The functional graph of some family of functions over finite fields

Fabio Enrique Brochero Martínez
joint work with Hugo Rodrigues Teixeira

Universidade Federal de Minas Gerais

Carleton Finite Fields eSeminar

Notation

- $\mathbb{F}_q$ denote a finite field with $q := p^s$ elements, where p is an odd prime.

Notation

- $\mathbb{F}_q$ denote a finite field with $q := p^s$ elements, where p is an odd prime.
- For each function $f : \mathbb{F}_q \to \mathbb{F}_q$, we define the functional graph of f as the directed graph $G_f = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \mathbb{F}_q$ and $\mathcal{E} = \{(x, f(x)) \mid x \in \mathbb{F}_q\}$.

Notation

- $\mathbb{F}_q$ denote a finite field with $q := p^s$ elements, where p is an odd prime.
- For each function $f : \mathbb{F}_q \to \mathbb{F}_q$, we define the functional graph of f as the directed graph $G_f = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \mathbb{F}_q$ and $\mathcal{E} = \{(x, f(x)) \mid x \in \mathbb{F}_q\}$.
- For $a \in \mathbb{F}_q$, there are integers $0 \le i < j$, minimal, such that $f^{(i)}(a) = f^{(j)}(a)$. We call the list

$$a, f(a), x^{(2)}(a), \cdots, f^{(i-1)}(a)$$

the pre-cycle and

$$f^{(i)}(a), f^{(i+1)}(a), \cdots, f^{(j-1)}(a)$$

the cycle of length $(j - i)$.

Notation

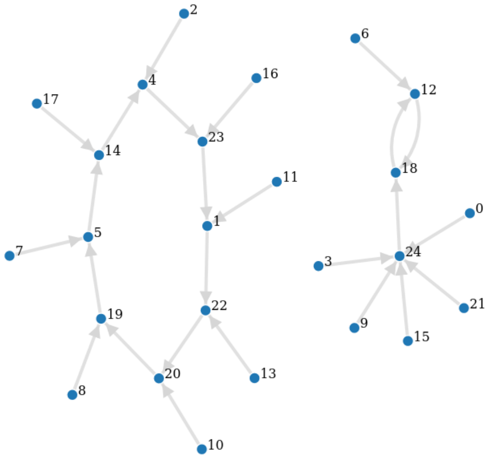
- $\mathbb{F}_q$ denote a finite field with $q := p^s$ elements, where p is an odd prime.
- For each function $f : \mathbb{F}_q \to \mathbb{F}_q$, we define the functional graph of f as the directed graph $G_f = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \mathbb{F}_q$ and $\mathcal{E} = \{(x, f(x)) \mid x \in \mathbb{F}_q\}$.
- For $a \in \mathbb{F}_q$, there are integers $0 \le i < j$, minimal, such that $f^{(i)}(a) = f^{(j)}(a)$. We call the list
$$a, f(a), x^{(2)}(a), \cdots, f^{(i-1)}(a)$$
the pre-cycle and
$$f^{(i)}(a), f^{(i+1)}(a), \cdots, f^{(j-1)}(a)$$
the cycle of length $(j - i)$.
- If $i = 0$ we say that a is a period point of f.

Notation

- $\mathbb{F}_q$ denote a finite field with $q := p^s$ elements, where p is an odd prime.
- For each function $f : \mathbb{F}_q \to \mathbb{F}_q$, we define the functional graph of f as the directed graph $G_f = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \mathbb{F}_q$ and $\mathcal{E} = \{(x, f(x)) \mid x \in \mathbb{F}_q\}$.
- For $a \in \mathbb{F}_q$, there are integers $0 \le i < j$, minimal, such that $f^{(i)}(a) = f^{(j)}(a)$. We call the list
$$a, f(a), x^{(2)}(a), \cdots, f^{(i-1)}(a)$$
the pre-cycle and
$$f^{(i)}(a), f^{(i+1)}(a), \cdots, f^{(j-1)}(a)$$
the cycle of length $(j - i)$.
- If $i = 0$ we say that a is a period point of f.
- If $f(a) = a$, we say it is a fixed point of f.

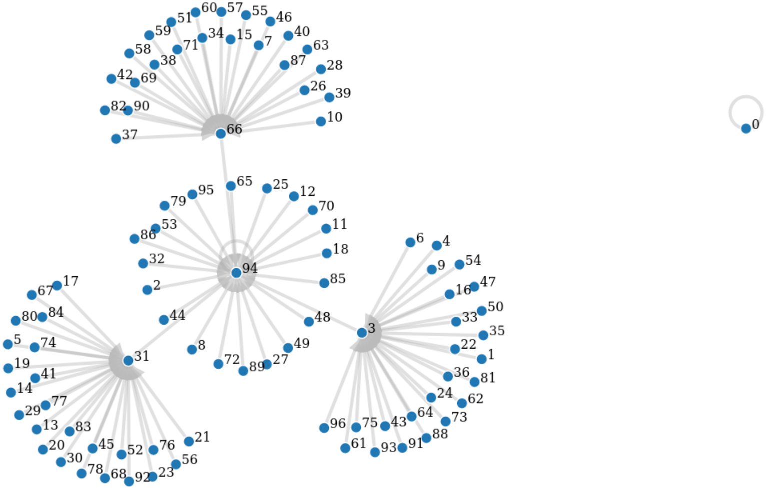
Example

If $f : \mathbb{F}_{25} \to \mathbb{F}_{25}$ is the function defined by $f(x) = x^6 + x^2 + 1$, then the functional graph of f is



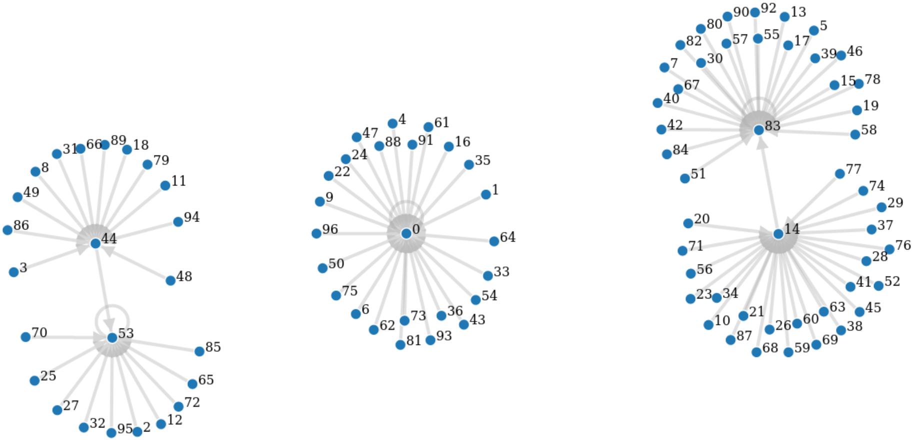
Example

If $f : \mathbb{F}_{97} \to \mathbb{F}_{97}$ is the function defined by $f(x) = 3x^{72}$, then the functional graph of f is



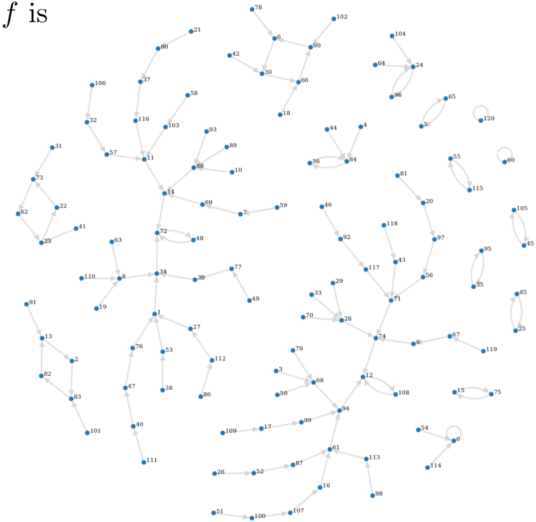
Example

If $f : \mathbb{F}_{97} \to \mathbb{F}_{97}$ is the function defined by $f(x) = x^{36} - x^{12}$, then the functional graph of f is



Example

If $f : \mathbb{F}_{121} \to \mathbb{F}_{121}$ is the function defined by $f(x) = x^{119} + x^{11} - x$, then the functional graph of f is



Some results about Functional Graph

- $f(x) = x^2$, Rogers (1996)

Some results about Functional Graph

- $f(x) = x^2$, Rogers (1996)
- $f(x) = x^e$, Chou & Shparlinski (2004)

Some results about Functional Graph

- $f(x) = x^2$, Rogers (1996)
- $f(x) = x^e$, Chou & Shparlinski (2004)
- $f(x) = x + x^{-1}$, where $char(\mathbb{F}_q) = 3$ or 5, Ugolini (2013)

Some results about Functional Graph

- $f(x) = x^2$, Rogers (1996)
- $f(x) = x^e$, Chou & Shparlinski (2004)
- $f(x) = x + x^{-1}$, where $char(\mathbb{F}_q) = 3$ or 5, Ugolini (2013)
- Redei Funciton, Qureshi & Panario (2015)

Some results about Functional Graph

- $f(x) = x^2$, Rogers (1996)
- $f(x) = x^e$, Chou & Shparlinski (2004)
- $f(x) = x + x^{-1}$, where $char(\mathbb{F}_q) = 3$ or 5, Ugolini (2013)
- Redei Funciton, Qureshi & Panario (2015)
- Elliptic curves, Ugolini (2018)

Some results about Functional Graph

- $f(x) = x^2$, Rogers (1996)
- $f(x) = x^e$, Chou & Shparlinski (2004)
- $f(x) = x + x^{-1}$, where $char(\mathbb{F}_q) = 3$ or 5, Ugolini (2013)
- Redei Funciton, Qureshi & Panario (2015)
- Elliptic curves, Ugolini (2018)
- Chebyshev Functions, Qureshi & Panario (2019)

Some results about Functional Graph

- $f(x) = x^2$, Rogers (1996)
- $f(x) = x^e$, Chou & Shparlinski (2004)
- $f(x) = x + x^{-1}$, where $char(\mathbb{F}_q) = 3$ or 5, Ugolini (2013)
- Redei Funciton, Qureshi & Panario (2015)
- Elliptic curves, Ugolini (2018)
- Chebyshev Functions, Qureshi & Panario (2019)
- Linearized Polynomials, Panario & Reis (2019)

Some results about Functional Graph

- $f(x) = x^2$, Rogers (1996)
- $f(x) = x^e$, Chou & Shparlinski (2004)
- $f(x) = x + x^{-1}$, where $char(\mathbb{F}_q) = 3$ or 5, Ugolini (2013)
- Redei Funciton, Qureshi & Panario (2015)
- Elliptic curves, Ugolini (2018)
- Chebyshev Functions, Qureshi & Panario (2019)
- Linearized Polynomials, Panario & Reis (2019)
- Survey about iteration mappings, Martins, Panario & Qureshi (2019)

Questions about functional graphs

Given a function $f : \mathbb{F}_q \to \mathbb{F}_q$, determine

- Fixed Point.

Questions about functional graphs

Given a function $f : \mathbb{F}_q \to \mathbb{F}_q$, determine

- Fixed Point.
- Number of cycles and lengths.

Questions about functional graphs

Given a function $f : \mathbb{F}_q \to \mathbb{F}_q$, determine

- Fixed Point.
- Number of cycles and lengths.
- Precycle lengths

Questions about functional graphs

Given a function $f : \mathbb{F}_q \to \mathbb{F}_q$, determine

- Fixed Point.
- Number of cycles and lengths.
- Precycle lengths
- Number of connected components

Classify the functions $f : \mathbb{F}_q \to \mathbb{F}_q$ such that

- They have the same functional graph.

Classify the functions $f : \mathbb{F}_q \to \mathbb{F}_q$ such that

- They have the same functional graph.
  In fact, $f, g : \mathbb{F}_q \to \mathbb{F}_q$ have the same functional graph if and only if there exists a permutation function $h : \mathbb{F}_q \to \mathbb{F}_q$ such that $f \circ h = h \circ g$.

Classify the functions $f : \mathbb{F}_q \to \mathbb{F}_q$ such that

- They have the same functional graph.
  In fact, $f, g : \mathbb{F}_q \to \mathbb{F}_q$ have the same functional graph if and only if there exists a permutation function $h : \mathbb{F}_q \to \mathbb{F}_q$ such that $f \circ h = h \circ g$.
- Any pre-periodic tree of the graph is the same.

Classify the functions $f : \mathbb{F}_q \to \mathbb{F}_q$ such that

- They have the same functional graph.
  In fact, $f, g : \mathbb{F}_q \to \mathbb{F}_q$ have the same functional graph if and only if there exists a permutation function $h : \mathbb{F}_q \to \mathbb{F}_q$ such that $f \circ h = h \circ g$.
- Any pre-periodic tree of the graph is the same.
  For example for any $n \in \mathbb{N}$, pre-periodic tree of a monomial function $f : \mathbb{F}_q^* \to \mathbb{F}_q^*$ defines as $x \mapsto x^n$ with root a periodic point is the same.

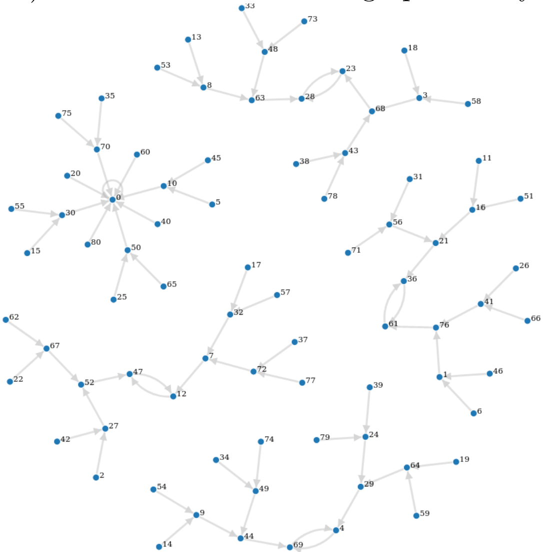
The functional graph of $a(x^{q+1} - x^2)$ over $\mathbb{F}_{q^2}$

Since $x \mapsto a(x^{q+1} - x^2)$ has the same functional graph for any $a \in \mathbb{F}_{q^2}^*$, we can suppose that $a = 1$.

The functional graph of $a(x^{q+1} - x^2)$ over $\mathbb{F}_{q^2}$

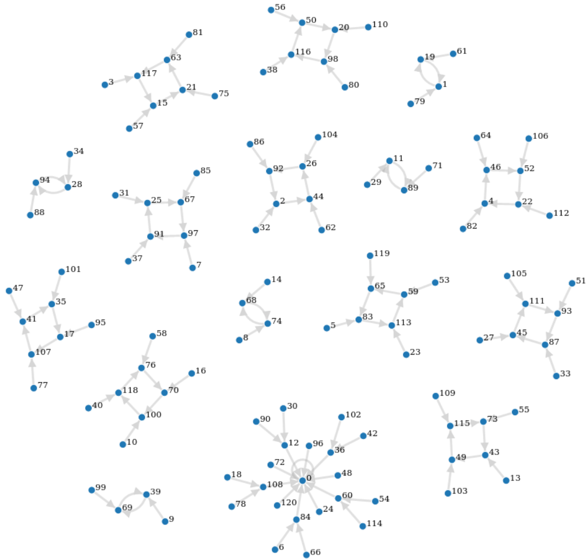
Since $x \mapsto a(x^{q+1} - x^2)$ has the same functional graph for any $a \in \mathbb{F}_{q^2}^*$, we can suppose that $a = 1$.

Case when $q = 9$



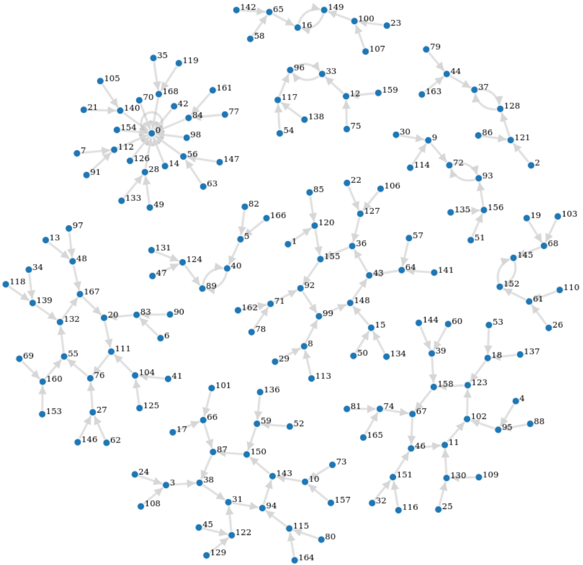
The functional graph of $x^{q+1} - x^2$ over $\mathbb{F}_{q^2}$

Case when $q = 11$



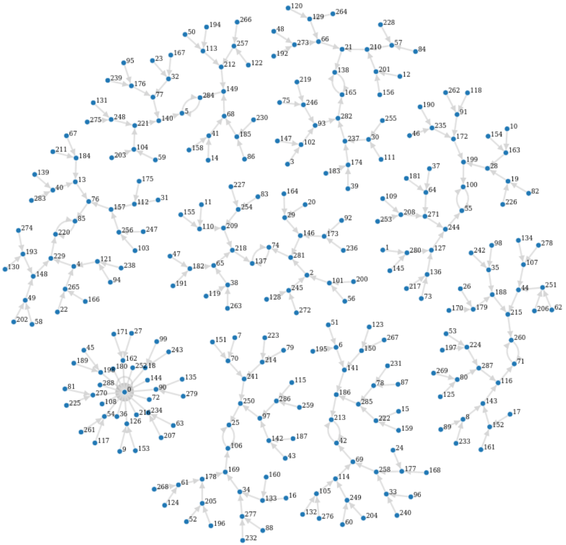
The functional graph of $x^{q+1} - x^2$ over $\mathbb{F}_{q^2}$

Case when $q = 13$



The functional graph of $x^{q+1} - x^2$ over $\mathbb{F}_{q^2}$

Case when $q = 17$



Connected component of Zero

Theorem

If $c \in \mathbb{F}_q$, then

1. $$\#f^{-1}(c) = \begin{cases} q, & \text{if } c = 0 \\ 2, & \text{if } \chi_2(-2c) = -1 \\ 0, & \text{if } \chi_2(-2c) = 1. \end{cases}$$
2. *If $a \in f^{-1}(c)$, then $f^{-1}(a) = \emptyset$.*

Connected component of Zero

Theorem

If $c \in \mathbb{F}_q$, then

1. $$\#f^{-1}(c) = \begin{cases} q, & \text{if } c = 0 \\ 2, & \text{if } \chi_2(-2c) = -1 \\ 0, & \text{if } \chi_2(-2c) = 1. \end{cases}$$
2. *If $a \in f^{-1}(c)$, then $f^{-1}(a) = \emptyset$.*

Theorem

If $c \in \mathbb{F}_q$, then

1. $$\#f^{-1}(c) = \begin{cases} q, & \text{if } c = 0 \\ 2, & \text{if } \chi_2(-2c) = -1 \\ 0, & \text{if } \chi_2(-2c) = 1. \end{cases}$$
2. *If $a \in f^{-1}(c)$, then $f^{-1}(a) = \emptyset$.*

In particular, the connected component of 0 has $2q-1$ elements of $\mathbb{F}_{q^2}$.

Periodic points

Theorem

The functional graph of $f(x) = x^{q+1} - x^2$ *over* $\mathbb{F}_{q^2}$ *has the following proprieties*

1. *The unique fixed point of the function is* $x = 0$.

Periodic points

Theorem

The functional graph of $f(x) = x^{q+1} - x^2$ over $\mathbb{F}_{q^2}$ has the following proprieties

1. *The unique fixed point of the function is $x = 0$.*
2. *Every cycle has even length.*

Theorem

The functional graph of $f(x) = x^{q+1} - x^2$ *over* $\mathbb{F}_{q^2}$ *has the following proprieties*

1. *The unique fixed point of the function is* $x = 0$.
2. *Every cycle has even length.*
3. *There are* $\dfrac{q-1}{2}$ *cycles of length two.*

Length of the cycles

Theorem

Let $q-1=2^k r$*, with* r *odd. Then for every* d *divisor of* r*, there are* $\dfrac{\varphi(d)(q-1)}{2\operatorname{ord}_{3d}(4)}$ *cycles of length* $2\operatorname{ord}_{3d}(4)$*, and those are the only cycles.*

Definition

a) $\mathscr{T}(1)$, *the tree composed by two points,* P_1 *and* P, *where* P_1 *is directed to* P. *For* $m \geq 1$, $\mathscr{T}(m+1)$ *is the tree obtained after attaching* 2 *points directed to each point in the last level of* $\mathscr{T}(m)$;

Definition

a) $\mathscr{T}(1)$, *the tree composed by two points*, P_1 *and* P, *where* P_1 *is directed to* P. *For* $m \geq 1$, $\mathscr{T}(m+1)$ *is the tree obtained after attaching* 2 *points directed to each point in the last level of* $\mathscr{T}(m)$;

b) *Given a graph* $\mathcal{H}$, $(\mathcal{H}, \mathscr{T}(m))$ *denotes the graph obtained after replacing each point of* $\mathcal{H}$ *by a tree isomorphic to* $\mathscr{T}(m)$.

Definition

a) $\mathscr{T}(1)$, *the tree composed by two points,* P_1 *and* P, *where* P_1 *is directed to* P. *For* $m \geq 1$, $\mathscr{T}(m+1)$ *is the tree obtained after attaching 2 points directed to each point in the last level of* $\mathscr{T}(m)$;

b) *Given a graph* $\mathcal{H}$, $(\mathcal{H}, \mathscr{T}(m))$ *denotes the graph obtained after replacing each point of* $\mathcal{H}$ *by a tree isomorphic to* $\mathscr{T}(m)$.

Definition

Given the functional graph $\mathcal{G}$ *of* $f(x) = x^{q+1} - x^2$ *over* $\mathbb{F}_{q^2}$, *let denote by*

a) $\mathcal{TC}_0$ *the connected component of zero.*

Definition

a) $\mathscr{T}(1)$, *the tree composed by two points,* P_1 *and* P, *where* P_1 *is directed to* P. *For* $m \geq 1$, $\mathscr{T}(m+1)$ *is the tree obtained after attaching* 2 *points directed to each point in the last level of* $\mathscr{T}(m)$;

b) *Given a graph* $\mathcal{H}$, $(\mathcal{H}, \mathscr{T}(m))$ *denotes the graph obtained after replacing each point of* $\mathcal{H}$ *by a tree isomorphic to* $\mathscr{T}(m)$.

Definition

Given the functional graph $\mathcal{G}$ *of* $f(x) = x^{q+1} - x^2$ *over* $\mathbb{F}_{q^2}$, *let denote by*

a) $\mathcal{TC}_0$ *the connected component of zero.*

b) $Cyc(\mathcal{G})$ *the sub-graph of* $\mathcal{G}$ *of every periodic point different of* 0.

Characterization of the pre-cycles

Theorem

Let $\mathcal{G}$ be the functional graph of $f(x) = x^{q+1} - x^2$ over $\mathbb{F}_{q^2}$. If $q - 1 = 2^k r$, then the graph $\mathcal{G}$ is isomorphic to

$$\mathcal{T}\mathcal{C}_0 \oplus (Cyc(\mathcal{G}), \mathscr{T}(k)).$$

Using the same technique we obtain the following result

Theorem

Let q be a power of a odd prime, such that $q-1 = 2^s r$ and r is odd. The functional graph of the function $f(x) = a(x^{q+1} + x^2)$ over $\mathbb{F}^{q^2}$ is isomorphic to

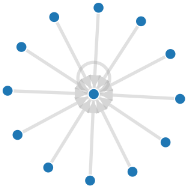
$$\mathscr{Z}^*(q) \bigoplus_{d|r} \frac{q \cdot \varphi(d)}{\mathrm{ord}_d(2)} \times (Cyc(\mathrm{ord}_d(2)), \mathscr{T}(s))$$

where $\mathscr{Z}^*(q)$ is the directed graph $Cyc(1)$ with $q-1$ trees isomorphic to $\mathscr{T}(1)$ attached to it.

For $q = 13$, we have that $q - 1 = 2^2 \times 3$ and the functional graph has the following components:

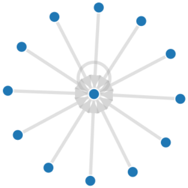
For $q = 13$, we have that $q - 1 = 2^2 \times 3$ and the functional graph has the following components:

One component isomorphic to

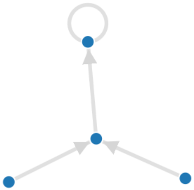


For $q = 13$, we have that $q - 1 = 2^2 \times 3$ and the functional graph has the following components:

One component isomorphic to

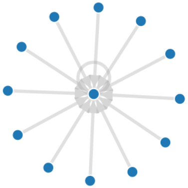


for $d = 1$, we have 13 components isomorphic to

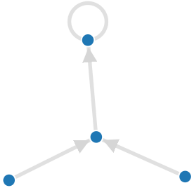


For $q = 13$, we have that $q - 1 = 2^2 \times 3$ and the functional graph has the following components:

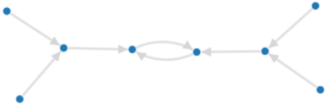
One component isomorphic to



for $d = 1$, we have 13 components isomorphic to



and, for $d = 3$, we have $\frac{13\cdot\varphi(3)}{\mathrm{ord}_3(2} = 13$ components isomorphic to



Idea of the proof

We can see $\mathbb{F}_{q^2}$ as a vector space over $\mathbb{F}_q$ with base $\{1, \beta\}$, where $\beta^2 = b \in \mathbb{F}_q$ is not a square in $\mathbb{F}_q$, We can see $\mathbb{F}_{q^2}$ as a vector space over $\mathbb{F}_q$ with base $\{1, \beta\}$, where $\beta^2 = b \in \mathbb{F}_q$ is not a square in $\mathbb{F}_q$, then the function $f(x) = x^{q+1} - dx^2$ (where $d = \pm 1$) over $\mathbb{F}_{q^2}$ is equivalent to the function $F : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q \times \mathbb{F}_q$,

$$\begin{aligned} \mathbb{F}_q \times \mathbb{F}_q &\to \mathbb{F}_q \times \mathbb{F}_q \\ \langle x, y\rangle &\mapsto \langle (d+1)x^2 + (d-1)by^2, 2dxy\rangle. \end{aligned} \tag{1}$$

Idea of the proof

We can see $\mathbb{F}_{q^2}$ as a vector space over $\mathbb{F}_q$ with base $\{1, \beta\}$, where $\beta^2 = b \in \mathbb{F}_q$ is not a square in $\mathbb{F}_q$, then the function $f(x) = x^{q+1} - dx^2$ (where $d = \pm 1$) over $\mathbb{F}_{q^2}$ is equivalent to the function $F : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q \times \mathbb{F}_q$,

$$\begin{aligned} \mathbb{F}_q \times \mathbb{F}_q &\to \mathbb{F}_q \times \mathbb{F}_q \\ \langle x, y \rangle &\mapsto \langle (d+1)x^2 + (d-1)by^2, 2dxy \rangle. \end{aligned} \tag{1}$$

In the case $d = 1$, we obtain

$$F(x, y) = -2y \langle by, x \rangle$$

Idea of the proof

We can see $\mathbb{F}_{q^2}$ as a vector space over $\mathbb{F}_q$ with base $\{1, \beta\}$, where $\beta^2 = b \in \mathbb{F}_q$ is not a square in $\mathbb{F}_q$, then the function $f(x) = x^{q+1} - dx^2$ (where $d = \pm 1$) over $\mathbb{F}_{q^2}$ is equivalent to the function $F : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q \times \mathbb{F}_q$,

$$\begin{aligned} \mathbb{F}_q \times \mathbb{F}_q &\to \mathbb{F}_q \times \mathbb{F}_q \\ \langle x, y\rangle &\mapsto \langle (d+1)x^2 + (d-1)by^2, 2dxy\rangle. \end{aligned} \tag{1}$$

In the case $d = 1$, we obtain

$$F(x, y) = -2y\langle by, x\rangle$$

and, applying f again,

$$F^{(2)}(x, y) = -8bxy^2\langle x, y\rangle.$$

By induction, we conclude that

$$F^{(2n)}(x,y) = g(x,y)^{\frac{4^n-1}{3}}\langle x,y\rangle,$$

where $g(x,y) = -8bxy^2$.

By induction, we conclude that

$$F^{(2n)}(x,y) = g(x,y)^{\frac{4^n-1}{3}}\langle x,y\rangle,$$

where $g(x,y) = -8bxy^2$.
Therefore $\langle x,y\rangle$ is a periodic point if and only if $\gcd(4, 3\cdot \mathrm{ord}_{\mathbb{F}_q}(g(x,y))) = 1$

Suppose that $\langle x_0, y_0\rangle$ be a periodic element and, for all $i \geq 1$, let $\langle x_i, y_i\rangle$ be a periodic point such that

$$f(x_i, y_i) = \langle x_{i-1}, y_{i-1}\rangle.$$

Suppose that $\langle x_0, y_0\rangle$ be a periodic element and, for all $i \geq 1$, let $\langle x_i, y_i\rangle$ be a periodic point such that

$$f(x_i, y_i) = \langle x_{i-1}, y_{i-1}\rangle.$$

Observe that $f(-x_i, -y_i) = f(x_i, y_i) = \langle x_{i-1}, y_{i-1}\rangle$ and $\langle -x_i, -y_i\rangle$ is not a periodic point.

Suppose that $\langle x_0, y_0\rangle$ be a periodic element and, for all $i \geq 1$, let $\langle x_i, y_i\rangle$ be a periodic point such that

$$f(x_i, y_i) = \langle x_{i-1}, y_{i-1}\rangle.$$

Observe that $f(-x_i, -y_i) = f(x_i, y_i) = \langle x_{i-1}, y_{i-1}\rangle$ and $\langle -x_i, -y_i\rangle$ is not a periodic point.

Now suppose by induction that $\langle \zeta_{2^{k-1}} x_{k-1}, \zeta_{2^{k-1}} y_{k-1}\rangle$ is a non periodic element that satisfies

$$f^{(k-1)}(\zeta_{2^{k-1}} x_{k-1}, \zeta_{2^{k-1}} y_{k-1}) = \langle x_0, y_0\rangle.$$

Suppose that $\langle x_0, y_0\rangle$ be a periodic element and, for all $i \geq 1$, let $\langle x_i, y_i\rangle$ be a periodic point such that

$$f(x_i, y_i) = \langle x_{i-1}, y_{i-1}\rangle.$$

Observe that $f(-x_i, -y_i) = f(x_i, y_i) = \langle x_{i-1}, y_{i-1}\rangle$ and $\langle -x_i, -y_i\rangle$ is not a periodic point.

Now suppose by induction that $\langle \zeta_{2^{k-1}} x_{k-1}, \zeta_{2^{k-1}} y_{k-1}\rangle$ is a non periodic element that satisfies

$$f^{(k-1)}(\zeta_{2^{k-1}} x_{k-1}, \zeta_{2^{k-1}} y_{k-1}) = \langle x_0, y_0\rangle.$$

If $\langle x, y\rangle \in f^{-1}(\zeta_{2^{k-1}} x_{k-1}, \zeta_{2^{k-1}} y_{k-1})$, then

$$y^2 = \zeta_{2^{k-1}} y_k^2$$

and, consequently, $f^{-1}(\zeta_{2^{k-1}} x_{k-1}, \zeta_{2^{k-1}} y_{k-1}) \neq \emptyset$ if, and only if, $\zeta_{2^{k-1}}$ is an square in $\mathbb{F}_q$, that is equivalent to $q \equiv 1 \pmod{2^k}$.

Future Works

Determine the functional graphs of

- $f(x) = ax^{q+1} + bx^2$ over $\mathbb{F}_{q^2}$.

Future Works

Determine the functional graphs of

- $f(x) = ax^{q+1} + bx^2$ over $\mathbb{F}_{q^2}$.
- $f(x) = a(x^q + bx)^2$ over $\mathbb{F}_{q^2}$.

Future Works

Determine the functional graphs of

- $f(x) = ax^{q+1} + bx^2$ over $\mathbb{F}_{q^2}$.
- $f(x) = a(x^q + bx)^2$ over $\mathbb{F}_{q^2}$.
- $f(x) = a(x^q + bx)(x^q + cx)$ over $\mathbb{F}_{q^2}$.

Future Works

Determine the functional graphs of

- $f(x) = ax^{q+1} + bx^2$ over $\mathbb{F}_{q^2}$.
- $f(x) = a(x^q + bx)^2$ over $\mathbb{F}_{q^2}$.
- $f(x) = a(x^q + bx)(x^q + cx)$ over $\mathbb{F}_{q^2}$.
- $f(x) = x^{q+1} - x^2$ over $\mathbb{F}_{q^3}$.

Some partial result for $d \neq \pm 1$

In general, the dynamic of $f(x) = x^{q+1} - dx^2 \in \mathbb{F}_q[x]$ over $\mathbb{F}_{q^2}$ is "quasi-chaotic".

Some partial result for $d \neq \pm 1$

In general, the dynamic of $f(x) = x^{q+1} - dx^2 \in \mathbb{F}_q[x]$ over $\mathbb{F}_{q^2}$ is "quasi-chaotic". We have some partial results

Theorem

For $a \in \mathbb{F}_q^*$,

1. $$\#f^{-1}(a) = \begin{cases} 0, & \textit{if } \chi_2(a(d-1)) = 1 \textit{ and } \chi_2(a(d+1)) = -1 \\ 4, & \textit{if } \chi_2(a(d-1)) = -1 \textit{ and } \chi_2(a(d+1)) = 1 \\ 2, & \textit{otherwise} \end{cases}$$

Some partial result for $d \neq \pm 1$

In general, the dynamic of $f(x) = x^{q+1} - dx^2 \in \mathbb{F}_q[x]$ over $\mathbb{F}_{q^2}$ is "quasi-chaotic".
We have some partial results

Theorem

For $a \in \mathbb{F}_q^*$,

1. $$\#f^{-1}(a) = \begin{cases} 0, & \text{if } \chi_2(a(d-1)) = 1 \text{ and } \chi_2(a(d+1)) = -1 \\ 4, & \text{if } \chi_2(a(d-1)) = -1 \text{ and } \chi_2(a(d+1)) = 1 \\ 2, & \text{otherwise} \end{cases}$$
2. *if $q \equiv 3 \pmod 4$, then* $$\#f^{-1}(a\beta) = \begin{cases} 0, & \text{if } \chi_2(-d^2+1) = 1 \\ 2, & \text{if } \chi_2(-d^2+1) = -1 \end{cases}$$

Some partial result for $d \neq \pm 1$

In general, the dynamic of $f(x) = x^{q+1} - dx^2 \in \mathbb{F}_q[x]$ over $\mathbb{F}_{q^2}$ is "quasi-chaotic". We have some partial results

Theorem

For $a \in \mathbb{F}_q^*$,

1. $$\#f^{-1}(a) = \begin{cases} 0, & \text{if } \chi_2(a(d-1)) = 1 \text{ and } \chi_2(a(d+1)) = -1 \\ 4, & \text{if } \chi_2(a(d-1)) = -1 \text{ and } \chi_2(a(d+1)) = 1 \\ 2, & \text{otherwise} \end{cases}$$
2. *if* $q \equiv 3 \pmod 4$, *then* $\#f^{-1}(a\beta) = \begin{cases} 0, & \text{if } \chi_2(-d^2+1) = 1 \\ 2, & \text{if } \chi_2(-d^2+1) = -1 \end{cases}$
3. *if* $q \equiv 1 \pmod 4$ *and* $\gamma_d^2 := -\frac{(d-1)b}{d+1}$, *then*

$$\#f^{-1}(a\beta) = \begin{cases} 4, & \text{if } \chi_2(-d^2+1) = -1 \text{ and } \chi_2(2\gamma_d a d) = -1 \\ 0, & \text{otherwise}, \end{cases}$$

Theorem

Let $q-1=2^s r$, *with* r *odd, and* $f(X)=X^{q+1}+dX^2$, *where* $d \neq \{\pm 1\}$. *If* $\chi_2(1-d^2)=1$, *then the connected components that contain the elements of* $\mathbb{F}_q$ *can be obtained by attaching two nodes to every point* $a \in \mathscr{G}(f|_{\mathbb{F}_q})$ *that satisfies* $\chi_2(a(d-1))=-1$.

Theorem

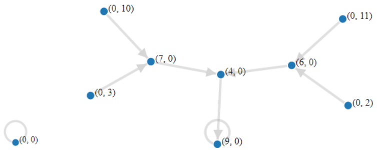
Let $q-1=2^s r$*, with* r *odd, and* $f(X)=X^{q+1}+dX^2$*, where* $d\neq\{\pm 1\}$*. If* $\chi_2(1-d^2)=1$*, then the connected components that contain the elements of* $\mathbb{F}_q$ *can be obtained by attaching two nodes to every point* $a\in\mathscr{G}(f|_{\mathbb{F}_q})$ *that satisfies* $\chi_2(a(d-1))=-1$*.*
In particular, 0 *is an isolated fixed point and* $\frac{1}{d+1}$ *is a fixed point with connected component isomorphic to*

- $\mathscr{Z}(4)$*, if* $s=1$*,*
- $(Cyc(1),\mathscr{T}(s+1))$*, if* $s\geq 2$*.*

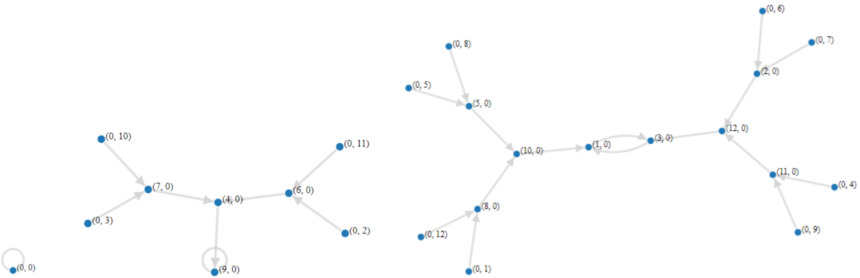
For $q = 13$ and $d = 2$, notice that $s = 2$ and that $\chi_2(1 - 2^2) = \chi_2(10) = 1$.

For $q = 13$ and $d = 2$, notice that $s = 2$ and that $\chi_2(1 - 2^2) = \chi_2(10) = 1$.Then the connected components of the elements in $\mathbb{F}_q$ are

For $q = 13$ and $d = 2$, notice that $s = 2$ and that $\chi_2(1 - 2^2) = \chi_2(10) = 1$.Then the connected components of the elements in $\mathbb{F}_q$ are



For $q = 13$ and $d = 2$, notice that $s = 2$ and that $\chi_2(1 - 2^2) = \chi_2(10) = 1$.Then the connected components of the elements in $\mathbb{F}_q$ are



- Chou, W.S., Shparlinski, I.E. *on the cycle structure of repeated exponentiation modulo prime*. Jour. of Number Theory **107** (2004) 345-356
- Martins, R., Panario, D., Qureshi, C. *A survey on iterations of mappings over finite fields* Radon Series on Computational and Applied Mathematics **23** (2019) 135-172
- Panario, D., Reis. L. *The functional graph of linear maps over finite fields and applications*, Designs, Codes and Cryptography **87** (2019) 437-453
- Quareshi, C., Panario, D. The graph structure of the Chebyshev polynomial over finite fields and applications, Designs, Codes and Cryptography *87* (2019) 393-416
- Rogers, T. *The Graph of the square mapping on the prime fields*, Disc Math. **148** (1996) 317-324
- Ugolini, S. *Graphs associated with the math* $x \mapsto x + x^{-1}$ *in finite fields of characteristic three and five*. Jour. of Number Theory **133** (2013)1207-1228