NUMBERS OF VALUES OF
POLYNOMIALS OVER FINITE
FIELDS

JIAOWEN YANG, AND MICHAEL E. ZIEVE

Abstract: Let $\mathbb{F}_q$ be a finite field of $q$ elements. For any polynomial $f \in \mathbb{F}_q[X]$, denote $\# f(\mathbb{F}_q)$ as the size of the value set of $f$. For any degree-$n$ polynomial $f(X) \in \mathbb{F}_q[X]$, we show that $\left| \frac{\# f(\mathbb{F}_q)}{q} - c \right| < \frac{d_n}{\sqrt{q}}$ where $d_n$ is a constant depending only on $n$ and where $c$ is a constant which can only take finitely many values for a given $n$ (even as $q$ and $f$ vary). Moreover, we list all the possibilities of $c$ when $f$ is indecomposable over $\mathbb{F}_q$ (i.e. $f$ cannot be written as a composition of two polynomials over $\mathbb{F}_q$ with degrees no less than 2) and $n$ is coprime to $2q$, not in $\{11, 23\}$ and cannot be written into the form $rd-1$ for any prime power $r$ and any integer $d > 1$.

Key-words: arithmetic monodromy group, geometric monodromy group, value set, Chebotarev density theorem, finite fields
Contents

1 Introduction 3
2 Galois-theoretic reformulation 5
3 Examples 7
4 Proof of the Value Set Formula 11
5 Constraints on the rational value c 17
6 Indecomposable Case 20
1 Introduction

Let $\mathbb{F}_q$ be a finite field of $q$ elements and let $X$ be transcendental over $\mathbb{F}_q$. For any polynomial $f \in \mathbb{F}_q(X)$, denote $\# f(\mathbb{F}_q)$ as the size of the value set of $f$.

An interesting problem is to determine the possibilities for $\# f(\mathbb{F}_q)$. The Lagrange interpolation formula shows that any function $\mathbb{F}_q \to \mathbb{F}_q$ is induced by a polynomial, so any subset of $\mathbb{F}_q$ occurs as the value set of some polynomial. However, if we restrict to polynomials of degree much less than $q$ then we obtain significant constraints on the value set. For instance, all degree-1 polynomials take $q$ values, and all degree-2 polynomials take roughly $q/2$ values (unless $q$ is even, when a degree-2 polynomial can take $q$ values). The following result of Birch and Swinnerton-Dyer [2] shows how this pattern extends to larger degrees:

**Theorem 1.1 (Value Set Formula).** For any integer $n \geq 1$, there exists a finite set $S(n)$ of rational numbers between 0 and 1 and a constant $d_n$ such that for every finite field $\mathbb{F}_q$ and every polynomial $f(X) \in \mathbb{F}_q[X]$ of degree $n$, we have
\[
\left| \frac{\# f(\mathbb{F}_q)}{q} - c \right| < \frac{d_n}{\sqrt{q}}
\]
for some element $c \in S(n)$.

In order to determine $\# f(\mathbb{F}_q)$ by applying the value set formula, we need to determine the $c$.

**Definition 1.1.** A non-constant polynomial $f$ in $\mathbb{F}_q[X]$ is decomposable if there exist two polynomials $g$ and $h$ in $\mathbb{F}_q[X]$ such that $f(X) = g(h(X))$ with $\deg(g) \geq 2$ and $\deg(h) \geq 2$. Otherwise, we call $f$ indecomposable.

Our main result is the following:

**Theorem 1.2.** Assume $f(X) \in \mathbb{F}_q[X]$ is an indecomposable polynomials of degree $n$ and $n$ is coprime to $2q$, not in $\{11, 23\}$ and cannot be written into the form $\frac{r^d-1}{r-1}$ for any prime power $r$ and any integer $d > 1$. Then the rational number $c$ in the value set formula has to be one of the following:

1. $1 - \frac{1}{2!} + \frac{1}{3!} - ... + (-1)^{n-1} \frac{1}{n!}$
2. $1 - \frac{1}{2!} + \frac{1}{3!} - ... + (-1)^{n-1} \frac{1}{(n-2)!}$ (if $n$ is a square in $\mathbb{F}_q$)
(3) \[1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-1} \cdot \frac{1}{(n-2)!} + \frac{2}{(n-1)!} \ (n \text{ is not a square in } \mathbb{F}_q)\]

(4) \[\frac{1}{(n, q-1)} \ (n \text{ is a prime})\]

(5) \[\frac{1}{(n, q+1)} + \frac{1}{(n, q-1)} \ (n \text{ is a prime})\]

Furthermore, all of these values occur for every such \(n\) and \(q\).

Remark. The assumption in our main theorem is not strong when \(q\) is much larger than \(n\). Denote \(I_n\) as the number of \(n\)-degree indecomposable polynomials in \(\mathbb{F}_q[X]\) and denote \(N_n\) as the number of all \(n\)-degree polynomials in \(\mathbb{F}_q[X]\). Bodin, Debes and Najib \([1]\) show that if \(n\) is coprime to \(q\), then \(\frac{I_n}{N_n}\) tends to 1 when \(q \to \infty\). That is to say, when \(q\) is large enough, almost all the degree-\(n\) polynomials are indecomposable over \(\mathbb{F}_q[X]\).

Remark. I will show in Lemma 2.3 that \(c(A, G)\) does not depend on the choice of generating coset.

The contents of this paper are as follows:

In the next section, we will give Galois-theoretic reformulation to the value set formula and show how to compute the rational number \(c\). This gives us a view of group theory to this problem which is important all over present paper.

In Section 3, we give some distinguished examples to illustrate the theorem. We will show that \(X^n\) and Dickson polynomials have the number \(c\) in the forth and fifth case in our main theorem, respectively.

In Section 4, we give the proof of the value set formula. The key strategy of the proof is to use Chebotarev density theorem.

In Section 5, we calculate the rational number \(c\) for most cases. We will show that these cases contributes to the first three cases in our theorem.

In Section 6, we focus on the case that \(f\) in indecomposable and \(n\) is coprime to \(q\), which makes huge constraints on the rational number \(c\). We can determine almost all the possibilities for \(c\) from the work of this section.
2 Galois-theoretic reformulation

Let us explain how to compute the rational number $c$ in the value set formula in terms of $f(x)$ and $q$. Assume $f$ is separable (i.e. assume $f(X) \notin \mathbb{F}_q(X^p)$ where $p$ is the characteristic of $\mathbb{F}_q$), denote $t = f(X)$ and let $\Omega$ be the Galois closure of $\mathbb{F}_q(X)/\mathbb{F}_q(t)$. And let $\mathbb{F}_q[t]$ be the algebraic closure of $\mathbb{F}_q$ in $\Omega$ and then let $A := Gal(\Omega/\mathbb{F}_q(t))$ and $G := Gal(\Omega/\mathbb{F}_q[t])$, which are known as the arithmetic monodromy groups and the geometric monodromy groups of $f$ respectively, viewed as groups of permutations of the set of roots of $f(X) - t$ [i.e. the set of conjugates of $X$ over $\mathbb{F}_q(t)$, or equivalently, the orbit of $X$ under $A$]. Noting that $A/G = Gal(\mathbb{F}_q[t]/\mathbb{F}_q)$ is cyclic, and picking any coset of $A/G$ which generates this cyclic group, and define $c(A,G)$ to be the proportion of elements in this coset which have at least one fixed point. And this ratio is exactly the number $c$.\[3\]

Remark. The results for inseparable polynomials follow from the separable case. Since $f$ is inseparable, we can always find an separable polynomial $g$ such that $f = g \circ X^p$ where $i$ is an integer. Note that $X^p$ acts as a permutation on $\mathbb{F}_q$, hence $f$ and $g$ has the same size of image set.

Actually, the value set formula is a consequence of a stronger result, we state it here as a theorem:

**Theorem 2.1.** For any specific polynomial $f(X) \in \mathbb{F}_q[X]$ of degree $n$ with $f'(X) \neq 0$, denote $g$ as the genus of the Galois closure of $\mathbb{F}_q(X)/\mathbb{F}_q(f(X))$, and $A, G$ as the arithmetic and geometric monodromy groups of $f$, respectively. Then

$$\left| \frac{\#(f(\mathbb{F}_q))}{q} - c(A,G) \right| \leq \frac{2g}{\sqrt{q}} + \frac{e_n}{q}$$

where $e_n$ is a constant depending only on $n$.

This implies the value set formula since we can bound $g$ in terms of $n$:

**Theorem 2.2.**

$$g \leq 1 + \frac{(\#G)(n-3)}{2} \leq 1 + \frac{(n!)(n-3)}{2}$$

**Proof.** See [10][Lemma 4.5] \[\Box\]

Note that $c(A,G)$ does not depend on the choice of coset. In fact, we have the following proposition
Lemma 2.3. If $G$ is a transitive subgroup of $S_n$, and $A$ is a group with $G \leq A \leq S_n$ such that $G$ is normal in $A$ and $A/G$ is cyclic, then for any two elements $a, b \in A$ such that $< aG > = < bG > = A/G$, the proportion of elements in $aG$ (or $bG$) which have a fixed point is the same as one another.

Proof. Choose two generators of $A/G$, $aG$ and $(aG)^k$ where $k$ is coprime to $r = [A : G]$. We claim that $(aG)^k = a^kG$. Actually, $(aG)^k \subseteq a^kG$ since $G$ is normal in $A$, and they are the same if and only if no two elements of $aG$ have the same $k$-th power as one another. Note that $a^{k+sG} = a^kG$ for any positive integers $s$. Note that $r|A|$ but $(k, r) = 1$, hence we can always find an integer $i$ such that $(k + ir, |A|) = 1$. We can now assume that $(k, |A|) = 1$. Then two elements of $aG$ have the same $k$-th power as one another if and only if they are the same. Hence the elements of $a^kG$ are precisely the elements $b^k$ with $b \in aG$, so since $b^k$ has at least as many fixed points as does $b$, we conclude that the proportion of elements with fixed points in $a^kG$ is at least as big as the proportion of elements with fixed points in $aG$. Conversely, we can do the same argument since we can find an integer $j$ such that $(a^k)^jG = aG$. Hence any two generating cosets of $A/G$ yield the same value for the proportion of elements with fixed points. \qed
3 Examples

We now illustrate the theorem for the following families of polynomials: $X^n$, Dickson polynomials, additive polynomials. For each family, we will compute $\# f(F_q)$ in two ways, via the value set formula and direct computation, and verify that the two results coincide. These three families of polynomials are important since the Galois closure of $F_q(x)/F_q(f(x))$ has genus 0.

Example 3.1. $X^n$

In this example, we assume $f(x) = x^n$ and calculate the size of value set.

If we compute via the main theorem, let us set $A = \text{Gal}(L/F_q(t))$, $G = \text{Gal}(L/F_q(t))$, where $L = F_q(x)$ and $x^n = t$.

Hence $A/G$ is isomorphic to $\text{Gal}(F_{q^r}/F_q)$ which is a r-cycle generated by $z \mapsto z^q$, then the number of generators of $A/G$ is $\phi(r) \cdot n$. Now if a generator $h \in A$ fixes some root, assume the root is $w^j x$, where $w$ is a primitive n-th root of unity and $h(z) = z^q$ for every $z$ in $F_{q^r}$, $h(x) = w^k x.$ (Note that $w \in F_{q^r}$) Hence we can get the following equality:

$$w^j x = h(w^j x) = w^{q^s j + k} x$$

which is equivalent to

$$j(q^s - 1) \equiv -k (\text{mod} n)$$

such $j$ exists if and only if

$$(q^s - 1, n) | k$$

That is to say, for given $s$ ( for a given coset of $G$ in $A$), the number of elements which fixes some root is $\frac{n}{(q^s - 1, n)}$. Hence we can compute

$$c(A,G) = \sum_{(s,r)=1}^{n} \frac{n}{(n,q^s-1)} \phi(r) \cdot n$$

Now if $d = (q^s - 1, n)$, since $n|(q^s - 1)$, both $s$ and $r$ are multiple of order of $q$ in $(\mathbb{Z}/d\mathbb{Z})^*$. Since $s$ and $r$ are coprime, we can imply that $d|(q-1)$ and consequently $(q^s - 1, n) = (q - 1, n)$. So

$$c(A,G) = \sum_{(s,r)=1}^{n} \frac{n}{(n,q-1)} \phi(r) \cdot n = \frac{1}{(n, q - 1)}$$

If we compute directly, $f(x)$ fixes 0 and is a homomorphism $F_q^* \to F_q^*$ whose kernel consists of the n-th roots of unity in $F_q^*$, hence the kernel has size $(n, q - 1)$, so the number of values is $1 + \frac{(q-1)}{(n,q-1)}$.

Those two results are coincident.
Example 3.2. Dickson polynomials

In this example, we assume \( f(x) = D_n(X, a) \), which is uniquely determined by the functional equation \( D_n(y + \frac{a}{y}, a) = y^n + \left( \frac{a}{y} \right)^n \).

Firstly, we give some definitions. Let \( x \) be a transcendental element over \( \mathbb{F}_q \), \( a \in \mathbb{F}_q \) and \( t = D_n(x, a) \). Put \( x = y + \frac{a}{y} \).

In fact, all the \( n \) roots of \( D_n(X, a) = t \) are \( zy + \frac{a}{zy} \), where \( z^n = 1 \). \( G \) consists of the following automorphisms: \( y \mapsto zy \) and \( y \mapsto \frac{za}{y} \) where \( z^n = 1 \). Assume \( z \) is the \( n \)-th primitive unit root. \( A \) is generated by \( G \) and \( \text{Gal}(\mathbb{F}_q(z)/\mathbb{F}_q) \). (Here we assume that \( k(y) \) is the Galois closure of \( \mathbb{F}_q(x)/\mathbb{F}_q(t) \) where \( k = \mathbb{F}_q(z) \)).

Now we can do the computation for \( c(A, G) \). Set \( r \) be the order of \( q \) in \((\mathbb{Z}/n\mathbb{Z})^*\), hence \( \text{Gal}(\mathbb{F}_q(z)/\mathbb{F}_q) \) is an \( r \)-cycle. The number of the generators of \( A/G \) is \( \varphi(r) \cdot 2n \). There are two kinds of elements in \( A \), one maps \( y \) to \( z^i y \) and the other to \( az^j/y \) where \( i = 1, 2, \ldots n \).

If one of the first kind elements fixes some root, we denote the element to be \( h \) where \( h(y) = z^i \cdot y \) with \( 1 \leq i \leq n \) and \( h(z) = z^n \) with \( 1 \leq s \leq r \) and the root to be \( z^j y + \frac{a}{z^j y} \) for some \( 1 \leq j \leq n \). We can deduce that

\[
z^j y + \frac{a}{z^j y} = h(z^j y + \frac{a}{z^j y}) = z^{n^s} z^{j+i} y + \frac{a}{z^{n^j} y^{j+i}}
\]

Then we have

\[
n|(q^n - 1)j + i
\]

For fixed \( s \), we have \( \frac{n}{(n,q^n-1)} = \frac{n}{(n,q-1)} \) choices. (Note that \( s \) is coprime with \( r \)). Hence for the first kind, we have totally \( \varphi(r) \frac{n}{(n,q^n-1)} \) elements that fixes some root and is a generator in \( A/G \) as well.

If the second kind elements fixes some root, we denote the element to be \( h \) where \( h(y) = z^i a/y \) with \( 1 \leq i \leq n \) and \( h(z) = z^s \) with \( 1 \leq s \leq r \) and the root to be \( z^j y + \frac{a}{z^j y} \) for some \( 1 \leq j \leq n \). We can deduce that

\[
z^j y + \frac{a}{z^j y} = h(z^j y + \frac{a}{z^j y}) = \frac{z^{n^s} z^{j+i} a}{y} + \frac{y}{z^{n^j} y^{j+i}}
\]

Then we have

\[
n|(q^n + 1)j + i
\]

For fixed \( s \), we have \( \frac{n}{(n,q^n+1)} \) choices. Now we want to figure out what \( (n,q^n+1) \) is.

We claim that \( (n,q^n+1) = (n,q+1) \) for odd \( s \) and \( (n,q^n+1) = (n,2) \) for even \( s \). In fact, denote \( d = (n,q^n+1) \), then \( q^n \equiv -1 \mod d \). Set \( m \) to
be the smallest integer such that \( q^m \equiv -1 \mod d \). Note that \( q^r \equiv 1 \mod d \) so we can conclude that \( s \) equals \( m \) times an odd number and \( r \) equals \( m \) times an even number. Since \((s, r) = 1\), \( m \) has to be 1. That is to say, \( d|(n, q + 1) \). If \( s \) is odd, we have \((n, q^s + 1) = (n, q + 1) \). If \( s \) is even, we have \((n, q^s + 1) = (n, q + 1) \)(here we assume \( q \) is odd). Futhermore, when \( q \) is odd, \((n, q + 1) = (n, 2) \). Since \((n, q^s + 1) | q^r - 1\), any divisor \( d \) of \((n, q + 1) \) satisfies \( q^r \equiv -1 \mod d \) and \( q^r \equiv 1 \mod d \), so 1 \( \equiv q^r \equiv (-1)^r \equiv -1 \mod d \), whence \( d|2 \).

Now we can conclude that

\[
c(A, G) = \left( \frac{1}{(n, q + 1)} + \frac{1}{(n, q - 1)} \right) / 2
\]

If we compute directly, we can find \( q - 1 \) elements in \( \mathbb{F}_q \) and \( q + 1 \) elements in \( \mathbb{F}_{q^2} \) satisfy that \( r + \frac{\alpha}{\gamma} \in \mathbb{F}_q \). Suppose \( r_1 \) and \( r_2 \) are among the \( 2q \) elements and satisfy that

\[
r_1^n + a^{rn} = r_2^n + a^{rn}
\]

We can easily know that the equation holds if and only if \( r_1 = r_2 \ast z \) or \( r_1 = r_2 \ast z \ast w \) where \( z^n = 1 \). Hence, for given \( r \) in \( \mathbb{F}_q \), set \( w = (n, q - 1) \) and we can find \( 2w \) elements: \( zr \) and \( \frac{a}{\gamma} \) which share the same value under \( D(y + \frac{a}{y}, a) \) (Here \( z \) satisfies that \( z^n = 1 \) and \( z^q = 1 \), which has \( w \) choices). Hence the number of values under \( D(y + \frac{a}{y}, a) \) for the \( q - 1 \) choices in \( \mathbb{F}_q \) is \( \frac{(q-1)}{2(n, q-1)} \). For the same reason, the number of values under \( D(y + \frac{a}{y}, a) \) for the \( q + 1 \) choices in \( \mathbb{F}_q^2 \) is \( \frac{(q+1)}{2(n, q+1)} \). Hence the size of value set is \( \frac{(q-1)}{2(n, q-1)} + \frac{(q+1)}{2(n, q+1)} \).

These two results are coincident.

**Example 3.3. Additive polynomials**

If a polynomial \( f = \sum a_i x^p \) where \( p \) is the characteristic of \( \mathbb{F}_q \), we call \( f \) additive polynomial. Note that additive polynomials are linear. Hence the roots of \( f \) form an additive group. Denote \( \Gamma \) as the set of the roots and \( Y \) as a root of \( f(x) = t \). Then \( G \) consists of maps: \( \tau_v : Y \rightarrow Y + v(v \in \Gamma) \) and \( A \) is generated by \( G \) and \( \sigma \), which fixes \( Y \) and acts as the Frobenius map on \( \mathbb{F}_{q^r} \).

Now let us compute the value \( c(A, G) \). Choose a generating coset \( \sigma G \), then the denominator is \( \#|G| \). We need to count the number of elements \( \tau_v \in G \) such that \( \sigma \tau_v \) fixes at least one root \( Y + \gamma_i \). Note that

\[
\sigma \tau_v(Y + \gamma_i) = \tau_v \sigma(Y + \gamma_i) = Y + v^q + \gamma_i^q
\]

These two results are coincident.
Then if $\tau_v$ fixes $Y + \gamma_i$, we can deduce that

$$v = \gamma_i^{\frac{1}{q}} - \gamma_i$$

Next, we just need to know when two roots $\gamma_i, \gamma_j$ of $f$ satisfy

$$\gamma_i^{\frac{1}{q}} - \gamma_i = \gamma_j^{\frac{1}{q}} - \gamma_j$$

This is equivalent to

$$\gamma_i^{\frac{1}{q}} - \gamma_j^{\frac{1}{q}} = \left(\gamma_i^{\frac{1}{q}} - \gamma_j^{\frac{1}{q}}\right)^q$$

which is equivalent to

$$\gamma_i^{\frac{1}{q}} - \gamma_j^{\frac{1}{q}} \in \mathbb{F}_q$$

which is equivalent to

$$\gamma_i - \gamma_j \in \mathbb{F}_q$$

Since $\gamma_i - \gamma_j$ is also a root of $f$, then the above is equivalent to $\gamma_i - \gamma_j \in \ker(f)$. Thus the number of elements $\tau_v \in G$ such that $\sigma \tau_v$ fixes at least one root $Y + \gamma_i$ is exactly $\frac{\#(G)}{\ker(f)}$. Hence

$$c(A, G) = \frac{1}{\#(\ker(f))}$$

Note that $f$ is a linear map from $\mathbb{F}_q$ to itself. Hence $\#(f(\mathbb{F}_q)) = \frac{q}{\#(\ker(f))}$ which is coincident with the value $c$. 

10
4 Proof of the Value Set Formula

In this section I will prove Theorem 2.1, which in turn implies Theorem 1.1.

We want a formula for

$\# f(F_q) = \# \{ c \in F_q | f^{-1}(c) \text{ has at least one point in } F_q \}$

Firstly, let us control the set $f^{-1}(c)$ in terms of decomposition and inertia groups. Recall some definitions here.

**Definition 4.1.** We consider $F'/F$ a Galois extension of algebraic function fields with $G$ its Galois group. Let $P$ be a place of $F$ and $P'$ be an extension of $P$ to $F'$. Define $D(P'|P) := \{ \sigma \in G | \sigma(P') = P' \}$ the decomposition group of $P'$ over $P$ and $I(P'|P) := \{ \sigma \in G | v_{P'}(\sigma z - z) > 0 \text{ for all } z \in O_{P'} \}$ the inertial group of $P'$ over $P$, where $O_{P'}$ is the valuation ring of the place $P$.

Denote $\Omega$ as the Galois closure of $F_q(x)/F_q(f(x))$, and for each $c \in F_q$, denote $Q_c$ as the place of $F_q(x)$ which contains $f(x) - c$ and $P_c$ as any place of $\Omega$ which lies over $Q_c$. Denote $f(P_c/Q_c)$ as the relative degree of $P_c$ over $Q_c$.

**Lemma 4.1.** The size of the set $F_q \cap f^{-1}(c)$ is equal to the number of places $R$ of $F_q(x)$ over $Q_c$ with $f(R/Q_c) = 1$

**Proof.** Since $Q_c$ is a degree one place of $F_q(f(x))$, $f(R/Q_c) = 1$ is equivalent with $R$ is a degree one place of $F_q(x)$. All the degree one places of $F_q(x)$ are the places $P_{x-\alpha}$ (where $\alpha$ is an element of $F_q$) and the infinite place $P_{\infty}$. [11][Theorem 1.2.2]. Since $P_{x-\alpha} \cap F_q(f(x)) = P_{f(x)-f(\alpha)}$, then $P_{x-\alpha}$ is over $Q_c$ if and only if $f(\alpha) = c$. \[ \square \]

Choose a place $Q$ of $\Omega$ over $P_c$. Denote $D(Q)$ and $I(Q)$ as the decomposition and inertia group of $Q/Q_c$ respectively. Denote $G$ as the Galois group of $\Omega/F_q(f(x))$ and denote $H$ as the set of embeddings of $F_q(x)$ in $\Omega$. Due to van der Waerden [16], we claim that:

**Lemma 4.2.** The set of places of $F_q(x)$ which contain $Q_c$ is in bijection with the set of orbits of $D(Q)$ (acts on the left coset of $G/H$ where $\sigma(qH) = (\sigma q)H$ for $\sigma \in D(Q)$ ), and this bijection can be chosen so that a place $R$ of $F_q(x)$ corresponds to a $D(Q)$-orbit which is the union of $f(R/Q_c)$ $I(Q)$-orbits, where each $I(Q)$-orbit has size $e(R/Q_c)$. 11
Proof. Since $G$ is Galois, for any place $\hat{Q}$ of $\Omega$ over $Q_c$, there exists an element $g$ of $G$ such that $g(Q) = \hat{Q}$. On the other hand, for any $g \in G$, $g(Q) \cap \mathbb{F}_q(x)$ is a place of $\mathbb{F}_q(x)$ over $Q_c$. Hence, all the places of $\Omega$ over $Q_c$ is exactly the set $\{g(Q)|g \in G\}$.

We claim that the set of places of $\mathbb{F}_q(x)$ over $Q_c$ is in bijection with the set $\{DgH|g \in G\}$ where $D = D(Q)$. In fact, for given $g, g' \in G$

\[g(Q) \cap \mathbb{F}_q(x) = g'(Q) \cap \mathbb{F}_q(x)
\]

$\iff \exists h \in H$ such that $hg(Q) = g'(Q)$

$\iff (g')^{-1}hg$ fixes $Q$

$\iff (g')^{-1}hg \in D$

$\iff Dg^{-1}h^{-1} = D(g')^{-1}$

$\iff Dg^{-1}H = D(g')^{-1}H$

Hence $Dg^{-1}H$ is linked with the place $g(Q) \cap \mathbb{F}_q(x)$.

We claim that the size of (in this lemma, we count for the number of cosets) $Dg^{-1}H$ equals to $e(R/Q_c)f(R/Q_c)$ where $R$ is the place linked with $Dg^{-1}H$.

Let $R = g(Q) \cap \mathbb{F}_q(x)$, then

\[e(R/Q_c) = \frac{e(g(Q)/Q_c)}{e(g(Q)/R)} = \frac{\# |gIg^{-1}|}{\# |H \cap gIg^{-1}|}\]

where $I = I(Q|Q_c)$. Since

\[f(R/Q_c) = \frac{f(Q/Q_c)}{f(Q/R)} = f(Q/Q_c) \frac{\# |H \cap gIg^{-1}|}{\# |H \cap gDg^{-1}|}\]

We can conclude that

\[e(R/Q_c)f(R/Q_c) = \frac{f(Q/Q_c)e(g(Q)/Q_c)}{\# |H \cap gDg^{-1}|} = \frac{\# |gDg^{-1}|}{\# |H \cap gDg^{-1}|}\]

On the other hand, we claim that for any $g \in G$, the size of $Dg^{-1}H$ is $e(R/Q_c)f(R/Q_c)$. In fact, $Dg^{-1}H$ is a subset of $G/H$ and $D$ acts transitively on it, hence

\[\# |Dg^{-1}H| = \frac{\# D}{\# \text{stab}(g^{-1}H)}\]
where $\text{stab}(g^{-1}H)$ is the stabilizer of $g^{-1}H$ in $D$ which is $\{d \in D | dg^{-1}H = g^{-1}H \}$. Since $dg^{-1}H = g^{-1}H \Leftrightarrow gdg^{-1} \in H \Leftrightarrow d \in g^{-1}Hg$, hence $\#\text{stab}(g^{-1}H) = \#(D \cap g^{-1}Hg) = \#(H \cap gdg^{-1})$. Since $\#D = \#gDg^{-1}$, we conclude that the size of the orbit $Dg^{-1}H$ is $\frac{\#|gDg^{-1}|}{\#|H \cap gdg^{-1}|}$ which is coincident with $e(R/Q_c)f(R/Q_c)$.

Finally, $Dg^{-1}H$ is the union of $I(Q/Q_c)$-orbits since $I$ is a normal subgroup in $D$. For any $g \in G$,

$$\#|Ig^{-1}H| = \frac{\#|gIg^{-1}|}{\#|H \cap Ig^{-1}|} = e(R/P)$$

then $Dg^{-1}H$ is the union of $f(R/P)I(Q/Q_c)$-orbits. \qed

In particular, there is a place $R$ of $\mathbb{F}_q(x)$ over $Q_c$ with $f(R/Q_c) = 1$ if and only if $D(Q)$ and $I(Q)$ have a common orbit. Thus, together with lemma 3.1, implies the following proposition:

**Proposition 4.3.** The number of points in $\mathbb{F}_q \cap f^{-1}(c)$ equals the number of common orbits of $D(Q)$ and $I(Q)$. Hence,

$$\#f(\mathbb{F}_q) = \#\{c \in \mathbb{F}_q | \text{for every choice of } Q, D(Q) \text{ and } I(Q) \text{ have at least one common orbit}$$

**Remark.** In fact, it does not depend on the choice of $Q$, since for a different choice, we just replace $D$, $I$ by $gDg^{-1}$, $gDg^{-1}$ respectively. This replacement will not change the fact whether $D$ and $I$ have common orbits.

Next, we show when $D(Q)$ and $I(Q)$ have at least one common orbit. Recall some facts of these two groups. The algebraic closure of $\mathbb{F}_q$ in $\Omega$ is exactly $\mathbb{F}_{q^r}$ where $r = [A : G]$. The group $I(Q)$ is a normal subgroup of $D(Q)$ and the quotient group $D(Q)/I(Q)$ is isomorphic to the Galois group of the extension of residue fields (namely, the residue field of $Q$ as an extension of the residue field of $Q_c$, where the latter field is $\mathbb{F}_q$ and the former field contains $\mathbb{F}_{q^r}$) \cite{11}[Theorem 3.8.2(c)]. In particular, $D(Q)/I(Q)$ is a finite cyclic group, and it has a distinguished generating coset $aI(Q)$ consisting of the elements which act as $q$-th powering on the residue field of $Q$. This is called the Frobenius coset since its elements act as the “Frobenius map”, namely $q$-th powering. Note that the Frobenius coset generates $A/G$ which is isomorphic to $\mathbb{F}_q(t)/\mathbb{F}_{q^r}(t)$. Then we have the following proposition:

**Proposition 4.4.** $D(Q)$ and $I(Q)$ have at least one common orbit if and only if the Frobenius coset has a fixed point on the space of orbits.
Due to the work of Chebotarev \[10\], we have the following theorem:

**Theorem 4.5.** For any element $a$ in $A$ which generates $A/G$, the number of places $P$ of $\Omega$ which lie over a degree-one place of $\mathbb{F}_q(f(x))$ (call it $Q$) and for which the decomposition group $D(P/Q)$ contains $a$ and also $aI(P/Q)$ is the Frobenius coset of $D(P/Q)/I(P/Q)$ equals the number of degree-one places on a certain function field over $\mathbb{F}_q$ which has the same genus as $\Omega$.

**Remark.** In fact this function field can be explicitly described: let $s$ be the order of $a$, and let $\Gamma$ be the field generated by $\Omega$ and $\mathbb{F}_{q^s}$. Extend $a$ to an automorphism of $\Gamma$ which acts as $q$-th powering on $\mathbb{F}_{q^s}$ and there is a unique way to do this. Then the function field in the theorem is the subfield $\Delta$ of $\Gamma$ fixed by this extension of $a$. Thus, $\Delta$ has the property that $\Delta \mathbb{F}_{q^s} = \Omega \mathbb{F}_{q^s}$. So we know a lot more than just that $\Delta$ and $\Omega$ have the same genus – they have all the same geometric properties.

We have a good estimate for the number of degree-one places on a genus-$g$ function field:

**Theorem 4.6 (Hasse-Weil Bound).** For any genus-$g$ function field $F$ over $\mathbb{F}_q$, denote $N$ as the number of degree-one places of $F$, then

$$q + 1 - 2g \sqrt{q} \leq N \leq q + 1 + 2g \sqrt{q}$$

**Proof.** See [11][Corollary 5.2.3]

Note Chebotarev counts places of $\Omega$ with certain properties, and we need to count places of $\mathbb{F}_q(f(x))$ with those properties. Thus, we need to count the number of places of $\Omega$ which lie over a specific degree-one place $Q$ of $\mathbb{F}_q(f(x))$. Note that all places $P$ of $\Omega$ which lie over $Q$ have the same value of $e(P/Q)$ as one another [call this common value $e$], and also the same value of $f(P/Q)$ as one another [call this common value $m$], and then the number of places $P$ of $\Omega$ which lie over $Q$ equals $(\#A)/(em)$. To apply this, we need to control $e$ and $m$. We know that $em$ is the size of the decomposition group $D(P/Q)$ for any choice of $P$. But the possible values of $e$ will depend on the specific polynomial $f$. For a place $Q$ for which $e = 1$, the number $f$ will be the order of the Frobenius element of any of these places $P$. So we should take a weighted sum where we divide each expression by $(\#A)/\# < a >$. Doing this gives an expression for

$$\sum_{a \in A, <aG>=A/G, a \text{ has at least one fixed point}} \frac{N_a}{\#A/\# < a >}$$

where $N_a$ denotes the number of places $P$ of $\Omega$ which lie over a degree-one place of $\mathbb{F}_q(f(x))$ and whose Frobenius coset contains $a$.  

14
Let’s split this up as the sum of two sums, one counting places $P$ which
don’t ramify over $\mathbb{F}_q(f(x))$ and the other counting places which do ramify.
The latter sum will wind up being part of the error term. The main con-
tribution comes from the sum over places which don’t ramify. That sum
equals the number of degree-one places of $\mathbb{F}_q(f(x))$ which don’t ramify in
$\mathbb{F}_q(x)/\mathbb{F}_q(f(x))$ and which lie under a place of $\Omega$ whose decomposition group
has at least one fixed point, which is the same thing as the number of points
in $f(\mathbb{F}_q)$ which don’t have any ramified preimages under $f$.

Putting the above together gives an expression for $\#f(\mathbb{F}_q)$ which has two
types of error terms: first, the error terms coming from Weil’s estimate for
the number of degree-one places on the various function fields arising in the
Chebotarev expressions for the different choices of $a$. These have the form
$2g\sqrt{q}$ where $g$ is the genus of Omega, and one can bound $g$ in terms of the
polynomial degree $n$. The second type of error term in the expression for
$\#f(\mathbb{F}_q)$ comes from points in $f(\mathbb{F}_q)$ which have ramified preimages under $f$.
Since if $f$ is a degree-$n$ polynomial then there are at most $n - 1$ elements of
$\mathbb{F}_q$ which have a ramified preimage under $f$ (namely the images of the roots of
the derivative).

Let us show that the contribution that these points make to the big
summation above is bounded by a function of $n$. That contribution is:

$$\sum_{a\in A, <aG> = A/G, a \text{ has at least one fixed point}} \frac{M_a}{\# A/\# <a>}$$

where $M_a$ denotes the number of places $P$ of $\Omega$ which lie over a degree-one
place of $\mathbb{F}_q(f(x))$ and whose Frobenius coset contains $a$ for which $P$ ramifies
over $\mathbb{F}_q(f(x))$.

Now, for any fixed degree-one place $Q$ of $\mathbb{F}_q(f(x))$, pick a place $P$ over $\Omega$
and let $e = e(P/Q)$ and $m = f(P/Q)$, and note that $e$ and $m$ do not depend
on the choice of $P$. So, as above, the number of such places $P$ is $(\#A)/(em)$.
Moreover, $m$ divides $\# <a>$ for any element $a$ in the Frobenius coset, and
also $\# <a> \leq em$ since $em$ is the size of $D(P/Q)$. Since $\#I(P/Q) = e$, for
any place $P$ the size of the Frobenius coset is $e$. So each of these $(\#A)/(em)$
places $P$ occurs in the above summation for at most $e$ distinct values $a$.

Also, when a place $P$ occurs in the summation for a given $a$, it contributes
$1/(\#A/\# <a>) \leq 1/(\#A/(em))$. Thus, for each fixed $Q$, the contribution
that places over $Q$ make to the above summation is at most $(\#A)/(em) * 
1/(\#A/(em)) = e$. Finally, we know that $e \leq \#A \leq n!$ and also that there
are at most \( n - 1 \) degree-one places \( Q \) which have ramified preimages under \( f \), so we get a bound that only depends on \( n \).

Remark. All of the above works for rational functions as well, see [12]. Actually the exact same proof works for maps between curves, meaning, extensions of arbitrary function fields \( L/M \) (not just extensions \( F_q(x)/F_q(f(x)) \)).
5 Constraints on the rational value $c$

In this section, we will calculate $c(A, G)$ when the pair $(A, G)$ is $(S_n, S_n)$, $(S_n, A_n)$ or $(A_n, A_n)$. Note that the only normal subgroups of $S_n$ for $n \geq 5$ are $S_n$, $A_n$ and the trivial group (only contains identity). Hence if $A = S_n$, then $G = S_n$ or $A_n$. The following result of Kenneth Williams [17] implies that in most cases, the value $c$ coincident with the case when the pair $(A, G)$ is $(S_n, S_n)$.

**Theorem 5.1.** A polynomial $f$ is called a general polynomial if its $c(A, G) = 1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-1}\frac{1}{n!}$, denote $N$ as the number of degree-$n$ general polynomials which is monic and constant term 0. Then

$$N = q^{n-1} + O(q^{n-2})$$

The $O$-symbol depends only on $n$.

Since there are $q^{n-1}$ monic polynomials with 0 constant in total, the theorem implies that for a fixed $n$, most polynomials are general polynomials. This really make sense. Denote $N_i$ as the number of $i$-element subsets of $\#f(\mathbb{F}_q)$ with the same image under $f$. If we choose $f$ randomly, $N_i$ should mostly be

$$\frac{\binom{q}{i}}{q^{i-1}} = \frac{q!}{i!(q-i)!q^{i-1}} = \frac{q}{i!} + O(1)$$

Then

$$\#f(\mathbb{F}_q) = \sum_{i=1}^{n} (-1)^{i-1}N_i = q(1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-1}\frac{1}{n!}) + O(1)$$

if $q$ is large enough to $n$.

On the other hand, we have the following theorem:

**Theorem 5.2.** If $A = G = S_n$, then $c(A, G) = 1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-1}\frac{1}{n!}$.

If $A = S_n$ and $G = A_n$, $c(A, G) = 1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-1}\frac{1}{(n-2)!}$.

If $A = G = A_n$, $c(A, G) = 1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-3}\frac{1}{(n-2)!} + \frac{2}{(n-1)!}$.

**Proof.** When $(A, G)$ is $(S_n, S_n)$, then the size of coset which generates $A/G$ is just $n!$ (the size of $S_n$). For calculating the value of $c$, we just need to know how many elements of $S_n$ have fixed points. Denote $N(r)$ as the number of elements of $S_n$ which have at least $r$ fixed points. Actually, $N(r)$ is not
exactly the number since we will count \( \binom{m}{r} \) times in \( N(r) \) for an element who has exactly \( m \) fixed points, but it does not matter since finally we will count the element exactly 1 time for the reason of the following equality:

\[
\binom{m}{1} - \binom{m}{2} + \binom{m}{3} - \ldots + (-1)^{m-1}\binom{m}{m} = 1
\]

And we can deduce that

\[
N(r) = \binom{n}{r} (n - r)! = \frac{n!}{r!}
\]

Denote \( \lambda(n) \) the number of elements of \( S_n \) which have fixed points, then we can deduce that

\[
\lambda(n) = \sum_{i=1}^{n} (-1)^{i-1} N(i) = n! \cdot (1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-1}\frac{1}{n!})
\]

Hence, \( c(S_n, S_n) = 1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-1}\frac{1}{n!} \)

When \((A, G)\) is \((S_n, A_n)\), then the size of coset which generates \( A/G \) is \( \frac{n!}{2} \) (the size of \( S_n - A_n \)). Actually, the coset consists of odd transform of \( S_n \).

Similarly, denote \( N(r) \) as the number of elements of the coset which have at least \( r \) fixed points. If \( r \leq n - 2 \), then we can determine that the restriction of the element acts as odd transformation on the rest \( n - r \) points, hence

\[
N(r) = \binom{n}{r} \cdot \frac{(n - r)!}{2}
\]

However, it obvious that \( N(n - 1) = N(n) = 0 \). Hence

\[
\lambda(n) = \sum_{i=1}^{n} (-1)^{i-1} N(i) = \frac{n!}{2} \cdot (1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-3}\frac{1}{(n-2)!})
\]

and

\[
c(S_n, A_n) = 1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-1}\frac{1}{(n-2)!}
\]

When \((A, G)\) is \((A_n, A_n)\), then the size of coset which generates \( A/G \) is \( \frac{n!}{2} \) (the size of \( A_n \)). Denote \( N(r) \) as the number of elements of the coset which have at least \( r \) fixed points. If \( r \leq n - 2 \), then we can determine that
the restriction of the element acts as even transformation on the rest \( n - r \) points, hence

\[
N(r) = \binom{n}{r} \cdot \frac{(n-r)!}{2}
\]

And \( N(n-1) = (n-1) \) and \( N(n) = 1 \), then we can deduce that

\[
\lambda(n) = \sum_{i=1}^{n} (-1)^{i-1} N(i) = \frac{n!}{2} \cdot (1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-3} \frac{1}{(n-2)!} + \frac{2}{(n-1)!})
\]

and

\[
c(A_n, A_n) = 1 - \frac{1}{2!} + \frac{1}{3!} - (-1)^{n-3} \frac{1}{(n-2)!} + \frac{2}{(n-1)!}
\]
6 Indecomposable Case

In this section, we will focus on the case of \( f \) indecomposable and its degree \( n \) coprime to \( q \). We will get big constraints on \( A \) and \( G \) and \( c \) as well. We will give constraints on \( n \) if both \( A \) and \( G \) are subsets of \( A_n \).

**Theorem 6.1.** A and \( G \) are arithmetic and geometric monodromy groups of \( f \).
1. If \( \gcd(n, q) = 1 \), then \( G \) contains an \( n \)-cycle.
2. If \( f \) is indecomposable over \( \mathbb{F}_q \), then \( A \) is a primitive subgroup of \( S_n \).
3. If \( f \) is indecomposable over \( \mathbb{F}_q \), then \( f \) is indecomposable over \( \overline{\mathbb{F}}_q \) (the algebraic closure of \( \mathbb{F}_q \)). Hence \( G \) is also a primitive subgroup of \( S_n \).

**Proof.** (1) See [15][Lemma 3.3]
(2) Recall the definition: a permutation group \( A \) acting on a set \( X \) is called primitive if \( A \) acts transitively on \( X \) and \( A \) preserves no nontrivial partition of \( X \). If \( A \) is not primitive, then we can find a field between \( \mathbb{F}_q (x) \) and \( \mathbb{F}_q (\nu(x)) \). And L"uroth theorem implies that the middle field is generated by an element in \( \mathbb{F}_q (x) \) which contradicts with \( f \) indecomposable.
(3) If \( f \) is decomposable over \( \mathbb{F}_q \), suppose \( g, h \in \mathbb{F}_q [x] \) satisfy \( f = g \circ h \).
We may assume \( h \) monic and \( h(0) = 0 \) since for any degree-1 polynomial \( \mu \in \mathbb{F}_q [x] \), \( f = (g \circ \mu^{-1}) \circ (\mu \circ h) \). Then the leading coefficient of \( g \) equals to that of \( f \), which is in \( \mathbb{F}_q^* \). Comparing coefficients of \( x^{n-i} \), \( i = 1, 2, ..., \deg(h) - 1 \), we can conclude that coefficients of \( x^{\deg(h)-i} \) in \( h(x) \) is in \( \mathbb{F}_q \). Then comparing coefficients of \( x^{\deg(h)-i} \) in \( g(x) \) is in \( \mathbb{F}_q \). That contradicts to \( f \) indecomposable.

If \( f \) is indecomposable and \( n \) coprime to \( q \), we can deduce that \( A \) primitive and contains an \( n \)-cycle. McSorley [15] shows the following theorem:

**Theorem 6.2.** A primitive subgroup \( G \) of \( S_n \) contains an \( n \)-cycle if and only if one of the following holds:
1. \( G = A_n \) (with \( n \) odd) or \( G = S_n \)
2. \( PGL_d(r) \leq G \leq PTL_d(r) \), where \( r \) is a prime power and \( n = \frac{r^d-1}{r-1} \).
3. \( C_p \leq G \leq AGL_1(p) \) where \( n = p \) is a prime
4. \( PSL_2(11) \) (with \( n = 11 \)) or \( M_{11} \) (with \( n = 11 \)) or \( M_{23} \) (with \( n = 23 \)).

Combining Theorem 6.1 and 6.2, we can deduce the following theorem:

**Theorem 6.3.** If \( n \) is coprime to \( q \), then every indecomposable degree-\( n \) polynomial over \( \mathbb{F}_q \) has geometric monodromy group being either
1. \( A_n \) (with \( n \) odd) or \( S_n \)
(2) a group between $PGL_d(r)$ and $PΓL_d(r)$, where $n = \frac{r^d - 1}{r - 1}$.
(3) cyclic of order $n$ (with $n$ prime)
(4) dihedral of order $2n$ (with $n$ an odd prime)
(5) $PSL_2(11)$ (with $n = 11$) or $M_{11}$ (with $n = 11$) or $M_{23}$ (with $n = 23$).

Note that the only polynomials in (3) are $x^n$ composed with degree-1 polynomials, and the only polynomials in (4) are $D_n(x, a)$ composed with degree-1 polynomials. We will also explore more on the case that $G = A_n$.

Theorem 6.4. Let $K$ be a field of characteristic $p$ where $p \neq 2$, $f(x) \in K[x]$ be a polynomial of degree $n$ where $n$ is coprime with $p$, with $A$ and $G$ the arithmetic and geometric monodromy group of $f$, respectively. Suppose that $G \subseteq A_n$. Then $n$ is odd, and $A \subseteq A_n$ if and only if $(-1)^{n-1}n$ is a square in $K$.

Peter Müller [13] proved the case of field of characteristic 0, but we find that it also works for the finite field case.

Proof. Let $x_1, x_2, ..., x_n$ be the roots of $f(X) - t$, and $y_1, y_2, ..., y_n$ be the roots of $f'(X)$. Without loss assume that $f$ is monic, hence $f'(X) = n \prod (X - y_k)$. From $f'(X) = \sum_j \prod_{i \neq j} (X - x_i)$ one obtains $f'(x_j) = \prod_{i \neq j} (x_j - x_i)$. Hence we get the following expression for the discriminant of $f(X) - t$ with respect to $X$.

\[
\begin{align*}
\text{dis}_X(f(X) - t)^2 &= \prod_{i < j} (x_i - x_j)^2 \\
&= (-1)^{n(n-1)/2} \prod_j \prod_{i \neq j} (x_i - x_j) \\
&= (-1)^{n(n-1)/2} \prod_j f'(x_j) \\
&= (-1)^{n(n-1)/2} n^n \prod_j \prod_k (x_j - y_k) \\
&= (-1)^{n(n-1)/2} n^n \prod_j \prod_k (y_k - x_j) \\
&= (-1)^{n(n-1)/2} n^n \prod_{k=1}^{n-1} (f(y_k) - t)
\end{align*}
\]

Since $G$ contains an $n$-cycle and $G \subseteq A_n$, then $n$ is odd. Therefore $\text{dis}_X(f(X) - t)^2$ is a polynomial in $t$ of degree $n - 1$ and highest coefficient $(-1)^{n(n-1)/2}n^n$. Since $(n, p) = 1$, $(-1)^{n(n-1)/2}n^n$ is a square in $K$ if and only if $(-1)^{(n-1)/2}n$
is a square in $K$. As $G$ is even, $(\text{dis}_X(f(X) - t))^2$ is a square in $\hat{K}(t)$ where $\hat{K}$ is the algebraic closure of $K$. Accordingly write

$$(\text{dis}_X(f(X) - t))^2 = (b_m t^m + \ldots + b_0)^2$$

with $m = \frac{n-1}{2}$ and $b_i \in \hat{K}$.

If $A \subset A_n$, note that the discriminant is invariant under $A$ and $G$, then we can assume $b_i \in K$. Then $(-1)^n (n-1)/2 n^2 = b_m^2$ is a square in $K$, which is the same meaning as $(-1)^{(n-1)/2} n$ being a square in $K$.

If $(-1)^{(n-1)/2} n$ is a square in $K$, we can find $b_m \in K$ such that $(-1)^n (n-1)/2 n^2 = b_m^2$. Set

$$(\text{dis}_X(f(X) - t))^2 = a_{n-1} t^{n-1} + \ldots + a_0$$

with $a_i \in K$. Note that we can solve $b_{m-1}$ by terms of $a_{n-2}$ and $b_m$ (actually it is $\frac{a_{n-2}}{2b_m}$). Hence $b_{m-1} \in K$. Note that it is similar when we solve for other $b_i$’s with only addition, multiplication and division. So we can get the conclusion that all the $b_i$’s are in $K$. Then the discriminant is invariant under $A$, hence $A \in A_n$.

From what we have done, we can deduce our main theorem:

**Theorem 6.5.** Assume $f(X) \in \mathbb{F}_q[X]$ is an indecomposable polynomials of degree $n$ and $n$ is coprime to $2q$, not in \{11, 23\} and cannot be written into the form $r^d - 1$ for any prime power $r$ and any integer $d > 1$. Then the rational number $c$ in the value set formula has to be one of the following:

1. $1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-1} \frac{1}{n!}$
2. $1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-1} \frac{1}{(n-2)!}$ ( $n$ is a square in $\mathbb{F}_q$ )
3. $1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-1} \frac{1}{(n-2)!} + \frac{2}{(n-1)!}$ ( $n$ is not a square in $\mathbb{F}_q$ )
4. $\frac{1}{(n,q-1)}$ ( $n$ is a prime )
5. $\frac{1}{(n,q+1)} + \frac{1}{(n,q-1)}$ ( $n$ is a prime )

Furthermore, all of these values occur for every such $n$ and $q$. 

22
References


