BLOKING SETS IN FINITE PLANES AND SPACES

Tamas SZONYI
Department of Computer Science, Eotvos University
H-1088, Budapest, Muzeum krt. 6.-8., Hungary

Abstract. We survey constructive and probabilistic results about the existence of blocking sets in higher dimensional spaces, blocking sets having few collinear points, and blocking sets in inversive planes.

1. Introduction

Blocking sets of projective planes were first introduced by di Paola in the sixties, and have been studied intensively since then. Let $\Pi(q)$ be a projective plane of order q. A subset S of $\Pi(q)$ is called a *blocking set* if S meets every line but contains no line. Using the same definition the notion of blocking set was extended to affine and projective spaces (see Mazzocca–Tallini [MT], Tallini [T]). Of course one can formulate the same condition in even more general structures such as hypergraphs and, surprisingly, blocking sets in hypergraphs and hypergraphs containing no blocking sets were studied by Erdős and others already at the beginning of sixties. They called a hypergraph having property B (after Bernstein) if there is a 2-colouring of the points without monochromatic edge. (Obviously any colour class in such a 2-colouring is just a blocking set in the hypergraph.) Today the name *2-colourable* is more common (and clearer) for these hypergraphs.

The aim of this short survey paper is to collect some interesting problems about blocking sets where the more general method gives stronger results than the explicit geometric constructions. For example, we tried to collect some easy applications of the probabilistic method and Lovász' bound concerning the ratio of the fractional and integral cover, as well as various refinements of Lovász' bound.

We concentrate only on the following problems: the existence problem of blocking sets in higher dimensional spaces, the existence of a blocking set having only few points on a line, and blocking sets in inversive planes. We survey the best results obtained by geometric constructions, and also the more general results for hypergraphs which are relevant. The main references about probabilistic results are the books Erdős–Spencer [ES], Spencer [S1] and Lovász [LL2].

This paper contains almost no new results, but some illustrative proofs are included. We hope that these results about hypergraphs are also interesting for geometers and can also orientate some future research.

I would like to end this introduction with my special thanks to **László Lovász, József Beck, Endre Boros and Zoltán Füredi**. I learnt the application of probabilistic methods in combinatorics (e.g. the use of Chernoff's inequality) from them.

2. Notation and preliminaries

Throughout the paper we use standard terminology ([F]). However as this survey is written to finite geometers, I would like to recall the terminology relevant to hypergraphs and probability theory. There are two technical comments on the notation, log denotes logarithm of base 2, and the end of the proof (or the absence of a proof) is marked by ∎.

Definition 2.1. A *hypergraph* $\mathcal{H}$ is a pair $(V(\mathcal{H}), E(\mathcal{H}))$, where $E(\mathcal{H})$ is a set of certain subsets of $V(\mathcal{H})$. We call the element of $V(\mathcal{H})$ *points*, while the elements of $E(\mathcal{H})$ *edges*. (So our definition does not allow repeated edges.) The *degree* of a point $P \in E(\mathcal{H})$ is just the number of edges that contain P. A hypergraph $\mathcal{H}$ is said to be *regular* (or: d-regular) if each point has the same degree d. More generally, if $A \subseteq V(\mathcal{H})$ then $deg(A)$ is the number of edges containing A. $\mathcal{H}$ is *uniform* (or: r-uniform) if every element of $E(\mathcal{H})$ has the same cardinality r. So, using the design theory terminology, a regular uniform hypergraph is just a 1-design.

So, for example the set of lines of a projective plane of order q form a hypergraph on q^2+q+1 points, which is $q+1$-regular and $q+1$-uniform. The set of lines of a space of three dimensions is still a $q+1$-uniform hypergraph, but the degree of a point is q^2+q+1, and the number of points is q^3+q^2+q+1.

Definition 2.2. The *covering number* of the hypergraph $\mathcal{H}$ is the minimum cardinality of points that intersect every edge of $\mathcal{H}$, and is denoted by $\tau(\mathcal{H})$.

For example, for any projective plane of order q, $\tau = q+1$ as it is easy to see that less than $q+1$ points cannot block every line, and a line is a set of $q+1$ points which intersects every line. Therefore this definition is not the same as the definition of a blocking set since our pointset might contain a line (sometimes the geometers call such a set an *intersection set*).

Definition 2.3. Let $\phi : V(\mathcal{H}) \longrightarrow \mathbf{R}^+$ be a mapping. If

$$\sum_{P \in E} \phi(P) \geq 1, \quad \text{for all} \quad E \in E(\mathcal{H}),$$

then we call ϕ a *fractional covering* of $\mathcal{H}$. The value

$$\min_{\phi} \sum_{P \in V(\mathcal{H})} \phi(P) = \tau^*$$

is called the *fractional covering number* of $\mathcal{H}$, where the minimum is taken over all fractional coverings.

For example, in case of regular and uniform hypergraphs, τ^* can easily be computed. It is not difficult to see that for a d-regular hypergraph,

$$|E(\mathcal{H})|/d \leq \tau^*.$$

On the other hand, $\tau^* \leq |V(\mathcal{H})|/r$ for r-uniform hypergraphs, as the mapping in which every point has weight $1/r$ is obviously a fractional covering. Counting incident point-hyperedge pairs yields

$$|V(\mathcal{H})| \cdot d = |E(\mathcal{H})| \cdot r$$

(which is just the standard equality for 1-designs), from which we immediately get

$$\tau^* = |V(\mathcal{H})|/r = |E(\mathcal{H})|/d$$

for d-regular r-uniform hypergraphs. For more details the reader is referred to [F, p.150].

A set that intersects every edge corresponds to a $0-1$ fractional covering, so we get immediately that $\tau^* \leq \tau$. On the other hand the difference between τ and τ^* is not too big as was proved by Lovász [LL1] (see also [LL2, 13.30]).

Theorem 2.4. (Lovász) If d denotes the maximum degree of the hypergraph $\mathcal{H}$ then

$$\tau(\mathcal{H}) \leq (1 + \log d)\tau^*(\mathcal{H}).$$

∎

Actually, this theorem was probably known before Lovász' paper, but he gave a greedy algorithm which produces intersection sets. The algorithm is the following: let us take first a point having maximum degree. This intersects some edges. Delete these edges and we get a hypergraph having fewer edges. Choose a point having maximum degree in this smaller hypergraph and iterate this process. We always end up with an intersection set. For example in case of a projective plane the first two points are arbitrary but the third is on the line determined by the first two. Then we always choose points of this line, so in the end we get a line which is an intersection set indeed. So in case of projective planes Lovász' greedy cover algorithm gives the best possible value.

Let us also include a very simple graph-version of this theorem.

Theorem 2.4'. Let G be a bipartite graph with bipartition $V(G) = L \cup U$. Suppose that the degree of every point of L is at least d. Then we can find a set B of at most $(|U| \log |L|)/d$ points of U such that each point of L is joined to at least one point of $B \subset U$. ∎

For every point $x \in L$ let

$$N(x) = \{\, y \in U \,:\, xy \text{ is an edge in } G \,\}$$

be the set of neighbours of x. Let $\mathcal{H}$ be the hypergraph with $V(\mathcal{H}) = U$, $E(\mathcal{H}) = \{N(x) : x \in L\}$. Of course we keep the repeated edges (which correspond to points with $N(x) = N(y)$) only once. Obviously the mapping $\phi(u) = 1/d$ $u \in U$ is a fractional covering, so $\tau^* \leq |U|/d$. Since the maximum degree of $\mathcal{H}$ is less than $|L|$, Theorem 2.4 gives this graph-version indeed.

There are other estimates on the ratio τ/τ^*, here we recall two of them. The first one was proved by Frankl and Rödl [FR] using the proof technique called the Rödl nibble (for an informal description see [S2]). This technique was originally used to show the existence of hypergraphs which are nearly designs. The result of [FR] says that sometimes the log-factor can be omitted from Theorem 2.4. Namely let our hypergraph be d-regular for some fixed d (having m vertices and n hyperedges), and suppose that it is almost uniform, i.e. each hyperedge has asymptotically $R = R(n)$ points. (Here $R(n)$ tends to infinity.) Moreover suppose that every two hyperedges intersect in only $o(R)$ points. Then there is an intersection set consisting of $\sim n/d$ points, which is obviously best possible. More precisely (with ε's and δ's) they proved the following fundamental result.

Theorem 2.5. ([FR]) Suppose $\varepsilon > 0$ is arbitrary, $\mathcal{H}$ is a d-regular hypergraph with a fixed d, $|E(\mathcal{H})| = n$, $a > 3$ is a real number. There exists a $\delta = \delta(\varepsilon) > 0$ such that if for some D one has $(1-\delta)D < |A| < (1+\delta)D$ for all $A \in V(\mathcal{H})$ and $|A \cap B| < D/(\log n)^a$ for all $A \neq B \in V(\mathcal{H})$, then for all $n > n_0(\delta)$,

$$\tau(\mathcal{H}) \leq n(1+\varepsilon)/d \quad \text{holds.}$$

∎

Of course this seems to be much better in geometric applications than Lovász' original result, since the intersection condition of Theorem 2.5 is quite natural in case of geometric problems (at least if the number of blocks is not exponential in D). However, the price is that the point-degrees are constant, which is quite restrictive in geometric problems. The $(\log n)^a$-factor in the intersection condition was eliminated by Pippenger and Spencer [PS], who strengthened and generalized the methods of Frankl and Rödl. As the affine plane $AG(2,q)$ satisfies all the conditions of Theorem 2.8 except that $d = q+1$ is not a constant, we see that some condition on the order of magnitude of d (compared to n) is indeed necessary.

The second refinement on Lovász' bound on τ/τ^* uses the notion of VC-dimension. The *Vapnik–Chervonenkis dimension* (or *VC-dimension*, for short) of a hypergraph $\mathcal{H} = (V(\mathcal{H}), E(\mathcal{H}))$ is the maximum size of a subset $A \subset V(\mathcal{H})$ with the property that every $B \subseteq A$ is a "trace" of an element of $E(\mathcal{H})$ on A, i.e. there exists an $E_B \in E(\mathcal{H})$ with $E_B \cap A = B$. For example if we take the lines of a projective space $PG(n,q)$ $(n \geq 2)$, then A itself is a trace, i.e. A is contained in a line r. Obviously, $|A| \leq 2$ as the

other lines intersect r in at most 1 point. Therefore the VC-dimension of this design is 2. Similarly, the VC-dimension of the design of hyperplanes of $PG(n,q)$ is n (and the points of a good A form a basis in a hyperplane).

A remarkable fact is that the number of edges in a hypergraph of small VC-dimension is polynomial in $|V(\mathcal{H})|$. Because of its importance, the theorem was rediscovered several times (by Sauer, Perles, Shelah, Vapnik–Chervonenkis). For the sake of simplicity we just refer to a recent survey [FP], where some proofs and all the references can be found.

Theorem 2.6. For any hypergraph with $|V(\mathcal{H})| = n$ and VC-dimension d,

$$|E(\mathcal{H})| \leq \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{d}.$$

∎

Now let us see some theorems which relate the VC-dimension of $\mathcal{H}$ with the ratio $\tau^*(\mathcal{H})/\tau(\mathcal{H})$. Again we only state the first and then the best result, other results and applications can be found in [FP].

Theorem 2.7. (Haussler, Welzl [HW]) Let $\mathcal{H}$ be a hypergraph with VC-dimension d all of whose edges are of size at most $\varepsilon|V(\mathcal{H})|$ for some fixed $0 < \varepsilon < 1$. Then

$$\tau(\mathcal{H}) \leq \left[\frac{8d}{\varepsilon}\log\frac{8d}{\varepsilon}\right].$$

Theorem 2.8. (Komlós, Pach and Woeginger [KPW]) For any hypergraph $\mathcal{H}$ with VC-dimension d we have

$$\tau(\mathcal{H}) \leq d\tau^*(\mathcal{H})(\log\tau^*(\mathcal{H}) + 2\log\log\tau^*(\mathcal{H}) + 3),$$

provided that $\tau^*(\mathcal{H})$ is sufficiently large.

We do not mention here the other important parameters of a hypergraph and their connections (including many other results in the spirit of Theorems 2.4–2.8), but the reader is referred to the excellent survey [F] by Füredi.

From probability theory only basic facts are used (see Rényi [Ré]). The probability of the event A will be denoted by $Prob(A)$, the expectation and variance of a random variable ξ will be denoted by $E(\xi)$ and $D(\xi)$ respectively. The following lemma of Chernoff, which is an improvement on Chebytcheff's famous inequality for a particular class of random variables, plays a crucial role in various probabilistic results.

Theorem 2.9. (Chernoff) Let ξ_i $(i = 1, \dots n)$ be independent (discrete) random variables with $Prob(\xi_i = 1) = p$, $Prob(\xi_i = 0) = 1 - p$ $(i = 1, \dots n)$. Let $\eta = \xi_1 + \dots + \xi_n$ (which is a random variable having binomial distribution). Then

$$Prob\Big(|\eta - E(\eta)| \geq x \cdot D(\eta)\Big) \leq \exp\Big(\frac{-x^2}{2}\Big)$$

for every $x \geq 0$.

Actually, the proof of 2.9 is quite easy, one applies Chebytcheff's inequality for the random variable $\zeta = \exp(\xi_1 + \dots + \xi_n)$. (Of course $\exp(x)$ denotes e^x.)

3. Blocking sets in higher dimensional spaces

The fundamental question about blocking sets in higher dimensions is that of existence. Roughly speaking the results tell us that there are no blocking sets if the dimension is large compared to the order, but there do exist blocking sets if the dimension is small enough. For example if $q = 2$ then there are no blocking sets in the plane, i.e. in $PG(2, 2)$, but for $q > 2$ there are blocking sets in any projective plane of order q.

Using a geometric version of Ramsey's theorem due to Graham, Leeb, and Rothschild [GLR], Mazzocca and Tallini [MT] proved the following non-existence result.

Theorem 3.1. There exist $h_a = h_a(q)$ (and $h_p = h_p(q)$) such that there are no blocking sets in $AG(h, q)$ (or in $PG(h, q)$) for $h \geq h_a$ (or $h \geq h_p$).

(See also 14.23. of [LL2].) Mazzocca and Tallini also studied the relation between h_a and h_p. Unfortunately, these h's are very big compared to q.

On the other hand, when the dimension is small blocking sets exist. First let us summarize the known constructions, then we will see that the probabilistic argument gives a much better bound for the dimension h_p. As we mentioned earlier, in $PG(2, q)$ blocking sets exist, when $q > 2$. In $PG(3, q)$, Rajola [R] showed that blocking sets exist for $q > 4$. For $q = 2, 3$ there are no blocking sets in $PG(3, q)$. The case $q = 4$ is still open, partial results can be found in Metsch [M]. Using a recursive construction, Beutelspacher and Eugeni [BE] showed that for $q \geq 2^h$ there do exist blocking sets in $AG(h, q)$. In $PG(3, q)$ Blokhuis and Fisher (private communication) gave the following example. Consider $AG(3, q)$ as $GF(q^3)$ and let S be the set of squares in $GF(q^3)$. Then S, regarded as a point set of $AG(3, q)$ is a blocking set for $q \geq 5$. (So this is another proof of Rajola's result.) Hirschfeld and Szőnyi [HSz] generalized this example and improved the bound $2^h \leq q$ to $h^2 - 1 \leq q$.

On the other hand, using probabilistic arguments much more is known for more general structures.

Theorem 3.2. (Erdős–Hajnal, [EH]) Let $\mathcal{H} = (V(\mathcal{H}), E(\mathcal{H}))$ be an n-uniform hypergraph with $|E(\mathcal{H})| \leq 2^{n-1}$. Then there is a subset $B \subset V(\mathcal{H})$ which intersects every edge, but contains no edge; in other words $\mathcal{H}$ is 2-colourable.

Sketch of the proof. List the edges, let $E(\mathcal{H}) = \{E_1, \ldots, E_m\}$. Colour the points with two colours at random, independently of each other and with probability $1/2$. If A_i denotes the event that E_i is monochromatic, then it is easy to see that $Prob(A_i) = 2^{-n+1}$. So the probability of having a monochromatic edge is

$$Prob(A_1 + \ldots A_m) < \sum_{i=1}^{m} Prob(A_i) = \frac{m}{2^{n-1}} \leq 1.$$

For the details we refer to [ES, p.19], [S1, p. 8] or [LL, 13.41.].

Using the geometric language this is a theorem about the existence of blocking sets. Although this result is quite good it can be improved. In general, Beck [Be] proved that every hypergraph on n points and with m edges has a blocking set if $m < 2^{n-1}n^{1/3-\epsilon}$. Beck's proof uses a very clever refinement of the probabilistic method, the "deletion method". Roughly speaking, one takes a random configuration and proves that it is bad in only a few places. Then these bad spots can be deleted and after this "small modification" the object has the desired property. More details on applications of the deletion method can be found in [S1, Lecture 2]. On the other hand this result is basically sharp as there are hypergraphs with m edges having no blocking sets, where $m = cn^2 \cdot 2^n$ (see [LL2, 13.42.]).

For the particular case when the edges of the hypergraph are either disjoint or have exactly one point in common, Erdős and Lovász [EL] proved the following theorem.

Theorem 3.3. (Erdős–Lovász) Let $\mathcal{H}$ be an r-uniform hypergraph having n points and m edges and suppose that two edges have at most one point in common. Then
(a) If $n \leq 2^{r-4}$, then there is a blocking set in $\mathcal{H}$ (in other words, $\mathcal{H}$ is 2-colorable).
(b) If $m \leq 4^{r-4}/r^3$, then there is a blocking set in $\mathcal{H}$.

(See also [LL2, 13.44].) This theorem is essentially sharp, as Erdős and Lovász [EL] proved that there do exist r-uniform hypergraphs with $m < cr^4 4^r$ hyperedges, which are not 2-colourable and any two edges intersect in at most 1 point.

The proof of (b) is based on the same idea as the proof of Theorem 3.2. The cornerstone is the following probabilistic lemma, which is now called "Lovász' local lemma".

Theorem 3.4. (Lovász' local lemma) Let G be a (finite) graph with maximum degree d and vertices $v_1, \ldots, v_n$. Let us associate an event A_i with v_i $(i = 1, \ldots, n)$ and suppose that A_i is independent of the set

$$\{A_j \ : \ (v_i, v_j) \notin E(G)\}.$$

Also suppose $Prob(A_i) \leq 1/(4d)$. Then

$$Prob(\bar{A}_1 \cdot \ldots \cdot \bar{A}_n) > 0.$$

∎

(In the proof of Theorem 3.3 the vertices of G are the hyperedges of $\mathcal{H}$ and A_i is the event that the hyperedge is monochromatic.)

Theorem 3.4 is a sieve method improving on the usual counting sieve if there is much independence among the events $A_1, \ldots, A_n$. The common feature of Lovász' local lemma and the deletion method is that they help us in finding (or at least in proving the existence of) rare points, i.e. it works even when the set of good points is very small. We saw another similar method, the Rödl nibble, in Section 2. An asymmetric version and various applications of the local lemma can be found in [S1, Lecture 8].

Let us see what Theorem 3.3 gives us for projective spaces. In $PG(n,q)$ we have roughly q^n points, q^{2n-2} lines. So as long as $q^{2n-2} \leq 4^{q-4}/q^3$ blocking sets exist. Taking logarithms of base 2 on both sides we get

$$(2n-2)\log q \leq 2(q-4) - 3\log q,$$

so for $n \leq \dfrac{q-4}{\log q} - \dfrac{1}{2}$ there do exist blocking sets in $PG(n,q)$, and this bound is much better than the bounds obtained from the various constructions.

Let us make some "philosophical" comments on the fact that the construction is much worse than the probabilistic method. The reason is that the constructions want to produce "regular" blocking sets. For example, the blocking sets in [HSz] have the property that every line intersects them in roughly $q/2$ points, at least when the dimension is small compared to q. (Other constructions produce blocking sets which are not regular in this sense but e.g. they contain q points on a line etc.) This procedure can be simulated using random selection. If one chooses each point independently with probability $1/2$, then what we get is a blocking set having roughly $q/2$ points on each line. This selection works if the dimension $n \leq \sqrt{q}/2$, which can be seen using Chernoff's inequality. So the essential difference is that in the proof of Theorem 3.2 every subset was taken into account, i.e. they had a chance of being chosen, while the constructions choose among "regular" or extremely irregular subsets.

4. Blocking sets with small line intersections

In this chapter we are dealing with blocking sets whose intersection with each line contains a limited number of points. We say that a projective plane π has property $B(c)$ if there is a blocking set S whose intersection with each line of π contains less than c points. For a blocking set B, $c(B)$ denotes the maximum number of collinear points of B. Before the results let us mention that the obvious examples of blocking

sets (Baer-subplanes, unitals, and blocking sets contained in the union of three lines) are very bad regarding $c(B)$, i.e. $c(B) = \sqrt{q} + 1$ or $c(B) \geq (q+1)/2$ in these cases.

Erdős has asked whether there exists an absolute constant c such that every projective plane has property $B(c)$. Instead of a constant c, Erdős, Silverman, and Stein [ESS] proved the following result.

Theorem 4.1. (Erdős–Silverman–Stein) Every projective plane of order n has property $B(c \log n)$, if n is sufficiently large and $c > 2e$.

Sketch of the proof. (I learnt the idea of this proof from Zoltán Füredi. We will only concentrate on showing the existence of a blocking set B with $c(B) \leq c \log n$, but not on the best value of c.) Let us denote the number of points (as usual) by v, the number of blocks by b, and the size of a line by k. Let us select the points independently at random with probability $p = (C \log k)/k$. Then first of all the expected number of points will be $p \cdot v \sim (C \cdot v \log k)/k$. Then list all the lines (blocks) $L_1, \ldots, L_b$ and concentrate on one line L_1, say. Let the points of L_1 be $P_1, \ldots, P_k$. Because of the independent selection to each point P_i $(i = 1, \ldots, k)$ there corresponds a random $0-1$-variable ξ_i which takes the value 1 iff the point is selected, and these independent random variables satisfy the conditions of Theorem 2.9 (Chernoff's inequality) with $p = (C \log k)/k$. Then the value of $\eta_1 = \xi_1 + \ldots + \xi_k$ is just the number of points selected on the line L_1. As η_1 has binomial distribution its expected value $E(\eta_1) = kp = C \log k$, its variance is $D(\eta_1) = \sqrt{kp(1-p)} \leq \sqrt{C \log k}$. So Chernoff's inequality gives (for $x \geq 0$) that

$$Prob\Big(|\eta_1 - E(\eta_1)| \geq x \cdot D(\eta_1)\Big) \leq \exp\Big(\frac{-x^2}{2}\Big).$$

We are going to apply this for $x = c^* \sqrt{\log k}$, where the new constant $c^* < C$. This is good a choice because then $xD(\eta_1)$ is less than $E(\eta_1)$. Therefore we will certainly bound using the previous inequality the probability that no points or more than $2C \log k$ points of L_1 are selected. The actual bound is at most

$$\exp((-x^2)/2) = \exp(((-c^{*2})/2) \log k) = k^{((-c^{*2})/2)}.$$

One can do this similarly for each line L_i. If B denotes the set of chosen points then $|B \cap L_i| = \eta_i$ and therefore

$$Prob\Big(|B \cap L_i| < (C - c^*) \log k, \quad \text{or} \quad |B \cap L_i| > C^* \log k\Big) \leq k^{((-c^{*2})/2)}.$$

Using the obvious bound for the probability of the sum of events we get immediately that

$$Prob\Big(\exists i : |B \cap L_i| < (C - c^*) \log k, \text{ or } |B \cap L_i| > C + c^*) \log k\Big) \leq b k^{((-c^{*2})/2)}.$$

In our case $b < k^2$ so if $c^* > 2$ then this probability is strictly less than 1, which means that there exists a B for which

$$(C-2) \log k \leq |B \cap L_i| \leq (C+2) \log k, \quad \forall i = 1, \ldots, b.$$

The only thing we needed was $C > c^*$, i.e. for $C > 4$ one can choose a c^* for which this proof works. ∎

First of all remark that in [ESS] the value of the constant is better. Our second remark is that the same computation can be done if we find a constant r so that $k^r > b$, which shows that blocking sets with small line intersections do exist in more general block designs. (Actually from this proof one gets $4r \log k$ as an upper bound for the number of points lying on one block.) Finally let us remark that Abbott and Liu [AL] improved this result for the special case of Galois planes $PG(2,q)$, q is an odd prime power, and proved that the condition on c may be replaced by $c > 2/\log 2$.

On the other hand, Ughi [U] proved that in $PG(2,q)$, q odd, from the union of c conics one can never get a blocking set, where c is a constant and q is large enough compared to c. Let us remark here that Ughi also proved that there are $c \log q$ suitably chosen conics that form a blocking sets. This is clear from Theorem 2.4' if we apply it for the following bipartite graph: points of the "upper" level U are the irreducible conics, points of the "lower" level L are the lines of $PG(2,q)$, a conic and a line being adjacent exactly when they are not disjoint. Here there are roughly q^2 points of the lower and q^5 of the upper level, while the degree of points of L is at least roughly $(q^5 - q^3)/2$ (roughly half of the conics intersect a given line in two points over $GF(q)$). Now Theorem 2.4' shows that one can choose at most $2\log(q^2+q+1)$ conics such that they intersect each line. (Actually Ughi's proof was based on a counting argument and was essentially the same as this.)

For particular classes of planes there are constructions showing the existence of blocking sets having at most 4 points on a line.

Theorem 4.2. (Bruen–Fisher, [BF]) $PG(2,3^r)$ has property $B(5)$. ∎

This result was generalized by Boros [Bo], who proved that in the plane $PG(2,p^r)$, $p > 2$ prime, there is a blocking set S of size $2p^r$ having not more than $p+1$ points on a line. In other words, the plane $PG(2,p^r)$, $p > 2$ has property $B(p+2)$. Let us remark that Theorem 4.2 is better than Theorem 4.1 only if r is very big compared to p.

Theorem 4.3. (Illés–Szőnyi–Wettl, [ISzW]) The plane $PG(2,2^r)$ has property $B(6)$ if r is even, and $B(7)$ if r is odd. ∎

In the case r is even the proof is similar to the constructions of Bruen–Fisher and Boros, while in the case r odd we proved that the union of three suitably chosen conics form a blocking set. This also shows that in the result of Ughi the condition q odd was necessary indeed.

5. Blocking sets in inversive planes

Of course blocking sets can be studied in various geometric structures. In case of projective and affine planes we know something about blocking sets. A natural next step would be to study blocking sets in an inversive plane as these are one-point extensions of affine planes. As usual we will concentrate on classical (i.e. Miquelian) inversive planes. Let $M(q)$ be such an inversive plane of order q and B be a blocking set (or better: intersection set) in $M(q)$. As $M(q)$ is a 3-design on q^2+1 points, it is a $q+1$-uniform, q^2+q-regular hypergraph, so by the remark after DEfinition 2.3 we get that $\tau^* = (q^2+1)/(q+1)$, which also yields a lower bound for the value of τ. This general bound on τ can be improved.

Take a point $P \notin B$ and form the point-residual of $M(q)$ with respect to P. This is the desarguesian affine plane $AG(2,q)$, and B has to block all the lines of $AG(2,q)$. Then by a result of Jamison [J] and Brouwer–Schrijver [BSch] one has $|B| \geq 2q-1$. Let us remark that the same lower bound is true for arbitrary inversive planes.

Theorem 5.1. (Bruen–Rothschild [BR]) If S is a blocking set in any inversive plane of order q, then $|S| \geq 2q$ for $q \geq 9$, and $|S| \geq 2q-1$ for $q \neq 3$. ∎

So we have a lower bound on $|B|$ but essentially no constructions are known. From Lovász' theorem (Theorem 2.4) one gets that there are intersection sets with cardinality $|B| \leq Cq\log q$.

Another approach would be to use random selection. In the previous section we formulated the proof of Theorem 4.1 in such a way that there is a blocking set intersecting every block in at most $c\log q$ points, if there is a fixed r for which $b < k^r$. In our case $k = q+1$, $b = (q^2+1)(q+1)q$, so this condition is satisfied with $r = 3$. This again gives the existence of a blocking set of size $Kq\log q$.

Finally, one can also show the existence of an intersection set consisting of $C\log q$ circles by using Theorem 2.4.' for the following graph: the point of the lower level are circles, the points of the upper level are again circles and we join two circles if they have non-empty intersection. What is the degree of a point in this graph? There are $\binom{q+1}{2}\cdot q$ circles intersecting the given circle in two points and other $(q+1)q$ circles intersecting it in one points. The total number of circles is $\binom{q^2+1}{3}/\binom{q+1}{3} = (q^2+1)q$. Therefore the minimum degree is roughly half the number of points, and Theorem 2.4' gives the existence of roughly $3\log q$ circles which intersect every other circle. So this is again an intersection set having about $Cq\log q$ points. It might be interesting to note that in this last construction we really need $c\log q$ circles as the following theorem shows.

Theorem 5.2. Suppose that the union of k circles of an inversive plane intersects every circle. Then $k > c\log q$, for a suitable constant $c > 0$.

Sketch of the proof. List the circles $C_1, \ldots C_k$ of our intersection set. Consider a point P which does not belong to the union of these circles. Then in particular we have to block all the circles through P. These are exactly the lines of a (classical) affine plane,

the point-residual of the inversive plane. Using coordinates on this affine plane let the equation of C_i be $(x-a_i)^2 - k(y-b_i)^2 = r_i$, where k is a fixed non-square of $GF(q)$. Take a point $A(a,b)$ of the affine plane and consider the lines through A. Such a line does not intersect C_i if and only if a certain quadratic polynomial $f_i(m)$ is a non-square, where m denotes the slope of the line. Without computation we can guess what these polynomials are. Namely the the zeroes of $f_i(m)$ correspond to the slopes of the tangents of C_i passing through A, so $f_i(m) = k_i(m-m_{i,1})(m-m_{i,2})$, where $m_{i,1}$ and $m_{i,2}$ denote the slopes of the tangents (which belong to $GF(q^2)$). (We can exclude the possibility that there is a vertical tangent through A; as C_i has two vertical tangents so if A does not lie on any of these $2k$ lines, then the polynomials $f_i(m)$ are quadratic polynomials indeed.) Also we can suppose that $A \notin C_i$ $(i = 1,\dots,k)$, so these polynomials have no multiple roots. We are going to apply Lemma 1 of [Sz]. In order to do this, it is sufficient that no two polynomials $f_i(m)$ have a common root. But a common root of f_i and f_j corresponds to a common tangent to C_i and C_j passing through A. There are at most 4 common tangents to each pair (i,j) so this condition excludes at most $(k-1)k/2$ tangents, which cover at most $qk(k-1)/2$ points of the plane. So the total number of excluded points is $k(q+1) + 2kq + qk(k-1)/2$. This is much less than the number of points, so we can find a point A, such that for the polynomials $f_i(m)$ $(i = 1,\dots,k)$ all conditions of Lemma 1 of [Sz] are satisfied. Therefore we find at least

$$\frac{q}{2^k} - k(\sqrt{q}+1)$$

values of m with $f_i(m)$ being a non-square for every $i = 1,\dots,k$. Geometrically this means that there is a line through A which does not intersect $C = \cup_i C_i$, that is C is not an intersection set, if $k \le (1/2 - \varepsilon)\log q$. ∎

Remark. Actually the same proof shows that Ughi's result (see [U]) is essentially sharp in the sense that if we want to block all the lines of a projective plane by the union of some conics then we really need about $c\log q$ conics. As we already remarked in the previous section, this theorem does not extend to planes of even order (cf. the remarks after Theorem 4.3).

6. References

[AL] Abbott, H.L. and Liu, A.: Property of B(s) and projective planes, *Ars Combinatoria* **20** (1985), 217–220.

[Be] Beck, J.: On 3-chromatic hypergraphs, *Discrete Math.* **24** (1978), 127–137.

[BE] Berardi, L. and Eugeni, F.: On the cardinality of blocking sets in $PG(2,q)$, *J. of Geometry* **22** (1984), 5–14.

[BeE] Beutelspacher, A. and Eugeni, F.: On blocking sets in projective and affine spaces of large order, *Rend. di Mat. (Roma)* **6**, (1986), 587–595.

[Bo] Boros, E.: $PG(2,p^s)$, $p>2$ has property B(p+2), *Ars Combinatoria* **25** (1988), 111–114.

[BSch] Brouwer, A.E. and Schrijver, A.: The blocking number of an affine space, *J. Comb. Theory (A)* **24** (1978), 251–253.

[B1] Bruen, A.A.: Baer subplanes and blocking sets, *Bull. Amer. Math. Soc.* **76** (1970), 342–344.

[B2] Bruen, A.A.: Blocking sets in finite projective planes, *SIAM. J. Appl. Math.* **21** (1971), 380–392.

[BF] Bruen, A. and Fisher, J.C.: Blocking sets and complete arcs, *Pacific J. Math.* **53** (1974), 73–84.

[BR] Bruen, A. and Rothschild, B.L.: Lower bounds on blocking sets, *Pacific J. Math.* **118** (1985), 303–311.

[BT] Bruen, A.A. and Thas, J.A.: Blocking sets, *Geom. Ded.* **6**, (1977), 193–203.

[D] Di Paola, J.W.: The shape of minimum blocking sets in small planes, *Ars Combinatoria* **20-B** (1985), 15–26.

[EH] Erdős, P. and Hajnal, A.: On a property of families of sets, *Acta Math. Hung.* **12** (1961), 87–123.

[EL] Erdős, P. and Lovász, L.: Problems and results on 3-chromatic hypergraphs and some related qusetions, in: *Infinite and Finite Sets*, Coll. Math. Soc. J. Bolyai **10**, Bolyai–North-Holland (1974), 609–627.

[ESS] Erdős, P., Silverman, R. and Stein, A.: Intersection properties of families of sets of nearly the same size, *Ars Comb.* **15** (1983), 247–259.

[ES] Erdős, P. and Spencer, J.: *Probabilistic Methods in Combinatorics*, Akadémiai Kiadó, Budapest, 1974.

[FR] Frankl, P. and Rödl, V.: Near Perfect Covers in Graphs and Hypergraphs, *Eur. J. Comb.* **6** (1985), 317–326.

[F] Füredi, Z.: Matchings and Covers in Hypergraphs, *Graphs and Combin.* **4** (1988), 115–206.

[FP] Füredi, Z. and Pach, J.: Traces of finite sets, extremal problems and geometric applications, in: *Extremal problems in combinatorics, Visegrád, Hungary 1991*, to appear.

[GLR] Graham, R.L., Leeb, K. and Rothschild, B.L.: Ramsey's theorem for a class of categories, *Adv. in Math.* **8** (1972), 417–433.

[HW] Haussler, D. and Welzl, E.: ε-nets and simple range queries, *Discr. Comput. Geom.* **2** (1987), 127–151.

[H] Hirschfeld, J.W.P.: *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1976.

[HSz] Hirschfeld, J.W.P. and Szőnyi, T.: Constructions of large minimal blocking sets and (k,n)-arcs in Galois-planes, *Europ. J. Comb.* **12** (1991), 499–511.

[ISzW] Illés, T., Szőnyi, T. and Wettl, F.: Blocking sets and maximal strong representative systems in finite projective planes, *Mitt. Math. Sem. Giessen* **201** (1991), 97–107.

[IM] Innamorati, S. and Maturo, A.: On irreducible blocking sets in projective planes, *Ratio Math.* **2** (1991), 151–155.

[J] Jamison, R.E.: Covering finite fields by cosets of subspaces, *J. Comb. Theory (A)* **22** (1977), 253–266.

[KPW] Komlós, J., Pach, J. and Woeginger, G.: Almost tight bounds for ε-nets, *Discr. Comput. Geometry* **7** (1992), to appear.

[LL1] Lovász, L.: On the ratio of optimal integral and fractional covers, *Discrete Math.* **13** (1975), 383–390.

[LL2] Lovász, L.: *Combinatorial problems and exercises*, Akadémiai Kiadó, Budapest, 1979.

[MT] Mazzocca, F. and Tallini, G.: On the non-existence of blocking sets in $PG(n,q)$ and $AG(n,q)$ for all large enough n, *Simon Stevin* **1** (1985), 43–50.

[M] Metsch, K.: Blocking sets in $PG(3,4)$?, *Mitt. Math. Sem. Giessen* **201** (1991), 119–131.

[PS] Pippenger, N. and Spencer, J.: Asymptotic Behavior of the Chromatic Index for Hypergraphs, *J. Comb. Theory A* **51** (1989), 24–42.

[R] Rajola, S.: A blocking set in $PG(3,q)$, $q \geq 5$, *Annals of Discrete Math.* **37** (1988), 391–394.

[Rö] Rödl, V.: Proof of the Erdős–Hanani conjecture, *European. J. of Comb.* **6** (1985), 69–78.

[Ré] Rényi, A.: *Probability Theory*, Akadémiai Kiadó, Budapest, 1970.

[S1] Spencer, J.: *Ten lectures on the probabilistic method*, SIAM Publication, 1987.

[S2] Spencer, J.: The probabilistic method, Chapter for *The Handbook of Combinatorics* (ed. by: R.L. Graham, M. Grötschel, L. Lovász), North-Holland, to appear.

[Sz] Szőnyi, T.: Note on the existence of large minimal blocking sets in PG(2,q), *Combinatorica* **12** (1992), to appear.

[T] Tallini, G.: Blocking sets in projective and affine spaces, *Ann. Discr. Math.* **37** (1988),433–450.

[U] Ughi, E.: On (k,n)-blocking sets which can be obtained as a union of conics, *Geom. Ded.* **26** (1988), 241–245.