Blocking sets of $\mathcal{H}(n, q^2)$ with respect to generators

Antonio Cossidente

Dipartimento di Matematica e Informatica, Università degli Studi della Basilicata, Contrada Macchia Romana, 85100 Potenza (ITALY)

Oliver H. King*

School of Mathematics and Statistics, Newcastle University, Newcastle upon Tyne NE1 7RU, England, UK

Abstract

We construct minimal blocking sets with respect to generators on the Hermitian surfaces $\mathcal{H}(n, q^2)$ when n and q are both odd. A blocking set arises from $q+1$ quadrics in $PG(n, q^2)$ whose polarities commute with a unitary polarity, constructed from the union of Baer sub-quadrics with the common intersections deleted.

Key words: blocking sets, Hermitian surface, commuting polarities

1. Introduction

We denote by $PG(n, q^2)$ the n-dimensional projective space over the field $GF(q^2)$, with $n \geq 3$ and q odd, and by $\mathcal{H}(n, q^2)$ a Hermitian variety in $PG(n, q^2)$ determined by a non-degenerate Hermitian form. A *blocking set* of $\mathcal{H}(n, q^2)$ with respect to k-dimensional subspaces of $PG(n, q^2)$ contained in $\mathcal{H}(n, q^2)$ is a set of points of $\mathcal{H}(n, q^2)$ that meets every k-dimensional subspace of $PG(n, q^2)$ contained in $\mathcal{H}(n, q^2)$; a blocking set is *minimal* if the removal of any point leads to a non-blocking set (thus each point is *essential*). In this paper we are interested in blocking sets of $\mathcal{H}(n, q^2)$ with respect to generators when n is odd, meaning blocking sets of $\mathcal{H}(n, q^2)$ with respect

*Corresponding author

Email addresses: `cossidente@unibas.it` (Antonio Cossidente), `O.H.King@ncl.ac.uk` (Oliver H. King)

to $(n-1)/2$-dimensional subspace of $PG(n,q^2)$ contained in $\mathcal{H}(n,q^2)$. We construct a family of small minimal blocking sets that are *non-linear* in the sense that they do not lie in a subspace of $PG(n,q^2)$ of dimension $(n+1)/2$. Blocking sets of Hermitian surfaces appear rare. Indeed the authors are aware of no examples of minimal blocking sets apart from the linear blocking sets investigated by Metsch in [6], the example in [1] that is generalised in the current work and some examples in $\mathcal{H}(3,q^2)$ given by Cimrakova, De Beule and Fack in [2].

An *ovoid* in $\mathcal{H}(n,q^2)$, if one exists, is a set of points of $\mathcal{H}(n,q^2)$ that meets each generator exactly once. The size of an ovoid would be q^n+1: this provides a lower bound for the size of a minimal blocking set. We show the blocking sets we construct have size $q^{n-1}(q+1)$. We are not aware of any upper bound for the size of a minimal blocking set besides the trivial one obtained by counting the number of generators: $(q+1)(q^3+1)\dots(q^n+1)$.

Metsch conjectures that the smallest minimal blocking sets with respect to k-dimensional subspaces of $PG(n,q^2)$ are linear (i.e., they lie in a subspace of $PG(n,q^2)$ of dimension $n-k$). In [6] he proves the conjecture (with a minor caveat) when $k \leq (n-3)/2$, and (with De Beule) in [4] he proves the conjecture (with a minor caveat) when n is even and $k < (n-1)/2$. For $k=(n-1)/2$ the conjecture remains unproven. Nevertheless linear blocking sets remain examples of small minimal blocking sets with sizes ranging from $(q^{(n+3)/2}-(-1)^{(n+3)/2})(q^{(n+1)/2}-(-1)^{(n+1)/2})/(q^2-1)$ to $q^{n-1}(q+1)$ (see Section 6). Our construction, which works for odd q, thus provides examples that are similar in size to the linear blocking sets.

2. The construction of a set $\mathbf{B}_n$

We suppose that n and q are both odd. We write $\mathcal{H}$ for the Hermitian variety $\mathcal{H}(n,q^2)$. We use properties of commuting polarities to construct a set of points $\mathbf{B}_n$ that we prove to be a minimal blocking set. The construction generalises that given in [1] for the case $n=3$.

The notion of commuting polarities was introduced by J. Tits ([9]). In [7], Segre extensively developed the theory of polarities commuting with a non–degenerate unitary polarity defined on a finite projective space; Segre's work forms the background to our construction of blocking sets.

Let $\mathcal{B}$ be a non-degenerate orthogonal polarity commuting with the Hermitian polarity $\mathcal{U}$ associated with $\mathcal{H}$, and let $\mathcal{Q}(n,q^2)$ be the quadric associated with $\mathcal{B}$. If $\mathcal{V}=\mathcal{B}\mathcal{U}=\mathcal{U}\mathcal{B}$, then $\mathcal{V}$ is a non–linear collineation, the fixed points of $\mathcal{V}$ form a Baer subspace $\Sigma_0 = PG(n,q)$ of $PG(n,q^2)$ which meets both $\mathcal{H}$ and $\mathcal{Q}(n,q^2)$ in a non–degenerate 'Baer quadric' $\mathcal{Q}(n,q)$.

Suppose that $\mathcal{H}$ is given by $X_0^{q+1} + \cdots + X_n^{q+1} = 0$ and that quadrics $\mathcal{R}_\alpha = \mathcal{Q}_\alpha(n,q^2)$ are given by $\alpha X_0^2 + X_1^2 + \cdots + X_n^2 = 0$ with $\alpha^{q+1} = 1$. Let $\mathcal{B}_\alpha$ be the orthogonal polarity of $\mathcal{R}_\alpha$. Each of the $q+1$ polarities $\mathcal{B}_\alpha$ commutes with $\mathcal{U}$, with an associated semilinear involution $\mathcal{V}_\alpha = \mathcal{U}\mathcal{B}_\alpha$. The fixed points of $\mathcal{V}_\alpha$ on $PG(n,q^2)$ are the points of a Baer subspace Σ_α which meets $\mathcal{H}$ in the Baer quadric $\mathcal{Q}_\alpha = \mathcal{Q}^\pm_\alpha(n,q)$; this quadric is elliptic for half the values of α and hyperbolic for the other half. The intersection $\mathcal{S}_\alpha$ of $\mathcal{Q}_\alpha(n,q^2)$ with $\mathcal{H}$ consists of the points of the quadric $\mathcal{Q}^\pm_\alpha(n,q)$ together with the $GF(q^2)$-extensions of the lines of $\mathcal{Q}^\pm_\alpha(n,q)$. The quadrics $\mathcal{Q}_\alpha(n,q^2)$ are all necessarily hyperbolic.

We denote by Δ the hyperplane $X_0 = 0$ of $PG(n,q^2)$, which is fixed (globally) by each $\mathcal{V}_\alpha$. The intersection of Δ and Σ_α is the same set Δ_0 for each α, and Δ_0 is a hyperplane of each Σ_α. If k is a subspace of Δ that is a $GF(q^2)$-extension of a subspace of Δ_0, then $k^{\mathcal{U}} = k^{\mathcal{B}_\alpha}$ for each α, and in these circumstances we write $k^\perp$ for $k^{\mathcal{U}}$. We observe that Δ_0 meets $\mathcal{H}$ and each $\mathcal{Q}_\alpha$ in the same set $\mathcal{P}_0$, a parabolic quadric of $PG(n-1,q)$; indeed $\mathcal{P}_0$ is the intersection of any two of the Baer quadrics $\mathcal{Q}^\pm_\alpha(n,q)$. Our main theorem is the following:

Theorem 2.1. For any odd $n \geq 3$, the set $\mathbf{B}_n = \cup_\alpha \mathcal{Q}^\pm_\alpha(n,q) \setminus \mathcal{P}_0$ is a minimal blocking set of $\mathcal{H}(n,q^2)$ with respect to generators.

We use a reduction argument, the initial case being:

Result 2.2 ([1])**.** $\mathbf{B}_3$ is a minimal blocking set of $\mathcal{H}(3,q^2)$ with respect to generators.

Remark 2.3. When n is even, it is still possible to define a set of quadrics $\mathcal{Q}_\alpha(n,q^2)$, although $\mathcal{P}_0$ is no longer parabolic, but there is no possibility of $\mathbf{B}_n$ being a blocking set. To see this, consider a generator π of $\mathcal{H}$ that lies in Δ. Any point of $\pi \cap \mathcal{Q}_\alpha(n,q)$ lies in Δ so lies in $\mathcal{Q}_\alpha(n,q) \cap \Delta = \mathcal{P}_0$, and by definition $\mathcal{P}_0 \cap \mathbf{B}_n = \emptyset$.

3. Preliminary results and observations

Suppose we have commuting polarities $\mathcal{U}, \mathcal{B}$ on $PG(n,q^2)$ with $\mathcal{H}, \mathcal{Q} = \mathbf{Q}(n,q^2), \Sigma_0, \mathcal{Q}_0 = \mathcal{Q}(n,q)$ as described in the previous section, and suppose that k is a non-degenerate hyperplane k of Σ_0. The hermitian form

h corresponding to $\mathcal{U}$ and the bilinear form b corresponding to $\mathcal{B}$ are each determined (up to a scalar) by the bilinear form corresponding to $\mathcal{Q}_0$; indeed we can regard them as coinciding on the vector space $V(n+1,q)$ corresponding to Σ_0. Thus we can set a co-ordinate system so that the restriction of $\mathcal{Q}_0$ to k is given by $X_1^2+\cdots+X_n^2=0$ and $\mathcal{H}$ is given on the corresponding hyperplane of $PG(n,q^2)$ by $X_1^{q+1}+\cdots+X_n^{q+1}=0$. Rather than extending the co-ordinate system to Σ_0, we can extend it to $PG(n,q^2)$ in such a way that $\mathcal{H}$ is given by $X_0^{q+1}+\cdots+X_n^{q+1}=0$, and then $\mathcal{Q}$ will be given by $\alpha X_0^2+X_1^2+\cdots+X_n^2=0$ for some $\alpha\in GF(q^2)$. It is a consequence of commuting polarities that $\alpha^{q+1}=1$. This means that if we have a set of $q+1$ non-degenerate quadrics of $PG(n,q^2)$ commuting with $\mathcal{H}$, such that the corresponding Baer subspaces share a common non-degenerate hyperplane, then the co-ordinate system can be chosen so that $\mathcal{H}$ and the quadrics are as given in the previous section. This observation allows us to establish a lemma that is useful in our reduction argument.

Lemma 3.1. Suppose that $n\geq 5$ and that ℓ_0 is a non-degenerate line of Δ_0, with ℓ the extension of ℓ_0 to $GF(q^2)$. Then $\ell^\perp\cap\mathbf{B}_n$ has the structure of $\mathbf{B}_{n-2}$.

Proof. We note that $\ell^\perp\cap\mathbf{B}_n=\cup_\alpha(\mathcal{Q}_\alpha^\pm(n,q)\cap\ell^\perp)\setminus(\mathcal{P}_0\cap\ell^\perp)$ and this is a subset of $\mathcal{H}(n-2,q^2)=\mathcal{H}\cap\ell^\perp$. For each α, the polarity of $\mathcal{Q}_\alpha^\pm(n,q)\cap\ell^\perp$ commutes with the polarity of $\mathcal{H}(n-2,q^2)$, and the product fixes each point in the parabolic quadric $\mathcal{P}_0\cap\ell^\perp$. It is clear that the quadrics $\mathcal{Q}_\alpha^\pm(n,q)\cap\ell^\perp$ are distinct. It now follows that there is a co-ordinate system for $\ell^\perp$, relative to which $\mathcal{H}(n-2,q^2)$ has equation $Y_0^{q+1}+Y_1^{q+1}+\cdots+Y_{n-2}^{q+1}=0$ and the quadrics have equations $\gamma Y_0^2+Y_1^2+\cdots+Y_{n-2}^2=0$ with $\gamma\in GF(q^2)$ with $\gamma^{q+1}=1$; further, $\mathcal{P}_0\cap\ell^\perp$ is given by $Y_1^2+\cdots+Y_{n-2}^2=0$ inside $Y_0=0$. Thus $\ell^\perp\cap\mathbf{B}_n$ has the structure of $\mathbf{B}_{n-2}$.

Remark 3.2. Notice that when $\mathcal{Q}_\alpha^\pm(n,q)\cap\ell^\perp$ has equation $\gamma Y_0^2+Y_1^2+\cdots+Y_{n-2}^2=0$, it is not necessarily the case that $\gamma=\alpha$. Indeed if ℓ_0 is external to $\mathcal{P}_0$, then $\mathcal{Q}_\alpha^\pm(n,q)\cap\ell^\perp$ is hyperbolic if and only if $\mathcal{Q}_\alpha^\pm(n,q)$ is elliptic, so $\gamma\neq\alpha$.

4. $\boldsymbol{B_n}$ is a blocking set for $\boldsymbol{n}$ odd

Lemma 4.1. Let π be any generator of $\mathcal{H}(n,q^2)$ and let $k=\pi\cap\Delta$. Then k meets the $GF(q^2)$-extension of a non-degenerate line of Δ_0.

Proof. Suppose first that π meets Δ_0, and let X be a point in the intersection. Then any non-degenerate line ℓ_0 of Δ_0 through X has the required properties.

Now suppose that π does not meet Δ_0 and choose any quadric $\mathcal{Q}_\alpha$. If k met $\mathcal{V}_\alpha(k)$, then $k \cap \mathcal{V}_\alpha(k)$ would be fixed (globally) by $\mathcal{V}_\alpha$ and would therefore extend a subspace of Δ_0, which would imply that π met Δ_0. Hence k and $\mathcal{V}_\alpha(k)$ are skew and span a $(n-2)$-dimensional subspace M of Δ; M is fixed by $\mathcal{V}_\alpha$ so it extends a subspace M_0 of Δ_0. Observe that $\mathcal{V}_\alpha(k)$ lies on $\mathcal{H}(n,q^2)$ so M is non-degenerate with respect to $\mathcal{U}$ and therefore M_0 is a non-degenerate subspace of Δ_0. As X varies on k, the $(q^{n-1}-1)/(q^2-1)$ lines $\ell(X) = \langle X, \mathcal{V}_\alpha(X)\rangle$ each extend a line $\ell(X)_0$ of M_0 and therefore each contain $q+1$ points of M_0. Any two lines $\ell(X), \ell(Y)$ are skew because $\langle X, Y, \mathcal{V}_\alpha(X), \mathcal{V}_\alpha(Y)\rangle$ has dimension 3. It follows that the $(q^{n-1}-1)/(q^2-1)$ lines $\ell(X)_0$ contain all the points of M_0 and hence form a line-spread of M_0. Each $\ell(X)$ meets $\mathcal{H}(n-2,q^2) = \mathcal{H} \cap M$ twice so $\ell(X_0)$ cannot be a tangent to $\mathcal{Q}_\alpha(n-2,q) = \mathcal{Q}_\alpha \cap M_0$. The lines $\ell(X)_0$ cannot all lie on $\mathcal{Q}_\alpha(n-2,q)$, so there is a line $\ell_0 = \ell(X)_0$ that is non-degenerate, and k meets $\ell(X)$ in X.

□

Theorem 4.2. For any odd $n \geq 3$, $\mathbf{B}_n$ is a blocking set of $\mathcal{H}(n,q^2)$ with respect to generators.

Proof. We argue by induction on n. The initial case is $n = 3$: it is shown in [1] that $\mathbf{B}_3$ is a blocking set of $\mathcal{H}(3,q^2)$ with respect to lines. Assume that $n \geq 5$ and that $\mathbf{B}_{n-2}$ is a blocking set of $\mathcal{H}(n-2,q^2)$ with respect to generators.

Let π be a generator of $\mathcal{H}$, let $k = \pi \cap \Delta$ and let ℓ_0 be a non-degenerate line of Δ_0 such that k meets the $GF(q^2)$-extension ℓ of ℓ_0. We write E for $\ell^\perp$. By Lemma 3.1, $E \cap \mathbf{B}_n$ has the structure of $\mathbf{B}_{n-2}$. By the inductive hypothesis, $E \cap \mathbf{B}_n$ is a blocking set of $\mathcal{H} \cap E$ with respect to generators of $\mathcal{H} \cap E$. In particular $\pi \cap E$ is a generator of $\mathcal{H} \cap E$, so it meets $E \cap \mathbf{B}_n$. But $E \cap \mathbf{B}_n$ is a subset of $\mathbf{B}_n$. We conclude that π meets $\mathbf{B}_n$.

Hence $\mathbf{B}_n$ is a blocking set of $\mathcal{H}(n,q^2)$ for any odd $n \geq 3$.

□

5. B_n is a minimal blocking set for n odd

Recall that $\mathcal{R}_\alpha$ denotes $\mathcal{Q}_\alpha(n,q^2)$, $\mathcal{Q}_\alpha$ denotes $\mathcal{Q}^{\pm}_\alpha(n,q)$ and $\mathcal{S}_\alpha$ denotes the subset of $\mathcal{R}_\alpha$ obtained by extending the lines on $\mathcal{Q}_\alpha$ to $GF(q^2)$.

In order to show that $\mathbf{B}_n$ is a minimal blocking set, we have to show that each point P is essential, i.e., that $\mathbf{B}_n \setminus \{P\}$ is not a blocking set. We thus have to show that there is a generator that meets $\mathbf{B}_n$ just in the point P. After an intitial Lemma, we prove that $\mathbf{B}_5$ is a minimal blocking set. This case is the hardest to prove, but it also turns out to be necessary in proving the result for larger n.

Lemma 5.1. Suppose that $P \in \mathcal{Q}_\alpha \setminus \mathcal{P}_0$. Then there exists a generator π of $\mathcal{H}$ such that $\pi \cap \mathcal{Q}_\alpha = \{P\}$.

Proof. Let $M = P^{\mathcal{U}} \cap \Delta = P^{\mathcal{B}_\alpha} \cap \Delta$. Since $P \notin M$, M is a non-degenerate $n-2$-subspace of Δ fixed by $\mathcal{V}_\alpha$ and so M extends a subspace M_0 of Δ_0. Let $\ell_1 + \cdots + \ell_r$ ($r = (n-1)/2$) be a decomposition of M_0 into pairwise orthogonal non-degenerate lines, and choose on the $GF(q^2)$-extension of each ℓ_i a point Y_i of $\mathcal{H} \setminus \Delta_0$ (each extension being a $q+1$ secant to $\mathcal{H}$); note that $\mathcal{V}_\alpha(Y_i)$ is distinct from Y_i but still lies on the $GF(q^2)$-extension of ℓ_i. Let π be the generator $\langle P, Y_1, Y_2, \ldots Y_r \rangle$ of $\mathcal{H}$. Then $\pi \cap \mathcal{V}_\alpha(\pi) = \{P\}$ so π does not meet $\mathcal{P}_0$. Suppose that $\pi \cap \mathcal{Q}_\alpha$ contains a point $R \neq P$, then $R \in \pi \subset P^{\mathcal{U}} = P^{\mathcal{B}_\alpha}$ and so PR is a line on $\mathcal{Q}_\alpha$; such a line must meet $\mathcal{P}_0$, a contradiction.

□

Lemma 5.2. Suppose $n = 5$ and that $P \in \mathcal{Q}_\alpha \setminus \mathcal{P}_0$. There exists a plane of $\mathcal{H}$ meeting $\mathcal{R}_\alpha$ in the single point P if and only if $\mathcal{Q}_\alpha$ is elliptic.

Proof. Suppose that π is a generator of $\mathcal{H}$ passing through P. Then $k = \pi \cap \Delta$ is line of Δ. Moreover $M = P^{\mathcal{U}} \cap \Delta$ is a solid fixed by $\mathcal{V}_\alpha$ and containing k. Conversely, whenever k is a line on $\mathcal{H} \cap M$, the plane $k + P$ is a generator of $\mathcal{H}$ passing through P. Suppose that there is a point $R \neq P$ of $\mathcal{R}_\alpha \cap \pi$. Then $R \in P^{\mathcal{U}} = P^{\mathcal{B}_\alpha}$ and so PR is a line on $\mathcal{R}_\alpha$ that necessarily meets k. It follows that k meets the $\mathcal{Q}^+(3, q^2)$ formed by the intersection of $\mathcal{R}_\alpha$ and M. Conversely any line k of $\mathcal{H} \cap M$ that meets $\mathcal{R}_\alpha$ gives rise to a generator $k + P$ that meets $\mathcal{R}_\alpha$ in at least a line. Thus the existence of a plane $\mathcal{H}$ meeting $\mathcal{R}_\alpha$ in the single point P is equivalent to the existence of a line of $\mathcal{H} \cap M$ that does not meet $\mathcal{R}_\alpha$.

Now consider lines of $\mathcal{H}(3, q^2)$ in relation to $\mathcal{R} = \mathcal{R}_\alpha \cap M$ and $\mathcal{Q} = \mathcal{Q}_\alpha \cap M$. This last is of the same type (elliptic or hyperbolic quadric) as $\mathcal{Q}_\alpha$. We write $\mathcal{S}$ for $\mathcal{S}_\alpha \cap M$ which happens to be $\mathcal{R} \cap \mathcal{H}$.

Suppose first that $\mathcal{Q}$ is elliptic. If a line of $\mathcal{H}$ met $\mathcal{Q}$ in two or more points, then it would extend a line on $\mathcal{Q}$ to $GF(q^2)$, but $\mathcal{Q}$ has no such line.

Hence a line of $\mathcal{H}$ meets $\mathcal{Q}$ in at most 1 point. Each of the q^2+1 points of $\mathcal{Q}$ lies on $q+1$ lines of $\mathcal{H}$, so $(q+1)(q^2+1)$ lines of $\mathcal{H}$ meet $\mathcal{Q}$ in one point. There are $(q+1)(q^3+1)$ lines on $\mathcal{H}$, so there are $(q+1)(q^3-q^2)$ lines that do not meet $\mathcal{Q}$. In this (elliptic) case, $\mathcal{S}=\mathcal{Q}$, so there are $(q+1)(q^3-q^2)$ lines of $\mathcal{H}$ that do not meet $\mathcal{R}$. Hence there exists a plane of $\mathcal{H}$ meeting $\mathcal{R}_\alpha$ in the single point P.

Now suppose that $\mathcal{Q}$ is hyperbolic. There are potentially 4 types of line of $\mathcal{H}$ when classified in terms of the intersection with $\mathcal{Q}$ and $\mathcal{S}$: lines of $\mathcal{S}$ (i.e., $GF(q^2)$ extensions of lines of $\mathcal{Q}$) - there are $2(q+1)$ of these; tangent lines to $\mathcal{Q}$ - there are $(q+1)^2$ points of $\mathcal{Q}$ and through each point there are $q+1$ lines of $\mathcal{H}$ of which 2 are lines of $\mathcal{S}$ so there are $(q-1)(q+1)^2$ tangents altogether; there are lines that meet $\mathcal{S}$ in 2 points not on $\mathcal{Q}$ and lines that don't meet $\mathcal{S}$ at all. In the third class we can choose a first point X in $2(q+1)(q^2-q)$ ways and the second point $Y=X^{\mathcal{U}}\cap m$ for one of q possible lines m on $\mathcal{S}$ arising from the same regulus as X but not containing X (if m were from the opposite regulus, the two lines would meet and span a plane on $\mathcal{H}$); given that each line is counted twice in this process, we have $q(q+1)(q^2-q)$ lines of this type. We have now accounted for $(q+1)(q^3+1)$ lines on $\mathcal{H}$, i.e., all of them. Therefore there are no lines of $\mathcal{H}$ that do not meet $\mathcal{S}$ (incidentally this also confirms that we have identified all possible types of line). Hence every plane of $\mathcal{H}$ that contains P contains a line of $\mathcal{R}_\alpha$.

□

Corollary 5.3. Suppose $n=5$ and that π is a plane of $\mathcal{H}$ passing through $P\in\mathcal{Q}_\alpha\backslash\mathcal{P}_0$ that does not meet $\mathcal{P}_0$. If $\mathcal{Q}_\alpha$ is elliptic, then $\pi\cap\mathcal{R}_\alpha$ is the single point P, while if $\mathcal{Q}_\alpha$ is hyperbolic, then $\pi\cap\mathcal{R}_\alpha$ is a pair of lines meeting in P, and intersecting $\mathcal{Q}_\alpha$ in P.

Proof. We observe that $\pi\cap\mathcal{R}_\alpha$ is a conic. Moreover $\pi\subset P^{\mathcal{U}}=P^{\mathcal{B}_\alpha}$ so the conic is degenerate. The possibilities for a degenerate conic are: a point, a line, a pair of lines and a plane. In the notation of the previous lemma, the line $k=\pi\cap\Delta$ cannot here meet $\mathcal{Q}$. There are then four possibilities for the way in which k interacts with $\mathcal{S}$: it can be disjoint from $\mathcal{S}$, it can meet $\mathcal{S}$ in one point, it can meet $\mathcal{S}$ in two points, or it can meet $\mathcal{S}$ in a line. The second and fourth possibilities do not occur at all (because π does not meet $\mathcal{P}_0$). The first possibility corresponds to the elliptic case and the third possibility to the hyperbolic case.

□

Proposition 5.4. Suppose that $n = 5$ and that P is a point of $\mathcal{Q}_\alpha \setminus \mathcal{P}_0$ and let π be a plane on $\mathcal{H}$ such that $\pi \cap \mathcal{Q}_\alpha = \{P\}$. Then π does not meet $\mathbf{B}_5 \setminus \{P\}$.

Proof. Suppose that π meets a $\mathcal{Q}_\beta$ ($\beta \neq \alpha$) in a point R.

Suppose that $\mathcal{Q}_\alpha$ and $\mathcal{Q}_\beta$ are both hyperbolic. By Corollary 5.3, $\pi \cap \mathcal{R}_\alpha$ is a pair of lines meeting in P and $\pi \cap \mathcal{R}_\beta$ is a pair of lines meeting in R. Each of the given lines through P meets each of the given lines through R, giving 4 non-collinear points in π, each lying in $\mathcal{R}_\alpha \cap \mathcal{R}_\beta$. But $\mathcal{R}_\alpha \cap \mathcal{R}_\beta$ is a parabolic quadric in Δ, implying that π lies in Δ, a contradiction.

Suppose that one of $\mathcal{Q}_\alpha$ and $\mathcal{Q}_\beta$ is elliptic - we may assume that $\mathcal{Q}_\alpha$ is elliptic. As we have already seen, $M = P^{\mathcal{U}} \cap \Delta$ is non-degenerate 3-space fixed by $\mathcal{V}_\alpha$ so it extends a non-degenerate 3-subspace of Δ_0, and $k = \pi \cap \Delta$ is a line of $\mathcal{H}(3, q^2) = \mathcal{H} \cap M$ that is external to $\mathcal{Q}^+(3, q^2) = \mathcal{R}_\alpha \cap M$; note that k and $\mathcal{V}_\alpha(k)$ are disjoint. Arguing as before, as X varies on k the $q^2 + 1$ lines $\ell(X) = \langle X, \mathcal{V}_\alpha(X)\rangle$ extend lines $\ell(X)_0$ of M_0 that form a spread. Note that M_0 meets both $\mathcal{H}(3, q^2)$ and $\mathcal{Q}^+(3, q^2)$ in an elliptic quadric, so none of the lines $\ell(X)_0$ can lie on the quadric. Moreover each $\ell(X)$ contains at least 2 points of $\mathcal{H}(3, q^2)$ so no $\ell(X)_0$ can be tangent to the elliptic quadric. Hence each $\ell(X)_0$ is non-degenerate. Now consider $R^{\mathcal{U}}$: it cannot contain M, since otherwise $M^{\mathcal{U}}$ would be PR which lies on $\mathcal{H}$. Therefore $R^{\mathcal{U}} \cap M$ is a plane containing k. In particular $R^{\mathcal{U}}$ meets $\mathcal{V}_\alpha(k)$ in a point $\mathcal{V}_\alpha(Y)$, and now the non-degenerate line $\ell = \ell(Y)$ lies in $P^{\mathcal{U}} \cap R^{\mathcal{U}}$. Put another way, P, R both lie in $\ell^{\mathcal{U}}$. The line $\ell_0 = \ell(Y)_0$ lies in Δ_0, so by Lemma 3.1, $\ell^\perp \cap \mathbf{B}_5$ has the structure of $\mathbf{B}_3$. Observe that P, R both lie on the line $\pi \cap \ell^{\mathcal{U}}$. In other words $\langle P, R\rangle$ is a generator of $\mathcal{H}(3, q^2) = \mathcal{H} \cap \ell^\perp$ that meets $\mathbf{B}_3$ in at least 2 points. It is shown in [1] that this cannot occur. This contradiction establishes that this case cannot occur either.

□

Theorem 5.5. $\mathbf{B}_5$ is a minimal blocking set of $\mathcal{H}(5, q^2)$ with respect to generators.

Proof. Let P be any point of $\mathbf{B}_5$, say P lies in $\mathcal{Q}_\alpha \setminus \mathcal{P}_0$ and let π be a plane on $\mathcal{H}$ such that $\pi \cap \mathcal{Q}_\alpha = \{P\}$. By Proposition 5.4, π meets $\mathbf{B}_5$ in the single point P, so π is a generator of $\mathcal{H}$ that does not meet $\mathbf{B}_5 \setminus \{P\}$. It follows that $\mathbf{B}_5 \setminus \{P\}$ is not a blocking set, so P is essential for every point P. Hence $\mathbf{B}_5$ is a minimal blocking set.

□

Theorem 5.6. If $n \geq 7$ is odd, then $\mathbf{B}_n$ is a minimal blocking set.

Proof. Let P be any point of $\mathbf{B}_n$, say P lies in $\mathcal{Q}_\alpha \setminus \mathcal{P}_0$ and let π be a generator of $\mathcal{H}$ such that $\pi \cap \mathcal{Q}_\alpha = \{P\}$. Suppose π meets $\mathcal{Q}_\beta$ in R for some $\beta \neq \alpha$. Construct $M = P^{\mathcal{U}} \cap \Delta, k = \pi \cap M$ and $\mathcal{V}_\alpha(k)$ as before. Note here that $\mathcal{V}_\alpha(k) = (k^{\mathcal{U}})^{\mathcal{B}_\alpha} = k^{\mathcal{B}_\alpha}$ (where here we regard $\mathcal{V}_\alpha, \mathcal{U}$ and $\mathcal{B}_\alpha$ as restricted to M), and $k, \mathcal{V}_\alpha(k)$ are disjoint so they are non-degenerate with respect to $\mathcal{B}_\alpha$. As argued before, the subspace $R^{\mathcal{U}}$ contains k but not M, so it meets $\mathcal{V}_\alpha(k)$ in an $(r-2)$-dimensional subspace (where $r = (n-1)/2$). Consider $W = R^{\mathcal{U}} \cap \mathcal{V}_\alpha(k)$ as a subspace of $\mathcal{V}_\alpha(k)$: since $\mathcal{V}_\alpha(k)$ is non-degenerate with respect to $\mathcal{B}_\alpha$, the subspace $Z = W \cap W^{\mathcal{B}_\alpha}$ is either empty or is a single point and hence a complement of Z in W has dimension at least $r-3$. Moreover such a complement must be non-degenerate with respect to $\mathcal{B}_\alpha$, so W contains a subspace N of dimension $r-3$ that is non-degenerate with respect to $\mathcal{B}_\alpha$. Then $N + \mathcal{V}_\alpha(N)$ is a subspace of Δ fixed by $\mathcal{V}_\alpha$, is non-degenerate with respect to both $\mathcal{B}_\alpha$ and $\mathcal{U}$, and has dimension $2r - 5 = n - 6$. Hence $E = (N + \mathcal{V}_\alpha(N))^{\mathcal{U}}$ is a non-degenerate subspace fixed by $\mathcal{V}_\alpha$ of dimension 5 that contains P. For each α, the restriction $\mathcal{B}_\alpha|_E$ commutes with $\mathcal{U}|_E$. The corresponding quadrics are $\mathcal{Q}_\alpha \cap E$, any two intersecting in $\mathcal{P}_0 \cap E$. Consider the set $\mathbf{B}_5 = \cup_\alpha(\mathcal{Q}_\alpha \cap E) \setminus (\mathcal{P}_0 \cap E)$ and the generator $\pi \cap E$ of $\mathcal{H}(5, q^2) = \mathcal{H} \cap E$: clearly $\pi \cap \mathcal{Q}_\alpha \cap E = \{P\}$. On the one hand, by Proposition 5.4, $\pi \cap E$ does not meet $\mathbf{B}_5 \setminus \{P\}$. On the other hand $N + \mathcal{V}_\alpha(N) \subseteq R^{\mathcal{U}}$, so $R \in E \cap \mathcal{Q}_\beta \cap \pi$ and therefore $R \in (\mathbf{B}_5 \setminus \{P\}) \cap (\pi \cap E)$. The contradiction proves that $\pi \cap \mathbf{B}_n = \{P\}$. Hence each $P \in \mathbf{B}_n$ is essential and $\mathbf{B}_n$ is a minimal blocking set.

6. Linear blocking sets and the size of $\mathbf{B}_n$

We recall here the notion of a linear blocking set as described by Metsch in [6]. A blocking set can be defined with respect to k-dimensional subspaces on $\mathcal{H}$, i.e., a set of points that meets each k-dimensional subspace on $\mathcal{H}$. Any $(n-k)$-dimensional subspace W of $PG(n, q^2)$ will be a blocking set with respect to k-dimensional subspaces on $\mathcal{H}$, indeed so will $W \cap \mathcal{H}$. This motivates Metsch to define a *linear* blocking set of $\mathcal{H}(n, q^2)$ with respect to k-dimensional subspaces to be a blocking set that lies in some $(n-k)$-dimensional subspace of $PG(n, q^2)$. Metsch states that $(W \setminus W^{\mathcal{U}}) \cap \mathcal{H}$ is a unique minimal blocking set inside $W \cap \mathcal{H}$ when $k < (n-1)/2$. This remains the case when $k = (n-1)/2$. We note that a different usage of the term 'linear blocking set' was introduced for projective planes by Lunardon in [5] and generalized for $PG(n,q)$ by Sziklai in [8].

We consider here the sizes of linear blocking sets (with respect to $(n-1)/2$-dimensional subspaces) and compare with sizes of $\mathbf{B}_n$. Let $r=(n-1)/2$. Then W is an $(r+1)$-dimensional subspace of $PG(n,q^2)$ and $R=W\cap W^{\mathcal{U}}$ is the *radical* of W: it has the property that any complement of R in W is non-degenerate. If the dimension of R is t (with necessarily $0\le t\le r-1$), then any complement has dimension $r-t$. Thus the number of points of $\mathcal{H}$ in W is $|\mathcal{H}(r-t,q^2)|(1+(q^2-1)|R|)+|R|=|\mathcal{H}(r-t,q^2)|q^{2t+2}+|R|$ and thus the number of points of $\mathcal{H}$ in $W\setminus R$ is $|\mathcal{H}(r-t,q^2)|q^{2t+2}=q^{2t+2}(q^{r-t+1}-(-1)^{r-t+1})(q^{r-t}-(-1)^{r-t})/(q^2-1)$ (from [3] for example): if R is empty, then the number of points of $\mathcal{H}$ in $W\setminus R$ corresponds to taking $t=-1$. In particular, when $t=r-1$, the figure is $q^{2r}(q+1)=q^{n-1}(q+1)$. The smallest value occurs when taking $t=-1$ and is $(q^{r+2}-(-1)^{r+2})(q^{r+1}-(-1)^{r+1})/(q^2-1)$.

In turning to $\mathbf{B}_n$, we first note that each secant line to $\mathcal{Q}_\alpha$ in Σ_α passing through $(1,0\ldots,0)$ contains two points of $\mathbf{B}_n$, which leads to the conclusion that $\mathbf{B}_n$ spans $PG(n,q^2)$ and is thus a non-linear blocking set. In considering the size of $\mathbf{B}_n$, we observe that the numbers of points on the quadrics $Q^+(n,q)$, $Q^-(n,q)$ and $Q(n-1,q)$ are respectively $(q^{r+1}-1)(q^r+1)/(q-1)$, $(q^{r+1}+1)(q^r-1)/(q-1)$ and $(q^r-1)(q^r+1)/(q-1)$ (again from [3]), from which we can calculate that $|\mathbf{B}_n|=q^{2r}(q+1)=q^{n-1}(q+1)$. It is not difficult to show that the size of $\mathbf{B}_n$ coincides with the size of the largest linear blocking set, namely that arising from $t=r-1$.

References

[1] A. Cossidente, Some constructions on the Hermitian surface, Des. Codes Cryptogr. 51 (2009), no. 2, 123-129.

[2] M. Cimrakova, J. De Beule and V. Fack, On small minimal blocking sets in classical generalized quadrangles, preprint.

[3] J.W.P. Hirschfeld, J.A. Thas, *General Galois Geometries*, Oxford University Press, Oxford, 1991.

[4] J. De Beule, K. Metsch, The smallest point sets that meet all generators of $H(2n,q^2)$. Discrete Math. 294 (2005), no. 1–2, 75-81.

[5] G Lunardon, Normal Spreads, Geometriae Dedicata 75 (1999): 245-261.

[6] K. Metsch, Blocking structures of Hermitian varieties. Des. Codes Cryptogr. 34 (2005), no. 2–3, 339–360.

[7] B. Segre, Forme e geometrie Hermitiane con particolare riguardo al caso finito, Ann. Mat. Pura Appl. 70 (1965), 1–201.

[8] P. Sziklai, On small blocking sets and their linearity, J. Comb. Th. A 115 (2008) 1167-1182.

[9] J. Tits, Sur certain classes d'espaces homogénes de groupes de Lie, Acad. Roy. Belg. Cl. Sci. Mém. Collect. 8 XXIX (1955).