q(q-2)$, it follows that every solid $S \neq m^\perp$ on π meets $\mathcal{B}$ in precisely $q+2$ points. Hence $t_{q+2} \geq \frac{1}{2}q(q^2+q)$.

Apart from the planes just considered, there are $(q^2+q+2)/2$ other planes π of $m^\perp$ on m. These meet $Q(4,q)$ either in one line or just in the point m, so they meet $\mathcal{B}$ either in no or two points. As $|\mathcal{B}| = q^2+2$ is an odd number, not all solids different from $m^\perp$ on such a plane can meet $\mathcal{B}$ in exactly two points. This implies that $t_2 \leq \frac{1}{2}(q^2+q+2)(q-1)$. $\square$

For the rest of the section we use $i_S := |S \cap \mathcal{B}|$ with S any solid of $\mathrm{PG}(4,q)$, and $\theta_n := \frac{q^{n+1}-1}{q-1} = q^n + q^{n-1} + \ldots + q + 1$ for any integer $n \geq 0$.

Lemma 6 *Put $c := \frac{1}{2}(q^2+1)$. Then*

$$\sum_S (i_S-1)(i_S-q-1)(i_S-c) \geq \frac{1}{2}\left(q^5+4q^4+q^3+7q^2+3\right).$$

Here the sum runs over all solids of $\mathrm{PG}(4,q)$.

Proof. Put $b := |\mathcal{B}| = q^2+2$. Standard counting arguments show

$$\sum_S i_S = b\theta_3 \quad \text{and} \quad \sum_S i_S(i_S-1) = b(b-1)\theta_2.$$

We know that every line of the quadric meets $\mathcal{B}$ in one or two points. Hence, any three points of $\mathcal{B}$ span a plane. Therefore

$$\sum_S i_S(i_S-1)(i_S-2) = b(b-1)(b-2)\theta_1.$$

It follows that

$$\begin{aligned}
&\sum_S (i_S-1)(i_S-q-1)(i_S-c) = \\
&\sum_S \Big(i_S(i_S-1)(i_S-2) - i_S(i_S-1)(c+q-1) + i_S c(q+1) - c(q+1) \Big) = \\
&b(b-1)(b-2)\theta_1 - (c+q-1)b(b-1)\theta_2 + c(q+1)b\theta_3 - c(q+1)\theta_4 = \\
&\frac{1}{2}\Big(q^5+4q^4+q^3+7q^2+3\Big).
\end{aligned}$$

This is the claim. □

Lemma 7 *There exists a solid $S \neq m^\perp$ meeting $\mathcal{B}$ in more than $(q^2+1)/2$ points.*

Proof. Again put $c = (q^2+1)/2$. Recall that q is odd, which implies that $q \geq 3$ and $c-q-2 \geq 0$. We already know that every solid meets $\mathcal{B}$ in one or two modulo q points. Hence, a solid meets $\mathcal{B}$ in 1, 2, $q+1$ or at least $q+2$ points. Recall that $m^\perp$ is a solid that meets $\mathcal{B}$ in $2q+2$ points. If $\mathcal{L}'$ is the set consisting of all solids S with $S \neq m^\perp$ and $|S \cap B| > q+2$, then the preceding lemma implies that

$$\begin{aligned}
&\sum_{S\in\mathcal{L}'} (i_S-1)(i_S-q-1)(i_S-c) \\
&\quad \geq \frac{1}{2}\Big(q^5+4q^4+q^3+7q^2+3\Big) + t_{q+2}(q+1)(c-q-2) \\
&\quad -t_2(q-1)(c-2) - (2q+1)(q+1)(2q+2-c)
\end{aligned}$$

Using the bounds for t_{q+2} and t_2, a calculation shows that the right hand side is positive. Thus, some solid of $\mathcal{L}'$ meets $\mathcal{B}$ in more than $\frac{1}{2}(q^2+1)$ points. □

Lemma 8 *The final contradiction.*

Proof. Let S be a solid meeting $\mathcal{B}$ in more than $\frac{1}{2}(q^2+1)$ points. As lines of the quadric meet $\mathcal{B}$ in at most two points, and lines of the quadric with two points pass through m, it follows that all parabolic solids different from $m^\perp$ and all hyperbolic solids meet $\mathcal{B}$ in at most $q+2$ points. Hence S is an elliptic solid, that is $S \cap Q(4,q)$ is a $Q^-(3,q)$. Denote by α the number of points of $S \cap Q(4,q)$ that are not in $\mathcal{B}$. Then $\mathcal{B}' := \mathcal{B} \setminus (\mathcal{B} \cap S)$ contains $\alpha+1$ points.

Assume that the $Q^-(3,q)$ contains a conic C such that no point of this conic belongs to $\mathcal{B}$. We count pairs $(u,v) \in C \times \mathcal{B}'$ for which uv is a line of the quadric. A point $u \in C$ lies on $q+1$ lines of the quadric, which meet $\mathcal{B}$ and thus $\mathcal{B}'$. Hence each $u \in C$ occurs in $q+1$ such pairs. Thus, the number of such pairs is at least $(q+1)^2$. A point $v \in \mathcal{B}'$ can be perpendicular to zero, one, two or $q+1$ points of C. However, as the quadric $Q(4,q)$ has only two points that are perpendicular to all points of the conic C, there are at most two points v in $\mathcal{B}'$ that occur in $q+1$ pairs (u,v). Hence, the number of pairs is at most

$$2(q+1) + (|\mathcal{B}'| - 2)2 = 2\alpha + 2q.$$

It follows that $2\alpha + 2q \geq (q+1)^2$, that is $\alpha \geq \frac{1}{2}(q^2+1)$. Then $|S \cap \mathcal{B}| = q^2 + 1 - \alpha \leq \frac{1}{2}(q^2+1)$, and this is a contradiction. Hence, every conic of the elliptic quadric $S \cap Q(4,q)$ meets $\mathcal{B}$.

Count pairs (u,v) with perpendicular points u and v where $u \in S \cap Q(4,q)$, $u \notin \mathcal{B}$ and $v \in \mathcal{B}'$. For $v \in \mathcal{B}'$, the subspace $v^\perp \cap S$ is a plane that meets the quadric in a conic, and we have just seen that at most q points of such a conic do not lie in $\mathcal{B}$. Hence, each point $v \in \mathcal{B}'$ occurs in at most q such pairs. Each point $u \in S \cap Q(4,q)$ with $u \notin \mathcal{B}$, lies on $q+1$ lines of the quadric, which meet $\mathcal{B}$ and hence which meet $\mathcal{B}'$. Thus, every such point u occurs in at least $q+1$ such pairs. It follows that $\alpha(q+1) \leq |\mathcal{B}'|q$. As $|\mathcal{B}'| = \alpha + 1$, this gives $\alpha \leq q$.

Hence $|S \cap \mathcal{B}| \geq q^2 + 1 - q$ and at most $q+1$ points of $\mathcal{B}$ do not lie in S. As the global assumption in this section is that $\mathcal{B}$ is minimal, it is not possible that all points of $S \cap Q(4,q) = Q^-(3,q)$ lie in $\mathcal{B}$. Let u be a point of $S \cap Q(4,q)$ does not lie in $\mathcal{B}$. We have just seen that the $q+1$ lines of the quadric on u meet $\mathcal{B}'$. Hence $|\mathcal{B}'| \geq q+1$. As $|S \cap \mathcal{B}| + |\mathcal{B}'| = |\mathcal{B}| = q^2 + 2$, it follows that $|S \cap \mathcal{B}| = q^2 + 1 - q$ and $|\mathcal{B}'| = q + 1$. The argument also shows that each of the q points u of $S \cap Q(4,q)$ that is not in $\mathcal{B}$ is perpendicular to each point of $\mathcal{B}'$. But q points of $S \cap Q(4,q)$ span at least a conic-plane and thus have at most two common perpendicular points in $Q(4,q)$. This is a contradiction. $\square$

Acknowledgement

The first author thanks Stefaan De Winter for the interesting chats on [1].

References

[1] S. Ball. On ovoids of $\mathrm{O}(5,q)$. *Adv. Geom.*, 4(1):1–7, 2004.

[2] S. Ball, P. Govaerts, and L. Storme. On Ovoids of Parabolic Quadrics. *J. London Math. Soc.* submitted.

[3] J. De Beule, L. Storme, and A. Hoogewijs. The Size of a minimal blocking sets of $Q(4, q)$. *SIGSAM Bulletin.* to appear.

[4] S. De Winter. Private Communication.

[5] J. Eisfeld, L. Storme, T. Szőnyi, and P. Sziklai. Covers and blocking sets of classical generalized quadrangles. *Discrete Math.*, 238(1-3):35–51, 2001. Designs, codes and finite geometries (Shanghai, 1999).

[6] S. E. Payne and J. A. Thas. *Finite generalized quadrangles*, volume 110 of *Research Notes in Mathematics*. Pitman (Advanced Publishing Program), Boston, MA, 1984.