RANDOM CONSTRUCTIONS AND DENSITY RESULTS

ANDRÁS GÁCS AND TAMÁS SZŐNYI

ABSTRACT. In this paper we outline a construction method which has been used for minimal blocking sets in $\mathrm{PG}(2,q)$ and maximal partial line spreads in $\mathrm{PG}(n,q)$ and which must have a lot of more applications. We also give a survey on what is known about the spectrum of sizes of maximal partial line spreads in $\mathrm{PG}(n,q)$. At the end we list some more elaborate random techniques used in finite geometry.

1. INTRODUCTION

The probabilistic method was invented by Erdős, and the simplest form is just a counting technique for existence proofs. This paper is written for finite geometers and our aim is to convince them that probabilistic methods may be helpful even if someone wants to end up with an explicit result. The standard sources for the probabilistic method are the books by Alon, Spencer [4] and Erdős, Spencer [32].

The paper is mainly devoted to a construction method used in [85] and [37] to find minimal blocking sets of $\mathrm{PG}(2,q)$ and maximal partial spreads in $\mathrm{PG}(n,q)$. One ingredient of the technique is to find a certain blocking set within a structure depending on the particular problem. This should be done by random choice. We already stress here that this probability argument is always trivial, one simply determines the number of possible choices for a structure of given size, then gives an upper bound on the number of "bad choices" which is still smaller than the previous number. It is not surprising that these simple applications of the probabilistic method work successfully for blocking sets in certain structures, since one of the first results obtained by the probabilistic method were about hypergraphs having property B (after Bernstein). A hypergraph has property B if there is a 2-colouring of the points without monochromatic edges. Obviously, any colour class in such a 2-colouring is just a blocking set in the hypergraph.

The paper is organized in 8 sections. In Section 2 we give the background for trivial random choice, in Sections 3, 4 and 5 we outline three constructions behind which there is always the same idea. In Section 6 we give a little more background for the trivial random choice by summarizing some notions and results about covers and fractional covers of hypergraphs. Finally, in Sections 7 and 8 we try to collect more applications of the probabilistic method in finite geometry. Section 7 still contains rather elementary applications of the method, while Section 8 is devoted to more sophisticated applications. For people only interested in the probabilistic part, we suggest that they read sections 2, 6, 7 and 8 (though in Sections 3, 4 and 5 they can learn about geometric results which might be improved by using more elaborate probabilistic techniques). For those readers

The first author was supported by Bolyai grant and OTKA grant F 043772. Both authors were supported by OTKA grants T 043758, T 049662 and T 67867, and TÉT grant E16/04.

who are only interested in the construction method, we suggest that they read the first half of Section 2 (until Lemma 2.3) and Sections 3, 4 and 5.

2. Some examples for trivial random choice

In this section we give some examples where the existence of a structure (with certain properties) of prescribed size can be guaranteed by counting the number of choices for such a set exactly and giving an upper bound still smaller than the previous number, for the number of bad choices. We call this method **trivial random choice**. This name will be explained later.

1. How to find a set of k points in $PG(2,q)$ meeting every line?

In $\mathrm{PG}(2,q)$ there are q^2+q+1 points, so the number of k-element point sets is $\binom{q^2+q+1}{k}$. How many of these point sets do not meet every line? If we fix a line ℓ, then there are exactly $\binom{q^2}{k}$ sets not meeting ℓ. If we multiply this by the number of lines of $\mathrm{PG}(2,q)$, we find the following (very bad) upper bound for the number of k-element point sets that are not blocking all lines: $\leq (q^2+q+1)\binom{q^2}{k}$. A little calculation shows that for $k \geq cq\log q$ with c sufficiently large, this is smaller than $\binom{q^2+q+1}{k}$, so this enumeration implies that there is at least one choice where our $cq\log q$-element point set does block every line. (We omit the calculation here, but it is a particular case of the proof of Lemma 2.3. Throughout the text log will mean natural base logarithm.)

Of course, there are at least two reasons why this method does not seem to be very useful at first glance: on the one hand, in $\mathrm{PG}(2,q)$ there are blocking sets of size $q+1$ (namely the lines), so we did not find examples close to the smallest possible size; on the other hand, usually one is looking for minimal blocking sets (that is, sets meeting every line and being minimal to this property) and this method is not good to handle such extra conditions. But as we shall see later, sometimes we do find the smallest desired sets and using extra geometric arguments together with random choice, we can guarantee the sets to be minimal (or maximal, according to which we need for the particular problem).

The first non-trivial application of this technique goes back to Erdős, who used it to derive the lower bound $2^{k/2}$ for the Ramsey number $R(k,k)$ [29], while the current best constructive lower bound is not nearly as good.

2. Small dominating sets in a Paley graph

Recall that the **Paley graph $\mathbf{P}(q)$** (defined for all prime powers $q \equiv 1(4)$) has the elements of the finite field $\mathrm{GF}(q)$ as vertices, and two distinct vertices a and b are joined by an edge if and only if $a-b$ is a square in $\mathrm{GF}(q)$. There are many nice properties of these graphs, see [25], all we will use here is that they are $\frac{q-1}{2}$-regular.

A **dominating set** $X \subseteq V(G)$ in any graph G is a set with the property that for any $v \in V(G)\setminus X$, v has at least one neighbour in X. For Paley graphs this is equivalent to saying that for any $t \in GF(q)$ there is an $x \in X$ s.t. $x-t$ is a square.

For a prime power $q \equiv 3 \pmod 4$ one can define the **Paley tournament** similarly to Paley graphs: the vertices are elements of $\mathrm{GF}(q)$ and the direction of the edge between x and y indicates, whether $x-y$ or $y-x$ is a square (note that in this case -1 is not a square, so for any $0 \neq t \in GF(q)$ exactly one of t and $-t$ is a square). In a tournament a

vertex v dominates a subset S of the vertices if for any $s \in S$ the edge between v and s is directed from v to s.

Let us try to find a small dominating set in the undirected $P(q)$ the same way as we did for blocking sets in $\mathrm{PG}(2,q)$.

Looking for a set of size k we have $\binom{q}{k}$ choices, the number of k-sets not dominating a particular vertex t is $\binom{(q-1)/2}{k}$, hence for the existence of a good choice, we need $q\binom{(q-1)/2}{k} < \binom{q}{k}$, which is true for $k \geq 2\log q$. (Again we omit the calculations, but this is also a particular case of Lemma 2.3.)

Unlike for the previous example, here one can prove that this is best possible (concerning the order of magnitude).

LEMMA 2.1. *Any dominating set in $P(q)$ contains at least $(\frac{1}{2}-\varepsilon)\log q$ points. (Here $\varepsilon > 0$ is arbitrary, $q > q(\varepsilon)$.)*

Before the proof we recall a result we shall use here and one more time and make some historical comments.

LEMMA 2.2. *(Character sum version of Weil's estimate) Suppose $f_1, ..., f_k, f_{k+1}, ..., f_l$ are polynomials over GF(q), q odd. Let N denote the number of solutions for the following requirements:*

- *$f_i(x)$ is a square for $i = 1, ..., k$;*
- *$f_i(x)$ is a non-square for $i = k+1, ..., l$.*

Then

$$\left| N - \frac{q}{2^l} \right| \leq \frac{\sqrt{q}+1}{2} \sum_{i=1}^{l} \deg(f_i)$$

holds, unless the product of some of the f_is is constant times the square of a polynomial (in this case the requirements can be contradicting).

Proof. see [81]. □

In fact the phrase 'character sum version of Weil's estimate' is usually referred to a result essentially due to Burgess which should be used for the proof of the just stated result. The first ones to use such ideas to deduce properties of Paley graphs were Graham and Spencer [41], who proved that in the Paley tournament for any subset S of the vertices of size at most $(\frac{1}{2}-\varepsilon)\log q$ there is a vertex dominating S (for $q > q(\varepsilon)$). Later Bollobás and Thomason [15] used a similar argument to deduce that the Paley graph $P(q)$ contains all graphs with at most $(\frac{1}{2}-\varepsilon)\log q$ vertices as an induced subgraph (for $q > q(\varepsilon)$). For more on these, we refer to [83].

We also mention that one can generalize Lemma 2.2 in the sense that instead of requiring that $f_i(x)$ is a square or not, we can prescribe the value of a multiplicative character on $f_i(x)$. This was done by Babai, Gál and Wigderson [6] for linear f_i's and by Sziklai [77] for arbitrary f_i's. Sziklai used it to deduce properties of generalized Paley graphs similar to the ones just mentioned. In the generalized Paley graph two elements of the finite field are connected by an edge if their difference is a d-th power.

Proof of Lemma 2.1 Suppose that $X = \{x_1, ..., x_l\}$ is a dominating set. Then for any $x \in X$ there is an i with $x - x_i$ square, hence there is no solution for the following requirements:

$x - x_i$ is a non-square for $i = 1, ..., l$.

On the other hand, by the previous lemma, the number of solutions is at least $q/2^l - l\frac{\sqrt{q}+1}{2}$. This is positive if $l < (\frac{1}{2} - \varepsilon)\log_2(q)$, hence any dominating set has size at least $(\frac{1}{2} - \varepsilon)\log_2(q)$. □

Using trivial random choice, usually one has to make calculations with binomial coefficients (depending on the particular problem) to look for the best constants. Instead of doing so, one can use the following lemma which is a general setting for a lot of cases where this method is applied.

LEMMA 2.3. *(S.K. Stein, see* [35]*) Consider a bipartite graph with colour classes: A and B (usually one can think of these as objects to be blocked and objects to block with, respectively). Denote by d the minimum degree in A. If A has at least two elements, then there is a set $B' \subseteq B$ dominating the vertices of A with*

$$|B'| \leq \left\lceil |B| \frac{\log(|A|)}{d} \right\rceil.$$

Proof. Write $n = |B|$ and let us look for a set B' of size k. The number of choices for such a set is $\binom{n}{k}$, while the number of bad choices for a particular vertex $a \in A$ is $\binom{n-\deg(a)}{k} \leq \binom{n-d}{k}$. Hence there are at most $|A|\binom{n-d}{k}$ bad choices. To deduce the existence of a dominating set of size k we need

$$|A|\binom{n-d}{k} < \binom{n}{k}.$$

This is equivalent to

$$|A| < \frac{n(n-1)\cdots(n-k+1)}{(n-d)(n-d-1)\cdots(n-d-k+1)}.$$

It is easy to see that among the fractions $\frac{n}{n-d}$, $\frac{n-1}{n-d-1}$,...,$\frac{n-k+1}{n-d-k+1}$, the first one is the smallest, so it is sufficient to achieve

$$|A| < (\frac{n}{n-d})^k.$$

One can rearrange the right hand side as $\left((1 + \frac{1}{n/d-1})^{n/d}\right)^{kd/n}$. Using that $(1 + \frac{1}{x-1})^x > e$ holds for $x > 1$, we find that it suffices to have

$$|A| \leq \exp(kd/n),$$

which, after taking natural base logarithms, gives the desired bound on k. □

Note that our two examples were particular cases of this lemma. For the first one, elements of A correspond to lines of $\mathrm{PG}(2,q)$, while the elements of B to the points, edge means incidence (hence the bipartite graph is the incidence graph of the plane). All degrees in A are the same: $d = q+1$. The lemma guarantees the existence of a blocking set of size at most $\left\lceil (q^2+q+1)\frac{\log(q^2+q+1)}{q+1} \right\rceil \leq 3q\log q$ for large enough q.

In the second example A and B both correspond to elements of $\mathrm{GF}(q)$, edge is drawn between x and y if and only if $x-y$ is a (possibly zero) square. The dominating set coming from the lemma is of size at most $\left\lceil q\frac{\log q}{(q+1)/2} \right\rceil \leq 2q\log q$.

Before going further, we make two comments. First, it is worth mentioning that, using the theory of fractional covers of hypergraphs, Lovász proved that with a greedy algorithm one can always guarantee an intersection set of size at most

$$|B|\,\frac{1+\log(D)}{d},$$

where D denotes the maximum degree in B (and this is obviously at most $|B|\,\frac{1+\log(|A|)}{d}$.)

We shall give more details in Section 6.

The other remark is that this is a good point to explain the random choice terminology. It is easy to see that one can reformulate the lemma just proved (and all the applications) in terms of probabilities: the lemma states that choosing a set at random, the probability that it is dominating is positive. It is also not very difficult to prove the following sharper version:

Lemma 2.4. *With the notation of Lemma 2.3, choosing a subset of B of size at least*

$$\frac{1}{\varepsilon}\,|B|\,\frac{\log(|A|)}{d},$$

the probability that the set obtained is not dominating (the vertices of A) is smaller than ε. □

We will not use this version, throughout the constructions we will simply use Lemma 2.3 (and recall that this is only a general form for trivial enumeration).

We end this section with some applications of Lemma 2.3 to blocking sets in inversive planes (or Möbius planes).

An **inversive plane** of order q is a $3-(q^2+1,q+1,1)$ design, that is, a collection of $(q+1)$-element subsets (usually called **circles**) of a set of size q^2+1 (usually called set of **points**) with the property that through any 3 distinct points there is exactly one circle. An easy calculation shows that the number of circles in such a design is q^3+q. For more on these, we refer to [26].

Lemma 2.5. *(Drake-Kitto* [27]*) In an inversive plane of order q there is a blocking set of size at most $4q\log q$.*

Proof. We use Lemma 2.3 with taking A as the set of circles, B as the set of points, and edges corresponding to incident point-circle pairs. We get a blocking set of size at most $\left\lceil (q^2+1)\frac{\log(q^3+q)}{q+1} \right\rceil \leq 4q \log q$. □

Perhaps it is a bit surprising, that all blocking sets known in inversive planes do have size at least $cq \log q$, while the best known lower bound is $2q$ (for $q \geq 9$), proved by Bruen and Rotschild [24].

We also consider the case when one is looking for a blocking set consisting of the union of circles. Here points of A and B both correspond to circles and an edge means that the two circles are intersecting. A little calculation shows that here $d \approx q^3/2$, and Lemma 2.3 gives that we need roughly $6 \log q$ circles, that is, roughly $6q \log q$ points.

In one of the constructions of this paper (Construction 4.4), we will be looking for a blocking set consisting of full circles in a particular inversive plane, so we discuss this in a bit more detail.

The *Miquelian* inversive plane consists of the points and plane sections of an elliptic quadric. There are several other representations, here we will use the following one, which only works for q odd. Consider the affine plane $AG(2,q)$ for an odd prime power q. The points of the inversive plane will be the points of $AG(2,q)$ together with one extra point called ∞. The circles are the lines of $AG(2,q)$ with ∞ added to all of them, while circles not through ∞ are the following conics: $(x-a)^2 + \varepsilon(y-b)^2 = c$, where a, b and $c \neq 0$ are the parameters of the circle, while ε is a fixed element such that $-\varepsilon$ is not a square. For more about this representation, we refer to [26].

Lemma 2.6. *In a Miquelian inversive plane of odd order one needs at least $cq \log q$ circles to block all the circles.*

Proof. The proof is based on the character sum version of Weil's estimate (see Lemma 2.2). For more details, see [80]. □

For q even (and large enough), all we know is that one needs at least three circles. This was recently proved by Kiss, Marcugini and Pambianco [62].

3. Minimal blocking sets in $\mathrm{PG}(2,q)$

In this section (based on [85]) we outline the first application of the method this paper is mainly about. Before the construction we have to recall a couple of definitions and results about blocking sets and Hermitian curves of $\mathrm{PG}(2,q)$.

A **minimal blocking set** in a projective plane is a set of points meeting every line and minimal (subject to set-inclusion) for this property.

The smallest blocking sets of $\mathrm{PG}(2,q)$ are the lines, it is easy to see that these are the only examples of size $q+1$. The next possible size (by the result of Bruen [19]) is $q+\sqrt{q}+1$ with equality if and only if the set is a Baer subplane. The biggest possible minimal blocking sets (by a result of Bruen and Thas [23]) are the unitals, that is, sets of size $q\sqrt{q}+1$ meeting every line in 1 or $\sqrt{q}+1$ points.

The construction to be outlined will produce minimal blocking sets in $\mathrm{PG}(2,q)$, q square, of various sizes. More precisely, the following result will be proved.

THEOREM 3.1. *(Szőnyi, Cossidente, Gács, Mengyán, Siciliano, Weiner* [85]*)*

In $PG(2,q)$, q square, there is a minimal blocking set of any size from

$$[4q\log q, q\sqrt{q}-q+2\sqrt{q}].$$

We will say a little more and give references about the spectrum at the end of the section.

The **Hermitian curve** is a curve projectively equivalent to the curve defined by the following equation:

$$X_0^{\sqrt{q}+1}+X_1^{\sqrt{q}+1}+X_2^{\sqrt{q}+1}=0$$

The set H of points of such a curve form a unital, that is, its size is $q\sqrt{q}+1$ and it meets every line in 1 or $\sqrt{q}+1$ points. (We shall call these lines **tangents** and **secants**, respectively.)

There is a unique tangent at each point of H, while through a point outside there are $\sqrt{q}+1$ tangents.

Tangents through a $p\notin H$ meet H in collinear points (the corresponding secant is called the **polar** of p and denoted by $p^\perp$), and vice versa, tangents at points of a secant ℓ are concurrent at a point called the **pole** of ℓ and denoted by $\ell^\perp$.

All secants meet the curve in a Baer subline. For proofs of the listed properties and for more properties of Baer sublines, we refer to [48].

As a first step of the construction, we define an operation which modifies H to produce another minimal blocking set.

Switching: Remove all but one points from a secant and add its pole.

It is easy to see that this operation results in a minimal blocking set of size $|H|-(\sqrt{q}-1)$. We wish to repeat this procedure several times. For the first $\sqrt{q}$ switches the resulting set is almost automatically a minimal blocking set, but after this point it is possible that we delete all points from a secant. The other problem is that it is not too easy to determine the size of the resulting set. Both problems can be handled though, if we only switch with respect to secants through a fixed point $p\in H$ and p is the point left on all the secants. It is easy to see that the only thing we have to guarantee to have a minimal blocking set, is that the points of H on secants through p for which we do not switch, block all secants not through p. This is the moment we have to use ideas from the previous section.

LEMMA 3.2. *Let H denote a Hermitian curve and $p\in H$. With trivial random choice one can find a set of no more than $2\sqrt{q}\log q$ secants through p with the property that the union of points of H on these secants block all secants not through p.*

Proof. We use Lemma 2.3 with vertices in A corresponding to secants not through p, vertices in B corresponding to secants through p, and edge meaning that the two lines meet within the curve. We have $|B|=q$, $|A|=q^2+q+1-(q\sqrt{q}+1)-q=q^2-q\sqrt{q}$, $d=\sqrt{q}+1$, hence there is a set B' with $|B'|\le 2\sqrt{q}\log q$. □

CONSTRUCTION 3.3. *Let H denote a Hermitian curve and $p \in H$. Choose a set B' (of size at least $2\sqrt{q}\log q$) containing a blocking set guaranteed by Lemma 3.2. Switch the rest of the secants through p, that is, delete all points besides p from the rest of the secants through p and add the poles of these secants.*

The size of the minimal blocking set just constructed is $q\sqrt{q}+1-(q-|B'|)(\sqrt{q}-1) = q+1+|B'|\,(\sqrt{q}-1)$. Using $2\sqrt{q}\log q \le |B'| \le q$, this gives an example for any size $\equiv 2 \pmod{\sqrt{q}-1}$ in $[2q\log q+q, q\sqrt{q}+1]$.

To achieve every size from the interval in Theorem 3.1, we have to make a final switch at the end with respect to a secant not through p. This will not decrease the size by $\sqrt{q}-1$: the new size will depend on how many points of this secant have already been deleted. For this, we first choose a secant m and a secant l_0 through p meeting m inside the curve. After this we try to modify Lemma 3.2 in such a way that the (hopefully still small) blocking set consists of l_0 and secants meeting m outside. After finding such a set one can add some lines meeting m inside so that the number of deleted points at the end is handled.

LEMMA 3.4. *Let H denote a Hermitian curve and $p \in H$. Choose a secant m not through p and a secant l_0 through p meeting m inside the curve. With trivial random choice one can find a set of no more than $2\sqrt{q}\log q$ secants through p meeting m outside the curve with the property that the union of points of H on these secants block all secants not through p, except for those blocked by l_0.*

Proof. We have to modify our bipartite graph in Lemma 3.2 as follows: the vertices of A correspond to secants not through p, not blocked by l_0, the vertices in B correspond to secants through p meeting m outside, the definition of edges remains the same: two vertices are joined if and only if the corresponding lines meet inside the curve.

Here $|A| < q^2 - q\sqrt{q}$ and $|B| = q-\sqrt{q}-1$, the only non-trivial part is a lower bound on d. We wish to prove $d \ge \sqrt{q}-1$. Suppose to the contrary that there is a vertex in A with degree at most $\sqrt{q}-2$. This corresponds to a secant ℓ not through p which has the property that from those $\sqrt{q}+1$ secants through p that meet ℓ inside, at least 3 also meet m inside. Using the fact that the points of H on a secant form a Baer subline and that 3 lines uniquely determine a dual Baer subline, we deduce that ℓ and m are met inside by the very same $\sqrt{q}+1$ secants through p. But this implies that l_0 blocks ℓ, a contradiction.

Hence Lemma 2.3 guarantees the existence of a set B' with $|B'| \le \left\lceil (q-\sqrt{q}-1)\frac{\log(q^2-q\sqrt{q})}{\sqrt{q}-1}\right\rceil \le 2\sqrt{q}\log q$. □

Proof of Theorem 3.1 Let b denote an arbitrary integer from the interval to be filled. Write $b = q\sqrt{q}+1-(q-b')(\sqrt{q}-1)-(r-2)$ with $0 \le r-2 \le \sqrt{q}-2$. If $r-2=0$, then Construction 3.3 can produce a minimal blocking set of size b, so suppose $r-2 \ne 0$, that is, $3 \le r \le \sqrt{q}$.

Let H denote a Hermitian curve, $p \in H$ and $l_p = p^\perp$, the pole of p. Choose a secant m not through p with the property that the pole of $m \cap l_p$ meets m outside the unital. Let l_0 denote a secant through p meeting m inside the unital.

By Lemma 3.4, we can find a set B' from the secants through p with the following properties:

- elements of B' meet m outside the unital;
- for any secant not through p there is at least one element in $B' \cup \{l_0\}$ that meets it inside the unital;
- $|B'| \leq 2\sqrt{q}\log q$.

Add to B' the line l_0, the pole of $m \cap l_p$, $r-1$ more lines through p meeting m inside the curve, finally, some lines meeting m outside in such a way that the size of B' becomes b'.

Use Construction 3.3 with B' to find a minimal blocking set of size $q\sqrt{q}+1-(q-b')(\sqrt{q}-1)$. Finally, remove points from m (there are r of them left) except for $l_0 \cap m$ and add the pole of m. This gives a minimal blocking set of size b. □

Let us mention here that recently Mengyán [72] proved that in an interval almost as large as the one in Theorem 3.1 each value can occur as the size of more than polynomial non-isomorphic minimal blocking sets.

We end this section with a brief description of the sizes of minimal blocking sets known. For a survey on the spectrum we refer to [86].

As mentioned at the beginning, the smallest and second smallest examples are the lines and Baer subplanes, respectively. In the interval $\left[q+\sqrt{q}+1, 3\frac{q+1}{2}\right)$, all known examples are part of an infinite series called **linear blocking sets** constructed by Polito, Polverino and Lunardon [67], [73], [68]. Results of Blokhuis [11], Szőnyi [82] and Sziklai [78] suggest that these are the only examples. We know that the whole interval cannot be covered, for example in [82] it is shown that all examples should have size 1 (mod p).

In the interval $[3\frac{q+1}{2}, 2q-2]$ there are some constructions by Megyesi ([75] p. 228. Example 6., see [86] for an explanation why it is a blocking set) and Polverino-Szőnyi-Weiner [74], we do not have non-existence result for any size, though it is not likely that every value can occur.

In the interval $[2q-1, 3q-3]$ every value can occur as the size of a minimal blocking set. This is a result by Innamorati-Maturo [55] and independently by Illés-Szőnyi-Wettl [54].

The surprising fact is that after this, for q prime, there is a large gap in the spectrum of existing constructions, the next examples have size $cq\log q$, see [81].

For q square, by Theorem 3.1, after $q\log q$ every value can occur almost up to the biggest possible size, which is $q\sqrt{q}+1$. It is natural to conjecture that (for q square) after the unitals, the biggest examples (coming from one switch of the Hermitian curve) have size $\sqrt{q}-1$ smaller. The best result towards this is due to Szőnyi and Weiner proving a $c\sqrt{q}$ gap below $q\sqrt{q}+1$ [87].

For general q it is difficult to give a survey on the sizes of examples known, all constructions use subfields of GF(q) (hence do not work for q prime). There are examples in the paper [85] this section was based on. Recently Mazzocca and Polverino [69] and Mazzocca, Polverino and Storme [70] constructed new examples.

4. Maximal partial line spreads in $\mathrm{PG}(3,q)$

We start this section by summarizing some definitions and basic facts about maximal partial line spreads. It will turn out that one can construct a lot of examples analogously to Construction 3.3.

A **line-spread** of the projective space $\mathrm{PG}(n,q)$ is a set of lines partitioning the points. A necessary condition for the existence of a line-spread is that the size of a line divides the number of points, that is $\frac{q^2-1}{q-1}|\frac{q^{n+1}-1}{q-1}$ and this is satisfied if and only if n is odd. Line-spreads do exist whenever the dimension is odd. To see this, consider $\mathrm{GF}(q^{n+1})$ as the underlying vectorspace of $P(n,q)$. Here points (that is, 1-dimensional subspaces) are the multiplicative cosets of $\mathrm{GF}(q)$, while some of the lines (that is, 2-dimensional subspaces) are the multiplicative cosets of $\mathrm{GF}(q^2)$. Taking only lines of this form, we find a line-spread of $\mathrm{PG}(n,q)$.

A **partial line spread** of $\mathrm{PG}(n,q)$ is a set of pairwise disjoint lines. Usually, one is interested in **maximal** partial line spreads, that is, examples which can not be extended to a larger one. Throughout the section we will omit the word line and simply call our structures (partial) spreads.

In this section (based on [37]) we outline the construction of small maximal partial line spreads of $\mathrm{PG}(3,q)$. It is basically due to Beutelspacher [10], the only extra idea is the use of random choice at a certain point. The theorem to be proved is the following.

Theorem 4.1. *In $PG(3,q)$ there are maximal partial spreads of size $cq+1$ for any c satisfying $6\log q + 1 \le c \le q$.*

The whole section will be analogous to the previous one, we will always recall the corresponding notions from the blocking set construction. First we list some properties of hyperbolic quadrics, reguli and regular spreads. For the proofs see [49].

A **hyperbolic quadric** in $\mathrm{PG}(3,q)$ contains $(q+1)^2$ points. There are two classes of lines on it, *red* and *blue* say, satisfying the following properties:

- There are $q+1$ red and $q+1$ blue lines on the hyperbolic quadric;
- two lines meet if and only if their colour is different;
- lines of both colour partition the points of the hyperbolic quadric;
- a line not on the hyperbolic quadric meets it in at most two points.

A **regulus** is a set of $q+1$ skew lines forming one colour class of a hyperbolic quadric. The other colour class of lines is called the **opposite regulus**. For a regulus R the opposite regulus will be denoted by R^{opp}. Any three skew lines of $\mathrm{PG}(3,q)$ generate a unique regulus. One can also find a regulus by taking all lines of the space meeting three fixed skew lines.

A **regular spread** S is a spread with the property that taking any three of its lines, the uniquely generated regulus is also in the spread. An equivalent definition is that taking any $\ell \notin S$, the $q+1$ lines of S meeting ℓ form a regulus.

Regular spreads do exist in $\mathrm{PG}(3,q)$, they are all equivalent to the one constructed at the beginning of this section.

In the construction regular spreads will play the role of Hermitian curves of the previous section, reguli will correspond to secants. In Construction 3.3 the first step was to find a transformation (switching) which started from the Hermitian curve and produced another minimal blocking set. We do the same here with the corresponding structures. This operation was developed by Bruen [20].

Switching: Take a regular spread S and regulus R inside. Drop all lines of R and add the lines of the opposite regulus.

Since R and R^{opp} cover the same points of the space, this will be another spread of $\mathrm{PG}(3,q)$. In fact, this operation works for any partial spread containing a regulus, and starting with a maximal partial spread, the result is also maximal.

Comparing this to the switching operation of the previous section, the difference is that here we do not find a smaller partial spread, while the switching operation for Hermitian curves automatically reduced the size. But this will change in the next step.

In Construction 3.3 the next step was to consider secants through a point of the Hermitian curve and try to switch with respect to them simultaneously. A property which perhaps had a role in the fact that the method worked is that the secants through a point of a Hermitian curve partition the rest of the points of the curve. The following two lemmas yield that we have a similar situation here.

LEMMA 4.2. *Lines and reguli of a regular spread form an inversive plane.*

Proof. From the properties just listed we see that in a regular spread there are q^2+1 lines. Any regulus contains $q+1$ lines and any three lines of the spread generate a unique regulus the lines of which are all contained in the (regular) spread. These are exactly the defining properties of inversive planes. (See Section 2 for the definition.) □

LEMMA 4.3. *Let S be a regular spread and $\ell \in S$. Then $S \setminus \{\ell\}$ can be partitioned into reguli through ℓ.*

Proof. The derived design, with respect to ℓ, of this $3-(q^2+1,q+1,1)$ design is a $2-(q^2,q,1)$ design, that is, an affine plane (see [25]). This can be partitioned into disjoint lines. □

Note that the previous partition also gives rise to a partition of the space into hyperbolic quadrics sharing a common line but having no more points in common.

The next step in Construction 3.3 is to switch simultaneously a lot of secants through a point. Let us try to do this here. Fix a line ℓ of a regular spread S and consider the partition $R_1,\dots,R_q$ guaranteed by Lemma 4.3. Suppose we want to switch with respect to $R_1,\dots R_k$. This means that we drop all lines in these R_is and add lines from the opposite reguli $R_1^{opp},\dots,R_k^{opp}$. In particular, ℓ will be dropped. Two lines from different R_i^{opp}s can meet, so we have to be careful. It is easy to see that any such intersection point has to be a point of ℓ. On the other hand, we only need 1 line from an R_i^{opp} to ensure that lines of R_i cannot be added to our (hopefully maximal) partial spread. Hence we end up with the following construction due to Beutelspacher [10].

CONSTRUCTION 4.4. *Let B' denote a subset of the reguli of the partition $R_1, \dots, R_q$ from Lemma 4.3. Delete all lines from reguli not in B' and add some opposite lines of these reguli in such a way that*

- *there are $q+1$ lines added covering the points of ℓ;*
- *we choose at least one line from each R_i^{opp} with $R_i \notin B'$.*

It is easy to see that Construction 4.4 produces a partial spread. Let us analyze whether it is maximal or not. Lines from the original regular spread cannot be added, since we have at least one line from the opposite regulus for each regulus of deleted lines. A line from an opposite regulus of any of the R_is cannot be added, since any opposite line meets ℓ, and the points of ℓ are covered. The only lines which are not automatically blocked by our partial spread are those outside S and not in any R_i or R_i^{opp}. Hence we have the following.

LEMMA 4.5. *Construction 4.4 produces a maximal partial spread if lines from reguli in B' meet all lines not in S and not in any R_i^{opp} $(i = 1, \dots, q)$.*

In the original construction Beutelspacher uses the fact that a hyperbolic quadric either contains a line or meets it in at most 2 points. Hence, if one lets B' contain at least $\frac{q}{2}$ reguli, then the switched reguli cannot cover all points of a line outside S. Using (trivial) random choice one can do better.

Before stating the lemma corresponding to Lemma 3.2, we make one further observation which will make the analogy even closer. By the equivalent definition of a regular spread, the $q+1$ lines of S meeting a line $l \notin S$ form a regulus. Hence by Lemma 4.5, we need to ensure that the union of reguli of B' contains at least one line from each regulus in S not containing ℓ. This is literally the translation of what was guaranteed by Lemma 3.2 in the previous section.

LEMMA 4.6. *With trivial random choice one can find B' with $|B'| \le 6 \log q$ in such a way that B' has at least one line from all reguli of S not containing ℓ.*

Proof. We use Lemma 2.3 with the vertices of A: reguli of S not through ℓ (that is, not containing ℓ), $B = \{R_1, ..., R_q\}$, and edge meaning that the corresponding reguli share at least one line.

$|A| \le \frac{(q^2+1)q^2(q^2-1)}{(q+1)q(q-1)} = q^3 + q$ (the number of reguli in S), $|B| = q$. For the minimal degree in A note that two distinct reguli can meet in at most two lines, so any regulus in S (not containing ℓ) has to intersect at least $\frac{q+1}{2}$ of the R_is. Hence $d \ge \frac{q+1}{2}$.

Lemma 2.3 gives an intersection set B' with $|B'| \le \left\lceil q \frac{\log(q^3+q)}{(q+1)/2} \right\rceil \le 6 \log q$. □

Now we are ready to prove Theorem 4.1.

Proof of Theorem 4.1 By Lemmas 4.5 and 4.6, we can construct maximal partial spreads using Construction 4.4 with $6 \log q \le |B'| \le q$. On the other hand, the size of the arising partial spread is $q + 1 + q\,|B'|$ □.

The natural question arising here is whether we can also repeat the final trick that worked for the Hermitian curve, that is, if a final switch with respect to another regulus (this time

not through ℓ) might produce a density result. Here it is much more difficult to handle the number of remaining lines in a regulus not through ℓ and even more difficult to tell how many lines of the opposite regulus we have to add at the end. In a joint work with L. Storme we are investigating this and it seems to be possible to prove a density result at least for the interval $\left[C\sqrt{q}\log q, q^2/2\right]$.

The other natural question is whether one could construct smaller maximal partial line spreads by using a more elaborate random choice in Lemma 4.6. Since the lines and reguli of a regular spread form an inversive plane (and it can be shown that the inversive plane is the Miquelian one), the lemma guarantees a blocking set in this inversive plane consisting of full circles. By Lemma 2.6, at least for q odd, this cannot be improved.

We end this section by summarising what is known about the spectrum of sizes of maximal partial spreads in $\mathrm{PG}(3,q)$.

The current best lower bound for the size is $2q$ by Glynn [38], while the smallest examples (coming from Theorem 4.1) have size $cq\log q$. After this we have an example for every q-th value up to the biggest size which is q^2+1 (size of a spread). There is a density result for the interval $\left[\frac{q^2+1}{2}+6, q^2-q+2\right]$ by Heden [44], [45], [46] for $q>7$ odd; and a similar result was proved in an unpublished manuscript by Govaerts, Heden and Storme [39] for the interval $\left[\frac{5q^2+q+16}{8}, q^2-q+2\right]$ for $q>q_0$ even. (The size q^2-q for q even was in fact missing from this interval but later Jungnickel and Storme [57] constructed such an example.) Besides this there is a sporadic example by Heden [47] of size $45=7^2-7+3$ in $\mathrm{PG}(3,7)$. The best upper bound (which is roughly $q^2-\sqrt{q}$ for general q) for the second largest example after the spreads was proved by Bruen [20] and a little bit improved by Blokhuis and Metsch [13]. All bounds use a nice observation due to Bruen [21] showing a connection between partial spreads of $\mathrm{PG}(3,q)$ and blocking sets of $\mathrm{PG}(2,q)$.

Before Heden's construction a lot of more people constructed examples like Beutelspacher, Ebert, Jungnickel, Storme, see [49] and [37] for references.

Hence the two main questions remaining is whether the smallest ones have size cq or $cq\log q$ and whether the second largest ones have size q^2-q+2 for large enough q. Both of these questions seem to require new algebraic methods or brand new construction tricks.

5. Maximal partial line spreads in higher dimensions

In this section we show how the examples in 3 dimension and our construction method can produce maximal partial line spreads in $\mathrm{PG}(n,q)$, $n\geq 5$.

The two results, both taken from [37], to be discussed are the following:

Theorem 5.1. *In $PG(n,q)$, $n\geq 5$ odd, q large enough, there is a maximal partial line spread for any size from the interval* $\left[9nq^{n-2}\log q, \frac{q^{n+1}-1}{q^2-1}-q+1\right]$.

Theorem 5.2. *In $PG(n,q)$, $n\geq 6$ even, q large enough, there is a maximal partial line spread for any size from the interval* $\left[9nq^{n-2}\log q, \frac{q^{n+1}-q}{q^2-1}-q^3+q^2-2q+2\right]$.

We outline the construction for the odd dimensional case only, since the other case is similar, though needs a bit more work. The interested reader is referred to the original paper [37]. Throughout the section, (partial) spread will mean (partial) line-spread.

As we saw at the beginning of the previous section, $\mathrm{PG}(n,q)$ has spreads for any odd n.

LEMMA 5.3. *Fix a line ℓ in $PG(n,q)$, $n \geq 5$ odd. The rest of the points can be partitioned by 3-dimensional subspaces through ℓ. (By dimension we always mean projective dimension).*

Proof. Translating the statement to the factor geometry with respect to ℓ, we are looking for a line-spread in $\mathrm{PG}(n-2,q)$; this exists by the paragraph before the lemma. □

CONSTRUCTION 5.4. *Let $U_1, \ldots, U_m$ denote 3-dimensional subspaces through the line ℓ partitioning the rest of the points (see the previous lemma). Put a spread (containing ℓ) to some of the U_is (denote the set of these by B') and any maximal partial spread (also through ℓ) to the rest. This yields a partial spread of $PG(n,q)$.*

LEMMA 5.5. *Construction 5.4 gives a maximal partial spread if those U_is where we put a spread block all lines not in any of the U_i's ($i = 1, ..., m$).*

Proof. No line can be added from one of the U_is, since we put a maximal partial spread to all of them (a spread is also a maximal partial spread). Hence what we need is that the rest of the lines are blocked. If these lines are blocked by those U_is where we have a spread, then (since these subspaces are fully covered), they are also blocked by lines of our partial spread. □

LEMMA 5.6. *In the partition $U_1, \ldots, U_m$ guaranteed by Lemma 5.3, with trivial random choice we can find a subset B' of size at most $4nq^{n-4}\log q$ with the property that the union of these block all lines not contained in any of the U_is.*

Proof. As usual, we apply Lemma 2.3. The vertices of A correspond to the lines to be blocked (that is, those which are not contained in any U_i), the vertices of B correspond to the U_is, the edge is for nonempty intersection. The size of A is smaller than the number of lines of the space, which is easily seen to be smaller than $4q^{2n-2}$. $|B| = m = \frac{q^{n-1}-1}{q^2-1} \leq 2q^{n-3}$, $d = q+1$. □

Proof of Theorem 5.1. For the smallest example, use Construction 5.4 with the smallest possible B' guaranteed by Lemma 5.6. To all U_is not in B' put maximal partial spreads of the smallest size coming from Theorem 4.1. After this, we change one of the partial spreads to an example of size roughly $5q^2/16$ guaranteed by the density results by Heden et. al., see the end of the last section. The size of this can be the lower end of the interval we can cover, since after this we can go up one by one by increasing the size of one of the partial spreads or increasing B'. We omit the calculations. □

The construction for the even dimensional case is similar, but a bit more technical, since in these spaces (and also in the factor spaces) spreads do not exist.

Now we wish to convince the reader, that this construction was also analogous to Constructions 3.3 and 4.4. If we put a spread to all of the U_is, we find a spread of the space,

this corresponds to a Hermitian curve and a regular spread in the previous two constructions. 3-dimensional subspaces (with which we partitioned the spread here) correspond to secants of the Hermitian curve and reguli of the regular spread, switching was to change a spread to a maximal partial spread in a 3-space. The "blocking set lemma" was similar, but not literally the same, as in the previous two sections.

This is perhaps the good moment to outline the method:

- Take a nice (regular) example S for the structure to be constructed;
- find a substructure R and a switching, that changes R within S to make a new example;
- take an element x of S and partition the rest of the elements by copies of R through x;
- choose a set B' at random from the copies of R in such a way that these already ensure the minimality/maximality/blocking property/etc. of the structure we wish to construct;
- switch with respect to all copies of R not in B'.

Usually, the set B' we are looking for is a blocking set (but it can vary what we want to block). Very often we want to block all copies of R within S which do not contain x.

Similarly to the previous sections, at the end we summarize what is known about the sizes of maximal partial spreads in $\mathrm{PG}(n,q)$, $n \geq 4$.

For $n = 4$ (where our construction did not work) little is known. By Beutelspacher [10] the smallest examples are just the spreads in hyperplanes (of size q^2+1) and for the interval $\left[q^2+1, q^2+q\sqrt{q}-\sqrt{q}\right]$ we know what values can occur and what the examples are (see also [37]). Beutelspacher also determined the largest examples, which are of size q^3+1. Besides this, all we have is a density result by Eisfeld-Storme-Sziklai [28] for the interval $[q^3-q+3, q^3+1]$.

For $n \geq 5$ odd, we know much more. The smallest partial spreads (having size approximately cq^{n-2}) can be constructed from the largest maximal partial spreads of a hyperplane (see [10]). We have the density result just outlined for the interval $[c'nq^{n-2}\log q, \frac{q^{n+1}-1}{q^2-1} - q + 1]$. Finally, there are the spreads of size $\frac{q^{n+1}-1}{q^2-1}$. Hence the most interesting open case is to decide whether there are examples in the interval $\left(\frac{q^{n+1}-1}{q^2-1} - q + 1, \frac{q^{n+1}-1}{q^2-1}\right)$. Upper bounds for the size of the second largest example (after spreads) similar to the 3-dimensional ones were achieved by Govaerts and Storme [40] and Metsch and Storme [71].

For $n \geq 6$ even, we know almost everything. The smallest examples are the spreads of hyperplanes and similarly to the $n = 4$ case, by Beutelspacher [10] (see also [37]) up to a certain value we know the size and structure of all examples. Then there is a little gap where it is not clear whether there are examples or not. Finally, we have a density result for $\left[Cnq^{n-2}\log q, q\frac{q^n-1}{q^2-1} - q + 1\right]$ (here the last q^3 values are due to Eisfeld-Storme-Sziklai [28]). Beutelspacher [10] proved that there are no examples of size bigger than the upper end of this example.

Fancsali and Sziklai [33] used the construction technique to construct maximal partial plane-spreads of various sizes in various dimensions.

6. Covers and fractional covers of hypergraphs

In this section the background on covers and fractional covers of hypergraphs is given. The key Lemma in Section 2 can be regarded as an immediate consequence of bounding the ratio τ/τ^*.

A **hypergraph** $\mathcal{H}$ is a pair $(V(\mathcal{H}), E(\mathcal{H}))$, where the elements of $E(\mathcal{H})$ are subsets of $V(\mathcal{H})$. The elements of $V(\mathcal{H})$ are called **points**, while the elements of $E(\mathcal{H})$ are called **edges**. If multiple edges are allowed, then the structure is often called an **incidence structure**. The **degree** of a point $P \in V(\mathcal{H})$ is the number of edges that contain P. A hypergraph $\mathcal{H}$ is d**-regular**, if all points have degree d. $\mathcal{H}$ is r**-uniform** if every element of $E(\mathcal{H})$ has cardinality r. Regular and uniform hypergraphs are also called **1-designs**. (This remark also shows that all the geometric structures mentioned earlier are regular and uniform hypergraphs.)

Let us define now the key parameters of hypergraphs (or incidence structures).

Definition 6.1. *The* covering number *of the hypergraph $\mathcal{H}$ is the minimum number of points that intersect every edge of $\mathcal{H}$, and is denoted by $\tau(\mathcal{H})$.*

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

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

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

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

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

(Note that allowing multiple edges does not affect the value of these parameters.)

For example, for projective planes $\tau = q + 1$, and $\tau^* = (q^2 + q + 1)/(q + 1)$. The corresponding result is also true for r-uniform, d-regular hypergraphs; $\tau^* = |V(\mathcal{H})|/r = |E(\mathcal{H})|/d$. A set that intersects every edge corresponds to a $0 - 1$ fractional covering, so we immediately get that $\tau^* \leq \tau$. For more details, see [35], p.150. The ratio τ/τ^* cannot be too big: if D denotes the maximum degree of the hypergraph, then $\tau/\tau^* \leq 1 + \frac{1}{2} + \ldots + \frac{1}{D} \leq (1 + \log D)$.

Note that Lovász [66] gave a greedy algorithm which produces a 1-cover of size $\leq (1 + \log D)\tau^*$: let us first take a point having maximum degree. This intersects some edges. Delete those edges and we get a hypergraph having fewer edges. Choose a point in this smaller hypergraphs having maximum degree and iterate this process. We always end up with a 1-cover. For example, for a projective plane the greedy algorithm produces a line.

To see how Lemma 2.3 and the ratio τ/τ^* are related, let us construct a bipartite graph with $A = E(\mathcal{H})$, $B = V(\mathcal{H})$, where the edges connect incident point-edge pairs. A

dominating set in B is just a 1-cover with the hypergraph terminology. If d is the minimum cardinality of the elements of $E(\mathcal{H})$ (that is, the minimum degree of the points in A), then $\phi(u) = 1/d$ is a fractional cover of $\mathcal{H}$. Hence $\tau^*(\mathcal{H}) \leq |V(\mathcal{H})|/d$. Using the trivial upper bound $D \leq |E(\mathcal{H})| = |B|$, one gets the bound in Lemma 2.3 with an extra 1. Typically D is smaller than $|B|$, so this gives a slightly better bound than Lemma 2.3. However, since we have to take the logarithm, it does not make much difference.

There are several other estimates for the ratio τ/τ^* using further properties of the hypergraph, such as results of Frankl, Rödl [34] and those of Haussler, Welzl [43], Komlós, Pach, Woeginger [63]. For even more details, the reader is referred to [36].

7. More applications of the probabilistic method

There were early applications of the probabilistic method in the theory of arcs, caps and so-called dense or saturated sets that used explicitly or implicitly Lemma 2.3. Let us begin with the definitions.

A (k, n)**-arc** in a projective plane of order q is a set of k points with some n but no $n+1$ points on a line. $(k, 2)$-arcs are simply called k**-arcs**. A k-arc is **complete** if it is not contained in a $(k+1)$-arc, that is, when it is maximal subject to inclusion. Similarly, a (k, n)-arc is **complete** if it is not contained in a $(k+1, n)$-arc.

We shall also use the following standard terminology: if K is a set of points and ℓ is a line intersecting K in exactly s points, then we call ℓ an s**-secant of** K. Instead of 1-secant also the expression **tangent** will be used.

The probabilistic method can be used to construct small complete arcs, and also large (k, n)-arcs, if n is substantially larger than $\log q$. It gives even better results for so-called dense sets, see Bartocci [8], and Ughi [89].

A set of points in a projective plane is **dense** (or: **saturated)** if the lines meeting the set in at least two points cover the entire plane.

Lunelli and Sce proved that a complete k-arc has to have at least $k \geq \sqrt{2q}$ points. The proof actually works for dense sets. Here the important question is to get close to this theoretical lower bound. This is relatively easy for dense sets (as we shall see soon), but much more difficult for complete arcs. We will return to this in the next section. Let us see the result for dense sets.

Proposition 7.1. *(S. J. Kovács* [65]*, with slightly better constants* [17]*) There is a dense set S of size at most $3\sqrt{3q \log q}$ in any projective plane Π_q of order q. Actually, S is contained in the union of two lines.*

For the proof the reader is referred to [17]. Note that this is slightly more complicated than just using Lemma 2.3. Form a bipartite graph whose colour classes are the following: $B = \{(P_1, P_2) \ : P_i \in \ell_i, i = 1, 2\}$, A is the set of points of the plane, and we join (P_1, P_2) with P when the line containing P_1 and P_2 passes through P. In this graph we need a dominating set in B which consists of all pairs of a given point set. The idea is to choose the points of S from the points of $\ell_1 \cup \ell_2$ independently with probability p. For a point $P \in A$ let A_P denote the event that P is covered by a secant of S. Then we have to determine p in such a way that the probability of $\cap_P A_P$ is positive when q is

large and we also have to control the size of S. This situation is quite typical, in other applications there are also events that describe the combinatorial properties of the set we wish to construct. To control the size of the chosen points is always easy, since it is the sum of independent indicator variables. For results about concentration of probability, see Janson [56]. Let us recall a relatively simple and useful such result, the so-called Chernoff's inequality (see [56]).

THEOREM 7.2. *Let X be a random variable having binomial distribution $Bi(n,p)$, and let $\lambda = np$ denote its expectation. Then*

$$\text{Prob}(X \geq E(X) + t) \leq \exp\left(-\frac{t^2}{2(\lambda + t/3)}\right), \quad t \geq 0; \tag{7.1}$$

$$\text{Prob}(X \leq E(X) - t) \leq \exp\left(-\frac{t^2}{2\lambda}\right), \quad t \geq 0. \tag{7.2}$$

To show that the probability of $\cap_P A_P = A$ is positive one can typically use the trivial upper bound $\sum_P \text{Prob}(\bar{A}_P)$ for $\text{Prob}(\bar{A})$ (here $\bar{A}_P$ denotes the complement of A_P), or the inequality

$$\text{Prob}\left(\cap_P A_P\right) \geq \prod_P \text{Prob}(A_P) - \frac{1}{2}.$$

In both cases one needs $\text{Prob}(A_P)$ to be close enough to 1.

There are other cases when this idea can be used, we recall here some results of Erdős, Silverman, Stein [31]. A projective plane π has **property** $B(c)$ if there is a blocking set S which intersects each line of π in less than c points.

THEOREM 7.3. *(Erdős, Silverman, Stein* [31]*) Every projective plane of order q has property $B(c\log q)$ if q is sufficiently large and $c > 2e$.*

Here the points of the entire plane are selected independently with an appropriate probability p and for each line ℓ we have an event A_ℓ which means that the number of points of ℓ that are chosen is at least 1 and at most $c\log q$. If we do not concentrate on the value $c > 2e$, just on the existence of c, then Chernoff's inequality is strong enough to guarantee that $\text{Prob}(\cap_\ell A_\ell)$ is positive (actually tends to 1, when q goes to infinity). For desarguesian planes of odd order, Abbott and Liu [2] improved the constant to $C > 2/\log 2$. For desarguesian planes one can also use Lemma 2.3 for the following bipartite graph: A is the set of irreducible conics, B is the set of lines and we join a conic with a line if they intersect. This gives the existence of at most $2\log(q^2+q+1)$ conics whose union is a blocking set. This was proved by Ughi [90] by using counting arguments. She also proved that one needs at least $c\log q$ conics to obtain a blocking set, if q is odd. Note that there are examples showing that this result does not extend to planes of even order, see [54]. The interest in these results came from the following question of Erdős:

Is there a constant c such that every projective plane has property $B(c)$?

There are explicit results for desarguesian planes of non-prime order: Bruen and Fisher [22] proved that $\text{PG}(2,3^r)$ has property $B(5)$, Boros generalized this by showing that $\text{PG}(2,p^r)$ ($p > 2$ prime) has property $B(p+2)$, Illés, Szőnyi and Wettl showed that $\text{PG}(2,2^r)$ has property $B(6)$ if r is even and it has property $B(7)$ if r is odd.

Essentially the same idea was used by Barát, Marcugini, Pambianco, Szőnyi [7], who proved that there is a constant $c > 0$ such that there are at least $cq/\log q$ disjoint blocking sets. For desarguesian planes there are explicit constructions for roughly $q/3$ disjoint blocking sets.

Chernoff's inequality can also be used to show the existence of large (k, n)-arcs, if n is large enough with respect to q. Let us choose a function $\lambda(q)$ so that $\log q = o(\lambda(q))$. Determine t so that $t^2/(2(\lambda + t/3)) = 3 \log q$. Note that for the solution in t we have $t = o(\lambda)$. Choose the points of the plane independently at random with probability $p = \lambda/(q + 1)$. Then Chernoff's inequality guarantees that for each line ℓ, the number of selected points on ℓ will be at most $\lambda + t$ with probability at most q^{-3}. As the number of lines is $q^2 + q + 1$, one can guarantee the same property simultaneously for all lines. Let us denote the number of selected points by k. Then we have $k \leq q\lambda(q)$, and actually $k \sim q\lambda(q)$. If we choose n to be the maximum number of selected points on a line, then $n \leq \lambda(q) + t$. Taking into account the orders of magnitudes of k, λ, t and n, we see that the random choice gives (k, n)-arcs with $k \sim qn$, $n \sim \lambda(q)$, and for a (k, n)-arc we have $k \leq (n-1)q+n$. Note that in this argument n (or rather $\lambda(q)$) can be anything essentially larger than $\log q$. For some explicit constructions for larger n, see [52].

8. More delicate applications of the probabilistic method

In this section we collect some results in finite geometry that are proven with much more sophisticated applications of the probabilistic method than the results in the previous sections.

Let us begin with a result, due to Kahn [58], answering an old question of Erdős and Lovász. Given a positive integer k what is the least $n = n(k)$ for which there exists a k-uniform hypergraph $\mathcal{H}$ with n edges so that the edges of $\mathcal{H}$ are pairwise intersecting and $\tau(\mathcal{H}) = k$. The function $n(k)$ was introduced by Erdős and Lovász [30] who proved that $n(k) \geq 8k/3 - 3$ and that $n(k) \leq 4k^{3/2} \log k$ if $k - 1$ is the order of a projective plane. Actually, they proved the upper bound by probabilistic arguments and showed that the hypergraph $\mathcal{H}$ on the points of a projective plane of order $k - 1$ whose edges are a random set of $m \geq 4k^{3/2} \log k$ lines of that projective plane has $\tau(\mathcal{H}) = k$ with high probability. Here a random set of m lines means that it is chosen uniformly at random from the m-subsets of the set of lines of the projective plane. The upper bound can be improved substantially.

Theorem 8.1. *(Kahn [58]) Let Π be a projective plane of order $k - 1$. Let $\mathcal{H}$ be a hypergraph with $V(\mathcal{H})$ being the set of points of Π, $E(\mathcal{H})$ being a random set of at least $22k \log k$ lines of Π. Then with high probability $\tau(\mathcal{H}) = k$.*

Further results on $n(k)$ can be found in another paper by Kahn [59]. A very slight modification of Kahn's argument can be applied to defining sets of projective planes, as observed in [17]. Gray [42] defined defining sets of designs as follows: A set of blocks which is a subset of a unique $t - (v, k, \lambda)$ design D is called a **defining set** of that design. A defining set is **minimal** if it does not properly contain a defining set of D, and **smallest** if no defining set of D has fewer blocks. The paper [17] contains several explicit and random constructions of defining sets of projective planes. For example, a random set

of at least $22k \log k$ lines will be a defining set with high probability. Another variant of Kahn's result is due to Alon, Bollobás, Kim and Vu [5] in the dual setting. Consider a plane of order q and a random set of points (each point is chosen with probability p). Kahn's result says that if p is sufficiently large ($p \geq p_0$), then one needs to use $q+1$ lines to cover this set. The result of Alon, Bollobás, Kim and Vu shows what happens if $p < p_0$.

A classical problem in finite geometry is the existence of complete arcs of a given size. Arcs and their completeness were defined in the previous section. There we also mentioned the bound by Lunelli and Sce which shows that the size of a complete arc is at least $\sqrt{2q}$. The first examples of complete arcs had size roughly $q/2$. Then Abatangelo [1], Korchmáros [64], Szőnyi [79] could construct much smaller complete arcs. The smallest size obtained for $\mathrm{PG}(2,q)$ via algebraic constructions was $cq^{3/4}$. For a particular class of André planes complete arcs of size at most $c\sqrt{q}(\log q)^2$ were obtained. However, the plane here was constructed simultaneously with the arc, so it only shows the existence of a plane having a small complete arc. For the details, see [84] and the survey [83]. The whole story is discussed in detail in the paper by Kim and Vu [60], where the authors apply dynamic random construction using Rödl's nibble. The nibble method was initiated by Ajtai, Komlós, Szemerédi [3] to construct a large independent set in a triangle-free graph. It became a well-known tool in combinatorics when Rödl [76] used it to settle the Erdős–Hanani conjecture regarding Steiner systems. An informal description of the method, together with its application to the problem of complete arcs in planes, can be found in [60]. We just state here the main result of the paper [60].

THEOREM 8.2. *(Kim, Vu* [60]*) There are absolute constants c, C, C' and M such that in any projective plane of order $q \geq M$, one can find an arc with at least $C\sqrt{q \log q}$ and at most $C'\sqrt{q \log q}$ points whose 2-secants cover all but $\sqrt{q}(\log q)^c$ points of the plane.*

Note that this theorem also shows that in any plane there are arcs with at least $C''\sqrt{q \log q}$ points. In the paper [60], Kim and Vu give a randomized algorithm running in roughly $\log^{5/2} q$ steps, each step consists of $O(q^4)$ basic operations, which produces the arc in the above theorem with high probability.

Acknowledgement. Special thanks are due to **László Lovász, József Beck, Endre Boros** and **Zoltán Füredi**. We learned the application of probabilistic methods in combinatorics (for example the use of Chernoff's inequality) from them. We also thank **Van Ha Vu** for suggestions on the first version of this paper.

REFERENCES

[1] V. ABATANGELO, A class of complete $((q+8)/3)$-arcs in $\mathrm{PG}(2,q)$, with $q = 2^h$ and $h \geq 6$ even, *Ars Comb.* **16** (1983), 103-111.

[2] H. L. ABBOTT AND A. LIU, Property of $B(s)$ and projective planes, *Ars Combin.* **20** (1985), 217–220.

[3] M. AJTAI, J. KOMLÓS, E. SZEMERÉDI, A dense infinite Sidon sequence, *Europ. J. Comb.* **2** (1981), 1–11.

[4] N. ALON, J. SPENCER, The probabilistic method, Wiley, New York, 1992.

[5] N. ALON, B. BOLLOBÁS, J. H. KIM, V. H. VU, personal communication by V. H. Vu, see the preprint at: http://www.math.ucsd.edu/ vanvu/papers/probmethod/ABKV.pdf

[6] L. BABAI, A. GÁL, A. WIGDERSON, Superpolynomial lower bounds for monotone span programs, *Combinatorica* **19** (1999) 301-319.

[7] J. Barát, S. Marcugini, F. Pambianco, T. Szőnyi, Note on disjoint blocking sets in Galois planes, *J. Combinatorial Designs*, **14** (2005) 149-158.
[8] U. Bartocci, Dense k-sets in Galois planes, *Boll. Unione Mat. Ital., VI. Ser. D, Algebra Geom. 2*, **1** (1983) 71-77.
[9] T. Béres, T. Illés, Computational investigation of the covering number of finite projective planes with small order (in Hungarian), *Alk. Mat. Lapok* **17** (1993/97), 397–411.
[10] A. Beutelspacher, Blocking sets and partial spreads in finite projective spaces, *Geometriae Dedicata* **9** (1980) 425-449.
[11] A. Blokhuis, On the size of a blocking set in $\mathrm{PG}(2,p)$, *Combinatorica* **14** (1994), 273–276.
[12] A. Blokhuis, Blocking sets in Desarguesian planes, in: *Paul Erdős is Eighty, Volume 2*, (D. Miklós, V.T. Sós and T. Szőnyi, eds.), Bolyai Soc. Math. Studies, **2**, Bolyai Society, Budapest, 1996, 133–155.
[13] A. Blokhuis, K. Metsch, On the size of a maximal partial spread. *Des. Codes Cryptogr.* **3** (1993), 187–191.
[14] A. Blokhuis, K. Metsch, Large minimal blocking sets, strong representative systems and partial unitals, in: *Finite Geometries*, (F. De Clerck et al. eds.), Cambridge Univ. Press, Cambridge, 1993, 37–52.
[15] B. Bollobás, A. Thomason, Graphs which contain all small graphs, *Europ. J. Comb.* **2** (1981), 13–15.
[16] E. Boros, $\mathrm{PG}(2,p^s)$, $p>2$ has property $\mathrm{B}(p+2)$, *Ars Comb.* **25** (1988), 111–114.
[17] E. Boros, T. Szőnyi, K. Tichler, On defining sets for projective planes, *Discrete Mathematics* **303** (2005), 17-31.
[18] A. A. Bruen, Baer subplanes and blocking sets, *Bull. Amer. Math. Soc.* **76** (1970), 342–344.
[19] A. A. Bruen, Blocking sets in finite projective planes, *SIAM J. Appl. Math.* **21** (1971), 380–392.
[20] A. A. Bruen, Spreads and a conjecture of Bruck and Bose, *J. Algebra 23* (1972), 519–537.
[21] A. A. Bruen, Partial spreads and replaceable nets, *Canad. J. Math.* **23** (1971), 381–391.
[22] A. A. Bruen, J. C. Fisher, Blocking sets and complete arcs, *Pacific J. Math.* **53** (1974), 73–84.
[23] A. A. Bruen, J. A. Thas, Blocking sets, *Geom. Dedicata* **6** (1977), 193–203.
[24] A. A. Bruen, B. L. Rotschild, Lower bounds on blocking sets, *Pacific J. Math.* **118** (1982), 303–311.
[25] P. J. Cameron, J. H. Van Lint, Designs, graphs, codes and their links, *Cambridge University Press* (1991).
[26] P. Dembowski, Finite Geometries, Springer, Berlin, 1968 and 1997.
[27] D. A. Drake, C. Kitto, Small blocking sets of Hermitian designs *J. Combin. Theory Ser. A* **65** (1994), 322–329.
[28] J. Eisfeld, L. Storme, P. Sziklai, On the spectrum of the sizes of maximal partial line spreads in $\mathrm{PG}(2n,q), n\geq 3$, *Des. Codes Cryptogr.* **36** (2005), 101–110.
[29] P. Erdős, On a problem in graph theory, *Math. Gazette* **47** (1963), 220–223.
[30] P. Erdős, L. Lovász, Problems and results on 3-chromatic hypergraphs and some related questions, in: *Infinite and finite sets* (Colloq., Keszthely, 1973; dedicated to P. Erdős on his 60th birthday), Vol. II, pp. 609–627, Colloq. Math. Soc. János Bolyai, **Vol. 10**, North-Holland, Amsterdam, 1975.
[31] P. Erdős, R. Silverman and A. Stein, Intersection properties of families of sets of nearly the same size, *Ars Combin.* **15** (1983), 247–259.
[32] P. Erdős, J. Spencer, *Probabilistic Methods in Combinatorics*, Akad. Kiadó, Academic Press, Budapest, New York, 1974.
[33] Sz. Fancsali, P. Sziklai, About Maximal Partial 2-Spreads in PG(3 m - 1,q), *Innovations in Incidence Geometry*, **4** (2007), 70–80.
[34] P. Frankl, V. Rödl, Near perfect covers in graphs and hypergraphs, *Eur. J. Comb.* **6** (1985), 317–326.
[35] Z. Füredi, Matchings and covers in hypergraphs, *Graphs and Combin.* **4** (1988), 115-206.
[36] Z. Füredi, J. Pach, Traces of finite sets, extremal problems and geometric applications, in: *Extremal problems in combinatorics, Visegrád, Hungary, 1991*, Bolyai Society Math. Studies **3**, 251–282.
[37] A. Gács, T Szőnyi, On maximal partial spreads in $\mathrm{PG}(n,q)$, *Designs, Codes and Cryptography* **29** (2003), 123–129.

[38] D. G. Glynn, A lower bound for maximal partial spreads in PG$(3, q)$, *Ars Combin.* **13** (1982), 39-40.
[39] P. Govaerts, O. Heden L. Storme, On the spectrum of sizes of maximal partial spreads in PG$(3, q)$, q even, manuscript.
[40] P. Govaerts, L. Storme, On a particular class of minihypers and its applications, I: The result for general q, *Des. Codes Cryptogr.* **28** (2003) 51-63.
[41] R. L. Graham, J. Spencer, A constructive solution to a tournament problem, *Canad. Math. Bull.* **14** (1971), 45–48.
[42] K. Gray, On the minimum number of blocks defining a design, *Bull. Austral. Math. Soc.* **41** (1990), 97–112.
[43] D. Haussler, E. Welzl, ε-nets and simple range queries, *Discr. Comput. Geom.* **2** (1987), 127–151.
[44] O. Heden, Maximal partial spreads and the modular n-queen problem, *Discrete Math.* **120** (1993), 75-91.
[45] O. Heden, Maximal partial spreads and the modular n-queen problem II, *Discrete Math.* **142** (1995), 97-106.
[46] O. Heden, Maximal partial spreads and the modular n-queen problem III, *Discrete Math.* **243** (2002), 135–150.
[47] O. Heden, A maximal partial spreads of size 45 in $PG(3, 7)$, *Designs, Codes and Cryptography* **22** (2001), 331–334.
[48] J. W. P. Hirschfeld, *Projective geometries over finite fields*, Clarendon Press, Oxford, 1979, 2nd edition, 1998.
[49] J.W.P. Hirschfeld, Finite projective spaces of three dimensions, Oxford Univ. Press (1985).
[50] J.W.P. Hirschfeld and J.A. Thas, General Galois geometries, Oxford Univ. Press (1991).
[51] J. W. P. Hirschfeld, L. Storme, The packing problem in statistics, coding theory and finite projective spaces, in: *Finite Geometries* (A. Blokhuis, J.W.P. Hirschfeld, D. Jungnickel, J. A. Thas, eds.) Developments of Mathematics, Kluwer, 2001, 201-246.
[52] J. W. P. Hirschfeld, T. Szőnyi, Constructions of large arcs and blocking sets in finite planes, *European J. Comb.*, **12** (1991), 499-511.
[53] T. Illés, D. Pisinger, Upper Bounds on the Covering Number of Galois-Planes with Small Order, *J. of Heuristics* **7** (2000), 59–76.
[54] T. Illés, T. Szőnyi and F. Wettl, Blocking sets and maximal strong representative systems in finite projective planes, *Mitt. Math. Sem. Giessen* **201** (1991), 97–107.
[55] S. Innamorati, A. Maturo, On irreducible blocking sets in projective planes, *Ratio Math.* **2** (1991), 151–155.
[56] S. Janson, On Concentration of Probability, in: *Contemporary Combinatorics* (B. Bollobás, ed.), Bolyai Society Mathematical Studies **10** (2002), 289–301.
[57] D. Jungnickel, L. Storme, A note on maximal partial spreads with deficiency $q + 1, q$ even. *J. Combin. Theory Ser. A* **102** (2003), 443-446.
[58] J. Kahn, On a problem of Erdős and Lovász: random lines in a projective plane, *Combinatorica* **12** (1992), 417–423.
[59] J. Kahn, On a problem of Erdős and Lovász II, $n(r) = O(r)$, *J. Amer. Math. Soc* **7** (1994), 125–143.
[60] J. H. Kim, V. H. Vu, Small complete arcs in projective planes, *Combinatorica* **23** (2003), 311–363.
[61] J. H. Kim, V. H. Vu, Concentration of multivariate polynomials and its applications, *Combinatorica* **20** (2000), 417–434.
[62] Gy. Kiss, S. Marcugini, F. Pambianco, On blocking sets of inversive planes, *J. of Combin. Designs* **13** (2005), 268–275.
[63] J. Komlós, J. Pach, G. Woeginger Almost tight bounds for ε-nets, *Discr. Comput. Geom.* **7** (1992) 163–173.
[64] G. Korchmáros, New examples of complete k-arcs in PG$(2, q)$, *Europ. J. Comb.* **4** (1983), 329–334.
[65] S. J. Kovács, Small saturated sets in finite projective planes, *Rend. Mat. (Roma)* **12** (1992), 157–164.
[66] L. Lovász, On the ratio of optimal integral and fractional covers, *Discrete Math.* **13** (1975), 383–390.
[67] G. Lunardon, Normal spreads, *Geom. Dedicata* **75** (1999), 245–261.

[68] G. Lunardon, O. Polverino, Linear blocking sets: a survey, in: *Finite fields and applications* (ed.: D. Jungnickel), Springer, 2001, 356–362.
[69] F. Mazzocca, O. Polverino, Blocking sets in PG$(2, q^n)$ from cones of PG$(2n, q)$, *J. Algebraic Combin.* **24** (2006), 61–81.
[70] F. Mazzocca, O. Polverino, L. Storme, Blocking sets in PG(r, q^n), *Designs, Codes and Cryptography*, to appear.
[71] K. Metsch, L. Storme, On a particular class of minihypers and its applications: II. Improvements for q square, *J. of Cominatorial Theory Ser. A* **97** (2002) 269-393.
[72] Cs. Mengyán, On the number of pairwise non-isomorphic minimal blocking sets in PG$(2, q)$, *Designs, Codes and Cryptography*, to appear.
[73] P. Polito, O. Polverino, On small blocking sets, *Combinatorica* **18** (1998), 133–137.
[74] O. Polverino, T. Szőnyi, Zs. Weiner, Blocking sets in Galois planes of square order, *Acta Sci. Math. (Szeged)* **65** (1999), 737–748.
[75] L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, Akadémiai Kiadó and Birkhäuser Verlag, Budapest and Basel, 1970.
[76] V. Rödl, On a packing and covering problem, *European J. Combinatorics* **5** (1985), 69–78.
[77] P. Sziklai, A lemma on the randomness of d-th powers in GF(q), $d|q-1$, *Bull. Belg. Math. Soc.*, **8** (2001), 95–98.
[78] P. Sziklai, On small blocking sets and their linearity, *Journal of Combinatorial Theory. Ser. A*, to appear.
[79] T. Szőnyi, Small complete arcs in Galois planes, *Geom. Dedicata* **18** (1985), 161–172.
[80] T. Szőnyi, Blocking sets in finite planes and spaces, *Ratio Math.* **5** (1992), 93–106.
[81] T. Szőnyi, Note on the existence of large minimal blocking sets in Galois planes, *Combinatorica* **12** (1992), 227–235.
[82] T. Szőnyi, Blocking sets in Desarguesian affine and projective planes, *Finite Fields Appl.* **3** (1997), 187–202.
[83] T. Szőnyi, Some applications of algebraic curves in finite geometry and combinatorics, in: *Surveys in Combinatorics* (R. A. Bailey, ed.), Cambridge Univ. Press, Cambridge, 1997, 198–236.
[84] T. Szőnyi, Small complete arcs in André planes of square order, *Graphs and Comb.* **8** (1992), 81–89.
[85] T. Szőnyi, A. Cossidente, A. Gács, Cs. Mengyán, A. Siciliano, Zs. Weiner, On large minimal blocking sets in PG$(2, q)$, *J. Combin. Des.* **13** (2005), 25–41.
[86] T. Szőnyi, A. Gács, Zs. Weiner, On the spectrum of minimal blocking sets in PG$(2, q)$, *J. of Geometry* **76** (2003),256–281.
[87] T. Szőnyi,Zs. Weiner, On large minimal blocking sets, preprint.
[88] A. Thomason, Random Graphs, Strongly Regular Graphs and Pseudo-random graphs, in: *Surveys in Combinatorics 1987*, (ed.: C. Whitehead), Cambridge Univ. Press, Cambridge, 1987, 173–195.
[89] E. Ughi, Saturated configurations of points in projective Galois spaces, *Europ. J. Comb.* **8** (1987), 325–334.
[90] E. Ughi, On (k, n)-fold blocking sets which can be obtained as a union of conics, *Geom. Dedicata*, **26** (1988), 241–246.
[91] V. H Vu, Concentration of non-Lipschitz functions and applications, *Random Struct. and Alg.* **20** (2002), 262–316.

Author's addresses:

András Gács, Tamás Szőnyi
Department of Computer Science, Eötvös Loránd University,
H-1117 Budapest, Pázmány Péter sétány 1/C, HUNGARY

e-mail: gacs@cs.elte.hu, szonyi@cs.elte.hu

Tamás Szőnyi,
Computer and Automation Research Institute of the Hungarian Academy of Sciences
H-1111 Budapest, Lágymányosi u. 11, HUNGARY

e-mail: szonyi@sztaki.hu