Finite Fields and Their Applications 87 (2023) 102152

Contents lists available at ScienceDirect

Finite Fields and Their Applications

journal homepage: www.elsevier.com/locate/ffa

Large blocking sets in PG$(2, q^2)$

Tamás Szőnyi [a,b], Zsuzsa Weiner [c,d,*]

[a] *ELTE Eötvös Loránd University, Department of Computer Science and MTA-ELTE Geometric and Algebraic Combinatorics Research Group, H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary*
[b] *University of Primorska, FAMNIT, SI-6000 Koper, Glagoljaška 8, Slovenia*
[c] *MTA-ELTE Geometric and Algebraic Combinatorics Research Group, H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary*
[d] *Prezi Inc, H-1065 Budapest, Nagymező utca 54-56, Hungary*

ARTICLE INFO

Article history:
Received 8 December 2021
Received in revised form 13 December 2022
Accepted 16 December 2022
Available online 16 January 2023
Communicated by Olga Polverino

MSC:
primary 51E21
secondary 05B25

Keywords:
Finite plane
Unital
Blocking set

ABSTRACT

Minimal blocking sets in PG$(2, q^2)$ have size at most $q^3 + 1$. This result is due to Bruen and Thas and the bound is sharp, sets attaining this bound are called unitals. In this paper, we show that the second largest minimal blocking sets have size at most $q^3 + 1 - (p - 3)/2$, if $q = p$, $p \geq 67$, or $q = p^h$, $p > 7$, $h > 1$. Our proof also works for sets having at least one tangent at each of its points (that is, for tangency sets).

* Corresponding author.
E-mail addresses: tamas.szonyi@ttk.elte.hu, tamas.szonyi@famnit.upr.si (T. Szőnyi), zsuzsa.weiner@gmail.com (Zs. Weiner).
URL: https://Prezi.com (Zs. Weiner).

https://doi.org/10.1016/j.ffa.2022.102152

1. Introduction

A *blocking set* in a projective plane is a set of points which intersects every line. The smallest blocking sets are lines. Blocking sets not containing a line will be called *non-trivial*. A point P of a blocking set B is said to be *essential* if there is a line that intersects B in P only. Geometrically, this means that there exists a tangent line to B at the point P. A blocking set is *minimal* when no proper subset of it is a blocking set. In other words, it is minimal if the points of the blocking set are all essential. Note that a minimal blocking set in a projective plane is either a line or does not contain a line. For a survey of blocking sets, see [10], [11] and [8].

Throughout this paper, we will work on the Desarguesian affine and projective planes $\mathrm{AG}(2,q)$ and $\mathrm{PG}(2,q)$; for their properties, see [10]. Hence $q=p^h$ is a prime power, the letter p denotes the characteristic. Note that we will work in planes of square order, so after the Introduction, we will use $\mathrm{AG}(2,q^2)$ and $\mathrm{PG}(2,q^2)$.

One of the most interesting questions on blocking sets is to determine the possible sizes of non-trivial minimal ones. The first result in this direction is due to Bruen [5], who proved that a non-trivial minimal blocking set has size at least $q+\sqrt{q}+1$. When q is a square, minimal blocking sets of that size exist; these are exactly the point sets of Baer-subplanes. A blocking set is *small* if it has size less than $3(q+1)/2$. There has been lot of attention paid on characterizing small minimal blocking sets. Blokhuis [3] showed that when q is a prime then there are no small minimal non-trivial blocking sets at all. In [14], Szőnyi proved that the possible sizes of small minimal blocking sets lie in certain intervals. This was further extended by Sziklai [13].

There are much less results concerning the other end of the spectrum. Bruen and Thas [6] showed that the largest minimal blocking sets have size at most $q\sqrt{q}+1$. When q is a square, equality holds and the minimal blocking sets attaining the bound have to be *unitals*. A unital is a point set with a unique tangent at each point and the secant lines intersect it in $\sqrt{q}+1$ points. When q is a square, unitals do exist, since the Hermitian curve is always a (Hermitian) unital. The upper bound by Bruen and Thas was generalized to tangency sets, that is sets having a tangent at each of their point (actually, for sets having at least as many tangent lines as the number of points), see [12]. When q is not a square, the upper bound can be (slightly) improved, see [7]. Similar results were obtained by Bishnoi, Mattheus, Schillewaert [2], who also gave different algebraic and combinatorial proofs for their results.

For q square, the next interesting question is to determine the size of the second largest minimal blocking set. Blokhuis and Metsch [4] proved that in $\mathrm{PG}(2,q)$ there are no minimal blocking sets with cardinality $q\sqrt{q}$, when $q\geq 49$. Hence there is a gap of size at least 1 between the size of the second largest and the largest minimal blocking set. If we wish to add a point P outside the unital U, then we have to delete the points of U on the tangent lines passing through P. If they are collinear, then one of the points could be added back to get a blocking set. For every unital, there are $\sqrt{q}+1$ tangents through P, and in case of Hermitian curves the common points of the tangents through P with

the unital are collinear. Hence there are minimal blocking sets of size $q\sqrt{q}+2-\sqrt{q}$ in $\mathrm{PG}(2,q)$ if q is a square. We may note that there are non-Hermitian unitals, hence there are also minimal blocking sets of size $q\sqrt{q}+1-\sqrt{q}$.

A set U of points in the projective plane of order q is called a *partial unital*, if (1) every point of U lies on at least one tangent line, (2) no line contains more than $\sqrt{q}+1$ points of U, and (3) there is at least one line meeting U in $\sqrt{q}+1$ points. Ball [1] showed that if a partial unital in $\mathrm{PG}(2,q)$ has more than $q\sqrt{q}+1-\sqrt{q}$ points, then it must be a subset of a unital; so it cannot be a minimal blocking set. Hence if we only consider minimal blocking sets that are partial unitals as well, then the above mentioned gap is at least $\sqrt{q}$. Another proof of this fact was given in [9].

In this paper, we will investigate in detail the case when the order of the plane is a square. Therefore the order of the plane will be denoted by q^2, the characteristic of the plane will be p throughout the paper, so $q=p^h$, $h\geq 1$. This implies that the Bruen, Thas upper bound is q^3+1 and the second largest known minimal blocking sets have size q^3+2-q. Earlier results used q for the order of the plane, as we did in the first part of the Introduction. We will cite them in their original form but mention the necessary changes for planes of order q^2. In the particular case when $q=p$, we could show that there is indeed a gap of size roughly $q/2$, if $q=p\geq 67$. (For the prime square case see Theorem 4.1, for the general square case see Theorem 5.4.) Since there are minimal blocking sets of size q^3+2-q, this result gives the correct order of magnitude for $q=p$. As in the case of the Bruen, Thas upper bound we will only assume that the set has a tangent at each point (the property of being a blocking set is not used). This is also motivated by the result above by Ball for partial unitals.

Our proof uses the stability results for k mod p multisets given by Szőnyi and Weiner [15]. The size of a multiset is the sum of multiplicities of the points. The intersection size of a line and a multiset is defined similarly for the points of the line. Since we consider the intersection size of a line and a multiset mod p, we can choose the multiplicity of a point mod p; hence instead of multiplicity $p-3$ we can also say that the multiplicity is -3. More precisely, we will choose the multiplicities to be between $-\frac{p-1}{2}$ and $\frac{p-1}{2}$, see Definition 3.5.

2. Combinatorial properties of sets of size close to q^3+1

Let B be a set of points in $\mathrm{PG}(2,q^2)$. Furthermore, let $\ell_1,\ell_2,\dots,\ell_{q^4+q^2+1}$ be the lines of $\mathrm{PG}(2,q^2)$ and let $n_i=|\ell_i\cap B|$, $i=1,2,\dots,q^4+q^2+1$, be their intersection numbers with B. The standard double counting arguments give the following equations for the integers n_i:

(1) $\sum_i n_i=|B|(q^2+1)$,
(2) $\sum_i n_i(n_i-1)=|B|(|B|-1)$.

The next equality follows easily from the equations above, when the size of B is $q^3+1-\varepsilon$.

Lemma 2.1. *Let B be a set of $q^3+1-\varepsilon$ points in $\mathrm{PG}(2,q^2)$. Then*

$$\sum_i (n_i-(q+1))^2 = q^5+(\varepsilon+1)q^2+2\varepsilon q+\varepsilon^2. \quad \square \tag{1}$$

Now we will pose an extra condition on B.

Definition 2.2. The point set B is a tangency set, if through each point P of B there exists at least one line (a tangent) intersecting B in exactly P. If we choose precisely one tangent line at each point of B then we call them the guaranteed tangents.

Lemma 2.3. *Let B be a set of $q^3+1-\varepsilon$ points in $\mathrm{PG}(2,q^2)$. Assume that B is a tangency set and suppose also that $\ell_1,\ell_2,\dots,\ell_{|B|}$ are the 1-secants guaranteed by Definition 2.2. Then*

$$\sum_{|B|<i} (n_i-(q+1))^2 = 2\varepsilon q^2+2\varepsilon q+\varepsilon^2. \tag{2}$$

Proof. Note that the $q^3+1-\varepsilon$ 1-secants gives $(q^3+1-\varepsilon)q^2$ in the sum in equation (2.1) and so the result follows from Lemma 2.1. $\square$

When ε is not too large, this means that except the "compulsory" 1-secants, most of the lines contain exactly $(q+1)$ points from B.

3. Embedding in 1 mod p set

3.1. Earlier stability results

In this section, we collect some earlier results which we will use later on. Note that we will use them in $\mathrm{PG}(2,q^2)$, but we will state them in their original form.

Result 3.1 *([15]). Let $\mathcal{M}$ be a multiset in $\mathrm{PG}(2,q)$, $17<q$, so that the number of lines intersecting it in not k mod p points is δ, where $\delta<(\lfloor\sqrt{q}\rfloor+1)(q+1-\lfloor\sqrt{q}\rfloor)$. Then the number of not k mod p secants through any point is at most $\sqrt{q}+1$ or at least $q-\sqrt{q}$.*

Our general aim is to show that if there are not too many lines intersecting $\mathcal{M}$ in not k mod p points then we can modify the multiplicity of the points through which there are at least $q-\sqrt{q}$ lines intersecting $\mathcal{M}$ in not k mod p points so that the resulting multiset intersects every line in k mod p points. This was given in Property 3.5 in [15], but instead of just restating it we try to explain it in more detail. To do this, we will introduce Property (T) for certain points of $\mathrm{PG}(2,q)$ with respect to a multiset $\mathcal{M}$

intersecting almost all lines in k mod p points. Intuitively, this property will assure that there are enough lines, which intersect $\mathcal{M}$ in the same number of points mod p through such a point. Property (T) is assumed in Result 3.3 and we will show that it holds automatically under the condition of Proposition 3.4.

Property 3.2 *([15], Property (T) with respect to a k and $\mathcal{M}$). Let $\mathcal{M}$ be a multiset in* $\mathrm{PG}(2,q)$, $q=p^h$, *where p is prime. Assume that there are δ lines that intersect $\mathcal{M}$ in not k mod p points. Let Q be an arbitrary point of* $\mathrm{PG}(2,q)$, *so that there are more than $q/2$ lines intersecting $\mathcal{M}$ in not k mod p points.*

We say that Q has Property (T) with respect to k and $\mathcal{M}$ *if there exists a value $r \not\equiv k \pmod p$ such that more than $2\frac{\delta}{q+1}+5$ of the lines through Q meet $\mathcal{M}$ in r mod p points.*

Result 3.3 *([15]). Let $\mathcal{M}$ be a multiset in* $\mathrm{PG}(2,q)$, $17<q$, $q=p^h$, *where p is prime. Assume that the number of lines intersecting $\mathcal{M}$ in not k mod p points is δ, where $\delta < (\lfloor\sqrt{q}\rfloor+1)(q+1-\lfloor\sqrt{q}\rfloor)$. Assume furthermore, that if a point Q is incident with more than $q/2$ lines meeting M in not k mod p points then Q has property (T). Then there exists a multiset $\mathcal{M}'$ with the property that it intersects every line in k mod p points and the number of different points whose mod p multiplicity is different in $\mathcal{M}$ and in $\mathcal{M}'$ is exactly $\lceil\frac{\delta}{q+1}\rceil$.*

In [15], the above result was phrased in a little bit different manner. The number of points we have to modify in order to obtain the multiset $\mathcal{M}'$ from $\mathcal{M}$ was given by the number of points in $(\mathcal{M}\cup\mathcal{M}')\setminus(\mathcal{M}\cap\mathcal{M}')$, which is a bit confusing when we speak about multisets.

Since in our paper the order of the plane is denoted by q^2, in Property 3.2, we have to replace q by q^2 everywhere. Similarly, in Result 3.1 and Result 3.3, the bound on δ is q^3+1. The number of not k mod p secants through any point is at most $q+1$ or at least q^2-q (Result 3.1) and the number of modified points in Result 3.3 is $\lceil\frac{\delta}{q^2+1}\rceil$. Remark that we can use the results above when $q>4$ (in $\mathrm{PG}(2,q^2)$).

In the rest of the paper, we will work with multisets and so all set operations are considered with multiplicity. Also, we will use these results when $k=1$.

3.2. Embedding

From now on, **we will assume that $\mathbf{q=p^h}$, $\mathbf{p\geq 67}$ if $\mathbf{h=1}$ and $\mathbf{q>4}$ otherwise**.

Also, B will always be a tangency set in $\mathrm{PG}(2,q^2)$ of size close to q^3+1. Then Lemma 2.3 and Result 3.3 yield the following proposition.

Proposition 3.4. *Let B be a point set of size $q^3+1-\varepsilon$ in* $\mathrm{PG}(2,q^2)$, $q=p^h$. *Assume that $p\geq 67$ if $h=1$ and $q>4$ otherwise. Suppose that $2\varepsilon q^2+2\varepsilon q+\varepsilon^2<q^3+1$. Assume also that B is a tangency set. Then there exists a multiset $\mathcal{N}$ containing at most $2\varepsilon+2$ different points, so that adding it to B, we get a multiset B^* intersecting every line in 1 mod p points.*

Proof. Note that $2\varepsilon < q$. By Lemma 2.3, the number δ of not 1 mod p secants of B is at most $2\varepsilon q^2 + 2\varepsilon q + \varepsilon^2$, which is less than $q^3 + 1$.

If Property (T) holds with respect to k and $\mathcal{M}$ then from Result 3.3, $\mathcal{N}$ exists and the number of different points in $\mathcal{N}$ is $\lceil \frac{\delta}{q^2+1} \rceil$ and hence the result follows.

We show that for $h \neq 1$, Property (T) holds with respect to k and $\mathcal{M}$ automatically. By Result 3.1, if there is a point through which there pass at least $q^2/2$ lines intersecting B in not 1 mod p points, then there are indeed at least $q^2 - q$ such lines. By the pigeon hole principle, at least $\frac{q^2-q}{p}$ lines intersect B in the same number of points modulo p. This is larger than $2q + 5 \geq 2\frac{\delta}{q^2+1} + 5$, when $q > 4$.

Now assume $h = 1$ and, on the contrary, that Property (T) does not hold with respect to k and $\mathcal{M}$. Let P be a point with at least $p^2/2$ lines on it so that they intersect B in not 1 mod p points. Again, by Result 3.1, this means that there must be at least $p^2 - p$ such lines through P. We will show that the contribution of these (at least) $p^2 - p$ lines (the sum of $(n_i - (q+1))^2$ for these lines) in the sum (2) of Lemma 2.3 is already too large and hence the proof follows. To see this, note that a not 1 mod p secant gives the least contribution in (2), if it is a 0 or 2 mod p secant. Their contribution is 1. The -1 or 3 mod p secants contribute 2^2, and so on. Hence if $n = \lfloor 2\frac{\delta}{p^2+1} + 5 \rfloor$, it follows that

$$L := 2n\left(1^2 + 2^2 + 3^2 + \cdots + \left\lfloor \frac{p^2-p}{2n} \right\rfloor^2\right) = 2n\frac{\left(\left\lfloor \frac{p^2-p}{2n} \right\rfloor\right)\left(\left\lfloor \frac{p^2-p}{2n} \right\rfloor + 1\right)\left(2\left\lfloor \frac{p^2-p}{2n} \right\rfloor + 1\right)}{6} \tag{3}$$

is a lower bound for the sum (2) in Lemma 2.3. Using that $\lfloor \frac{p^2-p}{2n} \rfloor > \frac{p^2-p}{2n} - 1$, we get that

$$L > \frac{(\frac{p^2-p}{2n} - 1)(p^2 - p)(2\frac{p^2-p}{2n} - 1)}{6}. \tag{4}$$

Note that $2n < 4p + 16$ when $\varepsilon < p/2$ and so $\frac{p^2-p}{2n} > \frac{p}{4} - 1.25$ and hence

$$L > \frac{(\frac{p}{4} - 2.25)(p^2 - p)(\frac{p}{2} - 3.5)}{6}. \tag{5}$$

We show that L is larger than $p^3 + p > 2\varepsilon p^2 + 2\varepsilon p + \varepsilon^2$ and so it is a contradiction by Lemma 2.3.

$$\frac{(\frac{p}{2} - 5.5)(p-1)(p-10)}{6} > p^2 + 1, \tag{6}$$

which is equivalent to

$$\frac{p^3}{8} - 65\frac{p^2}{8} + 79\frac{p}{8} - \frac{111}{8} > 0 \tag{7}$$

and this is true when $p \geq 67$. □

For $p = 2$ and $h > 1$, in the proposition above we had to exclude $q = 4$. For larger values of p, there is no q to be excluded, when $h > 1$.

Definition 3.5. The points in $\mathcal{N}$ will be called *modified points*. The multiplicity m_P of a point in $\mathcal{N}$ is the multiplicity mentioned in Proposition 3.4. Hence $B \cup \mathcal{N}$ with multiplicities is the multiset B^*. From now on, we will assume that for the multiplicity m_P of a point P in $\mathcal{N}$, we have $-\frac{p-1}{2} \leq m_P \leq \frac{p-1}{2}$.

By Proposition 3.4, all lines intersecting B in not 1 mod p points must contain a point from $\mathcal{N}$ and so the next corollary is straightforward.

Corollary 3.6. *Through a point $P \in \mathcal{N}$, there pass at least $q^2 - 2\varepsilon$ lines, which are not 1 mod p secants of B. Also, through a point $Q \notin \mathcal{N}$, there pass at most $2\varepsilon + 2$ lines, which are not 1 mod p secants of B.* □

Lemma 3.7. *Assume that $\varepsilon < p/2$. For the multiplicities m_{P_i} of the points P_i in $\mathcal{N}$, we have*

$$\sum_{P_i \in \mathcal{N}} m_{P_i}^2 \leq 2\varepsilon + 3.$$

Hence $\sum_{P_i \in \mathcal{N}} |m_{P_i}| \leq 2\varepsilon + 3$.

Proof. For a line ℓ_i through exactly one point $P_i \in \mathcal{N}$, the corresponding term in the sum in Lemma 2.3 gives at least $m_{P_i}^2$. By Corollary 3.6, there are at least $q^2 - 2\varepsilon$ such lines through P_i. So, by Lemma 2.3, we get $(q^2 - 2\varepsilon) \sum_{P_i \in \mathcal{N}} m_{P_i}^2 \leq 2\varepsilon q^2 + 2\varepsilon q + \varepsilon^2$ and hence the result follows. □

From now on, assume that $2\varepsilon + 5 \leq p$.

By Lemma 3.7, this means that the absolute value of the multiplicity of any point in $\mathcal{N}$ is less than $\sqrt{p}$. The set B^* intersects every line in 1 mod p points (with multiplicity). Since the number of points in $\mathcal{N}$ with multiplicity is less than p, we get the following two lemmas.

Lemma 3.8. *A tangent line to B must be tangent to B^*.* □

Since B^* intersects every line in 1 mod p points (with multiplicity), its size must also be 1 mod p (with multiplicity). The next lemma follows immediately from Lemma 3.7 and from $|B| = q^3 + 1 - \varepsilon$.

Lemma 3.9. *The size of B^* is either $q^3 + 1$ or $q^3 + 1 - p$.* □

4. The prime square case

In this section we will assume that $q = p$ (i.e. $h = 1$) and so $p \geq 67$. Our aim is to prove the following theorem.

Theorem 4.1. *Let B be a tangency set of size $p^3 + 1 - \varepsilon$ in $\mathrm{PG}(2, p^2)$, $p \geq 67$ and $2\varepsilon + 5 \leq p$. Then B is contained in a unital.*

A unital is a minimal blocking set and so the next corollary is a straightforward consequence of Theorem 4.1.

Corollary 4.2. *The largest minimal blocking set in $\mathrm{PG}(2, p^2)$, $p \geq 67$, which is not a unital, has size at most $p^3 + 1 - (p-3)/2$.* □

In order to prove Theorem 4.1, we will show that B^* (from the previous section) is a unital.

Lemma 4.3. *There is no point in B^* with multiplicity less than 0.*

Proof. Assume to the contrary that P has multiplicity $m_P < 0$ in B^*. Note that by Lemma 3.7 and since every line intersects B^* in 1 mod p points, the smallest intersection multiplicity of lines with B^* is 1. If each line through P intersected B^* in at least $p+1$ points, then B^* would have at least $(p^2+1)(p+1-m_P)+m_P$ points. But B^* has at most p^3+1 points, so there must pass at least $(-m_P+1)p+1$ lines through P which intersect B^* in exactly 1 point. By Lemma 3.7 and using that P must be a modified point, there are at least $-p \cdot m_P + 3$ lines through P which are tangents to B^* and P is the only modified point on it. These lines were either $(-m_P+2)$- or $(-m_P+1)$-secants of B, depending on P was in B or not. Hence they were not 1-secants, so they are counted in Lemma 2.3. Their contribution to the sum in Lemma 2.3 is at least $(-p \cdot m_P + 3)(p - 1 + m_P)^2$, which is at least $p^3 - p^2 - 8p + 12$ (since $m_P \leq -1$). This contradicts Lemma 2.3, when $2\varepsilon \leq p - 5$. □

Lemma 4.4. *The points of B are in B^*.*

Proof. To the contrary, assume that $P \in B$, but $P \notin B^*$ (so the multiplicity of P in $\mathcal{N}$ was -1). Since all lines intersect B^* in 1 mod p points and there are no points with negative multiplicity (Lemma 4.3), there pass at least $p+1$ tangent lines of B^* through P. One of them is the guaranteed tangent at P, the other at least p are tangents to B^* at $P_i (\neq P) \in B^*$; these should be counted in the sum (2) of Lemma 2.3. These at least p tangent lines may contain points which are in B, but not in B^*. So assume that the tangent line l_i at $P_i \in B^*$ contains k_i points from B which are not in B^*, by Lemma 3.7 $k_i < p$. Hence $|l_i \cap B| = 1 + k_i$ or k_i depending on $P_i \in B$ or not. This implies that $(|l_i \cap B| - (p+1))^2 \geq (k_i - p)^2$. So, the contribution of these lines to the sum (2) of

Lemma 2.3 is at least $\sum_{i=1}^{p}(k_i-p)^2 = p^3 - 2p\sum_{i=1}^{p} k_i + \sum_{i=1}^{p} k_i^2$. By Lemma 3.7, this is at least $p^3 - 2p^2$. This is a contradiction to Lemma 2.3, when $2\varepsilon \le p-5$. □

Lemma 4.5. *The size of B^* is p^3+1.* □

Lemma 4.6. *The points of B^* have multiplicity 1.*

Proof. We only have to show that there are no points with multiplicity at least 2. Assume to the contrary that there is a point $P \in B^*$ with multiplicity at least 2. This means that there is a line ℓ through P containing at least $2p+1$ points from B^*. By Proposition 3.4, we modify at most $2\varepsilon + 2 \le p-3$ points besides P. This also means that on this line there are at least $p+3$ points from $B \setminus \{P\}$, say $P_1, P_2, \ldots, P_s$, $s \ge p+3$ so that their multiplicity in B^* is one. By counting, a point P_i is on at least 2 tangent lines to B^*. By Lemma 4.3 and Lemma 4.4, such a tangent is a tangent to B as well. In the sum of Lemma 2.3, only one tangent through each point was excluded, so through these points of B, we see tangent lines contributing to the sum in Lemma 2.3 by at least $(p+3)p^2$, which is a contradiction. □

Proof of Theorem 4.1. Construct the point set B^* obtained by Proposition 3.4. By Lemma 4.6 and Lemma 4.5, B^* is a unital. □

5. The case $q = p^h$, $h > 1$

Now we are going to extend Theorem 4.1 to non prime squares. In this section we will work in $\mathrm{PG}(2, q^2)$, $q = p^h$ and we will assume $h > 1$ and $p > 7$.

We start from a set B of size $q^3 + 1 - \varepsilon$, which has at least one tangent line at each of its points. Let us choose precisely one tangent at each point and denote the set of these guaranteed tangents by $\mathcal{L}$. Let us recall that, by Lemma 3.9, B^* is a multiset of size q^3+1+b, $b \in \{0, -p\}$, intersecting every line in 1 mod p points. It is obtained from B by modifying the multiplicities of some points. The multiset $\mathcal{N}$ contains the modified points with multiplicity so that B^* is the union of B and $\mathcal{N}$ as multisets (see Definition 3.5).

Our aim is to show that every point in $\mathcal{N}$ has multiplicity 1 and they were not in B. We will see that if there was a point P in $\mathcal{N}$ which has multiplicity not 1 or which were in B, then calculating the sum (2) of Lemma 2.3, we get a contradiction. Actually, it will be enough to calculate this sum only for some lines on P. In order to do this, the next lemma will be crucial.

Lemma 5.1. *Let P be a point with multiplicity m_P in $\mathcal{N}$ and denote the lines through P by e_i, $i = 1, \ldots, q^2+1$. Lines intersect B^* in 1 mod p points, hence $|e_i \cap B^*| = q+1+r_i p$ for some integer r_i. Assume that for the index set $J \subset \{1, \ldots, q^2+1\}$, $\sum_{j\in J} |r_j| = A$. If $A \ge |J|$, then*

(1) $\sum_{j\in J}(q+1-|B\cap e_j|)^2 \ge A(p-|m_P|)^2 - 2(p-|m_P|)(p-2-|m_P|)$,

(2) $\sum_{j\in J}(q+1-|B\cap e_j|)^2 \geq (A-n)(p-|m_P|)^2$, *where* n *is the number of lines* e_i *containing at least one point from* $\mathcal{N}\setminus\{P\}$.

Proof. We define $I\subseteq J$ so that for every $l\in I$ the line e_l intersects $\mathcal{N}\setminus\{P\}$, and assume that there are k_l points of $\mathcal{N}\setminus\{P\}$ on e_l counted with their multiplicities in $\mathcal{N}$. Note that $|I|=n$ (see (2)). Hence

$$\sum_{j\in J}(q+1-|B\cap e_j|)^2 \geq \sum_{l\in I}(r_l p-(m_P+k_l))^2+\sum_{j\in J\setminus I}(r_j p-m_P)^2.$$

The right-hand side can be further lower bounded by

$$\sum_{l\in I}(|r_l|p-|m_P+k_l|)^2+\sum_{j\in J\setminus I}(|r_j|p-|m_P|)^2.$$

By Lemma 3.7, $0<|m_P|+|k_l|<p$ and as r_l is an integer, it is not difficult to show that $(|r_l|p-|m_P+k_l|)^2$ is at least $(|r_l|-1)p^2+(p-|m_P+k_l|)^2$, which is at least $(|r_l|-1)p^2+(p-|m_P|-|k_l|)^2$. Hence $\sum_{l\in I}(|r_l|p-|m_P+k_l|)^2+\sum_{j\in J\setminus I}(|r_j|p-|m_P|)^2 \geq (A-|J|)p^2+\sum_{l\in I}(p-|m_P|-|k_l|)^2+\sum_{j\in J\setminus I}(p-|m_P|)^2$. As $A\geq|J|$, this can be lower bounded by $(A-|J|)(p-|m_P|)^2+\sum_{l\in I}(p-|m_P|-|k_l|)^2+\sum_{j\in J\setminus I}(p-|m_P|)^2$. To deduce (2), we neglect the second term. To prove (1), let us rewrite the second term as $\sum_{l\in I}(p-|m_P|)^2-2(p-|m_P|)\sum_{l\in I}|k_l|+\sum_{l\in I}k_l^2$. By Lemma 3.7 and since $P\in\mathcal{N}$ and $\sum_{l\in I}|k_l|\leq(p-2-|m_P|)$, we are done. □

Lemma 5.2. *Let* P *be a point with multiplicity* m_P *in* $\mathcal{N}$ *and denote the lines through* P *by* e_i, $i=1,\ldots,q^2+1$. *Lines intersect* B^* *in* 1 *mod* p *points, hence* $|e_i\cap B^*|=q+1+r_i p$ *for some integer* r_i. *Let* a_P *be* 1 *if* $P\in B$ *and* 0 *otherwise, and let* $\mathcal{L}$ *be the set of tangent lines which was guaranteed by Definition 2.2. Then*

(1) $\sum_{i:r_i<0,e_i\notin\mathcal{L}}|r_i|\geq\frac{|m_P|q^2}{p}$, *when* $m_P\leq -1$,
(2) $\sum_{i:r_i>0,e_i\notin\mathcal{L}}|r_i|\geq\frac{(m_P+a_P-1)q^2-q-p}{p}$, *when* $m_P+a_P\geq 2$.

Proof. Let us count the number of points with multiplicity in B^* on the lines through the point P. We get

$$|B^*|=(m_P+a_P)+\sum_i(q+1+r_i p-(m_P+a_P)).$$

By Lemma 3.9, $|B^*|=q^3+1+b$, where $b\in\{0,-p\}$. Hence

$$\sum_i r_i=\frac{q^2(-1+m_P+a_P)-q+b}{p}. \tag{8}$$

First assume that $m_P \leq -1$. Then the right-hand side of (8) is negative and so if we only consider those lines through P for which $r_i < 0$, then we get (by omitting the term $-b$, since it is positive)

$$\sum_{i:r_i<0} |r_i| \geq \left| \frac{q^2(-1+m_P+a_P)-q+b}{p} \right| \geq \frac{q^2 \cdot |-1+m_P+a_P|+q}{p}.$$

If $P \in B$ ($a_P = 1$), then there is exactly one line in $\mathcal{L}$ through P, say e_k. By Lemma 3.8, the corresponding r_k value is $-q/p$ and so $\sum_{i:r_i<0, e_i \notin \mathcal{L}} |r_i| \geq \frac{q^2 \cdot |-1+m_P+1|}{p}$. When $P \notin B$ ($a_P = 0$), then there can be more than one (tangent) line of $\mathcal{L}$ through P. Note that, by Lemma 3.8, such a line is tangent to B^* as well. Hence it must contain a point from $\mathcal{N}$ different from P and hence (by Lemma 3.7) there can be at most $p-3$ such lines. Also for these lines the corresponding r_i value is $-q/p$ and so we have

$$\begin{aligned} \sum_{i:r_i<0, e_i \notin \mathcal{L}} |r_i| &\geq \frac{q^2 \cdot |-1+m_P| + q - (p-3)q}{p} = \frac{q^2|m_P| + q^2 + q - (p-3)q}{p} \\ &> \frac{q^2|m_P|}{p}, \end{aligned}$$

whence we proved (1).

Now assume that $m_P + a_P \geq 2$. Then the right-hand side of (8) is positive and so if we only consider those lines through P for which $r_i > 0$, then we get

$$\sum_{i:r_i>0} |r_i| \geq \left| \frac{q^2(-1+m_P+a_P)-q+b}{p} \right| \geq \frac{q^2(-1+m_P+a_P)-q-p}{p}.$$

By Lemma 3.8, all lines in $\mathcal{L}$ must be tangent to B^* and hence for $r_i > 0$, e_i is not tangent to B^*, proving (2). □

Proposition 5.3. *The points in $\mathcal{N}$ have multiplicity 1 and $\mathcal{N} \cap \mathcal{B} = \emptyset$.*

Proof. If the statement is not true then there must be a point in $\mathcal{N}$ so that its multiplicity m_P is at most -1 or $m_P + a_P \geq 2$, where a_P is 1 or 0 depending on P is in B or not. As before, let e_i be the lines through P and assume that on a line e_i there are $q + 1 + r_i p$ points of B^* counted with multiplicity. Let $\mathcal{L}$ be the set of tangent lines which was guaranteed by Definition 2.2.

If $m_P \leq -1$, then let J be the set of indices so that for every $j \in J$, $r_j < 0$ and e_j is not in $\mathcal{L}$. Clearly, $\sum_{j \in J} |r_j| \geq |J|$. Hence it follows from Lemma 5.2 (1) and from Lemma 5.1 (2) that

$$\sum_{j \in J} (q + 1 - |B \cap e_j|)^2 \geq \left(\frac{|m_P|q^2}{p} - (p-3) \right) (p - |m_P|)^2 := f(|m_P|).$$

Here we used that $\mathcal{N}$ contains at most $p-3$ points different from P. Let $x := |m_P|$ and define $f(x)$ by

$$f(x) = \left(\frac{q^2x}{p} - (p-3)\right)(p-x)^2 = \frac{q^2}{p}x^3 - (2q^2+p-3)x^2 + (q^2p+2p^2-6p)x - p^3 + 3p^2.$$

Note that $x = p$ is a root of $f(x)$ with multiplicity 2 and so it is a root of $f'(x)$ too. The other root of $f'(x)$ is $\frac{p}{3} + \frac{2p^2}{3q^2} - \frac{2p}{q^2}$. Also $f'(x)$ is a parabola opening upward and so f' is positive in the interval $[1, \frac{p}{3}]$, which means that $f(x)$ is strictly increasing on this interval. Note that now $1 \le |m_P|$ and $|m_P| < \sqrt{p}$ by Lemma 3.7. For $p > 7$, $\sqrt{p} < p/3$ and so

$$\sum_{j\in J}(q+1-|B\cap e_j|)^2 \ge f(1) = \frac{q^2}{p} - (2q^2+p-3) + (q^2p+2p^2-6p) - p^3 + 3p^2.$$

By Lemma 2.3 and $2\varepsilon \le p-5$, this cannot be larger than $(p-5)q^2 + (p-5)q + \frac{(p-5)^2}{4}$. As $p^3 < q^2$, we have a contradiction.

Now assume that $m_P + a_P \ge 2$ and let J' be the set of indices so that for every $j' \in J'$, $r_{j'} > 0$ and $e_{j'}$ is not in $\mathcal{L}$. Again, $\sum_{j'\in J'} |r_{j'}| \ge |J'|$. Hence it follows from Lemma 5.2 (2) and from Lemma 5.1 (2) that

$$\sum_{j'\in J'}(q+1-|B\cap e_{j'}|)^2 \ge \left(\frac{(m_P+a_P-1)q^2 - q - p}{p} - (p-3)\right)(p-|m_P|)^2.$$

Therefore,

$$\sum_{j'\in J'}(q+1-|B\cap e_{j'}|)^2 \ge \left(\frac{(m_P)q^2}{p} - (p-3)\right)(p-m_P)^2 + \frac{(a_P-1)q^2-q-p}{p}(p-m_P)^2.$$

When $a_P = 1$, then $m_P \ge 1$ and so the right-hand side is at least $f(1) + \frac{-q-p}{p}(p-m_P)^2 > f(1) - (q+p)p$. When $a_P = 0$, then $m_P \ge 2$ and so the right-hand side is at least $f(2) + \frac{-q^2-q-p}{p}(p-m_P)^2 > f(2) - (q^2+q+p)p$. As before, in both cases we get a contradiction by Lemma 2.3 and $2\varepsilon \le p-5$. □

Theorem 5.4. *Let B be a tangency set of size $q^3+1-\varepsilon$, in $\mathrm{PG}(2,q^2)$, $0 \le \varepsilon$, $q = p^h$, $p > 7$, $h > 1$ and $2\varepsilon + 5 \le p$. Then B is contained in a unital.*

Proof. For $\varepsilon = 0$, this well-known (see [12]). Otherwise, construct the point set B^* obtained by Proposition 3.4. By Proposition 5.3 and by Lemma 3.9, B^* is a unital. □

Of course, similarly to Corollary 4.2, this theorem gives an upper bound on the size of the second largest minimal blocking set.

Corollary 5.5. *The largest minimal blocking set in* $\mathrm{PG}(2, q^2)$, $q = p^h$, $p > 7$, $h > 1$, *which is not a unital, has size at most* $q^3 + 1 - (p-3)/2$. □

Data availability

No data was used for the research described in the article.

Acknowledgment

The authors are grateful to the anonymous referees for their valuable comments.

Both authors were supported by OTKA Grant K124950 of the Hungarian National Research, Development and Innovation (NRDI) Office. In case of the first author the "Application Domain Specific Highly Reliable IT Solutions project" has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the Thematic Excellence Programme TKP2020-NKA-06 (National Challenges Subprogramme) funding scheme. This work is also supported in part by the Slovenian Research Agency (Research Project J1-9110).

References

[1] S. Ball, Partial unitals and related structures in Desarguesian planes, Des. Codes Cryptogr. 15 (1998) 231–236.
[2] A. Bishnoi, S. Mattheus, J. Schillewaert, Minimal multiple blocking sets, Electron. J. Comb. 25 (4) (2018) P4.66.
[3] A. Blokhuis, On the size of a blocking set in $\mathrm{PG}(2, p)$, Combinatorica 14 (1994) 273–276.
[4] A. Blokhuis, K. Metsch, Large minimal blocking sets, strong representative systems and partial unitals, in: F. De Clerck, et al. (Eds.), Finite Geometries, Cambridge Univ. Press, Cambridge, 1993, pp. 37–52.
[5] A.A. Bruen, Baer subplanes and blocking sets, Bull. Am. Math. Soc. 76 (1970) 342–344.
[6] A.A. Bruen, J.A. Thas, Blocking sets, Geom. Dedic. 6 (1977) 193–203.
[7] A. Cossidente, A. Gács, Cs. Mengyán, T. Szőnyi, Zs. Weiner, On large minimal blocking sets, J. Comb. Des. 13 (2005) 25–41.
[8] A. Gács, T. Szőnyi, Zs. Weiner, On the spectrum of minimal blocking sets, J. Geom. 76 (2003) 256–281.
[9] É. Hadnagy, T. Szőnyi, On embedding large (k, n)-arcs and partial unitals, Ars Comb. 56 (2002) 299–308.
[10] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Clarendon Press, Oxford, 1979, 2nd edition, 1998.
[11] J.W.P. Hirschfeld, L. Storme, The packing problem in statistics, coding theory and finite projective spaces, update 2001, in: A. Blokhuis, J.W.P. Hirschfeld, D. Jungnickel, J.A. Thas (Eds.), Finite Geometries, in: Developments of Mathematics, Kluwer, 2001, pp. 201–246.
[12] T. Illés, T. Szőnyi, F. Wettl, Maximal strong representative systems and minimal blocking sets, Mitt. Math. Sem. Univ. Giessen 201 (1991) 97–107.
[13] P. Sziklai, On small blocking sets and their linearity, J. Comb. Theory, Ser. A 115 (2008) 1167–1182.
[14] T. Szőnyi, Blocking sets in Desarguesian affine and projective planes, Finite Fields Appl. 3 (1997) 187–202.
[15] T. Szőnyi, Zs. Weiner, Stability of k mod p multisets and small weight codewords of the code generated by the lines of $\mathrm{PG}(2, q)$, J. Comb. Theory, Ser. A 157 (2018) 321–333.