Value sets and periodic points for trinomials of the form $cx^d + x + a$ over $\mathbb{F}_p$

Kai Lu

July 27, 2021

Pseudorandom generators

Pseudorandom generators have many applications:

- Monte Carlo-method simulations.
- Key generation in cryptography.
- Simulate randomized algorithms.
- ...

Random mapping statistics

Our motivation is to find “simple” functions with “unpredictable” iterates that can potentially be good candidates or building blocks for pseudorandom generators.

Random mapping statistics

Our motivation is to find "simple" functions with "unpredictable" iterates that can potentially be good candidates or building blocks for pseudorandom generators.

Definition

A *t-nomial* is a polynomial with exactly t monomial terms.

Random mapping statistics

Our motivation is to find "simple" functions with "unpredictable" iterates that can potentially be good candidates or building blocks for pseudorandom generators.

Definition

A *t-nomial* is a polynomial with exactly t monomial terms.

Sparse polynomials over prime fields have not been explored in this direction.

Random mapping statistics

A first step is to analyze their behavior and see if there is evidence whether they can be good pseudorandom generators.

Random mapping statistics

A first step is to analyze their behavior and see if there is evidence whether they can be good pseudorandom generators.

Definition

Let $f(x) \in \mathbb{F}_p[x]$. The *value set* of f is the set $V_f = \{f(a) \mid a \in \mathbb{F}_p\}$. The cardinality of V_f is denoted by $\#V_f$.

Random mapping statistics

A first step is to analyze their behavior and see if there is evidence whether they can be good pseudorandom generators.

Definition

Let $f(x) \in \mathbb{F}_p[x]$. The *value set* of f is the set $V_f = \{f(a) \mid a \in \mathbb{F}_p\}$. The cardinality of V_f is denoted by $\#V_f$.

Let $f(x) \in \mathbb{F}_p[x]$. For any positive integer m, we write $f^m(x) = f \circ \cdots \circ f(x)$ for the mth iterate of f under composition.

Random mapping statistics

A first step is to analyze their behavior and see if there is evidence whether they can be good pseudorandom generators.

Definition

Let $f(x) \in \mathbb{F}_p[x]$. The *value set* of f is the set $V_f = \{f(a) \mid a \in \mathbb{F}_p\}$. The cardinality of V_f is denoted by $\#V_f$.

Let $f(x) \in \mathbb{F}_p[x]$. For any positive integer m, we write $f^m(x) = f \circ \cdots \circ f(x)$ for the mth iterate of f under composition.

Definition

Let $f(x) \in \mathbb{F}_p[x]$. We say $a \in \mathbb{F}_p$ is a *periodic point* of f if there exists positive integer n such that $f^n(a) = a$.

Value set

Observation

The value set of $f(x) = cx^d + x + a$ *differs from that of* $g(x) = cx^d + x$ *by a constant.*

Value set

Observation

The value set of $f(x) = cx^d + x + a$ *differs from that of* $g(x) = cx^d + x$ *by a constant.*

Therefore, for studying the value set of such polynomials, we can restrict ourselves to the case $f(x) = cx^d + x$.

Value set

Let's first look at a very special case when $d = (p+1)/2$.

Proposition

Let $f(x) = cx^{(p+1)/2} + x \in \mathbb{F}_p[x]$. If $c \neq \pm 1$ and $1 - c^2$ is a square in $\mathbb{F}_p$, then $\# V_f = p$. If $c = \pm 1$ or $1 - c^2$ is not a square in $\mathbb{F}_p$, then $\# V_f = (p+1)/2$.

Value set

Let's first look at a very special case when $d = (p+1)/2$.

Proposition

Let $f(x) = cx^{(p+1)/2} + x \in \mathbb{F}_p[x]$. If $c \neq \pm 1$ and $1 - c^2$ is a square in $\mathbb{F}_p$, then $\#V_f = p$. If $c = \pm 1$ or $1 - c^2$ is not a square in $\mathbb{F}_p$, then $\#V_f = (p+1)/2$.

We would like to generalize this.

Value set

Kai Lu

It is well known that $\mathbb{F}_p^*$ is cyclic.

Definition

$x \in \mathbb{F}_p^*$ is an *ith root of unity* if $x^i = 1$.

The set of ith roots of unity is a subgroup of $\mathbb{F}_p^*$ and has order $\gcd(p-1, i)$ for each i.

Value set

It is well known that $\mathbb{F}_p^*$ is cyclic.

Definition

$x \in \mathbb{F}_p^*$ is an *ith root of unity* if $x^i = 1$.

The set of ith roots of unity is a subgroup of $\mathbb{F}_p^*$ and has order $\gcd(p-1, i)$ for each i.
We define $H_p(d) = \gcd(p-1, d-1)$, H to be the subgroup of $H_p(d)$th roots of unity, and G to be the set of cosets of H.

Value set

Lemma

For a coset of H, if its elements do not evaluate to 0 under $f(x) = cx^d + x \in \mathbb{F}_p[x]$, then f maps it bijectively to a coset of H.

Value set

Lemma

For a coset of H, if its elements do not evaluate to 0 under $f(x) = cx^d + x \in \mathbb{F}_p[x]$, then f maps it bijectively to a coset of H.

Corollary

For $a \neq 0$, $f(x) = cx^d + x + a \in \mathbb{F}_p[x]$ has at most $(p-1)/H_p(d)$ roots.

Value set

Lemma

For a coset of H, if its elements do not evaluate to 0 under $f(x) = cx^d + x \in \mathbb{F}_p[x]$, then f maps it bijectively to a coset of H.

Corollary

For $a \neq 0$, $f(x) = cx^d + x + a \in \mathbb{F}_p[x]$ has at most $(p-1)/H_p(d)$ roots.

Corollary

The value set of $f(x) = cx^d + x \in \mathbb{F}_p[x]$ is a union of $\{0\}$ and cosets of H.

Value set

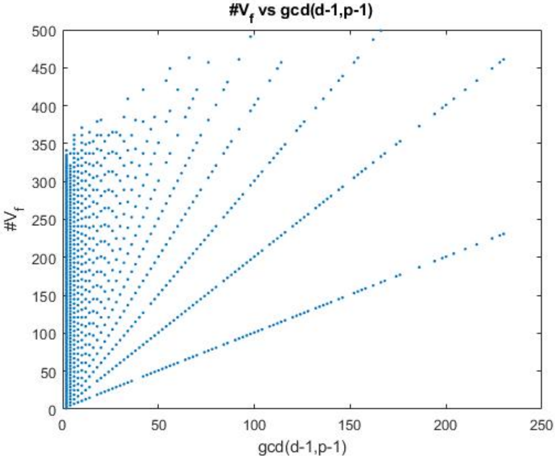

Figure: Plot of $\#V_f$ vs $\gcd(d-1, p-1)$ made with MATLAB.

Value set

Take a generator g of $\mathbb{F}_p^*$. Let $f(x) = cx^d + x \in \mathbb{F}_p[x]$.

Value set

Take a generator g of $\mathbb{F}_p^*$. Let $f(x) = cx^d + x \in \mathbb{F}_p[x]$. Define a relation $\sim_{(c,d)}$ on G by $g^i H \sim_{(c,d)} g^j H$ if $(cg^{i(d-1)} + 1)/(cg^{j(d-1)} + 1) \in g^{j-i} H$.

Value set

Kai Lu

Take a generator g of $\mathbb{F}_p^*$. Let $f(x) = cx^d + x \in \mathbb{F}_p[x]$. Define a relation $\sim_{(c,d)}$ on G by $g^i H \sim_{(c,d)} g^j H$ if $(cg^{i(d-1)} + 1)/(cg^{j(d-1)} + 1) \in g^{j-i} H$.

Lemma

If there exists i such that $i(d-1) \equiv \log_g(-1/c) \mod (p-1)$, then $\sim_{(c,d)}$ is an equivalence relation on $G \setminus \{g^i H\}$. Otherwise, $\sim_{(c,d)}$ is an equivalence relation on G.

Value set

Kai Lu

Theorem

Let $f(x) = cx^d + x \in \mathbb{F}_p[x]$.
If there exists i *such that* $i(d-1) \equiv \log_g(-1/c) \mod (p-1)$,
then $\#V_f = 1 + H_p(d)\left|(G \setminus \{g^i H\})/\sim_{(c,d)}\right|$.
Otherwise $\#V_f = 1 + H_p(d)\left|G/\sim_{(c,d)}\right|$.

Value set

Theorem

Let $f(x) = cx^d + x \in \mathbb{F}_p[x]$.
If there exists i *such that* $i(d-1) \equiv \log_g(-1/c) \mod (p-1)$,
then $\#V_f = 1 + H_p(d) \left|(G \setminus \{g^i H\})/ \sim_{(c,d)}\right|$.
Otherwise $\#V_f = 1 + H_p(d) \left|G/ \sim_{(c,d)}\right|$.

The previous proposition is a special case, as there are 2 cosets of $(p-1)/2$th roots of unity.

Periodic points

Definition

Given a function $f : \mathbb{F}_p \to \mathbb{F}_p$, the *functional graph* of f is a directed graph with p vertices labelled by the elements of $\mathbb{F}_p$, where there is an edge from u to v if and only if $f(u) = v$.

Periodic points

Definition

Given a function $f : \mathbb{F}_p \to \mathbb{F}_p$, the *functional graph* of f is a directed graph with p vertices labelled by the elements of $\mathbb{F}_p$, where there is an edge from u to v if and only if $f(u) = v$.

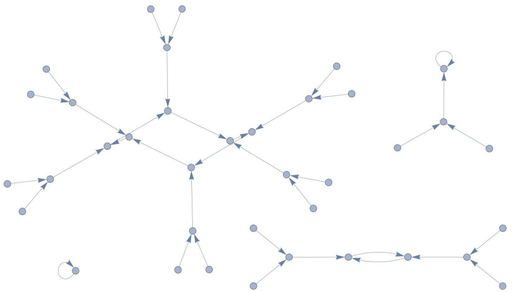

Figure: Functional graph of x^2 over $\mathbb{F}_{37}$ made with Wolfram Mathematica.

Periodic points

Proposition (Bach, Bridy 2013)

For a bijection $\varphi : \mathbb{F}_p \to \mathbb{F}_p$, the functional graph of $\varphi^{-1} \circ f \circ \varphi$ is isomorphic to that of f, for any $f : \mathbb{F}_p \to \mathbb{F}_p$.

For $f(x) = cx^d + x + a$, if $a \neq 0$, we can take $\varphi(x) = ax$, and we get
$\varphi^{-1} \circ f \circ \varphi(x) = (c(ax)^d + ax + a)/a = ca^{d-1}x^d + x + 1.$
Therefore, to study the behavior of such trinomials under iteration, it suffices to consider ones of the form
$f(x) = cx^d + x + 1$ and $f(x) = cx^d + x$.

Periodic points

Lemma

If $f(x) \in \mathbb{F}_p[x]$ is a bijection, then every element of $\mathbb{F}_p$ is a periodic point of f.

Periodic points

Lemma

If $f(x) \in \mathbb{F}_p[x]$ is a bijection, then every element of $\mathbb{F}_p$ is a periodic point of f.

This means that for bijective $f(x) = cx^d + x$,
$g(x) = cx^d + x + 1$ has the same number of periodic points.

Periodic points

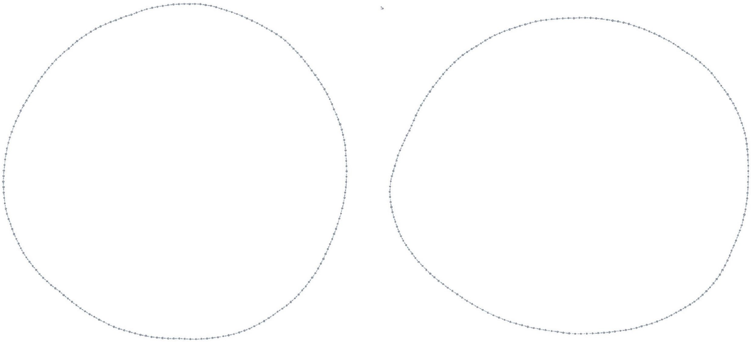

Figure: Functional graph of $133x^{195} + x$ over $\mathbb{F}_{389}$ made with Wolfram Mathematica.

Periodic points

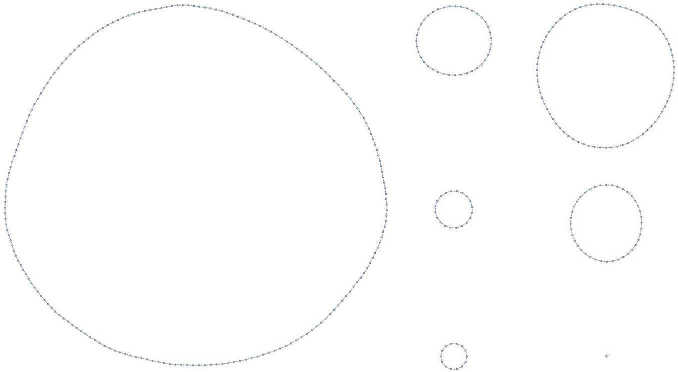

Figure: Functional graph of $133x^{195} + x + 1$ over $\mathbb{F}_{389}$ made with Wolfram Mathematica.

Periodic points

However, for non-bijective f, it appears that we can't hope for nice behavior.

Periodic points

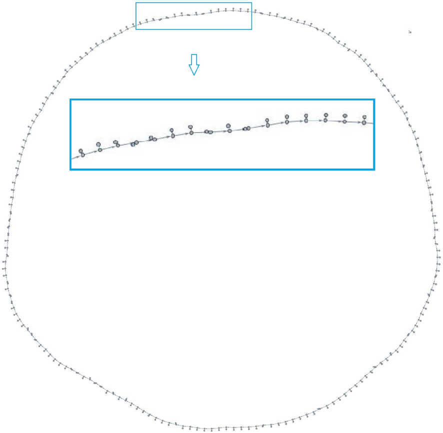

Figure: Functional graph of $122x^{195} + x$ over $\mathbb{F}_{389}$ made with Wolfram Mathematica.

Periodic points

Kai Lu

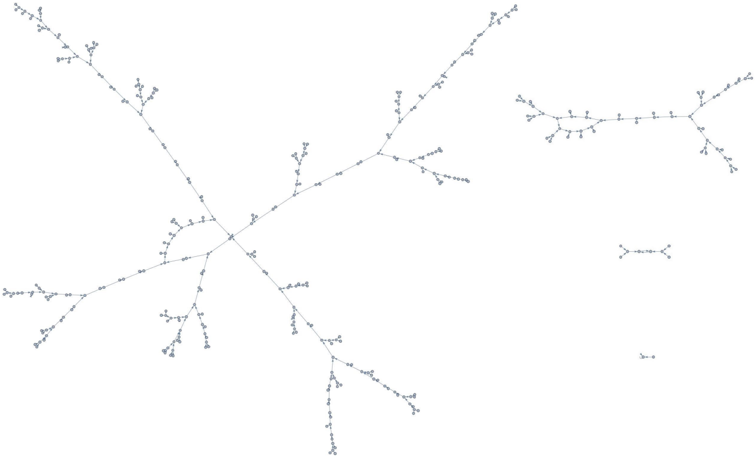

Figure: Functional graph of $122x^{195} + x + 1$ over $\mathbb{F}_{389}$ made with Wolfram Mathematica.

Periodic points

Let's try to understand the case when $f(x) = cx^d + x$ better.

Periodic points

Let's try to understand the case when $f(x) = cx^d + x$ better.

Definition

Let C, G be graphs. A *covering map* $f : C \to G$ is a surjection and a local isomorphism: the neighbourhood of a vertex v in C is mapped bijectively onto the neighbourhood of $f(v)$ in G.

Periodic points

Let's try to understand the case when $f(x) = cx^d + x$ better.

Definition

Let C, G be graphs. A *covering map* $f : C \to G$ is a surjection and a local isomorphism: the neighbourhood of a vertex v in C is mapped bijectively onto the neighbourhood of $f(v)$ in G.

Definition

A graph C is a *covering graph* of graph G if there is a covering map from C to G.

Periodic points

Kai Lu

Proposition

The functional graph of $f(x) = cx^d + x$ *excluding the connected component containing* $\{0\}$ *is a covering graph of the functional graph of the mapping that* $f(x) = cx^d + x$ *induces on* G*, the set of cosets.*

Corollary

The cycle lengths that appear in the functional graph of $f(x) = cx^d + x$ *are multiples of that of the functional graph of the mapping that* $f(x) = cx^d + x$ *induces on* G*.*

Periodic points

Kai Lu

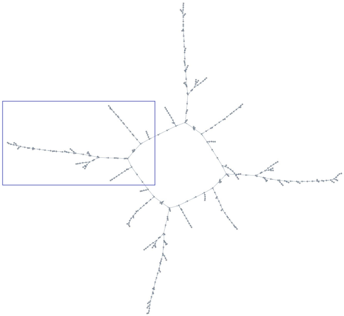

Figure: Functional graph of $122x^{137} + x$ over $\mathbb{F}_{389}$ excluding 0 made with Wolfram Mathematica.

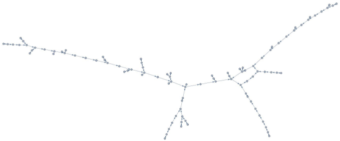

Figure: Functional graph of the mapping that $122x^{137} + x$ over $\mathbb{F}_{389}$ induces on G made with Wolfram Mathematica.

Periodic points

Kai Lu

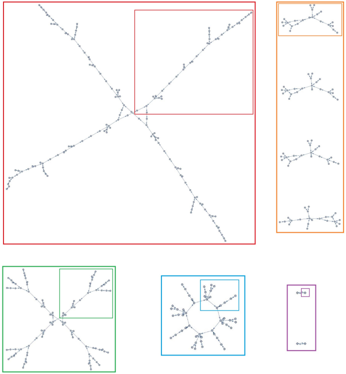

Figure: Functional graph of $145x^{137} + x$ over $\mathbb{F}_{389}$ excluding 0 made with Wolfram Mathematica.

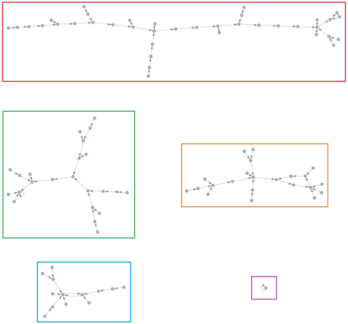

Figure: Functional graph of the mapping that $145x^{137} + x$ over $\mathbb{F}_{389}$ induces on G made with Wolfram Mathematica.

References

[1] Eric Bach and Andrew Bridy. *On the number of distinct functional graphs of affine-linear transformations over finite fields*. Linear Algebra and its Applications 2013.

Thank you

Thank you to Professor Rojas, TAMU, and NSF.
Thank you for your time.
Questions?