Growth of points on hyperelliptic curves

An Honors Thesis for the Department of Mathematics.

Christopher Keyes

Tufts University, 2018

1 Introduction

Let C be an algebraic curve over $\mathbb{Q}$, given by a polynomial equation in two variables. The set of rational points on C, denoted $C(\mathbb{Q})$, has long been an object of interest to number theorists. Given a number field K, we may also look at $C(K)$, and ask whether this leads to any new points on the curve.

Definition (gaining points)**.** Let C be a curve defined over $\mathbb{Q}$, and suppose (x_0, y_0) is an algebraic point on C. Then we call $\mathbb{Q}(x_0, y_0)$ the *field generated by* (x_0, y_0). If K be a finite extension of $\mathbb{Q}$, then C is said to *gain points over* K if $C(\mathbb{Q}) \subsetneq C(K)$ and K is the field generated by some point on C.

In a recent paper, Mazur and Rubin posed a question about the relationship between algebraic curves and the set of fields over which they gain points [10]. Simply stated, the question is: if two curves gain points over the same fields, are they the same curve? Alternatively, can we distinguish curves based on information about these fields?

A first step in understanding this question is to ask how often curves gain points over number fields. The aim of this thesis is to prove the existence of an unconditional lower bound on how often odd degree hyperelliptic curves gain points over number fields of large degree. This work builds on work of Lemke Oliver and Thorne [9] on the analogous problem for elliptic curves. Before stating the theorem, we define a few key terms.

Definition (hyperelliptic curve)**.** A *hyperelliptic curve*, C, is an algebraic curve given by

$$C \colon y^2 = f(x),$$

where $f(x)$ is a polynomial of degree at least 5 with rational coefficients and distinct roots. The *degree* of C is the degree of $f(x)$.

Given a hyperelliptic curve C, a nonnegative integer n, and a positive real number X, we use $N_n^{(C)}(X)$ to denote the number of degree n number fields over which C gains a point, with discriminant up to X. We use $N_n^{(C)}(X, S_n)$ to denote the number of those fields which have Galois closure S_n over $\mathbb{Q}$. We are now ready to state the main result.

Theorem 1.1. *Let C be a hyperelliptic curve with degree $d = 2g + 1$, where $g \geq 2$. Suppose $n \geq d$. Then*

$$N_n^{(C)}(X, S_n) \gg X^{\frac{1}{4}(1-\frac{2g}{n}+\frac{2g^2-6g-8}{n(n-1)})}.$$

To motivate this result, we will begin in Section 2 by introducing algebraic curves and their rational points, mentioning the familiar examples of lines, conics, and elliptic curves. We will state Faltings' Theorem, which establishes the finiteness of rational points on hyperelliptic curves.

In Section 3, we will state known bounds for counting number fields, without any restrictions that the fields induce a curve to gain points. We will also state a result of Granville that gives a conditional bound on the number of quadratic fields over which a hyperelliptic curve gains points. At this point, we will restate Theorem 1.1 and contrast it with Granville's result for quadratic fields.

We review some group theory in Section 4, establishing results that will be useful in later proofs. We will assume the reader has some familiarity with permutation groups and Galois theory.

We will introduce Newton polygons in Section 5, constructing them and working with examples. We will state a key result that relates the Newton polygon of a polynomial to its Galois group, a tool which comes in handy in subsequent proofs.

The proof of Theorem 1.1 is given in Section 6, and 7 offers some remarks and potential directions of future work.

2 Algebraic curves and rational points

Definition (algebraic curves and rational points)**.** An *plane algebraic curve* C is the set of solutions to a polynomial equation in two variables,

$$C\colon f(x,y) = 0.$$

The set of *rational points* on C, denoted $C(\mathbb{Q})$, contains those points in the solution set with rational coordinates,

$$C(\mathbb{Q}) = \{\, (x_0, y_0) \in \mathbb{Q}^2 \mid f(x_0, y_0) = 0 \,\}\,.$$

Given a number field K, the K-rational points are denoted $C(K)$.

In this thesis, we are interested in plane algebraic curves with rational coefficients. From here on, curves are assumed to have coefficients in $\mathbb{Q}$ unless stated otherwise.

Given a curve, C, we can ask many questions about $C(\mathbb{Q})$. For instance, how big is it? Can we put any additional structure on this set? If K is a number field, can we say the same things about $C(K)$ as we can about $C(\mathbb{Q})$? We will look at the answers to some of these questions for the familiar examples of lines, conics, and elliptic curves, then move on to hyperelliptic curves.

Example 2.1. A line L is defined by

$$L\colon Ax + By = C,$$

where $A, B, C \in \mathbb{Q}$. We would like to know about the size of $L(\mathbb{Q})$.

For any $x_0 \in \mathbb{Q}$, the point $(x_0, \frac{C-Ax_0}{B})$ is on L. The y-coordinate of this point is also a rational number, so in fact, $(x_0, \frac{C-Ax_0}{B}) \in$ Ł$(\mathbb{Q})$. Since each distinct choice of rational

x-coordinate gives rise to a distinct rational point on L, we have that $L(\mathbb{Q})$ is infinite.

Lines are the simplest case of algebraic curves. To see more interesting possibilities for the set of rational points, we consider conic sections. Recall that a conic section is an algebraic curve of degree two. In general, this is given by

$$Ax^2 + By^2 + Cxy + Dx + Ey + F = 0,$$

where $A, B, C, D, E, F \in \mathbb{Q}$.

Example 2.2. Consider the familiar unit circle,

$$U\colon x^2 + y^2 = 1.$$

The point $(-1, 0)$ is in $U(\mathbb{Q})$. We can use this point to find other rational points on the circle by looking at where lines passing through $(-1, 0)$ intersect U.

Let $m \in \mathbb{Q}$, and consider the line given by $y = m(x + 1)$, which passes through $(-1, 0)$. To find where this line intersects U, we substitute for y, and find

$$x^2 + m^2(x + 1)^2 - 1 = 0.$$

Factoring out $(x + 1)$, since $(-1, 0)$ is on both the line and the circle, we have

$$(x + 1)((1 + m^2)x + m^2 - 1) = 0.$$

This implies that

$$\Big(\frac{1 - m^2}{1 + m^2}, m\big(\frac{1 - m^2}{1 + m^2} + 1\big)\Big)$$

is on the unit circle, and since m is a rational number, it is also in $U(\mathbb{Q})$.

Moreover, any two distinct choices of $m \in \mathbb{Q}$ produce two lines that meet only at $(-1, 0)$. This means that the other point on U produced by each line is distinct, and thus we have that $U(\mathbb{Q})$ is infinite.

This method of using a rational point to parameterize other rational points may be generalized to any conic on which we can find a starting point. This means that if a conic has at least one rational point, it has infinitely many. We might hope that all conics have at least one rational point, but this turns out not to be so.

Example 2.3. Consider the circle, V, given by

$$V\colon x^2 + y^2 = 3.$$

Suppose $(x_0, y_0) \in V(\mathbb{Q})$. Then we may write

$$(x_0, y_0) = \left(\frac{X}{Z}, \frac{Y}{Z}\right),$$

for some $X, Y, Z \in \mathbb{Z}$ with $\gcd(X, Y, Z) = 1$. These integers satisfy the equation

$$X^2 + Y^2 = 3Z^2.$$

Reducing modulo 3, we find

$$X^2 + Y^2 \equiv 0 \pmod{3}.$$

The only squares in $\mathbb{Z}/3\mathbb{Z}$ are 0 and 1, so it must be that $X^2 \equiv Y^2 \equiv 0 \pmod 3$. If $3|X^2$, then $3|X$, and by the same argument, $3|Y$. This implies that $9|(X^2 + Y^2)$, so $9|3Z^2$, and thus we have $3|Z^2$.

However, this means that 3 is a common divisor for X, Y, and Z, so $3 | \gcd(X, Y, Z)$, which is a contradiction. Therefore, we conclude that the set of rational points $V(\mathbb{Q})$ is empty.

Examples 2.2 and 2.3 demonstrate that the story of rational points on conics is somewhat more complicated than for lines. While lines always have infinitely many rational points, the set of rational points on a conic may be either empty or infinite, but never finite. To see an example of an algebraic curve with finitely many rational points, we must turn to curves of nonzero genus.

Topologically, the genus of a surface is the number of holes. A donut, for example, has a single hole, so its genus is 1. Algebraic curves may be realized as surfaces in the projective plane, which keep track of their structure over $\mathbb{C}$. The genus of a curve is the topological genus of this surface. The first example of a curve with nonzero genus is an elliptic curve.

Definition (elliptic curve)**.** An *elliptic curve* is a nonsingular, smooth, projective algebraic curve of genus 1 with a distinguished point.

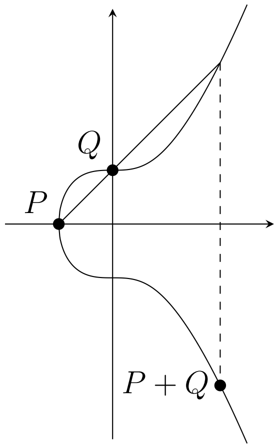
In this form, the definition is not the most enlightening. However, any elliptic curve E over $\mathbb{Q}$ may be written in short Weierstrass form as

$$E\colon y^2 = x^3 + Ax + B,$$

where $A, B \in \mathbb{Q}$.

As with our earlier examples, we want to understand $E(\mathbb{Q})$, which turns out to form an abelian group. The identity of this group is the point at infinity, which is rational for an elliptic curve with rational coefficients. The inverse of a rational point on E is its reflection across the x-axis. The sum of two distinct points P and Q in $E(\mathbb{Q})$ is found by taking the third point where the line between them intersects the curve and reflecting it across the x-axis. The sum of a point $P \in E(\mathbb{Q})$ with itself is found by taking the point where the tangent line at P intersects the curve again and reflecting across the x-axis. These operations may be proven to be well defined, associative, and commutative, leaving us with an abelian group. See Figure 2.1 for a visual depiction of adding points on an elliptic curve.

Figure 2.1: The group law on an elliptic curve



This additional structure is one of the reasons why elliptic curves have been so closely studied. However, since they are not the main focus of this thesis, we will merely highlight a few results about $E(\mathbb{Q})$.

Theorem 2.4 (Mordell-Weil)**.** *Given an elliptic curve E with coefficients in $\mathbb{Q}$, the set $E(\mathbb{Q})$ is a finitely generated abelian group. We may write*

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r,$$

where $E(\mathbb{Q})_{tors}$ is a finite abelian group and $r \geq 0$ is an integer, called the rank of E.

The torsion subgroup, $E(\mathbb{Q})_{tors}$, is the finite subgroup of $E(\mathbb{Q})$ containing points with finite order as group elements. The Mordell-Weil theorem is nonconstructive, in that it does not give a list of possible finite groups that can arise as $E(\mathbb{Q})_{tors}$ for some elliptic curve E. For this, we turn to a result of Mazur.

Theorem 2.5 (Mazur). *Let E be an elliptic curve with rational coefficients. Then*

$$E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & 1 \leq n \leq 10 \text{ or } n = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & 1 \leq n \leq 4 \end{cases}$$

Less is known about the rank. There are known to be infinitely many elliptic curves with rank 0, and these curves have finitely many rational points. There are also infinitely many elliptic curves of rank 1, and it is conjectured that in some sense, most elliptic curves have rank 0 or 1. However, there exist elliptic curves of higher rank. The largest known example, found by Elkies, has rank at least 28. The question of whether or not there exists an upper bound on the possible ranks of elliptic curves is still open.

We will now reintroduce hyperelliptic curves, which are the primary objects of study in this work.

Definition (hyperelliptic curve). A *hyperelliptic curve*, C, is an algebraic curve given by

$$C\colon y^2 = f(x),$$

where $f(x)$ is a polynomial of degree at least 5 with rational coefficients and distinct roots. The *degree* of C is the degree of $f(x)$.

The requirement $\deg(f(x)) \geq 5$ is to avoid overlap with the aforementioned curves. If $d = 1, 2$ then C is a conic section, and if $d = 3, 4$, then C may be written as an elliptic curve.

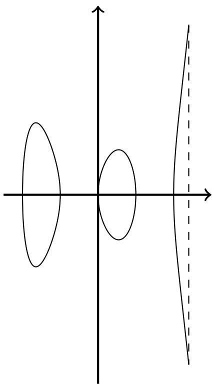
Enforcing that there are no repeated roots guarantees that the curve is nonsingular, with no cusps or self-intersections.

It turns out that the genus of a nonsingular hyperelliptic curve is related to its degree by a simple formula. We will not prove this here, but will instead provide an example and a little intuition.

Fact 2.6. *Let C be a nonsingular hyperelliptic curve of degree d. Then $d = 2g + 1$ or $d = 2g + 2$.*

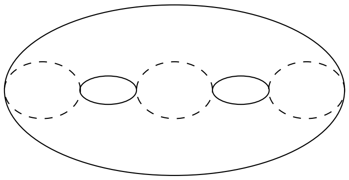
Example 2.7. To loosely visualize this fact, consider the hyperelliptic curve $C\colon y^2 = x^5 - 5x^3 + 4x$, plotted in Figure 2.2. Since it is degree 5, C has genus 2. We can imagine the plot of C in the real plane to be a slice of the surface formed by C in the projective plane. In this projective space, there is a point at infinity, so this cross section is three disjoint circles.

Figure 2.2: $C\colon y^2 = x^5 - 5x^3 + 4x$



This corresponds to a cross-section of a genus two surface that cuts through each of the two holes. An example of such a cross-section is shown in Figure 2.3. Other degree 5 hyperelliptic curves come from cross-sections of different genus 2 surfaces, resulting in the range of real graphs observed for hyperelliptic curves.

Figure 2.3: A cross-section of a genus 2 surface



We now ask the same question that we have asked for lines, conics, and elliptic curves. Given a hyperelliptic curve C what can we say about $C(\mathbb{Q})$? Unlike elliptic curves, there is no natural group structure on the rational points of C. However, we do know something about the size of $C(\mathbb{Q})$.

Theorem 2.8 (Faltings)**.** *Let C be a nonsingular algebraic curve of genus $g \geq 2$ over $\mathbb{Q}$. Then $C(\mathbb{Q})$ is finite.*

Hyperelliptic curves have genus at least 2, so by Faltings' theorem, the $C(\mathbb{Q})$ is finite for any hyperelliptic curve C.

Remark 2.9. Almost all of the results about rational points in this section may be generalized to number fields. In particular, if K is a finite extension of $\mathbb{Q}$, we have

i) If L is a line defined over K, then $L(K)$ is infinite;

ii) If S is a conic section defined over K, then $S(K)$ is either empty or infinite;

iii) If E is an elliptic curve defined over K, then $E(K)$ is a finitely generated group;

iv) If C is a nonsingular algebraic curve over K with genus at least 2, then $C(K)$ is finite.

3 Counting number fields

Before attempting to count how many fields admit new points on a curve, we would like to know how many there are to begin with. Since there are infinitely many degree n number fields for any $n > 1$, we need some way to order them. A natural choice is the discriminant. Let $N_n(X)$ be used to denote the number of degree n number fields with discriminant up to X,

$$N_n(X) := \# \{ K \supseteq \mathbb{Q} \mid [K : \mathbb{Q}] = n, \Delta_K \leq X \},$$

where Δ_K denotes the absolute discriminant of K. We use $N_n(X, S_n)$ to denote the number of fields satisfying the additional requirement of having Galois closure S_n.

A conjecture, attributed to Linnik, is that for fixed n

$$N_n(X) \sim c_n X.$$

That is, in the limit of large X, $N_n(X)$ approaches a multiple of X, with the constant depending on n. However, the best known upper and lower bounds for $N_n(X)$ have not reached this prediction for general n. A well known upper bound is due to Schmidt [11].

Theorem 3.1 (Schmidt)**.** *If n be a positive integer, then*

$$N_n(X) \ll X^{(n+2)/4}.$$

Ellenberg and Venkatesh [6] improved this bound, reducing the power of n in the exponent.

Theorem 3.2 (Ellenberg-Venkatesh)**.** *Let $n > 2$. Then*

$$N_n(X) \ll (XA_n)^{\exp(C\sqrt{\log n})},$$

where A_n is a constant depending on n and C is an absolute constant.

Lower bounds have been provided for $N_n(X, S_n)$, which serve as lower bounds to $N_n(X)$ as well. In the same paper as their upper bound, Ellenberg and Venkatesh presented such a lower bound. The proof of Theorem 1.1 takes a similar approach as that of Theorem 3.3, but makes use of a more refined estimate for multiplicity.

Theorem 3.3 (Ellenberg-Venkatesh)**.** *Let $n > 2$. Then*

$$N_n(X, S_n) \gg X^{1/2+1/n^2}.$$

Remark 3.4. Theorems 3.1, 3.2, and 3.3 can be made more general to allow the base field to be an arbitrary number field.

An improvement to Theorem 3.3 has been made by Bhargava, Shankar, and Wang [1]. They were able to reduce the power of $1/n$ in the exponent by 1. However, this result only holds over $\mathbb{Q}$ and has not been extended to arbitrary base fields.

Theorem 3.5 (Bhargava-Shankar-Wang)**.** *Let $n > 1$. Then*

$$N_n(X, S_n) \gg X^{1/2+1/n}.$$

So far, the results we have explored have been for counting arbitrary number fields. Our goal is to count the number fields which allow the hyperelliptic curve

$$C\colon y^2 = f(x)$$

to gain a point. For insight into the quadratic case, we turn to a conditional result of Granville [7].

Definition (quadratic twist)**.** Let $C\colon y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{Q}$ and d a squarefree integer. The *dth quadratic twist of* C is the hyperelliptic curve

$$C_d\colon dy^2 = f(x).$$

Theorem 3.6 (Granville)**.** *Assume the abc-conjecture is true and suppose $f(x) \in \mathbb{Z}[x]$ has distinct roots. Then if $\deg f \geq 5$, the genus g of C is at least 2, and the number of squarefree integers d with $|d| \leq D$ for which C_d has a nontrivial rational point is $\ll_f D^{1/(g-1)+o(1)}$.*

Here, trivial points are those that always appear on C_d, such as the point at infinity or those with $y = 0$. The nontrivial rational points on C_d correspond to irrational points in $C(\mathbb{Q}(\sqrt{d}))$, giving us the following corollary to Theorem 3.6.

Corollary 3.7. *Assume the abc-conjecture is true and let C have genus g. Then*

$$N_2^{(C)}(X) \ll X^{1/(g-1)+o(1)}.$$

The exponent of X in the bound in Corollary 3.7 decreases as the genus of C increases, approaching 0 in the limit. This suggests that as genus increases, the number of quadratic fields admitting new points decreases. Motivated by this, we ask how $N_n^{(C)}(X)$ depends on n when g is fixed. Theorem 1.1 gives an upper bound in the case of large n.

Theorem 1.1. *Let C be a hyperelliptic curve with degree $d = 2g + 1$, where $g \geq 2$. Suppose $n \geq d$. Then*

$$N_n^{(C)}(X, S_n) \gg X^{\frac{1}{4}(1-\frac{2g}{n}+\frac{2g^2-6g-8}{n(n-1)})}.$$

Note that for any fixed $g \geq 2$, the exponent on X approaches $1/4$ as n grows without bound. In fact, this exponent is positive for any $n \geq 2g + 1$ when $g \geq 4$. If g is allowed to grow without bound and n is kept at $2g + 1$, the exponent approaches $1/8$.

The proof of Theorem 1.1 involves finding parameterizations that produce polynomials whose roots give rise to points on C. By showing these polynomials are almost always irreducible and have Galois group S_n, we get a way to count S_n-extensions over which C gains points. Counting the number of polynomials produced by the parameterization and correcting for multiplicity produces a lower bound on $N_n^{(C)}(X, S_n)$.

Some key intermediate results in showing that the polynomials produced by the parameterization in fact have Galois group S_n are presented in Sections 4 and 5. The proof is detailed in Section 6.

4 Some algebra

Recall that S_n denotes the symmetric group on n letters. This group may be realized as the group of permutations on the n-element set $\{1, ..., n\}$. Consider the following question: given a subgroup $G \subseteq S_n$, what do we need to know about G to deduce that $G = S_n$? To answer this question, we consider some generating sets of S_n.

Example 4.1. The following sets generate S_n, where $n \geq 2$:

i) The set of cycles,

$$G_1 = \{ \sigma \in S_n \mid \sigma \text{ is a cycle} \};$$

ii) The set of transpositions,

$$G_2 = \{\, (a\ b) \in S_n \mid 1 \leq a < b \leq n \,\}\,;$$

iii) The set of transpositions containing 1,

$$G_3 = \{\, (1, b) \in S_n \mid 2 \leq b \leq 1 \,\}\,.$$

Note that $G_3 \subseteq G_2 \subseteq G_1$. It may be shown that G_3 generates G_2 by a conjugation argument using the principle of Lemma 4.2. G_2 generates G_1 since all cycles may be written as a product of transpositions. Finally, every element of S_n has a cycle decomposition, which implies G_1 (and also G_1 and G_2) generates S_n. The details of these proofs are covered in an introductory abstract algebra course. We refer the interested reader to [5] and [3].

The size of the generating sets in Example 4.1 all depend on n, but this need not be the case. In fact, for $n \geq 3$, the two-element set

$$\{\, (1\ 2), (2\ ...\ n) \,\}$$

generates S_n. To prove this, we introduce one lemma.

Lemma 4.2. *Let $(a_1\ ...\ a_m) \in S_n$ be an m-cycle and $\sigma \in S_n$ be an arbitrary element. Then*

$$\sigma(a_1\ ...\ a_m)\sigma^{-1} = (\sigma(a_1)\ ...\ \sigma(a_m)).$$

Proof. Consider the action of this permutation on elements of the form $\sigma(a_i)$ for $1 \leq i < m$. We have

$$\sigma(a_1\ ...\ a_m)\sigma^{-1}(\sigma(a_i)) = \sigma(a_1\ ...\ a_m)(a_i) = \sigma(a_{i+1}).$$

In the case of $i = m$, we have

$$\sigma(a_1 \ldots a_m)\sigma^{-1}(\sigma(a_m)) = \sigma(a_1 \ldots a_m)(a_m) = \sigma(a_1).$$

Suppose $b \neq \sigma(a_i)$ for $1 \leq i \leq m$. Then $\sigma^{-1}(b) \notin \{ a_i \mid 1 \leq i \leq m \}$, and we have

$$\sigma(a_1 \ldots a_m)\sigma^{-1}(\sigma(b) = \sigma(a_1 \ldots a_m)(\sigma^{-1}(b)) = \sigma(\sigma^{-1}(b)) = b.$$

We conclude that

$$\sigma(a_1 \ldots a_m)\sigma^{-1} = (\sigma(a_1) \ldots \sigma(a_m)).$$

□

Proposition 4.3. *Suppose $n \geq 3$. Then the set*

$$G = \{ (1\ 2), (2 \ldots n) \}$$

generates S_n.

Proof. By Lemma 4.2, we have

$$(2 \ldots n)^k(1\ 2)(2 \ldots n)^{-k} = (1\ 2+k)$$

for $0 \leq k \leq n-2$. This generates all transpositions of the form $(1\ b)$, where $2 \leq b \leq n$, which is exactly the generating set G_3 in Example 4.1. Hence, we have that G generates S_n. □

To use the generating set in Proposition 4.3 to show that our subgroup G is equal to S_n, we need to know very specific information about the contents of G. Suppose we knew that

G contained a transposition and an $(n-1)$-cycle, but not exactly which one. To handle this situation, we need an additional hypothesis about G.

Definition (transitive)**.** Let $G \subseteq S_n$ be a subgroup. G is said to be *transitive* if for any $i, j \in \{ 1, ..., n \}$, there exists $\sigma \in G$ such that $\sigma(i) = j$.

Proposition 4.4. *Let $n \geq 2$. If G is a transitive subgroup of S_n, containing an $(n-1)$-cycle and a transposition, then $G = S_n$.*

Proof. This proposition is trivial in the case of $n = 2$, since there is exactly one transposition and it generates S_2. We assume that $n \geq 3$.

Let $\sigma = (a_1 \ ... \ a_{n-1}) \in G$ be an $(n-1)$-cycle and $\tau = (b_1 \ b_2) \in G$ be a transposition. We may choose a labeling such that $a_i = i + 1$ for $1 \leq i \leq n-1$, which gives $\sigma = (2 \ ... \ n)$.

Since G is transitive, there exists $\rho \in G$ such that $\rho(b_1) = 1$, so we have $\rho\tau\rho^{-1} = (1 \ \rho(b_2)) \in G$. Since $2 \leq \rho(b_2) \leq n$, we may conjugate $\rho\tau\rho^{-1}$ by σ^{-1} several times to get a 2 in the second position,

$$\sigma^{2-\rho(b_2)}(1 \ \rho(b_2))\sigma^{-(2-\rho(b_2))} = \Big(1 \ \big(\rho(b_2) + 2 - \rho(b_2)\big)\Big) = (1 \ 2).$$

Conjugation by elements of G keeps us within G, so $(1 \ 2) \in G$. Hence, G contains $\{ (1 \ 2), (2 \ ... \ n) \}$, which is the generating set from Proposition 4.3, so G generates S_n. □

In the case that we have a cycle of prime order of sufficient length, we have a similar result.

Proposition 4.5. *Let $n \geq 2$. If G is a transitive subgroup of S_n, containing a transposition and a p-cycle for some prime $p > n/2$, then $G = S_n$.*

Proof. See the proof of Theorem 2.1 in [4]. □

Transitive subgroups of S_n arise naturally as the Galois groups of irreducible polynomials. Briefly, we will recall a few definitions from Galois theory, without going into great detail.

Definition (automorphism groups)**.** Let L be an extension of a field K. The *automorphism group of L over K*, denoted $\mathrm{Aut}(L/K)$, is the group of automorphisms of L that fix K,

$$\mathrm{Aut}(L/K) := \{\, \phi \in \mathrm{Aut}(L) \mid \phi(a) = a \ \forall a \in K \,\} .$$

Definition (Galois group)**.** Let L be an extension of a field K. We say L is *Galois* if it is the splitting field of a separable polynomial in $K[x]$. If this is the case, we call $\mathrm{Aut}(L/K)$ the *Galois group of L over K*, and denote it $\mathrm{Gal}(L/K)$.

Similarly, if $f(x) \in K[x]$ is separable, the *Galois group of $f(x)$ over K* is defined as the Galois group of its splitting field over K, and denoted $\mathrm{Gal}_K(f(x))$.

Definition (Galois closure)**.** If F is an extension of K, its *Galois closure*, denoted $\overline{F}$, is the smallest field containing F that is Galois.

This definition of a Galois closure makes more precise what we mean by S_n-extensions of $\mathbb{Q}$, as in the definition of $N_n(X, S_n)$ and the statement of Theorem 1.1. Such extensions come from adjoining roots of polynomials with Galois group S_n over $\mathbb{Q}$.

Theorem 4.6. *Let $f(x) \in K[x]$ be a separable polynomial. Then $f(x)$ is irreducible if and only if $\mathrm{Gal}_K(f(x))$ is transitive.*

Proof. See any introductory abstract algebra textbook. □

Theorem 4.6 justifies our statement that transitive subgroups of S_n come from Galois groups of irreducible polynomials. If we can argue that a Galois group is transitive, this also gives us a tool to argue that a polynomial is irreducible.

In Section 5, we will introduce Newton polygons. These constructions are helpful for deducing information about the Galois group of a polynomial. Specifically, they are useful for identifying certain cycle types in the Galois group, and arguing the group is transitive. If this information is sufficient to satisfy the hypotheses of Proposition 4.4 or 4.5 then we may conclude the Galois group is S_n.

Remark 4.7. In this thesis, we are primarily interested in $\mathbb{Q}$ as the base field. All extensions and Galois groups will be assumed to over $\mathbb{Q}$, unless specified otherwise.

5 Newton polygons

Definition (Newton polygon)**.** Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial in $\mathbb{Q}[x]$ such that $a_0 a_n \neq 0$. For a prime p, the *Newton polygon* $\mathcal{N}_p(f(x))$ is the lower convex hull of the set

$$\{\, (i, v_p(a_i)) \in \mathbb{R}^2 \mid a_i \neq 0 \,\},$$

where v_p denotes the p-adic valuation.

Denote the side with slope m by s_m, which has endpoints $(i_m, v_p(a_{i_m}))$ and $(t_m, v_p(a_{t_m}))$. Let $h(s_m) = v_p(a_{t_m}) - v_p(a_{i_m})$ be the height of s_m and $l(s_m) = t_m - i_m$ be the length of the s_m.

This is a busy definition, so we will take a look at a few examples.

Example 5.1. Consider the polynomial

$$f(x) = 18x^7 + 6x^6 - 10x^2 + 15.$$

Let $p = 3$. Then we have

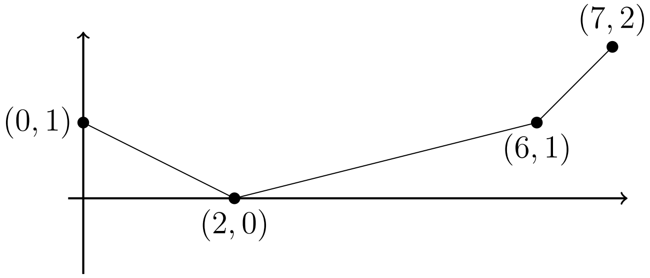
$$v_3(15) = 1,\ v_3(5) = 0,\ v_3(6) = 1,\ v_3(18) = 2,$$

so the points on $\mathcal{N}_3(f(x))$ are

$$(0, 1),\ (2, 0),\ (6, 1),\ (7, 2).$$

To draw the lower convex hull of these points, one may visualize a string hanging from $(0, 1)$ that is wrapped counter-clockwise until it has touched $(7, 2)$. Recall that $v_p(0) = \infty$ for all primes p, so any points of the form (i, ∞) will not be relevant for the Newton polygon. The resulting polygon is shown below in Figure 5.1.

Figure 5.1: $\mathcal{N}_3(18x^7 + 6x^6 - 10x^2 + 15)$

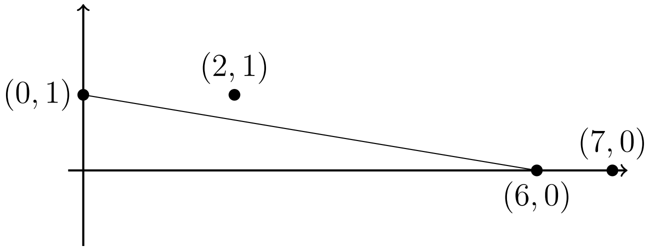


Suppose we take p to be 5 instead. The resulting polygon contains the points

$$(0,1),\ (2,1),\ (6,0),\ (7,0),$$

and is drawn in Figure 5.2.

Figure 5.2: $\mathcal{N}_5(18x^7 + 6x^6 - 10x^2 + 15)$



There is a surprising connection between the Newton polygon $\mathcal{N}_p(f(x))$ and the Galois group $\mathrm{Gal}_{\mathbb{Q}_p}(f(x))$, where $\mathbb{Q}_p$ denotes the p-adic numbers. Lemma 5.2 relates the lengths and slopes of the segments of $\mathcal{N}_p(f(x))$ to elements with certain cycle types in $\mathrm{Gal}_{\mathbb{Q}_p}(f(x))$.

Lemma 5.2. *Let $f(x) \in \mathbb{Q}[x]$ and p be prime. Let s_m be a segment of $\mathcal{N}_p(f(x))$, with slope $m = \frac{a}{k}$ in lowest terms. Let $d = l(s_m)/k$. Then $\mathrm{Gal}_{\mathbb{Q}_p}(f(x))$ contains a permutation which* *is the product of d disjoint k-cycles. In particular, if $l(s_m)$ and $h(s_m)$ are relatively prime, then $d = 1$ and there exists a k-cycle in* $\mathrm{Gal}_{\mathbb{Q}_p}(f(x))$.

We refer the reader interested in more information to a paper of Kölle and Schmid [8]. It it, they discuss a stronger form of the above theorem, which relates Newton polygons to certain subgroups of $\mathrm{Gal}_{K_\mathfrak{p}}(f(x))$ for an algebraic number field K and prime $\mathfrak{p}$.

Example 5.3. We will use Lemma 5.2 to compute $\mathrm{Gal}_{\mathbb{Q}}(f(x))$ for $f(x) = 18x^7 + 6x^6 - 10x^2 + 15$ from Example 5.1. The polygon $\mathcal{N}_3(f(x))$, depicted in 5.1, has three segments, the slopes and lengths of which are shown below.

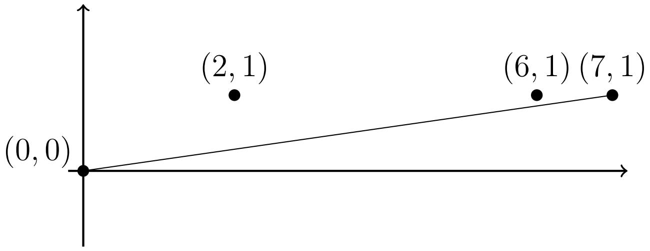
m	$l(s_m)$
-1/2	2
1/4	4
1	1

For the segment with slope -1/2, Lemma 5.2 gives that $\mathrm{Gal}_{\mathbb{Q}_3}(f(x))$ contains a 2-cycle. The other segments give rise to a 4-cycle and a 1-cycle, which is trivial. A similar application of Lemma 5.2 to $\mathcal{N}_5(f(x))$ shows $\mathrm{Gal}_{\mathbb{Q}_5}(f(x))$ contains a 6-cycle.

An automorphism of the splitting field of $f(x)$ over $\mathbb{Q}_p$ that fixes $\mathbb{Q}_p$ gives rise to an automorphism of the splitting field over $\mathbb{Q}$ that fixes $\mathbb{Q}$. Hence, $\mathrm{Gal}_{\mathbb{Q}_p}(f(x))$ is a subgroup of $\mathrm{Gal}_{\mathbb{Q}}(f(x))$. This implies that $\mathrm{Gal}_{\mathbb{Q}}(f(x))$ contains cycles we found in $\mathrm{Gal}_{\mathbb{Q}_3}(f(x))$ and $\mathrm{Gal}_{\mathbb{Q}_5}(f(x))$. In particular, we now know $\mathrm{Gal}_{\mathbb{Q}}(f(x))$ contains a transposition and a 6-cycle, so if $\mathrm{Gal}_{\mathbb{Q}}(f(x))$ is transitive then it is S_7 by Proposition 4.4.

Using algebraic means, or computer algebra software, we could show that $f(x)$ is irreducible, which is equivalent to $\mathrm{Gal}_{\mathbb{Q}}(f(x))$ transitive by Theorem 4.6. Newton polygons present an alternative, allowing us to show transitivity directly. Consider $\mathcal{N}_2(f(x))$, shown below in Figure 5.3.

Figure 5.3: $\mathcal{N}_2(18x^7 + 6x^6 - 10x^2 + 15)$



$\mathcal{N}_2(f(x))$ has a single segment of slope 1/7 and length 7, so by Lemma 5.2, $\mathrm{Gal}_{\mathbb{Q}_2}(f(x))$, and hence also $\mathrm{Gal}_{\mathbb{Q}}(f(x))$, contains a 7-cycle. Any subgroup of S_n containing an n-cycle is transitive, so $\mathrm{Gal}_{\mathbb{Q}}(f(x))$ is transitive, and we conclude $\mathrm{Gal}_{\mathbb{Q}}(f(x)) = S_7$.

In the proof of Theorem 1.1, we produce families of polynomials whose roots give rise to points on a hyperelliptic curve. Using Newton polygons in a similar manner as Example 5.3, we verify that the Galois groups of these polynomials are almost always S_n. This makes it possible to bound $N_n^{(C)}(X, S_n)$ by counting the polynomials instead.

6 Proof of Theorem 1.1

Let

$$C\colon y^2 = f(x) = \sum_{i=0}^{d} c_i x^i$$

be a nonsingular hyperelliptic curve over $\mathbb{Q}$ with degree $d = 2g+1$. Since C is nonsingular, the roots of f are distinct, denoted $\alpha_1, ..., \alpha_d$.

We may make a few assumptions about f. The first is that $f(x) \in \mathbb{Z}[x]$, since we may clear denominators on the right hand side with a square and absorb the square into y on the left. We will also assume that the coefficients of $f(x)$ are nonzero integers. We may justify this by considering the translation $f(x+k)$, which has roots $\alpha_i - k$. The i^{th} coefficient of this polynomial is thus

$$(-1)^{d-i} c_d \sum_{1 \leq j_1 < ... < j_{d-i} \leq n} (\alpha_{j_1} - k) \cdot ... \cdot (\alpha_{j_{d-i}} - k),$$

which is a degree $d-i$ polynomial in k. Hence, there are only $d-i$ choices of k for which the i^{th} coefficient of the translated polynomial $f(x+k)$ is zero. Since there are finitely many such k for each i, and finitely many i, we may choose $k \in \mathbb{Z}$ such that no coefficients of $f(x+k)$ are zero.

Our strategy will be to parameterize y as a rational function in x, $\frac{g(x)}{h(x)}$, where $g(x), h(x) \in \mathbb{Q}[x]$ are given by

$$g(x) = \sum_{i=0}^{d_g} a_i x^i$$

and

$$h(x) = \sum_{j=0}^{d_h} b_j x^j.$$

If n is odd, then $d_g = (n-1)/2$ and $d_h = (n-d)/2$. If n is even, then $d_g = n/2$ and

$d_h = (n-d-1)/2$. Define

$$F_n^{(C)}(\mathbf{a}, \mathbf{b}, x) = f(x)h(x)^2 - g(x)^2.$$

Proposition 6.1. *Suppose d is odd. Then as a polynomial in $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})[x]$, $F_n^{(C)}(x)$ is irreducible and*

$$\mathrm{Gal}_{\mathbb{Q}(\boldsymbol{a},\boldsymbol{b})}(F_n^{(C)}) = S_n.$$

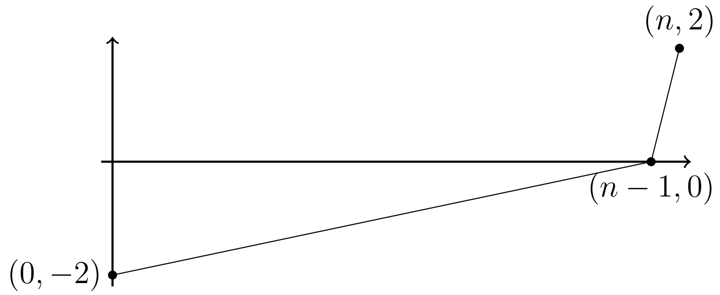
Proof. We will argue that there exists $(\mathbf{a}_0, \mathbf{b}_0)$ such that $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ is irreducible and has Galois group S_n over $\mathbb{Q}$. In order to do so, we will examine this specialization over $\mathbb{Q}_p$ for various primes p, and using Newton polygons, identify elements of the Galois group of $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ over $\mathbb{Q}_p$, which must then also be in the Galois group over $\mathbb{Q}$.

First, suppose n is even and consider specializations of the form

$$g(x) = a_{n/2}x^{n/2} + a_2x^2 + a_1x + a_0, \quad h(x) = b_{(n-d-1)/2}x^{(n-d-1)/2} + b_0.$$

Let p be a prime that does not divide the coefficients of $f(x)$. We will require that $v_p(a_{n/2}) = 1$, $v_p(a_0) = -1$, and $v_p(b_{(n-d-1)/2}) = 0$. For a_2, a_1, and b_0, we let the p-adic valuation be large enough to ensure that no points containing these terms are found in the lower convex hull of the Newton polygon. A value of 2 is sufficient. The resulting Newton polygon for $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ is shown in figure 6.1.

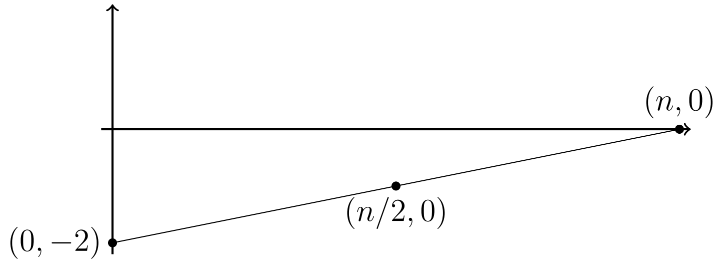
Figure 6.1: $\mathcal{N}_p(F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x))$



This polygon has a segment of slope $2/(n-1)$, and since n is even, 2 does not divide $(n-1)$. Thus by Lemma 5.2, there exists an $(n-1)$-cycle in the Galois group of $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ over $\mathbb{Q}_p$.

Choosing a different prime p that also doesn't divide the coefficients of $f(x)$, we can perform this procedure again. This time, we will have $v_p(a_{n/2}) = 0$ and $v_p(a_0) = -1$. All other coefficients, a_2, a_1, $b_{(n-d-1)/2}$, and b_0, we require to have valuation 2, to ensure that they do not affect the Newton polygon. The resulting polygon of $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ is shown in figure 6.2.

Figure 6.2: $\mathcal{N}_p(F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x))$



This polygon has one side of slope $2/n$. Since n is even, by Lemma 5.2 we have an element of cycle type $(\frac{n}{2}, \frac{n}{2})$ in $\mathrm{Gal}_{\mathbb{Q}_p}(F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x))$, and thus such an element is in the Galois group over $\mathbb{Q}$ as well.

Another way to interpret the polygon in 6.2 is that $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ factors into two irreducible polynomials, both of degree $n/2$, over $\mathbb{Q}_p$. If $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ was reducible over $\mathbb{Q}$, it would have to factor the same way. However, we know from the polygon in 6.1 that $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ has a linear factor and $n-1$ degree factor over $\mathbb{Q}_p$ for the first choice of p, which is inconsistent with reducing to degree $n/2$ factors over $\mathbb{Q}$. Hence, we have that $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ is irreducible over $\mathbb{Q}$. Note that this means $\mathrm{Gal}_{\mathbb{Q}}(F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x))$ is transitive by Theorem 4.6.

We will repeat this once more, for a different prime p, in order to find a transposition in the Galois group over $\mathbb{Q}$. If $n-d-1 \neq 0$ then we will set $v_p(b_{(n-d-1)/2}) = 2$, which will effectively let us ignore terms containing this constant in the Newton polygon. We now examine the lowest three terms of $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$, ignoring those containing $b_{(n-d-1)/2}$:

$$(c_0 b_0^2 - a_0^2) + (c_1 b_0^2 - 2a_1 a_0)x + (c_2 b_0^2 - 2a_2 a_0 - a_1^2)x^2.$$

Since c_0 is nonzero, we can select p such that c_0 is a quadratic residue, and write $c_0 \equiv m^2 \pmod{p}$, or $c_0 - m^2 = qp$ for some $q \in \mathbb{Z}$. Let k be an integer and let $a_0 = b_0(m + kp)$. Then the constant term becomes

$$c_0 b_0^2 - b_0^2(m^2 + 2mkp + k^2p^2) \equiv -b_0^2 p(2mk + k^2 p) \equiv 0 \pmod{p}.$$

We also have

$$c_0 b_0^2 - a_0^2 \equiv b_0^2(qp - 2kmp) \equiv p b_0^2(q - 2km) \pmod{p^2}$$

If k is chosen such that $q - 2km$ is not divisible by p, and $v_p(b_0) = 0$, then this constant term is nonzero mod p^2, and hence its valuation is exactly 1.

Next, we force the linear term to be divisible by p. We accomplish this by specifying

$$a_1 \equiv 2^{-1}a_0^{-1}c_1b_0^2 \pmod{p}.$$

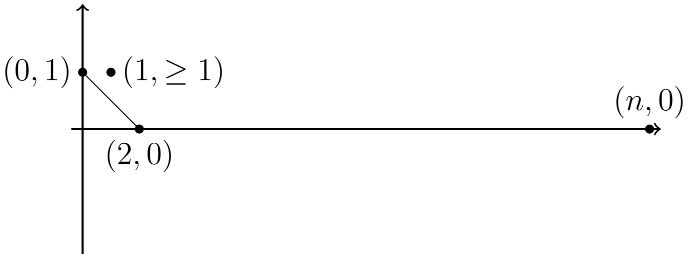
For the quadratic term, we want $c_2b_0^2 - 2a_2a_0 - a_1^2$ to not be divisible by p. By requiring

$$a_2 \equiv 2^{-1}a_0^{-1}(c_2b_0^2 - a_1^2 - 1) \pmod{p},$$

we get that $c_2b_0^2 - 2a_2a_0 - a_1^2 \equiv 1 \pmod{p}$, so $v_p(c_2b_0^2 - 2a_2a_0 - a_1^2) = 0$.

Choosing a_0, a_1, a_2, and b_0 in this way, and letting $v_p(a_{n/2}) = 0$, we produce the Newton polygon in Figure 6.3. Note that our choices of parameters have ensured that any terms of degree higher than 2 have valuation of at least 0, so they are not noted on the polygon.

Figure 6.3: $\mathcal{N}_p(F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x))$



The segment with slope 1/2 shows, by Lemma 5.2, that a transposition exists in the Galois group of $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ over $\mathbb{Q}_p$, and thus in the Galois group over $\mathbb{Q}$.

We have thus far shown that when n is even, there exists $(\mathbf{a}_0, \mathbf{b}_0)$ such that $\mathrm{Gal}_{\mathbb{Q}}(F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x))$ is transitive, containing a transposition and $(n-1)$-cycle. By Proposition 4.4 we conclude that $\mathrm{Gal}_{\mathbb{Q}}(F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)) = S_n$.

Next, we consider the case that n is odd, and use a slightly different argument to find $(\mathbf{a}_0, \mathbf{b}_0)$. First, we use Bertrand's postulate to argue that there exists a prime q such that

$\frac{n-1}{2} < q < n-1$. In particular, this means $n/2 < q < n$. We will use the specialization

$$g(x) = a_{(n-q)/2}x^{(n-q)/2} + a_2x^2 + a_1x + a_0, \quad h(x) = b_{(n-d)/2}x^{(n-d)/2} + b_0.$$

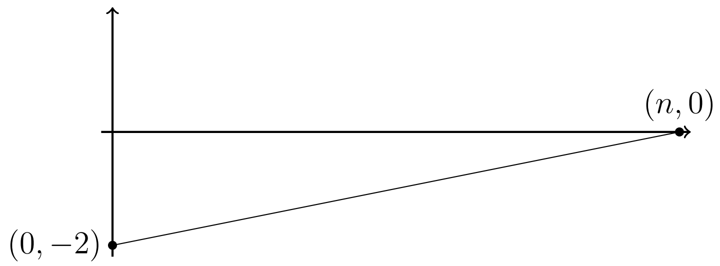
Note that since we are only interested in $n \geq 5$, q will be odd, and $(n-q)/2$ is a well defined integer. If $n-q = 2, 1$ or , then we only include it once.

Let p be an odd prime that does not divide the coefficients of $f(x)$. We set

$$v_p(a_{(n-q)/n}) = v_p(a_2) = v_p(a_1) = v_p(b_0) = 2$$

so that these terms will not be relevant in the Newton polygon. For the remaining parameters, let $v_p(a_0) = -1$ and $v_p(b_{(n-d)/2}) = 0$. These choices produce a Newton polygon with one segment, shown in figure 6.4.

Figure 6.4: $\mathcal{N}_p(F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x))$

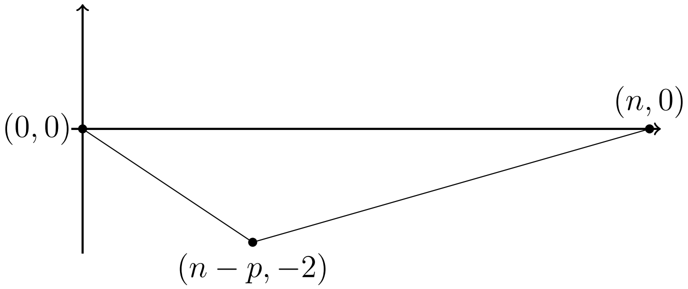


The existence of a sole segment with slope $2/n$ means that $\mathrm{Gal}_{\mathbb{Q}_p}(F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x))$ contains an n-cycle, and thus is transitive. Hence, $\mathrm{Gal}_{\mathbb{Q}}(F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x))$ is also transitive, so by Theorem 4.6, $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ is irreducible over $\mathbb{Q}$.

Next, we choose a different prime p, and let $v_p(a_{(n-q)/2}) = -1$, $v_p(a_0) = 0$, $v_p(b_{(n-d)/2}) = 0$. We also let $v_p(b_0) = 2$, and $v_p(a_1) = v_p(a_2) = 2$, unless a_1 or a_2 is equal to $a_{(n-q)/2}$. The resulting Newton polygon, shown in figure 6.5, has two segments, one of which has length

p and slope $2/p$. This segment indicates the presence of a p-cycle in the Galois group of $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ over $\mathbb{Q}_p$, by Lemma 5.2, and thus there is one in the Galois group over $\mathbb{Q}$ as well.

Figure 6.5: $\mathcal{N}_p(F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x))$



We need one more prime p to show that the Galois group over $\mathbb{Q}$ has a transposition. We follow the same approach as the even case, but set $v_p(b_{(n-d)/2}) = v_p(a_{(n-q)/2}) = 2$ to ensure that terms containing $b_{(n-d)/2}$ and $a_{(n-q)/2}$ aren't relevant for the Newton polygon. This takes care of the case that $n-d = 1$ or 2, or $(n-q)/2 = 1$ or 2, where the lowest three terms would look different than in the even n case. Note that if $n - d = 0$, we just let $h(x) = b_0$.

The lowest three terms, once $b_{(n-d)/2}$ and $a_{(n-q)/2}$ terms are removed, are identical to the even n case, so using the same approach, we can pick the values of a_0, a_1, a_2, and b_0, and obtain a segment of slope -1/2 in the Newton polygon. Again, Lemma 5.2 gives that the Galois group of $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ has a transposition over $\mathbb{Q}_p$, so there is a transposition in the group over $\mathbb{Q}$.

We have that $\mathrm{Gal}_{\mathbb{Q}}(F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x))$ is transitive, containing a q-cycle for a prime $q > n/2$ and a transposition. Hence, by Proposition 4.5 we have that $\mathrm{Gal}_{\mathbb{Q}}(F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)) = S_n$.

For all cases of $n \geq d$ when d is odd, we now have the existence of a specialization $(\mathbf{a}_0, \mathbf{b}_0)$ such that $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ is irreducible over $\mathbb{Q}$ with Galois group S_n. If $F_n^{(C)}(\mathbf{a}, \mathbf{b}, x)$ was reducible over $\mathbb{Q}(\mathbf{a},\mathbf{b})$, then all specializations would be reducible, which is a contradiction, so $F_n^{(C)}(\mathbf{a},\mathbf{b},x)$ must be irreducible over $\mathbb{Q}(\mathbf{a},\mathbf{b})$. Likewise, if its Galois group was not the full symmetric group, it would not be possible to achieve a specialization with the Galois group S_n. Hence, $\mathrm{Gal}_{\mathbb{Q}(\mathbf{a},\mathbf{b})}(F_n^{(C)}(\mathbf{a},\mathbf{b},x)) = S_n$.

□

Let $S(Y)$ be the set of polynomials in $\mathbb{Z}[x]$ of the form $F_n^{(C)}(\mathbf{a}_0,\mathbf{b}_0,x)$, for some $(\mathbf{a}_0,\mathbf{b}_0) \in \mathbb{Z}^{d_g+1} \times \mathbb{Z}^{d_h+1}$, such that the resulting polynomial is monic, degree n, trace 0, and all roots α satisfy $|\alpha| \leq Y$. Let $S(Y, S_n)$ be the subset of $S(Y)$ that contains only polynomials with Galois group S_n over $\mathbb{Q}$.

By Proposition 6.1, we have that $F_n^{(C)}(\mathbf{a},\mathbf{b},x)$ is irreducible and has Galois group S_n over $\mathbb{Q}(\mathbf{a},\mathbf{b})$. Hilbert's irreducibility theorem states that almost all specializations $(\mathbf{a}_0,\mathbf{b}_0)$ will result in $F_n^{(C)}(\mathbf{a}_0,\mathbf{b}_0,x)$ being irreducible with Galois group S_n over $\mathbb{Q}$. Hence, we can find a bound for the size of $S(Y, S_n)$ by the simpler task of bounding $S(Y)$.

Lemma 6.2. *Let $f(x)$ be a monic, degree n polynomial of the form $f(x) = \sum_{i=0}^{n} c_i x^{n-i}$. Then there exist positive constants k_i such that if $|c_i| \leq k_i Y^i$ for all i, then $|\alpha| \leq Y$ for all roots α.*

Proof. We begin by labeling the (complex) roots $\alpha_1, ..., \alpha_n$ of $f(x)$, such that $|\alpha_1| \geq ... \geq |\alpha_n|$. Suppose $|\alpha_1| > Y$. Using the relationship between a polynomial's roots and its coefficients, we will show that $|\alpha_1| \leq kY$ for a constant k that depends on the k_i. We will then argue that we can pick the k_i in such a way that $k \leq 1$, which contradicts $|\alpha_1| > Y$.

Rewriting $f(x)$ as $f(x) = (x - \alpha_1)...(x - \alpha_n)$, we see that

$$c_m = (-1)^m \sum_{1 \leq i_1 < ... < i_m \leq n} \alpha_{i_1} ... \alpha_{i_m}.$$

We can rearrange this sum to isolate α_1:

$$c_m = (-1)^m \Big[\alpha_1 (\sum_{2 \le i_2 < ... < i_m \le n} \alpha_{i_2} ... \alpha_{i_m}) + (\sum_{2 \le i_1 < ... < i_m \le n} \alpha_{i_1} ... \alpha_{i_m})\Big]$$

The above forms illustrate that c_m is the sum of all products of m roots. We will think of this as the sum of all products of α_1 and $m-1$ other roots, plus the sum of products of m roots other than α_1.

We claim that

$$\Big|\sum_{2 \le i_2 < ... < i_m \le n} \alpha_{i_2} ... \alpha_{i_m}\Big| \le (k_m + ... + k_n) Y^{m-1}$$

for $2 \le m \le n$. In the case of $m = n$, we have that $|c_i| = |\alpha_1 \alpha_2 ... \alpha_n| \le k_n Y^n$, so $|\alpha_2 ... \alpha_n| \le \frac{k_n Y^n}{|\alpha_1|} \le k_n Y^{n-1}$, since $|\alpha_1| > Y$.

Let $2 \le m < n$, and assume the claim is true for $m+1$. By this assumption, we may have

$$\Big|\sum_{2 \le i_1 < ... < i_m \le n} \alpha_{i_1} ... \alpha_{i_m}\Big| \le (k_{m+1} + ... + k_n) Y^m.$$

Then,

$$|\alpha_1| \Big|\sum_{2 \le i_2 < ... < i_m \le n} \alpha_{i_2} ... \alpha_{i_m}\Big| \le |c_m| + \Big|\sum_{2 \le i_1 < ... < i_m \le n} \alpha_{i_1} ... \alpha_{i_m}\Big|$$
$$\le k_m Y^m + (k_{m+1} + ... + k_n) Y^m = (k_m + ... + k_n) Y^m.$$

Dividing both sides of the inequality by $|\alpha_1|$ yields the claim.

In particular, for the $m = 2$ case we have

$$\Big|\sum_{2 \le i_2 \le n} \alpha_{i_2}\Big| \le (k_2 + ... + k_n) Y.$$

Turning our attention to c_1, we can write

$$c_1 = -\alpha_1 - \alpha_2 - ... - \alpha_n = -\alpha_1 - \sum_{2 \le i_2 \le n} \alpha_{i_2}.$$

Thus, we can place an upper bound on $|\alpha_1|$,

$$|\alpha_1| \le |c_1| + \Big| \sum_{2 \le i_2 \le n} \alpha_{i_2} \Big| \le k_1 Y + (k_2 + ... + k_n) Y = (k_1 + ... + k_n) Y.$$

However, if the k_i are chosen in such a way that $k_1 + ... + k_n \le 1$, then we have $|\alpha_1| \le Y$, which is a contradiction. One way to do this would be to have $k_1 = ... = k_n = 1/n$. We conclude that there exists some choice of constants k_i for which all roots α of $f(x)$ satisfy $|\alpha| \le Y$. □

Lemma 6.2 shows that there exist constants k_i such that if, for all i, we require the coefficient of the x^{n-i} term of a polynomial to be less than $k_i Y^i$, then all roots α satisfy $|\alpha| \le Y$. We may then find bounds for a_i and b_i to ensure that this condition is met for $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$, and count the number of possibilities.

Consider first the case that n is even, and let

$$g(x) = \sum_{i=0}^{n/2} a_{n/2-i} x^i, \quad h(x) = \sum_{j=0}^{(n-d-1)/2} b_{(n-d-1)/2-j} x^j.$$

Note that this is a slightly different indexing convention than used previously, which is for convenience of the following calculations. As before, $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x) = f(x)h(x)^2 - g(x)^2$, so

$$F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x) = \sum_{k=0}^{n} \Big(\big(\sum_{l=0}^{d} \sum_{i+j+1=k+d-l} c_l b_i b_j \big) - \big(\sum_{i+j=k} a_i a_j \big) \Big) x^{n-k}.$$

To make the k^{th} coefficient of $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ less than the upper bound in Lemma 6.2, we can find constants depending on C and n such that $|a_i a_j| \ll Y^{i+j}$ and $|b_i b_j| \ll Y^{i+j+1}$. Note that to bound the b_i, we only need consider the $l = d$ case, as higher terms need narrower bounds. Requiring $|a_i| \ll Y^i$ and $|b_i| \ll Y^{i+1/2}$ accomplishes this goal.

The leading term of the polynomial is $-a_0^2$, so to ensure it is monic, we need $a_0 = \pm 1$, and to multiply the whole thing by -1 to get the correct sign. The next term is $c_d b_0^2 - 2a_0 a_1$, so to guarantee the trace is zero, we let $a_1 = \frac{c_d b_0^2}{2a_0}$.

The number of integers with absolute value between $-m$ and m is greater than a constant multiple times m. Thus, we bound $|S(Y)|$ by taking the product of the absolute value bounds for a_i and b_i, removing that of a_1, since it is no longer a degree of freedom when we require the trace to be zero.

$$|S(Y)| \gg (\prod_{i=2}^{n/2} Y^i)(\prod_{j=0}^{\frac{(n-d-1)}{2}} Y^{1/2+j}) = Y^{(\sum_{i=1}^{n/2} i)-1+(\sum_{j=0}^{\frac{n-d-1}{2}} j+1/2)}$$

$$= Y^{\frac{(n)(n/2+1)}{4}} Y^{\frac{n-d-1}{4}} Y^{\frac{(n-d-1)((n-d-1)/2+1)}{4}} Y^{-1} = Y^{\frac{1}{4}(n^2+(2-d)n+(d^2-3)/2-d)-1}$$

$$|S(Y)| \gg Y^{\frac{n^2+(1-2g)n+2g^2-6}{4}}$$

Note that in the last step we substitute $d = 2g+1$ to replace the degree of the curve with the genus. This is only for convenience.

We can perform the same procedure to bound $S(Y)$ when n is odd. In this case, we have

$$g(x) = \sum_{i=0}^{(n-1)/2} a_{(n-1)/2-i} x^i, \quad h(x) = \sum_{j=0}^{(n-d)/2} b_{(n-d)/2-j} x^j.$$

Now,

$$F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x) = \sum_{k=0}^{n} \Big((\sum_{l=0}^{d} \sum_{i+j=k+d-l} c_l b_i b_j) - (\sum_{i+j+1=k} a_i a_j) \Big) x^{n-k}.$$

The criteria are satisfied for $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x) \in S(Y)$ if $|a_i a_j| \ll Y^{i+j+1}$ and $|b_i b_j| \ll Y^{i+j}$. This may be accomplished by requiring $|a_i| \ll Y^{i+1/2}$ and $|b_i| \ll Y^i$.

To get that $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$ is trace zero, we need $c_{d-1}b_0^2 + c_d b_0 b_1 - a_0^2 = 0$, which is satisfied if $b_1 = \frac{a_0^2 - c_{d-1}b_0^2}{c_d b_0}$. Similar to before, we bound $S(Y)$ and find the same lower bound as even n.

$$|S(Y)| \gg (\prod_{i=0}^{(n-1)/2} Y^{i+1/2})(\prod_{j=2}^{\frac{(n-d)}{2}} Y^j) = Y^{(\sum_{i=0}^{(n-1)/2} i+1/2)+(\sum_{j=1}^{\frac{n-d}{2}} j)-1}$$

$$= Y^{\frac{n-1}{4}} Y^{\frac{(n-1)((n-1)/2+1)}{4}} Y^{\frac{(n-d)((n-d)/2+1)}{4}} Y^{-1} = Y^{\frac{1}{4}(n^2+(2-d)n+(d^2-3)/2-d)-1}$$

$$|S(Y)| \gg Y^{\frac{n^2+(1-2g)n+2g^2-6}{4}}$$

Suppose α_1, ..., α_n are the roots of an element $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x) \in S(Y)$. Then $|\alpha_i| \leq Y$ for all Y, so $|\alpha_i - \alpha_j| \leq 2|Y|$ and we have a lower bound for the discriminant,

$$disc(F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)) = \prod_{i<j} (\alpha_i - \alpha_j)^2 \leq Y^{2(n(n-1)/2)} = Y^{n(n-1)}.$$

Thus, our lower bound of $|S(Y)|$ is a bound for the number of polynomials with discriminant less than $Y^{n(n-1)}$ that define degree n fields inducing C to gain a point. Since the polynomial discriminant is divisible by the field discriminant, these fields also have discriminant less than $Y^{n(n-1)}$. It remains to correct this bound to reflect multiplicity; that is, to correct for the fact that multiple polynomials in $S(Y)$ might define the same field.

For a rough estimate of this multiplicity, we appeal directly to Ellenberg and Venkatesh [6]. They show that for each element of $S(Y)$, at most some constant multiple of $(\frac{Y}{\Delta^{(1/n(n-1))}})^{(n-1)}$

other elements produce an isomorphic field. Assuming the worst case scenario, that these fields have discriminant 1, we may obtain a rough lower bound for $N_n^{(C)}(Y^{n(n-1)})$ by dividing our bound for $|S(Y)|$ by Y^{n-1}.

$$N_n^{(C)}(Y^{n(n-1)}) \gg Y^{\frac{n^2-(3+2g)n+2g^2-2}{4}}$$

We then substitute $X = Y^{n(n-1)}$ to find

$$N_n^{(C)}(X) \gg X^{(\frac{1}{n(n-1)})(\frac{n^2-(3+2g)n+2g^2-2}{4})} = X^{\frac{1}{4}(1-\frac{2+2g}{n}+\frac{2g^2-2g-4}{n^2}\sum_{k=0}^{\infty}\frac{1}{n^k})},$$

$$N_n^{(C)}(X) \gg X^{\frac{1}{4}-\frac{1+g}{2n}+\frac{g^2-g-2}{2n(n-1)}}.$$

We can improve this lower bound by appealing to the work of Lemke Oliver and Thorne for a better estimate of the multiplicity. More precisely, if K is a field such that $K \cong \mathbb{Q}[x]/\phi(x)$ for some $\phi \in S(Y)$, define $M_K(Y)$ to be the number of polynomials in $S(Y)$ that are the characteristic polynomial for the same field. That is,

$$M_K(Y) = \#\left\{\, \phi(x) \in S(Y) \mid K \cong \mathbb{Q}[x]/\phi(x) \,\right\}.$$

Lemma 6.3 (Lemke Oliver - Thorne [9]). *Let k be the largest integer such that $k \leq n-1$ and $\Delta_K \leq Y^{n(n-1)/k}$. Then*

$$M_K(Y) \ll \frac{Y^k}{\Delta_K^{\frac{k(k+1)}{2n(n-1)}}}.$$

We can further show that this bound is decreasing with respect to discriminant. That is, for fields K and L with $\Delta_L \leq \Delta_K$, we can use the bound on $M_L(Y)$ given in Lemma 6.3 for $M_K(Y)$.

Corollary 6.4. *If K, L are number fields of degree n, satisfying $\Delta_L \leq \Delta_K \leq Y^{n(n-1)}$, and*

$1 \leq l \leq n-1$ *is the largest integer such that* $\Delta_L \leq Y^{n(n-1)/l}$*, then*

$$M_K(Y) \ll \frac{Y^l}{\Delta_L^{\frac{l(l+1)}{2n(n-1)}}}$$

Proof. When $k \leq n-2$ is fixed, $\Delta_K \in (Y^{n(n-1)/(k+1)}, Y^{n(n-1)/k}]$, we have that the bound is decreasing, because Δ_K appears in the denominator of the bound. In the case of $k = n-1$, this is still true for $\Delta_K \in [1, Y^n]$.

For a field K with $\Delta_K = Y^{n(n-1)/k}$ exactly, we are right on the boundary of being able to use k as the largest integer such that $\Delta_K \leq Y^{n(n-1)/k}$. In this case, the bound is

$$\frac{Y^k}{Y^{\frac{n(n-1)}{k}\frac{k(k+1)}{2n(n-1)}}} = Y^{(k-1)/2}.$$

On the other hand, taking $k-1$ to be the largest such integer, we obtain the bound

$$\frac{Y^{k-1}}{Y^{\frac{n(n-1)}{k}\frac{k(k-1)}{n2(n-1)}}} = \frac{Y^{k-1}}{Y^{(k-1)/2}} = Y^{(k-1)/2}.$$

This shows that the bound is piecewise continuous as a function in Δ_K. It is decreasing on each interval with respect to Δ_K, so it must be decreasing on the entire interval $[1, Y^{n(n-1)}]$. This yields the result that $M_K(Y)$ is bounded above by the upper bound on the multiplicity for L, where L is a field with $\Delta_L \leq \Delta_K$. □

Let $T \leq Y^n$. For any number field K with $\Delta_K \leq T$, Lemma 6.3 gives that

$$M_K \ll \frac{Y^{n-1}}{\Delta_K^{1/2}}.$$

We would like to find a value of T such that even with worst case multiplicity, all number fields with $\Delta \leq T$ aren't sufficient to generate the polynomials in $S(Y)$. That is, we want the sum

$$\sum_{\Delta_K \leq T} M_K(Y)$$

to be strictly less than $|S(Y)|$.

Recall $N_n(X)$ denotes the number of degree n number fields, with no restrictions on the Galois closure or otherwise. From Theorem 3.1, we have

$$N_n(X) \ll X^{(n+2)/4}.$$

We can use this to help find an upper bound for the sum above, by setting it up as an integral with respect to the number of fields, and evaluating using integration by parts.

$$\begin{aligned}
\frac{1}{Y^{n-1}} \int_{1/2}^{T} M_K(Y) = \int_{1/2}^{T} \frac{dN_n(t)}{t^{1/2}} &= \frac{N_n(t)}{t^{1/2}}\Big|_{1/2}^{T} + \frac{1}{2}\int_{1/2}^{T} \frac{N_n(t)}{t^{3/2}} dt \\
\ll \frac{t^{(n-2)/4}}{t^{1/2}}\Big|_{1/2}^{T} + \frac{1}{2}\int_{1/2}^{T} \frac{t^{(n-2)/4}}{t^{3/2}} dt &= T^{n/4} + \frac{2t^{n/4}}{n}\Big|_{1/2}^{T} + O(1) \\
&= (1+\frac{2}{n})T^{n/4} + O(1) \ll T^{n/4}
\end{aligned}$$

Thus, we have

$$\sum_{\Delta_K \leq T} M_K(Y) \ll Y^{n-1} T^{(n+2)/4} T^{-1/2} = Y^{n-1} T^{n/4}.$$

Setting this equal to $S(Y)$ and solving for T, we have

$$Y^{n-1} T^{n/4} = Y^{\frac{n^2+(1-2g)n+2g^2-6}{4}}$$

$$\implies T = Y^{n-(3+2g)+\frac{2g^2-2}{n}}$$

$Y^{n-(3+2g)}$ is always less than the above quantity, so we bound the sum

$$\sum_{\Delta_K \leq Y^{n-(3+2g)}} M_K(Y) \ll Y^{n-1} Y^{(n-(3+2g))/4},$$

which is strictly less than $|S(Y)|$.

This means that the fields with discriminants less than $Y^{n-(3+2g)}$ contribute negligibly to the total number of polynomials in $S(Y)$, so we need only count those that produce fields with discriminant between $Y^{n-(3+2g)}$ and $Y^{n(n-1)}$. Let $\Delta_{WC} = Y^{n-(3+2g)}$. Lemma 6.3 and Corollary 6.4 tell us that a discriminant of Δ_{WC} produces an upper bound on multiplicity for any field K with $Y^{n-(3+2)g} \leq \Delta_K \leq Y^{n(n-1)}$. That is, for any such K, we have

$$M_K(Y) \ll M_{WC}(Y) = \frac{Y^{n-1}}{\Delta_{WC}^{1/2}}.$$

We are now ready to compute a lower bound for $N_n^{(C)}(X, S_n)$, by dividing the size of our set of polynomials $S(Y)$ by the worst case multiplicity $M_{WC}(Y)$.

$$N_n^{(C)}(Y^{n(n-1)}) \gg \frac{|S(Y)|}{M_{WC}(Y)} \gg \frac{Y^{\frac{n^2+(1-2g)n+2g^2-6}{4}}}{\frac{Y^{n-1}}{Y^{\frac{n-(3+2g)}{2}}}}$$

$$= Y^{\frac{1}{4}(n^2-(1+2g)n+2g^2-4g-8)}$$

Replacing $Y^{n(n-1)}$ with X, we have

$$N_n^{(C)}(X, S_n) \gg X^{\frac{1}{4}(1-\frac{2g}{n}+\frac{2g^2-6g-8}{n(n-1)})}.$$

This is the bound given in Theorem 1.1, thus concluding the proof.

7 Further work

The most significant hypothesis in Theorem 1.1 is that the degree of C is odd - what about even degree hyperelliptic curves? If $C\colon y^2 = f(x)$, and $f(x)$ is even degree, consider the same parameterization described in Section 6,

$$F_n^{(C)}(\mathbf{a}, \mathbf{b}, x) = f(x)h(x)^2 - g(x)^2.$$

This polynomial will always have even degree in $\mathbb{Q}(\mathbf{a}, \mathbf{b})$. Thus, it appears our method will not yield odd degree fields over which C gains points. In fact, Bhargava, Gross, and Wang [2], proved that a positive proportion of such curves have no points in any odd degree extension of $\mathbb{Q}$, and that this proportion approaches 100% as the genus $g \to \infty$.

We can still hope to find even degree fields in this case, however, and expect that similar methods may be exploited to produce a bound on $N_n^{(C)}(X, S_n)$ for even n. If we assume the analogous version of Proposition 6.1, that $F_n^{(C)}(\mathbf{a}, \mathbf{b}, x)$ is irreducible in $\mathbb{Q}(\mathbf{a}, \mathbf{b})[x]$ with Galois group S_n, we may use identical techniques to find

$$N_n^{(C)}(X, S_n) \gg X^{\frac{1}{4}(1 - \frac{1+2g}{n} + \frac{2g^2-4g-9}{n(n-1)})}.$$

This bound is very similar to that found in Theorem 1.1.

Showing the Galois group is S_n proves to be somewhat harder in the even case. We are able to extend the Newton polygon methods from the odd case to find cycles of all lengths between 2 and $n/2$, as well as a product of disjoint $(n/2)$-cycles in the Galois group of a specialization $F_n^{(C)}(\mathbf{a}_0, \mathbf{b}_0, x)$. An $(n/2 + 1)$-cycle would be sufficient to show this group is S_n, and the proof of its existence in the Galois group remains in progress.

We also suppose in Theorem 1.1 that $n \geq d$, leaving room to ask about the case of smaller degree fields. We might hope to find a result comparable to Theorem 3.6 for $n > 2$, and to better understand when we should expect hyperelliptic curves to gain points over small degree fields. This would help to round out our understanding of how hyperelliptic curves gain points over number fields of any degree.

Another exciting extension of this work is the study of other families of curves. If we were to obtain bounds for the number of fields over which a different type of curve gains points, we could compare them to our results for hyperelliptic curves. Significant differences in these bounds might indicate a way to tell different families of algebraic curves apart using fields - a first step in the direction of answering the question posed by Mazur and Rubin.

References

[1] M. Bhargava, A. Shankar, and X. Wang. Squarefree values of polynomial discriminants I. *ArXiv e-prints*, November 2016.

[2] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang. A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension. *J. Amer. Math. Soc.*, 30(2):451–493, 2017. With an appendix by Tim Dokchitser and Vladimir Dokchitser.

[3] Keith Conrad. Generating sets. Expository paper, http://www.math.uconn.edu/ kconrad/blurbs/grouptheory/genset.pdf.

[4] Keith Conrad. Recognizing galois grous S_n and A_n. Expository paper, http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/galoisSnAn.pdf.

[5] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2004.

[6] Jordan S. Ellenberg and Akshay Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math. (2)*, 163(2):723–741, 2006.

[7] Andrew Granville. Rational and integral points on quadratic twists of a given hyperelliptic curve. *Int. Math. Res. Not. IMRN*, (8):Art. ID 027, 24, 2007.

[8] Michael Kölle and Peter Schmid. Computing Galois groups by means of Newton polygons. *Acta Arith.*, 115(1):71–84, 2004.

[9] Robert Lemke Oliver and Frank Thorne. Rank 2 nonabelian twists of elliptic curves. Work in progress.

[10] B. Mazur, K. Rubin, and M. Larsen. Diophantine stability. *ArXiv e-prints*, March 2015.

[11] Wolfgang M. Schmidt. Number fields of given degree and bounded discriminant. *Astérisque*, (228):4, 189–195, 1995. Columbia University Number Theory Seminar (New York, 1992).