Serdica J. Computing **6** (2012), 175–184

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ON BLOCKING SETS IN AFFINE HJELMSLEV PLANES*

Stoyan Boev, Ivan Landjev

Abstract. We prove that the minimum size of an affine blocking set in the affine plane $\mathrm{AHG}({}_RR^2)$, $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$, is $q(2q-1)$ for all planes over chain rings R with $|R| = 4, 9$ or 16.

1. Introduction. In this paper, we study the problem of finding the minimal size of a blocking set in an affine Hjelmlsev plane over a chain ring of nilpotency index 2. A classical result by [1, 2, 6] says that the minimal size of a blocking set in an affine plane over a finite field is $2q-1$. All known proofs of this result use the so-called polynomial method which does not have an analogue for finite chain rings. An obvious upper bound for the cardinality of a blocking set in $\mathrm{AHG}({}_RR^2)$ with $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$, is $q(2q-1)$. An interesting question is whether this value is the best possible one, in other words, whether there exist blocking sets of size smaller than $q(2q-1)$.

ACM Computing Classification System (1998): G.2.1.

Key words: finite chian rings, affine Hjelmslev plane, affine blocking sets.

*This research has been supported by the Scientific Research Fund of Sofia University under Contract No 109/09.05.2012.

In this paper, we prove that for the chain rings with $q^2 = 4, 9, 16$ the smallest size is indeed $q(2q-1)$.

2. Basic Results and Facts. We consider Hjelmslev planes over chain rings of nilpotency index 2, i.e. chain rings with $\operatorname{rad} R \neq (0)$ and $(\operatorname{rad} R)^2 = (0)$. Thus $|R| = q^2$, where $R/\operatorname{rad} R \cong \mathbb{F}_q$. Chain rings with this property have been classified in [3, 9]. If $q = p^r$ there are exactly $r+1$ isomorphism classes of such rings. These are:

- for every $\sigma \in \operatorname{Aut} \mathbb{F}_q$ the ring $R_\sigma \cong \mathbb{F}_q[X;\sigma]/(X^2)$ of the so-called σ-dual numbers over $\mathbb{F}_q$ with underlying set $\mathbb{F}_q \times \mathbb{F}_q$, component-wise addition and multiplication given by $(a_0 + Xa_1)(b_0 + Xb_1) = a_0b_0 + X(a_1b_0 + a_0^\sigma b_1)$;
- the Galois ring $\mathrm{GR}(q^2, p^2) \cong \mathbb{Z}_{p^2}[X]/(f(X))$, where $f(X) \in \mathbb{Z}_{p^2}[X]$ is a monic polynomial of degree r, which is irreducible modulo p.

Let R be a finite chain ring of nilpotency index 2 and let $\operatorname{rad} R = \theta R = R\theta$ for some $\theta \in \operatorname{rad} R \setminus (0)$. Consider the module $M = {}_RR^3$ and define the sets $\mathcal{P}$ and $\mathcal{L}$ by

$$\mathcal{P} = \{Rx \mid x \in H\}, \quad \mathcal{L} = \{Rx + Ry \mid x, y \text{ linearly independent}\},$$

as well as an incidence relation $I \subseteq \mathcal{P} \times \mathcal{L}$ by set-theoretical inclusion. For the incidence structure $(\mathcal{P}, \mathcal{L}, I)$ define also a neighbour relation $\frown$ by the following axioms:

(N1) the points $X, Y \in \mathcal{P}$ are neighbours ($X \frown Y$) iff there exist two different lines incident with both of them;

(N2) the lines $s, t \in \mathcal{L}$ are neighbours ($s \frown t$) iff there exist two different points incident with both of them.

The incidence structure $\Pi = (\mathcal{P}, \mathcal{L}, I)$ with the neighbour relation $\frown$ is called the (left) projective Hjelmslev plane over R and is denoted by $\mathrm{PHG}({}_RR^3)$. The relation $\frown$ is an equivalence relation on $\mathcal{P}$ and on $\mathcal{L}$. The class $[X]$ of all points which are neighbours to the point $X = xR$ consists of all free rank 1 submodules contained in $xR + M\theta$. The class $[s]$ of all lines which are neighbours to $s = xR + yR$ contains all free rank 2 submodules contained in $xR + yR + M\theta$.

The next four theorems provide basic knowledge about the structure of projective Hjelmslev planes over finite chain rings. They are special cases of more general results (cf. [4, 5] and the references there).

Theorem 1. *Let* $\Pi = \mathrm{PHG}(R_R^3)$*, where* R *is a chain ring with* $|R| = q^2$*,* $R/\operatorname{rad} R \cong \mathbb{F}_q$*. Then*

(*i*) $|\mathcal{P}| = |\mathcal{L}| = q^2(q^2 + q + 1)$*;*

(*ii*) *every point(line) has* q^2 *neighbours;*

(*iii*) *every point (line) is incident with* $q(q + 1)$ *lines (points);*

(*iv*) *given a point* P *and a line* l *with* PIl*, there exist exactly* q *points on* l *which are neighbours to* P *and exactly* q *lines through* P *which are neighbours to* l*.*

Denote by π the natural homomorphism $\pi\colon R^3 \to R^3/R^3\theta$. It induces a mapping acting on the submodules of R^3 which is denoted again by π. For every point X and every line l, we have

$$[X] = \{Y \in \mathcal{P} | \pi(Y) = \pi(X)\}, \ \ [s] = \{t \in \mathcal{L} | \pi(t) = \pi(s)\}.$$

Denote by $\mathcal{P}^{(1)}$ (respectively $\mathcal{L}^{(1)}$) the set of all neighbour classes of points (respectively, neighbour classes of lines).

Theorem 2. *The incidence structure* $(\mathcal{P}^{(1)}, \mathcal{L}^{(1)}, I^{(1)})$ *with* $I^{(1)}$ *defined by*

$$[X]\, I^{(1)}\, [s] \Leftrightarrow \exists X' \in [X], \exists s' \in [s] \ : \ X'\, I\, s'$$

is isomorphic to the projective plane $\mathrm{PG}(2, q)$*.*

Let $\Pi = (\mathcal{P}, \mathcal{L}, I) = \mathrm{PHG}(R_R^3)$. Given a point P, denote by $\mathcal{L}(P)$ the set of all lines of $\mathcal{L}$ incident with points from $[P]$. For two lines $s, t \in \mathcal{L}$ we write $s \sim t$ if s and t coincide on $[P]$. Denote by $\mathcal{L}_1$ a complete set of representatives of the lines from $\mathcal{L}(P)$.

Theorem 3.

$$([P], \mathcal{L}_1, I|_{[P]\times\mathcal{L}_1}) \cong \mathrm{AG}(2, q).$$

Let l be a line in Π. Define $\mathfrak{P}$ by $\mathfrak{P} = \{s \cap [X] \mid X \bigcirc l, s \in \mathcal{L}, s \bigcirc l\} \cup \{P_\infty\}$ and an incidence relation $\mathfrak{I} \subseteq \mathfrak{P} \times \mathcal{L}$ by

$$(s \cap [P])\mathfrak{I}t \Longleftrightarrow t \cap (s \cap [P]) \neq \emptyset, \ \ (P_\infty)\mathfrak{I}t \Longleftrightarrow t \not\bigcirc l.$$

For two lines $l_1, l_2 \in \mathcal{L}$ we write $l_1 \sim l_2$ if they are incident under $\mathfrak{I}$ with the same elements of $\mathfrak{P}$. Denote by $\mathfrak{L}$ a set of lines containing exactly one representative from each equivalence class of $\mathcal{L}$ under $\sim$.

Theorem 4. *The incidence structure* $(\mathfrak{P}, \mathfrak{L}, \mathfrak{I} \mid_{\mathfrak{P}\times\mathfrak{L}})$ *is isomorphic to* $\mathrm{PG}(2, q)$.

By $\mathrm{AHG}({}_RR^2)$ we denote the (left) affine Hjelmslev plane over R, which is obtained by deleting a neighbourhood class of lines from $\mathrm{PHG}(R^3_R)$.

A set of points B in $\mathrm{AHG}\,{}_RR^2$ is called a k-blocking set if

(i) $|B| = k$;

(ii) $|B \cap L| \geq 1$ for every line L in $\mathrm{AHG}\,{}_RR^2$.

A k-blocking set B is called reducible if there exists a k'-blocking set B' with $B' \subsetneq B$. A blocking set that is not reducible is called irreducible.

3. Affine Blocking Sets in Small Planes. The problem of determining the smallest size of a blocking set in $\mathrm{AG}(2, q)$ has been solved by the so-called polynomial method. It is known to be $2q - 1$ where the upper bound is trivial and the lower bound has been proved by various authors [1, 2, 6].

It is natural to ask about the smallest blocking set in an affine Hjelmlsev plane. Unfortunately, the polynomial method does not work in the ring geometries. A trivial upper bound on the smallest size of a blocking set in $\mathrm{AHG}({}_RR^2)$ is $q(2q - 1)$. It is obtained by taking two intersecting lines that are not neighbours and deleting from the second one all its points in the common neighbour class apart from the intersection point of both lines. In this section, we are going to prove that this bound is sharp for the rings with 4, 9 and 16 elements.

We start with several important lemmas.

Lemma 1. *Let B be a blocking set in the affine plane* $\mathrm{AHG}({}_RR^2)$ *and L be a line in this plane with $|B \cap [L]| = q + \alpha$, where $0 \leq \alpha \leq q - 1$. Then for every neighbour class on points $[x]$:*

$$|B \cap [x]| \leq \alpha \quad \textit{or } |B \cap [x]| \geq q.$$

P r o o f. If $[L]$ contains a point class, $[x]$ say, with $\alpha < |B \cap [x]| < q$ then this point class has an empty segment with the direction of $[L]$. The q lines through this segment cannot be blocked by the points outside $[x]$ since their number is less than q. □

The next two lemmas imply the bound if there exists a "large" line in the affine plane.

Lemma 2. *Let B be a blocking set in the affine plane* $\mathrm{AHG}({}_RR^2)$, $|R| = q^2$. $R/\operatorname{rad} R \cong \mathbb{F}_q$. *If there exists a neighbour class of lines* $[L]$ *with* $|B \cap [L]| \geq q^2$ *then*

$$|B| \geq q(2q-1).$$

P r o o f. First assume that $|B \cap [L]| \geq q^2$. Consider the factor plane which is isomorphic to $\mathrm{AG}(2, q)$. There are $q-1$ line classes parallel to $[L]$ in this factor-plane. Each line class in $\mathrm{AHG}({}_RR^2)$ has itself the structre of a classical affine plane and its points are contained in q parallel neighbour lines from $\mathrm{AHG}({}_RR^2)$. Hence the points outside $[L]$ are contained in $q(q-1)$ parallel lines. These lines are not blocked by the points from $[L]$. Hence

$$|B| \geq q^2 + q(q-1) = q(2q-1).$$

Now assume that

$$q^2 - q \leq |B \cap [L]| \leq q^2 - 1.$$

There exists a point class $[x] \in [L]$ with $|B \cap [x] < q$. Hence $[x]$ has an unblocked line segment in each direction through $[x]$. The class $[x]$ is incident with $q+1$ line classes in the factor plane. In each of the line classes through $[x]$, different from $[L]$, there is a line segment in $[x]$. Hence we need at least q points to block the lines in each line class through $[x]$. Therefore

$$|B| \geq (q^2 - q) + q \cdot q = q(2q-1). \qquad \square$$

Let B be a blocking set in $\mathrm{AHG}({}_RR^2)$. By Lemma 2 we can assume without loss of generality that the number of points of B in each line class is between q and $q^2 - q - 1$.

Lemma 3. *Let B be a blocking set in the affine plane* $\mathrm{AHG}({}_RR^2)$, $|R| = q^2$. $R/\operatorname{rad} R \cong \mathbb{F}_q$. *Then for every line class* $[L]$

$$|B \cap [L]| \geq 2q - 1 - \lambda_0,$$

where λ_0 is the number of empty point classes in $[L]$.

Proof. Clearly, $[L]$ has the structure of an affine plane. The points from $B \cap [L]$ block all lines in the affine plane defined on $[L]$ except for the lines given by the empty point classes in $[L]$. We can block these lines by λ_0 points. Hence $|B \cap [L]| + \lambda_0 \geq 2q - 1$ and the result follows. □

Let us note that by this lemma a line class without empty point classes has a multiplicity of at least $2q - 1$.

Theorem 5. *Let R be a chain ring with* $|R| = 4$, $R/\operatorname{rad} R \cong \mathbb{F}_2$. *The minimal size of a blocking set in* $\mathrm{AHG}({}_RR^2)$ *is* 6.

Proof. The result follows immediately from Lemma 1 and 2. □

Theorem 6. *Let R be a chain ring with* $|R| = 9$, $R/\operatorname{rad} R \cong \mathbb{F}_3$. *The minimal size of a blocking set in* $\mathrm{AHG}({}_RR^2)$ *is* 15.

Proof. Assume there exists a blocking set B of size 14. Without loss of generality

$$3 \leq |B \cap [L] \leq 5. \tag{1}$$

Let $[L_0]$ be a line class of multiplicity 5. There is a point $[x]$ on $[L]$ for which $|B \cap [x]| = 0$ or 1. Denote by $[L_1]$, $[L_2]$, $[L_3]$ the other three lines through $[x]$ in the factor plane. By Lemma 1, each line $[L_i]$, $i = 1, 2, 3$, contains a point $[x_i] \in [L_i]$ with $|B \cap [x_i]| = 3$. But then we have

$$|B \cap \langle [x_1], [x_2] \rangle| \geq 6,$$

a contradiction to (1). □

For the chain rings of size 16 we need two preparatory lemmas.

Lemma 4. *Let R be a chain ring with* $|R| = 16$, $R/\operatorname{rad} R \cong \mathbb{F}_4$. *Let B be a blocking set in* $\mathrm{AHG}({}_RR^2)$ *with* $|B| = 27$. *Then* (*i*) *there is no line class* $[L_0]$ *with* $|B \cap [L_0]| = 11$*;*

(*ii*) *there is no line class* $[L_0]$ *with* $|B \cap [L_0]| = 10$*.*

Proof. By Lemmas 1 and 2, we have

$$4 \leq |B \cap [L]| \leq 11. \tag{2}$$

(i) Assume $[L_0]$ is a line with $|B \cap [L_0]| = 11$. Assume there exists a point $[x] \in [L_0]$ with $|B \cap [x]| \leq 1$. If $[L_i]$, $i = 1, \ldots, 4$, are the other four lines through $[x]$, there exist points $[x_i] \in [L_i]$, $i = 1, \ldots, 4$, with $|B \cap [x_i]| = 4$. No three of these points are collinear; otherwise there is a line of multiplicity 12, a contradiction to (2). Hence there is a point $[y] \in [L_0]$ such that the set $\{[x], [y], [x_1], \ldots, [x_4]\}$ is a hyperoval. All points outside $[L_0]$ different from $[x_i]$, $i = 1, \ldots, 4$, do not contain points from B.

Now let $[z] \in [L_0] \setminus \{[x], [y]\}$. We must have $|B \cap [z]| \geq 4$ since $[z]$ lies on an external line to the hyperoval. But then a secant $[M]$ to the hyperoval through $[z]$ has $|B \cap [M]| \geq 12$, a contradiction.

Now let $[x] \in [L_0]$ be a class with $|B \cap [x]| = 2$ and let $[L_i]$, $i = 1, \ldots, 4$, be the other four lines through $[x]$. Since the lines $[L_i]$ are of type $(4, 2, 0, 0)$ or $(2, 2, 2, 0)$, we have the following possibilities for the point classes outside $[L_0]$:

(A) four classes of four points and eight empty classes;

(B) three classes of four points, two classes of two points and seven empty classes;

(C) two classes of four points, four classes of two points and six empty classes;

(D) one class of four points, six classes of two points and five empty classes;

(E) eight classes of two points and four empty classes.

Case (A) is ruled out by the argument above.

In case (B) let $[L_4]$ be of type $(2, 2, 2, 0)$ and let $[L_1], [L_2], [L_3]$ be of type $(4, 2, 0, 0)$. If $[x_1], [x_2], [x_3]$ are the point classes of multiplicity 4 then the lines $\langle [x_i], [x_j] \rangle$ must be incident with the empty class on $[L_4]$. This is impossible.

In case (C) the three line classes parallel to $[L_0]$ are of type $(4, 0, 0, 0)$, $(4, 2, 0, 0)$ and $(2, 2, 2, 0)$. Now it is easy to check that there is a line of type $(2, 2, 0, 0)$, a contradiction to Lemma 1.

In case (D), it can be checked that the three line classes parallel to $[L_0]$ are of type $(4,0,0,0)$ (one line) and $(2,2,2,0)$ (two lines). Again, it is easily checked that there is a line of type $(2,2,0,0)$.

In case (E), there is a line class parallel to $[L_0]$ which is of type $(2,2,0,0)$, a contradiction to Lemma 1.

(ii) Now let us assume that $[L_0]$ is a line class with $|B \cap [L_0]| = 10$. As above, the line class $[L_0]$ is not incident with point classes $[x]$ with $|B \cap [x]| \leq 1$. There cannot be two point classes outside $[L_0]$ of multiplicity four since the line incident with them is of type $(4,4,2,*)$, which is impossible.

Hence for the multiplicities of the line classes we have two possibilities: $(7,6,4)$ and $(6,6,5)$. Moreover a line class of multiplicity 6 has type $(2,2,2,0)$; the other possibility would be $(4,2,0,0)$ which would introduce a second point class of multiplicity 4. In both cases there exist lines of type $(2,2,1,0)$ or $(2,2,0,0)$, which is impossible. □

Lemma 5. *Let R be a chain ring with $|R| = 16$, $R/\operatorname{rad} R \cong \mathbb{F}_4$ and let B be a blocking set in $\mathrm{AHG}({}_RR^2)$ with $|B| = 27$. Then*

(*i*) $|B \cap [x]| \leq 4$ *for every neighbour class of points* $[x]$.

(*ii*) $|B \cap [L]| \geq 6$ *for every neighbour class of lines* $[L]$. *Moreover, a class* $[L]$ *with* $|B \cap [L]| = 6$ *is of type* $(2,2,2,0)$.

Proof. This result is obtained by easy counting. □

Theorem 7. *Let R be a chain ring with $|R| = 16$, $R/\operatorname{rad} R \cong \mathbb{F}_4$. The minimal size of a blocking set in* $\mathrm{AHG}({}_RR^2)$ *is* 28.

Proof. Assume there exists a blocking set B of size 27 in $\mathrm{AHG}({}_RR^2)$. Denote by $[L_0]$, $[L_1]$, $[L_2]$, $[L_3]$, a quadruple of parallel lines in the factor plane. Because of Lemmas 4 and 5, we have the following possibilities:

(A) $(|B \cap [L_0]|, |B \cap [L_1]|, |B \cap [L_2]|, |B \cap [L_3]|) = (9,6,6,6)$;

(B) $(|B \cap [L_0]|, |B \cap [L_1]|, |B \cap [L_2]|, |B \cap [L_3]|) = (8,7,6,6)$;

(C) $(|B \cap [L_0]|, |B \cap [L_1]|, |B \cap [L_2]|, |B \cap [L_3]|) = (7,7,7,6)$.

(A) The line classes $[L_1]$, $[L_2]$ and $[L_3]$ are of type $(2,2,2,0)$ by Lemma 5. Further, the line class $[L_0]$ cannot contain a point class of multiplicity ≥ 4 since this would enforce the existence of a line class of multiplicity ≥ 10. On the other hand $[L_0]$ cannot have a point class of multiplicity ≤ 1 since then there would be line class of type $(2,2,\leq 1,0)$, in contradiction to Lemma 5. Hence $[L_0]$ is of type $(3,2,2,2)$, which implies the existence of a line class of multiplicity 4 or 5, again a contradiction.

(B) Since there is no line class of multiplicity 9, we get by a straightforward counting that $|B \cap [x]| \leq 3$ for every point class $[x]$. The line classes $[L_2]$ and $[L_3]$ are of type $(2,2,2,0)$ and hence the line class through the two zeros is of multiplicity at most 6. But then it is of type $(3,3,0,0)$, which is impossible.

(C) Now all line classes are of multiplicity 6 or 7. Moreover $|B \cap [x] \leq 2$ for every point class $[x]$. Now $[L_0]$, $[L_1]$ and $[L_2]$ are of type $(2,2,2,1)$ while $[L_3]$ is of type $(2,2,2,0)$. Clearly, there exists a line class of type $(2,2,2,2)$ which was ruled out in (B). This completes the proof. □

REFERENCES

[1] Brouwer A. E., A. Schrijver. The blocking number of an affine space. *J. Combin. Th.*, Ser. A, **24** (1978), 251–253.

[2] Bruen A. A. Polynomial multiplicities over finite fields and intersection sets. *J. Comb. Th.*, Ser. A, **60** (1992), 19–33.

[3] Cronheim A. Dual numbers, Witt vectors, and Hjelmslev planes. *Geometriae Dedicata*, **7** (1978), 287–302.

[4] Honold Th., I. Landjev. Linear Codes over Finite Chain Rings and projective Hjelmslev Geometries. Codes over Rings (Ed. P. Solé), World Scientific, 2009, 60–123.

[5] Honold Th., I. Landjev. Codes over Rings and Ring Geometries. Current Research Topics in Galois Geometry (Eds J. De Beule, L. Storme), Nova Science Publishers, 2011, 159–184.

[6] Jamison R. Covering finite fields with cosets of subspaces. *J. Comb. Th.*, Ser. A, **22** (1977), 253–256.

[7] Landjev I. On blocking sets in projective Hjelmslev planes. *Adv. in Math. of Comm.*, **1** (2007), 65–81.

[8] Landjev I., S. Boev. Blocking sets of Rédei type in projective Hjelmslev planes. *Discrete Math.*, **310** (2010), 65–81.

[9] Raghavendran R. Finite associative rings. *Compositio Mathematica*, **21** (1969), 195–229.

Stoyan Boev
New Bulgarian University
21, Montevideo Str.
1618 Sofia, Bulgaria
e-mail: `stoyan@nbu.bg`

Ivan Landjev
New Bulgarian University
21, Montevideo Str.
1618 Sofia, Bulgaria
e-mail: `i.landjev@nbu.bg`

Received March 2, 2012
Final Accepted April 19, 2012