Minimal Symmetric Differences of lines in Projective Planes

Paul Balister

University of Memphis

Mississippi Discrete Mathematics Workshop
November 15, 2014

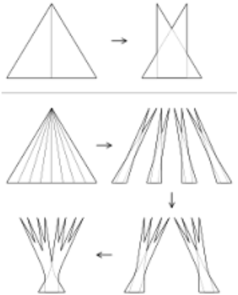
Joint work with Béla Bollobás, Zoltán Füredi, and John Thompson.

The Kakeya problem

What is the smallest set in the plane that contains a unit line segment in every direction?

Theorem (Besicovich, 1963)

The set can have arbitrarily small area.



The Kakeya problem in $\mathbb{F}_q^n$

What is the smallest set S in the affine space $\mathbb{F}_q^n$ that contains a line in every direction?

Theorem (Dvir, 2008)

$|S| \geq \binom{q^n+n-1}{n}$.

This proves the Finite field Kakeya conjecture (Wolfe, 1999) that $|S| \geq c_n|\mathbb{F}_q^n|$.

In 2 dimensions, $|S| \geq \frac{q(q+1)}{2}$.
Best known upper bound $|S| \leq \frac{q(q+1)}{2} + \frac{5q}{14} + O(1)$ (Cooper, 2006)

A generalization

Instead of insisting that all directions are represented, what if we just insist that we have r distinct lines. For simplicity we shall now work in projective space $PG(2,q)$.

Let $\mathcal{P}$ be the set of points, $\mathcal{L}$ the set of lines in $PG(2,q)$, and $N = |\mathcal{P}| = |\mathcal{L}| = q^2 + q + 1$.

Question

What is $$g(r) = \min_{R \subseteq \mathcal{L},\ |R|=r} \Big| \bigcup_{\ell \in R} \ell \Big| ?$$

Note that by duality between points and lines

$$g(r) = \min_{S \subseteq \mathcal{P},\ |S|=r} \Big| \{\ell \in \mathcal{L} : \ell \cap S \neq \emptyset\} \Big|.$$

Unions of lines

Clearly $g(r) \geq r(q+1) - \binom{r}{2}$ as each pair of lines intersects in one point, and the smallest union occurs when all these intersections are distinct.

In the dual viewpoint we have equality $g(s) = s(q+1) - \binom{s}{2}$ iff no three points of S are co-linear.

Lemma

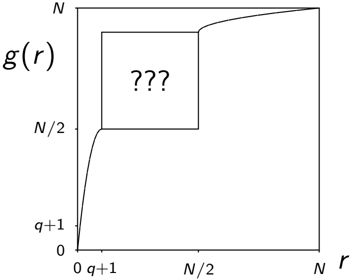
$g(r) = r(q+1) - \binom{r}{2}$ *for* $r \leq q+1$.

Proof. Use a subset S of size r of a conic in $PG(2,q)$. □

Unions of lines

$$g(r) \leq s \quad \Leftrightarrow \qquad g(N-s) \leq N-r \quad \Leftrightarrow$$

There exists a point set of size $N-s$ non-incident to a line set of size r. Hence



Question

What is $g(r)$ for $q+1 < r < (q+1)(q+2)/2$?

Symmetric differences

Instead of unions, what happens if we take symmetric differences?

Consider subsets of $\mathcal{P}$ as a binary vector in $\mathbb{F}_2^{\mathcal{P}}$.
From now on we shall always assume q is odd.

Define

$$f(r) = \min_{R \subseteq \mathcal{L},\ |R|=r} \Big| \sum_{\ell \in R} \ell \Big|$$

to be the size of the smallest symmetric difference between r distinct lines of $PG(2, q)$.

Symmetric differences

Define for $R \subseteq \mathcal{L}$, $S \subseteq \mathcal{P}$,

$$\mathcal{P}^o(R) = \sum_{\ell \in R} \ell = \{p \in \mathcal{P} : p \text{ lies in an odd number of } \ell \in R\},$$
$$\mathcal{L}^o(S) = \{\ell \in \mathcal{L} : |\ell \cap S| \text{ is odd}\}.$$

Then

- $\mathcal{P}^o \colon \mathbb{F}_2^{\mathcal{L}} \to \mathbb{F}_2^{\mathcal{P}}$ and $\mathcal{L}^o \colon \mathbb{F}_2^{\mathcal{P}} \to \mathbb{F}_2^{\mathcal{L}}$ are both linear maps.
- $\ker \mathcal{P}^o = \{\emptyset, \mathcal{L}\}$, $\ker \mathcal{L}^o = \{\emptyset, \mathcal{P}\}$.
- $|\mathcal{P}^o(R)|$ and $|\mathcal{L}^o(S)|$ are always even.
- $\mathcal{P}^o$ and $\mathcal{L}^o$ are inverse isomorphisms between the even weight subspaces of $\mathbb{F}_2^{\mathcal{P}}$ and $\mathbb{F}_2^{\mathcal{L}}$.

Also

$$f(r) = \min_{R \subseteq \mathcal{L},\ |R|=r} |\mathcal{P}^o(R)| = \min_{S \subseteq \mathcal{P},\ |S|=r} |\mathcal{L}^o(S)|.$$

Some simple observations

Lemma

$f(r) = f(N - r)$

Proof. Each point lies in $q + 1$ lines, and $q + 1$ is even, so $\sum_{\ell \in \mathcal{L}} \ell = 0$.
Thus $|\mathcal{P}^o(R)| = |\mathcal{P}^o(\mathcal{L} \setminus R)|$ and so $f(r) = f(N - r)$. □

Some simple observations

Lemma

- $r(q+2-r) \leq f(r) \leq rq + (r \bmod 1)$,
- $f(r) = r(q+2-r)$ *for* $0 \leq r \leq q+1$.

Proof. To minimize the symmetric difference between a set of lines, one would like all intersection points between lines to be distinct. Then $|\mathcal{P}^o(R)| = r(q+2-r)$. This can be obtained by taking the dual of r points on a conic if $r \leq q+1$.

It is clear that $f(1) = q+1$ and $f(2) = 2q$, and $f(x+y) \leq f(x) + f(y)$. Hence $f(r) \leq rq + (r \bmod 1)$. □

Some simple observations

Lemma

$f(r) \equiv r(q+2-r) \bmod 4.$

Proof. Consider adding the rth line. It must meet all previous $r-1$ lines, so the number of intersection points where it meets an odd number of previous lines is $x \equiv r-1 \bmod 2$. But the symmetric difference then increases by $q+1-2x \equiv q+3-2r \bmod 4$. Thus the symmetric difference is the same mod 4 as if all intersection points between pairs of lines are distinct. □

Some observations

Lemma

$|f(r+1) - f(r)| \le q - 1$ *for* $0 < r < N-1$.

Proof. One can always add a line that meets $\mathcal{P}^o(R)$ when $R \neq \emptyset, \mathcal{L}$. Thus $f(r+1) \le f(r) + q - 1$.
The reverse inequality follows as $f(r) = f(N-r)$. □

There are in fact several values of r for which $|f(r+1) - f(r)| = q - 1$.

The middle range

For almost all values $Cq^{3/2} < r < N - Cq^{3/2}$, it is possible to calculate $f(r)$ exactly. (However, there does not seem to be a nice way of describing the answer). In particular, for these vales of r, $f(r)$ is quite small.

Theorem

$f(r) \leq q$ for $Cq^{3/2} < r < N - Cq^{3/2}$.

The middle range

Fix an set S of points of even size. Then if $R = \mathcal{L}^o(S)$ we have $S = \mathcal{P}^o(R)$. As $f(r)$ is always even, determining $f(r)$ for even r is equivalent to the following:

Find the smallest even sized set S such that $|\mathcal{L}^o(S)| = r$.

For odd r we have $f(r) = f(N - r)$ and $N - r$ is even.

Clique decompositions

Given S, we can use the lines of the projective plane to edge-decompose the complete graph K_S into cliques $K_{\ell \cap S}$.
Indeed, each edge of K_S lines in a unique line $\ell \in \mathcal{L}$ and this line joins all pairs of points in $\ell \cap S$.

List the lines of $\mathcal{L}$ as $\ell_1, \ldots, \ell_N$ and define $s_i = |\ell_i \cap S|$.
Let Π be an edge-decomposition of K_S into cliques of size s_i. Define

$$M(\Pi) = \sum \left\lfloor \frac{s_i}{2} \right\rfloor$$

Lemma

If $|S| = s$ is even, and Π is the clique decomposition corresponding to S. Then $|\mathcal{L}^o(S)| = s(q+1) - 2M(\Pi)$.

Clique decompositions

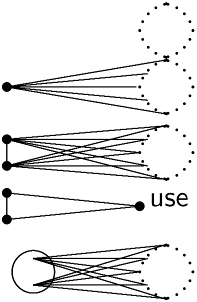
Hence for a given size s of S, it is enough to:

- Determine the possible values of $M(\Pi)$ when Π is an arbitrary clique decomposition of K_s.
- Determine which of these clique decompositions can be realized in the projective plane.

In practice, for s not too close to 0 or $q+1$, one gets a solid range of possible values for $M(\Pi)$, subject to parity, from about $s+O(\sqrt{s})$ to $\gg s$. We also get a few explicitly determined values from s to $s+O(\sqrt{s})$. From these it is easy to determine the minimum $|S|$ for which $|\mathcal{L}^o(S)|=r$ is solvable when r is not too close to 0 or N.

Clique decompositions

Π	$M(\Pi)$	Clique decomposition
s	$\lfloor \frac{s}{2} \rfloor$	
$s-1, 2, \ldots, 2$	$\lfloor \frac{s-1}{2} \rfloor + s - 1$	
$s-2, 2, 2, \ldots, 2$	$\lfloor \frac{s-2}{2} \rfloor + 2(s-2) + 1$	
$s-2, 3, 2, \ldots, 2$	$\lfloor \frac{s-2}{2} \rfloor + 2(s-2) - 1$	use as triangle
$s-i, 2, \ldots, 2$	$\lfloor \frac{s-i}{2} \rfloor + i(s-i) + \binom{i}{2}$	
$s-i, 3, \ldots, 2$	$\lfloor \frac{s-i}{2} \rfloor + i(s-i) - \binom{i}{2}$	varies in steps of 2



As $s_1 = s - i$ decreases, a range of values (in steps of 2) is possible. For $i \gg \sqrt{s}$ these ranges overlap and give a solid range of possible $M(\Pi)$.

Clique decompositions

Definition

Π is simple if all but one clique is either an edge or a triangle.

Theorem

If there exists a clique decomposition of K_s with $M(\Pi) < \frac{1}{4}s(\sqrt{4s-3}-1)$ then there exists a simple clique decomposition Π' with $M(\Pi') = M(\Pi)$.

As the interesting $M(\Pi)$ are $O(s)$, we can reduce to the case of simple clique decompositions.

Realizing decompositions

Suppose we have a (simple) clique decomposition of K_s, can we realize is with a set S of size s in $PG(2, q)$?

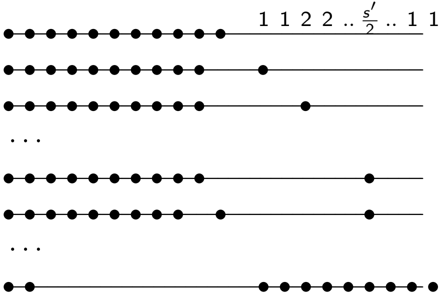
Construction:

Put s_1 points on a line at infinity ℓ_∞, say $T \subseteq \ell_\infty$. Put the other $s' = s - s_1$ points C on the conic $y = x^2$, at $(0, 0)$, $(1, 1)$, $(2, 4)$,. . . .

Then ℓ_∞ induces the clique K_{s_1} and all lines through the remaining points induce either K_2s or K_3s. The number of K_3s is the number of lines through two points of C that meet T.

Realizing decompositions

Note that there is 1 line through points of C with slope 1, 1 with slope 2, 2 with slope 3, 2 with slope 4, ...



Theorem

If $0 \leq s \leq q+1$ and $s_1 \geq \max\{(2s-3)/3, (2s-3)-(q+1)\}$ then any simple decomposition Π of K_s can be realized by a set of points in $PG(2,q)$.

Calculating $f(r)$

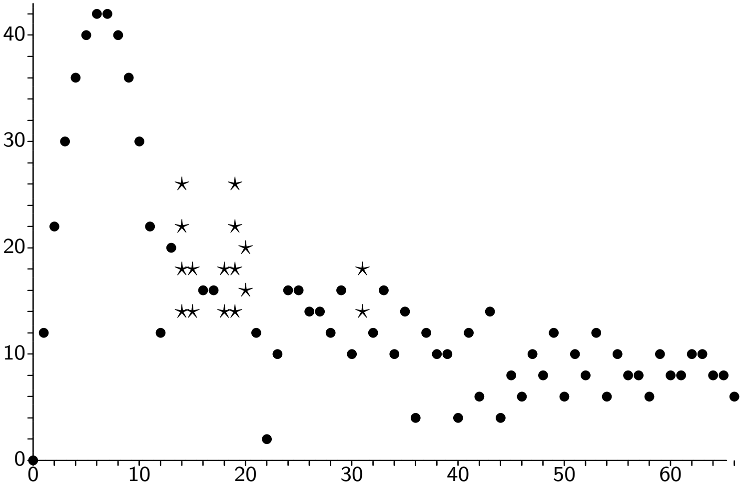
If r is odd, calculate $f(N-r)$ instead.

Loop through even s with $qs \geq r$.

> If there is a simple clique decompositions of K_s with $r = s(q+1) - 2M(\Pi)$ and it can be realized in $PG(2,q)$, return s.
>
> Otherwise, if there is a simple clique decompositions of K_s with $r = s(q+1) - 2M(\Pi)$, return "undetermined"
>
> If not every clique decomposition is equivalent to a simple one, return "undetermined".

Repeat

Numerical results $q = 11$



Other results

Theorem

The maximum of $f(r)$ *occurs at* $r = (q+1)/2, (q+3)/2, N-(q+1)/2, N-(q+3)/2.$

Theorem

$f(2q-1) = q+1$, $f(2q) = 2$, $f(2q+1) = q-1.$

Theorem

$3(q+1)/2 \le f(q+2) \le 2q-2.$

Conjecture

$f(q+2) = 2q-2.$

$f(q+2)$

Theorem (Bichara, Korchmáros, 1980)

Let R be a set of $q+2$ lines in $\mathcal{L}$, then there are at most 2 lines without triple points.

Proof. Assume there are 3 lines without triple points. Wlog they are $x=0$, $y=0$, and the line at infinity. But then each other point on these lines intersects exactly one of the remaining q lines of R.
The remaining lines are $a_i(x-b_i)$ with $\{a_i\}=\{b_i\}=\{a_ib_i\}=\mathbb{F}_q^\times$. But $\prod_{x\in\mathbb{F}_q^\times} x=-1$ so $-1=\prod a_ib_i=(\prod a_i)(\prod b_i)=(-1)(-1)$, a contradiction. □

$f(q+2)$

Theorem (Jamison (1977), Brouwer and Schrijver (1978))

Any blocking set in $\mathcal{P}$ contains at least $2q-1$ points.

Proof. Let B be a blocking set. Wlog $(0,0) \in B$. Consider
$$f(x,y) = \prod_{(a_i,b_i)\in B\setminus\{(0,0)\}} (a_i x + b_i y - 1).$$
Then for each $(a,b) \neq (0,0)$ the line $ua + vb - 1$ meets $B \setminus \{(0,0)\}$, so $f(a,b) = 0$. But $f(0,0) = \pm 1$.
Write $f(x,y) \equiv g(x,y) \bmod (x^q - x, y^q - y)$, with $\deg_x g, \deg_y g < q$. Then xg is identically zero on $\mathbb{F}_q^2$. Thus $xg \in (x^q - x, y^q - y)$. But $\deg_y g < q$, so $x^q - x \mid xg$ and so $x^{q-1} - 1 \mid g$. Similarly $y^{q-1} - 1 \mid g$. But then $(x^{q-1} - 1)(y^{q-1} - 1) \mid g$, so $\deg_{\text{total}} f \geq \deg_{\text{total}} g \geq 2q - 2$. Hence $|B \setminus \{(0,0)\}| \geq 2q - 2$ and $|B| \geq 2q - 1$. □

$f(q+2)$

Lemma

Suppose $|R| = q+2$ and at least one line of R has no triple points. Then $|\mathcal{P}^o(R)| \geq 2q-2$.

Proof. Assume the line at infinity ℓ_∞ lies in R and has no triple points. Then in the Affine plane, no two finite lines of R are parallel. As there are $q+1$ finite lines, every line in $\mathbb{F}_q^2$ must be parallel to a unique line of R.
Claim: $\mathcal{P}^o(R) \cap \mathbb{F}_q^2$ blocks all lines except those of R that have no triple point.
Proof. If $\ell \notin R$ then ℓ meets an odd number $(q+1-1)$ of finite lines of R and so has an odd point.
If $\ell \in R$ and R has a triple point, then not all points on ℓ intersect another element of R. Such a point is single, so odd.
Finally, we can assume there are at most 1 finite line of R without triple points and this can be blocked by adding a single point to $\mathcal{P}^o(R)$. Thus $|\mathcal{P}^o(R)| + 1 \geq 2q-1$. □

$f(q+2)$

If every line of R has a triple point, the best we can do is $|\mathcal{P}^o(R)| \geq \frac{3}{2}(q+1)$.

We know $f(q+2) = 2q-2$ for $q \leq 13$.

Other constructions

For $r \approx 3q/2$, $f(r)$ is quite small due to the following construction (due to J. di Paola):

Let $Q^+ \subseteq \mathbb{F}_q$ be the set of non-zero quadratic residues, and $Q^- \subseteq \mathbb{F}_q$ the set of quadratic non-residues. Define

$$Q = \{[x{:}0{:}1] : x \in Q^+\} \cup \{[1{:}x{:}0] : x \in Q^+\} \cup \{[0{:}1{:}x] : -x \in Q^-\}.$$

Then $|\mathcal{L}^o(Q)| = |Q| = 3(q-1)/2$, so $f(3(q-1)/2) \leq 3(q-1)/2$.

Similar constructions show that $f(r)$ is small near $2q, 5q/2, 3q, 7q/2, \ldots$

Open problems

- Calculating or just estimating $g(r)$ for $q + 1 < r < (q + 1)(q + 2)/2$.
- Proving $f(q + 2) = 2q - 2$.
- Determining at what point $f(r)$ becomes $O(q)$ as r increases.
- Determining a (polynomial time) algorithm for calculating $f(r)$ for all r.
- Non-Desarguesian planes? (The $f(r)$ is affected by the structure of the plane.)

The End