CONFERENCE ON FINITE GEOMETRIES IN HONOUR OF FRANK DE CLERCK

17 - 18 September, 2012

Francesco Mazzocca Seconda Università di Napoli

Kakeya sets over finite fields: problems and applications



Dedicated to Frank

Dedicated to Frank and his family

Ferrara - Castello Estense

Dedicated to Frank and his family



The Kakeya Problem over Finite Field

INTRODUCTION

A Kakeya set (or Besicovitch set) in the real plane \mathbb{R}^2 is a point set in which a unit line segment can continuously rotate around completely.

PROBLEM (Kakeya Needle Problem, 1917)

What is in the real plane the smallest area of a Kakeya set?



The circle of diameter 1 and area $\frac{\pi}{4}$, the semicircle of radius 1 and area $\frac{\pi}{2}$,

the equilateral triangle of height 1 and area $\frac{1}{\sqrt{3}}$, the deltoid inscribed in a circle of diameter $\frac{3}{2}$ and area $\frac{\pi}{8}$.

A Kakeya set (or Besicovitch set) in the real plane \mathbb{R}^2 is a point set in which a unit line segment can continuously rotate around completely.

PROBLEM (Kakeya Needle Problem, 1917)

What is in the real plane the smallest area of a Kakeya set?



THEOREM (Besicovitch, 1928)

There exist Kakeya sets in \mathbb{R}^2 of arbitrarily small area.

A Kakeya set (or Besicovitch set) in the real plane \mathbb{R}^2 is a point set in which a unit line segment can continuously rotate around completely.

PROBLEM (Kakeya Needle Problem, 1917)

What is in the real plane the smallest area of a Kakeya set?



THEOREM (Besicovitch, 1928)

There exist Kakeya sets in \mathbb{R}^2 of arbitrarily small area.

A Kakeya set (or Besicovitch set) in the real plane \mathbb{R}^2 is a point set in which a unit line segment can continuously rotate around completely.

REMARK

If continuity is not requested in the above definition, then there exist Kakeya sets in \mathbb{R}^2 with zero Lebesgue measure. If this is the case, the sets are still necessary two-dimensional, in the sense of Hausdorff dimension (M.Davies, 1971).

A Kakeya set in \mathbb{R}^n is a compact point set containing a unit line segment in every direction.

A Kakeya set in \mathbb{R}^n is a compact point set containing a unit line segment in every direction.

CONJECTURE

A Kakeya set in \mathbb{R}^n has Hausdorff dimension equal to n.

A Kakeya set in \mathbb{R}^n is a compact point set containing a unit line segment in every direction.

CONJECTURE

A Kakeya set in \mathbb{R}^n has Hausdorff dimension equal to n.

REMARK

The conjecture is still open for n > 2, although many partial results are known (*N.Katz*, *T.Tao*, *T.Wolff*).

It was *T.Wolff* who proposed the definition of Kakeya set over finite fields.

REFERENCE

T.Wolff, *Recent work connected with the Kakeya problem.* Prospects in mathematics (Princeton, NJ, 1996), pages 129-162, 1999. It was *T.Wolff* who proposed the definition of Kakeya set over finite fields.

DEFINITION

A point set *E* in the *n*-dimensional affine space AG(n, q) is said to be a Kakeya set if it contains lines in every directions.

REFERENCE

T.Wolff, *Recent work connected with the Kakeya problem.* Prospects in mathematics (Princeton, NJ, 1996), pages 129-162, 1999.

Kakeya Sets over Galois Fields

Standard Model for Minimal Kakeya Sets

Let π be the set of all directions of AG(n, q). For every $\alpha \in \pi$ let ℓ_{α} be a line with slope α . Then a standard model of minimal Kakeya set is given by

$$E = \bigcup_{lpha \in \pi} \ell_{lpha}.$$



Kakeya Sets over Galois Fields

Standard Model for Minimal Kakeya Sets

Let π be the set of all directions of AG(n, q). For every $\alpha \in \pi$ let ℓ_{α} be a line with slope α . Then a standard model of minimal Kakeya set is given by

$$\mathsf{E} = \bigcup_{\alpha \in \pi} \ell_{\alpha}.$$



REMARK

The case n = 1 is trivial: the unique Kakeya set is AG(1, q).

F.Mazzocca Seconda Università di Napoli

PROBLEM

Find the minimum size of a Kakeya set in AG(n, q).

REFERENCE

T.Wolff, *Recent work connected with the Kakeya problem.* Prospects in mathematics (Princeton, NJ, 1996), pages 129-162, 1999.

PROBLEM

Find the minimum size of a Kakeya set in AG(n, q).

REMARK

The problem was firstly raised by T.Wolff in the cited paper. In the same paper, according to the classical Kakeya conjecture, he also made the celebrated finite field Kakeya conjecture.

REFERENCE

T.Wolff, *Recent work connected with the Kakeya problem.* Prospects in mathematics (Princeton, NJ, 1996), pages 129-162, 1999.

The Finite Field Kakeya Conjecture

CONJECTURE

Let *E* be a Kakeya set in AG(n, q). Then $|E| \ge c_n q^n$, where $c_n > 0$ depends only on *n*.

CONJECTURE

Let *E* be a Kakeya set in AG(n, q). Then $|E| \ge c_n q^n$, where $c_n > 0$ depends only on *n*.

REMARK

The conjecture has had a significant influence in the subject of finite field Kakeya set theory and remained open for more than ten years.

CONJECTURE

Let *E* be a Kakeya set in AG(n, q). Then $|E| \ge c_n q^n$, where $c_n > 0$ depends only on *n*.

REMARK

The conjecture has had a significant influence in the subject of finite field Kakeya set theory and remained open for more than ten years.

It was completely solved in 2008 by Z.Dvir using the polynomial method with a beautifully simple argument.

REFERENCE

Z.Dvir, *On the size of Kakeya sets in finite fields*, J. Amer. Math. Soc., 22, 1093-1097, 2009.

The Kakeya Problem over Finite Field

THE DVIR'S THEOREM AND THE SOLUTION OF THE FFK CONJECTURE

The polynomials in $F_q[x_1, x_2, ..., x_n]$ of degree at most q - 1 in each variable and the zero polynomial are called *reduced polynomials*.

PROPOSITION

Let $f \in F_q[x_1, x_2, ..., x_n]$ be a reduced polynomial. If f(a) = 0 for all $a \in F_q^n$, then f is the zero polynomial.

Let *E* be a point set in AG(n, q) with $|E| < \binom{n+d}{n}$, for some positive integer *d*. Then there exists a non zero polynomial $f \in F_q[x_1, x_2, ..., x_n]$ of degree $\leq d$ and vanishing on *E*.

Let *E* be a point set in AG(n, q) with $|E| < \binom{n+d}{n}$, for some positive integer *d*. Then there exists a non zero polynomial $f \in F_q[x_1, x_2, ..., x_n]$ of degree $\leq d$ and vanishing on *E*.

COROLLARY

Let E be a point set in AG(n, q) and assume that there is no reduced polynomial of degree $\leq d$ vanishing on E. Then

$$|E| \geq \binom{n+d}{n}.$$

Let *E* be a point set in AG(n, q) with $|E| < \binom{n+d}{n}$, for some positive integer *d*. Then there exists a non zero polynomial $f \in F_q[x_1, x_2, ..., x_n]$ of degree $\leq d$ and vanishing on *E*.

COROLLARY (d = q - 1)

Let E be a point set in AG(n, q) and assume that there is no reduced polynomial of degree less than q vanishing on E. Then

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

Let *E* be a point set in AG(n, q) with $|E| < \binom{n+d}{n}$, for some positive integer *d*. Then there exists a non zero polynomial $f \in F_q[x_1, x_2, ..., x_n]$ of degree $\leq d$ and vanishing on *E*.

COROLLARY (d = q - 1)

Let E be a point set in AG(n, q) and assume that there is no reduced polynomial of degree less than q vanishing on E. Then

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

Let E be a Kakeya set in AG(n, q). Then there are no reduced polynomials $f \in F_q[x_1, x_2, ..., x_n]$ of degree < q vanishing on E.

Let E be a Kakeya set in AG(n, q). Then there are no reduced polynomials $f \in F_q[x_1, x_2, ..., x_n]$ of degree < q vanishing on E.

THEOREM

Let E be a Kakeya set in AG(n, q). Then

$$|\mathbf{E}| \geq \binom{q+n-1}{n} = \frac{1}{n!} q(q+1)\cdots(q+n-1) \geq \frac{1}{n!} q'$$

and Wolff's conjecture is true with $c_n = \frac{1}{n!}$.

The Kakeya Problem over Finite Field

IMPROVEMENTS OF DVIR'S THEOREM

In 2008, S. Saraf and M. Sudan derived an improvement to the Dvir's constant $c_n = \frac{1}{n!}$.

This was done by considering polynomials that vanish with high multiplicity on a Kakeya set E in AG(n, q). More precisely they proved that

 $|E|\geq \frac{1}{4^n} q^n$

REFERENCE

In 2008, S. Saraf and M. Sudan derived an improvement to the Dvir's constant $c_n = \frac{1}{n!}$. This was done by considering polynomials that vanish with high

multiplicity on a Kakeya set E in AG(n, q). More precisely they proved that

 $|E|\geq \frac{1}{4^n} q^n$

REMARK

Dvir noted that the constant 4 can be improved to 2.6.

REFERENCE

In 2008, S. Saraf and M. Sudan derived an improvement to the Dvir's constant $c_n = \frac{1}{n!}$. This was done by considering polynomials that vanish with high

multiplicity on a Kakeya set E in AG(n, q). More precisely they proved that

 $|E|\geq \frac{1}{4^n} q^n$

REMARK

Dvir noted that the constant 4 can be improved to 2.6.

REFERENCE

The Saraf-Sudan result is a corollary of the following theorem.

THEOREM

Let E be a point set in AG(n,q) such that

$$|| < q^n / \binom{m+n-1}{n}$$

for some positive integer m. Then there exists a non zero reduced polynomial $f \in F_q[x_1, x_2, ..., x_n]$ vanishing on E with multiplicity $\geq m$ on every point of E.

REFERENCE

Improvements of the Saraf-Sudan Constant

In 2009, Z. Dvir, S. Kopparty, S. Saraf, and M. Sudan derived an improvement to the previous Saraf-Sudan constant $c_n = \frac{1}{4^n}$. This was done by considering more deep arguments about polynomials that vanish with high multiplicity on a Kakeya set *E* in AG(n, q). They were able to prove that

$$|E|\geq rac{1}{2^n} q^n$$

REFERENCE

Z. Dvir, S. Kopparty, S. Saraf, and M. Sudan, *Extensions to the method of multiplicities, with applications to Kakeya sets and mergers*, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pages 181-190, Washington, DC, USA, 2009. IEEE Computer Society.

The problem of finding the exact value of the minimum size of a Kakeya set seems to be very hard and gets more difficult as the dimension n increases.

The problem of finding the exact value of the minimum size of a Kakeya set seems to be very hard and gets more difficult as the dimension n increases.

At this moment, it is completely solved only in dimension two and we will give a brief account of this.

REFERENCE

X.W.C.Faber, On the Finite Field Kakeya Problem in Two Dimensions, J. Number Theory, 117, 471-481, (2006).

REFERENCE

X.W.C.Faber, On the Finite Field Kakeya Problem in Two Dimensions, J. Number Theory, 117, 471-481, (2006).

REMARK

Some of central results by Faber were already known in their dual form (Bichara-Korchmáros (1982) and Blokhuis-Bruen (1989)).

REFERENCE

X.W.C.Faber, On the Finite Field Kakeya Problem in Two Dimensions, J. Number Theory, 117, 471-481, (2006).

REMARK

Some of central results by Faber were already known in their dual form (Bichara-Korchmáros (1982) and Blokhuis-Bruen (1989)).

REFERENCE

A. Bichara and G. Korchmáros, Note on (q+2)-Sets in a Galois Plane of Order q, Ann. Discrete Math., 14 (1982), 117121.

REFERENCE

X.W.C.Faber, On the Finite Field Kakeya Problem in Two Dimensions, J. Number Theory, 117, 471-481, (2006).

REMARK

Some of central results by Faber were already known in their dual form (Bichara-Korchmáros (1982) and Blokhuis-Bruen (1989)).

REFERENCE

A. Bichara and G. Korchmáros, Note on (q+2)-Sets in a Galois Plane of Order q, Ann. Discrete Math., 14 (1982), 117121.

REFERENCE

A. Blokhuis and A. A. Bruen, *The Minimal Number of Lines Intersected by a Set of q* +2 *Points, Blocking Sets, and Intersecting Circles, J.* Combin. Theory Ser. A, 50 (1989), 308315. In the following I will make use of the following plane configurations:

- ovals and hyperovals,
- (q + t, t)-arcs of type (0, 2, t),
- dual blocking sets.

In the following I will make use of the following plane configurations:

- ovals and hyperovals,
- (q + t, t)-arcs of type (0, 2, t),
- dual blocking sets.

Ovals and hyperovals are well known to the audience, so I will recall later the definitions and some properties only for (q + t, t)-arcs of type (0, 2, t) and dual blocking sets

The Finite Field Kakeya Problem: the case n = 2, q even

EXAMPLE (Kakeya Sets of Hyperoval type)

Assume q is even and consider in $PG(2,q) = AG(2,q) \cup \ell_{\infty}$ a dual hyperoval \mathcal{H} containing ℓ_{∞} . For every point $P \in \ell_{\infty}$, let ℓ_P the line of \mathcal{H} on P other than ℓ_{∞} . Then the Kakeya set in AG(2,q)

 $E = (\bigcup_{P \in \ell_{\infty}} \ell_P) \setminus \ell_{\infty}$

is of size $\frac{q(q+1)}{2}$.

PROPOSITION

In AG(2, q) with q even, $|E| \ge \frac{q(q+1)}{2}$ for every Kakeya set E. The equality holds iff E is of the hyperoval type.

The Finite Field Kakeya Problem: the case n = 2, q odd

EXAMPLE (Kakeya Sets of Oval type)

Assume q is odd and consider in $PG(2,q) = AG(2,q) \cup \ell_{\infty}$ a dual oval \mathcal{O} . Every point P on ℓ_{∞} , but one, belongs to a second line $\ell_P \in \mathcal{O}$ other than ℓ_{∞} . If A is this remaining point on ℓ_{∞} , let ℓ_A be a line through it different from ℓ_{∞} . Then the Kakeya set in AG(2,q)

$$\mathsf{E} = (\bigcup_{\mathsf{P} \in \ell_{\infty}} \ell_{\mathsf{P}}) \setminus \ell_{\infty}$$

is of size

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

The existence of Kakeya sets of oval type suggested to Faber to make the following congecture.

CONJECTURE (X.Faber Conjecture, 2006)

If q is odd and E is a Kakeya set in AG(2, q), then

$$|E|\geq \frac{q(q+1)}{2}+\frac{q-1}{2}$$

The equality holds if and only if E is of oval type.

The Finite Field Kakeya Problem: the case n = 2, q odd

PROPOSITION (A.Blokhuis - F.M., 2008)

The Faber's conjecture is true: if q is odd and E is a Kakeya set in AG(2,q), then

$$|E|\geq \frac{q(q+1)}{2}+\frac{q-1}{2}$$

The equality holds if and only if E is of oval type.

REFERENCE

A.Blokhuis and F.M., *The Finite Field Kakeya Problem*, Bridges Between Mathematics and Computer Science, Bolyay Society Mathematical Studies, Vol.19, Grötschel M., Katona G. ((Eds.), Springer, 2008.

The Finite Field Kakeya Problem: the case n = 2, q odd

PROPOSITION (A.Blokhuis - F.M., 2008)

The Faber's conjecture is true: if q is odd and E is a Kakeya set in AG(2,q), then

$$|E|\geq \frac{q(q+1)}{2}+\frac{q-1}{2}$$

The equality holds if and only if E is of oval type.

REFERENCE

A.Blokhuis and F.M., *The Finite Field Kakeya Problem*, Bridges Between Mathematics and Computer Science, Bolyay Society Mathematical Studies, Vol.19, Grötschel M., Katona G. ((Eds.), Springer, 2008.

REFERENCE

S.Ball, On sets of points in a finite affine plane containing a line in every direction, preprint, 2008.

The Finite Field Kakeya Problem in the case n = 2, q even: the second smallest size

EXAMPLE (Kakeya Sets of quasi-hyperoval type)

Assume q is even and consider in $PG(2,q) = AG(2,q) \cup \ell_{\infty}$ a Kakeya set $E(\mathcal{H})$ associated to a dual hyperoval \mathcal{H} containing ℓ_{∞} :

$$E(\mathcal{H}) = (\bigcup_{P \in \ell_{\infty}} \ell_P) \setminus \ell_{\infty}.$$

Fix a point $A \in \ell_{\infty}$ and a line ℓ' through A different from ℓ_A and ℓ_{∞} . Then the Kakeya set in AG(2, q)

 $E = (E(\mathcal{H}) \setminus \ell_A) \cup (\ell' \setminus \ell_\infty)$

is of size

$$\frac{q(q+2)}{2}$$

The Finite Field Kakeya Problem in the case n = 2, q even: the second smallest size

PROPOSITION (A. Blokhuis, A.A. Bruen, 1989)

There are no Kakeya sets E in AG(2, q), q even, with

$$\frac{1}{2}q(q+1) < |E| < \frac{1}{2}q(q+2).$$

Furthermore, all Kakeya sets of size $\frac{1}{2}q(q+2)$ are of quasi-hyperoval type.

REFERENCE

A. Blokhuis and A.A. Bruen, The minimal number of lines intersected by a set of q + 2 points, blocking sets, and intersecting circles, J. Combin. Theory Ser. A, 50, 308-315, 1989.

(q+t,t)-arcs of type (0,2,t) in PG(2,q)

DEFINITION

A (q+t,t)-arc of type (0,2,t) in PG(2,q), q even (and t|q), is a set of q+t points intersecting any line in 0,2 or t points.

REFERENCE

G. Korchmáros and F.M.: On (q + t, t)-arc of type (0, 2, t) in a desarguesian plane of order q, Math. Proc. Camb. Phil. Soc., 108(3), 445-459, (1990).

(q+t,t)-arcs of type (0,2,t) in PG(2,q)

DEFINITION

A (q+t,t)-arc of type (0,2,t) in PG(2,q), q even (and t|q), is a set of q+t points intersecting any line in 0,2 or t points.

REFERENCE

G. Korchmáros and F.M.: On (q + t, t)-arc of type (0, 2, t) in a desarguesian plane of order q, Math. Proc. Camb. Phil. Soc., 108(3), 445-459, (1990).

PROPOSITION

The t-secant lines to a (q + t, t)-arc of type (0, 2, t) of PG(2, q) are concurrent in a point (called the t-nucleus).

REFERENCE

A. Gács and Zs. Weiner: On (q + t, t) - arc of type (0, 2, t), Des. Codes Cryptogr., 29(1- 3), 131-139, (2003).

(q + 4, 4)-arcs of type (0, 2, 4) in PG(2, q)

For t = 4, it remains an open problem for which values of q a (q + 4, 4)-arc of type (0, 2, 4) exist.

There are know examples only for q = 8, 16, 32.

The conjecture is that these arcs do not exist for q > 32.

REFERENCE

G. Korchmáros and F.M.: On (q + t, t)-arc of type (0, 2, t) in a desarguesian plane of order q, Math. Proc. Camb. Phil. Soc., 108(3), 445-459, (1990).

REFERENCE

J.D. Key, T.P. McDonough, V.C. Mavron: An upper bound for the minimum weight of the dual codes of desarguesian planes, European J. Combin., 30(1), 220-229, (2009).

The Finite Field Kakeya Problem in the case n = 2, q even: the third smallest size

Now we describe a Kakeya set, which we will see to be the third smallest example, provided that it exists.

EXAMPLE (Kakeya Sets of (0, 2, 4)-arc type)

Let \mathcal{A} be a dual (q + 4)-arc of type (0, 2, 4) in PG(2, q), and let $\ell_0, \ell_1, \ell_2, \ell_\infty$ be four concurrent lines of \mathcal{A} . Consider the affine plane $AG(2, q) = PG(2, q) \setminus \ell_\infty$. Let \mathcal{A}' be the line set $\mathcal{A} \setminus \{\ell_1, \ell_2\}$. Consider the set

$$E(\mathcal{A}, \ell_1, \ell_2) = \bigcup_{L \in \mathcal{A}'} (L \setminus \ell_\infty).$$

This is a Kakeya set since there is precisely one line of $E(A, L_1, L_2)$ through every point of L_{∞} . It has size $\frac{1}{2}q(q+2) + \frac{1}{4}q$.

The Finite Field Kakeya Problem in the case n = 2, q even: the third smallest size

PROPOSITION (A. Blokhuis, M. De Boeck, F.M. and L. Storme, 2011)

There are no Kakeya sets E in AG(2, q), q even, with

$$rac{1}{2}q(q+2) < |E| < rac{1}{2}q(q+2) + rac{1}{4}q.$$

Furthermore, all Kakeya sets of size $\frac{1}{2}q(q+2) + \frac{1}{4}q$ are of (0, 2, 4)-arc type.

REFERENCE

A. Blokhuis, M. De Boeck, F.M. and L. Storme, *The Kakeya* problem: a gap in the spectrum and classification of the smallest examples, 2011.

The Kakeya Problem over Finite Field

APPLICATIONS

A *dual blocking set* (or *anti-blocking set*) S in $\pi_q = PG(2, q)$ is a point set meeting every blocking set and containing no lines.

REFERENCE

P.J.Cameron, F.M., R.Meshulam, *Dual blocking sets in projective and affine planes,* Geometriae Dedicata, 27, 1988, n.2, 203-207.

A *dual blocking set* (or *anti-blocking set*) S in $\pi_q = PG(2, q)$ is a point set meeting every blocking set and containing no lines.

PROPOSITION

Let S be a minimal dual blocking set in π_q . Then one of the two following possibilities occur:

- $S = (\bigcup_{P \in \ell} \ell_P) \setminus \ell$ is a Kakeya set;
- S = π_q \ (ℓ ∪ m) is the complement of the union of two distinct lines ℓ and m.

REFERENCE

P.J.Cameron, F.M., R.Meshulam, *Dual blocking sets in projective and affine planes,* Geometriae Dedicata, 27, 1988, n.2, 203-207.

PROPOSITION (1988)

Let S be a dual blocking set in π_q . Then

$$|S| \geq \frac{q(q+1)}{2}.$$

Equality holds if and only if either

- *S* is the Kakeya set associated to a dual hyperoval and one of its lines; or
- *q* = 3 and *S* is the complement of the union of two distinct lines.

The study of dual blocking sets in PG(2, q)is equivalent to the study of Kakeya sets in AG(2, q).

CONJECTURE (Cooper-Solymosi, 2005)

In AG(2, q), q odd, the number of the collinear triples in the graph of a permutation of GF(q) is at least (q - 1)/2.

CONJECTURE (Cooper-Solymosi, 2005)

In AG(2, q), q odd, the number of the collinear triples in the graph of a permutation of GF(q) is at least (q - 1)/2.

The points of the graph of a permutation σ of GF(q), q odd, in AG(2,q) together with the directions of the two frame axis form a (q+2) – set of points Σ in PG(2,q) with a nucleus.

CONJECTURE (Cooper-Solymosi, 2005)

In AG(2, q), q odd, the number of the collinear triples in the graph of a permutation of GF(q) is at least (q - 1)/2.

The points of the graph of a permutation σ of GF(q), q odd, in AG(2, q) together with the directions of the two frame axis form a (q + 2) - set of points Σ in PG(2, q) with a nucleus. The dual Σ^* of Σ is a Kakeya set of size

$$\frac{q(q+1)}{2} + \epsilon$$

and it is possible to prove that ϵ is just the number of collinear triples of the graph of $\sigma.$

THEOREM

The Cooper-Solymosi conjecture is true: in AG(2,q), q odd, the number of the collinear triples in the graph of a permutation of GF(q) is at least (q - 1)/2.

REFERENCE

S.Ball, On sets of points in a finite affine plane containing a line in every direction, preprint, 2008.

REFERENCE

L.Li, *Collinear triples in permutations*, Innovation in incidence geometry, vol.8, 2008.

The End



GRAZIE !

F.Mazzocca Seconda Università di Napoli