Special Monomial Maps:
Examples, Classification, Open Problems

Gohar Kyureghyan
Otto-von-Guericke University of Magdeburg, Germany

Fq12 - Saratoga
July 14, 2015

Outline

- Special maps yielding small Kakeya sets
- Non-linear monomial maps

Kakeya Sets

A subset $\mathcal{K}$ of $\mathbb{F}_q^n$ is called a Kakeya set if it contains a line in every direction.

Let $\alpha \in \mathbb{F}_q^n$, $\alpha \neq 0$. Then a line in direction α is just

$$\{\alpha \cdot t + \beta \,|\, t \in \mathbb{F}_q\},$$

where $\beta \in \mathbb{F}_q^n$ is arbitrary.

Goal: Constructions for small Kakeya sets.

Kakeya Sets

A subset $\mathcal{K} \subseteq \mathbb{F}_{\boldsymbol{q}}^{\boldsymbol{n}}$ is a Kakeya set if for every non-zero $\alpha \in \mathbb{F}_{\boldsymbol{q}}^{\boldsymbol{n}}$ there is a $\beta_\alpha \in \mathbb{F}_{\boldsymbol{q}}^{\boldsymbol{n}}$ such that the line

$$\{\alpha \cdot t + \beta_\alpha \,|\, t \in \mathbb{F}_{\boldsymbol{q}}\}$$

is contained in $\mathcal{K}$.

Suppose we know the map $\alpha \mapsto \beta_\alpha$, then the set

$$\bigcup_{\alpha} \{\alpha \cdot t + \beta_\alpha \,|\, t \in \mathbb{F}_{\boldsymbol{q}}\}$$

is a Kakeya set.

Hence, constructing a small Kakeya set is equivalent to finding a map $\alpha \mapsto \beta_\alpha$ such that the above union is small.

Kakeya Sets: A Construction

Problem: Find a map $\alpha \mapsto \beta_\alpha$ such that the union

$$\bigcup_\alpha \{\alpha \cdot t + \beta_\alpha \,|\, t \in \mathbb{F}_{\boldsymbol{q}}\}$$

is small.

Construction: [Kopparty-Lev-Saraf-Sudan (2011)]:

Let w.l.g. $\alpha = (a_1, a_2, \ldots, a_{j-1}, 1, 0, \ldots, 0)$ for some $1 \leq j \leq n$ and take

$$\beta_\alpha := (f(a_1),\, f(a_2), \ldots, f(a_{j-1}), 0, 0, \ldots, 0)$$

for some fixed map $f : \mathbb{F}_{\boldsymbol{q}} \to \mathbb{F}_{\boldsymbol{q}}$.

Kakeya Sets: A Construction

Then the line defined by $\alpha = (a_1, a_2, \ldots, a_{j-1}, 1, 0, \ldots, 0)$ is

$$\mathcal{L}_\alpha := \{(a_1 \cdot t + f(a_1),\ \ldots,\ a_{j-1} \cdot t + f(a_{j-1}),\ t,\ 0, \ldots, 0) \mid t \in \mathbb{F}_{\boldsymbol{q}}\}$$

and the corresponding Kakeya set is

$$\mathcal{K} = \bigcup_\alpha \mathcal{L}_\alpha.$$

Note that

$$\mathcal{K} = \{(y_1, \ldots, y_{j-1}, t, 0, \ldots, 0) \mid 1 \leq j \leq n,\ t \in \mathbb{F}_{\boldsymbol{q}},\ y_i \in Im_f(t)\},$$

with

$$Im_f(t) := \{f(x) + t \cdot x \mid x \in \mathbb{F}_{\boldsymbol{q}}\}.$$

Hence, to minimize $|\mathcal{K}|$ we need to find a map $f : \mathbb{F}_{\boldsymbol{q}} \to \mathbb{F}_{\boldsymbol{q}}$ with $|Im_f(t)|$ small for all $t \in \mathbb{F}_{\boldsymbol{q}}$.

Searching for good maps $f : \mathbb{F}_q \to \mathbb{F}_q$?

Result [Kopparty-Lev-Saraf-Sudan (2011)]:

(a) For every q and $f : \mathbb{F}_q \to \mathbb{F}_q$, there is an element $t \in \mathbb{F}_q$ with

$$|Im_f(t)| = |\{f(x) + t \cdot x \mid x \in \mathbb{F}_q\}| > \frac{q}{2}.$$

(b) If q is odd, then the map $s : \mathbb{F}_q \to \mathbb{F}_q$ with $x \mapsto x^2$ satisfies

$$|Im_s(t)| = |\{x^2 + t \cdot x \mid x \in \mathbb{F}_q\}| = \frac{q+1}{2}.$$

Hence s defines an (asymptotically) optimal Kakeya set (when the presented construction is used).

Searching for good maps for even q

Which maps $f : \mathbb{F}_q \to \mathbb{F}_q$ are optimal when q is even ? (Open)

It is worth to try to understand at first monomial maps $f(x) = x^k$, since

- a best solution for q odd is a monomial map; and

- they are easier to handle: Not all t must be checked: If there is $a \in \mathbb{F}_q$, such that $t = a^{k-1}$, then

$$x^k + tx = a^k \cdot \Big((x/a)^k + (x/a) \Big).$$

The best known maps for even q

Let $q = 2^m$. The best known choice for the map $f : \mathbb{F}_{\boldsymbol{q}} \to \mathbb{F}_{\boldsymbol{q}}$ is

- $f(x) = x^{2^{m/2}+1}$, when m is even
- $f(x) = x^4 + x^3$, when m is odd.

Open question: Let q be even. What is the best choice for f ?
What is the best choice for monomial f ?

A proof from the BOOK

Theorem: Let $q = 2^m$ with m even. Then

$$|\{x^{2^{m/2}+1} : x \in \mathbb{F}_{\boldsymbol{q}}\}| = 2^{m/2},$$

and for any non-zero $t \in \mathbb{F}_{\boldsymbol{q}}$

$$|\{x^{2^{m/2}+1} + tx : x \in \mathbb{F}_{\boldsymbol{q}}\}| = \frac{2^m + 2^{m/2}}{2}.$$

Proof [Peter Müller]: It is enough to compute the size of the image set of

$$g(x) := x^{2^{m/2}+1} + x,$$

that is to consider only $t = 1$.

A proof from the BOOK

The goal is to compute the image set of $g(x) := x^{2^{m/2}+1} + x$.

Note, if $y, z \in \mathbb{F}_{\boldsymbol{q}}$ are such that

$$g(z) = z^{2^{m/2}+1} + z = y^{2^{m/2}+1} + y = g(y),$$

then $z = y + u$ for some $u \in \mathbb{F}_{2^{m/2}}$.

So, let $u \in \mathbb{F}_{2^{m/2}}$. Then

$$\begin{aligned} g(y+u) &= y^{2^{m/2}+1} + y + u(y^{2^{m/2}} + y) + u^2 + u \\ &= g(y) + u(y^{2^{m/2}} + y) + u^2 + u \\ &= g(y) + u(Tr(y) + u + 1). \end{aligned}$$

Thus y and $y + u$, $u \neq 0$, have the same image if and only if

$$u = Tr(y) + 1.$$

The implied bounds for Kakeya sets

Theorem[Kopparty-Lev-Saraf-Sudan (2011); K.-Müller-Wang (2014)]:

Let $n \geq 1$. There is a Kakeya set $\mathcal{K} \subset \mathbb{F}_{\boldsymbol{q}}^{\boldsymbol{n}}$ such that

$$|K| < \begin{cases} 2\left(1 + \frac{1}{q-1}\right)\left(\frac{q+1}{2}\right)^n & \text{if } q \text{ is odd,} \\ \frac{2q}{q+\sqrt{q}-2}\left(\frac{q+\sqrt{q}}{2}\right)^n & \text{if } q \text{ is an even power of 2,} \\ \frac{8q}{5q+2\sqrt{q}-3}\left(\frac{5q+2\sqrt{q}+5}{8}\right)^n & \text{if } q \text{ is an odd power of 2.} \end{cases}$$

Non-linear maps

There are several criteria which measure (non-)linearity of a map:

(1) Algebraic degree: a linear map has algebraic degree 1

(2) Differential properties: Given a linear map L, for any fixed non-zero a the set $\{L(x+a)-L(x)\,|\,x \in \mathbb{F}_{\boldsymbol{q}}\}$ contains only one element, namely $L(a)$.

(3) Linear approximation: a non-linear map does not allow a good affine approximation.

APN maps

A map $\boldsymbol{f} : \mathbb{F}_{\mathbf{2}^{\boldsymbol{n}}} \to \mathbb{F}_{\mathbf{2}^{\boldsymbol{n}}}$ is called almost perfect nonlinear (APN), if for every fixed non-zero $\boldsymbol{a} \in \mathbb{F}_{\mathbf{2}^{\boldsymbol{n}}}$

$$|\{\boldsymbol{f}(\boldsymbol{x}+\boldsymbol{a})+\boldsymbol{f}(\boldsymbol{x}) : \boldsymbol{x} \in \mathbb{F}_{\mathbf{2}^{\boldsymbol{n}}}\}| = \mathbf{2}^{\boldsymbol{n}-\mathbf{1}}.$$

Applications

- Cryptology: The best resistance against differential attacks
- Coding theory: $[2^n - 1, 2^n - 2n - 1, 5]$-codes
- Finite geometry: Constructions of dimensional dual hyperovals

APN exponents on $\mathbb{F}_{2^n}$

An integer $1 \le d \le 2^n - 2$ is called an APN exponent on $\mathbb{F}_{2^n}$ if the corresponding map $x \mapsto x^d$ is APN on $\mathbb{F}_{2^n}$.

An APN exponent d is called exceptional, if it defines APN maps for infinitely many n.

Some questions on the classification of APN exponents:

- Characterize all APN exponents. (Open)
- Characterize all exceptional APN exponents. (Solved)
- What are the possible binary weights of APN exponents d (or equivalently, algebraic degree of x^d) on $\mathbb{F}_{2^n}$? (Open)

APN exponents on $\mathbb{F}_{2^n}$

(All known) APN exponents on $\mathbb{F}_{2^n}$:

- $2^k + 1$ with $\gcd(k, n) = 1$ (Gold's exponent)
- $2^{2k} - 2^k + 1$ with $\gcd(k, n) = 1$ (Kasami's exponent)
- $2^{4m} + 2^{3m} + 2^{2m} + 2^m - 1$ for $n = 5m$ (Dobbertin's exponent)
- $2^m + 3$ for $n = 2m + 1$ (Welch's exponent)
- $2^m + 2^{\frac{m}{2}} - 1$ for $n = 2m + 1$ with m even, and $2^m + 2^{\frac{3m+1}{2}} - 1$ for $n = 2m + 1$ with m odd (Niho's exponents)
- $2^n - 2$ for n odd (field inverse).

Only Gold and Kasami APN exponents are exceptional. [Hernando-McGuire(2011)]

APN exponents on $\mathbb{F}_{2^n}$

There are more APN exponents known.

Fact: If d is an APN exponent on $\mathbb{F}_{2^n}$, then:

$2 \cdot d \mod 2^n - 1$ is an APN exponent on $\mathbb{F}_{2^n}$ too;

and also its inverse d^{-1} modulo $2^n - 1$ is an APN exponent on $\mathbb{F}_{2^n}$, when n is odd.

Can we find the inverses of the APN exponents explicitly?

- Yes, if d depends on n;
- (probably) No, if d is exceptional.

Inverses of APN exponents

The inverses of all known APN exponents depending on n are explicitly known:

- field inverse (trivial)
- Niho's exponents (Portmann and Rennhard 1997)
- Welch's and Dobbertin's exponents (K. and Suder 2014)

Only partial results for Gold and Kasami exponents.

Inverse of Dobbertin's exponent

Theorem [K.-Suder (2014)] Let m be odd. Then the least positive residue of the inverse of Dobbertin's exponent $d = 2^{4m} + 2^{3m} + 2^{2m} + 2^m - 1$ modulo $2^{5m} - 1$ is

$$\frac{1}{2}\left(\frac{2^{5m}-1}{2^m-1}\cdot\frac{2^{m+1}-1}{3}-1\right)$$

and its binary weight is $\frac{5m+3}{2}$.

Remark:

- The key step in proving such results is to guess the formula.
- The inverse of Dobbertin's exponent shows existence of APN maps of algebraic degree $\frac{n+1}{2}+1$ on $\mathbb{F}_{2^n}$ when $n = 5m$ is odd.

Crooked maps

An APN map $\boldsymbol{f} : \mathbb{F}_{\mathbf{2}^{\boldsymbol{n}}} \to \mathbb{F}_{\mathbf{2}^{\boldsymbol{n}}}$ is called crooked, if for every fixed non-zero $\boldsymbol{a} \in \mathbb{F}_{\mathbf{2}^{\boldsymbol{n}}}$

$$\{f(x+a) + f(x) : x \in \mathbb{F}_{\mathbf{2}^{\boldsymbol{n}}}\}$$

is an affine hyperplane.

Fact: An exponent d is crooked if and only if it is a Gold APN exponent, that is $d = 2^i + 2^j$. [K.2007]

Conjecture: Every crooked map must be of shape

$$\sum_{\boldsymbol{i},\boldsymbol{j}} \boldsymbol{a}_{\boldsymbol{i},\boldsymbol{j}}\, \boldsymbol{x}^{\mathbf{2}^{\boldsymbol{i}}+\mathbf{2}^{\boldsymbol{j}}}.$$

However the Coulter-Matthews planar exponents do exist!

Planar maps

If $q = p^n$ odd, a map $\boldsymbol{f} : \mathbb{F}_{\boldsymbol{q}} \to \mathbb{F}_{\boldsymbol{q}}$ is called planar, if for every fixed non-zero $a \in \mathbb{F}_{\boldsymbol{q}}$

$$\{f(x+a) - f(x) : x \in \mathbb{F}_{\boldsymbol{q}}\} = \mathbb{F}_{\boldsymbol{q}}.$$

Easy examples: $\boldsymbol{x^2, x^{p^i+1}}$

Conjecture: [Dembowski and Ostrom (1967)]: Every planar map is given by

$$\sum_{\boldsymbol{i,j}} \boldsymbol{a_{i,j}\, x^{p^i+p^j}},$$

Counterexample [Coulter and Matthews (1996)]: The monomial

$$\boldsymbol{x^{\frac{3^k+1}{2}}}$$

defines a planar map on $\mathbb{F}_{3^n}$ iff k is odd and $\gcd(k, n) = 1$.

THANK YOU