# VALUE SET AND PERIODIC POINTS OF TRINOMIALS $cx^d + x + a$ OVER $\mathbb{F}_p$

KAIWEN LU

Abstract. It In this paper, we describe the cardinality of the value sets of trinomials of the form $cx^d + x + a$ over $\mathbb{F}_p$ in terms of cosets of subgroups of $\mathbb{F}_p^*$, and present some properties of the periodic points using functional graphs.

## 1. Introduction

It is very desirable to have "simple" function with "unpredictable" iterates, because they might be good candidates or building blocks of pseudorandom generators. Sparse polynomials over prime fields have not been explored in this direction as much. One notable example is a class of pseudorandom number generators based on trinomials with a large primitive factor presented in [BZ03].

It is conjectured that the range of $f(x) = cx^d + x$ for $\gcd(p-1, d) = 1$ and $p^{3/5} < d < p$ is close to all of $\mathbb{F}_p$, and if this were true, one might conjecture further that $f$ permutes $\mathbb{F}_p^*$ in an "unpredictable" way. A start on this problem would be to analyze their behaviors. We will specifically look at the value sets and periodic points of trinomials of the form $cx^d + x + a$ over $\mathbb{F}_p$.

## 2. Background

**Definition 2.1** (Value set)**.** 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 $\#V_f$.

Note that value set of $f(x) = cx^d + x + a$ differ from that of $g(x) = cx^d + x$ by a constant, so for studying the value set of such polynomials, we can restrict ourselves to the case when $f(x) = cx^d + x$.

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 $m$th iterate of $f$ under composition.

**Definition 2.2** (Periodic point)**.** 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 $f^n(a) = a$.

**Definition 2.3** (Functional graph)**.** 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 $f(u) = v$.

Functional graphs are relevant, because it is not hard to see that an element is a periodic point of $f$ if and only if its corresponding vertex is in a cycle in the functional graph, and its period, the least positive $n$ such that $f^n$ maps it to itself, is exactly the length of the cycle it's in.

Using definition 2 from [BB13], the following proposition helps us simplify the problem a bit. It is stated in terms of dynamical systems in [BB13], we use the functional graph interpretation of it.

**Proposition 2.4** ([BB13])**.** *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 $f \in \mathbb{F}_p[x]$.*

*Proof.* Let's denote the functional graph of $f$ as $G_f$, and that of $\varphi^{-1} \circ f \circ \varphi$ as $G_f^\varphi$. Consider the bijection $\varphi^{-1} : \mathbb{F}_p \to \mathbb{F}_p$. For any edge $a$ to $f(a)$ in $G_f$, we have $\varphi^{-1}(a)$ to $\varphi^{-1} \circ f \circ \varphi(\varphi^{-1}(a)) = \varphi^{-1}(f(a))$ is also an edge in $G_f^\varphi$.

For any edge $a$ to $\varphi^{-1} \circ f \circ \varphi(a)$ in $G_f^\varphi$, we have $\varphi(a)$ to $f \circ \varphi(a) = \varphi(\varphi^{-1} \circ f \circ \varphi(a))$ is also an edge in $G_f$. $\varphi^{-1}$ is a graph isomorphism. □

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 iterations, it suffices to consider ones of the form $f(x) = cx^d + x + 1$ and $f(x) = cx^d + x$.

Another relevant construction is the covering graph, we present its definition here as well.

**Definition 2.5.** 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 2.6.** A graph $C$ is a *covering graph* of graph $G$ if there is a covering map from $C$ to $G$.

## 3. Results

Let $f(x) = cx^d + x \in \mathbb{F}_p[x]$ such that $c, d \in \mathbb{F}_p^*$ and $d \neq 1$, we define $H_p(d) = \gcd(p - 1, d - 1)$, $H$ to be the subgroup of $H_p(d)$th roots of unity in $\mathbb{F}_p^*$, and $G$ to be the set of cosets of $H$.

### 3.1. Value set.

We would like to study the cardinality of the value set. Let's first consider a very special case when $d = (p + 1)/2$.

**Proposition 3.1.** *Let $f(x) = cx^{(p+1)/2} + x \in \mathbb{F}_p[x]$. If $c \neq \pm 1$ and $(1 - c)/(1 + c)$ is a square in $\mathbb{F}_p$, then $\#V_f = p$. If $c = \pm 1$ or $(1 - c)/(1 + c)$ is not a square in $\mathbb{F}_p$, then $\#V_f = (p + 1)/2$.*

*Proof.* $f(x) = x(cx^{(p-1)/2} + 1)$, so $f(x) = \begin{cases} x(c + 1), \text{ if } x \text{ is a square} \\ x(-c + 1), \text{ otherwise} \end{cases}$.

If $c = 1$, then $f(x) = \begin{cases} 2x, \text{ if } x \text{ is a square} \\ 0, \text{ otherwise} \end{cases}$, and $V_f = \{2x \mid x = a^2, a \in \mathbb{F}_p\}$ with $\#V_f = (p + 1)/2$. If $c = -1$, then $f(x) = \begin{cases} 0, \text{ if } x \text{ is a square} \\ 2x, \text{ otherwise} \end{cases}$, and $V_f = \{0\} \cup \{2x \mid x \neq a^2, \text{for all } a \in \mathbb{F}_p\}$ with $\#V_f = (p + 1)/2$.

Now assume $c \neq \pm 1$, then $f$ is injective on squares and non-squares respectively. Suppose $(1-c)/(1+c)$ is a square in $\mathbb{F}_p$. For $x, y \in \mathbb{F}_p$. consider the equation $x(1+c) = y(1-c)$ for $x, y \in \mathbb{F}_p$. $x = y(1-c)/(1+c)$ is never satisfied when $x$ is a square and $y$ is not a square, so the image of squares and non-squares are disjoint. We get $V_f = \mathbb{F}_p$ and $\#V_f = p$ in this case. If $(1-c)/(1+c)$ is not a square in $\mathbb{F}_p$, then $x = y(1-c)/(1+c)$ for $x$ a square and $y$ not a square is a bijection between the two cosets, where $f(x) = f(y)$, and $f$ is a 2-to-1 function on $\mathbb{F}_p^*$. We get $\#V_f = (p+1)/2$ in this case. □

We would like to generalize this. It turns out that the mapping given by $f(x) = cx^d + x \in \mathbb{F}_p[x]$ is highly relevant to cosets of $H$. We first present some lemmas that describe its properties.

**Lemma 3.2.** *Let $f(x) = cx^d + x \in \mathbb{F}_p[x]$. For a coset of $H$, if its elements do not evaluate to 0 under $f$, then $f$ maps it bijectively to a coset of $H$. Otherwise $f$ maps the entire coset to 0.*

*Proof.* Write $f(x) = x(cx^{d-1} + 1)$. Let $gH$ be a coset of $H$. For any element $x = gh$ in $gH$, $cx^{d-1} + 1 = cg^{d-1}h^{d-1} + 1 = cg^{d-1} + 1$ is a constant. Therefore $f(x) = (cg^{d-1} + 1)x$ for $x \in gH$. If elements of $gH$ do not evaluate to 0 under $f$, then $cg^{d-1} + 1 \neq 0$ is invertible, and $f$ is a bijection from $gH$ to $(cg^{d-1} + 1)gH$. If there exists $x \in gH$ such that $f(x) = 0$, then since $x \neq 0$, $cg^{d-1} + 1 = 0$, and $f(x) = 0x$ for $x \in gH$. □

**Corollary 3.3.** *For $a \neq 0$, $f(x) = cx^d + x + a \in \mathbb{F}_p[x]$ has at most $(p-1)/H_p(d)$ roots.*

*Proof.* Denote $g(x) = cx^d + x$. Note that the roots of $f$ are exactly the set $\{x \mid g(x) = -a\}$. Since $a \neq 0$, if $-a \in V_g$, then there is at most 1 element from each coset of $H$ that maps to it under $g$ by Lemma 3.2. There are $(p-1)/H_p(d)$ cosets of $H$, and the corollary follows. □

**Corollary 3.4.** *The value set of $f(x) = cx^d + x \in \mathbb{F}_p[x]$ is a union of $\{0\}$ and cosets of $H$.*

*Proof.* Varying $x$ over $\{0\}$ and cosets of $H$ gives us the corollary. □

We represent the cosets of $H$ by $G = \{H, gH, g^2H, \ldots, g^{(p-1)/H_p(d)-1}H\}$.

**Lemma 3.5.** *For $c \in \mathbb{F}_p^*$, $cg^{i(d-1)} + 1$ for $0 \leq i \leq (p-1)/H_p(d) - 1$ are distinct.*

*Proof.* for $1 \leq j < i \leq (p-1)/H_p(d)-1$, if $cg^{i(d-1)}+1 = cg^{j(d-1)}+1$, then $i(d-1) = j(d-1) \mod (p-1)$, which implies $(i-j)(d-1) \equiv 0 \mod (p-1)$. This only happens when $(p-1)/H_p(d) \mid (i-j)$, but $0 \leq i, j \leq (p-1)/H_p(d) - 1$. □

Define a relation $\sim_{(c,d)}$ on $G$ by $g^iH \sim_{(c,d)} g^jH$ if $(cg^{i(d-1)} + 1)/(cg^{j(d-1)} + 1) \in g^{j-i}H$. Our choice of coset representatives is well-defined for $\sim_{(c,d)}$, because $g^{(i+k(p-1)/H_p(d))(d-1)} = g^{i(d-1)}g^{k(p-1)(d-1)/H_p(d)} = g^{i(d-1)}$ for any $k$.

**Lemma 3.6.** *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 $G \setminus \{g^iH\}$. Otherwise, $\sim_{(c,d)}$ is an equivalence relation on $G$.*

*Proof.* $cg^{i(d-1)} + 1 = 0$ if and only if $i(d-1) \equiv \log_g(-1/c) \mod (p-1)$. Furthermore, if $i(d-1) = j(d-1) \mod (p-1)$, then $(i-j)(d-1) \equiv 0 \mod (p-1)$, which requires that $(p-1)/H_p(d) \mid (i-j)$, and $g^j \in g^iH$. Note that the existence of such $i$ is independent

of our choice of the generator $g$, because for any other generator $g'$ of $\mathbb{F}_p^*$, $\log_g(-1/c) = k \log_{g'}(-1/c) \mod (p-1)$, for some $k$ coprime to $p-1$.

With the assumption as stated in the lemma, we may now assume $cg^{i(d-1)}+1 \neq 0$ for all $i$. $\sim_{(c,d)}$ is reflexive because $(cg^{i(d-1)}+1)/(cg^{i(d-1)}+1) = 1 \in H$. It's symmetric because if $(cg^{i(d-1)}+1)/(cg^{j(d-1)}+1) \in g^{j-i}H$, then $(cg^{j(d-1)}+1)/(cg^{i(d-1)}+1) \in g^{i-j}H$. It's transitive because if $(cg^{i(d-1)}+1)/(cg^{j(d-1)}+1) \in g^{j-i}H$ and $(cg^{j(d-1)}+1)/(cg^{k(d-1)}+1) \in g^{k-j}H$, then $(cg^{i(d-1)}+1)/(cg^{k(d-1)}+1) \in g^{k-i}H$. □

We are now ready to make the generalization of Proposition 3.1.

**Theorem 3.7.** *Let $f(x) = cx^d + x \in \mathbb{F}_p[x]$. Let $g$ be a generator of $\mathbb{F}_p^*$. If there exists $i$ such that $i(d-1) \equiv \log_g(-1/c) \mod (p-1)$, then $\#V_f = 1 + H_p(d)\left|(G \setminus \{g^iH\})/\sim_{(c,d)}\right|$. Otherwise $\#V_f = 1 + H_p(d)\left|G/\sim_{(c,d)}\right|$.*

*Proof.* $f(x) = x(cg^{i(d-1)}+1)$ for $x \in g^iH$ by Lemma 3.2.

First suppose there is no $i$ such that $i(d-1) \equiv \log_g(-1/c) \mod (p-1)$, which implies $cg^{i(d-1)}+1 \neq 0$ for all $i$. If $(cg^{i(d-1)}+1)/(cg^{j(d-1)}+1) \in g^{j-i}H$, then $f(g^iH) = (cg^{i(d-1)}+1)g^iH = ((cg^{i(d-1)}+1)/(cg^{j(d-1)}+1))(cg^{j(d-1)}+1)g^iH = (cg^{j(d-1)}+1)g^jH = f(g^jH)$.

On the other hand, if $(cg^{i(d-1)}+1)/(cg^{j(d-1)}+1) \notin g^{j-i}H$, then $f(g^iH) = (cg^{i(d-1)}+1)g^iH = ((cg^{i(d-1)}+1)/(cg^{j(d-1)}+1))(cg^{j(d-1)}+1)g^iH \neq (cg^{j(d-1)}+1)g^jH = f(g^jH)$.

Therefore, $f(g^iH) = f(g^jH)$ if and only if $g^iH \sim_{(c,d)} g^jH$. We get $\left|G/\sim_{(c,d)}\right|$ distinct cosets of $H$ together with 0 in $V_f$, which gives us $\#V_f = 1 + H_p(d)\left|G/\sim_{(c,d)}\right|$.

Now suppose there exists $i$ such that $i(d-1) \equiv \log_g(-1/c) \mod (p-1)$, we get that $cg^{i(d-1)}+1 = 0$, and $f(g^iH) = \{0\}$. Since the constants $cg^{j(d-1)}+1$ are distinct for all $j$, $g^iH$ is the unique coset of $H$ that evaluates to 0. The same proof as above applies to $G \setminus \{g^iH\}$, and we get $\left|(G \setminus \{g^iH\})/\sim_{(c,d)}\right|$ distinct cosets of $H$ together with 0 in $V_f$, which gives us $\#V_f = 1 + H_p(d)\left|(G \setminus \{g^iH\})/\sim_{(c,d)}\right|$. □

We now see that Proposition 3.1 is a special case of Theorem 3.7, as $\left|G/\sim_{(c,d)}\right|$ and $\left|(G \setminus \{g^iH\})/\sim_{(c,d)}\right|$ can only be 1 or 2.

Next we present a simple lemma that describes $d$ with specific $H_p(d)$.

**Lemma 3.8.** *For $d < p-1$, where $p$ is prime, there exists $a, b \in \mathbb{Z}_{>0}$ coprime such that $d = (ap+b)/(a+b)$. Furthermore, $a, b$ are unique, and $a+b = (p-1)/H_p(d)$.*

*Proof.* Take $a = (d-1)/\gcd(p-d, d-1)$, $b = (p-d)/\gcd(p-d, d-1)$, we get

$$\begin{aligned}\frac{ap+b}{a+b} =& \frac{p(d-1)/\gcd(p-d,d-1) + (p-d)/\gcd(p-d,d-1)}{(d-1)/\gcd(p-d,d-1) + (p-d)/\gcd(p-d,d-1)} \\ =& \frac{dp-p+p-d}{p-1} \\ =& d\end{aligned}$$

. $a$ and $b$ are coprime, and $a+b = (p-1)/\gcd(p-d, d-1) = (p-1)/H_p(d)$.

Now suppose $d = (cp+d)/(c+d)$ for some $c, d \in \mathbb{Z}_{>0}$ coprime. We then have $(c+d)(ap+b) = (a+b)(cp+d)$, which yields $ad = bc$. Since $a$ is coprime to $b$, and $c$ is coprime to $d$,

anything on the right contributing to factors of $d$ have to come from $b$, so $d \mid b$, and similarly $a \mid c$. By a symmetric argument we get $b \mid d$ and $c \mid a$, which gives us equality in $\mathbb{Z}_{>0}$. □

With this lemma, when we want to find $d$ with a specific $H_p(d)$, we can just compute $k = (p-1)/H_p(d)$, and take $d = (ap + (k-a))/k$, where $1 \le a \le k-1$ and $a$ is coprime to $k - a$.

### 3.2. **Periodic points.**

Due to the connection between functional graphs and periodic points as described in the background section, we will mostly study properties of the functional graph.

**Lemma 3.9.** *$f(x) \in \mathbb{F}_p[x]$ is a bijection if and only if every element of $\mathbb{F}_p$ is a periodic point of $f$.*

*Proof.* Suppose $f(x) \in \mathbb{F}_p[x]$ is a bijection. Consider the functional graph of $f$, every vertex has degree 2 because it is the image of 1 element. Therefore the functional graph must be a union of directed cycles and loops, which implies that all elements are periodic.

Now suppose every element of $\mathbb{F}_p$ is a periodic point of $f$. Then $\#V_f = p$, and $f(x) \in \mathbb{F}_p[x]$ must be a bijection by counting. □

**Corollary 3.10.** *If every element of $\mathbb{F}_p$ is a periodic point of $f(x) = cx^d + x$, then every element of $\mathbb{F}_p$ is a periodic point of $f(x) = cx^d + x + 1$.* □

We focus on the functional graph of $f(x) = cx^d + x$. By Lemma 3.2, we know that $f$ also gives a mapping between cosets, sometimes excluding a coset that maps to 0.

**Proposition 3.11.** *Let $f(x) = cx^d + x$. If there exists $i$ such that $i(d-1) \equiv \log_g(-1/c) \mod (p-1)$, then the functional graph of $f$ on $\mathbb{F}_p^* \setminus g^i H$ is a covering graph of the functional graph of the mapping that $f$ induces on $G \setminus \{g^i H\}$. Otherwise, the functional graph of $f$ on $\mathbb{F}_p^*$ is a covering graph of the functional graph of the mapping that $f$ induces on $G$.*

*Proof.* First suppose there is no $i$ such that $i(d-1) \equiv \log_g(-1/c) \mod (p-1)$, which implies $cg^{i(d-1)} + 1 \neq 0$ for all $i$. Then $f$ indeed induces a mapping on $G$. Denote the functional graph of $f$ on $\mathbb{F}_p^*$ by $C$ and that on $G$ by $G'$. Define the mapping $\varphi : C \to G'$ by $\varphi(x) = xH$. We claim this is a covering map. Surjectivity is clear. Let $g$ be a generator of $\mathbb{F}_p^*$, let $x \in g^i H$. $f(x) = (cg^{i(d-1)}+1)x \in (cg^{i(d-1)}+1)g^i H$, so $\varphi(f(x)) = (cg^{i(d-1)}+1)g^i H = f(g^i H) = f(\varphi(x))$. For the edge $x$ to $f(x)$ in $C$, we have $\varphi(x)$ to $\varphi(f(x))$ is also an edge in $G'$. We see that $\varphi$ preserves outgoing edges. On the other hand, for any $y \in \mathbb{F}_p$ such that $f(y) = x$, by Lemma 3.2, $f$ maps $yH$ bijectively to $xH$, so there is exactly one element $y \in yH$ such that $f(y) = x$. We see that $\varphi$ preserves incoming edges as well. $\varphi$ is a local graph isomorphism and therefore a covering map.

If there exists $i$ such that $i(d-1) \equiv \log_g(-1/c) \mod (p-1)$, then the same proof as above goes through as long as we exclude $g^i H$, since $cg^{j(d-1)} + 1 \neq 0$ for all $j \neq i$. □

**Corollary 3.12.** *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 $G$.*

*Proof.* There is exactly one cycle or loop in each connected component of functional graphs. By the locally isomorphic property of covering graphs, degrees are preserved by covering maps, and it follows that every cycle of a covering graph is the preimage of a cycle or loop under a covering map. The corollary then follows from Proposition 3.11 and Proposition 1 in [Hli10], which states that preimage of a cycle $C_n$ under a covering map consists of a collection of disjoint cycles whose lengths are divisible by $n$. □

We close by showing an example of Proposition 3.11. Figure 1 is a covering graph of figure 2.

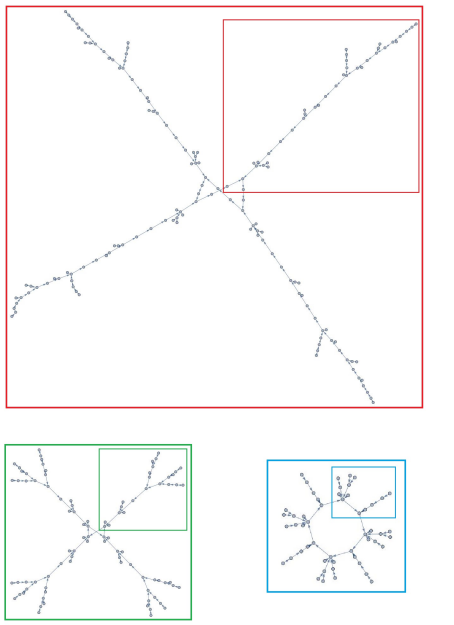

FIGURE 1 Functional graph of $145x^{137} + x$ over $\mathbb{F}_{389}^*$.

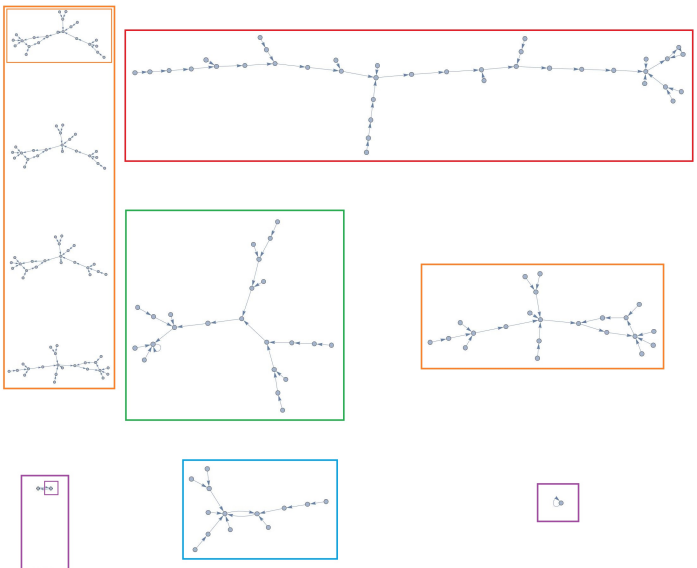

FIGURE 2 Functional graph of $145x^{137} + x$ over $G = \mathbb{F}_{389}^*/H$.

## 4. Future Directions

### 4.1. **Uniform distribution of value set.**

One necessary condition for a pseudorandom generator is that it should have uniform distribution. We first present a simple lemma to describe an elementary property of the distribution of $f(x) = cx^d + x \in \mathbb{F}_p[x]$.

**Lemma 4.1.** *For $f(x) = cx^d + x \in \mathbb{F}_p[x]$, if $d$ and $p$ are odd, then $|\{x \mid 1 \le f(x) \le (p-1)/2\}| = |\{x \mid (p-1)/2 + 1 \le f(x) \le (p-1)\}|$.*

*Proof.* If $d$ and $p$ are odd, then $H_p(d)$ is even, and by Lemma 3.2, the value set of $f$ is a union of cosets of $H$. For any element $x \in H$, $-x$ is also in $H$, because the order of $x$ is even. For any element $kx \in kH$, $-kx$ is also in $kH$, because $-1$ is in $H$. Therefore, multiplication by $-1$ is a bijection between $\{x \mid 1 \le f(x) \le (p-1)/2\}$ and $\{x \mid (p-1)/2 + 1 \le f(x) \le (p-1)\}$. □

This lemma could be generalized to other divisors of $H_p(d)$, and give us some information about how the value set of $f(x) = cx^d + x$ is distributed. We conjecture that the value set of $f(x) = cx^d + x \in \mathbb{F}_p[x]$ is "well-distributed" as $p$ grows large. To properly state "well-distributed", we use some notation from the theory of uniform distribution modulo one as in [KN74].

**Definition 4.2** ([KN74])**.** Let $x_1, \ldots, x_N$ be a finite sequence of real numbers, $A([\alpha, \beta); N) = |\{x_i \in [\alpha, \beta) \mid i \leq N\}|$. The number

$$D_N = D_N(x_1, \ldots, x_N) = \sup_{0 \leq \alpha < \beta \leq 1} \left| \frac{A([\alpha, \beta); N)}{N} - (\beta - \alpha) \right|$$

is called the *discrepancy* of the given sequence.

Using this language, our conjecture could then be formulated as followed:

**Conjecture 4.3.** *For $f(x) = cx^d + x \in \mathbb{F}_p$, consider $C = \{x \in \mathbb{F}_p \mid f(x) \neq 0\}$, denote its cardinality $N$. Construct the sequence $\omega_1, \ldots, \omega_N$, where $\omega_i = f(x_i)/p$ for $x_i \in C$. Then $D_N \to 0$ as $p \to \infty$.*

We exclude 0 because by Lemma 3.2, sometimes a coset of $H$ maps to 0, which is undesirable. We show some numerical evidence of this conjecture and its counterpart including 0. We computed an upperbound of $D_N$ as given by Theorem 2.5 of [KN74] for $p$ up to 349.

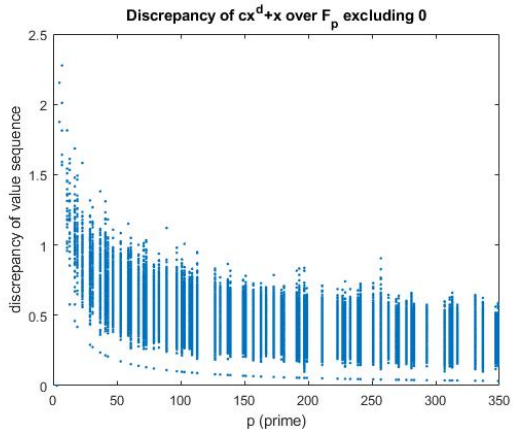


FIGURE 3 An upperbound for discrepancy for sequence $\omega_1, \ldots, \omega_N$.

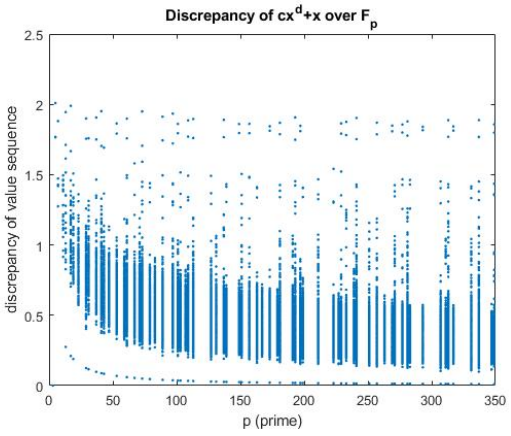


FIGURE 4 An upperbound for discrepancy for sequence $f(0)/p, f(1)/p, \ldots, f(p-1)/p$.

## 4.2. "Star graphs": $cx^d + x + 1$ for $cx^d + x$ with a coset of $H$ mapping to 0.

One interesting thing that happens when a coset of $H$ maps to 0 is that, since there is a degree preserving bijection from the functional graph of $cx^d + x$ to that of $cx^d + x + 1$ by taking $x$ to $x + 1$, 1 is an "attracting point" in the functional graph of $cx^d + x + 1$ when $H_p(d)$ is large. We illustrate this by an example:

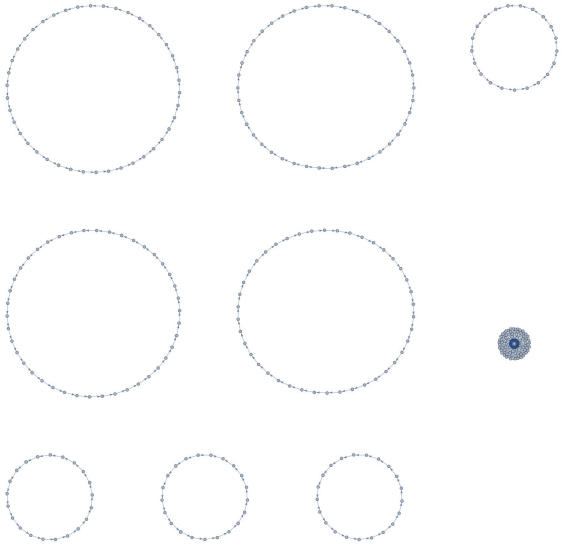

FIGURE 5 Functional graph of $148x^{85} + x$ over $\mathbb{F}_{337}$.

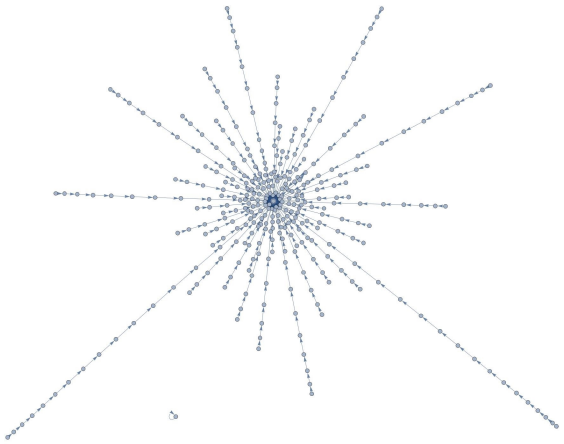

FIGURE 6 Functional graph of $148x^{85} + x + 1$ over $\mathbb{F}_{337}$.

The connected component containing 1 of the functional graph of $cx^d + x + 1$ in this case looks like a star, so we call functional graphs of such $cx^d + x + 1$ "star graphs" in this discussion. It should not be confused with stars in graph theory.

For each prime $p$ in $[10, 500]$, we chose $d$ randomly, and for each $c$ such that $cx^d + x$ has a coset of $H$ mapping to 0, we counted the number of cycles in the functional graph of $cx^d + x + 1$. We compare that with the average number of cycles in all trinomials of the form $cx^d + x + a$ for each $p$ and $d$ plotted against $H_p(d)$:

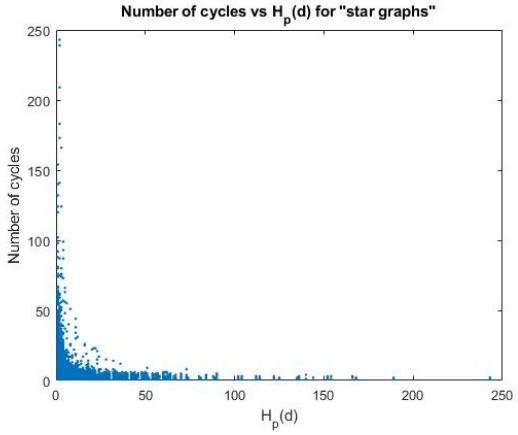


FIGURE 7 Number of cycles vs $H_p(d)$ for random samples of "star graphs".

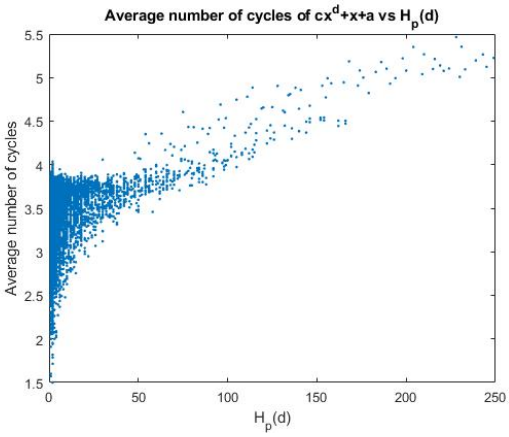


FIGURE 8 Average number of cycles vs $H_p(d)$ for every $p$ and $d$.

It appears that the number of cycles in "star graphs" decreases as $H_p(d)$ increases, and the opposite happens in the average case. Since every connected component has one cycle in it, and the vertex 1 in "star graphs" have in degree $H_p(d) + 1$, we expect to see fewer connected components, and therefore fewer cycles, as $H_p(d)$ increases.

### 4.3. **Lower bound on $\#V_f$.**

As shown in the proof of Theorem 3.7, $f(g^iH) = f(g^jH)$ if and only if $(cg^{i(d-1)} + 1)/(cg^{j(d-1)} + 1) \in g^{j-i}H$, which becomes an increasingly harsh condition on $c$ if we want multiple cosets of $H$ to have the same image under $f$. In the case of Proposition 3.1, it boils down to a bivariate polynomial $1 - c^2 = a^2$, which has $p - \sin(p\pi/2)$ roots by [AH18]. We hope that when $H_p(d)$ is small, the collection of conditions that $c$ has to satisfy to make many cosets of $H$ to have the same image under $f$ is too restrictive, which could potentially yield a lower bound on $\#V_f$.

### 4.4. **Generalization.**

Most of the results could be generalized to trinomials of the form $cx^d + bx + a$, yielding a slightly larger family of examples.

## Acknowledgement

This research was conducted as part of the NSF-funded REU at Texas A&M University (DMS-1757872). The author would like to thank Professor Maurice Rojas for his guidance and support throughout the project. The author would also like to thank Professor Michael Zieve for providing helpful comments.

## References

[AH18] Andreas Aabrandt and Vagn Lundsgaard Hansen. The circle equation over finite fields. *Quaest. Math.*, 41(5):665–674, 2018.

[BB13] Eric Bach and Andrew Bridy. On the number of distinct functional graphs of affine-linear transformations over finite fields. *Linear Algebra Appl.*, 439(5):1312–1320, 2013.

[BZ03] Richard P. Brent and Paul Zimmermann. Random number generators with period divisible by a Mersenne prime. In *Computational science and its applications—ICCSA 2003. Part I*, volume 2667 of *Lecture Notes in Comput. Sci.*, pages 1–10. Springer, Berlin, 2003.

[Hli10] Petr Hliněný. 20 years of Negami's planar cover conjecture. *Graphs Combin.*, 26(4):525–536, 2010.

[KN74] L. Kuipers and H. Niederreiter. *Uniform distribution of sequences*. Pure and Applied Mathematics. Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1974.