Available online at www.sciencedirect.com

SciVerse ScienceDirect

Electronic Notes in Discrete Mathematics 40 (2013) 347–351

Electronic Notes in DISCRETE MATHEMATICS

www.elsevier.com/locate/endm

New blocking semiovals in $\mathrm{PG}(2, 5^2)$ with a large homology group

Alessandro Siciliano [1]

Dipartimento di Matematica, Informatica ed Economia
Università della Basilicata
Potenza, Italy

Nicola Durante [2]

Dipartimento di Matematica ed Applicazioni "R. Caccioppoli"
Università di Napoli "Federico II"
Napoli, Italy

Abstract

A *blocking semioval* in a projective plane is a set of points which is both a semioval and a blocking set. In this paper, blocking semiovals in the Desaguesian projective plane $\mathrm{PG}(2, s^2)$ admitting an order $s+1$ homology group are considered. By looking at the geometry of the orbits on points of such a group we find two new blocking semiovals of large size in $\mathrm{PG}(2, 5^2)$.

Keywords: Projective planes, Blocking set, Semioval, Blocking semioval.

A *blocking set* in a projective plane Π is a set of points $\mathcal{B}$ with the property that every line meets $\mathcal{B}$ nontrivially, and no line of Π is contained in $\mathcal{B}$. A *semioval* in Π is a set of points $\mathcal{O}$ with the property that for every point P of

[1] Email: alessandro.siciliano@unibas.it
[2] Email: ndurante@unina.it

http://dx.doi.org/10.1016/j.endm.2013.05.061

$\mathcal{O}$, there exists exactly one tangent at P i.e., a line of Π meeting $\mathcal{O}$ precisely in P. A *blocking semioval* in Π is a set of points $\mathcal{S}$ which is both a blocking set and a semioval.

While the study of blocking semiovals was originally motivated by Batten [1] in connection with cryptography, these geometric objects are interesting in their own right since blocking semiovals are necessarily minimal blocking sets and also maximal semiovals.

Hubaut [8] (and independently Thas [11]) gave an upper bound on the size of a blocking semioval $\mathcal{S}$ namely, $|\mathcal{S}| \leq q\sqrt{q}+1$ and the equality holds if and only if $\mathcal{S}$ is a unital [2]. The lower bound $2q+\sqrt{2q-\frac{47}{7}}-\frac{1}{2}$ on the size of blocking semiovals in the Desarguesian projective plane $\mathrm{PG}(2,q)$ was recently proved by Dover [5].

Apart from unitals there is a further well-known example of blocking semioval namely, the *vertexless triangle*.

In the paper [4] Dover reported a different family of blocking semiovals of size $3q-4$ in any projective plane of order q containing a $\Delta-$configuration (we refer to [4] for the definition of $\Delta-$configuration). Suetake constructed three new families of blocking semiovals in the desarguesian projective plane $\mathrm{PG}(2,q)$ [9]. These families contain the family found by Dover as special cases. In the paper [7], five infinite families are added and four sporadic examples in $\mathrm{PG}(2,7)$ were described. Very recently, Dover, Mellinger and Wantz provide new constructions of blocking semiovals containing conics [6].

The problem of classifying blocking semiovals was posed by Batten at the CMS Special Session in Finite Geometry in 1997 but computer results applied to desarguesian projective plane of small order suggest that a complete classification of blocking semiovals is intractable [7]. Thus, it becomes quite natural to look at blocking semiovals with some interesting properties. Among the others, one approach is looking at blocking semiovals which admit certain central collineation groups [10].

Here we are interested in blocking semiovals of desarguesian projective planes of square order which are invariant under the action of a *large* homology group: In $\mathrm{PG}(2,s^2)$ we consider the unique homology group H of order $s+1$.

In the following we will denote by K^* the set of non-zero elements of any K.

Let $\mathrm{PG}(2,s^2)$ be the projective plane over $\mathrm{GF}(s^2)$, with s a prime power, modeled by a three-dimensional vector space over $\mathrm{GF}(s^2)$ using homogeneous coordinates. Point coordinates are denoted by (x,y,z), while line coordinates are written as $[x,y,z]$.

Let H denote the unique order $q+1$ subgroup of the homology group with center C and axis ℓ. Without loss of generality, we may assume $C=(0,0,1)$ and $\ell=[0,0,1]$. Then any collineation $h_\delta \in H$ is defined by

$$h_\delta(x,y,z)=\begin{pmatrix}1&0&0\\0&1&0\\0&0&\delta\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}$$

with $\delta \in \mathrm{GF}(s^2)^*$ an $(s+1)-$th root of unity. It turns out that the non-singeton orbits of H are the Baer sublines

$$B_{\beta,a}=\{(1,\beta,x): x^{s+1}=a\},\ B_{\infty,a}=\{(0,1,x): x^{s+1}=a\}$$

with $a \in \mathrm{GF}(s)^*$ and $\beta \in \mathrm{GF}(s^2)$.

Let $\mathcal{S}$ be a $H-$invariant blocking semioval of $\mathrm{PG}(2,s^2)$. Then it is easily seen that the axis of H must be a secant of $\mathcal{S}$ and the center of H is not a point of $\mathcal{S}$. We also assume the following.

Assumption 1: Any line through the center C intersects $\mathcal{S}$ in exactly one point-orbit.

Let $P_i=(1,\beta_i,0)\in\ell$, $i=1,\dots,n$. We write $\mathcal{S}=(\ell\setminus\{P_1,\dots,P_n\})\cup B_{\beta_1,a_1}\cup\ldots\cup B_{\beta_n,a_n}$ where $a_i\in\mathrm{GF}(s)^*$.

Let $\zeta\in\mathrm{GF}(s^2)\setminus\mathrm{GF}(s)$. We take $\{1,\zeta\}$ as a basis for $\mathrm{GF}(s^2)$ over $\mathrm{GF}(s)$.

Let us consider the affine plane $\mathrm{AG}(2,s^2)$ with respect to the line at infinity $x=0$. Let $\mathrm{AG}(3,s)$ denote the 3−dimensional affine space coordinatized by the finite field $\mathrm{GF}(s)$.

The map

$$\begin{aligned}\psi:\mathrm{AG}(2,s^2) &\longrightarrow \quad \mathrm{AG}(3,s)\\ (\beta,\alpha) &\longmapsto (b_0,b_1,\alpha^{s+1})\end{aligned} \tag{1}$$

where $b_0+b_1\zeta=\beta$, defines a one-to-one correspondence between the $H-$orbits on points of $\mathrm{AG}(2,s^2)$ and points of $\mathrm{AG}(3,s)$.

The image of lines of $\mathrm{AG}(2,s^2)$ under the map ψ are of three different types:

I. The line $[-\beta,1,0]$, with $\beta=b_0+b_1\zeta$ is mapped into the line $L_\beta=\{(b_0,b_1,a): a\in\mathrm{GF}(q)\}$ of $\mathrm{AG}(3,s)$;

II. The $H-$orbit of $[-\alpha,0,1]$, with $\alpha^{s+1}=a$ is mapped into the affine plane $\pi_a=\{(b_0,b_1,a): b_0,b_1\in\mathrm{GF}(q)\}$;

III. The $H-$orbit of $[\alpha\beta, -\alpha, 1]$, with $\alpha^{s+1} = a \neq 0$ is mapped into the elliptic quadric $Q_{\beta,a} = \{(\lambda, \mu, a((\lambda - b_0)^2 + t_1(\lambda - b_0)(\mu - b_1) - t_0(\mu - b_1)^2)) : \lambda, \mu \in \mathrm{GF}(s)\}$.

Let $\mathcal{F}$ denote the set of the quadrics $Q_{\beta,a}$. A *blocking semioval with respect to* $\mathcal{F}$ is a set of points $\mathcal{S}'$ in $\mathrm{AG}(3, s)$ with the following properties:

(i) every quadric of $\mathcal{F}$ meets $\mathcal{S}'$ nontrivially, and no quadric of $\mathcal{F}$ is contained in $\mathcal{S}'$,

(ii) for every point P of $\mathcal{S}'$, there exists exactly one quadric of $\mathcal{F}$ meeting $\mathcal{S}'$ precisely in the point P.

Let $\mathcal{S}$ be an $H-$invariant blocking semioval in $\mathrm{PG}(2, s^2)$ with Assumption 1. Then the set $\mathcal{S}' = \psi(\mathcal{S} \setminus \ell) \subset \mathrm{AG}(3, s)$ satisfies the following properties:

(P1) $\mathcal{S}' \cap \pi_0 = \emptyset$, $\mathcal{S}' \cap \pi_a \neq \emptyset$ and $\pi_a \not\subset \mathcal{S}'$, for all $a \in \mathrm{GF}(s)^*$,

(P2) $|L \cap \mathcal{S}'| \in \{0, 1\}$ for any affine line L through $P_\infty = (0, 0, 0, 1)$,

(P3) $\mathcal{S}'$ is a blocking semioval with respect to the family $\mathcal{F}$,

(P4) $\{Q_{\beta,a} \cap \pi_0 : Q_{\beta,a}$ is a tangent to $\mathcal{S}'\} \subseteq \Gamma'$ where Γ' is the projection of $\mathcal{S}'$ on π_0 from P_∞.

The reverse also holds.

Theorem 1.1 *Let $\mathcal{S}'$ be a set of points in $\mathrm{AG}(3, s)$ satisfying properties (P1), (P2), (P3), (P4) and Γ' denote the projection of $\mathcal{S}'$ on π_0 from P_∞. Set $\mathcal{I} = \pi_0 \setminus \Gamma'$. Then the set $\mathcal{S} = \psi^{-1}(\mathcal{S}' \cup \mathcal{I}) \cup \{(0, 1, 0)\}$ is a ($H-$invariant) blocking semioval of size $(s + 1)|\mathcal{S}'| + |\mathcal{I}| + 1$ in $\mathrm{PG}(2, s^2)$.*

In $\mathrm{PG}(2, s^2)$, a classical unital containing $(1, 0, 0), (0, 1, 0)$ with tangents ℓ_0 at $(1, 0, 0)$ and ℓ_∞ at $(0, 1, 0)$, has equation $\mathcal{U}_\alpha : z^{s+1} = \alpha y^s + \alpha^s y$ with $\alpha \in \mathrm{GF}(s^2)^*$.

It is easily seen that $\mathcal{U}_\alpha$ is $H-$invariant and that there are $s^2 - 1$ such unitals. If $\alpha = a_0 + \zeta a_1$, then $\psi(\mathcal{U}_\alpha \setminus \{(0, 1, 0)\})$ is a plane in $AG(3, s)$, which we denote by π_{a_0,a_1}, whose projective closure contains neither P_∞ nor the line $\langle(0, 1, 0, 0), (0, 0, 1, 0)\rangle$.

Proposition 1.2 *The map ψ defines a one-to-one correspondence between the set of the unitals $\mathcal{U}_\alpha$ and the set of (affine) planes in $\mathrm{PG}(3, s)$ containing neither P_∞ nor $\langle(0, 1, 0, 0), (0, 0, 1, 0)\rangle$.*

By using MAGMA [3], we found two projectively inequivalent sets of points in $\mathrm{AG}(3, s)$ satisfying (P1), (P2), (P3) and (P4) which are not affine planes. Both sets have the following geometric properties:

i) $|\mathcal{S}'| = m(s-1)$ with $m = 3, 4$

ii) $\mathcal{I}$ is union of $s+1-m$ affine lines of π_0 through the origin

iii) every plane π_a, $a \in \mathrm{GF}(s)^*$ intersects $\mathcal{S}'$ in m points.

Therefore, such sets yield blocking semiovals in $\mathrm{PG}(2, 5^2)$ of size $|\mathcal{S}| = m(5^2-1) + (5^2 - m(5-1)) + 1 \in \{86, 106\}$.

Among the formerly known semiovals in $\mathrm{PG}(2, 5^2)$ apart from unitals, just the blocking semiovals constructed in [6] have size 86, but our examples do not contain conics. This implies that the blocking semiovals we found are new. Based upon the properties above, we are hopeful that the two examples we found would generalize to Desarguesian projective planes of higher order.

References

[1] L.M. Batten, *Determining sets*, Australas. J. Combin. **22** (2000), 167–176.

[2] A.A. Bruen, J.A. Thas, *Blocking sets*, Geom. Dedicata **6** (1977), 193–203.

[3] J. Cannon, C. Playoust, MAGMA, University of Sidney, Sydney, 1993.

[4] J.M. Dover, *A lower bound on blocking semiovals*, European J. Combin. **21** (2000), 571–577.

[5] J.M. Dover, *Some new results on blocking semiovals*, Australas. J. Combin. **52** (2012), 269–280.

[6] J.M. Dover, K.E. Mellinger, K.L. Wantz, *Blocking semiovals containing conics*, Adv. Geom. DOI: 10.1515/advgeom-2012-0025.

[7] J.M. Dover, B.B. Ranson, *Blocking semiovals in* $\mathrm{PG}(2,7)$ *and beyond*, European J. Combin. **24** (2003), 183–193.

[8] X. Hubaut, *Limitation du nombre de points d'un* $(k,n)-$*arc règulier d'un plan projectif fini*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **48** (1970), 490–493.

[9] C. Suetake, *Two families of blocking semiovals*, European J. Combin.**21** (2000), 973–980.

[10] C. Suetake, *Some blocking semiovals which admit a homology group*, European J. Combin. **21** (2000), 967–972.

[11] J.A. Thas, *On semi ovals and semi ovoids*, Geom. Dedicata **3** (1974), 229–231.