Upper bounds on the size of Kakeya sets in finite vector spaces

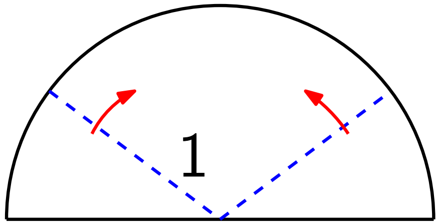
Gohar Kyureghyan[1], Peter Müller[2] and Qi Wang[1]

[1]Otto-von-Guericke University Magdeburg, Germany

[2]University of Würzburg, Germany

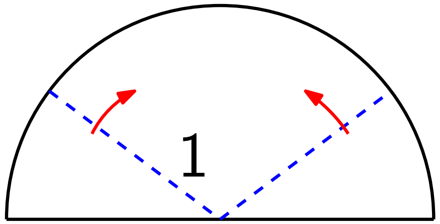
WCC 2013

The classical Kakeya problem

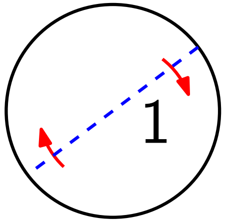


a semi-circle of radius 1

The classical Kakeya problem

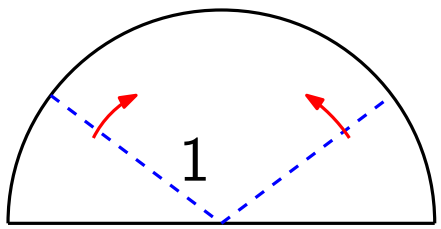


a semi-circle of radius 1

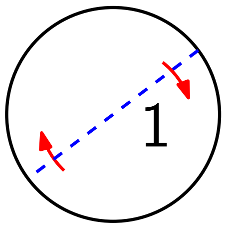


a circle of diameter 1

The classical Kakeya problem



a semi-circle of radius 1



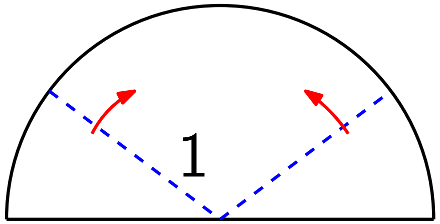
a circle of diameter 1

In the real plane $\mathbb{R}^2$, consider a point set which contains a unit segment in every direction.

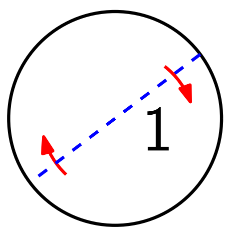
How small can the area of such a point set be in $\mathbb{R}^2$?

[Kakeya, 1917]

The classical Kakeya problem



a semi-circle of radius 1



a circle of diameter 1

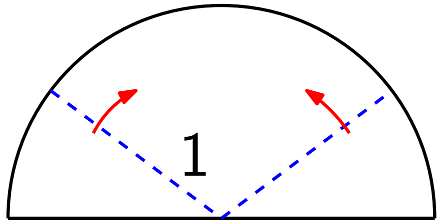
In the real plane $\mathbb{R}^2$, consider a point set which contains a unit segment in every direction.

Kakeya set

How small can the area of such a point set be in $\mathbb{R}^2$?

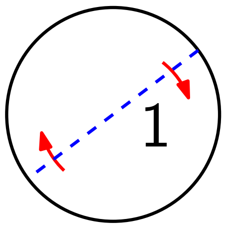
[Kakeya, 1917]

The classical Kakeya problem



$\frac{\pi}{2}$

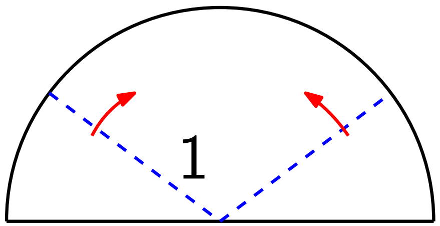
a semi-circle of radius 1



$\frac{\pi}{4}$

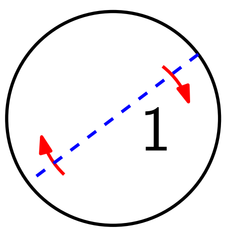
a circle of diameter 1

The classical Kakeya problem



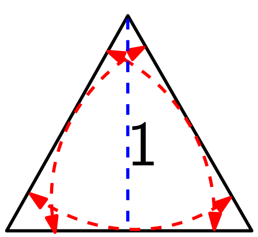
$\frac{\pi}{2}$

a semi-circle of radius 1



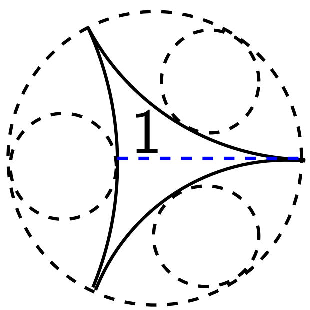
$\frac{\pi}{4}$

a circle of diameter 1



$\frac{\sqrt{3}}{3}$

an equilateral triangle of height 1



$\frac{\pi}{8}$

a deltoid inscribed in a circle of diameter $\frac{3}{2}$

The classical Kakeya problem

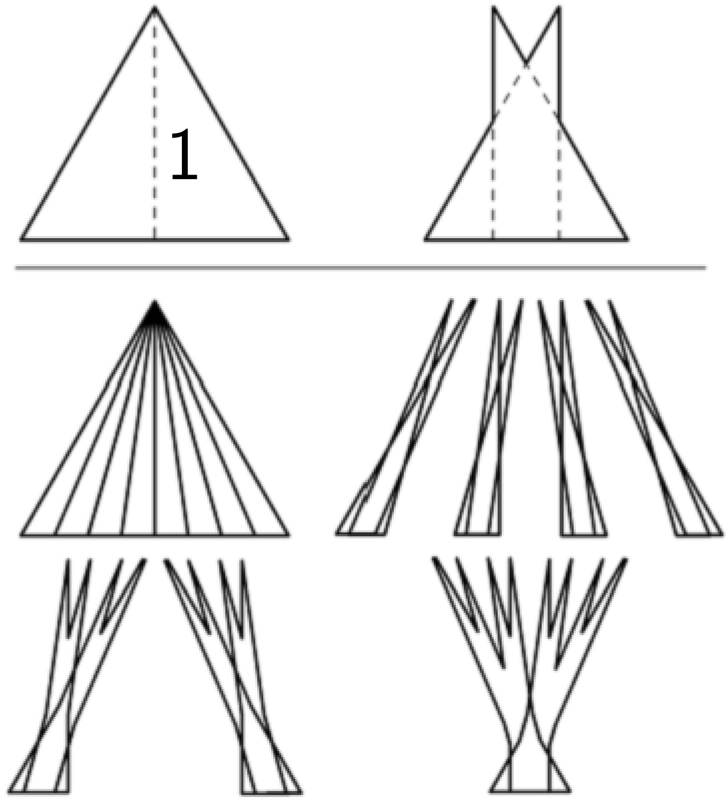
- *There exist Kakeya sets in* $\mathbb{R}^2$ *of arbitrarily small area.*

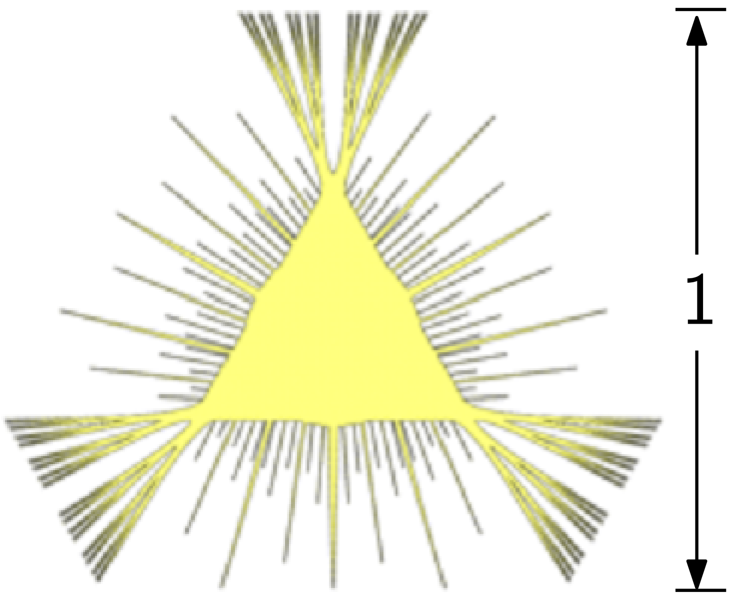
  [Besicovitch, 1928]

The classical Kakeya problem

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

[Besicovitch, 1928]





The Kakeya problem in finite vector spaces

- The classical Kakeya problem

  How small can a Kakeya set be in $\mathbb{R}^2$?

The Kakeya problem in finite vector spaces

- The classical Kakeya problem

  How small can a Kakeya set be in $\mathbb{R}^2$?

  $\mathbb{R}^n$

The Kakeya problem in finite vector spaces

- The classical Kakeya problem

  How small can a Kakeya set be in $\mathbb{R}^2$?

  $\mathbb{R}^n$

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

  How small can a subset K of $\mathbb{F}_q^n$ be, given that it contains a line in every direction?

The Kakeya problem in finite vector spaces

- The classical Kakeya problem

  How small can a Kakeya set be in $\mathbb{R}^2$?

  $\mathbb{R}^n$

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

  How small can a subset K of $\mathbb{F}_q^n$ be, given that it contains a line in every direction?

  $\Downarrow$

  For every $\mathbf{x} \in \mathbb{F}_q^n$, there exists $\mathbf{y} \in \mathbb{F}_q^n$ such that $\{\mathbf{y} + t\mathbf{x} : t \in \mathbb{F}_q\} \subseteq K$.

The Kakeya problem in finite vector spaces

Examples:

- trivial: $K = \mathbb{F}_q^n$

The Kakeya problem in finite vector spaces

Examples:

- trivial: $K = \mathbb{F}_q^n \quad \Rightarrow \quad |K| \leq q^n$

The Kakeya problem in finite vector spaces

Examples:

- trivial: $K = \mathbb{F}_q^n \quad \Rightarrow \quad |K| \leq q^n$

- $K = \{(0,0,0),(0,0,1),(0,1,1),(1,0,1),(1,1,1)\} \subset \mathbb{F}_2^3$

The Kakeya problem in finite vector spaces

Examples:

- trivial: $K = \mathbb{F}_q^n \quad \Rightarrow \quad |K| \leq q^n$

- $K = \{(0,0,0),(0,0,1),(0,1,1),(1,0,1),(1,1,1)\} \subset \mathbb{F}_2^3$

$\mathbf{x}$	$\mathbf{y}$	$\{\mathbf{y} + t\mathbf{x} : t \in \mathbb{F}_2\}$
$(0,0,1)$	$(1,0,0)$	$\{(1,0,0),(1,0,1)\} \not\subseteq K$

The Kakeya problem in finite vector spaces

Examples:

- trivial: $K = \mathbb{F}_q^n \quad \Rightarrow \quad |K| \leq q^n$
- $K = \{(0,0,0),(0,0,1),(0,1,1),(1,0,1),(1,1,1)\} \subset \mathbb{F}_2^3$

$\mathbf{x}$	$\mathbf{y}$	$\{\mathbf{y} + t\mathbf{x} : t \in \mathbb{F}_2\}$	
$(0,0,1)$	$(1,0,0)$	$\{(1,0,0),(1,0,1)\}$	$\not\subseteq K$
	$(0,0,1)$	$\{(0,0,1),(0,0,0)\}$	$\subseteq K$

The Kakeya problem in finite vector spaces

Examples:

- trivial: $K = \mathbb{F}_q^n \quad \Rightarrow \quad |K| \leq q^n$

- $K = \{(0,0,0),(0,0,1),(0,1,1),(1,0,1),(1,1,1)\} \subset \mathbb{F}_2^3$

$\mathbf{x}$	$\mathbf{y}$	$\{\mathbf{y} + t\mathbf{x} : t \in \mathbb{F}_2\}$
$(0,0,1)$	$(1,0,0)$	$\{(1,0,0),(1,0,1)\} \not\subseteq K$
	$(0,0,1)$	$\{(0,0,1),(0,0,0)\} \subseteq K$
$(0,1,0)$	$(1,1,1)$	$\{(1,1,1),(1,0,1)\} \subseteq K$

The Kakeya problem in finite vector spaces

Examples:

- trivial: $K = \mathbb{F}_q^n \quad \Rightarrow \quad |K| \leq q^n$
- $K = \{(0,0,0),(0,0,1),(0,1,1),(1,0,1),(1,1,1)\} \subset \mathbb{F}_2^3$

$\mathbf{x}$	$\mathbf{y}$	$\{\mathbf{y} + t\mathbf{x} : t \in \mathbb{F}_2\}$	
$(0,0,1)$	$(1,0,0)$	$\{(1,0,0),(1,0,1)\}$	$\not\subseteq K$
	$(0,0,1)$	$\{(0,0,1),(0,0,0)\}$	$\subseteq K$
$(0,1,0)$	$(1,1,1)$	$\{(1,1,1),(1,0,1)\}$	$\subseteq K$
$\vdots$			
$\vdots$			

The Kakeya problem in finite vector spaces

Conjecture [Wolff, 1999]

$|K| \geq C_n \cdot q^n$, where C_n depends only on n.

The Kakeya problem in finite vector spaces

Conjecture [Wolff, 1999]

$|K| \geq C_n \cdot q^n$, where C_n depends only on n.

"This conjecture has had a significant influence in the subject, in particular inspiring work on the sum-product phenomenon in finite fields, which has since proven to have many applications in number theory and computer science."

– Terence Tao, 24 March, 2008

The Kakeya problem in finite vector spaces

Conjecture [Wolff, 1999]

$|K| \geq C_n \cdot q^n$, where C_n depends only on n.

$|K| \geq (1/n!) \cdot q^n$ [Dvir, 2009]

The Kakeya problem in finite vector spaces

Conjecture [Wolff, 1999]

$|K| \geq C_n \cdot q^n$, where C_n depends only on n.

$|K| \geq (1/n!) \cdot q^n$ [Dvir, 2009]

$|K| \geq (1/2^n) \cdot q^n$ [Dvir, Kopparty, Saraf & Sudan, 2009]

The upper bound

$$|K| \geq (1/2^n) \cdot q^n$$

[Dvir, Kopparty, Saraf & Sudan, 2009]

$$|K| \leq 2 \cdot (1/2^n) \cdot q^n + O(q^{n-1})$$

The upper bound

$$|K| \geq (1/2^n) \cdot q^n$$

[Dvir, Kopparty, Saraf & Sudan, 2009]

$$|K| \leq 2 \cdot (1/2^n) \cdot q^n + O(q^{n-1})$$

two regimes:

- n is fixed, q grows

  $$|K| \leq 2 \cdot (1/2^n) \cdot q^n + O(q^{n-1})$$

The upper bound

$$|K| \geq (1/2^n) \cdot q^n$$

[Dvir, Kopparty, Saraf & Sudan, 2009]

$$|K| \leq 2 \cdot (1/2^n) \cdot q^n + O(q^{n-1})$$

two regimes:

- n is fixed, q grows

  $$|K| \leq 2 \cdot (1/2^n) \cdot q^n + O(q^{n-1})$$

The upper bound

$$|K| \geq (1/2^n) \cdot q^n$$

[Dvir, Kopparty, Saraf & Sudan, 2009]

$$|K| \leq 2 \cdot (1/2^n) \cdot q^n + O(q^{n-1})$$

two regimes:

- n is fixed, q grows

  $$|K| \leq 2 \cdot (1/2^n) \cdot q^n + O(q^{n-1})$$

- q is fixed, n grows

  $$|K| \leq 2 \cdot (1/2^n) \cdot q^n + O(q^{n-1})$$

The upper bound

$$|K| \geq (1/2^n) \cdot q^n$$

[Dvir, Kopparty, Saraf & Sudan, 2009]

$$|K| \leq 2 \cdot (1/2^n) \cdot q^n + O(q^{n-1})$$

two regimes:

- n is fixed, q grows

  $$|K| \leq 2 \cdot (1/2^n) \cdot q^n + O(q^{n-1})$$

- q is fixed, n grows

  $$|K| \leq 2 \cdot (1/2^n) \cdot q^n + O(q^{n-1})$$

The upper bound: q fixed, n grows

[Kopparty, Lev, Saraf & Sudan, 2011]

There exists a Kakeya set $K \subset \mathbb{F}_q^n$ bounded by

q odd	$C_q \cdot \left(\frac{q+1}{2}\right)^n$
$q = 2^m$ m even	$C_q \cdot \left(\frac{2q+1}{3}\right)^n$
$q = 2^m$ m odd	$\frac{3}{2} \cdot \left(\frac{2(q+\sqrt{q}+1)}{3}\right)^n$

The upper bound: q fixed, n grows

[Kopparty, Lev, Saraf & Sudan, 2011]

There exists a Kakeya set $K \subset \mathbb{F}_q^n$ bounded by

	known	Our bounds
q odd	$C_q \cdot \left(\frac{q+1}{2}\right)^n$	
$q = 2^m$, m even	$C_q \cdot \left(\frac{2q+1}{3}\right)^n$	$C_q \cdot \left(\frac{q+\sqrt{q}}{2}\right)^n$
$q = 2^m$, m odd	$\frac{3}{2} \cdot \left(\frac{2(q+\sqrt{q}+1)}{3}\right)^n$	$C_q \cdot \left(\frac{5q+2\sqrt{q}+5}{8}\right)^n$

Proof idea

[Saraf & Sudan, 2008]

For a function $f : \mathbb{F}_q \to \mathbb{F}_q$, define

$$I_f(t) := \{f(x) + tx : x \in \mathbb{F}_q\}, \ t \in \mathbb{F}_q.$$

Proof idea

[Saraf & Sudan, 2008]

For a function $f : \mathbb{F}_q \to \mathbb{F}_q$, define

$$I_f(t) := \{f(x) + tx : x \in \mathbb{F}_q\},\ t \in \mathbb{F}_q.$$

Construct

$$K := \{(x_1, \ldots, x_j, t, 0, \ldots, 0) : 0 \le j \le n-1, t \in \mathbb{F}_q, x_1, \ldots, x_j \in I_f(t)\}$$

If $f(x) \neq ax$, then K is a Kakeya set of cardinality

$$|K| = \sum_{j=0}^{n-1} \sum_{t \in \mathbb{F}_q} |I_f(t)|^j = \sum_{t \in \mathbb{F}_q} \frac{|I_f(t)|^n - 1}{|I_f(t)| - 1}$$

Proof idea

$$I_f(t) := \{f(x) + tx : x \in \mathbb{F}_q\}, \; t \in \mathbb{F}_q.$$

$$|K| = \sum_{t \in \mathbb{F}_q} \frac{|I_f(t)|^n - 1}{|I_f(t)| - 1}$$

$$\Downarrow$$

$$|K| < C_q \cdot (\max_{t \in \mathbb{F}_q} |I_f(t)|)^n$$

Proof idea

$$I_f(t) := \{f(x) + tx : x \in \mathbb{F}_q\},\ t \in \mathbb{F}_q.$$

$$|K| = \sum_{t \in \mathbb{F}_q} \frac{|I_f(t)|^n - 1}{|I_f(t)| - 1}$$

$$\Downarrow$$

$$|K| < C_q \cdot (\max_{t \in \mathbb{F}_q} |I_f(t)|)^n$$

Goal: Find a function $f : \mathbb{F}_q \to \mathbb{F}_q$, s.t.

$$\max_{t \in \mathbb{F}_q} |I_f(t)| \text{ as small as possible}$$

Choose such a function f

Goal: Find a function $f : \mathbb{F}_q \to \mathbb{F}_q$, s.t.

$$\max_{t \in \mathbb{F}_q} \left|\{f(x) + tx : x \in \mathbb{F}_q\}\right| \text{ as small as possible}$$

- To estimate $|I_f(t)| = \left|\{f(x) + tx : x \in \mathbb{F}_q\}\right|$.

Choose such a function f

Goal: Find a function $f : \mathbb{F}_q \to \mathbb{F}_q$, s.t.

$$\max_{t \in \mathbb{F}_q} \left| \{ f(x) + tx : x \in \mathbb{F}_q \} \right| \quad \text{as small as possible}$$

- To estimate $|I_f(t)| = \left| \{ f(x) + tx : x \in \mathbb{F}_q \} \right|$.
- For all f, there always exists a $t \in \mathbb{F}_q$, s.t.

$$|I_f(t)| > q/2$$

[Kopparty, Lev, Saraf & Sudan, 2011]

Previous choices

$$|K| < C_q \cdot \left(\max_{t \in \mathbb{F}_q} |I_f(t)|\right)^n$$

[Kopparty, Lev, Saraf & Sudan, 2011]

- q odd, $f(x) = x^2 \quad \Rightarrow \quad |I_f(t)| = \frac{q+1}{2}$ for each $t \in \mathbb{F}_q$

cannot do better!

Previous choices

$$|K| < C_q \cdot \left(\max_{t\in\mathbb{F}_q} |I_f(t)|\right)^n$$

[Kopparty, Lev, Saraf & Sudan, 2011]

- q odd, $f(x) = x^2 \quad \Rightarrow \; |I_f(t)| = \frac{q+1}{2}$ for each $t \in \mathbb{F}_q$

  cannot do better!

- q even power of 2, $f(x) = x^3$

  $\Rightarrow \; |K| \leq C_q \cdot \left(\frac{2q+1}{3}\right)^n$

Previous choices

$$|K| < C_q \cdot \left(\max_{t\in\mathbb{F}_q} |I_f(t)|\right)^n$$

[Kopparty, Lev, Saraf & Sudan, 2011]

- q odd, $f(x) = x^2 \quad \Rightarrow \quad |I_f(t)| = \frac{q+1}{2}$ for each $t \in \mathbb{F}_q$

  cannot do better!

- q even power of 2, $f(x) = x^3$

  $\Rightarrow \; |K| \leq C_q \cdot \left(\frac{2q+1}{3}\right)^n$

- q odd power of 2, $f(x) = x^{q-2} + x^2$

  $\Rightarrow \; |K| \leq \frac{3}{2} \cdot \left(\frac{2(q+\sqrt{q}+1)}{3}\right)^n$

Previous choices

$$|K| < C_q \cdot (\max_{t\in\mathbb{F}_q} |I_f(t)|)^n$$

[Kopparty, Lev, Saraf & Sudan, 2011]

- q odd, $f(x) = x^2 \quad \Rightarrow \; |I_f(t)| = \frac{q+1}{2}$ for each $t \in \mathbb{F}_q$

  cannot do better!

- q even power of 2, $f(x) = x^3$

  $\Rightarrow \; |K| \leq C_q \cdot \left(\frac{2q+1}{3}\right)^n$

- q odd power of 2, $f(x) = x^{q-2} + x^2$

  $\Rightarrow \; |K| \leq \frac{3}{2} \cdot \left(\frac{2(q+\sqrt{q}+1)}{3}\right)^n$

NEW bound I: $q = 2^m$, m even

Choose $f(x) = x^{2^i+1}$ $\qquad 0 \leq i \leq m-1$

NEW bound I: $q = 2^m$, m even

Choose $f(x) = x^{2^i+1}$ $\qquad 0 \leq i \leq m-1$

- We explicitly determine $|I_f(t)|$ for each $t \in \mathbb{F}_q$

  Using the results in [A. Bluher, On $x^{q+1} + ax + b$, FFTA, 2004].

NEW bound I: $q = 2^m$, m even

Choose $f(x) = x^{2^i+1}$ $\quad 0 \leq i \leq m-1$

- We explicitly determine $|I_f(t)|$ for each $t \in \mathbb{F}_q$

  Using the results in [A. Bluher, On $x^{q+1} + ax + b$, FFTA, 2004].

- Choose $f(x) = x^{2^{m/2}+1}$

$$|I_f(t)| \leq \frac{q + \sqrt{q}}{2}$$

NEW bound I: $q = 2^m$, m even

Choose $f(x) = x^{2^i+1}$ $\quad 0 \leq i \leq m-1$

- We explicitly determine $|I_f(t)|$ for each $t \in \mathbb{F}_q$

  Using the results in [A. Bluher, On $x^{q+1} + ax + b$, FFTA, 2004].

- Choose $f(x) = x^{2^{m/2}+1}$

$$|I_f(t)| \leq \frac{q+\sqrt{q}}{2} \qquad \Rightarrow \qquad |K| < C_q \cdot \left(\frac{q+\sqrt{q}}{2}\right)^n$$

NEW bound I: $q = 2^m$, m even

Choose $f(x) = x^{2^i+1}$ $\quad 0 \le i \le m-1$

- We explicitly determine $|I_f(t)|$ for each $t \in \mathbb{F}_q$

  Using the results in [A. Bluher, On $x^{q+1} + ax + b$, FFTA, 2004].

- Choose $f(x) = x^{2^{m/2}+1}$

$$|I_f(t)| \le \frac{q+\sqrt{q}}{2} \qquad \Rightarrow \qquad |K| < C_q \cdot \left(\frac{q+\sqrt{q}}{2}\right)^n$$

recall: $|K| < C_q \cdot \left(\frac{2q+1}{3}\right)^n$

[Kopparty, Lev, Saraf & Sudan, 2011]

NEW bound II: $q = 2^m$, m odd

Choose $f(x) = x^4 + x^3$

$$|I_f(t)| \leq \frac{5q + 2\sqrt{q} + 5}{8}$$

NEW bound II: $q = 2^m$, m odd

Choose $f(x) = x^4 + x^3$

$$|I_f(t)| \leq \frac{5q + 2\sqrt{q} + 5}{8} \;\Rightarrow\; |K| < C_q \cdot \left(\frac{5q+2\sqrt{q}+5}{8}\right)^n$$

NEW bound II: $q = 2^m$, m odd

Choose $f(x) = x^4 + x^3$

$$|I_f(t)| \leq \frac{5q + 2\sqrt{q} + 5}{8} \quad \Rightarrow \quad |K| < C_q \cdot \left(\frac{5q+2\sqrt{q}+5}{8}\right)^n$$

recall: $|K| \leq \frac{3}{2} \cdot \left(\frac{2(q+\sqrt{q}+1)}{3}\right)^n$

NEW bound II: $q = 2^m$, m odd

Choose $f(x) = x^4 + x^3$

$$|I_f(t)| \leq \frac{5q + 2\sqrt{q} + 5}{8} \quad \Rightarrow \quad |K| < C_q \cdot \left(\frac{5q+2\sqrt{q}+5}{8}\right)^n$$

recall: $|K| \leq \frac{3}{2} \cdot \left(\frac{2(q+\sqrt{q}+1)}{3}\right)^n$

- Remark

  $f(x)$ is of the form Gold APN power$+x^{2^i}$.

Conclusions and Problems

- For $q = 2^m$, we gave the BEST known upper bounds for Kakeya sets in $\mathbb{F}_q^n$.

Conclusions and Problems

- For $q = 2^m$, we gave the BEST known upper bounds for Kakeya sets in $\mathbb{F}_q^n$.

- For m odd, up to $m = 13$, we made the BEST choice among functions of the form APN power$+x^{2^i}$.

Conclusions and Problems

- For $q = 2^m$, we gave the BEST known upper bounds for Kakeya sets in $\mathbb{F}_q^n$.

- For m odd, up to $m = 13$, we made the BEST choice among functions of the form APN power$+x^{2^i}$.

- For m odd, is there a function $f : \mathbb{F}_q \to \mathbb{F}_q$, s.t.

$$\max_{t \in \mathbb{F}_q} \left| \{ f(x) + tx : x \in \mathbb{F}_q \} \right| < (1/2 + o(1))q \text{ ?}$$

Conclusions and Problems

- For $q = 2^m$, we gave the BEST known upper bounds for Kakeya sets in $\mathbb{F}_q^n$.

- For m odd, up to $m = 13$, we made the BEST choice among functions of the form APN power$+x^{2^i}$.

- For m odd, is there a function $f : \mathbb{F}_q \to \mathbb{F}_q$, s.t.

$$\max_{t \in \mathbb{F}_q} \left| \{ f(x) + tx : x \in \mathbb{F}_q \} \right| < (1/2 + o(1))q \ ?$$

known: $(5/8 + o(1))q$

References

- S. Kakeya, Some problems on maximum and minimum regarding ovals, *Tohoku Science Reports* , 6 (1917) 71–88.
- A. Besicovitch, On Kakeya's problem and a similar one, *Mathematische Zeitschrift*, 27 (1928) 312–320.
- T. Wolff, Recent work connected with the Kakeya problem, *Prospects in Mathematics, AMS*, (1999) 129–162.
- S. Saraf and M. Sudan, An improved lower bound on the size of Kakeya sets over finite fields, *Anal. PDE*, (1) (2008), 375 –379.
- Z. Dvir, On the size of Kakeya sets in finite fields, *J. Amer. Math. Soc.*, 22 (4) (2009) 1093–1097.
- A. Bluher, On $x^{q+1} + ax + b$, *Finite Fields and Their Applications*, 10 (2004) 285-305.

References

- S. Kopparty, V.F. Lev, S. Saraf, M. Sudan, Kakeya-type sets in finite vector spaces, *J. Algebraic Combin.*, (34) (2011), 337 –355.
- Z. Dvir, S. Kopparty, S. Saraf and M. Sudan, Extensions to the method of multiplicities with applications to Kakeya sets and mergers, *Proc. of 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009)*, (2009) 181–190.