Large minimal blocking sets in planes of square order

Tamás Szőnyi

Eötvös Loránd University and MTA-ELTE GAC Research Group
Budapest; and University of Primorska, FAMNIT, Koper

30th June, 2022
10th PhD Summer School in Discrete Mathematics, Rogla

Coauthors

This talk is based on joint work with ZSUZSA WEINER.

Motivation of the problem

Definition

A *blocking set* in an incidence structure is a set of points which intersects each line.

In hypergraph terminology, they are called 1-covers. Considered also in configurations.
First, blocking sets were studied in projective planes.

Proposition

In Π_q any blocking set has at least $q+1$ points. In case of equality, the blocking set is a line.

In projective planes, a blocking set is called *trivial* if it contains a line.

Some early results

For projective planes we have the following results (Bruen's bound).

Theorem (Bruen; Pelikán)

For a non-trivial blocking set of Π_q we have $|B| \geq q + \sqrt{q} + 1$, and in case of equality we have a subplane of order $\sqrt{q}$ (Baer subplane).

For the plane $\mathrm{PG}(2, q)$ much better results are known.

Theorem (Blokhuis)

Let B be a non-trivial blocking set of $\mathrm{PG}(2, q)$. If q is a prime, then $|B| \geq 3(p + 1)/2$. If $q = p^h$, is not a prime and h is odd, then $|B| \geq q + \sqrt{pq} + 1$.

Small blocking sets

For general planes Π_q, Bruen's bound is improved by 1 (BIERBRAUER), by 2 only for special blocking sets (of Rédei type) by DRAKE, KITTO.

Definition

A blocking set in $\mathrm{PG}(2,q)$ is small, if its size is $\leq 3(q+1)/2$.

Small minimal blocking sets have some structure: there is an e such that lines intersect them in 1 modulo p^e points (SzT), and the largest such e divides h if $q = p^h$ (SZIKLAI).
There are also examples of small blocking sets coming from linear sets. LUNARDON, POLVERINO, POMPEO. Many other people, including MICHEL LAVRAUW study linear sets (there is a Belgian and an Italian group).
Big open question (SZIKLAI): are all small minimal blocking sets linear?

Upper bounds

Definition

A blcking set is *minimal* if it contains no proper subset which is a blocking set: geometrically, this means that there is a tangent at each point.

Theorem (BRUEN-THAS)

The size of a minimal blocking set in Π_q *is at most* $q\sqrt{q}+1$.

For q a square, it can be sharp (in case of equality, we have a unital; lines meet it in 1 or $\sqrt{q}$ pts).
For q not a square it can be slightly improved, see Cossidente, Gács, Mengyán, Siciliano, SzT, Weiner.

Proposition

Let s *denote the fractional part of* $\sqrt{q}$ *and let* B *be a minimal blocking set in* Π_q, $q \geq 53$. *Then* $|B| \leq q\sqrt{q}+1-\frac{1}{4}s(1-s)q$.

More results in this direction

We remark that in the previous proposition for $q = 5$, the vertexless triangle is the largest minimal blocking set. Essentially, the result is true also for $q < 53$, except for $q = 26$.
The upper bound is extended to sets having a tangent at each of its points (so-called tangency sets, see later), by Illés, SzT, Wettl (related to a question of Gyárfás on the strong chromatic index of graphs).
The upper bound can also be proved using interlacing eigenvalues (HAEMERS).

Examples of (large min.) blocking sets

There are some constructions for blocking sets of size between $3(q+1)/2$ and $3q$ but relatively few larger examples are known (especially when q is not a square), for example when q is prime. In that case the largest examples come from cliques in the Paley graph (for $q \equiv 1$ modulo 4). The examples have size far from $q\sqrt{q}$, $q^{4/3}$ for q a cube.

A beautiful result of GÁCS shows that for Rédei type blocking sets the size is at least roughly $5q/3$, if q is a prime. There are very good results for Rédei type blocking set: BLOKHUIS, BALL, BROUWER, STORME, SzT; BALL.

One natural question is then to find the second largest minimal blocking set. Not much is known about it. BLOKHUIS, METSCH: in $\mathrm{PG}(2,q)$ there are no min.bl.set of size $q\sqrt{q}$.

What to expect? Add a point to the (classical) unital and delete its feet (the points where the tangents meet the unital). This way we can get min. bl. sets of size $q\sqrt{q}-\sqrt{q}+2$.

Some open questions

Let me mention some open questions about possible sizes of minimal blocking set. In some cases the answer is not known even for $\mathrm{PG}(2, q)$.

1. (Erdős) Is there a constant C such that there is a blocking set in any Π_q meeting every line in at most C points?
2. Improve the combinatorial bounds on the smallest and the largest minimal blocking set!
3. Given a constant C, is there a minimal blocking set of size roughly Cq in $\mathrm{PG}(2, q)$?
4. Given an exponent $1 < s < 3/2$, is there a minimal blocking set of size roughly q^s in $\mathrm{PG}(2, q)$?

Partial unitals

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.

Theorem (BALL)

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, we cannot get (very) large minimal blocking sets by locally modifying unitals.

Our main result

We will only work in Galois planes of square order, namely in $\mathrm{PG}(2, q^2)$.

Theorem (WEINER, SZT)

Let B be a point set of size at most $p^3 + 1 - (p-3)/2$ in $\mathrm{PG}(2, p^2)$, $p > 67$. Suppose that through each point of B there pass at least one 1-secant (tangent), in other words B is a tangeny set. Then B can be embedded in a unital.

We can also extend the result for general $q = p^h$, $p > 7$, $h > 1$ (with the same difference $(p-3)/2$).

Combinatorial properties

Let B be a set of points in $\mathrm{PG}(2, q^2)$. Furthermore, let $\ell_1, \ell_2, \ldots, \ell_{q^4+q^2+1}$ be the lines of $\mathrm{PG}(2, q^2)$ and let $n_i = |\ell_i \cap B|$, $i = 1, 2, \ldots, q^4 + q^2 + 1$, 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. $\sum_i n_i(n_i - 1) = |B|(|B| - 1)$.

Further combinatorial properties

Lemma

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

$$\sum_i (n_i-(q+1))^2 = q^5+(\varepsilon+1)q^2+2\varepsilon q+\varepsilon^2. \qquad (1)$$

Definition

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

Line-intersections

Lemma

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 $\ell_1, \ell_2, \ldots, \ell_{|B|}$ are the 1-secants guaranteed by Definition 12. Then

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

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.

Stability of k modulo p sets in $\mathrm{PG}(2, p)$

Result (WEINER, SZT; JCT A, 2018)

Let 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 $q - \sqrt{q}$.

Property

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. If, through a point Q, there are more than $q/2$ lines intersecting $\mathcal{M}$ in not k mod p points, then 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.

The general stability result

Result (WEINER-SZT; JCT A, 2018)

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 Property 15 holds. 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 the original paper by Weiner and SzT (JCTA, 2018), 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 15, we have to replace q by q^2 everywhere. Similarly, in Result 14 and Result 16, 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 14) and the number of modified points in Result 16 is $\lceil \frac{\delta}{q^2+1} \rceil$. Remark that we can use the results above when $q > 4$ (in $\mathrm{PG}(2, q^2)$).

Embedding in a 1 mod p multiset

Proposition

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.

We can verify the above Property 15 using the pigeon hole principle.

Modified points

Definition

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 17. 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 $-\frac{p-1}{2} \leq m_P \leq \frac{p-1}{2}$.

Corollary

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.

Bounds on multiplicities

Lemma

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

Lemma

A tangent line to B *must be tangent to* B^*.

Lemma

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

Theorem

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 23.

Corollary

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 23, we will show that B^* (from the previous section) is a unital.

Lemma

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

Embedding in a unital

Corollary

The size of B^* *is* $p^3 + 1$.

Lemma

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

Lemma

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

General case: the crucial counting lemma

Lemma

Let P be a point with multiplicity m_P in $\mathcal{N}$ and denote the lines through P by e_i, $i = 1, \ldots, q+1$. 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 $J \subset \{1, \ldots, q+1\}$, $\sum_{j \in J} |r_j| = A$. If $A \geq |J|$, then

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

(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 r_i containing at least one point from $\mathcal{N} \setminus \{P\}$.*

Another useful counting lemma

Lemma

Let P be a point with multiplicity m_P in $\mathcal{N}$ and denote the lines through P by e_i, $i = 1, \ldots, q+1$. Lines intersect B^* in $1 \bmod p$ 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 12. 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* $m_P + a_P \geq 2$.

General case: the steps

Proposition

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

Theorem

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

Corollary

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* $q^3 + 1 - (p - 3)/2$. □

Acknowledgment

Both authors (Zuzsa Weiner and SzT) were supported by OTKA Grant K124950 of the Hungarian National Research, Development and Innovation (NRDI) Office. In case of the second 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).

Thank you for your attention!