

Diophantine Equations With Two Separated Variables

by
Benjamin Leonard Weiss

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2011

Doctoral Committee:

Professor Michael E. Zieve, Co-Chair
Professor Jeffrey C. Lagarias, Co-Chair
Professor Karen E. Smith
Professor Kevin J. Compton
Assistant Professor Bhargav Bhatt

© Benjamin L. Weiss 2011
All Rights Reserved

To Alison.

ACKNOWLEDGEMENTS

I thank Marie Snipes for her help constructing the many diagrams in Chapter VIII. I also thank Aubrey da Cunha for his many helpful conversations about combinatorics and graph theory which were useful in constructing the arguments in Chapter VIII.

I wish to acknowledge my advisor, Jeffrey Lagarias. For the past five years he has been instrumental in teaching me how to approach mathematics. He has been a very instructive mentor, and a tireless and goal-oriented advisor. I cannot thank him enough for the help and encouragement he has given me.

Finally, this thesis could not have been started nor finished without the tireless and patient help from my advisor, Michael Zieve. He found me a wonderful problem to work on, taught me the field and the techniques, and has helped me prove various theorems and edit every page. More so, he has been a great teacher; I enjoyed every meeting with him as there was always something interesting to discuss, and I am appreciative for having had the chance to learn from him.

I thank the National Science Foundation for partially supporting my training on an RTG grant, and for support from NSF grant DMS-0801029 for the writing of this thesis.

TABLE OF CONTENTS

DEDICATION	ii
ACKNOWLEDGEMENTS	iii
LIST OF FIGURES	vi
CHAPTER	
I. Introduction	1
II. Basic Concepts & Notation	11
2.1 Branch Points and Ramification Indices	11
2.2 Riemann-Hurwitz Formula	14
2.3 Equivalence of Polynomials and Polynomial Pairs	14
2.4 Cyclic Polynomials	15
2.5 Chebyshev and Dihedral Polynomials	16
2.6 Ramification Criteria for $G(X)$ to be Equivalent to a Power of a Polynomial	18
2.7 Decomposable Polynomials	19
2.8 Sporadic Pairs	19
III. Cyclic Polynomials	23
3.1 Strategy of Proof of Theorem III.1	24
3.2 Proof of Theorem III.1	24
IV. Power Free Polynomials: Three or More Branch Point Case	31
4.1 Strategy of the Proofs	33
4.2 Reduction Lemmas	34
4.3 Proof of Theorem IV.1	40
4.4 Three Branch Point Case: Proof of Theorem IV.2	40
4.5 Two Branch Point Case: Proof of Theorem IV.4	44
V. Power Free Polynomials: Two Shared Branch Points	49
5.1 Method of Proof	51
5.2 Preliminary Lemmas	52
5.3 Uniformity of Multisets	53
5.4 Main Results	57
5.5 Proof of Proposition V.10	57
5.6 Proof of Proposition V.11	60
5.7 Proof of Proposition V.12	61

5.8	Remaining Sporadic Cases	65
5.8.1	$\ell = \mathbf{2}$	65
5.8.2	$\ell = \mathbf{3}$	76
5.8.3	$\ell > \frac{\mathbf{n-3}}{\mathbf{2}}$	80
5.9	Proof of Theorem V.1	115
VI. Irreducibility of $G(X) - H(Y)$		116
6.1	Main Theorems	116
6.2	Strategy of Proof	118
6.3	Fried's Theorem on Decomposability	119
6.4	Ramification and Irreducibility Criteria	120
6.5	Proof of Theorem VI.1	121
6.6	Proof of Theorem VI.3	122
6.7	Proof of Theorem VI.2	123
6.8	Decompositions of Polynomials from Theorem VI.5	124
6.9	Optimal Decompositions of Polynomials from Theorem VI.5	136
6.10	Proof Theorem VI.5	140
VII. Proofs of the Main Theorems		142
7.1	Faltings' theorem and its converse	142
7.2	Reducibility of $G(X) - H(Y)$ when G and H are indecomposable	143
7.3	Proof of Theorem I.4	144
7.4	Proof of Theorem I.5	146
VIII. Counting Equivalence Classes of Polynomials of Given Degrees		148
8.1	Equivalence and Right-Equivalence	148
8.2	Multiplicity Theorems	150
8.3	Riemann's Existence Theorem	151
8.4	Strategy of the Proofs	153
8.5	Connectivity of Graphs	154
8.6	Proofs of Multiplicity Theorems	154
8.7	Multiplicity Results Counting Indecomposable Polynomials	178
IX. Powers of Non-Linear Polynomials		181
APPENDIX		196
BIBLIOGRAPHY		202

LIST OF FIGURES

Figure

8.1	The Graph of Actions in Theorem VIII.4	155
8.2	The Graph of Actions in Theorem VIII.5	157
8.3	The Graph of Actions in Theorem VIII.6	159
8.4	The Graph of Actions in Theorem VIII.7	161
8.5	The First Graph of Actions in Theorem VIII.8	163
8.6	The Second Graph of Actions in Theorem VIII.8	163
8.7	The Graph of Actions in Theorem VIII.9	166
8.8	The First Graph of Actions in Theorem VIII.10	171
8.9	The Second Graph of Actions in Theorem VIII.10	172
8.10	The Third Graph of Actions in Theorem VIII.10	172
8.11	The Graph of All 2-cycles in Theorem VIII.11	174
8.12	The First Graph with a 3-cycle in Theorem VIII.11	174
8.13	The Second Graph with a 3-cycle in Theorem VIII.11	175
8.14	The Third Graph with a 3-cycle in Theorem VIII.11	175
8.15	The First Graph with a 4-cycle in Theorem VIII.11	176
8.16	The Second Graph with a 4-cycle in Theorem VIII.11	177
8.17	The Third Graph with a 4-cycle in Theorem VIII.11	177
8.18	The Fourth Graph with a 4-cycle in Theorem VIII.11	178

CHAPTER I

Introduction

This thesis addresses the following problem:

Problem I.1. *Determine all polynomials $G(T), H(T) \in \mathbb{Q}[T]$ for which the equation $G(X) = H(Y)$ has infinitely many solutions in $\mathbb{Q} \times \mathbb{Q}$.*

Special cases of this problem have served as milestones throughout the history of number theory. For instance, Archimedes studied an instance of the Pell equation¹ $X^2 = dY^2 + 1$; this equation was later shown to have infinitely many integral solutions for any fixed nonsquare integer $d > 0$ [15, p. 184]. Significant portions of algebraic number theory were developed in order to study integral solutions of the Fermat equation $U^n = V^n + W^n$; for any such solution with $W \neq 0$, dividing by W^n yields a rational solution of the equation $X^n = Y^n + 1$. Finally, Problem I.1 includes the problem of determining which elliptic curves $X^2 = Y^3 + aY + b$ (with $a, b \in \mathbb{Q}$ fixed) have infinitely many rational points, or equivalently, have positive rank; this rank is the key quantity in the Birch–Swinnerton-Dyer conjecture.

It is also of interest to study the analogue of Problem I.1 over an arbitrary algebraic number field. This leads to the following problem, which addresses all number fields at once:

¹Named by Euler because he confused Pell with Brouncker, both of whom were English mathematicians who did not study this equation.

Problem I.2. *Determine all $G(T), H(T) \in \overline{\mathbb{Q}}[T]$ for which there exists a number field K such that the equation $G(X) = H(Y)$ has infinitely many solutions in $K \times K$.*

We will show in Section 7.1 that, due to Faltings' theorem (previously Mordell's conjecture), the arithmetical Problem I.2 is equivalent to the following geometric Problem I.3:

Problem I.3. *Classify all nonconstant $G(T), H(T) \in \overline{\mathbb{Q}}[T]$ such that $G(X) = H(Y)$ has an irreducible factor $F(X, Y) \in \overline{\mathbb{Q}}[X, Y]$ for which the curve $F(X, Y) = 0$ has genus zero or one.*

Here, by the *genus* of $F(X, Y) = 0$, we mean the geometric genus of the unique smooth, projective, irreducible curve over \mathbb{C} which is birationally equivalent to the affine plane curve $F(X, Y) = 0$ (for more details, see [5] or [12]).

We will address a generalization of Problem I.3, in which $\overline{\mathbb{Q}}$ is replaced by an arbitrary algebraically closed field \mathbb{K} of characteristic zero. This generalization is useful for applications to complex analysis, including the theory of uniqueness polynomials and unique range sets in value distribution theory. We solve the “genus zero half” of this generalized problem in two situations. The first situation is that $G, H \in \mathbb{K}[T]$ are *indecomposable*, which means that they are nonconstant polynomials that cannot be written as the composition of two nonlinear polynomials. Note that all polynomials of prime degree are indecomposable, and that a randomly chosen polynomial of any fixed degree $d \geq 2$ will be indecomposable with probability one.

Theorem I.4. *Let \mathbb{K} be an algebraically closed field of characteristic zero, and let $G, H \in \mathbb{K}[T]$ be indecomposable. The curve $G(X) = H(Y)$ has an irreducible component of genus zero if and only if the pair $(G(X), H(Y))$ is equivalent (in the sense of Definition I.7) to one of the following pairs:*

0. $(F(X), F(Y))$ with $F(Y) \in \mathbb{K}[Y]$;
1. $(X^m, Y^a F(Y)^m)$ with m prime, a an integer satisfying $0 < a < m$, and $F(Y) \in \mathbb{K}[Y]$;
2. $(X^m, Y^a(Y-1)^{m-a}F(Y)^m)$ with m prime, a an integer satisfying $0 < a < m$, and $F(Y) \in \mathbb{K}[Y]$;
3. $(X^a(X-1)^{m-a}, cY^a(Y-1)^{m-a})$ with $c \in \mathbb{K} \setminus \{0, 1\}$ and $m, a \in \mathbb{Z}$ such that $0 < a < m$ and $(a, m) = 1$;
4. $(T_m(X), T_n(Y))$ with m, n distinct primes, where $T_m(X)$ denotes the normalized degree- m Chebyshev polynomial (see Definition I.6);
5. $(T_m(X), F(Y))$ with m an odd prime and $F(Y) \in \mathbb{K}[Y]$ such that $m \mid \deg(F)$ and one of the following holds:
 - (a) $F(Y)^2 - 4 = P(Y)Q(Y)^2R(Y)^4$ for some coprime, squarefree polynomials $P, Q, R \in \mathbb{K}[Y]$ with $\deg(P) = 4$ and $\deg(R) = 1$;
 - (b) $F(Y)^2 - 4 = P(Y)Q(Y)^2R(Y)^3$ for some coprime, squarefree polynomials $P, Q, R \in \mathbb{K}[Y]$ with $\deg(P) = 3$ and $\deg(R) = 1$;
 - (c) $F(Y)^2 - 4 = P(Y)Q(Y)^2$ for some coprime, squarefree polynomials $P, Q \in \mathbb{K}[Y]$ with $\deg(P) = 4$;
6. Any pair of polynomials listed in Section 2.8, except for the pair in case 4 or a pair in case 12 which includes a polynomial from case 12(a). (Note that all polynomials listed in Section 2.8 have degree at most 13.)

Although we do not know explicit forms for all solutions of the “polynomial Pell equations” occurring in case 5 of this result, we are able to count the solutions to our original problem which arise from each such Pell equation. To this end, fix an odd

prime m and a positive multiple n of m . Let $S_a(n, m)$ be the set of equivalence classes of pairs of polynomials in $\mathbb{K}[T]$ which include a pair of the form $(T_m(X), F(Y))$ where $F(Y)$ is an indecomposable degree n polynomial satisfying the constraint in case 5(a) of the above result, and define $S_b(n, m)$ and $S_c(n, m)$ analogously. Then

$$\begin{aligned} |S_a(n, m)| &= \frac{n-6}{24} J_2(n) + \frac{1}{2} \phi(n) \\ |S_b(n, m)| &= \frac{1}{6} J_2(n) - \frac{1}{2} \phi(n) \quad \text{if } n > 3 \end{aligned}$$

where

$$J_k(n) := n^k \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p^k}\right)$$

is Jacobi's totient function and $\phi(n) := J_1(n)$ is Euler's totient function. The set $S_c(n, m)$ is infinite.

Theorem I.4 restricts to indecomposable polynomials G and H . Our next result solves Problem I.3 in a setting which allows decomposable polynomials. Specifically, we will assume that G and H satisfy the following hypotheses:

H1: $G(X) - H(Y)$ is irreducible in $\overline{\mathbb{Q}}[X, Y]$.

H2: The curve $G(X) = H(Y)$ has genus zero.

H3: For each $U(T) \in \{G(T), H(T)\}$ and each $\lambda \in \overline{\mathbb{Q}}$, if $U(T) + \lambda$ is a power of a lower-degree polynomial then $U(T) + \lambda = \nu(T)^k$ for some linear $\nu \in \overline{\mathbb{Q}}[T]$ and some positive integer k .

Theorem I.5. *Let \mathbb{K} be an algebraically closed field of characteristic zero. If $G(T)$ and $H(T)$ are nonconstant polynomials in $\mathbb{K}[T]$ satisfying conditions H1–H3, then $(G(X), H(Y))$ is equivalent to one of the following pairs (in which a and m are coprime positive integers, and $F(Y) \in \mathbb{K}[Y]$ is nonzero):*

1. $(X^m, Y^a F(Y)^m)$;
2. $(X^m, Y^a(Y-1)^{m-a} F(Y)^m)$ where $a < m$;
3. $(X^a(X-1)^{m-a}, cY^a(Y-1)^{m-a})$ where $a < m$ and $c \in \mathbb{K} \setminus \{0, 1\}$;
4. $(T_m(X), T_n(Y))$ where $m, n > 1$ are coprime;
5. $(T_m(X), F(Y))$ where $m > 1$ is odd and $F(Y)$ satisfies one of the following (with $n := \deg(F)$):
 - (a) $F(Y)^2 - 4 = P(Y)Q(Y)^2R(Y)^4$ for some coprime, squarefree polynomials $P, Q, R \in \mathbb{K}[Y]$ with $\deg(P) = 4$ and $\deg(R) = 1$;
 - (b) $F(Y)^2 - 4 = P(Y)Q(Y)^2R(Y)^3$ for some coprime, squarefree polynomials $P, Q, R \in \mathbb{K}[Y]$ with $\deg(P) = 3$ and $\deg(R) = 1$;
 - (c) $F(Y)^2 - 4 = P(Y)Q(Y)^2$ for some coprime, squarefree polynomials $P, Q \in \mathbb{K}[Y]$ with $\deg(P) = 4$;
6. A pair of polynomials from cases 1–23 of Section 2.8 (in which case both G and H have degree at most 10).

Conversely, for any $G(T), H(T) \in \mathbb{K}[T]$ such that $(G(X), H(Y))$ is equivalent to a pair in the above list, hypotheses H1–H3 hold for G and H if and only if none of the following hold:

- in case 1: $m = 1$ and $U(T) = T^a F(T)$ violates H3;
- in case 1: $m > 1$ and $Y^a F(Y)$ is a power of a lower-degree polynomial;
- in case 2: $m > 2$ and $Y(Y-1)F(Y)^2 = c \cdot (-4 + T_r(4Y-2)^2)$ with $r > 1$ and $c \in \mathbb{K}^*$;
- in case 2: $Y^a(Y-1)^{m-a} F(Y)^m$ is a power of a lower-degree polynomial;

- *in case 5: either $F(Y) + 2$ or $F(Y) - 2$ is a square.*

The similarity between the previous two results suggests that *perhaps all solutions of Problem I.3 have a shape resembling one of the solutions occurring in our results.* We are presently studying Problem I.3 in general, and we will report our findings elsewhere.

We can count the solutions occurring in case 5 of Theorem I.5. For instance, pick an odd $m > 1$ and a positive multiple n of m . Let N be the number of equivalence classes which contain a pair $(T_m(X), F(Y))$ with $F(Y)$ a degree- n polynomial satisfying the constraint in case 5(b). Then N is the least integer such that $N \geq a^2 J_2(b)$, where $n = ab$ and a is the “coprime-to- $2m$ ” part of n ; thus, a, b are coprime positive integers such that $n = ab$, and for any prime factor p of n we have $p \mid b$ if and only if $p \mid 2m$.

In the first four cases of Theorem I.5, we can exhibit infinitely many solutions to $G(X) = H(Y)$ in some number field K :

1. If $F(Y)$ lies in $K[Y]$, then the equation $X^m = Y^a F(Y)^m$ is solved by $X = t^a F(t^m)$ and $Y = t^m$ for any $t \in K$;
2. If $F(Y)$ lies in $K[Y]$, then the equation $X^m = Y^a (Y - 1)^{m-a} F(Y)^m$ is solved by $X = t^{a-m} Y F(Y)$ and $Y = \frac{t^m}{t^m - 1}$, for any $t \in K$ such that $t^m \neq 1$;
3. For any $c \in K \setminus \{0, 1\}$, the equation $X^a (X - 1)^{m-a} = c Y^a (Y - 1)^{m-a}$ is solved by $X = \frac{c^u t^a - 1}{c^{u+v} t^m - 1}$ and $Y = c^v t^{m-a} X$, where $u, v \in \mathbb{Z}$ satisfy $(m - a)u - av = 1$ and $t \in K$ satisfies $c^{u+v} t^m \neq 1$.
4. The equation $T_m(X) = T_n(Y)$ is solved by $X = T_n(t)$ and $Y = T_m(t)$ for any $t \in \mathbb{Q}$.

In a subsequent paper we will describe the number fields K in which $G(X) = H(Y)$ has infinitely many solutions, for each pair $(G(X), H(Y))$ occurring in Theorem I.4 or Theorem I.5. In particular, we will describe all pairs from these theorems which yield solutions to Problem I.1. A simple example from case 5(b) of Theorem I.5 is $T_3(X) = T_k(Y^3 - 2)$, which is solved by $X = T_k\left(\frac{t^3 + 2}{t^3 - 1}\right)$ and $Y = \frac{3t}{t^3 - 1}$ for any $t \in \mathbb{Q}$.

The above results use the following terminology.

Definition I.6. The *normalized Chebyshev polynomial of degree m* is the unique polynomial $T_m(X) \in \mathbb{Z}[X]$ which satisfies the functional equation $T_m(U + U^{-1}) = U^m + U^{-m}$; see Section 2.5 for more details.

Definition I.7. For any field K , and any $G, H, \overline{G}, \overline{H} \in K[T] \setminus K$, we say that the pairs $(G(X), H(Y))$ and $(\overline{G}(X), \overline{H}(Y))$ are *equivalent* (over K) if there exist linear $\mu, \nu, \phi \in K[T]$ such that either

$$G = \mu \circ \overline{G} \circ \nu \quad \text{and} \quad H = \mu \circ \overline{H} \circ \phi$$

or

$$G = \mu \circ \overline{H} \circ \nu \quad \text{and} \quad H = \mu \circ \overline{G} \circ \phi.$$

We will discuss this notion further in Section 2.3. In particular, if (G, H) satisfies H1–H3 then so does any equivalent pair $(\overline{G}, \overline{H})$. Also, if K is algebraically closed then equivalence over K (for pairs of polynomials over K) is the same as equivalence over any extension of K .

Several authors have studied Problem I.3 for specific families of polynomials. For example, the equation

$$X(X + d_1) \cdots (X + (m_1 - 1)d_1) = Y(Y + d_2) \cdots (Y + (m_2 - 1)d_2),$$

for given integers d_1, d_2, m_1 and m_2 was studied in a long series of papers, culminating in a definitive account by Beukers, Shorey and Tijdeman [3]. The equation

$$X^m + X^{m-1} + \cdots + X + 1 = Y^n + Y^{n-1} + \cdots + Y + 1$$

with $n > m > 1$ was studied by Davenport, Lewis and Schinzel [7]. Other papers have examined the situation when the two polynomials are Bernoulli polynomials, power-sum polynomials, Jacobi polynomials, or members of several other distinguished families of polynomials.

A few authors have studied Problem I.3 for more general classes of polynomials G and H , although nearly all prior work in this direction has restricted to the case $\gcd(\deg(G), \deg(H)) \leq 2$. Ritt [18] classified the cases when $G(X)$ and $H(Y)$ have co-prime degrees and $G(X) = H(Y)$ has genus zero. Following subsequent developments by Fried, Schinzel, and others, Bilu and Tichy [4] classified the cases when $\gcd(\deg(G), \deg(H)) = 2$ and $G(X) = H(Y)$ has a genus-zero component. Avanzi and Zannier [1] classified the cases when $G(X)$ and $H(Y)$ have co-prime degrees and $G(X) = H(Y)$ has genus one. Without any assumption on $\gcd(\deg(G), \deg(H))$, Bilu and Tichy [4] classified the cases when $G(X) = H(Y)$ has a genus-zero component with at most two places at infinity; as a corollary, they solved the analogue of Problem I.1 over the integers. Finally, Avanzi and Zannier [2] determined all instances when $G(X) = H(Y)$ has a genus-zero component, under the assumption that H is a constant times G .

We build on the techniques of these prior papers when possible; in particular, the arguments in chapter 3 (which addresses the case that $H(Y) = Y^n$) follow those of Avanzi and Zannier [1]. However, the hypothesis $\gcd(\deg(G), \deg(H)) \leq 2$ was crucially used in the prior papers; since we do not assume this hypothesis, we are forced to introduce new techniques to handle the situations that arise in this thesis.

We note that all solutions in cases 5 and 6 of our results have $\gcd(\deg(G), \deg(H)) > 2$, as do all solutions in cases 2 and 3 with $m > 2$.

We now outline the proofs of our results. Assuming that $G(X) - H(Y)$ is irreducible, we express the genus of the curve $G(X) = H(Y)$ in terms of the ramification of the maps $G: \mathbb{P}^1 \rightarrow \mathbb{P}^1$ and $H: \mathbb{P}^1 \rightarrow \mathbb{P}^1$. We then determine which numerically plausible ramification configurations could conceivably yield genus-zero curves. At the same time, we obtain a converse result: if $G(X)$ and $H(Y)$ have the stated ramification, and $G(X) - H(Y)$ is irreducible, then the curve $G(X) = H(Y)$ has genus zero. We use various techniques and results from Galois theory and from the theory of functional decomposition in order to describe which pairs (G, H) having the required ramification yield irreducible polynomials $G(X) - H(Y)$. The shape of the answer is that either (G, H) is equivalent to a pair listed in cases 1, 2, 3, 4, or 6 of the above results, or (G, H) is equivalent to a pair $(T_m(X), T_k(F(Y)))$ where $\gcd(k, m) = 1$ and $F(Y)$ is an indecomposable polynomial whose ramification type lies in one of eight infinite families. These eight families of ramification types are encoded in the functional equations in case 5 of the above results. This yields Theorem I.5; we obtain Theorem I.4 by applying known results about irreducibility of polynomials of the form $G(X) - H(Y)$. Then, over the complex numbers, we use Riemann's existence theorem (see Theorem VIII.13) to translate the problem of counting equivalence classes of pairs $(T_m(X), T_k(F(Y)))$ of prescribed degrees and prescribed ramification types into the problem of counting tuples of elements of the symmetric group S_n which satisfy certain constraints. For each of our eight families of ramification types, we count these tuples via graph-theoretic techniques. Finally, we use descent and specialization to deduce the counts of polynomials over an arbitrary algebraically closed field \mathbb{K} of characteristic zero from the counts in the case

$\mathbb{K} = \mathbb{C}$.

This thesis is organized as follows. In Chapter II we introduce some notation and lemmas which will be used throughout the thesis. In Chapter III we determine all $G(X)$ for which $G(X) = Y^n$ has genus zero, assuming that $G(X) - Y^n$ is irreducible. In Chapter IV, assuming that G and H satisfy hypotheses H1–H3, we determine all possibilities in which at least finite points occur as branch points of G and/or H . This leaves the situation in which G and H have the same two finite branch points (and no other finite branch points), which we treat in Chapter V by an assortment of techniques. In Chapter VI we determine which pairs of polynomials $(G(X), H(Y))$ arising in previous chapters will actually yield irreducible polynomials $G(X) - H(Y)$; this involves a comprehensive study of the functional decompositions of G and H . In Chapter VII we prove our main results by combining the results of previous chapters. In Chapter VIII we apply Riemann’s existence theorem to count the number of polynomials of a given degree in the infinite families which arise in our results. Finally in Chapter IX we will present our partial results on the classification of genus zero curves defined by $G(X) - H(Y)$ when $H(Y) = H_0(Y)^r$ for some $r \geq 2$.

CHAPTER II

Basic Concepts & Notation

In this chapter we will set notation used throughout the thesis. We will also state some key definitions and concepts.

Notation II.1. Throughout this thesis, \mathbb{K} is an algebraically closed field of characteristic zero. Also, $G(X)$ and $H(Y)$ always denote non-constant polynomials. We will let $m = \deg(G(X))$ and $n = \deg(H(Y))$, so $m, n \geq 1$. We will also let $d = \gcd(m, n)$.

2.1 Branch Points and Ramification Indices

Definition II.2. Given any non-constant polynomial $G(X) \in \mathbb{K}[X]$ and constant $\lambda \in \mathbb{K}$ we can factor

$$G(X) - \lambda = c \prod_{i=1}^k (X - x_i)^{r_i}$$

where the r_i 's are positive integers, the x_i 's are distinct elements of \mathbb{K} , and $c \in \mathbb{K}^*$. We define the *ramification indices* of $G(X)$ over the point λ to be the numbers r_1, r_2, \dots, r_k . The *ramification multiset* is the multiset $[r_1, \dots, r_k]$.

Definition II.3. We define a (*finite*) *branch point* of $G(X)$ to be any $\lambda \in \mathbb{K}$ such that $G(X)$ has some ramification index $r_i \geq 2$ over the point λ . We let $\text{Br}(G)$ denote the set of all branch points of G .

Notation II.4. For $G(X), H(X) \in \mathbb{K}[X]$, let $\mathcal{G}_1, \dots, \mathcal{G}_R$ (resp. $\mathcal{H}_1, \dots, \mathcal{H}_R$) be the multisets of ramification indices of $G(X)$ (resp. $H(X)$) over $\text{Br}(G) \cup \text{Br}(H)$. We will also adopt the convention that \mathcal{G}_i and \mathcal{H}_i (for any $1 \leq i \leq R$) are the ramification indices of $G(X)$ and $H(Y)$ over the same point.

Notation II.5. When writing the elements of a multiset, we use exponents to denote the number of elements of the multiset which take a prescribed value. For example:

$$[3, 2, 2, 2, 1, 1] = [3, 2^3, 1^2].$$

The following simple results about ramification multisets play a crucial role in this thesis.

Lemma II.6. *For each $1 \leq i \leq R$ we have*

$$\sum_{\alpha \in \mathcal{G}_i} \alpha = m;$$

and

$$\sum_{\beta \in \mathcal{H}_i} \beta = n.$$

Proof. For any λ_i , we have

$$G(X) - \lambda_i = c \prod_{j=1}^k (X - x_j)^{\alpha_j}$$

where the α_j 's are the ramification indices of G over λ_i . Equating degrees of both sides yields the first equation in the result. The second equation is proved similarly.

□

Lemma II.7. *The following two relations hold:*

$$\sum_{i=1}^R \sum_{\alpha \in \mathcal{G}_i} [\alpha - 1] = m - 1;$$

$$\sum_{i=1}^R \sum_{\beta \in \mathcal{H}_i} [\beta - 1] = n - 1.$$

Proof. For any $\lambda \in \mathbb{K}$, the multiplicity of λ as a root of $G(X) - G(\lambda)$ is one more than the multiplicity of λ as a root of $G'(X)$. The first relation in the result now follows from equating degrees of both sides of the equation

$$G'(X) = c \prod_{i=1}^k (X - \alpha_i)^{r_i}.$$

The second relation is proved similarly. \square

The next lemma is a proof that ramification indices are multiplicative under composition.

Lemma II.8. *Let $F, \mu, \nu \in \mathbb{K}[X] \setminus \mathbb{K}$ satisfy $F = \mu \circ \nu$. Let $\lambda, \psi_1, \psi_2, \dots, \psi_r \in \mathbb{K}$ satisfy $\mu^{-1}(\lambda) = \{\psi_1, \dots, \psi_r\}$. Let e_1, \dots, e_r be the ramification indices of $\mu(X)$ over λ , i.e.*

$$\mu(X) - \lambda = c \prod_{i=1}^r (X - \psi_i)^{e_i}$$

with the ψ_i 's being distinct elements of \mathbb{K} , the e_i 's being positive integers, and $c \in \mathbb{K}^$. Let $\mathcal{N}_1, \dots, \mathcal{N}_r$ be the multisets of ramification indices of $\nu(X)$ over ψ_1, \dots, ψ_r , respectively. Then the ramification multiset of $F(X)$ over λ is*

$$\bigcup_{i=1}^r \{e_i a : a \in \mathcal{N}_i\}.$$

Proof. We denote the ramification indices of $\nu(X)$ over ψ_i as $a_{i,j}$ for $1 \leq j \leq s_i$, and the leading coefficient of $\nu(X)$ as k . Then

$$\begin{aligned} F(X) - \lambda &= \mu(\nu(X)) - \lambda \\ &= c \prod_{i=1}^r (\nu(X) - \psi_i)^{e_i} \\ &= c \prod_{i=1}^r \left(k \prod_{j=1}^{s_i} (X - x_{i,j})^{a_{i,j}} \right)^{e_i} \\ &= c \prod_{i=1}^r k^{e_i} \prod_{j=1}^{s_i} (X - x_{i,j})^{a_{i,j} e_i}. \end{aligned} \quad \square$$

2.2 Riemann-Hurwitz Formula

We will use the following instance of the Riemann-Hurwitz genus formula.

Lemma II.9 (Riemann-Hurwitz Formula). *Suppose that $G(X) - H(Y)$ is irreducible.*

If the curve $\mathcal{C}: G(X) = H(Y)$ has genus g then

$$\sum_{i=1}^R \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\alpha - (\alpha, \beta)] = m + d + 2g - 2$$

and

$$\sum_{i=1}^R \sum_{\beta \in \mathcal{H}_i} \sum_{\alpha \in \mathcal{G}_i} [\beta - (\alpha, \beta)] = n + d + 2g - 2.$$

This lemma is derived by Avanzi and Zannier [1, Remark 2.6]. However, they do not prove their Proposition 2.5 (which is crucial for the proof), but a proof is given by Müller and Zieve [17, Lemma 3.1]. By subtracting the equations in Lemma II.7 from the equations in Lemma II.9 we deduce the following corollary:

Corollary II.10. *Suppose that $G(X) - H(Y)$ is irreducible. If the curve $\mathcal{C}: G(X) = H(Y)$ has genus g then*

$$\sum_{i=1}^R \sum_{\alpha \in \mathcal{G}_i} \left(\sum_{\beta \in \mathcal{H}_i} [\alpha - (\alpha, \beta)] - (\alpha - 1) \right) = d + 2g - 1$$

and

$$\sum_{i=1}^R \sum_{\beta \in \mathcal{H}_i} \left(\sum_{\alpha \in \mathcal{G}_i} [\beta - (\alpha, \beta)] - (\beta - 1) \right) = d + 2g - 1.$$

2.3 Equivalence of Polynomials and Polynomial Pairs

Definition II.11. We say two polynomials G and \overline{G} with coefficients in \mathbb{K} are *equivalent* if there are two linear polynomials $\mu, \psi \in \mathbb{K}[X]$ such that

$$\overline{G} = \mu \circ G \circ \psi.$$

We remark that two equivalent polynomials have the same number of branch points as one another, and there is a bijection between their branch points which induces a bijection between ramification multisets.

Definition II.12. We say two pairs of polynomials (G, H) and $(\overline{G}, \overline{H})$ with coefficients in \mathbb{K} are *equivalent* if there are three linear polynomials $\mu, \psi, \phi \in \mathbb{K}[X]$ such that $(\overline{G}, \overline{H})$ is either

$$(\mu \circ G \circ \psi, \mu \circ H \circ \phi)$$

or

$$(\mu \circ H \circ \psi, \mu \circ G \circ \phi).$$

Let us mention some consequences of the equivalence of two pairs (G, H) and $(\overline{G}, \overline{H})$. First, $G(X) - H(Y)$ is irreducible if and only if $\overline{G}(X) - \overline{H}(Y)$ is irreducible. Also, assuming irreducibility, the genus of $G(X) = H(Y)$ equals the genus of $\overline{G}(X) = \overline{H}(Y)$. Finally, there is a bijection $\psi: \text{Br}(G) \cup \text{Br}(H) \rightarrow \text{Br}(\overline{G}) \cup \text{Br}(\overline{H})$ such that the unordered pair of ramification multisets of G and H over a point P equals the unordered pair of ramification multisets of \overline{G} and \overline{H} over $\psi(P)$.

2.4 Cyclic Polynomials

Polynomials that are equivalent to X^m play a key role in this thesis.

Definition II.13. [Cyclic Polynomials] We define *cyclic polynomials* to be those polynomials which are equivalent to X^m for some positive integer m .

Lemma II.14. *Let $G(X) \in \mathbb{K}[X]$ have degree $m \geq 2$. Then $G(X)$ is cyclic if and only if it has a unique finite branch point. This branch point necessarily has ramification multiset $[m]$.*

Proof. See Müller and Zieve [17, Lemma 3.2]. □

2.5 Chebyshev and Dihedral Polynomials

Polynomials that are equivalent to $T_m(X)$, the (normalized) Chebyshev polynomial, also play a key role in this thesis.

Definition II.15. [Chebyshev Polynomials] We define the (*normalized*) Chebyshev polynomial of degree $m \geq 1$ to be the unique polynomial which satisfies the functional equation

$$T_m\left(X + \frac{1}{X}\right) = X^m + \frac{1}{X^m}.$$

The polynomial $T_m(X)$ is sometimes denoted $D_m(X, 1)$, and referred to as the degree- m Dickson polynomial with parameter 1. The usual Chebyshev polynomial $C_m(X)$ is defined by $C_m(\cos \theta) = \cos m\theta$, and is related to $T_m(X)$ by $C_m(X) = \frac{1}{2}T_m(2X)$.

Lemma II.16. Fix an odd integer $m \geq 3$. Then the finite branch points of $T_m(X)$ are 2 and -2 , each of which have ramification multiset $\left[2^{\frac{m-1}{2}}, 1\right]$. The unique preimage of 2 under $T_m(X)$ which has ramification index 1 is $X = 2$; the unique preimage of -2 under $T_m(X)$ which has ramification index 1 is $X = -2$.

Proof. For $m = 2k + 1$ and ζ_m a primitive m^{th} root of unity, we have

$$\begin{aligned} T_m\left(U + \frac{1}{U}\right) - 2 &= U^m + \frac{1}{U^m} - 2 \\ &= \frac{(U^m - 1)^2}{U} \\ &= \frac{(U - 1)^2}{U} \prod_{j=1}^k \frac{(U - \zeta_m^j)^2 (U - \frac{1}{\zeta_m^j})^2}{U^2}. \end{aligned}$$

Substituting $X = U + U^{-1}$ gives

$$T_m(X) - 2 = (X - 2) \prod_{j=1}^k \left(X - \left(\zeta_m^j + \frac{1}{\zeta_m^j}\right)\right)^2.$$

Since $T_m(-X) = -T_m(X)$ for odd m , we have

$$T_m(X) + 2 = (X + 2) \prod_{j=1}^k \left(X + \left(\zeta_m^j + \frac{1}{\zeta_m^j} \right) \right)^2.$$

Thus these two branch points have ramification indices $\left[2^{\frac{m-1}{2}}, 1 \right]$ and $\sum_{\alpha \in \mathcal{G}_i} (\alpha - 1) = \frac{m-1}{2}$ for each of them. However Lemma II.7 says that

$$\sum_{i=1}^R \sum_{\alpha \in \mathcal{G}_i} [\alpha - 1] = m - 1.$$

Using the fact that any branch point contributes $\sum_{\alpha \in \mathcal{G}_i} [\alpha - 1] > 0$, we conclude that $R = 2$, hence -2 and 2 are the only finite branch points. \square

Definition II.17. [Dihedral Polynomials] We define a *dihedral polynomial* to be any polynomial which is equivalent to $T_m(X)$ for some integer $m \geq 2$.

We make use of the following well known characterization of dihedral polynomials.

Lemma II.18. *Let $G(X) \in \mathbb{K}[X]$ have degree $m \geq 1$.*

1. *$G(X)$ is dihedral of degree at least 3 if and only if it has precisely two branch points, each having maximal ramification index 2.*
2. *If $G(X)$ is a dihedral polynomial of odd degree m , then its two branch points both have ramification type $\left[2^{\frac{m-1}{2}}, 1 \right]$.*

Proof. (1) is shown in Müller and Zieve [17, Lemma 3.2]. (2) follows from Lemma II.16. \square

We will also need the fact that odd degree Chebyshev polynomials are odd polynomials.

Lemma II.19. *Let m be an odd positive integer. Then $T_m(X)$ is an odd polynomial.*

Proof. For any $x \in \mathbb{K}$ let $\alpha \in \mathbb{K}$ be such that

$$x = \alpha + \frac{1}{\alpha}.$$

Then

$$T_m(-x) = T_m\left(-\alpha + \frac{1}{-\alpha}\right) = -\alpha^m - \frac{1}{\alpha^m} = -T_m(x).$$

□

2.6 Ramification Criteria for $G(X)$ to be Equivalent to a Power of a Polynomial

In this thesis we shall prove some theorems having as a hypothesis that neither $G(X)$ nor $H(Y)$ is equivalent to a power of a polynomial. Here we reformulate this hypothesis in terms of the ramification types of $G(X)$ and $H(Y)$.

Lemma II.20. *A non-constant polynomial $G(X) \in \mathbb{K}[X]$ is equivalent to a power of a smaller degree polynomial if and only if there is a finite branch point, λ , of $G(X)$ such that the multiset \mathcal{G} of ramification indices of $G(X)$ over λ satisfies*

$$\gcd(\alpha : \alpha \in \mathcal{G}) > 1.$$

Proof. If $G(X)$ is equivalent to a power of a smaller degree polynomial, then there is a linear polynomial $\mu \in \mathbb{K}[X]$ such that

$$\mu \circ G(X) = G_0(X)^r \quad \text{for } r > 1.$$

Then 0 is a branch point of $\mu \circ G(X)$, and all the ramification indices over 0 are divisible by r . Finally, $\mu^{-1}(0)$ is a branch point of $G(X)$ with the same ramification that 0 has for the polynomial $\mu \circ G(X)$.

If $G(X)$ has a branch point whose ramification indices have greatest common divisor $r > 1$, there is a linear polynomial $\mu \in \mathbb{K}[X]$ such that $\mu \circ G(X)$ has the same

ramification over the branch point 0. Thus by Definition II.2

$$\mu \circ G(X) = c \prod_{i=1}^k (X - x_i)^r$$

for not necessarily distinct constants $x_i \in \mathbb{K}$. Therefore $G(X)$ is equivalent to the r -th power of the polynomial $\prod_{i=1}^k (X - x_i)$. \square

2.7 Decomposable Polynomials

An important property of a polynomial $F(X)$ is the following.

Definition II.21. A polynomial $F[X] \in \mathbb{K}[X]$ is *decomposable* if there are two non-linear polynomials $\mu, \nu \in \mathbb{K}[X]$ such that

$$F = \mu \circ \nu.$$

A polynomial which is not decomposable is said to be *indecomposable*.

2.8 Sporadic Pairs

The sporadic pairs from Theorem I.5 are as follows:

1. $G(X) = -\frac{1}{108}X^3(X-1)^2$, and $H(Y) = 4Y^5 - Y^4$;
2. $G(X) = X^5 + 5X^4 + 40X^3$, and $H(Y) = \frac{1}{2}Y^3(Y-10)^2$;
3. $G(X)$ and $H(Y)$ are distinct polynomials of the form $(30u^2 + 21u - 8)X^3(X - 1)^2(X - 2(3u^2 + 9u + 2)/25)$ where $u^3 = 2$;
4. $G(X) = -X^4(X^2 + X + 25/36)$, and $H(Y) = \frac{4}{5}Y^4(Y^2 + 25/36)$;
5. $G(X)$ and $H(Y)$ are distinct polynomials of the form $(287u^2 + 368u - 1519)X^3(X - 75)^2(X^2 + \frac{1}{3}(19u^2 + 28u - 89)X + 32u^2 + 1184u - 1192)$ with $u^3 = 28$;
6. $G(X)$ and $H(Y)$ are distinct polynomials of the form $(77u + 353)X^3(X^2 + \frac{7}{5}(u - 4)X + \frac{7}{2}(5 - u))^2$ where $u^2 = 21$;

7. $G(X)$ and $H(Y)$ are distinct polynomials from the following four polynomials (but not both type (a)):

(a) $3(49 + 13s)X^4(X - 1)^2(X + \frac{1-s}{4})$ where $s^2 = -7$;

(b) $50(49 - 34r)X^4(X + 3/5)^2(X + \frac{3-2r}{15})$ where $r^2 = 21$;

8. $G(X) = 27X^4(X - 1)^3$, and $H(Y) = 4Y^6(Y - 1)$;

9. $G(X) = \frac{4}{(1+2j)^5}X^2(X^2+8X+14-2j)^3$, and $H(Y) = -Y^4+4Y^3$ where $j^2 = -1$;

10. $G(x) = (4s+5)(X^2-2s+1)^3(X^2-(\frac{8}{7})(2s+1)X+9-2s)$, and $H(Y) = Y^4-8Y^3$, where $s^2 = 2$;

11. $G(X)$ and $H(Y)$ are distinct polynomials among

(a) $4X^2(X^2 + 2)^3$ and

(b) $\frac{1}{(-1+2i)^5}X^2(X^2 + 8X + 14 + 2i)^3$ and

(c) $\frac{1}{(-1-2i)^5}X^2(X^2 + 8X + 14 - 2i)^3$;

12. $G(X)$ and $H(Y)$ are distinct polynomials from the following four polynomials (but not both type (a)):

(a) $\frac{r-1}{(1+r)^3}(X^2 - 1)^3(X^2 + (1 + r)^{4/3})$ with $r^2 = -2$;

(b) $-\frac{5+4s}{2^4 \cdot 3^3}(X^2 + 1 - 2s)^3(X^2 + \frac{8}{7}(2s + 1)X + 9 - 2s)$ where $s^2 = 2$;

13. $G(X)$ and $H(Y)$ are distinct polynomials of the form $(1197u^2+639u+1093)X(X^2+3X+(7+u-u^2)/4)^4$ where $u^3 = 3$;

14. $G(X)$ and $H(Y)$ are distinct polynomials of the form $4(3s+13)X(X^4 - \frac{9(s+5)}{14X^3} + \frac{9(s+3)}{8X^2} - \frac{3(s+5)}{8X} + \frac{9}{16})^2$ where $s^2 = -3$;

15. $G(X)$ and $H(Y)$ are distinct polynomials of the form $(26435u^4 + 612820u^3 - 373360u^2 - 370010u - 76456)X(X^3 + 30X^2 + 3(5u^4 + 10u^3 + 5u^2 + 10u + 95)X + (140u^4 + 250u^3 + 80u^2 + 220u + 740))^3$ where $u^5 = 2$;
16. $G(X) = (X - 2)^2(X^2 - 3v + 5)$, and $H(Y) = -(Y - 2)^2(Y^2 - 3v + 5)$, where $v^2 = 3$;
17. For a single fixed v with $v^2 = 3$, and any j with $j^2 = -1$, $G(X) = (9 + 5v)(X - 2)^2(X^2 - 3v + 5)$ and $H(Y) = j(9 - 5v)(Y - 2)^2(Y^2 + 3v + 5)$;
18. $G(X) = -6(X^4 - X)$ and $H(Y) = 2Y^4 + 6Y^2 + 2Y + 3$;
19. $G(X)$ and $H(Y)$ are distinct polynomials of the form $j(X^4 + 3X^2 + X + \frac{3}{2})$ where $j^3 = 1$;
20. For any fixed $a \in \mathbb{K} \setminus \{0, -\frac{27}{4}\}$, $G(X)$ and $H(Y)$ are distinct polynomials of the form $\frac{(3a+d^2)^2}{d^3}x^4 + \frac{3a+d^2}{d}(3x^2 + x) + \frac{3}{2}d$ where $d^4 + 2d^2a - 4da - \frac{1}{3}a^2 = 0$.
21. $G(X) = \frac{3}{4}X(X^2 - 4e)^2$, and $H(Y) = (Y - 5)(Y^2 + (3e - 5)/2)^2$ where $e^2 = -15$;
22. $G(X)$ and $H(Y)$ are distinct polynomials of form $uX(X^2 + 10X + 3(e + 15)/2)^2$ where $e^2 = -15$ and $u^2 = -1/e$;
23. For any fixed $a \in \mathbb{K} \setminus \{0, 4\}$, $G(X)$ and $H(Y)$ are distinct polynomials of the form $uX(X^2 + X + d)^2$ where $d^3(d - \frac{1}{4})^2a = 5(d^2 - \frac{9}{20}d + \frac{27}{500})^2$ and $u = \frac{125}{27 - 225d + 500d^2}$;
24. $G(X) = (X - 4u + 2)(X^2 - 4(u - 2))^3$ and $H(Y) = (Y + 3u - 5)(Y^2 + 5u - 7)^3$ where $u^2 - u = -2$;
25. $G(X) = X^4(X - a - 4)^2(X + 2a + 1)$ and $H(Y) = Y^4(Y + a - 3)^2(Y - 2a - 1)$ where $a^2 + 2 = -2$;

26.

$$G(X) = X^3(X + \frac{1}{3}(14a^3 + 15a^2 + 22a - 72))(X^3 + \frac{1}{3}(-35a^3 - 57a^2 - 94a + 102)X^2 + (119a^3 + 166a^2 + 263a - 465)X + 524a^3 + 2668a^2 + 5620a + 6288)^3$$

and

$$H(Y) = Y^3(Y - a^3 - 5a^2 - 11a - 12)(Y^3 + (9a^3 + 19a^2 + 34a - 9)Y^2 + \frac{1}{3}(-191a^3 - 498a^2 - 955a - 249)Y + \frac{1}{3}(-7240a^3 - 8004a^2 - 11192a + 37296))^3$$

where $a^4 + a^3 + 2a^2 - 4a = -3$.

The polynomials in this list have degree at most 13, and only the polynomials in the last case have degree more than 10.

CHAPTER III

Cyclic Polynomials

In this chapter we prove the following result, where \mathbb{K} denotes an algebraically closed field of characteristic zero.

Theorem III.1. *Fix an integer $n \geq 2$. Let $G(X) \in \mathbb{K}[X]$ be such that $G(X) - Y^n$ is irreducible. Then the curve $\mathcal{C}: Y^n = G(X)$ has genus 0 if and only if $G(X)$ is equal to a polynomial in one of the following two families:*

1. $G(X) = (X - x_0)^a F(X)^n$, for any positive integer a which is coprime to n , any constant $x_0 \in \mathbb{K}$, and any non-zero polynomial $F(X) \in \mathbb{K}[X]$;
2. $G(X) = (X - x_1)^a (X - x_2)^{n-a} F(X)^n$, for any integer $1 \leq a < n$ which is coprime to n , any non-equal constants $x_1, x_2 \in \mathbb{K}$, and any non-zero polynomial $F(X) \in \mathbb{K}[X]$.

Remark III.2. In Theorem VI.1 we will show that $G(X) - Y^n$ is irreducible whenever $n \geq 2$ and $G(X)$ is of a form given in cases 1 or 2 above.

We set $m = \deg(G)$ and $d = \gcd(m, n)$, and write $\text{Br}(G)$ and $\text{Br}(H)$ for the sets of (finite) branch points of $G(X)$ and $H(Y) := Y^n$, respectively. Furthermore, the symbols \mathcal{G}_i and \mathcal{H}_i (for $1 \leq i \leq R$) denote the multi-sets of ramification indices of $G(X)$ and $H(Y) = Y^n$, respectively, over the points in $\text{Br}(G) \cup \text{Br}(H)$.

3.1 Strategy of Proof of Theorem III.1

We use the Riemann-Hurwitz formula from Lemma II.9 to express the genus g of the curve $Y^n = G(X)$ in terms of the ramification of $G(X)$ and Y^n . This expression simplifies considerably when we substitute into it the explicit form of the ramification of Y^n . We then combinatorially determine all possibilities for the ramification of $G(X)$ which correspond to the case $g = 0$, subject to the assumption that $Y^n - G(X)$ is irreducible.

3.2 Proof of Theorem III.1

Proof. Note that $\text{Br}(Y^n) = \{0\}$. Let \mathcal{G}_1 and \mathcal{H}_1 be the ramification multisets of $G(X)$ and $H(Y) = Y^n$ over the point 0, so that $\mathcal{H}_1 = [n]$ and $\mathcal{H}_i = [1^n]$ for $i > 1$.

First, if $Y^n - (X - x_0)^a F(X)^n$ is assumed to be irreducible, where a , x_0 , and $F(X)$ satisfy the constraints in case 1 of the theorem, then we show that the curve $Y^n = (X - x_0)^a F(X)^n$ has genus zero. We calculate this genus (denoted g) using Lemma II.9. The ramification multiset \mathcal{G}_1 contains a unique element α_1 not divisible by n . Here $\alpha_1 = a + n\alpha'$ where $\alpha' = \text{ord}_{X=x_0} F(X)$. Thus we have

$$\begin{aligned} n + d + 2g - 2 &= \sum_{i=1}^R \sum_{\beta \in \mathcal{H}_i} \sum_{\alpha \in \mathcal{G}_i} [\beta - (\alpha, \beta)] = \sum_{\alpha \in \mathcal{G}_1} [n - (\alpha, n)] \\ &= n - (\alpha_1, n) \\ &= n - (a, n). \end{aligned}$$

Since $(a, n) = 1$ by hypothesis, we have $d = (m, n) = 1$ and so $g = 0$.

Second, if $Y^n - (X - x_1)^a (X - x_2)^{n-a} F(X)^n$ is assumed to be irreducible, where a , x_1 , x_2 , and $F(X)$ satisfy the constraints in case 2 of the theorem, then we show that the genus of the corresponding curve is zero. Over the point 0 we have $\mathcal{H}_1 = [n]$ and \mathcal{G}_1 contains exactly two elements α_1, α_2 not divisible by n . Here $\alpha_1 = a + n\alpha'$ with

$\alpha' = \text{ord}_{X=x_1} F(X)$, and $\alpha_2 = n - a + n\alpha''$ with $\alpha'' = \text{ord}_{X=x_2} F(X)$. We calculate using Lemma II.9 that

$$\begin{aligned}
n + d + 2g - 2 &= \sum_{i=1}^R \sum_{\beta \in \mathcal{H}_i} \sum_{\alpha \in \mathcal{G}_i} [\beta - (\alpha, \beta)] = \sum_{\alpha \in \mathcal{G}_1} [n - (\alpha, n)] \\
&= 2n - (\alpha_1, n) - (\alpha_2, n) \\
&= 2n - (a, n) - (n - a, n) \\
&= 2n - 2.
\end{aligned}$$

Here $d = n$, so we again find that $g = 0$.

To prove the converse direction, we assume that $Y^n - G(X)$ is irreducible and defines a curve of genus $g = 0$. We then have by Lemma II.9 that

$$\sum_{\alpha \in \mathcal{G}_1} [n - (n, \alpha)] = n + d + 2g - 2 = n + d - 2.$$

We first show that \mathcal{G}_1 contains an element which is not divisible by n . To see this, note that $G(X)$ factors as

$$G(X) = c \prod_{\alpha \in \mathcal{G}_1} (X - x_\alpha)^\alpha.$$

So if n divides every element of \mathcal{G}_1 , then $G(X) = G_0(X)^n$ for some $G_0(X) \in \mathbb{K}[X]$, and so $Y^n - G(X) = \prod_{\zeta^{n-1}} (Y - \zeta G_0(X))$ is reducible, a contradiction.

Note that

$$(3.1) \quad n + d - 2 = \sum_{\alpha \in \mathcal{G}_1} [n - (n, \alpha)] = \sum_{\substack{\alpha \in \mathcal{G}_1 \\ n \nmid \alpha}} [n - (n, \alpha)].$$

Also each non-zero summand is at least $\frac{n}{2}$, because $(n, \alpha) \leq \frac{n}{2}$ when $n \nmid \alpha$. Therefore \mathcal{G}_1 has at most three elements not divisible by n , since otherwise

$$2n = 4 \cdot \frac{n}{2} \leq \sum_{\substack{\alpha \in \mathcal{G}_1 \\ n \nmid \alpha}} [n - (n, \alpha)] = n + d - 2 < 2n,$$

a contradiction. Furthermore, if $d < n$ then $d \leq \frac{n}{2}$ (since $d = \gcd(m, n)$ divides n), and so there are at most two elements of \mathcal{G}_1 not divisible by n , since otherwise

$$\frac{3}{2}n \leq \sum_{\alpha \in \mathcal{G}_1} [n - (n, \alpha)] = n + d - 2,$$

contradicting $d \leq \frac{n}{2}$.

The only remaining possible cases are:

1. There is exactly one element $\alpha \in \mathcal{G}_1$ not divisible by n ;
2. There are exactly two elements $\alpha_1, \alpha_2 \in \mathcal{G}_1$ not divisible by n :
 - (a) $d = n$;
 - (b) $d < n$;
3. There are exactly three elements of \mathcal{G}_1 not divisible by n , where $d = n$.

Case 1, there is exactly one element of \mathcal{G}_1 not divisible by n :

If there is exactly one element $\alpha \in \mathcal{G}_1$ not divisible by n , then

$$G(X) = (X - x_0)^\alpha F(X)^n,$$

where $F(X) \in \mathbb{K}[X]$ and $x_0 \in \mathbb{K}$ satisfy $F(x_0) \neq 0$. Here equation (3.1) becomes

$$n + d - 2 = n - (n, \alpha),$$

which simplifies to

$$(n, \alpha) = 2 - d.$$

Since $(n, \alpha) > 0$, it must be that

$$d = (n, \alpha) = 1.$$

This yields case 1 of the theorem.

Case 2, exactly two elements of \mathcal{G}_1 are not divisible by \mathbf{n} :

We write these elements as α_1 and α_2 , so that

$$G(X) = (X - x_1)^{\alpha_1}(X - x_2)^{\alpha_2}F(X)^n$$

for some $F(X) \in \mathbb{K}[X]$ such that $F(x_1), F(x_2) \neq 0$, where $x_1, x_2 \in \mathbb{K}$ are distinct.

Without loss of generality we may assume that $(n, \alpha_1) \geq (n, \alpha_2)$. We have from equation (3.1) that

$$(3.2) \quad (n, \alpha_1) + (n, \alpha_2) = n - d + 2.$$

Furthermore, we know that $\gcd(n, \alpha_1, \alpha_2) = 1$ because if $\gcd(n, \alpha_1, \alpha_2) = k \geq 2$, then $G(X)$ would equal $G_0(X)^k$ for some $G_0(X) \in \mathbb{K}[X]$, but then $Y^n - G(X) = (Y^{\frac{n}{k}})^k - G_0(X)^k$ would not be irreducible.

Case 2(a), $\mathbf{d} = \mathbf{n}$:

By substituting $d = n$ into equation (3.2), we see that

$$(n, \alpha_1) + (n, \alpha_2) = 2,$$

so both summands must be 1. Here we have $(n, m) = d = n$, so $n \mid m$. Since

$$m = \deg(G) = \alpha_1 + \alpha_2 + n \cdot \deg(F),$$

it follows that $\alpha_1 + \alpha_2 \equiv 0 \pmod{n}$. This yields case 2 of the theorem.

Case 2(b), $\mathbf{d} < \mathbf{n}$.

Since $d < n$ and $d = (n, m) \mid n$, we have $d \leq \frac{n}{2}$, so (3.2) implies that

$$(n, \alpha_1) + (n, \alpha_2) = n - d + 2 \geq \frac{n}{2} + 2.$$

Thus, the average of (n, α_1) and (n, α_2) is greater than $\frac{n}{4}$, so $(n, \alpha_1) \in \{\frac{n}{3}, \frac{n}{2}\}$. If

$(n, \alpha_1) = \frac{n}{2}$ then

$$(3.3) \quad (n, \alpha_2) = \frac{n}{2} - d + 2,$$

and if $(n, \alpha_1) = \frac{n}{3}$ then

$$(3.4) \quad (n, \alpha_2) = \frac{2n}{3} - d + 2.$$

We treat several subcases.

Case 2(b)(i), $d = \frac{n}{2}$ and $(n, \alpha_1) = \frac{n}{2}$:

We show that this subcase cannot occur.

If $d = \frac{n}{2}$ and $(n, \alpha_1) = \frac{n}{2}$, then equation (3.3) implies that $(n, \alpha_2) = 2$. Now

$$m = \deg(G) = \alpha_1 + \alpha_2 + n(\deg(F)).$$

Since $\frac{n}{2}$ divides m and α_1 , we have that $\frac{n}{2}$ divides α_2 . Now $(n, \alpha_2) = 2$ gives $\frac{n}{2} = 1$ or 2. If $n = 4$, then we get $\gcd(n, \alpha_1, \alpha_2) = 2$, contradicting $\gcd(n, \alpha_1, \alpha_2) = 1$. If $n = 2$ then

$$(n, \alpha_1) = \frac{n}{2} = 1 < 2 = (n, \alpha_2),$$

contradicting $(n, \alpha_1) \geq (n, \alpha_2)$.

Case 2(b)(ii), $d = \frac{n}{2}$ and $(n, \alpha_1) = \frac{n}{3} \geq (n, \alpha_2)$:

We show this subcase cannot occur.

In this case equation (3.4) yields $(n, \alpha_2) = \frac{n}{6} + 2$. Thus, the ratio $k = \frac{n}{\frac{n}{6} + 2}$ is an integer, so

$$n = \frac{12k}{6 - k}$$

for some positive integer $k \leq 5$. It follows that $n \in \{6, 12, 24, 60\}$. If $n > 6$ then we see by inspection that $2 \mid \gcd(n, \alpha_1, \alpha_2)$, whereas we showed above that $\gcd(n, \alpha_1, \alpha_2) = 1$. If $n = 6$ then $(n, \alpha_1) = 2$ and $(n, \alpha_2) = 3$, contrary to our assumption that $(n, \alpha_1) \geq (n, \alpha_2)$.

Case 2(b)(iii), $d < \frac{n}{2}$:

We show this subcase cannot occur. Since $d < \frac{n}{2}$ and $d = \gcd(m, n) \mid n$, we have $d \leq \frac{n}{3}$. Substituting into equation (3.2) yields

$$(n, \alpha_1) + (n, \alpha_2) = n - d + 2 \geq \frac{2n}{3} + 2.$$

Thus the average of (n, α_1) and (n, α_2) is greater than $\frac{n}{3}$. We conclude that $\gcd(n, \alpha_1) = \frac{n}{2}$, so

$$\gcd(n, \alpha_2) = \frac{n}{2} - d + 2.$$

If $d = \frac{n}{3}$ then $\gcd(n, \alpha_2) = \frac{n}{6} + 2$. Arguing as in case 2(b)(ii), the only possibilities for n are 6, 12, 24, and 60. By inspection, in each of these cases we find that $\gcd(n, \alpha_1, \alpha_2) > 1$, a contradiction.

We now know that $d < \frac{n}{3}$, so $d \leq \frac{n}{4}$, and thus

$$(n, \alpha_2) = \frac{n}{2} - d + 2 \geq \frac{n}{4} + 2.$$

It follows that $(n, \alpha_2) \in \{\frac{n}{3}, \frac{n}{2}\}$. If $(n, \alpha_1) = (n, \alpha_2) = \frac{n}{2}$ and $(n, \alpha_1, \alpha_2) = 1$ then necessarily $n = 2$. However, since $d \leq \frac{n}{4}$ it cannot be that n is less than four, so this cannot occur. If $(n, \alpha_1) = \frac{n}{2}$ and $(n, \alpha_2) = \frac{n}{3}$, then $n = 6$. Since $n \geq 4d$ this requires $d = 1$. However these parameters do not satisfy (3.2), and so cannot occur.

Case 3, exactly three elements of \mathcal{G}_1 are not divisible by \mathbf{n} , where $\mathbf{d} = \mathbf{n}$:

We will show this case cannot occur.

We have

$$G(X) = (X - x_1)^{\alpha_1} (X - x_2)^{\alpha_2} (X - x_3)^{\alpha_3} F(X)^n,$$

where the x_i 's are distinct.

By substituting our assumptions into equation (3.1) we obtain

$$2n - 2 = 3n - \sum_{i=1}^3 (n, \alpha_i)$$

so that

$$(n, \alpha_1) + (n, \alpha_2) + (n, \alpha_3) = n + 2.$$

We will assume without loss of generality that $(n, \alpha_1) \geq (n, \alpha_2) \geq (n, \alpha_3)$. Since the average of the summands is greater than $\frac{n}{3}$, it follows that $\gcd(n, \alpha_1) = \frac{n}{2}$. Thus we have

$$(3.5) \quad (n, \alpha_2) + (n, \alpha_3) = \frac{n}{2} + 2,$$

so the average of the summands is greater than $\frac{n}{4}$, and thus $(n, \alpha_2) \in \{\frac{n}{2}, \frac{n}{3}\}$.

If $(n, \alpha_2) = \frac{n}{2}$ then $\alpha_1 \equiv \alpha_2 \equiv \frac{n}{2} \pmod{n}$, so

$$\alpha_1 + \alpha_2 \equiv \frac{n}{2} + \frac{n}{2} \equiv 0 \pmod{n}.$$

Now $d = (m, n) = n$ gives that $m \equiv 0 \pmod{n}$, so the equation

$$m = \alpha_1 + \alpha_2 + \alpha_3 + n \cdot \deg(F)$$

implies that $\alpha_3 \equiv 0 \pmod{n}$, a contradiction.

If $(n, \alpha_2) = \frac{n}{3}$ we have from (3.5) that $(n, \alpha_3) = \frac{n}{6} + 2$. We again have that n is 6, 12, 24, or 60. By inspection, we see that when $n = 12, 24, 60$ we have $\gcd(n, \alpha_1, \alpha_2, \alpha_3) > 1$ and so $G(X) - Y^n$ is reducible. For $n = 6$, we have $(n, \alpha_2) = 2 < 3 = (n, \alpha_3)$ contradicting $(n, \alpha_2) \geq (n, \alpha_3)$. Therefore, this case cannot occur. \square

CHAPTER IV

Power Free Polynomials: Three or More Branch Point Case

In this chapter we consider pairs of nonconstant polynomials $(G(X), H(Y))$ where $G(X) - H(Y)$ is irreducible, the curve $\mathcal{C}: G(X) = H(Y)$ has genus 0, and neither polynomial is equivalent to a power of a smaller degree polynomial. We will classify all the cases when $|\text{Br}(G) \cup \text{Br}(H)| \geq 3$, where $\text{Br}(G)$ and $\text{Br}(H)$ denote the sets of finite branch points of $G(X)$ and $H(Y)$, respectively. Our first result is as follows, where \mathbb{K} denotes an algebraically closed field of characteristic zero:

Theorem IV.1. *Let $G(T), H(T) \in \mathbb{K}[T]$ be nonconstant polynomials such that $G(X) - H(Y)$ is irreducible and the curve $\mathcal{C}: G(X) = H(Y)$ has genus 0. If $H(Y)$ has at least two (finite) branch points and is not equivalent to a power of a smaller degree polynomial, then $G(X)$ has at most three finite branch points.*

We then classify all possibilities in which $G(X)$ has three branch points:

Theorem IV.2. *(i) If $G(X)$ and $H(Y)$ are as in Theorem IV.1, and $G(X)$ has exactly three finite branch points, then one of the following holds:*

1. $\deg(G) = m \geq 5$, $n|m$, $n > 1$ is odd, and $H(Y)$ has precisely two branch points x_1 and x_2 , both of which have ramification type $[2^{\frac{n-1}{2}}, 1]$. Furthermore the branch points of G are x_1 , x_2 , and x_3 , with corresponding ramification either

- $\mathcal{G}_1 = \mathcal{G}_2 = [2^{\frac{m-2}{2}}, 1^2]$, $\mathcal{G}_3 = [2, 1^{m-2}]$; or
- $\mathcal{G}_1 = [2^{\frac{m-3}{2}}, 1^3]$, $\mathcal{G}_2 = [2^{\frac{m-1}{2}}, 1]$, $\mathcal{G}_3 = [2, 1^{m-2}]$.

2. $\deg(G) = 4$, $G(X)$ has ramification $\mathcal{G}_1 = \mathcal{G}_2 = \mathcal{G}_3 = [2, 1^2]$, and $H(Y)$ has corresponding ramification $\mathcal{H}_1 = \mathcal{H}_2 = \mathcal{H}_3 = [2, 1^2]$;
3. $\deg(G) = 5$, $G(X)$ has ramification $\mathcal{G}_1 = [2^2, 1]$, $\mathcal{G}_2 = \mathcal{G}_3 = [2, 1^3]$, and $H(Y)$ has corresponding ramification $\mathcal{H}_1 = [2^2, 1]$, $\mathcal{H}_2 = \mathcal{H}_3 = [2, 1^3]$;

(ii) Conversely, for any pair (G, H) satisfying one of the above three sets of constraints, the polynomial $G(X)$ has exactly three finite branch points, and if the polynomial $G(X) - H(Y)$ is irreducible then the curve $G(X) = H(Y)$ has genus 0.

Remark IV.3. We will determine in Theorem VI.5 exactly which pairs (G, H) in case 1 above are such that $G(X) - H(Y)$ is irreducible. We will address cases 2 and 3 in Chapter VII.

In the previous chapter we described all possibilities when either $G(X)$ or $H(Y)$ has just one (finite) branch point. The above results address the case where both $G(X)$ and $H(Y)$ have at least two branch points, and one of them has at least three. It remains to treat the case that both $G(X)$ and $H(Y)$ have exactly two branch points. In the next chapter we will treat the case that $\text{Br}(G) = \text{Br}(H)$ and $|\text{Br}(G)| = 2$. The remaining cases are classified in the following theorem.

Theorem IV.4. *Assume $G(X) - H(Y)$ is irreducible, and the curve $\mathcal{C}: G(X) = H(Y)$ has genus 0. Also assume that both $G(X)$ and $H(Y)$ have exactly two branch points, and neither is equivalent to a power of a smaller degree polynomial. If the polynomials have at most one branch point in common then $(G(X), H(Y))$ is equivalent to the pair $(X^a(X-1)^{m-a}, cY^a(Y-1)^{m-a})$ for some $m \geq 3$, some $1 \leq a < m$*

with $(a, m) = 1$, and some $c \in \mathbb{K} \setminus \{0, 1\}$.

Conversely, if (G, H) is equivalent to $(X^a(X-1)^{m-a}, cY^a(Y-1)^{m-a})$ with m, a, c as above, then $|\text{Br}(G)| = |\text{Br}(H)| = 2$ and $|\text{Br}(G) \cap \text{Br}(H)| = 1$, and if the polynomial $G(X) - H(Y)$ is irreducible then the curve $G(X) - H(Y)$ has genus 0.

Remark IV.5. We will prove in Theorem VI.2 that, if (G, H) is equivalent to any pair $(X^a(X-1)^{m-a}, cY^a(Y-1)^{m-a})$ with m, a, c as in Theorem IV.4, then $G(X) - H(Y)$ is irreducible.

4.1 Strategy of the Proofs

The proofs again use the Riemann-Hurwitz formula to extract restrictions on the ramification indices, and in particular to bound the number of elements N_i in the ramification multiset \mathcal{H}_i which are not divisible by the largest element of \mathcal{G}_i (Lemma IV.7). Note that for distinct $\lambda_1, \lambda_2 \in \mathbb{K}$ the factors of

$$H(Y) - \lambda_1$$

and

$$H(Y) - \lambda_2$$

are distinct. We will use this fact to bound the ramification of $H(Y)$ over all branch points of $G(X)$. This leads to Lemma IV.10 which concludes that the number S of branch points of G satisfies

$$n \leq \frac{S + d - 3}{S - 2}$$

if $S \geq 3$. This implies Theorem IV.1.

In the case $S = 3$, the above inequality becomes $n \leq d$, so we must have $n = d$.

Detailed analysis of the equality case leads to Theorem IV.2.

4.2 Reduction Lemmas

Let S be the the number of branch points of $G(X)$. Let x_1, \dots, x_T be the points in $\text{Br}(G) \cup \text{Br}(H)$, and order the x_i 's so that the elements of $\text{Br}(G)$ are x_1, \dots, x_S . Recall that \mathcal{G}_i and \mathcal{H}_i are the ramification multisets of $G(X)$ and $H(Y)$ over x_i , respectively.

Lemma IV.6. *Assume that $G(X)$ and $H(Y)$ are as in Theorem IV.1. Then for any $x_i \in \text{Br}(G) \cup \text{Br}(H)$ and any $\alpha \in \mathcal{G}_i$ we have*

$$\sum_{\beta \in \mathcal{H}_i} [\alpha - \gcd(\alpha, \beta)] - (\alpha - 1) \geq 0,$$

with equality if and only if either $\alpha = 1$ or there is exactly one element of \mathcal{H}_i not divisible by α .

Proof. If $\alpha = 1$ equality holds. Now suppose $\alpha \geq 2$. Since $H(Y)$ is not equivalent to a power of a lower degree polynomial, we have $\gcd(\beta \mid \beta \in \mathcal{H}_i) = 1$ (by Lemma II.20). Thus, if at most one element of \mathcal{H}_i is not divisible by α , then this exceptional element must exist and must be coprime to α , so equality holds. Henceforth assume that \mathcal{H}_i contains at least two elements β_1, β_2 which are not divisible by α . Then

$$\begin{aligned} \sum_{\beta \in \mathcal{H}_i} (\alpha - \gcd(\alpha, \beta)) &\geq \sum_{j=1}^2 (\alpha - \gcd(\alpha, \beta_j)) \\ &\geq \sum_{j=1}^2 \frac{\alpha}{2} = \alpha \\ &> \alpha - 1. \end{aligned}$$

□

We introduce further notation. For each $1 \leq i \leq S$, we let ω_i be the largest element of \mathcal{G}_i . Additionally, N_i will be the number of elements of \mathcal{H}_i which are not

divisible by ω_i . Finally, we will denote

$$t_i := \sum_{\beta \in \mathcal{H}_i} [\omega_i - \gcd(\omega_i, \beta)] - (\omega_i - 1)$$

for each $1 \leq i \leq S$. Here $t_i \geq 0$, by Lemma IV.6.

Lemma IV.7. *Assume that $G(X)$ and $H(Y)$ are as in Theorem IV.1. Then for each $1 \leq i \leq S$ we have*

$$N_i \leq t_i + 1,$$

with equality if and only if $N_i = 1$ or $\omega_i = 2$.

Proof. If $N_i = 1$ then Lemma IV.6 shows that $t_i = 0$. Suppose now that $N_i \geq 2$.

First, if $\omega_i = 2$, then the sum

$$t_i + \omega_i - 1 = \sum_{\beta \in \mathcal{H}_i} (\omega_i - \gcd(\omega_i, \beta)) = N_i,$$

and so $t_i = N_i - 1$.

Second, suppose $\omega_i > 2$. Now each non-zero summand in $\sum_{\beta \in \mathcal{H}_i} (\omega_i - \gcd(\omega_i, \beta))$ is at least $\frac{\omega_i}{2}$. Since $H(Y)$ is not equivalent to a power, Lemma II.20 implies that some element of \mathcal{H}_i is not divisible by $\frac{\omega_i}{2}$, so the corresponding summand $\omega_i - \gcd(\omega_i, \beta)$ is at least $2\omega_i/3$. Thus we have

$$\sum_{\beta \in \mathcal{H}_i} [\omega_i - \gcd(\omega_i, \beta)] > \frac{N_i \omega_i}{2},$$

so

$$t_i > \frac{N_i \omega_i}{2} - \omega_i + 1.$$

Adding $1 - N_i$ to both sides gives

$$t_i - N_i + 1 > \frac{N_i(\omega_i - 2)}{2} - \omega_i + 2 = \frac{1}{2}(N_i - 2)(\omega_i - 2) \geq 0,$$

as required. □

We will denote $\mathcal{G}_i \setminus \{\omega_i\}$ as the multiset obtained by removing a single copy of ω_i from \mathcal{G}_i ; thus, $\mathcal{G}_i \setminus \{\omega_i\}$ could contain ω_i , but it contains one fewer copy of ω_i than does \mathcal{G}_i .

Recall that d is defined to be $\gcd(m, n)$, where $m := \deg(G)$ and $n := \deg(H)$.

Lemma IV.8. *Assume that $G(X)$ and $H(Y)$ are as in Theorem IV.1. Then*

$$\sum_{i=1}^S N_i \leq S + d - 1,$$

with equality holding if and only if, for all $1 \leq i \leq S$,

- if $N_i > 1$ then $\omega_i = 2$, and
- for any $\alpha \in \mathcal{G}_i \setminus \{\omega_i\}$, if $\alpha \neq 1$ then \mathcal{H}_i contains exactly one element which is not divisible by α .

Proof. By Lemma IV.7 we have that

$$(4.1) \quad \sum_{i=1}^S N_i \leq \sum_{i=1}^S (t_i + 1) = S + \sum_{i=1}^S t_i,$$

with equality holding if and only if, for each i , either $N_i = 1$ or $\omega_i = 2$. By the definition of t_i and the non-negativity of the sum $\sum_{\beta \in \mathcal{H}_i} (\alpha - \gcd(\alpha, \beta)) - (\alpha - 1)$ for every α in each of the \mathcal{G}_i (for $1 \leq i \leq S$) (by Lemma IV.6), we have that

$$\begin{aligned} \sum_{i=1}^S t_i &= \sum_{i=1}^S \left(\sum_{\beta \in \mathcal{H}_i} [\omega_i - \gcd(\omega_i, \beta)] - (\omega_i - 1) \right) \\ &\leq \sum_{i=1}^S \sum_{\alpha \in \mathcal{G}_i} \left(\sum_{\beta \in \mathcal{H}_i} [\alpha - \gcd(\alpha, \beta)] - (\alpha - 1) \right). \end{aligned}$$

Now Corollary II.10 shows the right side is $d - 1$, so

$$(4.2) \quad \sum_{i=1}^S t_i \leq d - 1,$$

with equality holding if and only if for each i and each $\alpha \in \mathcal{G}_i \setminus \{\omega_i\}$ we have

$$\sum_{\beta \in \mathcal{H}_i} [\alpha - \gcd(\alpha, \beta)] - (\alpha - 1) = 0.$$

By Lemma IV.6, this last condition is equivalent to requiring that either $\alpha = 1$ or α divides all but exactly one element of \mathcal{H}_i . The result now follows from the inequalities (4.1) and (4.2), together with the associated equality conditions. \square

Lemma IV.9. *Assume that $G(X)$ and $H(Y)$ are as in Theorem IV.1. Then*

$$(S - 2)n \leq \left(\sum_{i=1}^S N_i \right) - 2.$$

Moreover, equality holds if and only if

1. If $N_i \neq n$ then $\omega_i = 2$ (for all $1 \leq i \leq S$), and
2. for all $1 \leq i \leq S$ every element of \mathcal{H}_i which is not divisible by ω_i is equal to 1, and
3. for all $1 \leq i \leq S$ every element of \mathcal{H}_i which is divisible by ω_i is equal to ω_i , and
4. every branch point of $H(Y)$ is a branch point of $G(X)$, and if x_i is a branch point of $H(Y)$ then every element of both \mathcal{G}_i and \mathcal{H}_i equals either 1 or 2.

Proof. For each $1 \leq i \leq S$ we define the nonnegative integer C_i by

$$C_i := \frac{1}{\omega_i} \sum_{\substack{\beta \in \mathcal{H}_i \\ \omega_i | \beta}} \beta,$$

and set $C_i = 0$ if the sum is empty. Note that $C_i \leq \frac{1}{\omega_i}(n - N_i)$ because $\sum_{\beta \in \mathcal{H}_i} \beta = n$ and $N_i \leq \sum_{\substack{\beta \in \mathcal{H}_i \\ \omega_i \nmid \beta}} \beta$. Since we are also assuming that $\omega_i \geq 2$ we have that $C_i \leq \frac{1}{2}(n - N_i)$, with equality holding if and only if either $N_i = n$, or $\omega_i = 2$ and every odd element of \mathcal{H}_i equals 1.

We have the following series of inequalities. The first inequality asserts:

$$n - 1 \geq \sum_{i=1}^S \sum_{\beta \in \mathcal{H}_i} (\beta - 1).$$

This inequality is valid because if we summed over all branch points of $H(Y)$ and all ramification indices, we would have equality, and since no summand is negative we instead have the inequality. Thus there is equality if and only if every branch point of $H(Y)$ is a branch point of $G(X)$.

The next inequality asserts:

$$\sum_{i=1}^S \sum_{\beta \in \mathcal{H}_i} (\beta - 1) \geq \sum_{i=1}^S \left[\sum_{\substack{\beta \in \mathcal{H}_i \\ \omega_i \nmid \beta}} (\beta - 1) + \sum_{\substack{\beta \in \mathcal{H}_i \\ \omega_i \mid \beta}} \left(\beta - \frac{\beta}{\omega_i} \right) \right].$$

It substituted $\frac{\beta}{\omega_i} \geq 1$ which can only make the sum smaller, and is therefore an equality if and only if (for every $1 \leq i \leq S$) every $\beta \in \mathcal{H}_i$ divisible by ω_i is equal to ω_i .

The final inequality is an equality, and asserts:

$$\sum_{i=1}^S \left[\sum_{\substack{\beta \in \mathcal{H}_i \\ \omega_i \nmid \beta}} (\beta - 1) + \sum_{\substack{\beta \in \mathcal{H}_i \\ \omega_i \mid \beta}} \left(\beta - \frac{\beta}{\omega_i} \right) \right] = \sum_{i=1}^S \left[\left(\sum_{\beta \in \mathcal{H}_i} \beta \right) - N_i - C_i \right] = \sum_{i=1}^S (n - N_i - C_i).$$

It is valid since it makes the substitutions $N_i = \sum_{\substack{\beta \in \mathcal{H}_i \\ \omega_i \nmid \beta}} 1$, and $C_i = \frac{1}{\omega_i} \sum_{\substack{\beta \in \mathcal{H}_i \\ \omega_i \mid \beta}} \beta$. The final equality uses the fact that $n = \sum_{\beta \in \mathcal{H}_i} \beta$ for $1 \leq i \leq S$.

Combining these inequalities and substituting the relation $C_i \leq \frac{1}{2}(n - N_i)$ we obtain

$$n - 1 \geq \frac{S}{2}n - \frac{1}{2} \left(\sum_{i=1}^S N_i \right).$$

This yields

$$\left(\sum_{i=1}^S N_i \right) - 2 \geq (S - 2)n,$$

with equality holding if and only if the stated conditions occur. \square

Lemma IV.10. *Assume that $G(X)$ and $H(Y)$ are as in Theorem IV.1. If $S \geq 3$ then*

$$n \leq \frac{S + d - 3}{S - 2}.$$

Moreover, equality holds if and only if

1. *every branch point of $H(Y)$ is a branch point of $G(X)$, and*
2. *all ramification indices of both $G(X)$ and $H(Y)$ are either 1 or 2, and*
3. *for any branch point x_i of $G(X)$, either $\mathcal{H}_i = [2^{\frac{n-1}{2}}, 1]$ or $\mathcal{G}_i = [2, 1^{m-2}]$.*

Proof. By Lemmas IV.8 and IV.9 we have

$$(S - 2)n \leq \left(\sum_{i=1}^S N_i \right) - 2 \leq S + d - 3,$$

so that

$$(4.3) \quad n \leq \frac{S + d - 3}{S - 2}.$$

Furthermore, we have equality if and only if all the conditions for equalities in Lemmas IV.8, and IV.9 must hold. These conditions from Lemma IV.8 and IV.9 are:

1. for all $1 \leq i \leq S$
 - (a) if $N_i > 1$ then $\omega_i = 2$, and
 - (b) for any $\alpha \in \mathcal{G}_i \setminus \{\omega_i\}$, if $\alpha \neq 1$ then \mathcal{H}_i contains exactly one element which is not divisible by α .
2. for every $x_i \in \text{Br}(H)$, every element of both \mathcal{G}_i and \mathcal{H}_i is 1 or 2, and
3. every branch point of $H(Y)$ is a branch point of $G(X)$.

The result follows at once. □

4.3 Proof of Theorem IV.1

Proof of Theorem IV.1. Suppose $S \geq 4$. Then by Lemma IV.10 we have that

$$n \leq \frac{S+d-3}{S-2} \leq \frac{d+1}{2} \leq \frac{n+1}{2},$$

which gives a contradiction unless $n = 1$. When $n = 1$ then $H(Y)$ cannot have two branch points (as assumed), a contradiction. We conclude that $S \leq 3$. \square

4.4 Three Branch Point Case: Proof of Theorem IV.2

Proof of Theorem IV.2. (i). By hypothesis $G(X)$ has $S = 3$ finite branch points. Thus $(S+d-3)/(S-2) = d \leq n$, so equality holds in Lemma IV.10. In particular, $d = n \mid m$, and every branch point of $H(Y)$ is a branch point of $G(X)$, and neither polynomial has any ramification greater than 2.

Now suppose that at least two branch points of $G(X)$ have more than one preimage with ramification index 2. Lemma IV.10 then implies that over those branch points $H(Y)$ has ramification type $[2^{(n-1)/2}, 1]$. In particular, n is odd, so Lemma II.18 implies that $H(Y)$ is dihedral (i.e. equivalent to a Chebyshev polynomial). By a linear change of variable we may suppose $H(Y) = T_n(Y)$ so its branch points are at $x_1 = 2$ and $x_2 = -2$, by Lemma II.16.

At the remaining branch point x_3 of $G(X)$ we must have $\mathcal{H}_3 = [1^n]$. The equality case in Lemma IV.10 case 4 gives that $\mathcal{G}_3 = [2, 1^{m-2}]$.

The Riemann-Hurwitz formula now implies that $G(X)$ has exactly 4 unramified points over the branch points $x_1 = 2$ and $x_2 = -2$. To see this, by Corollary II.9, for genus 0 we must have

$$(4.4) \quad \sum_{i=1}^3 \sum_{\beta \in \mathcal{H}_i} \left(\sum_{\alpha \in \mathcal{G}_i} ([\beta - (\alpha, \beta)]) - (\beta - 1) \right) = n - 1.$$

But $\mathcal{H}_3 = [1^n]$ gives

$$\sum_{\beta \in \mathcal{H}_3} \left(\sum_{\alpha \in \mathcal{G}_3} ([\beta - (\alpha, \beta)]) - (\beta - 1) \right) = 0.$$

Writing $\mathcal{G}_i = [2^{a_i}, 1^{b_i}]$ for $i = 1, 2$ we calculate

$$\sum_{i=1}^2 \sum_{\beta \in \mathcal{H}_i} \left(\sum_{\alpha \in \mathcal{G}_i} ([\beta - (\alpha, \beta)]) - (\beta - 1) \right) = (b_1 + b_2 - 2) \binom{n-1}{2},$$

whence comparison with (4.4) gives $b_1 + b_2 = 4$.

Now the above gives

$$\mathcal{G}_1 = [2^{a_1}, 1^{b_1}], \quad \mathcal{G}_2 = [2^{a_2}, 1^{b_2}]$$

with $b_1 + b_2 = 4$. We also must have $b_1 \geq 1, b_2 \geq 1$, for if some $b_i = 0$ then $G(X)$ would be equivalent to a power of a smaller degree polynomial (see Lemma II.20), which we excluded.

Thus the possibilities are

$$\mathcal{G}_1 = \mathcal{G}_2 = \left[2^{\frac{m-2}{2}}, 1^2 \right], \quad \text{whence } \mathcal{G}_3 = [2, 1^{m-2}]$$

or

$$\mathcal{G}_1 = \left[2^{\frac{m-3}{2}}, 1^3 \right], \quad \mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1 \right], \quad \text{whence } \mathcal{G}_3 = [2, 1^{m-2}]$$

or

$$\mathcal{G}_1 = \left[2^{\frac{m-1}{2}}, 1 \right], \quad \mathcal{G}_2 = \left[2^{\frac{m-3}{2}}, 1^3 \right], \quad \text{whence } \mathcal{G}_3 = [2, 1^{m-2}].$$

But the last case is equivalent to the second case, using (since n is odd) the equivalence

$$(G(X), T_n(Y)) \sim (-G(X), -T_n(Y)) \sim (-G(X), T_n(Y))$$

which exchanges the branch points $x_1 = 2$ and $x_2 = -2$.

Our assumption that $H(Y)$ has at least two finite branch points implies that $n \geq 3$, and likewise our assumption that $S = 3$ implies that $m \geq 4$. Since n is odd and $n|m$, it follows that in fact $m \geq 5$. This corresponds to case 1 of Theorem IV.2.

There are $m - 1$ ramified points of $G(X)$ over its three branch points, and no branch point has more than $\frac{m}{2}$ ramified points over it. Thus for $m \geq 7$ there are at least two branch points of $G(X)$ with two or more $\alpha = 2$.

The remaining cases to study are when $m \leq 6$, and at most one branch point of $G(X)$ has more than one ramified preimage (under G). Note that because $G(X)$ has three finite branch points we must have $m \geq 4$.

If $m = 4$ then $G(X)$ necessarily has ramification $\mathcal{G}_1 = \mathcal{G}_2 = \mathcal{G}_3 = [2, 1^2]$. Then the only restrictions implied by Lemma IV.10 are that $H(Y)$ does not have branch points different from those of $G(X)$, and $H(Y)$ has no ramification greater than 2. This means that over the three branch points, $H(Y)$ has a total of $n - 1$ ramified points of ramification index 2, and has $n + 2$ unramified points. Since $n|m$, and $H(Y)$ is not cyclic it must have degree at least 3, hence $H(Y)$ has degree 4. This requires $\mathcal{H}_1 = \mathcal{H}_2 = \mathcal{H}_3 = [2, 1^2]$. This corresponds to case 2 of Theorem IV.2.

If $m = 5$ then without loss of generality, $G(X)$ has ramification $\mathcal{G}_1 = [2^2, 1]$, $\mathcal{G}_2 = \mathcal{G}_3 = [2, 1^3]$. From Lemma IV.10 this means that $\mathcal{H}_1 = [2^{\frac{n-1}{2}}, 1]$, and $H(Y)$ has no branch point not equal to a branch point of $G(X)$. This means that in the union of \mathcal{H}_2 and \mathcal{H}_3 there are $\frac{n-1}{2}$ elements equal to 2 and $n + 1$ elements equal to 1. We again have that $n|m$ which means that $n = 5$. This corresponds to case 3 of Theorem IV.2.

If $m = 6$ and at most one branch point of $G(X)$ has more than one ramified preimage, then $G(X)$ has ramification $\mathcal{G}_1 = [2^3]$, $\mathcal{G}_2 = \mathcal{G}_3 = [2, 1^4]$. Therefore this

case cannot occur as Lemma II.20 implies that $G(X)$ would be a power of a smaller degree polynomial.

(ii). We now prove the converse statement. If (G, H) is equivalent to a pair listed in cases 1–3 then by definition $G(X)$ has exactly three finite branch points. This is clear as we have defined ramification over three finite branch points, and the ramification is such that

$$\sum_{i=1}^3 \sum_{\alpha \in \mathcal{G}_i} [\alpha - 1] = m - 1,$$

and so by Lemma II.7 there can be no other branch points of $G(X)$. In case 1 we have that there are exactly four unramified preimages over $x_1 = 2$ and $x_2 = -2$.

Since $m \geq 5$, it must be that both $\mu^{-1}(2)$ and $\mu^{-1}(-2)$ are branch points of $G(X)$. Since $G(X)$ has a total of $m - 2$ ramified preimages of these two points, all with ramification index 2, it follows from Lemma II.7 that $G(X)$ has exactly one more branch point, and that this point has ramification $[2, 1^{m-2}]$. Finally, if the polynomial $G(X) - H(Y)$ is irreducible, we can calculate the genus using Lemma II.9, and in all four cases the genus is 0. \square

Remark IV.11. In case 1 we showed that the polynomial $G(X)$ has exactly four unramified points over the branch points $x_1 = 2$ and $x_2 = -2$. This implies that

$$(G(X) + 2)(G(X) - 2) = F(X)R(X)^2,$$

in which $F(X)$ is of degree exactly four and $F(X)R(X)$ is a square-free polynomial. Thus $G(X)$ satisfies the Pell-type equation

$$(4.5) \quad G(X)^2 - F(X)R(X)^2 = 4.$$

4.5 Two Branch Point Case: Proof of Theorem IV.4

The case where both polynomials have exactly two finite branch points will be addressed in the rest of this chapter, and in Chapter V. Here we treat the case where $|\text{Br}(G) \cup \text{Br}(H)| \geq 3$ (i.e. the two polynomials do not have the same two branch points). In the next chapter we address the case where the polynomials have the same two branch points.

Lemma IV.12. *Assume that $G(X) - H(Y)$ is irreducible, and that the curve $C: G(X) = H(Y)$ has genus 0. Assume neither polynomial is equivalent to a power of a smaller degree polynomial. If both polynomials have exactly two branch points, then they must have at least one branch point in common.*

Proof. Assume for a contradiction that the polynomials have no branch points in common. Since both polynomials have two finite branch points, we must have $m, n \geq 3$. Let \mathcal{G}_1 and \mathcal{G}_2 be the multi-sets of ramification indices of $G(X)$ and $\mathcal{H}_1 = \mathcal{H}_2 = [1^n]$ the corresponding ramification for $H(Y)$ over these points. Then by Lemma II.9:

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\alpha - (\alpha, \beta)] = m + d - 2.$$

Since all $\beta = 1$, we have

$$\sum_{i=1}^2 |\mathcal{H}_i| \sum_{\alpha \in \mathcal{G}_i} (\alpha - 1) = m + d - 2.$$

By Lemma II.7 we obtain

$$n(m - 1) = m + d - 2.$$

This is a contradiction because the right side is at most $2m - 2$, while the left side is at least $3m - 3$ because $m, n \geq 3$. \square

To prove Theorem IV.4 we will need the following Lemma.

Lemma IV.13. *If $(a, m) = (b, m) = 1$ with $a \geq 1$, then*

$$(a, b) + (a, m - b) \leq a + 1$$

with equality if and only if $(a, b) = a$ or $(a, m - b) = a$.

Proof. We first observe that

$$(4.6) \quad (a, b)(a, m - b) \leq a.$$

This follows since (a, b) and $(a, m - b)$ are coprime and divide a .

Now rewrite equation (4.6) as $XY \leq a$. For positive integers X, Y and $a \geq 1$, this implies $X + Y \leq a + 1$, with equality if and only if $\{X, Y\} = \{a, 1\}$. \square

Proof of Theorem IV.4. Without loss of generality we assume that $\mathcal{G}_3 = [1^m]$ and $\mathcal{H}_1 = [1^n]$.

We first show that $m = n$. If $n > m$ then necessarily $n \geq m + d$. Then since there is at least one element of \mathcal{G}_1 which is greater than 1 we have that $\sum_{\alpha \in \mathcal{G}_1} \sum_{\beta \in \mathcal{H}_1} [\alpha - (\alpha, \beta)] \geq n$ because when $\alpha > 1$ there are n summands that are all positive. So we have that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\alpha - (\alpha, \beta)] \geq n > m + d - 2.$$

However Lemma II.9 states that this sum should equal $m + d - 2$, so we have a contradiction. Thus $n \leq m$.

By a symmetric argument it also cannot be that $m > n$, and so it must be that $m = n = d$.

Next we show that $\mathcal{G}_1 = [2, 1^{m-2}]$. If not, then over the branch point corresponding to \mathcal{G}_1 that $G(X)$ has more ramification than just one ramified point of ramification

degree 2 (either it has more than one ramified point, or a point of ramification degree at least 3). Then, using $m = n$,

$$\begin{aligned} m + d + g - 2 &= \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\alpha - (\alpha, \beta)] \geq \sum_{\alpha \in \mathcal{G}_1} [n(\alpha - 1)] \\ &\geq 2n = 2m > m + d - 2, \end{aligned}$$

a contradiction. By a symmetric argument, it must be that $\mathcal{H}_3 = [2, 1^{m-2}]$.

Next we show $\mathcal{G}_2 = [a, m - a]$ with $(a, m) = 1$. Since Lemma II.9 states that $\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} (\alpha - 1) = m - 1$ and we also have that $\sum_{\alpha \in \mathcal{G}_1} (\alpha - 1) = 1$, it must be that

$$\left(\sum_{\alpha \in \mathcal{G}_2} \alpha - 1 \right) = m - 2.$$

Thus

$$m - |\mathcal{G}_2| = m - 2,$$

so $|\mathcal{G}_2| = 2$. We conclude $\mathcal{G}_2 = [a, m - a]$ for $1 \leq a \leq m - 1$. We must have $(a, m) = 1$ since if $(a, m) > 1$ then Lemma II.20 shows $G(X)$ is equivalent to a power of a smaller degree polynomial.

By a similar argument, we have that $|\mathcal{H}_2| = 2$, and $\mathcal{H}_2 = [b, m - b]$ with $(b, m) = 1$.

Next we show that necessarily $a = b$ or $a = m - b$. Now

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\alpha - (\alpha, \beta)] = m + d - 2$$

simplifies to

$$m + \sum_{\alpha \in \mathcal{G}_2} \sum_{\beta \in \mathcal{H}_2} [\alpha - (\alpha, \beta)] = 2m - 2.$$

So that

$$(4.7) \quad \sum_{\alpha \in \mathcal{G}_2} \sum_{\beta \in \mathcal{H}_2} [\alpha - (\alpha, \beta)] = m - 2.$$

The left side of (4.7) equals

$$2m - [(a, b) + (a, m - b) + (m - a, b) + (m - a, m - b)],$$

hence a and b must satisfy

$$(a, b) + (a, m - b) + (m - a, b) + (m - a, m - b) = m + 2.$$

By Lemma IV.13 we know that

$$(a, b) + (a, m - b) + (m - a, b) + (m - a, m - b) \leq (a + 1) + [(m - a) + 1] = m + 2,$$

with equality if and only if $\{(a, b), (a, m - b)\} = \{a, 1\}$ and $\{(m - a, b), (m - a, m - b)\} = \{m - a, 1\}$. By permuting a with $m - a$ if necessarily, we may suppose that $(a, b) = a$, and $(m - a, b) = m - a$ or $(m - a, m - b) = m - a$.

Suppose first $(m - a, b) = m - a$. Then $a|b$ and $m - a|b$ so $a(m - a)|b$. Since $b \leq m - 1$ this can only occur with $\{a, m - a\} = \{1, m - 1\}$ and $b = m - 1$. So $a = b$ or $a = m - b$.

Now suppose $(m - a, m - b) = m - a$. Then $m - a|m - b$ implies $b \leq a$ and $a|b$ implies $a \leq b$ hence $a = b$.

Thus the ramification structure of $G(X)$ and $H(Y)$ is necessarily

$$\mathcal{G}_1 = \mathcal{H}_3 = [2, 1^{m-2}], \quad \mathcal{G}_2 = \mathcal{H}_2 = [a, m - a], \quad \mathcal{G}_3 = \mathcal{H}_1 = [1^m],$$

for any $1 \leq a < m$ with $(a, m) = 1$.

By linear equivalence, we can move the branch point corresponding to \mathcal{G}_2 to zero.

There are linear polynomials μ and ν such that

$$\mu \circ G \circ \nu = X^a(X - 1)^{m-a}.$$

Now we can find linear ρ so that

$$\mu \circ H \circ \rho = cY^a(Y - 1)^{m-a},$$

with $c \neq 0$. Furthermore $c \neq 1$, otherwise they would be the same polynomial and so share all branch points in common. Thus $(G(X), H(Y))$ is equivalent to $(X^a(X - 1)^{m-a}, cY^a(Y - 1)^{m-a})$ for any $m \geq 3$, any $1 \leq a < m$ with $(a, m) = 1$ and any constant c not equal to 0 or 1.

It is clear that over zero both polynomials have ramification structure $[a, m - a]$. By Lemma II.7 we see that each polynomial has exactly one other finite branch point and the ramification structure over that point is $[2, 1^{m-2}]$. Let λ be the other finite branch point of $X^a(X - 1)^{m-a}$. Then we have

$$cY^a(Y - 1)^{m-a} - c\lambda = c[Y^a(Y - 1)^{m-a} - \lambda].$$

It follows that the ramification structure of $X^a(X - 1)^{m-a}$ over λ is equal to the ramification structure of $cY^a(Y - 1)^{m-a}$ over $c\lambda \neq \lambda$. Finally, the curve defined by $X^a(X - 1)^{m-a} - cY^a(Y - 1)^{m-a}$ can be seen to have genus zero by substituting the derived ramification structures into Lemma II.10. Finally, $X^a(X - 1)^{m-a}$ is not equivalent to a power of a smaller degree polynomial. This is clear as the ramification indices $[a, m - a]$ are coprime and the only non-zero branch point has ramification $[2, 1^{m-2}]$, thus Lemma II.20 implies that $X^a(X - 1)^{m-a}$ is not equivalent to a power of a smaller degree polynomial.

□

CHAPTER V

Power Free Polynomials: Two Shared Branch Points

In this chapter we will prove the following theorem, in which \mathbb{K} denotes an algebraically closed field of characteristic zero:

Theorem V.1. *Let $G(T), H(T) \in \mathbb{K}[T]$ with $0 < \deg(H) \leq \deg(G)$ be such that $G(X) - H(Y)$ is irreducible. Suppose that neither $G(X)$ nor $H(Y)$ is equivalent to a power of a smaller degree polynomial, and that $\text{Br}(G) = \text{Br}(H) = \{-2, 2\}$. Then $G(X) - H(Y)$ defines a genus 0 curve if and only if either $(G(X), H(Y))$ is equivalent to a pair of polynomials from the list \mathcal{R}_1 (defined below) or $H(Y) = T_n \circ \ell(Y)$ for some linear polynomial ℓ with $n \geq 3$ odd and one of the following possibilities for $G(X)$ occurs:*

1. $\gcd(m, n) = 1$, and $G(X) = T_m \circ \mu(X)$ with μ some linear polynomial and m an odd integer;
2. n divides m , and $G(X)$ has one of the following six ramification structures:

$$(a) \mathcal{G}_1 = \left[4, 2^{\frac{m-5}{2}}, 1\right], \mathcal{G}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right];$$

$$(b) \mathcal{G}_1 = \left[4, 2^{\frac{m-7}{2}}, 1^3\right], \mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1\right];$$

$$(c) \mathcal{G}_1 = \left[3, 2^{\frac{m-3}{2}}\right], \mathcal{G}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right];$$

$$(d) \mathcal{G}_1 = \left[3, 2^{\frac{m-5}{2}}, 1^2\right], \mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1\right];$$

$$(e) \mathcal{G}_1 = \left[4, 2^{\frac{m-6}{2}}, 1^2\right], \mathcal{G}_2 = \left[2^{\frac{m-2}{2}}, 1^2\right];$$

$$(f) \mathcal{G}_1 = \left[3, 2^{\frac{m-4}{2}}, 1\right], \mathcal{G}_2 = \left[2^{\frac{m-2}{2}}, 1^2\right].$$

Definition V.2 (Sporadic Pairs). We define the set \mathcal{R}_0 to be the collection of pairs of polynomials $(G(X), H(Y))$ with $\text{Br}(G) = \text{Br}(H) = \{-2, 2\}$ and any of the following ramification structures:

1. $\mathcal{G}_1 = \mathcal{H}_1 = \mathcal{G}_2 = \mathcal{H}_2 = [3, 1^2]$;
2. $\mathcal{G}_1 = [3, 2]$, $\mathcal{H}_1 = [4, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2, 1^3]$;
3. $\mathcal{G}_1 = [3, 1^2]$, $\mathcal{G}_2 = [2^2, 1]$, $\mathcal{H}_1 = [3, 2]$, $\mathcal{H}_2 = [2, 1^3]$;
4. $\mathcal{G}_1 = \mathcal{H}_1 = [3, 2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^2]$;
5. $\mathcal{G}_1 = \mathcal{H}_1 = [4, 1^2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^2]$;
6. $\mathcal{G}_1 = \mathcal{H}_1 = [3, 2, 1^2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^3, 1]$;
7. $\mathcal{G}_1 = \mathcal{H}_1 = [4, 1^3]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^3, 1]$;
8. $\mathcal{G}_1 = \mathcal{H}_1 = [3, 2^2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^3]$;
9. $\mathcal{G}_1 = \mathcal{H}_1 = [3^2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [3, 1^4]$;
10. $\mathcal{G}_1 = \mathcal{H}_1 = [3^2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^3]$;
11. $\mathcal{G}_1 = \mathcal{H}_1 = [4, 2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^3]$;
12. $\mathcal{G}_1 = [4, 3]$, $\mathcal{H}_1 = [6, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2, 1^5]$;
13. $\mathcal{G}_1 = [3^2, 2]$, $\mathcal{G}_2 = [2^2, 1^4]$, $\mathcal{H}_1 = [3, 1]$, $\mathcal{H}_2 = [2, 1^2]$;
14. $\mathcal{G}_1 = [3^2, 1^2]$, $\mathcal{G}_2 = [2^3, 1^2]$, $\mathcal{H}_1 = [3, 1]$, $\mathcal{H}_2 = [2, 1^2]$;
15. $\mathcal{G}_1 = \mathcal{H}_1 = [3^2, 2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^4]$;

16. $\mathcal{G}_1 = \mathcal{H}_1 = [3^2, 1^2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^3, 1^2]$;
17. $\mathcal{G}_1 = \mathcal{H}_1 = [4^2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^5]$;
18. $\mathcal{G}_1 = \mathcal{H}_1 = [3^2, 1^3]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^4, 1]$;
19. $\mathcal{G}_1 = \mathcal{H}_1 = [3^3, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^3, 1^4]$.

5.1 Method of Proof

For the rest of this chapter we will always assume (without loss of generality) that $m \geq n$. By permuting the two branch points of $G(X)$, if necessary, we may assume without loss of generality that $k := |\mathcal{G}_1| \leq |\mathcal{G}_2|$, where $|\mathcal{G}_i|$ counts the number of elements in \mathcal{G}_i , which is $|\mathcal{G}_i| = m - \sum_{\alpha \in \mathcal{G}_i} (\alpha - 1)$. Using Lemma II.7 we obtain $|\mathcal{G}_1| + |\mathcal{G}_2| = m + 1$, therefore we have $1 \leq k \leq \frac{m+1}{2}$. We shall set $\ell = |\mathcal{H}_1|$ and we know that $1 \leq \ell \leq n - 1$. In Section 5.2 we use the Riemann-Hurwitz formula in Lemma V.4 to establish a fundamental relationship between k, ℓ and the ramification indices, namely (with $d = \gcd(m, n)$)

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k - 1)(n - \ell) + (\ell - 1)(m - k) - d + 1.$$

We introduce the concept of uniform multiset (of ramification indices) in Section 5.3, and the proofs will show that in the infinite families the set \mathcal{G}_2 is uniform.

In Section 5.4 we formulate three propositions limiting the ranges of k and ℓ . Together they show that for k in the range $1 \leq k \leq (m + 1)/2$ and $m \geq 19$ either $1 \leq \ell \leq 4$ or $(n + 1)/2 \leq \ell \leq (n + 4)/2$. (Propositions V.10 and V.12). We also show that on setting $\ell = (n - a)/2$ and $k = (m - b)/2$ with $a + b \geq 3$, then

$$m \leq \frac{4ab + 2a + 2b}{a + b - 2}$$

(Proposition V.11). This result is useful to upper bound the degrees of the sporadic cases. We prove these Propositions in Sections 5.5 to 5.7.

These three results leave only sporadic possibilities for the values m, n, k , and ℓ , and these are handled exhaustively in Section 5.8. The proof of Theorem V.1 is presented in Section 5.9, as a corollary of earlier results.

5.2 Preliminary Lemmas

Lemma V.3. *Let $G(X)$ be a polynomial with exactly two finite branch points. Let \mathcal{G}_1 and \mathcal{G}_2 be the multi-sets of ramification indices over these branch points. Then*

$$|\mathcal{G}_1| + |\mathcal{G}_2| = \deg(G) + 1.$$

Proof. We have the two relations:

$$(5.1) \quad \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} (\alpha - 1) = \deg(G) - 1$$

and

$$(5.2) \quad \sum_{\alpha \in \mathcal{G}_i} \alpha = \deg(G), \text{ for } i \in \{1, 2\}.$$

Substituting equation (5.2) into equation (5.1) we have

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} (\alpha) - \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} 1 = \deg(G) - 1$$

$$2 \deg(G) - |\mathcal{G}_1| - |\mathcal{G}_2| = \deg(G) - 1$$

$$|\mathcal{G}_1| + |\mathcal{G}_2| = \deg(G) + 1. \quad \square$$

Lemma V.4. *If $G(X)$ and $H(Y)$ are as in Theorem V.1, then*

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (|\mathcal{G}_1| - 1)(n - |\mathcal{H}_1|) + (|\mathcal{H}_1| - 1)(m - |\mathcal{G}_1|) - d + 1.$$

Proof. We know from Lemma II.9 that

$$\begin{aligned}
& \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\alpha - (\alpha, \beta)] = m + d - 2 \\
& \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \left[|\mathcal{H}_i| \alpha - \sum_{\beta \in \mathcal{H}_i} (\alpha, \beta) \right] = m + d - 2 \\
& (|\mathcal{H}_1| + |\mathcal{H}_2|)m - \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} (\alpha, \beta) = m + d - 2 \\
& (|\mathcal{H}_1| + |\mathcal{H}_2| - 1)m - d + 2 = \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} (\alpha, \beta) \\
& (|\mathcal{H}_1| + |\mathcal{H}_2| - 1)m - d + 2 - |\mathcal{G}_1| |\mathcal{H}_1| - |\mathcal{G}_2| |\mathcal{H}_2| = \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1].
\end{aligned}$$

Then by Lemma V.3 we know that $m = |\mathcal{G}_1| + |\mathcal{G}_2| - 1$ and $n = |\mathcal{H}_1| + |\mathcal{H}_2| - 1$.

Substituting these relations in we have

$$\begin{aligned}
& \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = |\mathcal{G}_1| |\mathcal{H}_2| + |\mathcal{H}_1| |\mathcal{G}_2| - |\mathcal{G}_1| - |\mathcal{G}_2| - |\mathcal{H}_1| - |\mathcal{H}_2| - d + 3 \\
& \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = |\mathcal{G}_1| (n - |\mathcal{H}_1| + 1) + (m - |\mathcal{G}_1| + 1) |\mathcal{H}_1| - m - n - d + 1 \\
& \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (|\mathcal{G}_1| - 1)(n - |\mathcal{H}_1|) + (|\mathcal{H}_1| - 1)(m - |\mathcal{G}_1|) - d + 1.
\end{aligned}$$

□

5.3 Uniformity of Multisets

In order to state the main results which lead to the proof of Theorem V.1 we will first need to define the term *uniform* with respect to multisets, and derive some basics properties of uniform multisets.

Definition V.5. We will set $k := |\mathcal{G}_1|$ and $\ell := |\mathcal{H}_1|$.

Note that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] \leq \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1].$$

We will classify tuples (m, n, k, ℓ) with

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

Thus, ramification structures associated to those tuples cannot be associated to irreducible genus 0 curves.

Definition V.6. A finite multi-set of positive integers is *uniform* if every element is equal to either the floor or ceiling of the average value of the elements.

Let $\mathcal{P}_{m,k}$ be the set of partitions of the positive integer m into k parts (i.e. the collection of multi-sets that have k elements which sum to m).

Definition V.7. Let \mathcal{G} be a non-uniform multi-set of positive integers and let ω_1 be a largest element of \mathcal{G} and ω_2 a smallest element of \mathcal{G} . Then if the multi-set $\tilde{\mathcal{G}}$ satisfies

$$\tilde{\mathcal{G}} = \{\omega_1 - 1, \omega_2 + 1\} \cup \mathcal{G} \setminus \{\omega_1, \omega_2\},$$

we say it is a *refinement* of \mathcal{G} . If \mathcal{G} is uniform we say it is its own *refinement*.

For any two elements $\mathcal{G}, \mathcal{H} \in \mathcal{P}_{m,k}$ we say $\mathcal{G} \geq \mathcal{H}$ if there is a sequence of refinements beginning at \mathcal{H} and ending at \mathcal{G} .

We also say that a tuple of multi-sets of positive integers $(\tilde{\mathcal{G}}_1, \tilde{\mathcal{G}}_2, \tilde{\mathcal{G}}_3, \tilde{\mathcal{G}}_4)$ is a *refinement* of another tuple of multi-sets $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3, \mathcal{G}_4)$ if for three integers $1 \leq i \leq 4$ we have $\mathcal{G}_i = \tilde{\mathcal{G}}_i$ and for the fourth integer i we have $\tilde{\mathcal{G}}_i$ is a refinement of \mathcal{G}_i .

Lemma V.8. *For any positive integers m and k with $1 \leq k \leq m$, the relation \geq on elements of $\mathcal{P}_{m,k}$ is a partial ordering on $\mathcal{P}_{m,k}$. Furthermore, the unique maximal element under this partial ordering is the unique uniform element of $\mathcal{P}_{m,k}$.*

Proof. The three properties of \geq being a partial ordering is

1. for all $A \in \mathcal{P}_{m,k}$ we have $A \geq A$;

2. for all $A, B \in \mathcal{P}_{m,k}$ if $A \geq B$ and $B \geq A$ then $A = B$;
3. for all $A, B, C \in \mathcal{P}_{m,k}$ if $A \geq B$ and $B \geq A$ then $A \geq C$.

It is clear that for any $A \in \mathcal{P}_{m,k}$ that the trivial sequence of just the element A satisfies the definition so that $A \geq A$.

If $A \geq B$ and $B \geq A$ and $A \neq B$, then by definition there are a non-trivial sequence of refinements from B to A . However, in every step of a non-trivial sequence of refinements, it is necessary that a largest element of the multi-set decreases by 1. Therefore, A necessarily has fewer elements than B which are maximal in B . However, since there is a non-trivial sequence of refinements from B to A it must B that B has fewer elements of the maximal value of B as well, but this is a contradiction.

From the definition of \geq it is clear that if there is a sequence of refinements from A to B and from B to C then by combining them, there is a sequence of refinements from A to C .

To see that there is a unique uniform element of $\mathcal{P}_{m,k}$ note that since every element of a uniform element is the floor or ceiling of the average, that the number of elements equal to the ceiling of the average must be $m - k \lfloor \frac{m}{k} \rfloor$. This is because $k \lfloor \frac{m}{k} \rfloor$ is what the sum of the elements would be if every element were the floor of $\frac{m}{k}$, and the sum increases by 1 for every element which is equal to the ceiling of $\frac{m}{k}$. Thus the uniform multi-set is uniquely defined by m and k .

Note that the uniform element of $\mathcal{P}_{m,k}$ is the unique maximal element of the partial ordering, because any element which is not uniform has two elements ω_1 and ω_2 with $\omega_1 > \omega_2 + 1$ and so has a non-trivial refinement (if there were not two such elements, then necessarily the multi-set would be uniform). Therefore if $A \in \mathcal{P}_{m,k}$ is not uniform, there is a non-trivial reduction of A . Since there are finitely many elements of $\mathcal{P}_{m,k}$ it must be that the uniform element is the unique maximal element. \square

Lemma V.9. *Fix a positive integer m and a positive integer $k \in [1, m]$. Let $A, C \in \mathcal{P}_{m,k}$ be such that C is a refinement of A . Then for any multi-set of positive integers B we have*

$$\sum_{\alpha \in A} \sum_{\beta \in B} [\min(\alpha, \beta) - 1] \leq \sum_{\alpha \in C} \sum_{\beta \in B} [\min(\alpha, \beta) - 1].$$

Proof. Let α_1 be a largest element of A and let α_2 be a smallest element of A . If $\alpha_1 \leq \alpha_2 + 1$ then A is uniform and equal to C . Assume that A is not uniform, and so $\alpha_1 > \alpha_2 + 1$.

We can construct the refinement

$$C := \{\alpha_1 - 1, \alpha_2 + 1\} \cup A \setminus \{\alpha_1, \alpha_2\}.$$

We claim that

$$\sum_{\alpha \in C} \sum_{\beta \in B} [\min(\alpha, \beta) - 1] \geq \sum_{\alpha \in A} \sum_{\beta \in B} [\min(\alpha, \beta) - 1].$$

To see that the claim is true note that the summands are unchanged for every $\alpha \in A \setminus \{\alpha_1, \alpha_2\}$. Additionally for the summands with α_1 and α_2 there are three cases

1. If $\beta \in B$ is such that $\beta \leq \alpha_2$ then the summands involving β are unchanged as the values of α_1 and α_2 change, because β is the minimum;
2. If $\beta \in B$ is such that $\beta \geq \alpha_1$ then the $\min(\alpha_1, \beta)$ decreases by 1 when α_1 decreases by 1, and $\min(\alpha_2, \beta)$ increases by 1 when α_2 increases by 1, and so the sum of these two terms is unchanged;
3. If $\beta \in B$ is such that $\alpha_1 > \beta > \alpha_2$ then $\min(\alpha_1, \beta)$ is unchanged when α_1 decreases by 1, but $\min(\alpha_2, \beta)$ increases by 1 when α_2 increases by 1.

□

5.4 Main Results

We prove Theorem V.1 by proving many subcases of the Theorem. Most subcases are handled by the following three results.

Proposition V.10. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1, then if $k \leq \frac{m+1}{2}$ and $\ell > \frac{n+1}{2}$, it cannot be that $\ell - \frac{n}{2} \geq k - \frac{m}{2} + 2$. In particular, it must be that $\ell \leq \frac{n+4}{2}$.*

If in addition $m > n$ then it cannot be that $\ell - \frac{n}{2} \geq k - \frac{m}{2} + \frac{3}{2}$.

Proposition V.11. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. Let a and b be positive integers such that $a + b \geq 3$. Then if $k = \frac{m-a}{2}$ and $\ell = \frac{n-b}{2}$ then $m \leq \frac{4ab+2a+2b}{a+b-2}$.*

Proposition V.12. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. If $m \geq 19$ and both $k < \frac{m+1}{2}$ and $\ell < \frac{n+1}{2}$ then it cannot be that $4 \leq \ell < \frac{n-3}{2}$.*

5.5 Proof of Proposition V.10

Lemma V.13. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. Let $a = k - \frac{m}{2}$, and $b = \ell - \frac{n}{2}$. If $k < \frac{m+1}{2}$, and $\ell > \frac{n+1}{2}$, and $b \geq a + 2$ then*

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (m-k)(\ell-1) - d + 1.$$

Proof. By Lemma V.9 the maximum the sum can be is when the multi-sets are uniform. Since $\ell > \frac{n+1}{2}$ we have that \mathcal{H}_1 is uniform when it is equal to $[2^{n-\ell}, 1^{2\ell-n}]$. Likewise since $k < \frac{m+1}{2}$, we have that \mathcal{G}_2 is uniform when it is equal to $[2^{k-1}, 1^{m+2-2k}]$. Furthermore, when \mathcal{G}_1 and \mathcal{H}_2 are uniform, every element of the multi-sets is at least 2. Therefore, for any $\alpha \in \mathcal{G}_1$ and $\beta \in \mathcal{H}_1$ then $\min(\alpha, \beta) = \beta$. Likewise for any

$\alpha \in \mathcal{G}_2$ and $\beta \in \mathcal{H}_2$ then $\min(\alpha, \beta) = \alpha$. Therefore

$$\begin{aligned} \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] &= \sum_{\beta \in \mathcal{H}_1} [|\mathcal{G}_1| (\beta - 1)] + \sum_{\alpha \in \mathcal{G}_2} [|\mathcal{H}_2| (\alpha - 1)] \\ &= k(n - \ell) + (n - \ell + 1)(k - 1) \\ &= 2nk - 2k\ell - n + \ell + k - 1. \end{aligned}$$

To see that this is strictly less than $(k - 1)(n - \ell) + (m - k)(\ell - 1) - d + 1$ note that $na < (b - 1)m - d + 1$ because $b \geq a + 2$, and $m \geq n \geq d$. Thus

$$\begin{aligned} na + \frac{mn}{2} &< (b - 1)m + \frac{mn}{2} - d + 1 \\ nk &< m\ell - m - d + 1 \end{aligned}$$

$$2nk - 2k\ell + k + \ell - n - 1 < nk - 2k\ell + k + \ell - n + m\ell - m - d$$

$$k(n - \ell) + (k - 1)(n + 1 - \ell) < (k - 1)(n - \ell) + (m - k)(\ell - 1) - d. \quad \square$$

Lemma V.14. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. Let $a = k - \frac{m}{2}$, and $b = \ell - \frac{n}{2}$. If $m > n$, with $k < \frac{m+1}{2}$, and $\ell > \frac{n+1}{2}$, and $b \geq a + \frac{3}{2}$ then*

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k - 1)(n - \ell) + (m - k)(\ell - 1) - d + 1.$$

Proof. For the identical reasons as in the proof of Lemma V.13 we have that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] = k(n - \ell) + (n - \ell + 1)(k - 1) = 2nk - 2k\ell - n + \ell + k - 1.$$

To see that this is strictly less than $(k - 1)(n - \ell) + (m - k)(\ell - 1) - d + 1$ note that $m \geq n + d$, and $b \geq a + \frac{3}{2}$. Therefore $na < (b - 1)m - d + 1$. We therefore have (as done in the proof of Lemma V.13) that

$$\begin{aligned} k(n - \ell) + (n - \ell + 1)(k - 1) &= 2nk - 2k\ell - n + \ell + k - 1 \\ &< (k - 1)(n - \ell) + (m - k)(\ell - 1) - d + 1. \quad \square \end{aligned}$$

Lemma V.15. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. If $k = \frac{m+1}{2}$, and $\ell \geq \frac{n+5}{2}$ then*

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (m-k)(\ell-1) - d + 1.$$

Proof. Like before denote $b = \ell - \frac{n}{2}$, and let $a = \frac{1}{2} = k - \frac{m}{2}$. We again have by Lemma V.9 that the sum is minimized when the multi-sets are uniform. Since $\ell > \frac{n+1}{2}$ we have that \mathcal{H}_1 is uniform when it is equal to $[2^{n-\ell}, 1^{2\ell-n}]$. Furthermore, we have that if \mathcal{H}_2 were uniform, then every element in \mathcal{H}_2 would be at least 2. We also have that \mathcal{G}_1 and \mathcal{G}_2 are uniform when they are equal to $[2^{\frac{m-1}{2}}, 1]$.

Therefore

$$\begin{aligned} \sum_{\alpha \in \mathcal{G}_1} \sum_{\beta \in \mathcal{H}_1} [\min(\alpha, \beta) - 1] + \sum_{\alpha \in \mathcal{G}_1} \sum_{\beta \in \mathcal{H}_1} [\min(\alpha, \beta) - 1] &\leq \\ &\leq (n-\ell) \left(\frac{m-1}{2} \right) + \left(\frac{m-1}{2} \right) |\mathcal{H}_2| \\ &\leq (n-\ell)(k-1) + (m-k)(n+1-\ell). \end{aligned}$$

To see that this is less than $(k-1)(n-k) + (\ell-1)(m-k) - d + 1$ we use the assumption that $2\ell \geq n+5$. Also note that $d-1 < \frac{3m-3}{2}$ because $d \leq m$, and $m \geq 3$. We have:

$$d-1 < \frac{3m-3}{2}$$

$$d-1 < 3(m-k) \leq (m-k)(2\ell - n - 2)$$

$$(m-k)(n+1-\ell) < (m-k)(\ell-1) - d + 1. \quad \square$$

Proof of Proposition V.10. Under the given assumptions we can apply one of Lemma V.13, Lemma V.14, or Lemma V.15. We then have that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (m-k)(\ell-1) - d + 1.$$

Since the left side is greater than or equal to

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\gcd(\alpha, \beta) - 1],$$

it cannot be that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\gcd(\alpha, \beta) - 1] = (k-1)(n-\ell) + (m-k)(\ell-1) - d + 1.$$

However, Lemma V.4 states that the above must hold, and so we have a contradiction. □

Lemma V.16. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1 with $m = n$. Then $\ell \neq k + \frac{3}{2}$.*

Proof. It cannot be that both k and ℓ are integers if their difference is $\frac{3}{2}$. □

5.6 Proof of Proposition V.11

Proof of Proposition V.11. We have from Lemma V.9 that the sum

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

is maximized when the multi-sets are uniform. This sum is an upper bound for

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1].$$

We also know from Lemma V.4 that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

So if

$$(5.3) \quad \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1,$$

then there will be a contradiction.

The multi-sets are uniform when they are

$$\mathcal{G}_1 = \left[3^a, 2^{\frac{m-3a}{2}} \right], \mathcal{G}_2 = \left[2^{\frac{m-a-2}{2}}, 1^{a+2} \right], \mathcal{H}_1 = \left[3^b, 2^{\frac{n-3b}{2}} \right], \mathcal{H}_2 = \left[2^{\frac{n-b-2}{2}}, 1^{b+2} \right].$$

Substituting these multi-sets into the inequality (5.3) we have

$$\begin{aligned} & \left(\frac{m-3a}{2} \right) \left(\frac{n-b}{2} \right) + a \left(2b + \frac{n-3b}{2} \right) + \left(\frac{m-a-2}{2} \right) \left(\frac{n-b-2}{2} \right) < \\ & < \left(\frac{m-a-2}{2} \right) \left(\frac{n+b}{2} \right) + \left(\frac{n-b-2}{2} \right) \left(\frac{m+a}{2} \right) - d + 1 \\ & 2ab + a + b < \frac{mb}{2} + \frac{na}{2} - d < \frac{a+b-2}{2}m \\ & \frac{4ab+2a+2b}{a+b-2} < m. \end{aligned}$$

Therefore, whenever $m > \frac{4ab+2a+2b}{a+b-2}$ there is a contradiction, and so $m \leq \frac{4ab+2a+2b}{a+b-2}$. □

5.7 Proof of Proposition V.12

Lemma V.17. *Let m, n, k , and ℓ be as in Proposition V.12. Then*

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] \leq \min\{m\ell - k - \ell + 1, nk - k - \ell + 1\}.$$

Proof. We know from Lemma V.9 that the sum $\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$ is maximized when the multi-sets are uniform. Under the assumptions that $k < \frac{m+1}{2}$ and $\ell < \frac{n+1}{2}$ we have that \mathcal{G}_2 and \mathcal{H}_2 are uniform when

$$\mathcal{G}_2 = [2^{k-1}, 1^{m+2-2k}], \mathcal{H}_2 = [2^{\ell-1}, 1^{n+2-2\ell}].$$

From this we have that

$$(5.4) \quad \sum_{\alpha \in \mathcal{G}_2} \sum_{\beta \in \mathcal{H}_2} [\min(\alpha, \beta) - 1] = (k-1)(\ell-1).$$

If $\lceil \frac{m}{k} \rceil \leq \lfloor \frac{n}{\ell} \rfloor$ then for uniform multi-sets \mathcal{G}_1 and \mathcal{H}_1 we have that

$$\sum_{\alpha \in \mathcal{G}_1} \sum_{\beta \in \mathcal{H}_1} [\min(\alpha, \beta) - 1] = \sum_{\alpha \in \mathcal{G}_1} \sum_{\beta \in \mathcal{H}_1} [\alpha - 1] = \ell(m-k).$$

Note as well that the sum is also less than $k(n - \ell)$ because by assumption that $\frac{m}{k} \leq \frac{n}{\ell}$ we have that $m\ell \leq nk$. So we have that $\ell(m - k) \leq k(n - \ell)$.

Likewise, if $\lceil \frac{n}{\ell} \rceil \leq \lfloor \frac{m}{k} \rfloor$ then for uniform multi-sets \mathcal{G}_1 and \mathcal{H}_1 we have that

$$\sum_{\alpha \in \mathcal{G}_1} \sum_{\beta \in \mathcal{H}_1} [\min(\alpha, \beta) - 1] = \sum_{\alpha \in \mathcal{G}_1} \sum_{\beta \in \mathcal{H}_1} [\beta - 1] = k(n - \ell).$$

Again note that the sum is also less than $m(k - \ell)$, because by assumption $\frac{n}{\ell} \leq \frac{m}{k}$ which implies that $nk \leq m\ell$. So we have that $k(n - \ell) \leq \ell(m - k)$.

Finally, if $\lceil \frac{m}{k} \rceil > \lfloor \frac{n}{\ell} \rfloor$ and $\lceil \frac{n}{\ell} \rceil > \lfloor \frac{m}{k} \rfloor$ then it must be that $\lceil \frac{m}{k} \rceil = \lceil \frac{n}{\ell} \rceil$. Let $\omega = \lfloor \frac{m}{k} \rfloor = \lfloor \frac{n}{\ell} \rfloor$. Then for uniform multi-sets \mathcal{G}_1 and \mathcal{H}_1 we have that

$$\begin{aligned} \sum_{\alpha \in \mathcal{G}_1} \sum_{\beta \in \mathcal{H}_1} [\min(\alpha, \beta) - 1] &< \sum_{\substack{\alpha \in \mathcal{G}_1 \\ \alpha = \omega}} \sum_{\beta \in \mathcal{H}_1} [\alpha - 1] + \sum_{\substack{\alpha \in \mathcal{G}_1 \\ \alpha = \omega + 1}} \sum_{\beta \in \mathcal{H}_1} [\alpha - 1] \\ &< \ell(m - k). \end{aligned}$$

Note that we could have done the symmetric argument—summing over the elements of \mathcal{H}_1 and \mathcal{H}_2 —to see that the sum is also less than $k(n - \ell)$.

Combining the above results we see that

$$(5.5) \quad \sum_{\alpha \in \mathcal{G}_1} \sum_{\beta \in \mathcal{H}_1} [\min(\alpha, \beta) - 1] \leq \min\{\ell(m - k), k(n - \ell)\}.$$

Combining equations (5.4) and (5.5) we have that

$$\begin{aligned} \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] &\leq (k - 1)(\ell - 1) + \min\{\ell(m - k), k(n - \ell)\} \\ &\leq \min\{m\ell - k - \ell + 1, nk - k - \ell + 1\}. \quad \square \end{aligned}$$

Lemma V.18. *Let k, ℓ, m and n be positive integers such that $m \geq 19$ and $k < \frac{m+1}{2}$ and $4 \leq \ell \leq \frac{n-3}{2}$. Then*

$$\min\{m\ell - k - \ell + 1, nk - k - \ell + 1\} < (k - 1)(n - \ell) + (\ell - 1)(m - k) - d + 1.$$

Proof. We will begin with a proof by contradiction in the case that $4 \leq \ell \leq \frac{n-10}{2}$.

Assume that

$$\min\{m\ell - k - \ell + 1, nk - k - \ell + 1\} \geq (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

This inequality holds if and only if both

$$m\ell - k - \ell + 1 \geq (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and

$$nk - k - \ell + 1 \geq (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

hold. By simplifying these equations we conclude that the first is equivalent to

$$(5.6) \quad m + d - 2 \geq (k-1)(n - 2(\ell - 1)),$$

and the second is equivalent to

$$(5.7) \quad n + d - 2 \geq (\ell - 1)(m - 2(k - 1)).$$

However we then conclude (because $n \geq d$) that both

$$2n \geq n + d - 2 \geq (\ell - 1)(m - 2(k - 1)) \geq 3(m - 2(k - 1))$$

and

$$2m > m + d - 2 \geq (k-1)(n - 2(\ell - 1)) > m/6(n - 2(\ell - 1))$$

hold. Simplifying we see that both

$$k - 1 > \frac{m}{2} - \frac{n}{3} \geq \frac{m}{6}$$

and

$$\ell - 1 > (n - 12)/2$$

must hold.

We proceed with the remaining possibility that $\frac{n-9}{2} \leq \ell \leq \frac{n-3}{2}$ on a case by case basis. We will again use a proof by contradiction so that the above calculations still hold.

Substituting $\ell = \frac{n-9}{2}$ into equations (5.6) and (5.7) we see that

$$m \geq 11k - 9 - d$$

and

$$n + d - 2 \geq \left(\frac{n - 11}{2} \right) (m - 2(k - 1)).$$

If we define $2c := (m - 2(k - 1))$, then we have that

$$\begin{aligned} n + d - 2 &\geq c(n - 11) \\ c &\leq \frac{d + 9}{n - 11} + 1. \end{aligned}$$

Note that $n \geq 17$ since $4 \leq \frac{n-9}{2}$. Then since $d \leq n$ we have that $\frac{d+9}{n-11} \leq 9$. Substituting for the definition for c we can conclude that

$$m \leq 9 + 2k.$$

Combining this with the other inequality that $m \geq 11k - 9 - d$ we can see that $k \leq 2 + \frac{d}{9}$. We now conclude that $m \leq 18$. Since we have assumed that $m > 18$ we have a contradiction.

The method of proof is identical for the remaining cases and is left to the reader.

□

Proof of Proposition V.12. By Lemma V.17 we know that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] \leq \min\{m\ell - k - \ell + 1, nk - k - \ell + 1\}.$$

Furthermore, by Lemma V.18 we know that

$$\min\{m\ell - k - \ell + 1, nk - k - \ell + 1\} < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

Combining these, and the fact that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] \leq \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1],$$

we have that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

However, Lemma V.4 states that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1,$$

and so we have a contradiction. □

In Lemmas V.19–V.26 we classify all possibilities for Theorem V.1 with $\ell \leq 4$.

5.8 Remaining Sporadic Cases

The three main propositions have shown that most (m, n, k, ℓ) tuples do not correspond to polynomials $G(X), H(Y)$ from Theorem V.1. We handle the remaining cases in an exhaust.

5.8.1 $\ell = 2$

Lemma V.19. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. Furthermore, let $m \geq n \geq 6$ and $\ell = 2$. Then it cannot be that $3 \leq k \leq \frac{m+1}{2}$.*

Proof. We will show that if $3 \leq k \leq \frac{m+1}{2}$ then

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1,$$

so in particular there is no equality. This would be a contradiction because we proved in Lemma V.4 that this must be an equality.

Note that since $\ell = 2$ it must be that the ramification of $H(Y)$ is

$$\mathcal{H}_1 = [b, n-b], \quad \mathcal{H}_2 = [2, 1^{n-2}],$$

for some $1 \leq b < n$ with $(b, n) = 1$. We also know from Lemma V.9 that the sum

$$\sum_{\alpha \in \mathcal{G}_2} \sum_{\beta \in \mathcal{H}_2} [\min(\alpha, \beta) - 1]$$

is maximized when \mathcal{G}_2 is uniform. This occurs when $\mathcal{G}_2 = [2^{k-1}, 1^{m+2-2k}]$. In this case we have that

$$(5.8) \quad \sum_{\alpha \in \mathcal{G}_2} \sum_{\beta \in \mathcal{H}_2} [(\alpha, \beta) - 1] \leq \sum_{\alpha \in \mathcal{G}_2} \sum_{\beta \in \mathcal{H}_2} [\min(\alpha, \beta) - 1] = k - 1.$$

We also know from Lemma IV.13 that for every element $\alpha \in \mathcal{G}_1$

$$(\alpha, b) + (\alpha, n-b) \leq \alpha + 1.$$

Using this we see that

$$\sum_{\alpha \in \mathcal{G}_1} \sum_{\beta \in \mathcal{H}_1} [(\alpha, \beta) - 1] \leq \sum_{\alpha \in \mathcal{G}_1} [\alpha - 1] = m - k.$$

Combining this with equation (5.8) we have that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] \leq m - k + k - 1 = m - 1.$$

Note that if $n \geq 6$ and $k \geq 3$ then $m-1$ is less than $(k-1)(n-2) + (m-k) - d + 1$. To see this note that $(n-3)(k-2) - 2 > 0$. We then have

$$(n-3)(k-2) - 2 > 0$$

$$nk - 3k - 2n + 4 > 0$$

$$nk + 4 > 2n + 3k \geq 3k + n + d$$

$$nk - 2k - n + 2 + m - k - d + 1 > m - 1$$

$$(k-1)(n-2) + (m-k) - d + 1 > m - 1. \quad \square$$

Lemma V.20. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. Furthermore, let $m \geq n \geq 4$ and $\ell = 2$. Then it cannot be that $5 \leq k \leq \frac{m+1}{2}$.*

Proof. We will show that if $5 \leq k \leq \frac{m+1}{2}$ then

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1,$$

so in particular there is no equality. This would be a contradiction because we proved in Lemma V.4 that this must be an equality.

Note that since $\ell = 2$ it must be that the ramification of $H(Y)$ is

$$\mathcal{H}_1 = [b, n-b], \quad \mathcal{H}_2 = [2, 1^{n-2}],$$

for some $1 \leq b < n$ with $(b, n) = 1$. We also know from Lemma V.9 that the sum

$$\sum_{\alpha \in \mathcal{G}_2} \sum_{\beta \in \mathcal{H}_2} [\min(\alpha, \beta) - 1]$$

is maximized when \mathcal{G}_2 is uniform. This occurs when $\mathcal{G}_2 = [2^{k-1}, 1^{m+2-2k}]$. In this case we have that

$$(5.9) \quad \sum_{\alpha \in \mathcal{G}_2} \sum_{\beta \in \mathcal{H}_2} [(\alpha, \beta) - 1] \leq \sum_{\alpha \in \mathcal{G}_2} \sum_{\beta \in \mathcal{H}_2} [\min(\alpha, \beta) - 1] = k - 1.$$

We again use the fact from Lemma IV.13 that for every element $\alpha \in \mathcal{G}_1$

$$(\alpha, b) + (\alpha, n - b) \leq \alpha + 1.$$

Using this we see that

$$\sum_{\alpha \in \mathcal{G}_1} \sum_{\beta \in \mathcal{H}_1} [(\alpha, \beta) - 1] \leq \sum_{\alpha \in \mathcal{G}_1} [\alpha - 1] = m - k.$$

Combining this with equation (5.9) we have that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] \leq m - k + k - 1 = m - 1.$$

Note that if $n \geq 4$ and $k \geq 5$ then $m - 1$ is less than $(k - 1)(n - 2) + (m - k) - d + 1$.

To see this note that $(n - 3)(k - 2) - 2 > 0$. We then have

$$(n - 3)(k - 2) - 2 > 0$$

$$nk - 3k - 2n + 4 > 0$$

$$nk + 4 > 2n + 3k \geq 3k + n + d$$

$$nk - 2k - n + 2 + m - k - d + 1 > m - 1$$

$$(k - 1)(n - 2) + (m - k) - d + 1 > m - 1. \quad \square$$

Lemma V.21. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. Furthermore, let $m \geq n = 3$ and $\ell = 2$. Then either*

- $3 \nmid m$ and $(G(X), H(Y))$ is equivalent to $(T_m(X), T_3(Y))$ —with $T_m(X)$ and $T_3(Y)$ Chebyshev polynomials with the same branch points, or
- $3 \mid m$ and $G(X)$ has one ramification point of index either 4 or 3, and all other finite ramification points of index 2 or 1.

Proof. First we study the case with $3 \nmid m$:

We have from Lemma II.9 that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} [2\alpha - (\alpha, 2) - (\alpha, 1)] = m - 1.$$

Furthermore, we know that $\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} [\alpha - (\alpha, 1)] = m - 1$. Therefore, it must be that $\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} [\alpha - (\alpha, 2)] = 0$, which means that every element of \mathcal{G}_1 and \mathcal{G}_2 is either 2 or 1. Since there are $m + 1$ elements in \mathcal{G}_1 and \mathcal{G}_2 combined, and the sum of all of the elements is $2m$ this means there are exactly two elements equal to 1. In this case $G(X)$ equivalent to a Chebyshev polynomial.

In the case where $3|m$, we again apply Lemma II.9 and see that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} [2\alpha - (\alpha, 2) - (\alpha, 1)] = m + 1.$$

Since we still have that $\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} [\alpha - (\alpha, 1)] = m - 1$, we can conclude that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} [\alpha - (\alpha, 2)] = 2.$$

Furthermore, if $\alpha - (\alpha, 2) \neq 0$ then $\alpha - (\alpha, 2) \geq 2$. In particular, there is exactly one element of \mathcal{G}_1 and \mathcal{G}_2 which is greater than 2, and the element cannot be larger than 4, because $\alpha - (\alpha, 2) = 2$ if and only if α is 3 or 4. \square

Lemma V.22. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. If $\ell = k = 2$ then $G(X)$ and $H(Y)$ have ramification structure equal to one of the following:*

- $\mathcal{G}_1 = [1, 4], \mathcal{H}_1 = [3, 2], \mathcal{G}_2 = \mathcal{H}_2 = [2, 1^3];$
- $\mathcal{H}_1 = [1, 4], \mathcal{G}_1 = [3, 2], \mathcal{G}_2 = \mathcal{H}_2 = [2, 1^3];$
- $\mathcal{G}_1 = [4, 3], \mathcal{H}_1 = [6, 1], \mathcal{G}_2 = \mathcal{H}_2 = [2, 1^5].$
- $\mathcal{H}_1 = [4, 3], \mathcal{G}_1 = [6, 1], \mathcal{G}_2 = \mathcal{H}_2 = [2, 1^5].$

Note that these are cases 2 and 12 of \mathcal{R}_0 .

Proof. We begin by showing that under these assumptions it must be that $m = n$. If $m > n$, then $m \geq n + d$. It must be that $\mathcal{G}_2 = [2, 1^{m-2}]$ and $\mathcal{H}_2 = [2, 1^{n-2}]$. Therefore

$$\sum_{\alpha \in \mathcal{G}_2} \sum_{\beta \in \mathcal{H}_2} [\beta - (\alpha, \beta)] = m - 2.$$

We also have that $\sum_{\alpha \in \mathcal{G}_1} \sum_{\beta \in \mathcal{H}_1} [\beta - (\alpha, \beta)] > 0$, which means that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\beta - (\alpha, \beta)] > m - 2.$$

However, we know by Lemma II.9 that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\beta - (\alpha, \beta)] = n + d - 2,$$

which is a contradiction because $m - 2 \geq n + d - 2$.

Therefore the set $\mathcal{G}_1 = [a, m - a]$ for some $1 \leq a < m$ with $(a, m) = 1$ and likewise $\mathcal{H}_1 = [b, m - b]$ with $1 \leq b < m$ with $(b, m) = 1$. Plugging these values into Lemma II.9 we have

$$(5.10) \quad 2m - (a, b) - (a, m - b) - (m - a, b) - (m - a, m - b) + m - 2 = 2m - 2$$

$$(5.11) \quad (a, b) + (a, m - b) + (m - a, b) + (m - a, m - b) = m.$$

However we have from the proof of Proposition IV.4 that

$$(a, b) + (a, m - b) \leq a + 1,$$

with equality if and only if a divides one of b or $m - b$. Additionally, if $(a, b) + (a, m - b) < a + 1$ then $(a, b) + (a, m - b) = a$ if and only if $a = 2$. This is because if a divides neither b nor $m - b$ then each of the summands is at most $\frac{a}{2}$. However if both summands are $\frac{a}{2}$, then by coprimality of b and m it must be that $\frac{a}{2} = 1$. It cannot be that both a and $m - a$ are equal to 2, and so it cannot be that both

$(a, b) + (a, m - b) = a$, and $(m - a, b) + (m - a, m - b) = m - a$. Therefore the only way that

$$(a, b) + (a, m - b) + (m - a, b) + (m - a, m - b) = m$$

is if (up to exchanging a and $m - a$) $(a, b) + (a, m - b) = a - 1$ and $(m - a, b) + (m - a, m - b) = m - a + 1$.

Furthermore if $a \geq 3$ and $(a, b) + (a, m - b) < a$ then

$$(a, b) + (a, m - b) \leq \frac{a}{2} + \frac{a}{3} \leq \frac{5a}{6}.$$

In particular, if $a > 6$ this is less than $a - 1$. Additionally, if $a = 5$ we also have that

$(a, b) + (a, m - b) = 2 < a - 1$ if the sum is not equal to $a + 1$.

If $(a, b) + (a, m - b) < a - 1$ then

$$(a, b) + (a, m - b) + (m - a, b) + (m - a, m - b) \neq m.$$

So up to equivalence of switching a and $m - a$, the only possible ways the sum can equal m is if $a \in \{3, 4, 6\}$ and $m - a$ divides one of b or $m - b$.

If $a = 3$, then a must be coprime to both b and $m - b$. Additionally, $m - a$ must divide one of b or $m - b$. If $m > 6$ the only way this can occur is if $m - a = m - b$ or $m - a = b$ since $m - a > \frac{m}{2}$. It cannot be that $m - a = m - b$ because then $a = b = 3$. Likewise, if $m - a = b$ then $a = m - b = 3$. So $m \leq 6$, and cannot equal 6 because then $(a, m) \neq 1$. If $m = 5$, then it must be that $b = 1$ or $b = 4$. Both cases satisfy equation (5.10). This corresponds to the second case in the Lemma. Furthermore, if $m = 4$ it is clear that b or $m - b$ would equal 3, and so would be equal to a .

If $a = 4$, then we can see in the same way that $m < 8$. If m were equal to 8 then it wouldn't be coprime to a . If m were greater than 8, then since $m - a$ would be greater than $\frac{m}{2}$ it would have to be equal to one of b or $m - b$, which would lead to a contradiction.

If $m = 7$, then a simple exhaust reveals that the only options for b which satisfy equation (5.10) are $b = 1$ or $b = 6$. This corresponds to the third and fourth cases in the Lemma. If $m = 5$ we have the same solutions as before.

Finally, if $a = 6$, we can again conclude that $m < 12$. Another exhaust reveals that the only possible solutions to equation (5.10) are when $m = 7$ and $b = 3$ or $b = 4$. This again corresponds to the third and fourth cases in the Lemma. \square

Lemma V.23. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. Furthermore, let $n \in \{4, 5\}$ and $\ell = 2$. If $k \in \{3, 4\}$ then the only possibilities are*

- $\mathcal{G}_1 = [3^2, 2]$, $\mathcal{G}_2 = [2^2, 1^4]$, $\mathcal{H}_1 = [3, 1]$, $\mathcal{H}_2 = [2, 1^2]$;
- $\mathcal{G}_1 = [3^2, 1^2]$, $\mathcal{G}_2 = [2^3, 1^2]$, $\mathcal{H}_1 = [3, 1]$, $\mathcal{H}_2 = [2, 1^2]$;
- $\mathcal{G}_1 = [3, 1^2]$, $\mathcal{G}_2 = [2^2, 1]$, $\mathcal{H}_1 = [3, 2]$, $\mathcal{H}_2 = [2, 1^3]$;
- $\mathcal{G}_1 = [2^2, 1]$, $\mathcal{G}_2 = [2^2, 1]$, $\mathcal{H}_1 = [3, 2]$, $\mathcal{H}_2 = [2, 1^3]$;
- $\mathcal{G}_1 = [2^2, 1]$, $\mathcal{G}_2 = [2^2, 1]$, $\mathcal{H}_1 = [4, 1]$, $\mathcal{H}_2 = [2, 1^3]$;

These correspond to cases 3, 13, 14 in the list \mathcal{R}_0 , and the infinite families 1 and 3 in the list \mathcal{S}_1 .

Proof. If $n = 4$ the only ramification structure that $H(Y)$ can have is $\mathcal{H}_1 = [3, 1]$, and $\mathcal{H}_2 = [2, 1^2]$. We have from Lemma II.9 that

$$(5.12) \quad \sum_{\alpha \in \mathcal{G}_1} [2\alpha - (\alpha, 3) - 1] + \sum_{\alpha \in \mathcal{G}_2} [3\alpha - (\alpha, 2) - 2] = m + d - 2.$$

We also have that

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} [\alpha - 1] = m - 1.$$

Substituting into equation (5.12) we have:

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} [\alpha - 1] + \sum_{\alpha \in \mathcal{G}_1} [\alpha - (\alpha, 3)] + \sum_{\alpha \in \mathcal{G}_2} [2\alpha - (\alpha, 2) - 1] = m + d - 2$$

$$\sum_{\alpha \in \mathcal{G}_1} [\alpha - (\alpha, 3)] + \sum_{\alpha \in \mathcal{G}_2} [2\alpha - (\alpha, 2) - 1] = d - 1.$$

Since $d \in \{1, 2, 4\}$ we have that $d - 1 \in \{0, 1, 3\}$.

If $k = 3$ then \mathcal{G}_2 is either $[2^2, 1^{m-4}]$ or $[3, 1^{m-3}]$. In either case $\sum_{\alpha \in \mathcal{G}_2} [\alpha - 1] = 2$.

This means that $d - 1$ must equal 3. We then also have that

$$\sum_{\alpha \in \mathcal{G}_1} [\alpha - (\alpha, 3)] + \sum_{\alpha \in A_2} [\alpha - (\alpha, 2)] = 1.$$

However, there is no positive integer α such that $\alpha - (\alpha, 2) = 1$. The only positive integer α such that $\alpha - (\alpha, 3) = 1$ is $\alpha = 2$. Since $k = 3$ this means that \mathcal{G}_1 has to have one element equal to 2 and the other two elements equal to either 3 or 1.

Furthermore $\mathcal{G}_2 = [2^2, 1^{m-4}]$ so that $\sum_{\alpha \in \mathcal{G}_2} [\alpha - (\alpha, 2)] = 0$. These possibilities are

- $\mathcal{G}_1 = [3^2, 2]$;
- $\mathcal{G}_1 = [3, 2, 1]$;
- $\mathcal{G}_1 = [2, 1^2]$.

Since we also require that $4|m$ either of $[3^2, 2]$ or $[2, 1^2]$ are possible. However if $m = 4$ then $\mathcal{G}_2 = [2^2]$ and so $G(X)$ is equivalent to a power of a smaller degree polynomial.

If $k = 4$ then \mathcal{G}_2 is either $[2^3, 1^{m-6}]$, $[3, 2, 1^{m-5}]$, or $[4, 1^{m-4}]$. In any of these cases $\sum_{\alpha \in \mathcal{G}_2} [\alpha - 1] = 3$. This again means that $d - 1$ must equal 3. We also have that

$$\sum_{\alpha \in \mathcal{G}_1} [\alpha - (\alpha, 3)] + \sum_{\alpha \in A_2} [\alpha - (\alpha, 2)] = 0.$$

The only option for \mathcal{G}_2 which has $\sum_{\alpha \in A_2} [\alpha - (\alpha, 2)] = 0$ is $\mathcal{G}_2 = [2^3, 1^{m-6}]$. Additionally, we have that $\sum_{\alpha \in \mathcal{G}_1} [\alpha - (\alpha, 3)] = 0$ if and only if every element of \mathcal{G}_1 is equal

to either 3 or 1. Therefore the only options for \mathcal{H}_1 are $[3^j, 1^{m-3j}]$ for any positive integer j . However, we know that

$$\sum_{i=1}^2 \sum_{\beta \in \mathcal{H}_i} [\beta - 1] = m - 1.$$

Therefore, $2j + 3 = m - 1$ and so $j = \frac{m-4}{2}$. We also know that $3j \leq m$ so we have that $\frac{3m-12}{2} \leq m$, so that $m \leq 12$. We also know that $4|m$ and so $m \in \{4, 8, 12\}$.

Plugging in when $m = 12$ we have $\mathcal{G}_1 = [3^4]$, $\mathcal{G}_2 = [2^3, 1^6]$, but this is not allowed because then $G(X)$ would be a cube of a smaller degree polynomial. When $m = 8$ we have $\mathcal{G}_1 = [3^2, 1^2]$, $\mathcal{G}_2 = [2^3, 1^2]$, which is admissible. If $m = 4$ then $k \neq 4$.

If $n = 5$ then \mathcal{H}_1 can equal either $[4, 1]$ or $[3, 2]$ and \mathcal{H}_2 is equal to $[2, 1^3]$. We let ω_1 and ω_2 denote the elements of \mathcal{H}_1 . Again we have from Lemma II.9 that

$$(5.13) \quad \sum_{\alpha \in \mathcal{G}_1} \sum_{\beta \in \mathcal{H}_1} [\alpha - (\alpha, \beta)] + \sum_{\alpha \in \mathcal{G}_2} [4\alpha - (\alpha, 2) - 3] = m + d - 2.$$

Substituting that $\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} [\alpha - 1] = m - 1$ we have

$$\begin{aligned} m - 1 + \sum_{\alpha \in \mathcal{G}_1} [\alpha - (\alpha, \omega_1) - (\alpha, \omega_2) + 1] + \sum_{\alpha \in \mathcal{G}_2} [3\alpha - (\alpha, 2) - 2] &= m + d - 2 \\ \sum_{\alpha \in \mathcal{G}_1} [\alpha - (\alpha, \omega_1) - (\alpha, \omega_2) + 1] + \sum_{\alpha \in \mathcal{G}_2} [3\alpha - (\alpha, 2) - 2] &= d - 1. \end{aligned}$$

We have that $d \in \{1, 5\}$ and so $d - 1 \in \{0, 4\}$. If $k = 3$ then like before $\sum_{\alpha \in \mathcal{G}_2} [\alpha - 1] =$

2. So we have that

$$\sum_{\alpha \in \mathcal{G}_1} [\alpha - (\alpha, \omega_1) - (\alpha, \omega_2) + 1] + \sum_{\alpha \in \mathcal{G}_2} [\alpha - (\alpha, 2)] = d - 5.$$

This means that $d = 5$. The only way that $\sum_{\alpha \in \mathcal{G}_2} [\alpha - (\alpha, 2)] = 0$ is if $\mathcal{G}_2 = [2^2, 1^{m-4}]$.

Furthermore, if $\mathcal{H}_1 = [3, 2]$ then $\sum_{\alpha \in \mathcal{G}_1} [\alpha - (\alpha, \omega_1) - (\alpha, \omega_2) + 1] = 0$ if and only if every element of \mathcal{G}_1 is in $\{1, 2, 3\}$. Since $k = 3$, the options for \mathcal{G}_1 with coprime elements are

- $[3^2, 2]$;
- $[3^2, 1]$;
- $[3, 2^2]$;
- $[3, 2, 1]$;
- $[3, 1^2]$;
- $[2^2, 1]$;
- $[2, 1^2]$.

We also need that m is divisible by 5 so that $d = 5$. The only options which satisfy this are

- $[3, 1^2]$;
- $[2^2, 1]$.

If $\mathcal{H}_1 = [4, 1]$ then $\sum_{\alpha \in \mathcal{G}_1} [\alpha - (\alpha, \omega_1) - (\alpha, \omega_2) + 1] = 0$ if and only if every element of \mathcal{G}_1 is in $\{1, 2, 4\}$. Since $k = 3$ the options for \mathcal{G}_1 with coprimality of elements are

- $[4^2, 1]$;
- $[4, 2, 1]$;
- $[4, 1^2]$;
- $[2^2, 1]$;
- $[2, 1^2]$.

We also need that m is divisible by 5 so that $d = 5$. The only option which satisfies this is $\mathcal{G}_2 = [2^2, 1]$. This corresponds to the last possibility in the Lemma.

If instead we have that $k = 4$ then like before $\sum_{\alpha \in \mathcal{G}_2} [\alpha - 1] = 3$. So we have that

$$\sum_{\alpha \in \mathcal{G}_1} [\alpha - (\alpha, \omega_1) - (\alpha, \omega_2) + 1] + \sum_{\alpha \in \mathcal{G}_2} [\alpha - (\alpha, 2)] = d - 7.$$

However, this cannot happen since $d \in \{1, 5\}$. \square

5.8.2 $\ell = 3$

Lemma V.24. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. Furthermore, let $m \geq n \geq 10$ and $\ell = 3$. Then it cannot be that $3 \leq k \leq \frac{m+1}{2}$.*

Proof. We will show, following the same methods as used in the proof of the previous Lemma, that if $3 \leq k \leq \frac{m+1}{2}$ then

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1,$$

which again would be a contradiction of Lemma V.4.

Note that since $\ell = 3$ the ramification of $H(Y)$ over one branch point must have the form $\mathcal{H}_1 = [b_1, b_2, n - b_1 - b_2]$. The ramification over the other branch point can be either $\mathcal{H}_2 = [3, 1^{n-3}]$, or $\mathcal{H}_2 = [2^2, 1^{n-4}]$. However we know from Lemma V.9 that the sum

$$\sum_{\alpha \in \mathcal{G}_2} \sum_{\beta \in \mathcal{H}_2} [\min(\alpha, \beta) - 1]$$

is maximized when both \mathcal{G}_2 and \mathcal{H}_2 are uniform. This occurs when

$$\mathcal{G}_2 = [2^{k-1}, 1^{m+2-2k}], \quad \text{and} \quad \mathcal{H}_2 = [2^2, 1^{n-4}].$$

In this case we have that

$$(5.14) \quad \sum_{\alpha \in \mathcal{G}_2} \sum_{\beta \in \mathcal{H}_2} [(\alpha, \beta) - 1] \leq \sum_{\alpha \in \mathcal{G}_2} \sum_{\beta \in \mathcal{H}_2} [\min(\alpha, \beta) - 1] = 2k - 2.$$

Furthermore, since $\gcd(b_1, b_2, n) = 1$ we know that for any positive integer a , the sum

$$(a, b_1) + (a, b_2) + (a, n - b_1 - b_2) \leq 2a + 1.$$

This clearly holds for $a = 1$, so we need only check that it also holds for $a > 1$. In this case, if a divides two of b_1, b_2 , and $n - b_1 - b_2$ then the sum is also clearly equal to $2a + 1$. If a divides one or none of them, then the sum is at most $2a$, because for any positive integer r with $a \nmid r$ it holds that $(a, r) \leq \frac{a}{2}$. We therefore have that

$$\sum_{\alpha \in \mathcal{G}_1} \sum_{\beta \in \mathcal{H}_1} [(\alpha, \beta) - 1] \leq \sum_{\alpha \in \mathcal{G}_1} [2\alpha - 2] = 2m - 2k.$$

Combining this with equation (5.14) gives

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] \leq 2m - 2k + 2k - 2 = 2m - 2.$$

Note that if $n \geq 10$ and $k \geq 3$ then $2m - 2$ is less than $(k-1)(n-3) + 2(m-k) - d + 1$.

To see this, note that $(n-5)(k-2) - 4 > 0$. We then have

$$(n-5)(k-2) - 4 > 0$$

$$nk - 5k - 2n + 6 > 0$$

$$nk + 6 > 2n + 5k \geq 5k + n + d$$

$$nk - 3k - n + 3 + 2m - 2k - d + 1 > 2m - 2$$

$$(k-1)(n-2) + (m-k) - d + 1 > 2m - 2. \quad \square$$

Lemma V.25. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. If $\ell = 3$ and $k = 2$ then $G(X)$ and $H(Y)$ have ramification in one of the following types:*

- $\mathcal{G}_1 = [3, 2]$, $\mathcal{G}_2 = [2, 1^3]$, $\mathcal{H}_1 = [3, 1^2]$, $\mathcal{H}_2 = [2^2, 1]$;
- $\mathcal{G}_1 = [4, 1]$, $\mathcal{G}_2 = [2, 1^3]$, $\mathcal{H}_1 = [2^2, 1]$, $\mathcal{H}_2 = [2^2, 1]$;

These possibilities correspond to case 3 in the list \mathcal{R}_0 . The last of these possibilities corresponds to the infinite family 1 in \mathcal{S}_1 .

Proof. Since $k = 2$ we have that $G(X)$ has ramification structure $\mathcal{G}_1 = [a, m - a]$, $\mathcal{G}_2 = [2, 1^{m-2}]$ for any $1 \leq a < m$ with $(a, m) = 1$. Likewise since $\ell = 3$ then

$\mathcal{H}_1 = [b, c, n - b - c]$ for integer b and c with $n - b - c > 0$ and $(b, c, n) = 1$. Also \mathcal{H}_2 will equal one of $[3, 1^{n-3}]$ or $[2^2, 1^{n-4}]$.

If $\mathcal{H}_2 = [3, 1^{n-3}]$, then

$$\sum_{\beta \in \mathcal{H}_2} \sum_{\alpha \in \mathcal{G}_2} [\beta - (\beta, \alpha)] = 3m - 3 \geq 3n - 3.$$

However, we know from Lemma II.9 that this is at most $2n - 2$, which means that n is at most 1, and so cannot occur.

If $\mathcal{H}_2 = [2^2, 1^{n-4}]$ then

$$\sum_{\beta \in \mathcal{H}_2} \sum_{\alpha \in \mathcal{G}_2} [\beta - (\beta, \alpha)] = 2m - 4.$$

If $m > n + d$ then $2m - 4 > 2n - 4 + 2d \geq 2n - 2$, which again is a contradiction.

Furthermore, if $m = n + d$, then $2m - 4 = 2n - 2$ if and only if $d = 1$. However we would also need that $\sum_{\beta \in \mathcal{H}_1} \sum_{\alpha \in \mathcal{G}_1} [\beta - (\alpha, \beta)] = 0$, which cannot happen when the elements of \mathcal{G}_1 are coprime. Therefore, it must be that $m = n$.

It therefore must be that

$$\sum_{\beta \in \mathcal{H}_1} \sum_{\alpha \in \mathcal{G}_1} [\beta - (\alpha, \beta)] = 2.$$

Since a and $m - a$ are coprime, then for every $\beta \in \mathcal{H}_1$

$$2\beta - (a, \beta) - (m - a, \beta) \geq \beta - 1.$$

So there is no element of \mathcal{H}_1 greater than 3. If there is an element of \mathcal{H}_1 equal to 3, then the other two must be equal to 1. Furthermore, in order that $6 - (3, a) - (3, m - a) = 2$ it is necessary that one of a or $m - a$ is divisible by 3. Therefore

$$\mathcal{H}_1 = [3, 1^2], [2^2, 1], \mathcal{G}_1 = [3, 2], \mathcal{G}_2 = [2, 1^3].$$

If no element of \mathcal{H}_1 is equal to 3, there can be either one or two elements of \mathcal{H}_1 equal to 2. If $\mathcal{H}_1 = [2, 1^2]$, then $\mathcal{H}_2 = [2^2]$ which by Lemma II.20 means $H(Y)$ is a square—which is a contradiction.

The only remaining option is that $\mathcal{H}_1 = \mathcal{H}_2 = [2^2, 1]$. However, we still need that one of the elements in \mathcal{G}_1 is divisible by 2, which gives that \mathcal{G}_1 is either $[2, 3]$ or $[4, 1]$. \square

Lemma V.26. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. If $\ell = k = 3$ then $G(X)$ and $H(Y)$ have ramification in one of the following types:*

- $\mathcal{G}_1 = \mathcal{H}_1 = \mathcal{G}_2 = \mathcal{H}_2 = [3, 1^2]$;
- $\mathcal{G}_1 = [3, 1^2]$, $\mathcal{H}_1 = \mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [4, 1^2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^2]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [3, 2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^2]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [4, 2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^3]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [3^2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [3, 1^4]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [3, 2^2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^3]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [3^2, 2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^4]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [4^2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^5]$;

These correspond to cases 1, 4, 5, 9, 10, 11, 15, and 17 of the list \mathcal{R}_0 . The second case above corresponds to the infinite family 4 in the list \mathcal{S}_1 .

Proof. We proved in Lemma V.24 that if $\ell = k = 3$ that $n \leq 22$. Furthermore, note that when $k = 3$ that \mathcal{G}_2 is either $[2^2, 1^{m-4}]$ or $[3, 1^{m-3}]$. Likewise, when $\ell = 3$ it must be that \mathcal{H}_2 is either $[2^2, 1^{n-4}]$ or $[3, 1^{n-3}]$. We substitute these into

$$\sum_{\alpha \in \mathcal{G}_2} \sum_{\beta \in \mathcal{H}_2} [\beta - (\alpha, \beta)]$$

and note that the smallest this can be is $2m - 8$.

Additionally, for every element $\beta \in \mathcal{H}_1$ it holds that $\sum_{\alpha \in \mathcal{G}_1} [\beta - (\alpha, \beta)] \geq \beta - 1$.

So in particular

$$\sum_{\beta \in \mathcal{H}_1} \sum_{\alpha \in \mathcal{G}_1} [\beta - (\alpha, \beta)] \geq n - \ell = n - 3.$$

By Lemma II.9 we know that

$$\sum_{i=1}^2 \sum_{\beta \in \mathcal{H}_1} \sum_{\alpha \in \mathcal{G}_1} [\beta - (\alpha, \beta)] = n + d - 2 \leq 2n - 2.$$

Plugging in our values for these sums we see that

$$\begin{aligned} 2m - 8 + n - 3 &\leq 2n - 2 \\ m &\leq \frac{n + 9}{2}. \end{aligned}$$

Since $n \leq 22$ we have that $m \leq 16$. We can now exhaust over these limited options.

The only options which satisfy Lemma II.9 while also having the elements each of the multi-sets be coprime are the ones listed in the statement of the Lemma. \square

5.8.3 $\ell > \frac{n-3}{2}$

Lemma V.27. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. Also let $k < \frac{m+1}{2}$ and $4 \leq \ell \leq \frac{n+1}{2}$. Then if $\ell = \frac{n-b}{2}$ for $b \in [-1, 14]$ then $k \geq \frac{m-12}{2}$.*

Proof. Since $\ell = \frac{n-b}{2} \geq 4$ we have that $n > 8 + b$.

Let $k = \frac{m-c}{2}$. Then since there are $m - k + 1$ elements of \mathcal{G}_2 , there are at least $c + 2$ elements of \mathcal{G}_2 equal to 1. We also have that

$$\sum_{\beta \in \mathcal{H}_2} [\beta - 1] = n - |\mathcal{H}_2| = n - (n + 1 - \ell) = \ell - 1.$$

So in particular

$$\sum_{\beta \in \mathcal{H}_2} \sum_{\alpha \in \mathcal{G}_2} [\beta - (\alpha, \beta)] \geq \sum_{\beta \in \mathcal{H}_2} \sum_{\substack{\alpha \in \mathcal{G}_2 \\ \alpha=1}} [\beta - (\alpha, \beta)] \geq (c + 2)(\ell - 1).$$

Since we know by Lemma II.9 that this is at most $2n - 2$ we have

$$\begin{aligned} (c+2) \binom{n-b-2}{2} &\leq 2n-2 \\ \binom{c-2}{2} n &\leq \frac{(c+2)(b+2)}{2} - 2 \\ n &\leq \frac{2}{c-2} \left[\frac{(c+2)(b+2)}{2} - 2 \right], \end{aligned}$$

whenever $c > 2$.

Furthermore, since $\ell = \frac{n-b}{2} \geq 4$ we have that $n \geq 8 + b$.

So we have that for $c > 2$

$$\begin{aligned} \frac{2}{c-2} \left[\frac{(c+2)(b+2)}{2} - 2 \right] &\geq n \geq 8 + b \\ (c+2)(b+2) - 4 &\geq (8+b)(c-2) \\ 16 + 4b &\geq 6c. \end{aligned}$$

So with $b \in [-1, 14]$ the largest that c can be is 12.

□

Lemma V.28. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. Let $4 \leq \ell \leq \frac{n+1}{2}$. Let a and b be positive integers such that $a + b \geq 3$. Then if $k = \frac{m-b}{2}$ and $\ell = \frac{n-a}{2}$ then the only possible ramification structures of $G(X)$ and $H(Y)$ are*

- $\mathcal{G}_1 = \mathcal{H}_1 = [3^2, 2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^4]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [3^3, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^3, 1^4]$;
- $\mathcal{G}_1 = [4, 3]$, $\mathcal{H}_1 = [6, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2, 1^5]$;
- $\mathcal{G}_1 = [6, 1]$, $\mathcal{H}_1 = [4, 3]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2, 1^5]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [4^2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^5]$.

These correspond to cases 12, 15, 17, and 19 from the list \mathcal{R}_0 .

Proof. From Proposition V.12 we know that $a \leq 14$ (because when $n \geq 22$ then $a \leq 3$). By Proposition V.27 we know that $b \leq 12$. This means there are only 168 possible pairings of a and b . Furthermore, for each a and b we know that $\frac{4ab+2a+2b}{a+b-2} \geq m \geq n \geq 3$. So we can exhaust over all the possible m, n, k , and ℓ which satisfy the requirements. The only possibilities are the ones stated. \square

Lemma V.29. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. Then it cannot be that $k = \frac{m}{2}$ and $\ell = \frac{n-1}{2}$.*

Proof. We know from Lemma V.9 that the sum

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

is maximized when the multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are uniform. However when \mathcal{G}_1 is uniform it is equal to $\left[2^{\frac{m}{2}}\right]$ which by Lemma II.20 means $G(X)$ is equivalent to a square of a smaller degree polynomial, which contradicts the assumptions. However, there is a unique element $\left[3, 2^{\frac{m-4}{2}}, 1\right]$ in $\mathcal{P}_{m,k}$ such that for all $C \in \mathcal{P}_{m,k}$ which are not uniform,

$$\left[3, 2^{\frac{m-4}{2}}, 1\right] \geq C.$$

This is true because it is the unique element whose refinement is the maximal element.

Therefore, for any non-uniform $C \in \mathcal{P}_{m,k}$ we have that

$$\sum_{\alpha \in \left[3, 2^{\frac{m-4}{2}}, 1\right]} \sum_{\beta \in \mathcal{H}_1} [\min(\alpha, \beta) - 1] \geq \sum_{\alpha \in C} \sum_{\beta \in \mathcal{H}_1} [\min(\alpha, \beta) - 1].$$

So the most uniform the multi-sets can be is

$$\mathcal{G}_1 = \left[3, 2^{\frac{m-4}{2}}, 1\right], \mathcal{G}_2 = \left[2^{\frac{m-2}{2}}, 1^2\right], \mathcal{H}_1 = \left[3, 2^{\frac{n-3}{2}}\right], \mathcal{H}_2 = \left[2^{\frac{n-3}{2}}, 1^3\right].$$

We will have a contradiction with Lemma V.4 whenever

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

However, we do not have the desired contradiction because

$$\begin{aligned}
& \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1 \\
& \left(\frac{n-3}{2}\right) \left(\frac{m-2}{2}\right) + \left(2 + \frac{m-4}{2}\right) + \left(\frac{m-2}{2}\right) \left(\frac{n-3}{2}\right) < \\
& < \left(\frac{m-2}{2}\right) \left(\frac{n+1}{2}\right) + \left(\frac{n-3}{2}\right) \left(\frac{m}{2}\right) - d + 1 \\
& d - 1 < m - 2 - \frac{m}{2} + \frac{n}{2} - \frac{3}{2} \\
& d + \frac{5}{2} < \frac{m+n}{2}.
\end{aligned}$$

Thus there is not necessarily a contradiction. In particular, when $m = n = d$ the inequality does not hold. However, we claim that for $m > 9$ there are no other possible multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 which do not have a contradiction. We will examine every tuple for which

$$\left(\left[3, 2^{\frac{m-4}{2}}, 1\right], \left[2^{\frac{m-2}{2}}, 1^2\right], \left[3, 2^{\frac{n-3}{2}}\right], \left[2^{\frac{m-3}{2}}, 1^3\right] \right)$$

is a refinement, and show that there is a contradiction in all of those cases. Since every possible tuple $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ has

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

upper bounded by at least one of the examined tuples we will see that only the most uniform case is possible.

Note that the only two multi-sets which have $\left[3, 2^{\frac{m-4}{2}}, 1\right]$ as a refinement are $\left[4, 2^{\frac{m-6}{2}}, 1^2\right]$ and $\left[3^2, 2^{\frac{m-8}{2}}, 1^2\right]$. Letting either be \mathcal{G}_1 and keeping the other three multi-sets uniform, we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and see there is a contradiction when $m > 8$.

The only multi-set which has $\left[2^{\frac{m-2}{2}}, 1^2\right]$ as a refinement is $\left[3, 2^{\frac{m-6}{2}}, 1^3\right]$. Letting this be \mathcal{G}_2 and keeping the other three multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and have a contradiction whenever $m > 8$.

The only two multi-sets which have $\left[3, 2^{\frac{n-3}{2}}\right]$ as a refinement are $\left[4, 2^{\frac{n-5}{2}}, 1\right]$ and $\left[3^2, 2^{\frac{n-7}{2}}, 1\right]$. Letting either be \mathcal{H}_1 while keeping the other multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and get a contradiction whenever $m > 9$.

Finally the only multi-set which as $\left[2^{\frac{n-3}{2}}, 1^3\right]$ as a refinement is $\left[3, 2^{\frac{n-7}{2}}, 1^4\right]$. Letting it be \mathcal{H}_2 while keeping the other multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and get a contradiction whenever $m > 9$.

An exhaust over all possibilities when $9 \geq m \geq n \geq 3$ reveals no examples of multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 which satisfy the stated properties.

Finally, when $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are as uniform as possible we have that

$$\begin{aligned} \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] &= 2 + \binom{m-4}{2} \binom{n-3}{2} + \binom{m-2}{2} \binom{n-3}{2} \\ &= \binom{m}{2} \binom{n-3}{2} + \binom{m-2}{2} \binom{n+3}{2} - n - \frac{3m}{2} + 8. \end{aligned}$$

This is equal to $(k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$ if and only if

$$d = n + \frac{3m}{2} - 7.$$

However when $m \geq 5$ this cannot occur since the right side will always be less than d .

□

Lemma V.30. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. Then it cannot be that $k = \frac{m-1}{2}$ and $\ell = \frac{n}{2}$.*

Proof. We proceed in the same way as the previous proof. We know from Lemma V.9 that the sum

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

is maximized when the multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are uniform. However when \mathcal{H}_1 is uniform it is equal to $\lceil 2^{\frac{n}{2}} \rceil$ which by Lemma II.20 means $G(X)$ is equivalent to a square of a smaller degree polynomial, which contradicts the assumptions. However, there is a unique element $\left[3, 2^{\frac{n-4}{2}}, 1\right]$ in $\mathcal{P}_{n,\ell}$ such that for all $C \in \mathcal{P}_{n,\ell}$ which are not uniform,

$$\left[3, 2^{\frac{n-4}{2}}, 1\right] \geq C.$$

This is true because it is the unique element whose refinement is the maximal element.

Therefore, for any non-uniform $C \in \mathcal{P}_{n,\ell}$ we have that

$$\sum_{\beta \in \left[3, 2^{\frac{n-4}{2}}, 1\right]} \sum_{\alpha \in \mathcal{G}_1} [\min(\alpha, \beta) - 1] \geq \sum_{\beta \in C} \sum_{\alpha \in \mathcal{G}_1} [\min(\alpha, \beta) - 1].$$

So the most uniform the multi-sets can be is

$$\mathcal{G}_1 = \left[3, 2^{\frac{m-3}{2}}\right], \mathcal{G}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right], \mathcal{H}_1 = \left[3, 2^{\frac{n-4}{2}}, 1\right], \mathcal{H}_2 = \left[2^{\frac{m-2}{2}}, 1^2\right].$$

We will have a contradiction with Lemma V.4 whenever

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

However, we do not have the desired contradiction because

$$\begin{aligned}
& \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1 \\
& \left(\frac{n-4}{2}\right) \left(\frac{m-1}{2}\right) + \left(2 + \frac{m-3}{2}\right) + \left(\frac{m-3}{2}\right) \left(\frac{n-2}{2}\right) < \\
& < \left(\frac{m-3}{2}\right) \left(\frac{n}{2}\right) + \left(\frac{n-2}{2}\right) \left(\frac{m+1}{2}\right) - d + 1 \\
& d + 4 < \frac{m}{2} + \frac{n}{2} - \frac{1}{2} \\
& d + \frac{9}{2} < \frac{m+n}{2}.
\end{aligned}$$

Thus there is not necessarily a contradiction. In particular, when $m = n = d$ the inequality does not hold. However, we claim that for $m > 13$ there are no other possible multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 which do not have a contradiction. We will examine every tuple for which

$$\left(\left[3, 2^{\frac{m-3}{2}}\right], \left[2^{\frac{m-3}{2}}, 1^3\right], \left[3, 2^{\frac{n-4}{2}}, 1\right], \left[2^{\frac{n-2}{2}}, 1^2\right] \right)$$

is a refinement, and show that there is a contradiction in all of those cases. Since every possible tuple $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ has

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

upper bounded by at least one of the examined tuples we will see that only the most uniform case is possible.

Note that the only two multi-sets which have $\left[3, 2^{\frac{m-3}{2}}\right]$ as a refinement are $\left[4, 2^{\frac{m-5}{2}}, 1\right]$ and $\left[3^2, 2^{\frac{m-7}{2}}, 1\right]$. Letting either be \mathcal{G}_1 and keeping the other three multi-sets uniform, we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and see there is a contradiction when $m > 13$.

The only multi-set which has $\left[2^{\frac{m-3}{2}}, 1^3\right]$ as a refinement is $\left[3, 2^{\frac{m-7}{2}}, 1^4\right]$. Letting this be \mathcal{G}_2 and keeping the other three multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and have a contradiction whenever $m > 11$.

The only two multi-sets which have $\left[3, 2^{\frac{n-4}{2}}, 1\right]$ as a refinement are $\left[4, 2^{\frac{n-6}{2}}, 1^2\right]$ and $\left[3^2, 2^{\frac{n-8}{2}}, 1^2\right]$. Letting either be \mathcal{H}_1 while keeping the other multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and get a contradiction whenever $m > 12$.

Finally the only multi-set which has $\left[2^{\frac{n-2}{2}}, 1^2\right]$ as a refinement is $\left[3, 2^{\frac{n-6}{2}}, 1^3\right]$. Letting it be \mathcal{H}_2 while keeping the other multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and get a contradiction whenever $m > 12$.

An exhaust over all possibilities when $13 \geq m \geq n \geq 3$ reveals no examples of multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 which satisfy the stated properties.

Finally, when $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are as uniform as possible we have that

$$\begin{aligned} \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] &= 2 + \binom{n-4}{2} \binom{m-3}{2} + \binom{n-2}{2} \binom{m-3}{2} \\ &= \binom{n}{2} \binom{m-3}{2} + \binom{n-2}{2} \binom{m+3}{2} - m - \frac{3n}{2} + 8. \end{aligned}$$

This is equal to $(k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$ if and only if

$$d = m + \frac{3n}{2} - 8.$$

However when $m \geq 5$ this cannot occur since the right side will always be less than d . □

Lemma V.31. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. If $k = \frac{m}{2}$ and $\ell = \frac{n}{2}$ then one of the following occurs:*

1. $\mathcal{G}_1 = [3^2, 1^2]$, $\mathcal{G}_2 = [2^3, 1^2]$, $\mathcal{H}_1 = [3, 1]$, $\mathcal{H}_2 = [2, 1^2]$;
2. $\mathcal{G}_1 = \mathcal{H}_1 = [4, 1^2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^2]$;
3. $\mathcal{G}_1 = \mathcal{H}_1 = [3, 2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^2]$;
4. $\mathcal{G}_1 = \mathcal{H}_1 = [3^2, 1^2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^3, 1^2]$.

These correspond to cases 4, 5, 14, and 16 of the list \mathcal{R}_0 .

Proof. We proceed in the same way as the previous proofs. We know from Lemma V.9 that the sum

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

is maximized when the multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are uniform. However when \mathcal{H}_1 is uniform it is equal to $[2^{\frac{n}{2}}]$ which by Lemma II.20 means $G(X)$ is equivalent to a square of a smaller degree polynomial, which contradicts the assumptions. However, there is a unique element $[3, 2^{\frac{n-4}{2}}, 1]$ in $\mathcal{P}_{n,\ell}$ such that for all $C \in \mathcal{P}_{n,\ell}$ which are not uniform,

$$[3, 2^{\frac{n-4}{2}}, 1] \geq C.$$

This is true because it is the unique element whose refinement is the maximal element.

Therefore, for any non-uniform $C \in \mathcal{P}_{n,\ell}$ we have that

$$\sum_{\beta \in [3, 2^{\frac{n-4}{2}}, 1]} \sum_{\alpha \in \mathcal{G}_1} [\min(\alpha, \beta) - 1] \geq \sum_{\beta \in C} \sum_{\alpha \in \mathcal{G}_1} [\min(\alpha, \beta) - 1].$$

Likewise, the most uniform that \mathcal{G}_1 can be is $\left[3, 2^{\frac{m-4}{2}}, 1\right]$.

So the most uniform the multi-sets can be is

$$\mathcal{G}_1 = \left[3, 2^{\frac{m-3}{2}}\right], \mathcal{G}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right], \mathcal{H}_1 = \left[3, 2^{\frac{n-4}{2}}, 1\right], \mathcal{H}_2 = \left[2^{\frac{m-2}{2}}, 1^2\right].$$

We will have a contradiction with Lemma V.4 whenever

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

However, we do not have the desired contradiction because

$$\begin{aligned} \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] &< (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1 \\ \left(\frac{n-4}{2}\right) \left(\frac{m-2}{2}\right) + \left(2 + \frac{m-4}{2}\right) + \left(\frac{m-2}{2}\right) \left(\frac{n-2}{2}\right) &< \\ &< \left(\frac{m-2}{2}\right) \binom{n}{2} + \left(\frac{n-2}{2}\right) \binom{m}{2} - d + 1 \\ d + 2 &< \frac{m}{2} + \frac{n}{2} \end{aligned}$$

Thus there is not necessarily a contradiction. In particular, when $m = n = d$ the inequality does not hold. However, we claim that for $m > 8$ there are no other possible multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1,$ and \mathcal{H}_2 which do not have a contradiction. We will examine every tuple for which

$$\left(\left[3, 2^{\frac{m-4}{2}}, 1\right], \left[2^{\frac{m-2}{2}}, 1^2\right], \left[3, 2^{\frac{n-3}{2}}\right], \left[2^{\frac{m-3}{2}}, 1^3\right]\right)$$

is a refinement, and show that there is a contradiction in all of those cases. Since every possible tuple $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ has

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

upper bounded by at least one of the examined tuples we will see that only the most uniform case is possible.

Note that the only two multi-sets which have $\left[3, 2^{\frac{m-4}{2}}, 1\right]$ as a refinement are $\left[4, 2^{\frac{m-6}{2}}, 1^2\right]$ and $\left[3^2, 2^{\frac{m-8}{2}}, 1^2\right]$. Letting either be \mathcal{G}_1 and keeping the other three multi-sets uniform, we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and see there is a contradiction when $m > 8$.

The only multi-set which has $\left[2^{\frac{m-2}{2}}, 1^2\right]$ as a refinement is $\left[3, 2^{\frac{m-6}{2}}, 1^3\right]$. Letting this be \mathcal{G}_2 and keeping the other three multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and have a contradiction whenever $m > 6$.

The only two multi-sets which have $\left[3, 2^{\frac{n-4}{2}}, 1\right]$ as a refinement are $\left[4, 2^{\frac{n-6}{2}}, 1^2\right]$ and $\left[3^2, 2^{\frac{n-8}{2}}, 1^2\right]$. Letting either be \mathcal{H}_1 while keeping the other multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and get a contradiction whenever $m > 8$.

Finally the only multi-set which has $\left[2^{\frac{n-2}{2}}, 1^2\right]$ as a refinement is $\left[3, 2^{\frac{n-6}{2}}, 1^3\right]$. Letting it be \mathcal{H}_2 while keeping the other multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and get a contradiction whenever $m > 6$.

An exhaust over all possibilities when $8 \geq m \geq n \geq 3$ reveals the following examples of multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 which satisfy the stated properties:

- $\mathcal{G}_1 = [3^2, 1^2]$, $\mathcal{G}_2 = [2^3, 1^2]$, $\mathcal{H}_1 = [3, 1]$, $\mathcal{H}_2 = [2, 1^2]$;

- $\mathcal{G}_1 = \mathcal{H}_1 = [4, 1^2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^2]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [3, 2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^2]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [3^2, 1^2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^3, 1^2]$.

Finally, when $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are as uniform as possible we have that

$$\begin{aligned} \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] &= 2 + \binom{n-4}{2} \binom{m-4}{2} + \binom{n-2}{2} \binom{m-2}{2} \\ &= \binom{n}{2} \binom{m-2}{2} + \binom{n-2}{2} \binom{m}{2} - m - n + 7. \end{aligned}$$

This is equal to $(k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$ if and only if

$$d = m + n - 7.$$

However when $m \geq 8$ this cannot occur since the right side will always be less than d . □

Lemma V.32. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. It cannot be that $k = \frac{m}{2}$ and $\ell = \frac{n+2}{2}$.*

Proof. We proceed in the same way as the previous proofs. We know from Lemma V.9 that the sum

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

is maximized when the multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are uniform. However when \mathcal{H}_2 is uniform it is equal to $\lfloor 2^{\frac{n}{2}} \rfloor$ which by Lemma II.20 means $G(X)$ is equivalent to a square of a smaller degree polynomial, which contradicts the assumptions. However, there is a unique element $\left[3, 2^{\frac{n-4}{2}}, 1\right]$ in $\mathcal{P}_{n,\ell}$ such that for all $C \in \mathcal{P}_{n,\ell}$ which are not uniform,

$$\left[3, 2^{\frac{n-4}{2}}, 1\right] \geq C.$$

This is true because it is the unique element whose refinement is the maximal element.

Therefore, for any non-uniform $C \in \mathcal{P}_{n,\ell}$ we have that

$$\sum_{\beta \in \left[3, 2^{\frac{n-4}{2}}, 1\right]} \sum_{\alpha \in \mathcal{G}_1} [\min(\alpha, \beta) - 1] \geq \sum_{\beta \in C} \sum_{\alpha \in \mathcal{G}_1} [\min(\alpha, \beta) - 1].$$

Likewise, the most uniform that \mathcal{G}_1 can be is $\left[3, 2^{\frac{m-4}{2}}, 1\right]$.

So the most uniform the multi-sets can be is

$$\mathcal{G}_1 = \left[3, 2^{\frac{m-3}{2}}\right], \mathcal{G}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right], \mathcal{H}_1 = \left[2^{\frac{n-2}{2}}, 1^2\right], \mathcal{H}_2 = \left[3, 2^{\frac{m-4}{2}}, 1\right].$$

We will have a contradiction with Lemma V.4 whenever

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

However, we do not have the desired contradiction because

$$\begin{aligned} \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] &< (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1 \\ 2 \binom{n-2}{2} \binom{m-2}{2} &< \binom{m-2}{2} \binom{n-2}{2} + \binom{n}{2} \binom{m}{2} - d + 1 \\ d &< \frac{m}{2} + \frac{n}{2} \end{aligned}$$

Thus there is not necessarily a contradiction. In particular, when $m = n = d$ the inequality does not hold. However, we claim that for $m > 8$ there are no other possible multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 which do not have a contradiction. We will examine every tuple for which

$$\left(\left[3, 2^{\frac{m-4}{2}}, 1\right], \left[2^{\frac{m-2}{2}}, 1^2\right], \left[2^{\frac{m-3}{2}}, 1^3\right], \left[3, 2^{\frac{n-3}{2}}\right] \right)$$

is a refinement, and show that there is a contradiction in all of those cases. Since every possible tuple $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ has

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

upper bounded by at least one of the examined tuples we will see that only the most uniform case is possible.

Note that the only two multi-sets which have $\left[3, 2^{\frac{m-4}{2}}, 1\right]$ as a refinement are $\left[4, 2^{\frac{m-6}{2}}, 1^2\right]$ and $\left[3^2, 2^{\frac{m-8}{2}}, 1^2\right]$. Letting either be \mathcal{G}_1 and keeping the other three multi-sets uniform, we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and see there is a contradiction when $m > 2$, which is always.

The only multi-set which has $\left[2^{\frac{m-2}{2}}, 1^2\right]$ as a refinement is $\left[3, 2^{\frac{m-6}{2}}, 1^3\right]$. Letting this be \mathcal{G}_2 and keeping the other three multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and have a contradiction whenever $m > 4$.

The only two multi-sets which have $\left[3, 2^{\frac{n-4}{2}}, 1\right]$ as a refinement are $\left[4, 2^{\frac{n-6}{2}}, 1^2\right]$ and $\left[3^2, 2^{\frac{n-8}{2}}, 1^2\right]$. Letting either be \mathcal{H}_2 while keeping the other multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and get a contradiction whenever $m > 2$, which is always.

Finally the only multi-set which has $\left[2^{\frac{n-2}{2}}, 1^2\right]$ as a refinement is $\left[3, 2^{\frac{n-6}{2}}, 1^3\right]$. Letting it be \mathcal{H}_1 while keeping the other multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and get a contradiction whenever $m > 4$.

An exhaust over all possibilities when $4 \geq m \geq n \geq 3$ reveals no possible multi-sets that satisfy the equality in Lemma II.9.

Finally, when $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are as uniform as possible we have that

$$\begin{aligned} \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] &= \binom{n-2}{2} \binom{m-4}{2} + \binom{n-4}{2} \binom{m-2}{2} \\ &= \binom{n-2}{2} \binom{m-2}{2} + \binom{n}{2} \binom{m}{2} - m - n + 3. \end{aligned}$$

This is equal to $(k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$ if and only if

$$d = m + n - 3.$$

However when $m \geq 4$ this cannot occur since the right side will always be less than d . □

Lemma V.33. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. If $k = \frac{m+1}{2}$ and $\ell = \frac{n+1}{2}$ then the multi-sets are in one of the following infinite families or sporadic cases. The infinite families are:*

1. $\mathcal{G}_1 = \mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1\right]$, $\mathcal{H}_1 = \mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right]$, with $(m, n) = 1$;
2. $\mathcal{G}_1 = \left[4, 2^{\frac{m-7}{2}}, 1^3\right]$, $\mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1\right]$, $\mathcal{H}_1 = \mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right]$, with $n|m$;
3. $\mathcal{G}_1 = \left[2^{\frac{m-1}{2}}, 1\right]$, $\mathcal{G}_2 = \left[4, 2^{\frac{m-7}{2}}, 1^3\right]$, $\mathcal{H}_1 = \mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right]$, with $n|m$;
4. $\mathcal{G}_1 = \mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1\right]$, $\mathcal{H}_1 = \left[4, 2^{\frac{n-7}{2}}, 1^3\right]$, $\mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right]$, with $m = n$;
5. $\mathcal{G}_1 = \mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1\right]$, $\mathcal{H}_1 = \left[2^{\frac{n-1}{2}}, 1\right]$, $\mathcal{H}_2 = \left[4, 2^{\frac{n-7}{2}}, 1^3\right]$, with $m = n$;
6. $\mathcal{G}_1 = \left[3, 2^{\frac{m-5}{2}}, 1^2\right]$, $\mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1\right]$, $\mathcal{H}_1 = \mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right]$, with $n|m$;
7. $\mathcal{G}_1 = \left[2^{\frac{m-1}{2}}, 1\right]$, $\mathcal{G}_2 = \left[3, 2^{\frac{m-5}{2}}, 1^2\right]$, $\mathcal{H}_1 = \mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right]$, with $n|m$;
8. $\mathcal{G}_1 = \mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1\right]$, $\mathcal{H}_1 = \left[3, 2^{\frac{n-5}{2}}, 1^2\right]$, $\mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right]$, with $m = n$;
9. $\mathcal{G}_1 = \mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1\right]$, $\mathcal{H}_1 = \left[2^{\frac{n-1}{2}}, 1\right]$, $\mathcal{H}_2 = \left[3, 2^{\frac{n-5}{2}}, 1^2\right]$, with $m = n$.

The sporadic examples are:

1. $\mathcal{G}_1 = \mathcal{H}_1 = [2^4, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [3^2, 1^3]$;
2. $\mathcal{G}_1 = \mathcal{H}_1 = [3^2, 1^3]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^4, 1]$;
3. $\mathcal{G}_1 = \mathcal{H}_1 = [2^3, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [3, 2, 1^2]$;
4. $\mathcal{G}_1 = \mathcal{H}_1 = [3, 2, 1^2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^3, 1]$;
5. $\mathcal{G}_1 = \mathcal{H}_1 = [2^3, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [4, 1^3]$;
6. $\mathcal{G}_1 = \mathcal{H}_1 = [4, 1^3]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^3, 1]$;
7. $\mathcal{G}_1 = \mathcal{H}_1 = \mathcal{G}_2 = \mathcal{H}_2 = [3, 1^2]$;

The infinite families correspond to the case $(T_m(X), T_n(Y))$, and cases 2 and 4 in the list \mathcal{S}_1 . The sporadic examples correspond to cases 1, 6, 7, and 18 in the list \mathcal{R}_0 .

Proof. We proceed in the same way as the previous proofs. We know from Lemma V.9 that the sum

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

is maximized when the multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are uniform. The most uniform the multi-sets can be is

$$\mathcal{G}_1 = \mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1\right], \quad \mathcal{H}_1 = \mathcal{H}_2 = \left[2^{\frac{n-3}{2}}, 1\right].$$

We will have a contradiction with Lemma V.4 whenever

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

However, we do not have the desired contradiction because

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

$$2 \binom{n-1}{2} \binom{m-1}{2} < 2 \binom{m-1}{2} \binom{n-1}{2} - d + 1$$

$$d < 1.$$

Thus there is not necessarily a contradiction. In particular, when $d \geq 1$ the inequality does not hold (which is always). However, we claim that there are only eighteen other possible tuples of multi-sets $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ which do not necessarily have a contradiction. We will examine every tuple for which

$$\left(\left[3, 2^{\frac{m-3}{2}} \right], \left[2^{\frac{m-3}{2}}, 1^3 \right], \left[2^{\frac{n-1}{2}}, 1 \right], \left[2^{\frac{n-1}{2}}, 1 \right] \right)$$

is three refinements of the tuple and show that there is a contradiction in all of those cases. Since every possible tuple which is does not have the uniform tuple as a refinement has $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ has

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

upper bounded by at least one of the examined tuples we will see that only the most uniform case or a tuple which has it as one or two refinements is possible.

We first proceed by examining all multi-sets such that three refinements of the multi-set are equal to one of the uniform multi-sets. Afterwards, we'll examine the cases where we replace two uniform sets by non-uniform sets.

Note that the only three multi-sets which have $\left[2^{\frac{m-1}{2}}, 1 \right]$ as three refinements are $\left[5, 2^{\frac{m-9}{2}}, 1^4 \right]$, $\left[4, 3, 2^{\frac{m-11}{2}}, 1^4 \right]$, and $\left[3^3, 2^{\frac{m-13}{2}}, 1^4 \right]$. Letting any of these be \mathcal{G}_1 or \mathcal{G}_2 while keeping the other three multi-sets uniform, we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and see there is a contradiction whenever $\frac{1}{2} < \frac{n}{2}$ —which is always.

Likewise, the only three multi-sets which have $\left[2^{\frac{n-1}{2}}, 1 \right]$ as three refinements are $\left[5, 2^{\frac{m-9}{2}}, 1^4 \right]$, $\left[4, 3, 2^{\frac{m-11}{2}}, 1^4 \right]$, and $\left[3^3, 2^{\frac{m-13}{2}}, 1^4 \right]$. Letting any of these be \mathcal{H}_1 or \mathcal{H}_2 while keeping the other three multi-sets uniform, we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and see there is again a contradiction whenever $\frac{1}{2} < \frac{m}{2}$, which is still always.

We now analyze the case where one multi-set has the uniform case as a refinement of a refinement, one other multi-set has the uniform case as a refinement, and the other two multi-sets are uniform.

The only two multi-sets which have $\left[2^{\frac{n-1}{2}}, 1\right]$ as a refinement of a refinement are $\left[4, 2^{\frac{n-7}{2}}, 1^3\right]$ and $\left[3^2, 2^{\frac{n-9}{2}}, 1^3\right]$. Likewise the only two multi-sets which have $\left[2^{\frac{m-1}{2}}, 1\right]$ as a refinement of a refinement are $\left[4, 2^{\frac{m-7}{2}}, 1^3\right]$ and $\left[3^2, 2^{\frac{m-9}{2}}, 1^3\right]$. Finally, the only multi-set which has $\left[2^{\frac{n-1}{2}}, 1\right]$ as a refinement is $\left[3, 2^{\frac{n-5}{2}}, 1^2\right]$, and the only multi-set which has $\left[2^{\frac{m-1}{2}}, 1\right]$ as a refinement is $\left[3, 2^{\frac{m-5}{2}}, 1^2\right]$.

If \mathcal{G}_1 is either $\left[4, 2^{\frac{m-7}{2}}, 1^3\right]$ and $\left[3^2, 2^{\frac{m-9}{2}}, 1^3\right]$, with two of the other multi-sets uniform and the fourth the unique multi-set whose refinement is uniform then for $m > 13$ there is necessarily a contradiction. By symmetry of the uniform cases, it is clear that this holds for any case where one multi-set has the uniform case as a refinement of a refinement, one other multi-set has the uniform case as a refinement, and the other two multi-sets are uniform.

We now examine when we fix one of the multi-sets as uniform, and allow three of them to be such that their refinements are uniform.

Since the uniform case is symmetric, there is only one case to check. It is clear if three of the multi-sets are the unique option which has the uniform multi-set as its refinement, and the fourth is uniform then there is a contradiction whenever $m > 6$.

An exhaust over all possibilities when $13 \geq m \geq n \geq 3$ reveals the following examples of multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 which satisfy the stated properties and are not in one of the infinite families described below:

- $\mathcal{G}_1 = \mathcal{H}_1 = [2^4, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [3^2, 1^3]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [3^2, 1^3]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^4, 1]$;

- $\mathcal{G}_1 = \mathcal{H}_1 = [2^3, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [3, 2, 1^2]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [3, 2, 1^2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^3, 1]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [2^3, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [4, 1^3]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [4, 1^3]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^3, 1]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = \mathcal{G}_2 = \mathcal{H}_2 = [3, 1^2]$;

We now need to examine when $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ is uniform, has a refinement which is uniform, or has a refinement of a refinement which is uniform.

When $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are all uniform the equality

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

will hold whenever $d = 1$. Therefore, these are possible multi-sets whenever $(m, n) = 1$.

When \mathcal{G}_1 or \mathcal{G}_2 is $\left[3, 2^{\frac{m-5}{2}}, 1^2\right]$ and the other three multi-sets are uniform we have the equality

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

will hold whenever $n = d$, which means $n|m$.

Likewise (by symmetry), whenever \mathcal{H}_1 or \mathcal{H}_2 is $\left[3, 2^{\frac{n-5}{2}}, 1^2\right]$ and the other three multi-sets are uniform we have the equality

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

will hold whenever $m = d$, which means $m|n$. However since $m \geq n$ by assumption, this requires $m = n$.

Finally we examine the tuples of multi-sets which are two refinements from uniform. If \mathcal{G}_1 or \mathcal{G}_2 is $\left[4, 2^{\frac{m-7}{2}}, 1^3\right]$ and the other three multi-sets are uniform then the equality

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

will hold whenever $n = d$, which means $n|m$.

Likewise (by symmetry), whenever \mathcal{H}_1 or \mathcal{H}_2 is $\left[4, 2^{\frac{n-7}{2}}, 1^3\right]$ and the other three multi-sets are uniform then the equality

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

will hold whenever $m = d$, which means $m|n$, and hence $m = n$.

If \mathcal{G}_1 or \mathcal{G}_2 is $\left[3^2, 2^{\frac{m-9}{2}}, 1^3\right]$ and the other three multi-sets are uniform, then the equality

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

will not hold whenever $n > 2$. However, n is always at least 3 under our assumptions.

Likewise, If \mathcal{H}_1 or \mathcal{H}_2 is $\left[3^2, 2^{\frac{n-9}{2}}, 1^3\right]$ and the other three multi-sets are uniform, then the equality

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

will not hold whenever $m > 2$. However, m is always at least 3 under our assumptions.

If both \mathcal{G}_1 and \mathcal{G}_2 are $\left[3, 2^{\frac{m-5}{2}}, 1^2\right]$ while \mathcal{H}_1 and \mathcal{H}_2 are uniform, then the equality

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

will not hold whenever $n > 2$. However, n is always at least 3 under our assumptions.

Likewise, if both \mathcal{H}_1 and \mathcal{H}_2 are $\left[3, 2^{\frac{n-5}{2}}, 1^2\right]$ while \mathcal{G}_1 and \mathcal{G}_2 are uniform, then the equality

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

will not hold whenever $m > 2$. However, m is always at least 3 under our assumptions.

Finally, if any two multi-sets are such that their refinements are uniform, and the other two multi-sets are uniform, and if $m > 7$ then the equality

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

will not hold. □

Lemma V.34. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. If $k = \frac{m-1}{2}$ and $\ell = \frac{n-1}{2}$ then one of the following occurs:*

1. $\mathcal{G}_1 = [4, 1]$, $\mathcal{G}_2 = [2, 1^3]$, $\mathcal{H}_1 = [3, 2]$, $\mathcal{H}_2 = [2, 1^3]$;
2. $\mathcal{G}_1 = [3, 2]$, $\mathcal{G}_2 = [2, 1^3]$, $\mathcal{H}_1 = [4, 1]$, $\mathcal{H}_2 = [2, 1^3]$;
3. $\mathcal{G}_1 = \mathcal{H}_1 = [4, 2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^3]$;
4. $\mathcal{G}_1 = \mathcal{H}_1 = [3^2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [3, 1^4]$;
5. $\mathcal{G}_1 = \mathcal{H}_1 = [3, 2^2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^3]$.

These correspond to cases 2, 8, 9, and 11 in the list \mathcal{R}_0 .

Proof. We proceed in the same way as the previous proofs. We know from Lemma V.9 that the sum

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

is maximized when the multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are uniform. The most uniform the multi-sets can be is

$$\mathcal{G}_1 = \left[3, 2^{\frac{m-3}{2}}\right], \mathcal{G}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right], \mathcal{H}_1 = \left[3, 2^{\frac{n-3}{2}}\right], \mathcal{H}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right].$$

We will have a contradiction with Lemma V.4 whenever

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

However, we do not have the desired contradiction because

$$\begin{aligned} & \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1 \\ & \left(\frac{n-3}{2}\right) \left(\frac{m-1}{2}\right) + \left(2 + \frac{m-3}{2}\right) + \left(\frac{m-3}{2}\right) \left(\frac{n-3}{2}\right) < \\ & < \left(\frac{m-3}{2}\right) \left(\frac{n+1}{2}\right) + \left(\frac{n-3}{2}\right) \left(\frac{m+1}{2}\right) - d + 1 \\ & d + 1 < \frac{m}{2} + \frac{n}{2} - 3 \\ & d + 4 < \frac{m+n}{2}. \end{aligned}$$

Thus there is not necessarily a contradiction. In particular, when $m = n = d$ the inequality does not hold. However, we claim that for $m > 11$ there are no other possible multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 which do not have a contradiction. We will examine every tuple for which

$$\left(\left[3, 2^{\frac{m-3}{2}}\right], \left[2^{\frac{m-2}{2}}, 1^2\right], \left[3, 2^{\frac{n-3}{2}}\right], \left[2^{\frac{n-3}{2}}, 1^3\right]\right)$$

is a refinement, and show that there is a contradiction in all of those cases. Since every possible tuple $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ has

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

upper bounded by at least one of the examined tuples we will see that only the most uniform case is possible.

Note that the only two multi-sets which have $\left[3, 2^{\frac{m-3}{2}}\right]$ as a refinement are $\left[4, 2^{\frac{m-5}{2}}, 1\right]$ and $\left[3^2, 2^{\frac{m-7}{2}}, 1\right]$. Letting either be \mathcal{G}_1 and keeping the other three multi-sets uniform, we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and see there is a contradiction when $m > 11$.

The only multi-set which has $\left[2^{\frac{m-3}{2}}, 1^3\right]$ as a refinement is $\left[3, 2^{\frac{m-7}{2}}, 1^4\right]$. Letting this be \mathcal{G}_2 and keeping the other three multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and have a contradiction whenever $m > 11$.

The only two multi-sets which have $\left[3, 2^{\frac{n-3}{2}}\right]$ as a refinement are $\left[4, 2^{\frac{n-5}{2}}, 1\right]$ and $\left[3^2, 2^{\frac{n-7}{2}}, 1\right]$. Letting either be \mathcal{H}_1 while keeping the other multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and get a contradiction whenever $m > 11$.

Finally the only multi-set which has $\left[2^{\frac{n-3}{2}}, 1^3\right]$ as a refinement is $\left[3, 2^{\frac{n-7}{2}}, 1^4\right]$. Letting it be \mathcal{H}_2 while keeping the other multi-sets as uniform as possible we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and get a contradiction whenever $m > 11$.

An exhaust over all possibilities when $11 \geq m \geq n \geq 3$ reveals the following examples of multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 which satisfy the stated properties:

- $\mathcal{G}_1 = [4, 1]$, $\mathcal{G}_2 = [2, 1^3]$, $\mathcal{H}_1 = [3, 2]$, $\mathcal{H}_2 = [2, 1^3]$;

- $\mathcal{G}_1 = [3, 2]$, $\mathcal{G}_2 = [2, 1^3]$, $\mathcal{H}_1 = [4, 1]$, $\mathcal{H}_2 = [2, 1^3]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [4, 2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^3]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [3^2, 1]$, $\mathcal{G}_2 = \mathcal{H}_2 = [3, 1^4]$;
- $\mathcal{G}_1 = \mathcal{H}_1 = [3, 2^2]$, $\mathcal{G}_2 = \mathcal{H}_2 = [2^2, 1^3]$.

Finally, when $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are as uniform as possible we have that

$$\begin{aligned} \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] &= 2 + 2 \binom{n-3}{2} \binom{m-3}{2} \\ &= \binom{n+1}{2} \binom{m-3}{2} + \binom{n-3}{2} \binom{m+1}{2} - m - n + 8. \end{aligned}$$

This is equal to $(k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$ if and only if

$$d = m + n - 8.$$

However when $m \geq 9$ this cannot occur since the right side will always be less than d . □

Lemma V.35. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. If $k = \frac{m-1}{2}$ and $\ell = \frac{n+1}{2}$ then one of the following infinite families occurs:*

1. $\mathcal{G}_1 = \left[3, 2^{\frac{m-3}{2}}\right]$, $\mathcal{G}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right]$, $\mathcal{H}_1 = \mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right]$, with $n|m$, or
2. $\mathcal{G}_1 = \left[4, 2^{\frac{m-5}{2}}, 1\right]$, $\mathcal{G}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right]$, $\mathcal{H}_1 = \mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right]$, with $n|m$.

These correspond to the infinite families 1, and 3 in the list \mathcal{S}_1 .

Proof. We proceed in the same way as the previous proofs. We know from Lemma V.9 that the sum

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

is maximized when the multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are uniform. The most uniform the multi-sets can be is

$$\mathcal{G}_1 = \left[3, 2^{\frac{m-3}{2}}\right], \mathcal{G}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right], \mathcal{H}_1 = \mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right].$$

We will have a contradiction with Lemma V.4 whenever

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

However, we do not have the desired contradiction because

$$\begin{aligned} \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] &< (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1 \\ &= \binom{n-1}{2} \binom{m-1}{2} + \binom{m-3}{2} \binom{n-1}{2} < \\ &< \binom{m-3}{2} \binom{n-1}{2} + \binom{n-1}{2} \binom{m+1}{2} - d + 1 \\ &= d - \frac{1}{2} < \frac{n}{2}. \end{aligned}$$

Thus there is not necessarily a contradiction. In particular, when $n = d$ the inequality does not hold. However, we claim that for $m > 5$ there are only five other possible tuples of multi-sets $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ which do not have a contradiction. We will examine every tuple for which

$$\left(\left[3, 2^{\frac{m-3}{2}}\right], \left[2^{\frac{m-3}{2}}, 1^3\right], \left[2^{\frac{n-1}{2}}, 1\right], \left[2^{\frac{n-1}{2}}, 1\right] \right)$$

is a refinement of a refinement, and show that there is a contradiction in all of those cases. Since every possible tuple which is does not have the uniform tuple as a refinement has $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ has

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

upper bounded by at least one of the examined tuples we will see that only the most uniform case or a tuple which has it as a refinement is possible.

We first proceed by examining all multi-sets such that two refinements of the multi-set are equal to one of the uniform multi-sets. Afterwards, we'll examine the cases where we replace two uniform sets by non-uniform sets.

Note that the only three multi-sets which have $\left[3, 2^{\frac{m-3}{2}}\right]$ as a refinement of a refinement are $\left[5, 2^{\frac{m-7}{2}}, 1^2\right]$, $\left[4, 3, 2^{\frac{m-9}{2}}, 1^2\right]$, and $\left[3^3, 2^{\frac{m-11}{2}}, 1^2\right]$. Letting any of these be \mathcal{G}_1 and keeping the other three multi-sets uniform, we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and see there is a contradiction whenever $\frac{1}{2} < \frac{n}{2}$ —which is always.

The only two multi-sets which have $\left[2^{\frac{m-3}{2}}, 1^3\right]$ as a refinement of a refinement are $\left[4, 2^{\frac{m-9}{2}}, 1^5\right]$, and $\left[3^2, 2^{\frac{m-11}{2}}, 1^5\right]$. Letting either be \mathcal{G}_2 while keeping the other three multi-sets uniform, we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and see there is again a contradiction whenever $\frac{1}{2} < \frac{n}{2}$, which is still always.

The only two multi-sets which have $\left[2^{\frac{n-1}{2}}, 1\right]$ as a refinement of a refinement are $\left[4, 2^{\frac{n-7}{2}}, 1^3\right]$ and $\left[3^2, 2^{\frac{n-9}{2}}, 1^3\right]$. Plugging in either for \mathcal{H}_1 or \mathcal{H}_2 while keeping the other multi-sets uniform arrives at a contradiction whenever $m > 5$.

We now examine when we fix two of the multi-sets as uniform, and allow two of them to be such that their refinements are uniform.

The only two multi-sets which have $\left[3, 2^{\frac{m-3}{2}}\right]$ as a refinement are $\left[4, 2^{\frac{m-5}{2}}, 1\right]$, and $\left[3^2, 2^{\frac{m-7}{2}}, 1\right]$. The only multi-set having $\left[2^{\frac{m-3}{2}}, 1^3\right]$ as a refinement is $\left[3, 2^{\frac{m-7}{2}}, 1^4\right]$. Plugging either of the first two in for \mathcal{G}_1 and the latter in for \mathcal{G}_2 while keeping \mathcal{H}_1 and \mathcal{H}_2 uniform we have a contradiction whenever $\frac{1}{2} < \frac{n}{2}$, and again have a contradiction.

If instead we fix \mathcal{G}_2 as uniform and replace either \mathcal{H}_1 or \mathcal{H}_2 with the only multi-set having $\left[2^{\frac{n-1}{2}}, 1\right]$ as a refinement (the unique such multi-set is $\left[3, 2^{\frac{n-5}{2}}, 1^2\right]$) we have a contradiction whenever $m > 5$.

Likewise if we fix \mathcal{G}_1 as uniform, and allow two of the other multi-sets to not be uniform, we have a contradiction whenever $m > 5$.

An exhaust over all possibilities when $5 \geq m \geq n \geq 3$ reveals no examples of multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 which satisfy the stated properties and are not in one of the infinite families described below.

We now need to examine when $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ is uniform, or has a refinement which is uniform.

When $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are all uniform the equality

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

will hold whenever $n = d$. Therefore, these are possible multi-sets whenever $n|m$.

When $\mathcal{G}_1 = \left[4, 2^{\frac{m-5}{2}}, 1\right]$ and $\mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2$ are uniform we again have the equality holding whenever $n|m$.

However, every other tuple $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ with the uniform tuple as its refinement fails to satisfy the equality whenever $m > 5$. □

Lemma V.36. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. If $k = \frac{m}{2}$ and $\ell = \frac{n+1}{2}$ then one of the following infinite families occurs:*

1. $\mathcal{G}_1 = \left[3, 2^{\frac{m-4}{2}}, 1\right]$, $\mathcal{G}_2 = \left[2^{\frac{m-2}{2}}, 1^2\right]$, $\mathcal{H}_1 = \mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right]$, with $n|m$, or
2. $\mathcal{G}_1 = \left[4, 2^{\frac{m-6}{2}}, 1^2\right]$, $\mathcal{G}_2 = \left[2^{\frac{m-2}{2}}, 1^2\right]$, $\mathcal{H}_1 = \mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right]$ with $n|m$.

These correspond to the infinite families 5, and 6 in the list \mathcal{S}_1 .

Proof. We proceed in the same way as the previous proofs. We know from Lemma V.9 that the sum

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

is maximized when the multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1,$ and \mathcal{H}_2 are uniform. However when \mathcal{G}_1 is uniform it is equal to $\lfloor 2^{\frac{m}{2}} \rfloor$ which by Lemma II.20 means $G(X)$ is equivalent to a square of a smaller degree polynomial, which contradicts the assumptions. However, there is a unique element $\left[3, 2^{\frac{m-4}{2}}, 1\right]$ in $\mathcal{P}_{m,k}$ such that for all $C \in \mathcal{P}_{m,k}$ which are not uniform,

$$\left[3, 2^{\frac{m-4}{2}}, 1\right] \geq C.$$

This is true because it is the unique element whose refinement is the maximal element.

Therefore, for any non-uniform $C \in \mathcal{P}_{m,k}$ we have that

$$\sum_{\alpha \in \left[3, 2^{\frac{m-4}{2}}, 1\right]} \sum_{\beta \in \mathcal{H}_1} [\min(\alpha, \beta) - 1] \geq \sum_{\alpha \in C} \sum_{\beta \in \mathcal{H}_1} [\min(\alpha, \beta) - 1].$$

So the most uniform the multi-sets can be is

$$\mathcal{G}_1 = \left[3, 2^{\frac{m-4}{2}}, 1\right], \mathcal{G}_2 = \left[2^{\frac{m-2}{2}}, 1^2\right], \mathcal{H}_1 = \mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right].$$

We will have a contradiction with Lemma V.4 whenever

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

However, we do not have the desired contradiction because

$$\begin{aligned} \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] &< (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1 \\ 2 \binom{n-1}{2} \binom{m-2}{2} &< \binom{m-2}{2} \binom{n-1}{2} + \binom{n-1}{2} \binom{m}{2} - d + 1 \\ d - \frac{1}{2} &< \frac{n}{2}. \end{aligned}$$

Thus there is not necessarily a contradiction. In particular, when $n = d$ the inequality does not hold. However, we claim that for $m > 7$ there are only five other possible tuples of multi-sets $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ which do not have a contradiction. We will examine every tuple for which

$$\left(\left[3, 2^{\frac{m-4}{2}}, 1 \right], \left[2^{\frac{m-2}{2}}, 1^2 \right], \left[2^{\frac{n-1}{2}}, 1 \right], \left[2^{\frac{n-1}{2}}, 1 \right] \right)$$

is a refinement of a refinement, and show that there is a contradiction in all of those cases. Since every possible tuple which is does not have the uniform tuple as a refinement has $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ has

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

upper bounded by at least one of the examined tuples we will see that only the most uniform case or a tuple which has it as a refinement is possible.

We first proceed by examining all multi-sets such that two refinements of the multi-set are equal to one of the uniform multi-sets. Afterwards, we'll examine the cases where we replace two uniform sets by non-uniform sets.

Note that the only three multi-sets which have $\left[3, 2^{\frac{m-4}{2}}, 1 \right]$ as a refinement of a refinement are $\left[5, 2^{\frac{m-8}{2}}, 1^3 \right]$, $\left[4, 3, 2^{\frac{m-10}{2}}, 1^3 \right]$, and $\left[3^3, 2^{\frac{m-12}{2}}, 1^3 \right]$. Letting any of these be \mathcal{G}_1 and keeping the other three multi-sets uniform, we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and see there is a contradiction whenever $\frac{1}{2} < \frac{n}{2}$ —which is always.

The only two multi-sets which have $\left[2^{\frac{m-2}{2}}, 1^2 \right]$ as a refinement of a refinement are $\left[4, 2^{\frac{m-8}{2}}, 1^4 \right]$, and $\left[3^2, 2^{\frac{m-10}{2}}, 1^4 \right]$. Letting either be \mathcal{G}_2 while keeping the other three multi-sets uniform, we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and see there is again a contradiction whenever $\frac{1}{2} < \frac{n}{2}$, which is still always.

The only two multi-sets which have $\left[2^{\frac{n-1}{2}}, 1\right]$ as a refinement of a refinement are $\left[4, 2^{\frac{n-7}{2}}, 1^3\right]$ and $\left[3^2, 2^{\frac{n-9}{2}}, 1^3\right]$. Plugging in either for \mathcal{H}_1 or \mathcal{H}_2 while keeping the other multi-sets uniform arrives at a contradiction whenever $m > 7$.

We now examine when we fix two of the multi-sets as uniform, and allow two of them to be such that their refinements are uniform.

The only two multi-sets which have $\left[3, 2^{\frac{m-4}{2}}, 1\right]$ as a refinement are $\left[4, 2^{\frac{m-6}{2}}, 1^2\right]$, and $\left[3^2, 2^{\frac{m-8}{2}}, 1^2\right]$. The only multi-set having $\left[2^{\frac{m-2}{2}}, 1^2\right]$ as a refinement is

$$\left[3, 2^{\frac{m-6}{2}}, 1^3\right].$$

Plugging either of the first two in for \mathcal{G}_1 and the latter in for \mathcal{G}_2 while keeping \mathcal{H}_1 and \mathcal{H}_2 uniform we have a contradiction whenever $\frac{1}{2} < \frac{n}{2}$, and again have a contradiction.

If instead we fix \mathcal{G}_2 as uniform and replace either \mathcal{H}_1 or \mathcal{H}_2 with the only multi-set having $\left[2^{\frac{n-1}{2}}, 1\right]$ as a refinement (the unique such multi-set is $\left[3, 2^{\frac{n-5}{2}}, 1^2\right]$) we have a contradiction whenever $m > 4$.

Likewise if we fix \mathcal{G}_1 as uniform, and allow two of the other multi-sets to not be uniform, we have a contradiction whenever $m > 4$.

An exhaust over all possibilities when $7 \geq m \geq n \geq 3$ reveals no examples of multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 which satisfy the stated properties and are not in one of the infinite families described below.

We now need to examine when $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ is uniform, or has a refinement which is uniform.

When $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are the stated ones which are “as uniform as possible”, then the equality

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

will hold whenever $n = d$. Therefore, these are possible multi-sets whenever $n|m$.

When $\mathcal{G}_1 = \left[4, 2^{\frac{m-6}{2}}, 1^2\right]$ and $\mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2$ are uniform we again have the equality holding whenever $n|m$.

However, every other tuple $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ with the uniform tuple as its refinement fails to satisfy the equality whenever $m > 4$. \square

Lemma V.37. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1. If $k = \frac{m+1}{2}$ and $\ell = \frac{n+3}{2}$ then one of the following infinite families or sporadic examples occurs. The infinite families:*

1. $\mathcal{G}_1 = \mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1\right]$, $\mathcal{H}_1 = \left[2^{\frac{n-3}{2}}, 1^3\right]$, $\mathcal{H}_2 = \left[4, 2^{\frac{n-5}{2}}, 1\right]$, with $m = n$, or
2. $\mathcal{G}_1 = \mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1\right]$, $\mathcal{H}_1 = \left[2^{\frac{n-3}{2}}, 1^3\right]$, $\mathcal{H}_2 = \left[3, 2^{\frac{n-3}{2}}\right]$, with $m = n$.

The one sporadic example is

$$\mathcal{G}_1 = [2^2, 1], \mathcal{G}_2 = [3, 1^2], \mathcal{H}_1 = [2, 1^3], \mathcal{H}_2 = [3, 2].$$

The infinite families correspond to cases 1 and 3 in the list \mathcal{S}_1 . The sporadic example corresponds to the case 3 in the list \mathcal{R}_0 .

Proof. We proceed in the same way as the previous proofs. We know from Lemma V.9 that the sum

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

is maximized when the multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are uniform. The most uniform the multi-sets can be is

$$\mathcal{G}_1 = \mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1\right], \mathcal{H}_1 = \left[2^{\frac{n-3}{2}}, 1^3\right], \mathcal{H}_2 = \left[3, 2^{\frac{n-3}{2}}\right].$$

We will have a contradiction with Lemma V.4 whenever

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

However, we do not have the desired contradiction because

$$\begin{aligned}
& \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1 \\
& \qquad \left(\frac{n-3}{2} \right) \left(\frac{m-1}{2} \right) + \left(\frac{m-1}{2} \right) \left(\frac{n-1}{2} \right) < \\
& < \left(\frac{m-1}{2} \right) \left(\frac{n-3}{2} \right) + \left(\frac{n+1}{2} \right) \left(\frac{m-1}{2} \right) - d + 1 \\
& \qquad \qquad \qquad d - \frac{1}{2} < \frac{m}{2}.
\end{aligned}$$

Thus there is not necessarily a contradiction. In particular, when $m = d$ the inequality does not hold. However, we claim that for $m > 7$ there are only five other possible tuples of multi-sets $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ which do not have a contradiction. We will examine every tuple for which

$$\left(\left[2^{\frac{m-1}{2}}, 1 \right], \left[2^{\frac{m-1}{2}}, 1 \right], \left[2^{\frac{n-3}{2}}, 1^3 \right], \left[3, 2^{\frac{n-3}{2}} \right] \right)$$

is a refinement of a refinement, and show that there is a contradiction in all of those cases. Since every possible tuple which is does not have the uniform tuple as a refinement has $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ has

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

upper bounded by at least one of the examined tuples we will see that only the most uniform case or a tuple which has it as a refinement is possible.

We first proceed by examining all multi-sets such that two refinements of the multi-set are equal to one of the uniform multi-sets. Afterwards, we'll examine the cases where we replace two uniform sets by non-uniform sets.

Note that the only two multi-sets which have $\left[2^{\frac{m-1}{2}}, 1 \right]$ as a refinement of a refinement are $\left[4, 2^{\frac{m-7}{2}}, 1^3 \right]$, and $\left[3^2, 2^{\frac{m-9}{2}}, 1^3 \right]$. Letting either of these be \mathcal{G}_1 or \mathcal{G}_2 while

keeping the other three multi-sets uniform, we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and see there is a contradiction whenever $m > 5$.

The only two multi-sets which have $\left[2^{\frac{n-3}{2}}, 1^3\right]$ as a refinement of a refinement are $\left[4, 2^{\frac{n-9}{2}}, 1^5\right]$, and $\left[3^2, 2^{\frac{n-11}{2}}, 1^5\right]$. Letting either be \mathcal{H}_1 while keeping the other three multi-sets uniform, we plug into

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

and see there is again a contradiction whenever $\frac{1}{2} < \frac{m}{2}$, which always.

The only three multi-sets which have $\left[3, 2^{\frac{n-3}{2}}\right]$ as a refinement of a refinement are $\left[5, 2^{\frac{n-7}{2}}, 1^2\right]$, $\left[4, 3, 2^{\frac{n-9}{2}}, 1^2\right]$, and $\left[3^3, 2^{\frac{n-11}{2}}, 1^2\right]$. Plugging in any for \mathcal{H}_2 while keeping the other multi-sets uniform arrives at a contradiction whenever $m > 1$, which is always.

We now examine when we fix two of the multi-sets as uniform, and allow two of them to be such that their refinements are uniform.

The only multi-set which has $\left[2^{\frac{m-1}{2}}, 1\right]$ as a refinement is $\left[3, 2^{\frac{m-5}{2}}, 1^2\right]$. Plugging this in for \mathcal{G}_1 and \mathcal{G}_2 while keeping \mathcal{H}_1 and \mathcal{H}_2 uniform we have a contradiction whenever $m > 5$.

There is a unique multi-set $\left[3, 2^{\frac{n-7}{2}}, 1^4\right]$ which has $\left[2^{\frac{n-3}{2}}, 1^3\right]$ as a refinement. The only two multi-sets which have $\left[3, 2^{\frac{n-3}{2}}\right]$ as a refinement are $\left[4, 2^{\frac{n-5}{2}}, 1\right]$ and $\left[3^2, 2^{\frac{n-7}{2}}, 1\right]$. Allowing \mathcal{H}_1 to be $\left[3, 2^{\frac{n-7}{2}}, 1^4\right]$ and \mathcal{H}_2 either of the stated options while keeping \mathcal{G}_1 and \mathcal{G}_2 uniform always produces a contradiction.

Finally, allowing any combination where one of the \mathcal{G}_i is non-uniform and one of the \mathcal{H}_j is non-uniform, while the other two multi-sets are uniform produces a contradiction whenever $m > 7$.

An exhaust over all possibilities when $7 \geq m \geq n \geq 3$ reveals the only example of multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 which satisfy the stated properties and are not in one of the infinite families described below is

$$\mathcal{G}_1 = [2^2, 1], \mathcal{G}_2 = [3, 1^2], \mathcal{H}_1 = [2, 1^3], \mathcal{H}_2 = [3, 2].$$

We now need to examine when $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ is uniform, or has a refinement which is uniform.

When $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are all uniform the equality

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [(\alpha, \beta) - 1] = (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1$$

will hold whenever $m = d$. Therefore, these are possible multi-sets whenever $m|n$.

However, since $m \geq n$, this means that $m = n$.

When $\mathcal{G}_2 = [4, 2^{\frac{n-5}{2}}, 1]$ and $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$ are uniform we again have the equality holding whenever $m = n$.

Every other tuple $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1, \mathcal{H}_2)$ with the uniform tuple as its refinement fails to satisfy the equality whenever $m > 3$. \square

Lemma V.38. *Let $G(X)$ and $H(Y)$ be as in Theorem V.1, then it cannot be that $k = \frac{m+1}{2}$ and $\ell = \frac{n+2}{2}$.*

Proof. We proceed in the same way as the previous proofs. We know from Lemma V.9 that the sum

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1]$$

is maximized when the multi-sets $\mathcal{G}_1, \mathcal{G}_2, \mathcal{H}_1$, and \mathcal{H}_2 are uniform. However when \mathcal{H}_2 is uniform it is equal to $[2^{\frac{n}{2}}]$ which by Lemma II.20 means $G(X)$ is equivalent to a square of a smaller degree polynomial, which contradicts the assumptions. However,

there is a unique element $\left[3, 2^{\frac{n-4}{2}}, 1\right]$ in $\mathcal{P}_{n,\ell}$ such that for all $C \in \mathcal{P}_{n,\ell}$ which are not uniform,

$$\left[3, 2^{\frac{n-4}{2}}, 1\right] \geq C.$$

This is true because it is the unique element whose refinement is the maximal element.

Therefore, for any non-uniform $C \in \mathcal{P}_{n,\ell}$ we have that

$$\sum_{\beta \in \left[3, 2^{\frac{n-4}{2}}, 1\right]} \sum_{\alpha \in \mathcal{G}_1} [\min(\alpha, \beta) - 1] \geq \sum_{\beta \in C} \sum_{\alpha \in \mathcal{G}_1} [\min(\alpha, \beta) - 1].$$

Likewise, the most uniform that \mathcal{G}_1 can be is $\left[3, 2^{\frac{m-4}{2}}, 1\right]$.

So the most uniform the multi-sets can be is

$$\mathcal{G}_1 = \mathcal{G}_2 = \left[2^{\frac{m-1}{2}}, 1\right], \quad \mathcal{H}_1 = \left[2^{\frac{n-2}{2}}, 1^2\right], \quad \mathcal{H}_2 = \left[3, 2^{\frac{m-4}{2}}, 1\right].$$

We will have a contradiction with Lemma V.4 whenever

$$\sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] < (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1.$$

However, we do not have the desired contradiction because

$$\begin{aligned} \sum_{i=1}^2 \sum_{\alpha \in \mathcal{G}_i} \sum_{\beta \in \mathcal{H}_i} [\min(\alpha, \beta) - 1] &< (k-1)(n-\ell) + (\ell-1)(m-k) - d + 1 \\ 2 \binom{\frac{n-2}{2}}{\frac{m-1}{2}} &< \binom{\frac{m-1}{2}}{\frac{n-2}{2}} + \binom{\frac{m-1}{2}}{\frac{n}{2}} - d + 1 \\ d &< \frac{m}{2} + \frac{1}{2}. \end{aligned}$$

Note however that this case is symmetric to the case handled in Lemma V.36. However, since $m > n$ (they cannot be equal since their parities are different) the two infinite families which occur in Lemma V.36 cannot occur here. Therefore the identical analysis and exhaust will reveal no examples of multi-sets which satisfy the stated requirements. \square

5.9 Proof of Theorem V.1

Proof of Theorem V.1. We assume without loss of generality that $m \geq n$ and $|\mathcal{G}_1| \leq |\mathcal{G}_2|$. Let $k = |\mathcal{G}_1|$ and $\ell = |\mathcal{H}_1|$. Every possible pair of (m, n) with $m \geq n \geq 22$ and every possible pair (k, ℓ) with $2 \leq k \leq \frac{m+1}{2}$ and $2 \leq \ell \leq n-1$ is considered in one of Lemmas V.13–V.38, except the cases $k = \frac{m+1}{2}$ with $4 \leq \ell \leq \frac{n}{2}$ and $\frac{m-12}{2} \leq k \leq \frac{m-2}{2}$ with $\ell = \lceil \frac{n}{2} \rceil$. The union of the possibilities from these Lemmas is exactly the possibilities stated. We conclude that the stated possibilities are the only ones which occur. □

CHAPTER VI

Irreducibility of $G(X) - H(Y)$

In the previous three chapters we proved theorems giving lists of pairs of polynomials $(G(X), H(X))$. The theorems show that these lists include all polynomials for which $G(X) - H(Y) = 0$ defines an irreducible genus-zero curve, subject to some additional constraints on G and H . The theorems also show that, for any (G, H) on any of the lists, if $G(X) - H(Y)$ is irreducible then $G(X) = H(Y)$ has genus zero. In this chapter we determine all pairs (G, H) on these lists for which $G(X) - H(Y)$ is irreducible.

6.1 Main Theorems

We first treat the pairs $(G(X), H(Y))$ from Theorem III.1.

Theorem VI.1. *Suppose that the pair $(G(X), H(Y))$ has one of the forms*

1. $((X - x_0)^a F(X)^n, Y^n)$, for any positive, coprime positive integers n and a , any constant x_0 , and any non-zero polynomial $F(X) \in \mathbb{C}[X]$;
2. $((X - x_1)^a (X - x_2)^{n-a} F(X)^n, Y^n)$, for any coprime integers n and $1 \leq a < n$, any constants $x_1 \neq x_2$, and any non-zero polynomial $F(X) \in \mathbb{C}[X]$;

Then $G(X) - H(Y)$ is irreducible.

We next address the polynomials from Theorem IV.4.

Theorem VI.2. *For any coprime integers a and m satisfying $1 \leq a < m$, and any constant $c \in \mathbb{C} \setminus \{0, 1\}$, the polynomial*

$$X^a(X-1)^{m-a} - cY^a(Y-1)^{m-a}$$

is irreducible.

We next address pairs of Chebyshev polynomials; these arose in Theorem V.1.

Theorem VI.3. *The polynomial $T_m(X) - T_n(Y)$ is irreducible if and only if m and n are coprime positive integers.*

The most difficult result in this chapter addresses the infinite families in Theorem IV.2 and Theorem V.1. Excluding pairs of Chebyshev polynomials, these families have the form $(T_n(X), F(Y))$ where $F(Y)$ lies in the set $\mathcal{S}(n)$ defined below.

Definition VI.4. Fix an odd integer $n > 1$. We define $\mathcal{S}(n)$ to be the set of nonconstant polynomials $F(X) \in \mathbb{C}[X]$ such that $n \mid \deg(F)$ and the ramification types of F over $x_1 = 2$ and $x_2 = -2$ are one of the following:

1. $\mathcal{F}_1 = \left[2^{\frac{m-1}{2}}, 1\right]$, $\mathcal{F}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right]$;
2. $\mathcal{F}_1 = \left[2^{\frac{m-2}{2}}, 1^2\right]$, $\mathcal{F}_2 = \left[2^{\frac{m-2}{2}}, 1^2\right]$;
3. $\mathcal{F}_1 = \left[4, 2^{\frac{m-5}{2}}, 1\right]$, $\mathcal{F}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right]$;
4. $\mathcal{F}_1 = \left[4, 2^{\frac{m-7}{2}}, 1^3\right]$, $\mathcal{F}_2 = \left[2^{\frac{m-1}{2}}, 1\right]$;
5. $\mathcal{F}_1 = \left[3, 2^{\frac{m-3}{2}}\right]$, $\mathcal{F}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right]$;
6. $\mathcal{F}_1 = \left[3, 2^{\frac{m-5}{2}}, 1^2\right]$, $\mathcal{F}_2 = \left[2^{\frac{m-1}{2}}, 1\right]$;
7. $\mathcal{F}_1 = \left[4, 2^{\frac{m-6}{2}}, 1^2\right]$, $\mathcal{F}_2 = \left[2^{\frac{m-2}{2}}, 1^2\right]$;
8. $\mathcal{F}_1 = \left[3, 2^{\frac{m-4}{2}}, 1\right]$, $\mathcal{F}_2 = \left[2^{\frac{m-2}{2}}, 1^2\right]$.

Recall that a polynomial $F(X) \in \mathbb{C}[X]$ is called *indecomposable* if $\deg(F) \geq 2$ and F cannot be written as the composition of two smaller degree polynomials.

Theorem VI.5. *Pick any odd $n \geq 3$ and any $G(X) \in \mathbb{C}[X]$ whose degree is a multiple of n . Then the following are equivalent:*

- $G(X)$ lies in $\mathcal{S}(n)$, and $G(X) - T_n(Y)$ is irreducible in $\mathbb{C}[X, Y]$;
- $G = T_k \circ \overline{G}$ where k is an odd positive integer with $(k, n) = 1$ and $\overline{G}(X)$ is an indecomposable polynomial in $\mathcal{S}(n)$.

6.2 Strategy of Proof

Our proofs of Theorems VI.1–VI.5 rely on a result due to Fried (Theorem VI.6). This result implies that if $G(X) - H(Y)$ is reducible then there must exist decompositions $G = G_1 \circ G_2$ and $H = H_1 \circ H_2$ in which G_1 and H_1 satisfy some severe constraints (specifically, they are nonlinear and have the same degrees and the same sets of branch points). For each pair $(G(X), H(Y))$ under consideration, we will determine all pairs of decompositions in which G_1 and H_1 satisfy the constraints mentioned above. It turns out that such decompositions exist if and only if $G(X) - H(Y)$ is reducible.

Our technique for finding all decompositions of $G(X)$ and $H(Y)$ is combinatorial. We use the multiplicativity of ramification indices in towers of field extensions in order to determine the ramification in any of the polynomials G_i or H_i . We find that the polynomials $G(X)$ in Theorems VI.1 and VI.2 are indecomposable, whereas if we write a polynomial $G(X)$ from Theorem VI.5 as $G = A \circ B$ with A, B nonlinear, then $A = T_k \circ \mu$ for some linear $\mu \in \mathbb{C}[X]$.

6.3 Fried's Theorem on Decomposability

Throughout this chapter, the symbol t refers to an element of an extension of \mathbb{C} such that t is transcendental over \mathbb{C} . We will use the following theorem of Fried [13, Proposition 2].

Theorem VI.6 (Fried). *For any $G(X), H(X) \in \mathbb{C}[X] \setminus \mathbb{C}$, there exist $G_1, G_2, H_1, H_2 \in \mathbb{C}[X]$ such that*

$$G = G_1 \circ G_2, \quad H = H_1 \circ H_2,$$

and both of the following hold:

1. all factors of $G(X) - H(Y)$ in $\mathbb{C}[X, Y]$ lie in $\mathbb{C}[G_2(X), H_2(Y)]$; and
2. the splitting fields of $G_1(X) - t$ and $H_1(Y) - t$ over $\mathbb{C}(t)$ are the same.

Proof. See Fried [13, Proposition 2] or Bilu–Tichy [4, Theorem 8.1]. □

Note that reducibility of $G(X) - H(Y)$ is not assumed in the above result; when $G(X) - H(Y)$ is irreducible, we may take $G_1 = H_1 = X$, $G_2 = G$, and $H_2 = H$. Conversely, for ‘most’ choices of G and H , it turns out that any decompositions satisfying the splitting field constraint must have G_1 and H_1 being linear; by our next lemma, this implies that $G(X) - H(Y)$ is irreducible.

Lemma VI.7. *If either of the polynomials G_1 or H_1 in Theorem VI.6 are linear, then $G(X) - H(Y)$ is irreducible.*

Proof. Assume without loss that $G_1(X)$ is linear. If $G(X) - H(Y)$ is reducible, then it has a factor $F(X, Y)$ whose Y -degree lies strictly between 0 and $\deg(H)$. But this contradicts condition 1 of Theorem VI.6. □

6.4 Ramification and Irreducibility Criteria

The splitting field constraint in Theorem VI.6 imposes severe constraints on the polynomials G_1 and H_1 . We exhibit two such constraints in Lemmas VI.9 and VI.10, the proofs of which involve the following well-known property of ramification indices. In this section we assume familiarity with basic concepts of function fields; a convenient reference for this material is Stichtenoth [22].

Lemma VI.8. *Let K_1, K_2 be finite extensions of $\mathbb{C}(t)$ whose compositum is E . Let Q be a place of $K := K_1 \cap K_2$, let P_i be a place of K_i lying over Q , and let e_i denote the ramification index of P_i/Q . Then for each place P of E lying over both P_1 and P_2 , the ramification index of P/Q is $\text{lcm}(e_1, e_2)$.*

Proof. See Müller and Zieve [17, Lemma 3.1] or Stichtenoth [22, Proposition III.8.9].

□

Lemma VI.9. *Let $G_1, H_1 \in \mathbb{C}[X] \setminus \mathbb{C}$, and suppose that $G_1(X) - t$ and $H_1(X) - t$ have the same splitting field over $\mathbb{C}(t)$. Then $G(X)$ and $H(Y)$ have the same branch points.*

Proof. We prove this result by contradiction.

We let Ω_G and Ω_H denote the splitting fields of $G(X) - t$ and $H(X) - t$ over $\mathbb{C}(t)$, respectively. Assume without loss of generality that $G(X)$ has a (finite) branch point α which is not a branch point of $H(Y)$. Then, for any root y of $H(Y) - t$, the extension $\mathbb{C}(y)/\mathbb{C}(t)$ is unramified over the place $t = \alpha$. Since Ω_H is the compositum of all such fields $\mathbb{C}(y)$, it follows by Lemma VI.8 that $\Omega_H/\mathbb{C}(t)$ is unramified over $t = \alpha$. However, since α is a branch point of $G(X)$, the same reasoning implies that $\Omega_G/\mathbb{C}(t)$ is *not* unramified over $t = \alpha$, contradicting our assumption that $\Omega_H = \Omega_G$. □

Lemma VI.10. *Let $G_1, H_1 \in \mathbb{C}[X] \setminus \mathbb{C}$ be such that $G_1(X) - t$ and $H_1(X) - t$ have the same splitting field over $\mathbb{C}(t)$. Then $\deg(G_1) = \deg(H_1)$.*

Proof. Let Ω be the splitting field of $G_1(X) - t$ and $H_1(Y) - t$. Note that for any polynomial $F(X)$ and any extension $\mathbb{C}(x)/\mathbb{C}(t)$ (with $F(x) = t$) there is a unique place of $\mathbb{C}(x)$ lying over $t = \infty$. Therefore, since Ω is the compositum of all extension fields $\mathbb{C}(x)$ with $G_1(x) = t$ we can apply Lemma VI.8 to see that any place in Ω lying over $t = \infty$ has ramification equal to the degree of $G_1(X)$. Since Ω is also the splitting field of $H_1(Y)$ we see that $H_1(Y)$ and $G_1(X)$ must have the same degrees, because the degrees are both equal to the ramification index of points lying over $t = \infty$. \square

Lemma VI.11. *If $G, H \in \mathbb{C}[X] \setminus \mathbb{C}$ have coprime degrees, then $G(X) - H(Y)$ is irreducible.*

Proof. If $G = G_1 \circ G_2$ and $H = H_1 \circ H_2$ such that $G_1(X) - t$ and $H_1(Y) - t$ have the same splitting field over $\mathbb{C}(t)$ then by Lemma VI.10 $\deg(G_1) = \deg(H_1)$. However, since degree multiplies under composition of polynomials, it must be that $\deg(G_1) = \deg(H_1) = 1$. In this case Lemma VI.7 implies that $G(X) - H(Y)$ is irreducible. \square

The results in this section were known previously. Fried used versions of Lemmas VI.9 and VI.10 in several papers, and Lemma VI.11 is due to Ehrenfeucht [8].

6.5 Proof of Theorem VI.1

Proof of Theorem VI.1. In the first case the degrees of $G(X)$ and $H(Y)$ are coprime, so Theorem VI.11 implies that $G(X) - H(Y)$ is irreducible.

Now assume that $(G(X), H(Y))$ comes from the second case of Theorem VI.1. If

$G(X) - H(Y)$ is reducible, then Theorem VI.6 and Lemma VI.7 imply that $G = G_1 \circ G_2$ and $H = H_1 \circ H_2$ with G_1 and H_1 nonlinear polynomials such that $G_1(X) - t$ and $H_1(Y) - t$ have the same splitting field over $\mathbb{C}(t)$. It follows from Lemmas VI.9 and VI.10 that G_1 and H_1 have the same branch points and the same degree. But since zero is the unique finite branch point of $H(Y) = Y^n$, the equation $H = H_1 \circ H_2$ implies that zero is the unique finite branch point of H_1 , so zero is also the unique finite branch point of G_1 . Now Lemma II.14 implies that $G_1(X)$ is equivalent to X^k for some $k > 1$, so the ramification type of G_1 over 0 must be $[k]$. Since $G = G_1 \circ G_2$, it follows that every G -preimage of 0 has ramification index divisible by k , so that k divides $u := a + n \cdot \text{ord}_{X=x_1} F(X)$. But $k := \deg(G_1) = \deg(H_1)$ also divides $\deg(H) = n$, so k divides $\gcd(u, n) = \gcd(a, n) = 1$, a contradiction. Therefore $G(X) - H(Y)$ is irreducible. \square

6.6 Proof of Theorem VI.3

Proof of Theorem VI.3. By Lemma VI.11 we can conclude that $T_m(X) - T_n(Y)$ is irreducible whenever m is coprime to n .

We can also see, by inspection of the functional equation from the definition of $T_m(X)$ (see Definition II.15) that $T_a(X) \circ T_b(X) = T_{ab}(X)$. Therefore, if $\gcd(m, n) = d > 1$ we can decompose our polynomials as $T_m = T_d \circ T_{m/d}$ and $T_n = T_d \circ T_{n/d}$ and see that

$$T_m(X) - T_n(Y) = T_d \circ T_{m/d}(X) - T_d \circ T_{n/d}(Y) = (T_{m/d}(X) - T_{n/d}(Y))F(X, Y).$$

\square

6.7 Proof of Theorem VI.2

Lemma VI.12. *For any coprime integers a and m satisfying $1 \leq a < m$, and any constant $c \in \mathbb{C} \setminus \{0\}$, the polynomial*

$$F(X) := cX^a(X - 1)^{m-a}$$

is indecomposable.

Proof. Assume that the polynomial decomposes as $F = \mu \circ \nu$ for non-linear polynomials $\mu(X)$ and $\nu(X)$. The ramification of $F(X)$ over zero is $[a, m - a]$. Since $F^{-1}(0) = \nu^{-1}(\mu^{-1}(0))$, it follows that $|\mu^{-1}(0)| \leq 2$.

If $|\mu^{-1}(0)| = 1$, then the ramification of $\mu(X)$ over 0 is $[k]$ where $k := \deg(\mu)$. Since ramification is multiplicative under composition, it follows that k divides the ramification index under F of each point in $F^{-1}(0)$, whence $k \mid \gcd(a, m - a) = 1$, a contradiction.

If $|\mu^{-1}(0)| = 2$ then, since also $|F^{-1}(0)| = 2$, it follows that each point in $\mu^{-1}(0)$ has a unique pre-image under $\nu(X)$. Thus, each point in $F^{-1}(0)$ has ramification index $\deg(\nu)$ under ν , whence $\deg(\nu) \mid \gcd(a, m - a) = 1$, a contradiction. \square

Proof of Theorem VI.2. From Lemma VI.12 we know that the polynomials $X^a(X - 1)^{m-a}$ and $cY^a(Y - 1)^{m-a}$ are both indecomposable. Since the polynomials are indecomposable, Theorem VI.6 and Lemma VI.7 imply that

$$X^a(X - 1)^{m-a} - cY^a(Y - 1)^{m-a}$$

is irreducible if

$$X^a(X - 1)^{m-a} - t$$

and

$$cY^a(Y - 1)^{m-a} - t$$

have different splitting fields over $\mathbb{C}(t)$.

We show that the polynomials do not share all their branch points, and so Lemma VI.9 implies they have different splitting fields. Both polynomials have exactly one non-zero finite branch point (by Lemma II.7). Let γ be the non-zero finite branch point of $X^a(X - 1)^{m-a}$. Then it is clear that $c\gamma$ is a finite branch point of $cY^a(Y - 1)^{m-a}$ (by composing with the polynomial cX). Since γ is necessarily non-zero and c is neither zero nor one, the polynomials do not have the same branch points, and so cannot have the same splitting field. \square

6.8 Decompositions of Polynomials from Theorem VI.5

To apply Fried's theorem to the pairs (G, H) from Theorems IV.2 or V.1 we need to classify the possible decompositions of all such polynomials G and H . We will use the following lemma.

Lemma VI.13. *Let $F(X) \in \mathbb{C}[X] \setminus \mathbb{C}$. Suppose that, for any $\alpha \in \mathbb{C}$, at most one point in $F^{-1}(\alpha)$ has ramification index more than 2, and every point in $F^{-1}(\alpha)$ has ramification index at most 4. If non-linear polynomials $\mu(X)$ and $\nu(X)$ satisfy $F = \mu \circ \nu$, then $\mu(X)$ has no ramification index greater than two over any finite point.*

Proof. We will assume that $\mu(X)$ has a point of ramification index greater than two and proceed to derive a contradiction. We denote this point λ . It cannot be that λ is a branch point of $\nu(X)$, because by the multiplicative property of ramification there would be a ramification index larger than four for $F(X)$. If λ were not a branch

point of $\nu(X)$, then $\nu(X)$ would have more than one pre-image of λ , and so $F^{-1}(\lambda)$ would have more than one point of ramification index larger than two. So we have a contradiction. Therefore, every ramification index of $\mu(X)$ over finite points must be either two or one. \square

Proposition VI.14. *Let $F(X) \in \mathbb{C}[X]$ have degree $m \geq 5$, and suppose that the ramification types of $F(X)$ over 2 and -2 are*

$$\mathcal{F}_1 = \left[4, 2^{\frac{m-5}{2}}, 1\right], \quad \text{and} \quad \mathcal{F}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right],$$

respectively. For any non-linear $\mu, \nu \in \mathbb{C}[X]$ such that $F = \mu \circ \nu$, there is a unique linear $\psi \in \mathbb{C}[X]$ such that $\mu = T_k \circ \psi$ (with $k := \deg(\mu)$). The ramification types \mathcal{N}_1 and \mathcal{N}_2 of $\nu(X)$ over $P_1 = \psi^{-1}(2)$ and $P_2 = \psi^{-1}(-2)$ are either

$$\mathcal{N}_1 = [4, 2, 2, \dots, 2, 1], \quad \text{and} \quad \mathcal{N}_2 = [2, 2, \dots, 2, 1^3]$$

or

$$\mathcal{N}_1 = [2, 2, \dots, 2, 1], \quad \text{and} \quad \mathcal{N}_2 = [2, 2, \dots, 2, 1^3].$$

Proof. By Lemma VI.13, every ramification index of $\mu(X)$ over its finite branch points is either 2 or 1. Also $\mu(X)$ has at most two finite branch points because every branch point of $\mu(X)$ is a branch point of $F(X)$. Additionally, $\mu(X)$ cannot have just one finite branch point, because then it would be a cyclic polynomial and by the multiplicative property of ramification $F(X)$ could not have unramified points over both its finite branch points. This means that $\mu(X) = \phi \circ T_k \circ \psi$ for some linear $\phi, \psi \in \mathbb{C}[X]$ (by Lemma II.18).

Lemma II.18 implies that $\mu(X)$ has ramification structure

$$\mathcal{M}_1 = \mathcal{M}_2 = [2, 2, \dots, 2, 1]$$

with corresponding branch points $\psi^{-1}(2)$ and $\psi^{-1}(-2)$, respectively. One of $\phi(2)$ and $\phi(-2)$ has three unramified F -preimages. We may assume that this point is $\phi(-2)$, since if it were $\phi(2)$ then we could replace $\phi(X)$ by $\phi(-X)$ and replace $\psi(X)$ by $-\psi(X)$ in order to interchange the roles of $\phi(2)$ and $\phi(-2)$, in light of Lemma II.19. Thus $\psi^{-1}(-2)$ is a branch point of $\nu(X)$ with ramification

$$[2, 2, \dots, 2, 1, 1, 1].$$

If no point in $\mu^{-1}(2) \setminus \{\psi^{-1}(2)\}$ is a branch point of $\nu(X)$, then $\psi^{-1}(2)$ must be a branch point of $\nu(X)$ with ramification

$$[4, 2, 2, \dots, 2, 1].$$

If some point $x_1 \in \mu^{-1}(2) \setminus \{\psi^{-1}(2)\}$ is a branch point of $\nu(X)$, then the ramification of $\nu(X)$ over x_1 must be

$$[2, 1, 1, \dots, 1].$$

For the ramification of $\mu \circ \nu(X)$ to agree with the ramification of $F(X)$, it must be that the ramification of $\nu(X)$ over $\psi^{-1}(2)$ is

$$(6.1) \quad [2, 2, \dots, 2, 1].$$

This completes the proof. □

Proposition VI.15. *Let $F(X) \in \mathbb{C}[X]$ have degree $m \geq 7$, and suppose that the ramification types of $F(X)$ over 2 and -2 are*

$$\mathcal{F}_1 = \left[4, 2^{\frac{m-7}{2}}, 1^3\right], \quad \text{and} \quad \mathcal{F}_2 = \left[2^{\frac{m-1}{2}}, 1\right],$$

respectively. For any non-linear $\mu, \nu \in \mathbb{C}[X]$ such that $F = \mu \circ \nu$, there is a unique linear $\psi \in \mathbb{C}[X]$ such that $\mu = T_k \circ \psi$ (with $k := \deg(\mu)$). The ramification types \mathcal{N}_1

and \mathcal{N}_2 of $\nu(X)$ over $P_1 = \psi^{-1}(2)$ and $P_2 = \psi^{-1}(-2)$ are either

$$\mathcal{N}_1 = [4, 2, 2, \dots, 2, 1^3], \quad \text{and} \quad \mathcal{N}_2 = [2, 2, \dots, 2, 1],$$

or

$$\mathcal{N}_1 = [2, 2, \dots, 2, 1^3], \quad \text{and} \quad \mathcal{N}_2 = [2, 2, \dots, 2, 1].$$

Proof. By Lemma VI.13, every ramification index of $\mu(X)$ over its finite branch points is either 2 or 1. Also $\mu(X)$ has at most two finite branch points because every branch point of $\mu(X)$ is a branch point of $F(X)$. Additionally, $\mu(X)$ cannot have just one finite branch point, because then it would be a cyclic polynomial and by the multiplicative property of ramification $F(X)$ could not have unramified points over both its finite branch points. This means that $\mu(X) = \phi \circ T_k \circ \psi$ for some linear $\phi, \psi \in \mathbb{C}[X]$ (by Lemma II.18).

Lemma II.18 implies that $\mu(X)$ has ramification structure

$$\mathcal{M}_1 = \mathcal{M}_2 = [2, 2, \dots, 2, 1]$$

with corresponding branch points $\psi^{-1}(2)$ and $\psi^{-1}(-2)$, respectively. One of $\phi(2)$ and $\phi(-2)$ has three unramified F -preimages. We may assume that this point is $\phi(2)$, since if it were $\phi(-2)$ then we could replace $\phi(X)$ by $\phi(-X)$ and replace $\psi(X)$ by $-\psi(X)$ in order to interchange the roles of $\phi(2)$ and $\phi(-2)$, in light of Lemma II.19. Thus $\psi^{-1}(-2)$ is a branch point of $\nu(X)$ with ramification

$$[2, 2, \dots, 2, 1].$$

If no point in $\mu^{-1}(2) \setminus \{\psi^{-1}(2)\}$ is a branch point of $\nu(X)$, then $\psi^{-1}(2)$ must be a branch point of $\nu(X)$ with ramification

$$[4, 2, 2, \dots, 2, 1, 1, 1].$$

If some point $x_1 \in \mu^{-1}(2) \setminus \{\psi^{-1}(2)\}$ is a branch point of $\nu(X)$, then the ramification of $\nu(X)$ over x_1 must be

$$[2, 1, 1, \dots, 1].$$

For the ramification of $\mu \circ \nu(X)$ to agree with the ramification of $F(X)$, it must be that the ramification of $\nu(X)$ over $\psi^{-1}(2)$ is

$$(6.2) \quad [2, 2, \dots, 2, 1, 1, 1].$$

This completes the proof. □

Proposition VI.16. *Let $F(X) \in \mathbb{C}[X]$ have degree $m \geq 5$, and suppose that the ramification types of $F(X)$ over 2 and -2 are*

$$\mathcal{F}_1 = \left[3, 2^{\frac{m-3}{2}}\right], \quad \mathcal{F}_2 = \left[2^{\frac{m-3}{2}}, 1^3\right],$$

respectively. For any non-linear $\mu, \nu \in \mathbb{C}[X]$ such that $F = \mu \circ \nu$, there is a unique linear $\psi \in \mathbb{C}[X]$ such that $\mu = T_k \circ \psi$ (with $k := \deg(\mu)$). The ramification types \mathcal{N}_1 and \mathcal{N}_2 of $\nu(X)$ over $P_1 = \psi^{-1}(2)$ and $P_2 = \psi^{-1}(-2)$ are

$$\mathcal{N}_1 = [3, 2, 2, \dots, 2], \quad \text{and} \quad \mathcal{N}_2 = [2, 2, \dots, 2, 1^3].$$

Proof. By Lemma VI.13, every ramification index of $\mu(X)$ over its finite branch points is either 2 or 1. Also $\mu(X)$ has at most two finite branch points because every branch point of $\mu(X)$ is a branch point of $F(X)$. Additionally, $\mu(X)$ cannot have just one finite branch point, because then it would be a cyclic polynomial and by the multiplicative property of ramification $F(X)$ would necessarily have a branch point whose greatest common divisor of its ramification would be greater than one. This means that $\mu(X) = \phi \circ T_k \circ \psi$ for some linear $\phi, \psi \in \mathbb{C}[X]$ (by Lemma II.18).

Lemma II.18 implies that $\mu(X)$ has ramification structure

$$\mathcal{M}_1 = \mathcal{M}_2 = [2, 2, \dots, 2, 1]$$

with corresponding branch points $\psi^{-1}(2)$ and $\psi^{-1}(-2)$, respectively. One of $\phi(2)$ and $\phi(-2)$ has three unramified F -preimages. We may assume that this point is $\phi(-2)$, since if it were $\phi(2)$ then we could replace $\phi(X)$ by $\phi(-X)$ and replace $\psi(X)$ by $-\psi(X)$ in order to interchange the roles of $\phi(2)$ and $\phi(-2)$, in light of Lemma II.19. Thus $\psi^{-1}(-2)$ is a branch point of $\nu(X)$ with ramification

$$[2, 2, \dots, 2, 1, 1, 1].$$

Since ramification is multiplicative, no point in $\mu^{-1}(2) \setminus \{\psi^{-1}(2)\}$ is a branch point of $\nu(X)$. Therefore $\psi^{-1}(2)$ must be a branch point of $\nu(X)$ with ramification

$$[3, 2, 2, \dots, 2]. \quad \square$$

Proposition VI.17. *Let $F(X) \in \mathbb{C}[X]$ have degree $m \geq 5$, and suppose that the ramification types of $F(X)$ over 2 and -2 are*

$$\mathcal{F}_1 = \left[3, 2^{\frac{m-5}{2}}, 1^2\right], \quad \mathcal{F}_2 = \left[2^{\frac{m-1}{2}}, 1\right],$$

respectively. For any non-linear $\mu, \nu \in \mathbb{C}[X]$ such that $F = \mu \circ \nu$, there is a unique linear $\psi \in \mathbb{C}[X]$ such that $\mu = T_k \circ \psi$ (with $k := \deg(\mu)$). The ramification types \mathcal{N}_1 and \mathcal{N}_2 of $\nu(X)$ over $P_1 = \psi^{-1}(2)$ and $P_2 = \psi^{-1}(-2)$ are $\nu(X)$ is

$$\mathcal{N}_1 = [3, 2, 2, \dots, 2, 1^2], \quad \mathcal{N}_2 = [2, 2, \dots, 2, 1].$$

Proof. By Lemma VI.13, every ramification index of $\mu(X)$ over its finite branch points is either 2 or 1. Also $\mu(X)$ has at most two finite branch points because every branch point of $\mu(X)$ is a branch point of $F(X)$. Additionally, $\mu(X)$ cannot have just one finite branch point, because then it would be a cyclic polynomial and by the multiplicative property of ramification $F(X)$ could not have unramified points over both its finite branch points. This means that $\mu(X) = \phi \circ T_k \circ \psi$ for some linear $\phi, \psi \in \mathbb{C}[X]$ (by Lemma II.18).

Lemma II.18 implies that $\mu(X)$ has ramification structure

$$\mathcal{M}_1 = \mathcal{M}_2 = [2, 2, \dots, 2, 1]$$

with corresponding branch points $\psi^{-1}(2)$ and $\psi^{-1}(-2)$, respectively. One of $\phi(2)$ and $\phi(-2)$ has one unramified F -preimage. We may assume that this point is $\phi(-2)$, since if it were $\phi(2)$ then we could replace $\phi(X)$ by $\phi(-X)$ and replace $\psi(X)$ by $-\psi(X)$ in order to interchange the roles of $\phi(2)$ and $\phi(-2)$, in light of Lemma II.19. Thus $\psi^{-1}(-2)$ is a branch point of $\nu(X)$ with ramification

$$[2, 2, \dots, 2, 1].$$

Since ramification is multiplicative, no point in $\mu^{-1}(2) \setminus \{\psi^{-1}(2)\}$ is a branch point of $\nu(X)$. Therefore $\psi^{-1}(2)$ must be a branch point of $\nu(X)$ with ramification

$$[3, 2, 2, \dots, 2, 1, 1]. \quad \square$$

Proposition VI.18. *Let $F(X) \in \mathbb{C}[X]$ have degree $m \geq 6$, and suppose that the ramification types of $F(X)$ over 2 and -2 are*

$$\mathcal{F}_1 = \left[4, 2^{\frac{m-6}{2}}, 1^2\right], \quad \text{and} \quad \mathcal{F}_2 = \left[2^{\frac{m-2}{2}}, 1^2\right],$$

respectively. For any non-linear $\mu, \nu \in \mathbb{C}[X]$ such that $F = \mu \circ \nu$, there is a unique linear $\psi \in \mathbb{C}[X]$ such that $\mu = T_k \circ \psi$ (with $k := \deg(\mu)$). The ramification types \mathcal{N}_1 and \mathcal{N}_2 of $\nu(X)$ over $P_1 = \psi^{-1}(2)$ and $P_2 = \psi^{-1}(-2)$ are either

$$\mathcal{N}_1 = [4, 2, 2, \dots, 2, 1^2], \quad \text{and} \quad \mathcal{N}_2 = [2, 2, \dots, 2, 1^2]$$

or

$$\mathcal{N}_1 = [2, 2, \dots, 2, 1^2], \quad \text{and} \quad \mathcal{N}_2 = [2, 2, \dots, 2, 1^2].$$

Proof. By Lemma VI.13, every ramification index of $\mu(X)$ over its finite branch points is either 2 or 1. Also $\mu(X)$ has at most two finite branch points because every branch point of $\mu(X)$ is a branch point of $F(X)$. Additionally, $\mu(X)$ cannot have just one finite branch point, because then it would be a cyclic polynomial and by the multiplicative property of ramification $F(X)$ could not have unramified points over both its finite branch points. This means that $\mu(X) = \phi \circ T_k \circ \psi$ for some linear $\phi, \psi \in \mathbb{C}[X]$ (by Lemma II.18). Lemma II.18 implies that the two possible ramification structures for $\mu(X)$ are

$$\mathcal{M}_1 = \mathcal{M}_2 = [2, 2, \dots, 2, 1],$$

and

$$\mathcal{M}_1 = [2, 2, \dots, 2], \quad \mathcal{M}_2 = [2, 2, \dots, 2, 1, 1],$$

with corresponding branch points $\psi^{-1}(2)$ and $\psi^{-1}(-2)$. However, it cannot be that $\mu(X)$ has the second type of ramification, because then $F(X)$ would have a branch point with all its ramification divisible by two.

One of $\phi(2)$ and $\phi(-2)$ has no F -preimage with ramification index larger than 2. We may assume that this point is $\psi(-2)$, since if it were $\psi(2)$ then we could replace $\phi(X)$ by $\phi(-X)$ and replace $\psi(X)$ by $-\psi(X)$ in order to interchange the roles of $\phi(2)$ and $\phi(-2)$, in light of Lemma II.19. Thus $\psi^{-1}(-2)$ is a branch point of $\nu(X)$ with ramification

$$[2, 2, \dots, 2, 1, 1].$$

If no point in $\mu^{-1}(2) \setminus \{\psi^{-1}(2)\}$ is a branch point of $\nu(X)$, then $\psi^{-1}(2)$ must be a branch point of $\nu(X)$ with ramification

$$[4, 2, 2, \dots, 2, 1, 1].$$

If some point $x_1 \in \mu^{-1}(2) \setminus \{\psi^{-1}(2)\}$ is a branch point of $\nu(X)$, then the ramification of $\nu(X)$ over x_1 must be

$$[2, 1, 1, \dots, 1].$$

For the ramification of $\mu \circ \nu(X)$ to agree with the ramification of $F(X)$, it must be that the ramification of $\nu(X)$ over $\psi^{-1}(2)$ is

$$(6.3) \quad [2, 2, \dots, 2, 1, 1].$$

This completes the proof. □

Proposition VI.19. *Let $F(X) \in \mathbb{C}[X]$ have degree $m \geq 4$, and suppose that the ramification types of $F(X)$ over 2 and -2 are*

$$\mathcal{F}_1 = \left[3, 2^{\frac{m-4}{2}}, 1\right], \quad \mathcal{F}_2 = \left[2^{\frac{m-2}{2}}, 1^2\right],$$

respectively. For any non-linear $\mu, \nu \in \mathbb{C}[X]$ such that $F = \mu \circ \nu$, there is a unique linear $\psi \in \mathbb{C}[X]$ such that $\mu = T_k \circ \psi$ (with $k := \deg(\mu)$ odd). The ramification types \mathcal{N}_1 and \mathcal{N}_2 of $\nu(X)$ over $P_1 = \psi^{-1}(2)$ and $P_2 = \psi^{-1}(-2)$ are

$$\mathcal{N}_1 = [3, 2, 2, \dots, 2, 1], \quad \text{and} \quad \mathcal{N}_2 = [2, 2, \dots, 2, 1^2].$$

Proof. By Lemma VI.13, every ramification index of $\mu(X)$ over its finite branch points is either 2 or 1. Also $\mu(X)$ has at most two finite branch points because every branch point of $\mu(X)$ is a branch point of $F(X)$. Additionally, $\mu(X)$ cannot have just one finite branch point, because then it would be a cyclic polynomial and by the multiplicative property of ramification $F(X)$ could not have unramified points over both its finite branch points. This means that $\mu(X) = \phi \circ T_k \circ \psi$ for some linear $\phi, \psi \in \mathbb{C}[X]$ (by Lemma II.18). Lemma II.18 implies that the two possible ramification structures for $\mu(X)$ are

$$\mathcal{M}_1 = \mathcal{M}_2 = [2, 2, \dots, 2, 1],$$

and

$$\mathcal{M}_1 = [2, 2, \dots, 2], \quad \mathcal{M}_2 = [2, 2, \dots, 2, 1, 1],$$

with corresponding branch points $\psi^{-1}(2)$ and $\psi^{-1}(-2)$. However, it cannot be that $\mu(X)$ has the second type of ramification, because then $F(X)$ would have a branch point with all its ramification divisible by two.

One of $\phi(2)$ and $\phi(-2)$ has two unramified F -preimages. We may assume that this point is $\phi(-2)$, since if it were $\phi(2)$ then we could replace $\phi(X)$ by $\phi(-X)$ and replace $\psi(X)$ by $-\psi(X)$ in order to interchange the roles of $\phi(2)$ and $\phi(-2)$, in light of Lemma II.19. Thus $\psi^{-1}(-2)$ is a branch point of $\nu(X)$ with ramification

$$[2, 2, \dots, 2, 1, 1, 1].$$

Since ramification is multiplicative, no point in $\mu^{-1}(2) \setminus \{\psi^{-1}(2)\}$ is a branch point of $\nu(X)$. Therefore $\psi^{-1}(2)$ must be a branch point of $\nu(X)$ with ramification

$$[3, 2, 2, \dots, 2, 1]. \quad \square$$

Proposition VI.20. *For any $b \in \mathbb{C} \setminus \{-2, 2\}$, let $F(X) \in \mathbb{C}[X]$ have degree $m \geq 5$, and suppose that the ramification types of $F(X)$ over 2 and -2 and b are*

$$\mathcal{F}_1 = \left[2^{\frac{m-3}{2}}, 1^3\right], \quad \mathcal{F}_2 = \left[2^{\frac{m-1}{2}}, 1\right], \quad \mathcal{F}_3 = [2, 1^{m-2}],$$

respectively. For any non-linear $\mu, \nu \in \mathbb{C}[X]$ such that $F = \mu \circ \nu$, there is a unique linear $\psi \in \mathbb{C}[X]$ such that $\mu = T_k \circ \psi$ (with $k := \deg(\mu)$). The ramification types \mathcal{N}_1 , \mathcal{N}_2 , and \mathcal{N}_3 of $\nu(X)$ over $P_1 = \psi^{-1}(2)$, $P_2 = \psi^{-1}(-2)$, and $P_3 = \psi^{-1}(b)$ are

$$\mathcal{N}_1 = [2, 2, \dots, 2, 1^3], \quad \mathcal{N}_2 = [2, 2, \dots, 2, 1], \quad \mathcal{N}_3 = [2, 1, 1, \dots, 1].$$

Proof. First note that $\mu(X)$ has exactly two finite branch points. If it had exactly one finite branch point, then it would be cyclic, and so $F(X)$ would have a branch

point with ramification indices all divisible by an integer larger than 1. Furthermore, $\mu(X)$ cannot have more branch points than $F(X)$, as every branch point of $\mu(X)$ is a branch point of $F(X)$. Lastly, it cannot be that $\mu(X)$ has three finite branch points, because if λ is the branch point of $F(X)$ with ramification $[2, 1^{m-2}]$, then $\mu(X)$ must have ramification $[2, 1, 1, \dots, 1]$ over λ . However, the point in $\mu^{-1}(\lambda)$ of ramification index two is either a branch point of $\nu(X)$ or not. If it is a branch point of $\nu(X)$, then $F(X)$ will have a ramification index greater than two. If it is not a branch point of $\nu(X)$ then $F(X)$ will have more than one ramified point over λ . In either case, $F(X)$ will not have the desired ramification, and so $\mu(X)$ has exactly two finite branch points.

By Lemma VI.13, every ramification index of $\mu(X)$ over its finite branch points is either 2 or 1, and as $\mu(X)$ has exactly two finite branch points, we conclude that $\mu(X) = \phi \circ T_k \circ \psi$ for some linear $\phi, \psi \in \mathbb{C}[X]$ (by Lemma II.18).

Lemma II.18 implies that $\mu(X)$ has ramification structure

$$\mathcal{M}_1 = \mathcal{M}_2 = [2, 2, \dots, 2, 1]$$

with corresponding branch points $\psi^{-1}(2)$ and $\psi^{-1}(-2)$, respectively. One of $\phi(2)$ and $\phi(-2)$ has one unramified F -preimage. We may assume that this point is $\phi(-2)$, since if it were $\phi(2)$ then we could replace $\phi(X)$ by $\phi(-X)$ and replace $\psi(X)$ by $-\psi(X)$ in order to interchange the roles of $\phi(2)$ and $\phi(-2)$, in light of Lemma II.19. Thus $\psi^{-1}(-2)$ is a branch point of $\nu(X)$ with ramification

$$[2, 2, \dots, 2, 1].$$

Since ramification is multiplicative, no point in $\mu^{-1}(2) \setminus \{\psi^{-1}(2)\}$ is a branch point of $\nu(X)$. Therefore $\psi^{-1}(2)$ must be a branch point of $\nu(X)$ with ramification

$$[2, 2, \dots, 2, 1, 1, 1].$$

Finally, there must be one branch point of ν not in $\mu^{-1}(2) \cup \mu^{-1}(-2)$ with ramification

$$[2, 1, 1, \dots, 1]. \quad \square$$

Proposition VI.21. *For any $b \in \mathbb{C} \setminus \{-2, 2\}$, let $F(X) \in \mathbb{C}[X]$ have degree $m \geq 4$, and suppose that the ramification types of $F(X)$ over 2 , -2 , and b are*

$$\mathcal{F}_1 = \left[2^{\frac{m-2}{2}}, 1^2\right], \quad \mathcal{F}_2 = \left[2^{\frac{m-2}{2}}, 1^2\right], \quad \mathcal{F}_3 = [2, 1^{m-2}],$$

respectively. For any non-linear $\mu, \nu \in \mathbb{C}[X]$ such that $F = \mu \circ \nu$, there is a unique linear $\psi \in \mathbb{C}[X]$ such that $\mu = T_k \circ \psi$ (with $k := \deg(\mu)$ odd). The ramification types $\mathcal{N}_1, \mathcal{N}_2$, and \mathcal{N}_3 of $\nu(X)$ over $P_1 = \psi^{-1}(2)$, $P_2 = \psi^{-1}(-2)$, and $P_3 = \psi^{-1}(b)$ are

$$\mathcal{N}_1 = [2, 2, \dots, 2, 1^2], \quad \mathcal{N}_2 = [2, 2, \dots, 2, 1^2], \quad \mathcal{N}_3 = [2, 1, 1, \dots, 1].$$

Proof. First note that $\mu(X)$ has exactly two finite branch points. If it had exactly one finite branch point, then it would be cyclic, and so $F(X)$ would have a branch point with ramification indices all divisible by an integer larger than 1. Furthermore, $\mu(X)$ cannot have more branch points than $F(X)$, as every branch point of $\mu(X)$ is a branch point of $F(X)$. Lastly, it cannot be that $\mu(X)$ has three finite branch points, because if λ is the branch point of $F(X)$ with ramification $[2, 1^{m-2}]$, then $\mu(X)$ must have ramification $[2, 1, 1, \dots, 1]$ over λ . However, the point in $\mu^{-1}(\lambda)$ of ramification index two is either a branch point of $\nu(X)$ or not. If it is a branch point of $\nu(X)$, then $F(X)$ will have a ramification index greater than two. If it is not a branch point of $\nu(X)$ then $F(X)$ will have more than one ramified point over λ . In either case, $F(X)$ will not have the desired ramification, and so $\mu(X)$ has exactly two finite branch points.

By Lemma VI.13, every ramification index of $\mu(X)$ over its finite branch points is either 2 or 1, and as $\mu(X)$ has exactly two finite branch points, we conclude that

$\mu(X) = \phi \circ T_k \circ \psi$ for some linear $\phi, \psi \in \mathbb{C}[X]$ (by Lemma II.18). The two possible ramification structures for $\mu(X)$ are

$$\mathcal{M}_1 = \mathcal{M}_2 = [2, 2, \dots, 2, 1],$$

and

$$\mathcal{M}_1 = [2, 2, \dots, 2], \quad \mathcal{M}_2 = [2, 2, \dots, 2, 1, 1],$$

with corresponding branch points $\psi^{-1}(2)$ and $\psi^{-1}(-2)$. However, it cannot be that $\mu(X)$ has the second type of ramification, because then $F(X)$ would have a branch point with all its ramification divisible by two.

Both of $\phi(2)$ and $\phi(-2)$ have two unramified F -preimages, and so $\psi^{-1}(-2)$ and $\psi^{-1}(2)$ are both branch points of $\nu(X)$ with ramification

$$[2, 2, \dots, 2, 1, 1].$$

Since ramification is multiplicative, $\nu(X)$ can have no additional branch points in $\mu^{-1}(2) \cup \mu^{-1}(-2)$. Finally $\nu(X)$ must also have a branch point not in $\mu^{-1}(2) \cup \mu^{-1}(-2)$ with ramification

$$[2, 1, 1, \dots, 1]. \quad \square$$

6.9 Optimal Decompositions of Polynomials from Theorem VI.5

The purpose of this section is to prove Proposition VI.22 which ties together all decompositions of the polynomials in Theorem VI.5. This result will be used in proving Theorem VI.5, and will also be used in Chapter IX.

Proposition VI.22. *Let $G(X) \in \mathcal{S}(n)$, where $n > 1$ is odd. Then there exist an odd integer $k \geq 1$ and an indecomposable polynomial $\overline{G}(X)$ such that both of the following hold:*

1. $G = T_k \circ \bar{G}$, and
2. for any nonlinear $\mu, \nu \in \mathbb{C}[X]$ such that $G = \mu \circ \nu$, there exist a divisor \bar{k} of k and a linear polynomial $\beta \in \mathbb{C}[X]$ such that $\mu = T_{\bar{k}} \circ \beta$.

We now state three known results, and then use them to prove Proposition VI.22.

Lemma VI.23. *Let $a, b, c, d \in \mathbb{C}[X] \setminus \mathbb{C}$ satisfy $a \circ b = c \circ d$, then there exists $\bar{a}, \bar{b}, \bar{c}, \bar{d}, g, h \in \mathbb{C}[X]$ such that*

- $g \circ \bar{a} = a$, $g \circ \bar{c} = c$, $\deg(g) = \gcd(\deg(a), \deg(c))$;
- $\bar{b} \circ h = b$, $\bar{d} \circ h = d$, $\deg(h) = \gcd(\deg(b), \deg(d))$; and
- $\bar{a} \circ \bar{b} = \bar{c} \circ \bar{d}$.

Proof. See Müller and Zieve [17, Lemma 2.8]. □

Lemma VI.24. *If $a, b \in \mathbb{C}[X] \setminus \mathbb{C}$ satisfy $a \circ b = T_n$ then $a = T_k \circ \ell$ and $b = \ell^{-1} \circ T_{n/k}$ for some linear polynomial $\ell \in \mathbb{C}[X]$.*

Proof. See Müller and Zieve [17, Lemma 3.8]. □

Lemma VI.25. *Suppose $n > 2$ and $a \circ b = c \circ d$ where $a, b, c, d \in \mathbb{C}[X] \setminus \mathbb{C}$ satisfy $\gcd(\deg(a), \deg(c)) = \gcd(\deg(b), \deg(d)) = 1$. If $c = T_n$ then $d = \varepsilon T_m \circ \ell$ and $a = \varepsilon^n T_m \circ \hat{\ell}$ and $b = \hat{\ell}^{-1} \circ T_n \circ \ell$ where $\ell, \hat{\ell} \in \mathbb{C}[X]$ are linear and $\varepsilon \in \{1, -1\}$.*

Proof. See Müller and Zieve [17, Lemma 3.16]. □

Lemma VI.26. *Let T_a and T_c be odd degree Chebyshev polynomials, and let $B, D \in \mathbb{C}[X] \setminus \mathbb{C}$ satisfy*

$$G(X) = T_a \circ B = T_c \circ D.$$

Then there exists $V \in \mathbb{C}[X]$ such that $G = T_e \circ V$, where $e = \text{lcm}(a, c)$.

Proof. If $c = a$ then we are done since $\text{lcm}(a, c) = a$. So we may assume that $c > a$.

By Lemma VI.23, there are polynomials $\bar{A}, \bar{B}, \bar{C}, \bar{D}, M$ and N such that

- $M \circ \bar{A} = T_a, M \circ \bar{C} = T_c, \deg(M) = \gcd(a, c);$
- $\bar{B} \circ N = B, \bar{D} \circ N = D, \deg N = \gcd(\deg(B), \deg(D));$ and
- $\bar{A} \circ \bar{B} = \bar{C} \circ \bar{D}.$

Since $M \circ \bar{C} = T_c$, Lemma VI.24 implies that $M = T_b \circ \ell$ and $\bar{C} = \ell^{-1} \circ T_{\bar{c}}$ for some linear $\ell \in \mathbb{C}[X]$. The above identities remain unchanged if we replace (M, \bar{A}, \bar{C}) by $(T_b, \ell \circ \bar{A}, T_{\bar{c}})$; thus we may assume that $M = T_b$ and $\bar{C} = T_{\bar{c}}$. Since $\bar{A} \circ \bar{B} = \bar{C} \circ \bar{D}$, where

$$\gcd(\deg(\bar{A}), \deg(\bar{C})) = \gcd(\deg(\bar{B}), \deg(\bar{D})) = 1$$

and $\deg(\bar{C}) = \bar{c} = c / \gcd(a, c)$ is an odd integer greater than 1, Lemma VI.25 implies that $\bar{D} = \epsilon T_{\bar{d}} \circ \mu$ for some linear $\mu \in \mathbb{C}[X]$ and some $\epsilon \in \{1, -1\}$. Thus

$$\begin{aligned} G &= T_c \circ D = T_c \circ \bar{D} \circ N \\ &= T_c \circ \epsilon T_{\bar{d}} \circ \mu \circ N \\ &= \epsilon T_{c\bar{d}} \circ \mu \circ N, \end{aligned}$$

where in the last equality we used the fact that T_c is an odd polynomial (Lemma II.19). Finally, since $T_a \circ B = T_c \circ D$, we have

$$c\bar{d} = c \frac{\deg(D)}{\gcd(\deg(B), \deg(D))} = \text{lcm}(a, c).$$

Since $e := \text{lcm}(a, c)$ is odd, we have $\epsilon T_e(X) = T_e(\epsilon X)$, which proves the result with $V = \epsilon \mu \circ N$. □

Proof of Proposition VI.22. Let k be the largest integer for which there exists $\bar{G} \in \mathbb{C}[X]$ with $G = T_k \circ \bar{G}$ (such a k exists because $G = T_1 \circ G$). We will show that k

and the associated \overline{G} have the required properties. Note that \overline{G} is not linear, since $G(X)$ is not dihedral.

For any nonlinear $\mu, \nu \in \mathbb{C}[X]$ such that $G = \mu \circ \nu$, Propositions VI.14–VI.21 imply that $\mu = \alpha \circ T_{\overline{k}} \circ \beta$ for some odd \overline{k} and some linear $\alpha, \beta \in \mathbb{C}[X]$, and so if $k = 1$ we are done. We may therefore assume that $k > 1$. We now show that $\alpha \in \{X, -X\}$. Note that the branch points of μ are $\alpha(2)$ and $\alpha(-2)$, which must also be branch points of G . If $(G(X), T_n(Y))$ comes from $\mathcal{S}(n)$ cases 3–8, then the branch points of G are 2 and -2 , so α maps $\{2, -2\}$ to itself, whence $\alpha \in \{X, -X\}$. If $(G(X), T_n(Y))$ comes from $\mathcal{S}(n)$ cases 1 or 2, then the branch points of G are 2, -2 , and P , where the ramification type of P is $[2, 1^{m-2}]$. If P has a ramified preimage Q under μ , then we get a contradiction because the ramification type of P in G forces $\nu^{-1}(Q)$ to consist of a single point which is unramified in ν . Thus P is not a branch point of μ , so we again find that α maps $\{2, -2\}$ to itself, whence $\alpha \in \{X, -X\}$.

We have shown that, for nonlinear $\mu, \nu \in \mathbb{C}[X]$ such that $G = \mu \circ \nu$, we have $\mu = \alpha \circ T_{\overline{k}} \circ \beta$ with \overline{k} odd, β linear, and $\alpha \in \{X, -X\}$. In fact we may assume that $\alpha = X$, since if $\alpha = -X$ then we may replace α and β by X and $-\beta$. By applying this to the decomposition $G = T_k \circ \overline{G}$, we conclude that k is odd. By applying it to an arbitrary decomposition, and appealing to Lemma VI.26, we conclude that $\text{lcm}(\overline{k}, k) \leq k$, so $\overline{k} \mid k$. Here $\mu = T_{\overline{k}} \circ \beta$, as desired. Finally, \overline{G} must be indecomposable, since if $\overline{G} = \theta \circ \rho$ with θ, ρ nonlinear, then applying the above to the decomposition $G = (T_k \circ \theta) \circ \rho$ implies that the degree of $T_k \circ \theta$ divides k , a contradiction. \square

6.10 Proof Theorem VI.5

Proof of Theorem VI.5. Let H_1 and H_2 be any two polynomials such that $H_1 \circ H_2(Y) = H(Y) = T_n(Y)$. Recall that Lemma VI.24 implies that $H_1(Y)$ is dihedral with the same two branch points as $T_n(Y)$. We claim that $G(X) - t$ and $H_1(Y) - t$ cannot have the same splitting fields. This is because given any $G(X)$ satisfying the hypotheses, either $G(X)$ has a branch point which is not a branch point of $H_1(Y)$ or it has a point of ramification larger than 2. In the first case Lemma VI.9 states the polynomials have different splitting fields. In the second case, it must be that the splitting field of $G(X)$ has a point of ramification larger than 2, however by Lemma VI.8 the splitting field of $H_1(Y)$ has no point of ramification larger than 2. Thus, $G(X) - t$ and $H_1(Y) - t$ have different splitting fields.

If $G(Y)$ is indecomposable then Theorem VI.6 and Lemma VI.7 imply that $G(X) - T_n(Y)$ is irreducible.

Now assume that $G(X)$ is decomposable. Fried's Theorem implies that if $G(X) - H(Y)$ is reducible, then we have $G = G_1 \circ G_2$ and $H = H_1 \circ H_2$ with $G_1(X) - H_1(Y)$ reducible and $G_1(X) - t$ and $H_1(Y) - t$ having the same splitting field over $\mathbb{C}(t)$. Since $H(Y) = T_n(Y)$ is a Chebyshev polynomial, then by Lemma VI.24 the identity $H = H_1 \circ H_2$ implies that $H_1 = T_k \circ \ell$ for some linear polynomial ℓ .

By Lemma VI.10 we see that $\deg G_1 = \deg H_1$.

By invoking Propositions VI.14–VI.21 we see that for any $G(X)$ with $(G(X), T_n(Y))$ a pair in one of the stated infinite families, and any decomposition $G = G_1 \circ G_2$ with G_2 non-linear such that $G_1 = a \circ T_k \circ b$ for linear polynomials $a, b \in \mathbb{C}[X]$ and odd positive integer k . Since $G_1(X) - t$ and $T_k \circ \ell(Y) - t$ have the same splitting field, they must have the same branch points (by Lemma VI.9). If $k > 2$, the finite branch

points of $T_k(Y) \circ \ell$ are ± 2 . It must be that $G_1(X) = a \circ T_k \circ b$ has those two branch points as well, and so $a(X) = \pm X$ because these are the only linear polynomials which preserve the set $\{-2, +2\}$. The only remaining possible value for k is $k = 1$, because k is odd. Then $G_1(X) - H_1(Y)$ is linear and hence irreducible.

We have shown that $G(X) - T_n(Y)$ is reducible only if we can write $G = \pm T_k \circ G_2$ with $k > 2$ and $k|n$. By Proposition VI.22 we know that there is a decomposition of G as $G = T_s \circ G_2$ with G_2 indecomposable, and every other decomposition of G as $G = \overline{G}_1 \circ \overline{G}_2$ has $\deg(\overline{G}_1)|s$. Therefore, $G(X) - T_n(Y)$ is irreducible if $G(X)$ decomposes as $T_k \circ \overline{G}$ with \overline{G} indecomposable and $(k, n) = 1$.

Furthermore if $G(X)$ decomposes as $T_k \circ \overline{G}$ with \overline{G} indecomposable and $(k, n) = \ell > 1$, then since T_n decomposes as $T_\ell \circ T_{n/\ell}$ and T_k decomposes as $T_\ell \circ T_{k/\ell}$ we have that

$$G(X) - T_n(Y) = T_\ell \circ (T_{k/\ell} \circ \overline{G})(X) - T_\ell \circ T_{n/\ell}(Y),$$

and so is divisible by

$$T_{k/\ell} \circ \overline{G}(X) - T_{n/\ell}(Y).$$

□

CHAPTER VII

Proofs of the Main Theorems

In this chapter we prove Theorems I.4 and I.5.

7.1 Faltings' theorem and its converse

Faltings' theorem (previously Mordell's conjecture) allows us to reduce an inherently number theoretic question (whether a curve has infinitely many rational points) to a question about the geometry of the curve.

Theorem VII.1 (Faltings' Theorem). *Let \mathcal{C} be a smooth, projective, geometrically irreducible curve defined over a number field K . If the genus of \mathcal{C} is bigger than 1, then \mathcal{C} has only finitely many K -rational points.*

If we allow for finite extensions of the field of definition of the curve, then the converse to Faltings' theorem holds. We state the combined result as follows, including the case of curves which are not assumed to be smooth or projective.

Theorem VII.2. *Let \mathcal{C} be a geometrically irreducible curve defined over a number field K . Then \mathcal{C} has genus 0 or 1 if and only if there is a finite extension L/K such that \mathcal{C} has infinitely many L -rational points.*

Proof. First assume that \mathcal{C} has genus bigger than 1. The curve \mathcal{C} is birationally equivalent over K to a smooth, projective, geometrically irreducible curve $\hat{\mathcal{C}}$. Since

$\hat{\mathcal{C}}$ has only finitely many K -rational points, the same holds for \mathcal{C} .

Now assume that \mathcal{C} has genus 0. Pick a non-singular point p in $\mathcal{C}(\overline{K})$, and let L be a finite extension of K such that $p \in \mathcal{C}(L)$. By the Riemann–Roch theorem, there is a rational function $\psi: \mathcal{C} \rightarrow \mathbb{P}^1$ which is defined over L and which has pole divisor p . In particular, $\deg(\psi) = 1$, so ψ is a birational equivalence between \mathcal{C} and \mathbb{P}^1 . Since $\mathbb{P}^1(L)$ is infinite, it follows that $\mathcal{C}(L)$ is infinite as well.

Finally, assume that \mathcal{C} has genus 1. Pick a non-singular point p in $\mathcal{C}(\overline{K})$, and let K_1 be a finite extension of K such that $p \in \mathcal{C}(K_1)$. Then the pair (\mathcal{C}, p) defines an elliptic curve over K_1 in which p is the identity element. Let $q \in \mathcal{C}(\overline{K}_1)$ be a point whose image in this elliptic curve has infinite order. Let L be a finite extension of K_1 such that $q \in \mathcal{C}(L)$. Then, since $\mathcal{C}(L)$ is a group, it must contain all of the infinitely many distinct multiples of q , and in particular it must be infinite. \square

7.2 Reducibility of $G(X) - H(Y)$ when G and H are indecomposable

Many papers have addressed irreducibility of polynomials of the form $G(X) - H(Y)$. The following result due to Feit goes a long ways towards classifying the reducible situations when G and H are indecomposable.

Theorem VII.3 (Feit). *If $G, H \in \mathbb{K}[T]$ are indecomposable polynomials such that $G(X) - H(Y)$ is reducible, then either $H = G \circ \mu$ for some linear $\mu \in \mathbb{C}[T]$ or*

$$\deg(G) = \deg(H) = m \in \{7, 11, 13, 15, 21, 31\}.$$

Moreover, in the latter cases, $G(X) - t$ and $H(Y) - t$ have the same splitting field Ω over $\mathbb{K}(t)$, and the Galois group $\text{Gal}(\Omega/\mathbb{K}(t))$ is either $\text{PGL}_3(2)$ (if $m = 7$), $\text{PSL}_2(11)$ (if $m = 11$), $\text{PGL}_3(3)$ (if $m = 13$), $\text{PGL}_4(2)$ (if $m = 15$), $\text{PTL}_3(4)$ (if $m = 21$), or $\text{PGL}_5(2)$ (if $m = 31$).

Proof. See [10] and [11]. □

We will use a refined version of this result, due to Cassou-Nogues and Couveignes, in which the relevant polynomials are explicitly computed. Due to the complicated nature of the polynomials in these examples, we do not write the polynomials here, but simply refer to the original paper [6, Theorem 2].

7.3 Proof of Theorem I.4

First note that since $G(X)$ and $H(Y)$ are indecomposable, it is also true that neither $G(X)$ nor $H(Y)$ is equivalent to a non-trivial power of a non-linear polynomial. Therefore, Theorem IV.1 implies that if either $G(X)$ or $H(Y)$ has more than three finite branch points then at least one of these polynomials must be cyclic.

The proof will proceed in the following cases:

1. The polynomial $G(X) - H(Y)$ is reducible;
2. At least one of $G(X)$ or $H(Y)$ is cyclic;
3. At least one of $G(X)$ or $H(Y)$ has three finite branch points;
4. Both $G(X)$ and $H(Y)$ have exactly two finite branch points.

If $G(X) - H(Y)$ is reducible then we apply Theorem VII.3 to conclude that either $H = G \circ \mu$ with $\mu \in \mathbb{K}[Y]$ linear or $\deg(G) = \deg(H) = m \in \{7, 11, 13, 15, 21, 31\}$. In the former case, $G(X) - H(Y)$ has the genus-zero factor $X - \mu(Y)$. The latter case can only yield low-degree solutions, so we do not write out all details of our calculations in this case. Here we use knowledge of the Galois group of the splitting field Ω of $G(X) - t$ over $\mathbb{K}(t)$ in order to compute all possibilities for the ramification in the extension $\Omega/\mathbb{K}(t)$, and from this we determine the genera of the irreducible factors of $G(X) - H(Y)$. Genus 0 factors occur in only three cases (two with $m = 7$

but with distinct ramification types, one with $m = 13$). In these cases we use the explicit polynomials found by Cassou-Nogues and Couveignes [6], which after some simplifications are listed as cases 24, 25, and 26 in Section 2.8.

Henceforth we assume that $G(X) - H(Y)$ is irreducible. If $G(X)$ is cyclic, our indecomposability hypothesis implies that $G(X)$ has prime degree. We can conclude from Theorem III.1 that $G(X) = H(Y)$ has genus 0 if and only if $(G(X), H(Y))$ is equivalent to one of the two following possibilities:

1. $(X^m, Y^a F(Y)^m)$ with m prime, a an integer satisfying $0 < a < m$, and $F(Y) \in \mathbb{K}[Y]$;
2. $(X^m, Y^a (Y - 1)^{m-a} F(Y)^m)$ with m prime, a an integer satisfying $0 < a < m$, and $F(Y) \in \mathbb{K}[Y]$.

If $G(X)$ has three finite branch points and $H(Y)$ is not cyclic, then Theorem ref:g0three implies that $G(X) = H(Y)$ has genus 0 if and only if either $(G(X), H(Y))$ has one of the two sporadic ramification configurations listed in cases 2 or 3 of Theorem IV.2, or $(G(X), H(Y))$ is equivalent to a pair of polynomials $(R(X), S(Y))$ which satisfy: $\deg(R) = m \geq 5$, $n|m$, $n > 1$ is odd, and $S(Y) = T_n(Y)$. Furthermore the branch points of R are $x_1 = 2$, $x_2 = -2$, and x_3 , with corresponding ramification either

- $\mathcal{R}_1 = \mathcal{R}_2 = [2^{\frac{m-2}{2}}, 1^2]$, $\mathcal{R}_3 = [2, 1^{m-2}]$; or
- $\mathcal{R}_1 = [2^{\frac{m-3}{2}}, 1^3]$, $\mathcal{R}_2 = [2^{\frac{m-1}{2}}, 1]$, $\mathcal{R}_3 = [2, 1^{m-2}]$.

In both of these cases we have that

$$(G(X) - 2)(G(X) + 2) = P(X)Q(X)^2,$$

with $Q(X)$ square free and $P(X)$ degree four and coprime to $Q(X)$. This is exactly case 4(d) of Theorem I.4.

If both $G(X)$ and $H(Y)$ have exactly two finite branch points, there are three possibilities:

1. $|\text{Br}(G) \cup \text{Br}(H)| = 4$;
2. $|\text{Br}(G) \cup \text{Br}(H)| = 3$;
3. $|\text{Br}(G) \cup \text{Br}(H)| = 2$.

The case that $|\text{Br}(G) \cup \text{Br}(H)| = 4$ was shown to not be possible in Lemma IV.12.

The case that $|\text{Br}(G) \cup \text{Br}(H)| = 3$ was handled in Theorem IV.4. The Theorem implies that the only possibility in this case is that $(G(X), H(Y))$ is equivalent to $(X^a(X-1)^{m-a}, cY^a(Y-1)^{m-a})$ with $c \in \mathbb{K} \setminus \{0, 1\}$, m and a integers satisfying $0 < a < m$ and $(a, m) = 1$, and $F(Y) \in \mathbb{K}[Y]$. These polynomials were shown to be indecomposable in Lemma VI.12.

Finally, the case that $|\text{Br}(G) \cup \text{Br}(H)| = 2$ was handled in Theorem V.1. We conclude from the theorem that the only possibilities in this case are the remaining sporadic examples (except for case 4 and case 12 because those polynomials are decomposable) or cases 4, 5(a), 5(b), or 5(c) of the theorem.

We show in Theorem VI.5 that the infinite families in case 5 are all irreducible if both polynomials are indecomposable.

7.4 Proof of Theorem I.5

The proof that a pair of polynomials $(G(X), H(Y))$ which satisfy conditions H1, H2, and H3 are exactly the polynomials stated is identical to the proof of Theorem I.4. In particular, we draw the conclusion from the results of Theorems III.1, IV.1, IV.2, IV.4, and V.1.

These same theorems imply that if our polynomials satisfy H1 and H3, then these

are the only polynomials which satisfy H2. Finally, Theorems VI.1–VI.5 imply that the only polynomials which satisfy H1, H2, and H3 are the stated ones.

CHAPTER VIII

Counting Equivalence Classes of Polynomials of Given Degrees

In Theorem I.5 we classified the pairs of polynomials $(G(X), H(Y))$ satisfying certain constraints. The classification asserted that either $(G(X), H(Y))$ belongs to an explicit list, or $(G(X), H(Y))$ is equivalent to a pair $(F(X), T_n(Y))$ where $F(X)$ satisfies a certain functional equation and $F = T_k \circ \hat{F}$ with \hat{F} indecomposable. In this chapter we count the number of equivalence classes of such pairs $(F(X), T_n(Y))$. For most of the functional equations, there are finitely many such classes, but in some cases we obtain finitely many one-parameter families of such classes. We begin by counting equivalence classes of pairs without assuming the constraint on the decomposition of F . In case F has prime degree, the decomposition constraint is automatically satisfied, so our count gives the desired answer. When F has composite degree, we show at the end of the chapter how to deduce the desired counts from the simpler counts performed earlier in the chapter.

8.1 Equivalence and Right-Equivalence

We will prove several theorems counting the number of equivalence classes of polynomials $H(Y)$ having two or three finite branch points with certain prescribed ramification types. Recall that polynomials $H(Y)$ and $\bar{H}(Y)$ are *equivalent* if there

exist linear polynomials $\mu(X), \psi(X)$ such that

$$\overline{H}(Y) = \mu \circ H \circ \psi(Y).$$

Also, \mathbb{K} denotes an algebraically closed field of characteristic zero.

Definition VIII.1. We say that two polynomials $F, G \in \mathbb{K}[T]$ are *right-equivalent* (over \mathbb{K}) if there is a linear polynomial $\mu \in \mathbb{K}[T]$ with $F = G \circ \mu$.

Note that if two polynomials $F, G \in \mathbb{K}[T]$ satisfy $\text{Br}(F) = \text{Br}(G) = \{P_1, P_2\}$, where F and G have the same ramification type as each other over P_i (for each $i \in \{1, 2\}$) but the ramification type of F over P_1 differs from the ramification type of F over P_2 , then F and G are equivalent (over \mathbb{K}) if and only if they are right-equivalent over \mathbb{K} .

We also remind the reader of the definition of equivalence of pairs of polynomials:

Definition VIII.2. We say two pairs of polynomials (G, H) and $(\overline{G}, \overline{H})$ with coefficients in \mathbb{K} are *equivalent* if there are three linear polynomials $\mu, \psi, \phi \in \mathbb{K}[X]$ such that $(\overline{G}, \overline{H})$ is either

$$(\mu \circ G \circ \psi, \mu \circ H \circ \phi)$$

or

$$(\mu \circ H \circ \psi, \mu \circ G \circ \phi).$$

Lemma VIII.3. For $m > 1$ odd, the pairs $(T_m(X), F(Y))$ and $(T_m(X), G(Y))$ are equivalent (as pairs) if and only if $F(Y)$ is right-equivalent to either $G(Y)$ or $-G(Y)$.

Proof. $T_m = \mu \circ T_m \circ \nu$ if and only if either $a = b = X$ or $a = b = -X$ [17, Lemma 3.13]. So equivalence of pairs means that either $F = G \circ \phi$ or $F = -G \circ \phi$, for ϕ linear. Therefore, equivalence of pairs means right-equivalence of F to either G or $-G$. □

8.2 Multiplicity Theorems

Theorem VIII.4. *If $n \geq 5$ is odd, there are $\frac{(n-3)(n-1)(n+1)}{48}$ equivalence classes of polynomials $H(Y) \in \mathbb{K}[Y]$ with ramification type*

$$\mathcal{H}_1 = \left[4, 2^{\frac{n-5}{2}}, 1\right], \mathcal{H}_2 = \left[2^{\frac{n-3}{2}}, 1^3\right].$$

Theorem VIII.5. *If $n \geq 7$ is odd, there are $\frac{(n-5)(n-3)(n-1)}{48}$ equivalence classes of polynomials $H(Y) \in \mathbb{K}[Y]$ with ramification type*

$$\mathcal{H}_1 = \left[4, 2^{\frac{n-7}{2}}, 1^3\right], \mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right].$$

Theorem VIII.6. *If $n \geq 5$ is odd, there are $\frac{(n-3)(n-1)}{8}$ equivalence classes of polynomials $H(Y) \in \mathbb{K}[Y]$ with ramification type*

$$\mathcal{H}_1 = \left[3, 2^{\frac{n-5}{2}}, 1^2\right], \mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1\right].$$

Theorem VIII.7. *If $n \geq 4$ is even, there are $\frac{n(n-2)}{8}$ equivalence classes of polynomials $H(Y) \in \mathbb{K}[Y]$ with ramification type*

$$\mathcal{H}_1 = \left[3, 2^{\frac{n-4}{2}}, 1\right], \mathcal{H}_2 = \left[2^{\frac{n-2}{2}}, 1^2\right].$$

Theorem VIII.8. *If $n \geq 6$ is divisible by 4 then there are $\frac{(n-4)(n-2)n}{32}$ equivalence classes of polynomials $H(Y) \in \mathbb{K}[Y]$ with ramification type*

$$\mathcal{H}_1 = \left[4, 2^{\frac{n-6}{2}}, 1^2\right], \mathcal{H}_2 = \left[2^{\frac{n-2}{2}}, 1^2\right].$$

If $n \geq 6$ is congruent to 2 modulo 4 then there are $\frac{(n-2)^3}{32}$ equivalence classes of polynomials $H(Y) \in \mathbb{K}[Y]$ with ramification type

$$\mathcal{H}_1 = \left[4, 2^{\frac{n-6}{2}}, 1^2\right], \mathcal{H}_2 = \left[2^{\frac{n-2}{2}}, 1^2\right].$$

Theorem VIII.9. For odd $n \geq 3$ there are $\left\lceil \frac{n^2-1}{24} \right\rceil$ equivalence classes of polynomials $H(Y) \in \mathbb{K}[Y]$ with ramification type

$$\mathcal{H}_1 = \left[3, 2^{\frac{n-3}{2}} \right], \mathcal{H}_2 = \left[2^{\frac{n-3}{2}}, 1^3 \right].$$

Theorem VIII.10. For odd $n \geq 5$ and any $b \in \mathbb{K} \setminus \{2, -2\}$, there are

$$\frac{n^3 - n}{24}$$

right-equivalence classes of polynomials $H(Y) \in \mathbb{K}[Y]$ with ramification type

$$\mathcal{H}_1 = \left[2^{\frac{n-3}{2}}, 1^3 \right], \mathcal{H}_2 = \left[2^{\frac{n-1}{2}}, 1 \right], \mathcal{H}_3 = [2, 1^{n-2}],$$

with corresponding branch points $2, -2$, and b .

Theorem VIII.11. For even $n \geq 6$ and any $b \in \mathbb{K} \setminus \{2, -2\}$ there are

$$\begin{aligned} & \frac{n^3}{16} \text{ for } n \equiv 0 \pmod{4} \\ & \frac{n^3}{16} + \frac{n}{4} \text{ for } n \equiv 2 \pmod{4} \end{aligned}$$

right-equivalence classes of polynomials $H(Y) \in \mathbb{K}[Y]$ with ramification type

$$\mathcal{H}_1 = \left[2^{\frac{n-2}{2}}, 1^2 \right], \mathcal{H}_2 = \left[2^{\frac{n-2}{2}}, 1^2 \right], \mathcal{H}_3 = [2, 1^{n-2}],$$

with corresponding branch points $2, -2$, and b .

8.3 Riemann's Existence Theorem

Our main technical device to prove the above results is a version of Riemann's existence theorem. We first introduce two concepts used in the statement of this theorem. If \mathcal{G}_1 is a multiset of positive integers whose sum is m , we define the associated conjugacy class of the symmetric group S_m to be the conjugacy class of elements whose multiset of cycle lengths is equal to \mathcal{G}_1 .

Definition VIII.12. Two tuples (a_1, \dots, a_R) and $(\tilde{a}_1, \dots, \tilde{a}_R)$ in S_m^R are *equivalent* if there is an element $g \in S_m$ such that $ga_i g^{-1} = \tilde{a}_i$ for $1 \leq i \leq R$.

Theorem VIII.13 (Riemann Existence Theorem). *Fix a positive integer m , and distinct $\lambda_1, \dots, \lambda_R \in \mathbb{K}$. Let $\mathcal{G}_1, \dots, \mathcal{G}_R$ be multisets of positive integers such that the following hold:*

- $\sum_{\alpha \in \mathcal{G}_i} \alpha = m$ for each i with $1 \leq i \leq R$;
- $\max_{\alpha \in \mathcal{G}_i} \alpha > 1$ for each i ;
- $m - 1 = \sum_{i=1}^R \sum_{\alpha \in \mathcal{G}_i} (\alpha - 1)$.

Then the number of right-equivalence classes of polynomials $G(X) \in \mathbb{K}[X]$ with branch points $\lambda_1, \dots, \lambda_R$ and with corresponding ramification multisets $\mathcal{G}_1, \dots, \mathcal{G}_R$ is equal to the number of equivalence classes of tuples $(a_1, \dots, a_R) \in S_m^R$ such that a_i is in the conjugacy class associated to \mathcal{G}_i (for $1 \leq i \leq R$) and $a_1 \dots a_R$ is an m -cycle.

Proof. For the case $\mathbb{K} = \mathbb{C}$, see [14, Theorem 1.1] or [23, Remark 7.4]. We will deduce the result for arbitrary \mathbb{K} from the result for the case $\mathbb{K} = \mathbb{C}$.

First suppose that \mathbb{K} is a subfield of \mathbb{C} . To prove the result for \mathbb{K} , it suffices to show that every right-equivalence class of polynomials in $\mathbb{C}[X]$ which has specified branch points in \mathbb{K} must contain a polynomial in $\mathbb{K}[X]$. To this end, note that any degree- m polynomial in $\mathbb{C}[X]$ is right-equivalent to a monic polynomial which has no term of degree $m - 1$. Moreover, each right-equivalence class contains only finitely many polynomials with these properties. Since there are only finitely many right-equivalence classes of polynomials in $\mathbb{C}[X]$ which have specified branch points and specified ramification, it follows that there are only finitely many monic degree- m polynomials which have no term of degree $m - 1$ and which have specified branch

points and specified ramification. In our situation the branch points are in \mathbb{K} , so our finite set of polynomials must be preserved by every automorphism of \mathbb{C} which acts as the identity on \mathbb{K} . Since each element of $\mathbb{C} \setminus \mathbb{K}$ has an infinite orbit under this group of automorphisms, it follows that each of the finitely many polynomials must lie in $\mathbb{K}[X]$. Thus, the result for subfields \mathbb{K} of \mathbb{C} follows from the result for the case $\mathbb{K} = \mathbb{C}$.

Now let \mathbb{K} be an arbitrary algebraically closed field of characteristic zero. Pick distinct $\lambda_1, \dots, \lambda_R$ in \mathbb{K} , and write $L = \mathbb{Q}(\lambda_1, \dots, \lambda_R)$. Since L is a finitely-generated extension of \mathbb{Q} , there is an embedding $\psi: L \hookrightarrow \mathbb{C}$. As above, every right-equivalence class of degree- m polynomials in $\mathbb{K}[X]$ includes a nonzero finite number of monic polynomials which have no term of degree $m - 1$. Pick any polynomial $f(X)$ of the latter form, and let M be the extension of L gotten by adjoining the coefficients of this polynomial. Again, M is a finitely-generated extension of \mathbb{Q} , so we can extend ψ to an embedding $\hat{\psi}: M \hookrightarrow \mathbb{C}$. Then $\hat{\psi}(f(X))$ is a monic degree- m polynomial in $\mathbb{C}[X]$ which has no term of degree $m - 1$, so it follows from the previous paragraph that all coefficients of $\hat{\psi}(f(X))$ lie in the algebraic closure $\overline{\psi(L)}$ of $\psi(L)$ in \mathbb{C} . Thus, all coefficients of $f(X)$ must lie in the algebraic closure \overline{L} of L in \mathbb{K} . Since we can extend ψ to an embedding $\overline{\psi}: \overline{L} \rightarrow \mathbb{C}$, the result for arbitrary \mathbb{K} now follows from the result for subfields of \mathbb{C} , which was shown above. \square

8.4 Strategy of the Proofs

By Riemann's existence theorem, counting equivalence classes of polynomials $H(Y)$ of degree n with two branch points having a specific ramification structure reduces to the combinatorial problem of counting equivalence classes of pairs of permutations $(a, b) \in S_n \times S_n$ with equivalence relation $(a, b) \sim (gag^{-1}, bg^{-1})$, having

given cycle structures and with ab being an n -cycle.

We do this by associating to each such pair (a, b) a graph with n vertices and two kinds of labeled edges (solid edges and dotted edges) encoding the actions of a and b . The graph must be connected, which puts severe constraints on a and b , which we analyze.

8.5 Connectivity of Graphs

We use the following simple result for finite undirected graphs.

Lemma VIII.14. *A graph G with n connected components requires at least $n - 1$ edges added to it to become connected. If a connected graph \tilde{G} is formed from G by adding exactly $n - 1$ new edges, then \tilde{G} has no new cycles.*

Proof. One can draw a new graph with a vertex representing each connected component. A graph with n vertices and no edges has n connected components. Adding an edge reduces the number of connected components by at most 1, thus a graph with only 1 connected component has at least $n - 1$ edges.

If a connected graph with n vertices has $n - 1$ edges and a cycle, then at least one of the edges can be removed without disconnecting the graph; this is a contradiction with the minimality of edges result. \square

8.6 Proofs of Multiplicity Theorems

Proof of Theorem VIII.4. To count the number of equivalence classes of polynomials with the given ramification structure the Riemann Existence Theorem (stated here as Theorem VIII.13) implies that it is sufficient to count (up to conjugacy in S_n) the number of tuples $(a, b) \in S_n^2$ such that ab is an n -cycle and such that a is a 4-cycle and $\frac{n-5}{2}$ 2-cycles and b is a product of $\frac{n-3}{2}$ 2-cycles is primitive. We may therefore

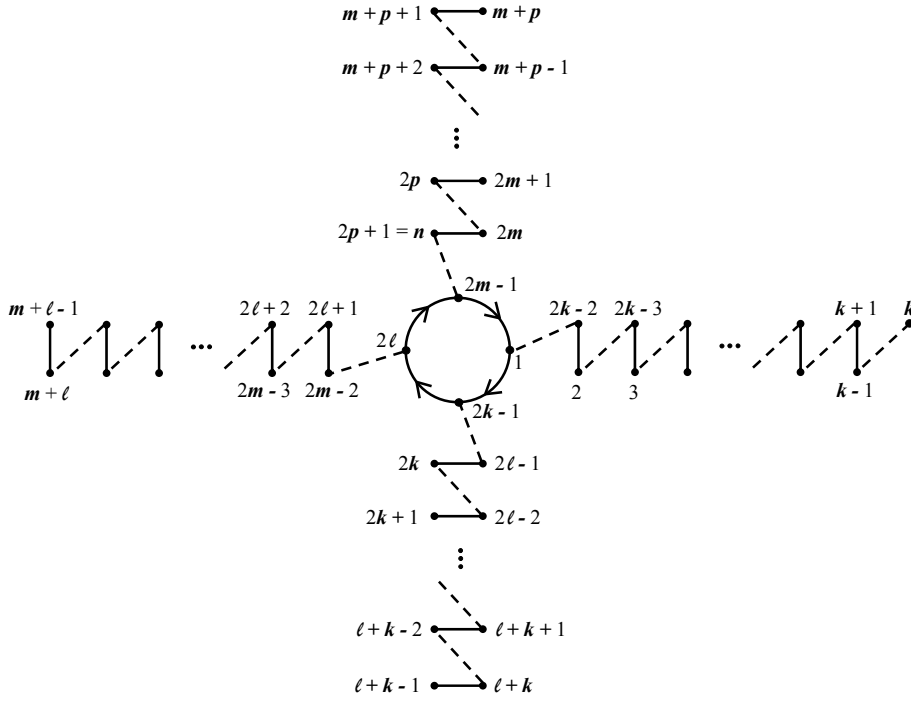


Figure 8.1: The Graph of Actions in Theorem VIII.4

assume that $ab = (1\ 2\ 3\ \dots\ n)$.

We can draw a graph with labeled vertices $1, \dots, n$, a solid edge between two vertices if the action a maps one of the vertices' label to the other's, and a dotted edge between two vertices if the action b maps one of the vertices' label to the other's. If ab is an n -cycle, then it is necessary that this graph be connected. Since every cycle of a is a connected component (if the edges associated to b were removed), there are $\frac{n-1}{2}$ such components. Therefore by Lemma VIII.14 b has exactly the minimum number of 2-cycles to make the graph connected, but b cannot introduce any cycles. Therefore, the graph must be structurally like the drawing, since every 2-cycle of a and its fixed point must be connected to one of the elements of its 4-cycle.

In addition, there is no symmetry in the numbering, since we assume that k is the fixed point, that $\ell + k$ is the end of the next branch of the 4-cycle, etc.

Therefore, up to S_n conjugacy, the element a is the product of the cycles

$$\begin{aligned} a = & (1, 2k + 1, 2\ell + 2, 2m + 3)(2, 2k - 2)(3, 2k - 3) \cdots (k - 1, k + 1) \\ & (2k, 2\ell - 1) \cdots (\ell + k - 1, \ell + k)(2\ell + 1, 2m - 2) \cdots (m + \ell - 1, m + \ell) \\ & (2m, 2p + 1) \cdots (m + p, m + p + 1), \end{aligned}$$

and the element b is the product of the cycles

$$\begin{aligned} b = & (1, 2k - 2)(2, 2k - 3) \cdots (k - 1, k) \\ & (2k - 1, 2\ell - 1) \cdots (\ell + k - 2, \ell + k) \\ & (2\ell, 2m - 2) \cdots (m + \ell - 2, m + \ell) \\ & (2m - 1, 2p + 1) \cdots (m + p - 1, m + p + 1) \end{aligned}$$

for any integers k, ℓ, m , and p satisfying

$$2 \leq k \leq \ell < m \leq \frac{n+1}{2}, \text{ and } p = \frac{n-1}{2}.$$

So we need only count the number of choices of k, ℓ , and m satisfying the above inequality. We denote $\text{Tri}(x) = \frac{x(x+1)}{2}$ the triangle number. This is:

$$\begin{aligned} \sum_{k=1}^{\frac{n-3}{2}} \sum_{\ell=k}^{\frac{n-3}{2}} \sum_{m=\ell+1}^{\frac{n-1}{2}} 1 &= \sum_{k=1}^{\frac{n-3}{2}} \sum_{\ell=k}^{\frac{n-3}{2}} \left[\frac{n-1}{2} - \ell \right] \\ &= \sum_{k=1}^{\frac{n-3}{2}} \sum_{\ell=1}^{\frac{n-1}{2}-k} [\ell] \\ &= \sum_{k=1}^{\frac{n-3}{2}} \left[\text{Tri} \left(\frac{n-1}{2} - k \right) \right] \\ &= \sum_{k=1}^{\frac{n-3}{2}} [\text{Tri}(k)] \\ &= \sum_{k=1}^{\frac{n-3}{2}} \left[\frac{k(k+1)}{2} \right] \\ &= \frac{(n-5)(n-3)(n-1)}{48}. \end{aligned}$$

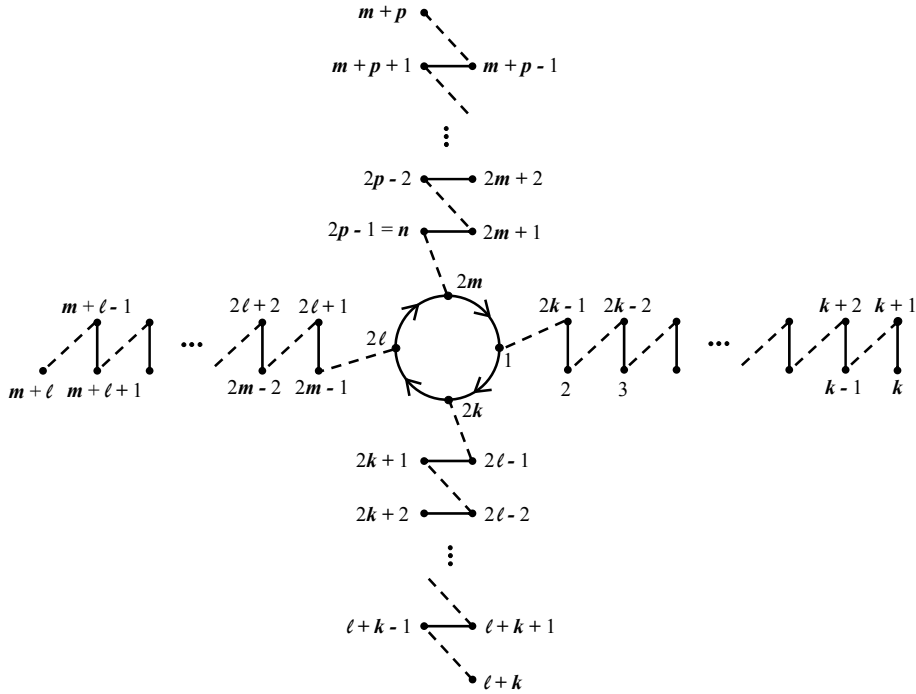


Figure 8.2: The Graph of Actions in Theorem VIII.5

The last line is due to the relation

$$\sum_{i=1}^n i^2 = \frac{n(n+1)(n+2)}{6}.$$

□

Proof of Theorem VIII.5. The proof is similar to the previous proof. We draw the graph associated to the action of a (a 4-cycle, and $\frac{n-7}{2}$ 2-cycles) and b ($\frac{n-1}{2}$ 2-cycles). We can again show by Lemma VIII.14 that the graph must have the structure of the image below.

In addition, there is no symmetry in the numbering, since we assume that the branch without a fixed point attaches to the vertex labeled 1, that $\ell + k$ is the end of the next branch of the 4-cycle, etc.

Therefore, if $ab = (1\ 2\ 3\ \dots\ n)$ then up to S_n conjugacy it must be that a is the

product of the cycles

$$\begin{aligned}
 a &= (1, 2k, 2\ell, 2m)(2, 2k - 1)(3, 2k - 2) \cdots (k, k + 1) \\
 &(2k + 1, 2\ell - 1) \cdots (\ell + k - 1, \ell + k + 1)(2\ell + 1, 2m - 1) \cdots (m + \ell - 1, m + \ell + 1) \\
 &(2m + 1, 2p - 1) \cdots (m + p - 1, m + p + 1),
 \end{aligned}$$

and the element b is the product of the cycles

$$\begin{aligned}
 b &= (1, 2k - 1)(2, 2k - 2) \cdots (k - 1, k + 1) \\
 &(2k, 2\ell - 1) \cdots (\ell + k - 1, \ell + k) \\
 &(2\ell, 2m - 1) \cdots (m + \ell - 1, m + \ell) \\
 &(2m, 2p - 1) \cdots (m + p - 1, m + p)
 \end{aligned}$$

for any integers k, ℓ, m , and p satisfying

$$1 \leq k < \ell < m < p = \frac{n+1}{2}.$$

So we need only count the number of choices of k, ℓ , and m satisfying the above inequality. Like before, we denote $\text{Tri}(x) = \frac{x(x+1)}{2}$ the triangle number. This is:

$$\begin{aligned}
 \sum_{k=1}^{\frac{n-5}{2}} \sum_{\ell=k+1}^{\frac{n-3}{2}} \sum_{m=\ell+1}^{\frac{n-1}{2}} 1 &= \sum_{k=1}^{\frac{n-5}{2}} \sum_{\ell=k+1}^{\frac{n-3}{2}} \left[\frac{n-1}{2} - \ell \right] \\
 &= \sum_{k=1}^{\frac{n-3}{2}} \sum_{\ell=1}^{\frac{n-3}{2}-k} [\ell] \\
 &= \sum_{k=1}^{\frac{n-3}{2}} \left[\text{Tri} \left(\frac{n-3}{2} - k \right) \right] \\
 &= \sum_{k=0}^{\frac{n-3}{2}} [\text{Tri}(k)] \\
 &= \sum_{k=0}^{\frac{n-3}{2}} \left[\frac{k(k+1)}{2} \right] \\
 &= \frac{(n-1)(n+1)(n+3)}{48}.
 \end{aligned}$$

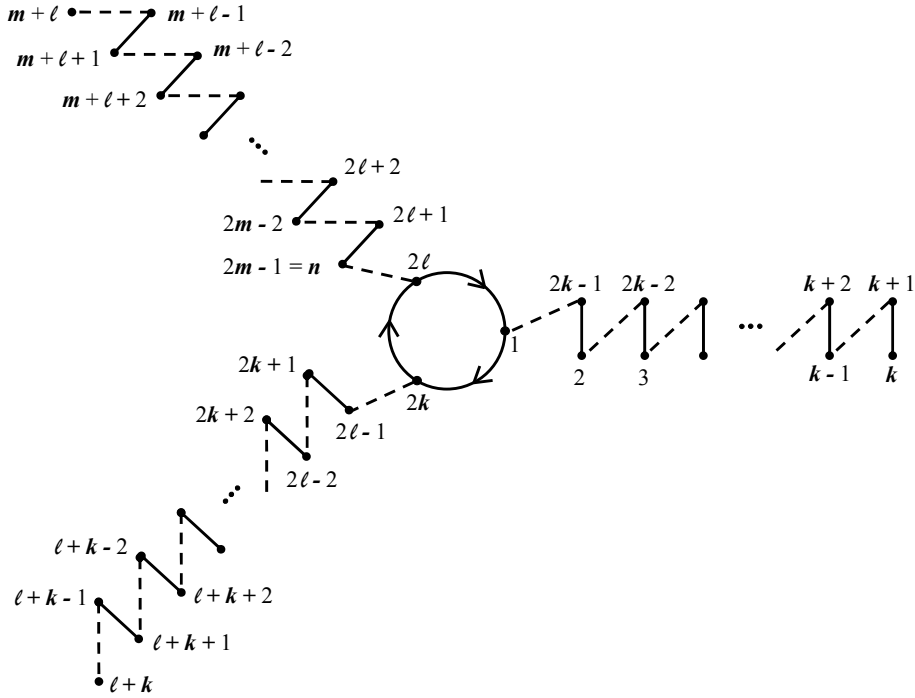


Figure 8.3: The Graph of Actions in Theorem VIII.6

□

Proof of Theorem VIII.6. We draw the graph associated to the action of a (a 3-cycle, and $\frac{n-5}{2}$ 2-cycles) and b ($\frac{n-1}{2}$ 2-cycles). We can again show by Lemma VIII.14 that the graph must have the structure of the image below.

In addition, there is no symmetry in the numbering, since we assume that the branch without a fixed point attaches to the vertex labeled 1, that $\ell + k$ is the end of the next branch of the 3-cycle, etc.

Therefore, if $ab = (1\ 2\ 3\ \dots\ n)$ then up to S_n conjugacy it must be that a is the product of the cycles

$$a = (1, 2k, 2\ell)(2, 2k - 1)(3, 2k - 2) \cdots (k, k + 1)$$

$$(2k + 1, 2\ell - 1) \cdots (\ell + k - 1, \ell + k + 1)(2\ell + 1, 2m - 1) \cdots (m + \ell - 1, m + \ell + 1),$$

and the element b is the product of the cycles

$$\begin{aligned} b &= (1, 2k - 1)(2, 2k - 2) \cdots (k - 1, k + 1) \\ &\quad (2k, 2\ell - 1) \cdots (\ell + k - 1, \ell + k) \\ &\quad (2\ell, 2m - 1) \cdots (m + \ell - 1, m + \ell) \end{aligned}$$

for any integers k, ℓ , and m satisfying

$$1 \leq k < \ell < m = \frac{n+1}{2}.$$

So we need only count the number of choices of k and ℓ satisfying the above inequality. This is:

$$\begin{aligned} \sum_{k=1}^{\frac{n-3}{2}} \sum_{\ell=k+1}^{\frac{n-1}{2}} 1 &= \sum_{k=1}^{\frac{n-3}{2}} \left[\frac{n-1}{2} - k \right] \\ &= \sum_{k=1}^{\frac{n-3}{2}} [k] \\ &= \frac{(n-3)(n-1)}{8}. \end{aligned}$$

□

Proof of Theorem VIII.7. We draw the graph associated to the action of a (a 3-cycle, and $\frac{n-4}{2}$ 2-cycles) and b ($\frac{n-2}{2}$ 2-cycles). We can again show by Lemma VIII.14 that the graph must have the structure of the image below.

In addition, there is no symmetry in the numbering, since we assume that the branch without a fixed point attaches to the vertex labeled 1, that $\ell + k$ is the end of the next branch of the 3-cycle, and $m + \ell$ is the last vertex in the third branch.

Therefore, if $ab = (1\ 2\ 3 \dots n)$ then up to S_n conjugacy it must be that a is the

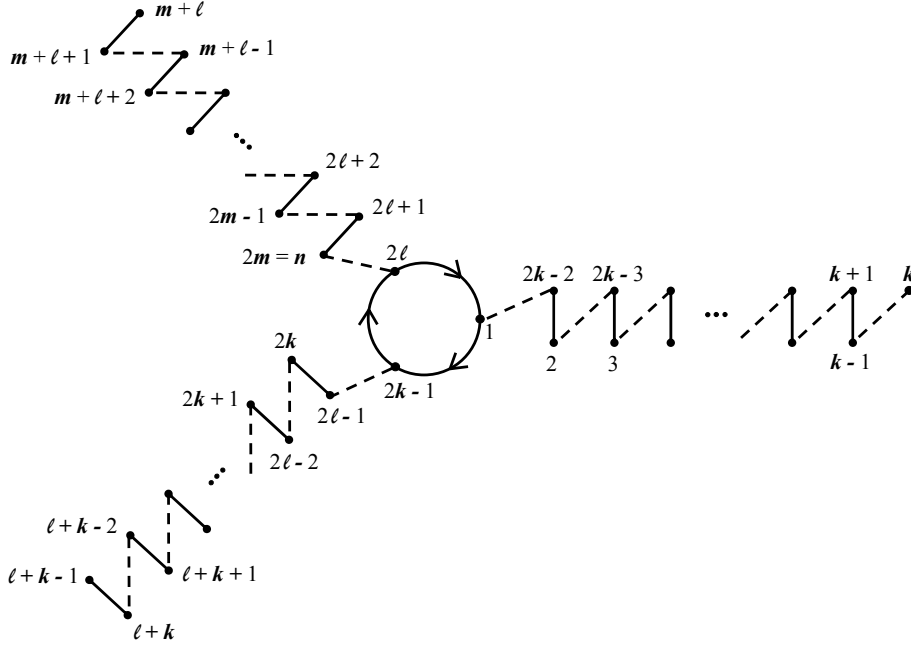


Figure 8.4: The Graph of Actions in Theorem VIII.7

product of the cycles

$$a = (1, 2k-1, 2l)(2, 2k-2)(3, 2k-3) \cdots (k-1, k+1) \\ (2k, 2l-1) \cdots (\ell+k-1, \ell+k)(2l+1, 2m) \cdots (m+l, m+l+1),$$

and the element b is the product of the cycles

$$b = (1, 2k-2)(2, 2k-3) \cdots (k-1, k) \\ (2k-1, 2l-1) \cdots (\ell+k-2, \ell+k) \\ (2l, 2m) \cdots (m+l-1, m+l+1)$$

for any integers k, ℓ , and m satisfying

$$2 \leq k \leq \ell \leq m = \frac{n}{2}.$$

So we need only count the number of choices of k and ℓ satisfying the above

inequality. This is:

$$\begin{aligned}
 \sum_{k=2}^{\frac{n}{2}} \sum_{\ell=k}^{\frac{n}{2}} 1 &= \sum_{k=2}^{\frac{n}{2}} \left[\frac{n+2}{2} - k \right] \\
 &= \sum_{k=1}^{\frac{n-2}{2}} [k] \\
 &= \frac{n(n-2)}{8}.
 \end{aligned}$$

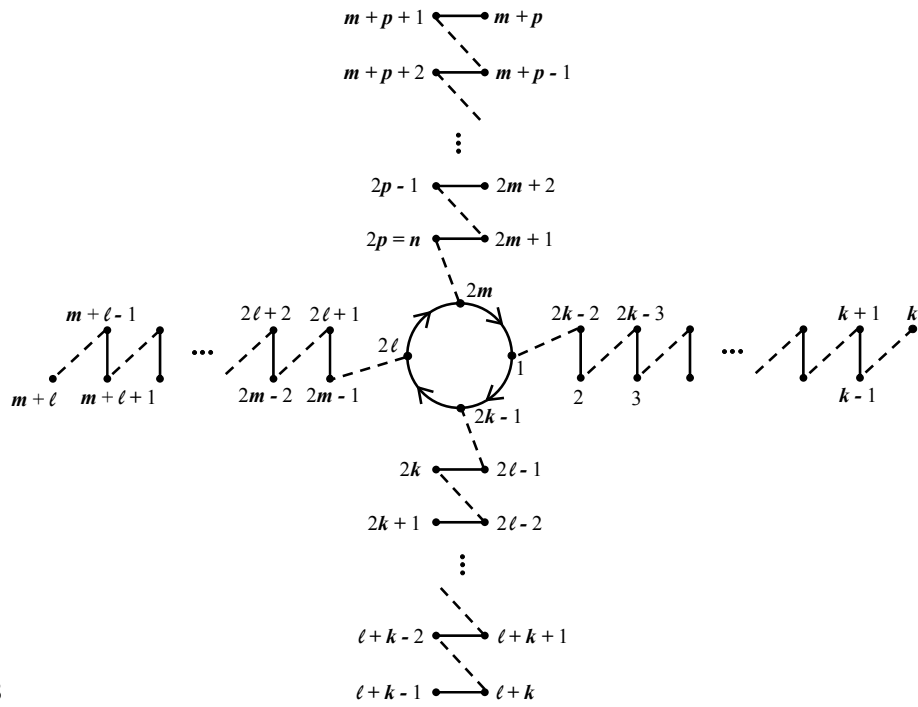
□

Proof of Theorem VIII.8. We draw the graphs associated to the action of a (a 3-cycle, and $\frac{n-4}{2}$ 2-cycles) and b ($\frac{n-2}{2}$ 2-cycles). There are two possible structures because of symmetry. We again know by Lemma VIII.14 that the graph must have the 4-cycle in the center and branches of two cycles off from them. The two branches that end in fixed points of a can either be adjacent, or opposite each other. So the two possible graphs are:

or

In the case that the two fixed points are on adjacent branches, there is no symmetry in the count. In this case if $ab = (1\ 2\ 3 \dots n)$ then up to S_n conjugacy, the element a is the product of the cycles

$$\begin{aligned}
 a &= (1, 2k-1, 2\ell-1, 2m)(2, 2k-2)(3, 2k-3) \cdots (k-1, k+1) \\
 &(2k, 2\ell-2) \cdots (\ell+k-2, \ell+k)(2\ell, 2m-1) \cdots (m+\ell-1, m+\ell) \\
 &(2m+1, 2p) \cdots (m+p, m+p+1),
 \end{aligned}$$



label:slide3

Figure 8.5: The First Graph of Actions in Theorem VIII.8

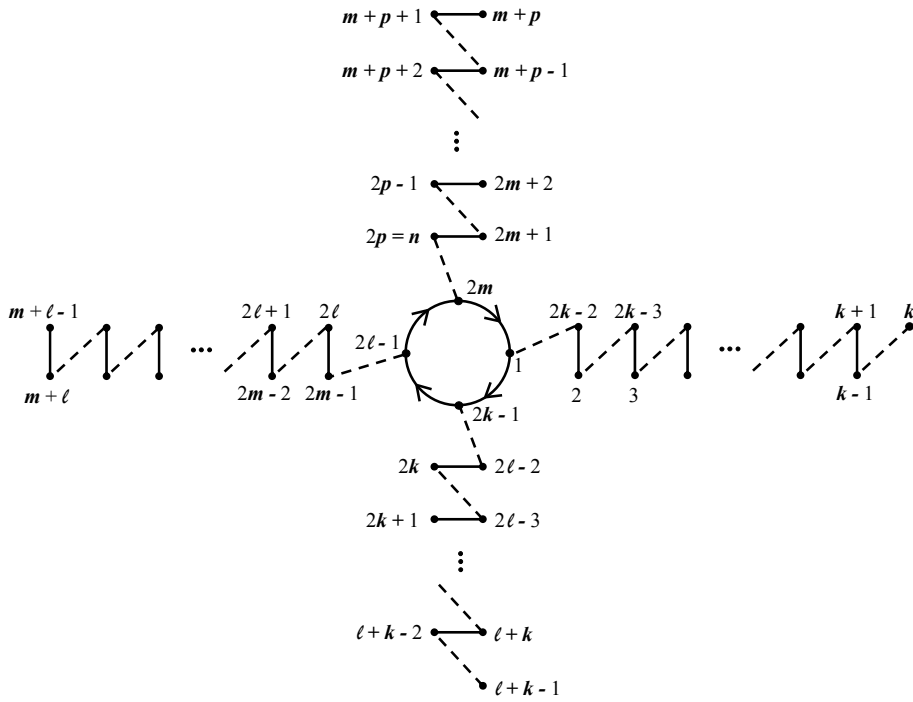


Figure 8.6: The Second Graph of Actions in Theorem VIII.8

and the element b is the product of the cycles

$$\begin{aligned} b &= (1, 2k - 2)(2, 2k - 3) \cdots (k - 1, k) \\ &(2k - 1, 2\ell - 2) \cdots (\ell + k - 2, \ell + k - 1) \\ &(2\ell - 1\ell, 2m - 1) \cdots (m + \ell - 2, m + \ell) \\ &(2m, 2p) \cdots (m + p - 1, m + p + 1) \end{aligned}$$

for any integers k, ℓ, m , and p satisfying

$$2 \leq k < \ell \leq m \leq p = \frac{n}{2}.$$

So we need only count the number of choices of k, ℓ , and m satisfying the above inequality. Like before, we denote $\text{Tri}(x) = \frac{x(x+1)}{2}$ the triangle number. This is:

$$\begin{aligned} \sum_{k=2}^{\frac{n-2}{2}} \sum_{\ell=k+1}^{\frac{n}{2}} \sum_{m=\ell}^{\frac{n}{2}} 1 &= \sum_{k=2}^{\frac{n-2}{2}} \sum_{\ell=k+1}^{\frac{n}{2}} \left[\frac{n+2}{2} - \ell \right] \\ &= \sum_{k=2}^{\frac{n-2}{2}} \sum_{\ell=1}^{\frac{n+2}{2}-k} [\ell] \\ &= \sum_{k=2}^{\frac{n-2}{2}} \left[\text{Tri} \left(\frac{n+2}{2} - k \right) \right] \\ &= \sum_{k=2}^{\frac{n-4}{2}} [\text{Tri}(k)] \\ &= \sum_{k=2}^{\frac{n-4}{2}} \left[\frac{k(k+1)}{2} \right] \\ &= \frac{n^3 - 28n - 95}{48}. \end{aligned}$$

In the second case, there is usually a unique way of choosing the branch which attaches to the vertex numbered 1. We can always choose it to be a branch with a fixed point at the end. Furthermore, we choose it such that $k - 1 \geq m - \ell$. In the case that $k - 1 = m - \ell$ we can still choose our branches such that $\ell - k \geq p - m$, which

are the number of 2-cycles in the branches which do not have fixed points at the end.

These conditions give us the following counts. First the case where $k - 1 > m - \ell$:

$$\begin{aligned} \sum_{k=2}^{\frac{n-2}{2}} \sum_{\ell=k}^{\frac{n-2}{2}} \sum_{\substack{m=\ell+1 \\ k-1 \neq m-\ell}}^{\min\{n/2, k-2+\ell\}} 1 &= \\ &= \sum_{k=2}^{\frac{n-2}{2}} \left[\sum_{\ell=k}^{\frac{n}{2}-k+2} (k-2) + \sum_{\ell=\frac{n}{2}-k+3}^{\frac{n-2}{2}} \left(\frac{n}{2} - \ell \right) \right]. \end{aligned}$$

The conclusion of this calculation depends on whether n is divisible by 4 or not. We

first continue by assuming that n is divisible by 4:

$$\begin{aligned} &= \sum_{k=2}^{\frac{n}{4}+1} \left[\sum_{\ell=k}^{\frac{n}{2}-k+2} (k-2) + \sum_{\ell=\frac{n}{2}-k+3}^{\frac{n-2}{2}} \left(\frac{n}{2} - \ell \right) \right] + \sum_{k=\frac{n}{4}+2}^{\frac{n-2}{2}} \sum_{\ell=\frac{n}{2}-k+2}^{\frac{n-2}{2}} \left[\frac{n}{2} - \ell \right] \\ &= \frac{(n-4)(5n^2 - 58n + 192)}{192}. \end{aligned}$$

If instead n were even but not divisible by 4 we would have:

$$\begin{aligned} &= \sum_{k=2}^{\frac{n+2}{4}} \left[\sum_{\ell=k}^{\frac{n}{2}-k+2} (k-2) + \sum_{\ell=\frac{n}{2}-k+3}^{\frac{n-2}{2}} \left(\frac{n}{2} - \ell \right) \right] + \sum_{k=\frac{n+2}{4}+1}^{\frac{n-2}{2}} \sum_{\ell=\frac{n}{2}-k+2}^{\frac{n-2}{2}} \left[\frac{n}{2} - \ell \right] \\ &= \frac{(n-6)(5n^2 - 48n + 124)}{192}. \end{aligned}$$

Finally, we count the cases where $k - 1 = m - \ell$ while $\ell - k \geq p - m$. We first handle the case where n is divisible by 4:

$$\begin{aligned} \sum_{k=2}^{\frac{n}{4}+1} \sum_{\ell \geq \max(k, \frac{p+1}{2})}^{\frac{n}{2}-k+1} 1 &= \\ &= \sum_{k=2}^{\frac{n}{4}+1} \min\left(\frac{n}{2} - 2k + 2, \frac{n}{4} - k + 1\right) \\ &= \sum_{k=2}^{\frac{n}{4}+1} \left[\frac{n}{4} - k + 1 \right] \\ &= \frac{n(n-4)}{32}. \end{aligned}$$

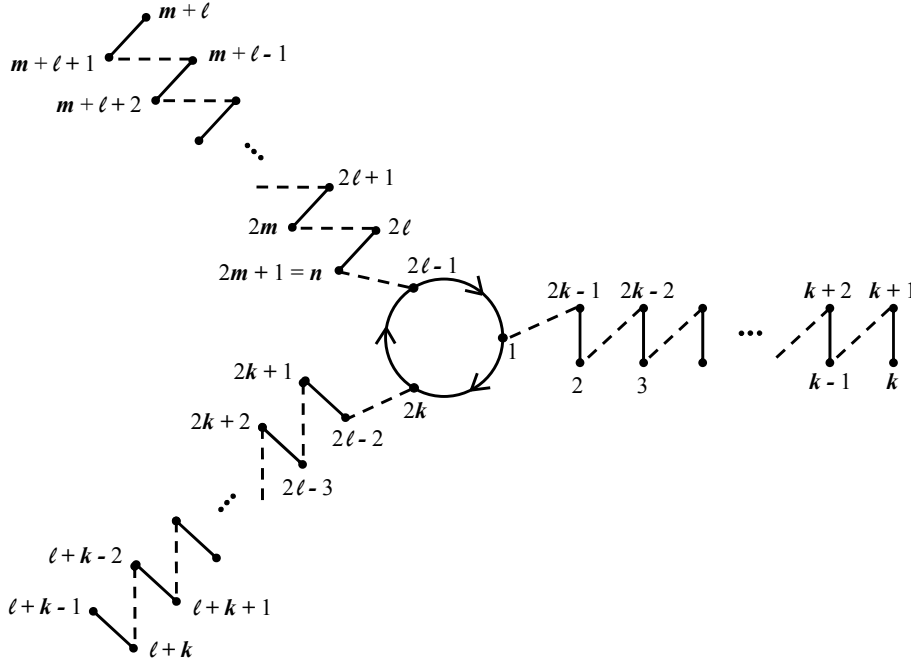


Figure 8.7: The Graph of Actions in Theorem VIII.9

If n is even but not divisible by 4 we instead have:

$$\begin{aligned}
 \sum_{k=2}^{\frac{n+2}{4}} \sum_{\ell \geq \max(k, \frac{n+1}{2})}^{\frac{n}{2}-k+1} 1 &= \\
 &= \sum_{k=2}^{\frac{n+2}{4}} \min\left(\frac{n}{2} - 2k + 2, \frac{n+6}{4} - k\right) \\
 &= \sum_{k=2}^{\frac{n+2}{4}} \left[\frac{n+6}{4} - k \right] \\
 &= \frac{(n+2)(n-2)}{32}.
 \end{aligned}$$

Summing these results gives us the stated total. □

Proof of Theorem VIII.9. We draw the graph associated to the action of a (a 3-cycle, and $\frac{n-3}{2}$ 2-cycles) and b ($\frac{n-3}{2}$ 2-cycles). There are several possible symmetries of this graph depending on which branch is longest and which is shortest. Without loss of generality we choose the branch attaching to the vertex labeled 1 to be a longest branch. Then if none of the branch lengths are equal, there is no longer symmetry,

and in fact there are two cases depending on whether the branch attached to $2k$ is shortest or not. If two branches are longest (or two are shortest) then there is no symmetry, and we need to be careful not to double count these cases. Our drawing shows that

$$1 \leq k < \ell \leq m + 1 = \frac{n + 1}{2}.$$

Furthermore, our assumption that the branch attached to the vertex labeled 1 is longest is equivalent to the two assumptions that

$$k - 1 \geq \ell - k - 1$$

and

$$k - 1 \geq m - \ell + 1.$$

Summing those bounds we see that $k \geq \frac{n}{6} + 6$. Since n is not even this bound is one of

$$k \geq \frac{n + 1}{6} + 1 \text{ if } n \equiv 5 \pmod{6}$$

$$k \geq \frac{n + 3}{6} + 1 \text{ if } n \equiv 3 \pmod{6}$$

$$k \geq \frac{n + 5}{6} + 1 \text{ if } n \equiv 5 \pmod{6}.$$

Simply based on these bounds, we have the sum:

$$\sum_{k=\lceil \frac{n}{6} \rceil + 1}^{\frac{n-1}{2}} \sum_{\ell=\max(k+1, \frac{n+3}{2}-k)}^{\min(2k, \frac{n+1}{2})} 1.$$

However, we wish to not double count the cases with symmetries. It is easiest to first count all the cases where no two branches have the same length. We must change the bounds then to:

$$k - 1 > \ell - k - 1$$

and

$$k - 1 > m - \ell + 1,$$

or equivalently

$$k - 1 \geq \ell - k$$

and

$$k - 1 \geq m - \ell + 2.$$

Furthermore, we need it to be such that

$$\ell - k - 1 \neq m - \ell + 1$$

$$2\ell \neq m + k + 2$$

$$2\ell \neq \frac{n+3}{2} + k$$

$$\ell \neq \frac{n+3}{4} + \frac{k}{2}.$$

We have that

$$k + 1 \leq \frac{n+3}{4} + \frac{k}{2} \leq \frac{n+1}{2}$$

with equalities if and only if $k = \frac{n-1}{2}$. Therefore, we must subtract 1 from our double

sum to account for the case that $\ell = \frac{n+3}{4} + \frac{k}{2}$. So we have the sum

$$\begin{aligned} & \sum_{k=\lfloor \frac{n}{6} \rfloor + 1}^{\frac{n-1}{2}} \left[\sum_{\ell=\max(k+1, \frac{n+3}{2}-k)+1}^{\min(2k, \frac{n+1}{2})-1} (1) - 1 \right] = \\ & = \sum_{k=\lfloor \frac{n}{6} \rfloor + 1}^{\lfloor \frac{n+1}{4} \rfloor} \left[\sum_{\ell=k+2}^{\frac{n-1}{2}} (1) - 1 \right] + \sum_{k=\lfloor \frac{n+1}{4} \rfloor + 1}^{\frac{n-1}{2}} \left[\sum_{\ell=\frac{n+5}{2}-k}^{2k-1} (1) - 1 \right] \\ & = \frac{13}{72}n^2 + \begin{cases} \frac{313}{72} - \frac{55}{36}n & \text{if } n \equiv 1 \pmod{12} \\ \frac{21}{8} - \frac{17}{12}n & \text{if } n \equiv 3 \pmod{12} \\ \frac{109}{72} - \frac{29}{36}n & \text{if } n \equiv 5 \pmod{12} \\ \frac{277}{72} - \frac{55}{36}n & \text{if } n \equiv 7 \pmod{12} \\ \frac{25}{8} - \frac{17}{12}n & \text{if } n \equiv 9 \pmod{12} \\ \frac{1}{72} - \frac{29}{36}n & \text{if } n \equiv 11 \pmod{12}. \end{cases} \end{aligned}$$

There are three cases where at least two branches have the same length. They are when all branches have equal length; when two branches are the same length and longer than the third; when two branches are the same length and shorter than the third. Continuing to assume that the branch attached to the vertex labeled 1 is always a longest branch, these cases can be expressed as:

$$k - 1 = \ell - k - 1 = m - \ell + 1$$

or

$$k - 1 = \ell - k - 1 > m - \ell + 1$$

or

$$k - 1 > m - \ell + 1 = \ell - k - 1.$$

In the first case, we have that

$$k = \frac{n+3}{6}, \text{ and } \ell = \frac{n+3}{3}.$$

This case can only occur when $n \equiv 3 \pmod{6}$, and will occur exactly once. In the second case we have that

$$k > \frac{n+3}{6}, \text{ and } \ell = 2k.$$

Finally, the last case has

$$k > \frac{n+3}{6}, \text{ and } \ell = \frac{n+3}{4} - \frac{k}{2}.$$

These possibilities are easy to total as there is exactly one possibility for each value of k , and indeed we have that the total from these three cases is:

$$\begin{aligned} & \frac{5}{12}n - \frac{5}{12} \text{ if } n \equiv 1 \pmod{12} \\ & \frac{5}{12}n - \frac{1}{4} \text{ if } n \equiv 3 \pmod{12} \\ & \frac{5}{12}n - \frac{13}{12} \text{ if } n \equiv 5 \pmod{12} \\ & \frac{5}{12}n + \frac{1}{12} \text{ if } n \equiv 7 \pmod{12} \\ & \frac{5}{12}n - \frac{3}{4} \text{ if } n \equiv 9 \pmod{12} \\ & \frac{5}{12}n - \frac{7}{12} \text{ if } n \equiv 11 \pmod{12}. \end{aligned}$$

Summing our results gives the stated total. □

Proof of Theorem VIII.10. The Riemann existence theorem implies that the number of equivalence classes of such polynomials is equal to the number of equivalence classes of tuples $(a, b, c) \in \mathfrak{S}_n^3$ such that abc is an n -cycle, a is a product of $\frac{n-3}{2}$ 2-cycles, b is a product of $\frac{n-1}{2}$ 2-cycles, and c is a 2-cycle. We consider two such tuples (a, b, c) and $(\bar{a}, \bar{b}, \bar{c})$ equivalent if there is an element $g \in S_n$ such that

$$a = g\bar{a}g^{-1}, \quad b = g\bar{b}g^{-1}, \quad c = g\bar{c}g^{-1}.$$

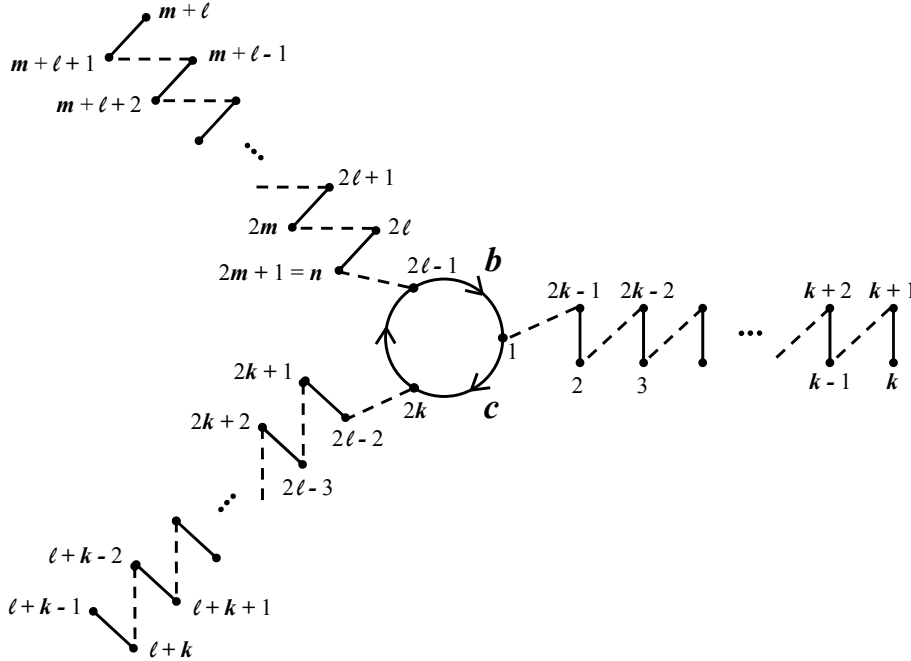


Figure 8.8: The First Graph of Actions in Theorem VIII.10

Based on the structure of b and c it must be that either bc is a 3-cycle together with $\frac{n-3}{2}$ 2-cycles, or bc is a 4-cycle with $\frac{n-5}{2}$ 2-cycles. The three possible figures associated to these situations are Figures 8.8, 8.9, and 8.10.

We must count the differences in Figures 8.9 and 8.10 because while we can choose without loss of generality that the fixed point connects to the vertex labeled 1, we can not choose whether c acts on 1 or not.

However, the counts of possibilities from Figures 8.9 and 8.10 are identical, and have been done before. We therefore cite from Theorem VIII.4 that combined there are

$$\frac{(n-5)(n-3)(n-1)}{24}$$

possibilities contributed from these two cases.

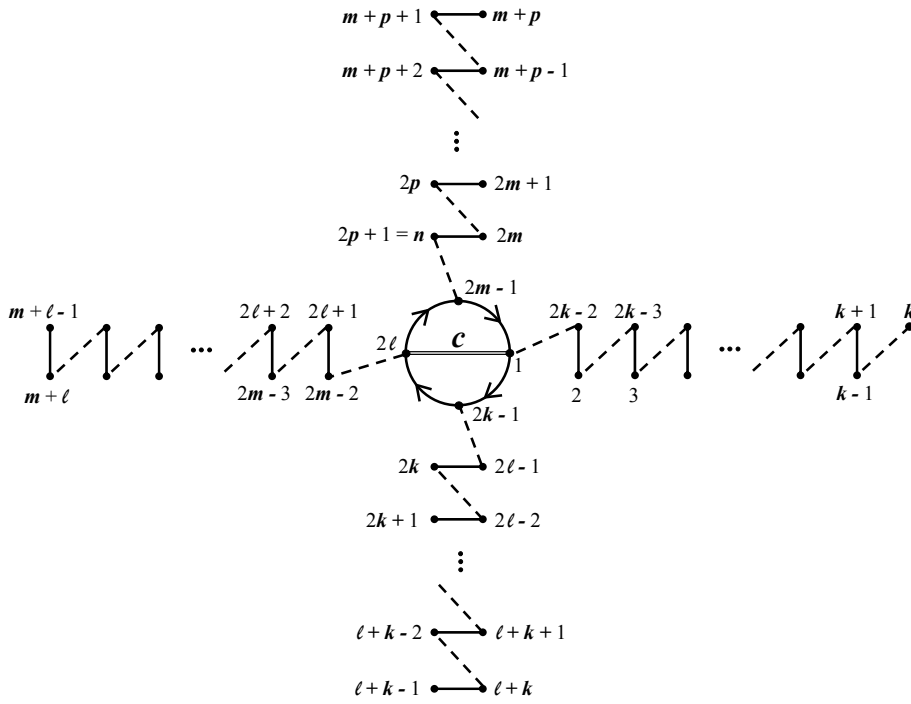


Figure 8.9: The Second Graph of Actions in Theorem VIII.10

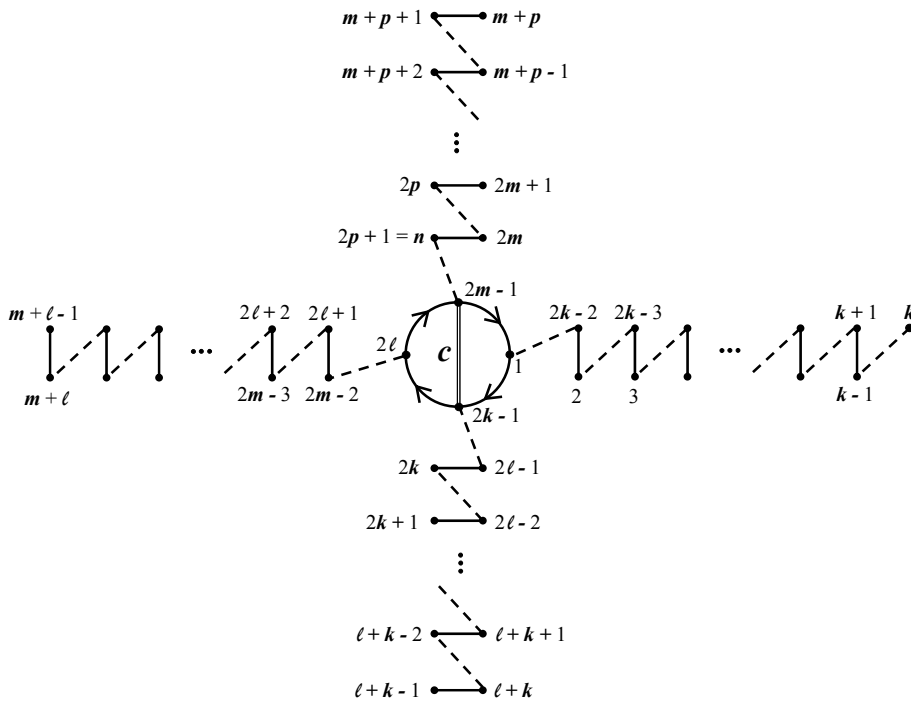


Figure 8.10: The Third Graph of Actions in Theorem VIII.10

The number of possible graphs of the type in Figure 8.8 is similar to the case of Theorem VIII.9, however we can now uniquely choose 1 to be the vertex of the three cycle that is acted on by both b and c . We choose (without loss of generality) that $2k$ is the fixed point of b . Then the three branches can have any length so long as

$$1 \leq k < \ell \leq m + 1 = \frac{n + 1}{2}.$$

So the number of such cases is:

$$\sum_{k=1}^{\frac{n-1}{2}} \sum_{\ell=k+1}^{\frac{n+1}{2}} 1 = \frac{n^2 - 1}{8}.$$

Therefore the total is

$$\frac{n^2 - 1}{8} + \frac{(n - 5)(n - 3)(n - 1)}{24} = \frac{n^3 - 9n^2 + 23n + 57}{24}. \quad \square$$

Proof of Theorem VIII.11. The Riemann existence theorem implies that the number of equivalence classes of such polynomials is equal to the number of equivalence classes of tuples $(a, b, c) \in \mathfrak{S}_n^3$ such that abc is an n -cycle, a is a product of $\frac{n-2}{2}$ 2-cycles, b is a product of $\frac{n-2}{2}$ 2-cycles, and c is a 2-cycle. We consider two such tuples (a, b, c) and $(\bar{a}, \bar{b}, \bar{c})$ equivalent if there is an element $g \in S_n$ such that

$$a = g\bar{a}g^{-1}, \quad b = g\bar{b}g^{-1}, \quad c = g\bar{c}g^{-1}.$$

Based on the structure of b and c it must be that either bc is $\frac{n}{2}$ 2-cycles, or bc is a 3-cycle with $\frac{n-4}{2}$ 2-cycles, or bc is a 4-cycle with $\frac{n-6}{2}$ 2-cycles. There are many possible graphs in the second two cases.

When bc is $\frac{n}{2}$ 2-cycles, the graph of actions looks like:

Thus, the only possible differences in such graphs is which vertical line is due to c , and so there are $\frac{n}{2}$ such graphs.

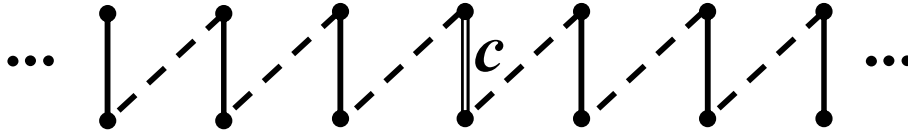


Figure 8.11: The Graph of All 2-cycles in Theorem VIII.11

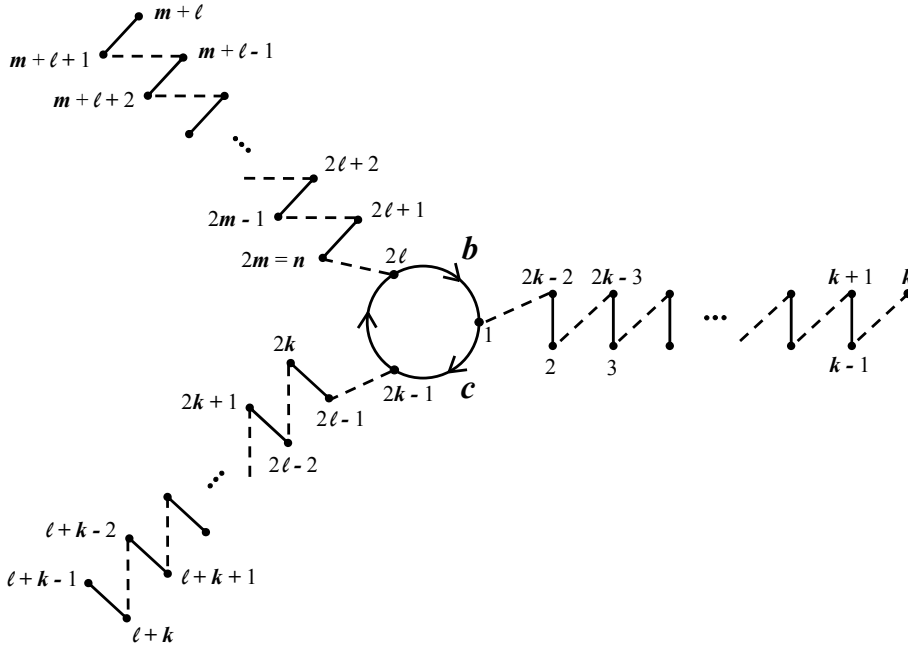


Figure 8.12: The First Graph with a 3-cycle in Theorem VIII.11

When bc is a 3-cycle with $\frac{n-4}{2}$ 2-cycles, there are three possible graphs. Without loss of generality, we assume that 1 is the vertex of the three cycle whose branch connects to the fixed point of bc . Therefore, the graphs differ on whether b and c both act on 1, whether just b acts on 1, or whether just c acts on 1.

Each graph has no symmetry, just like in Theorem VIII.7. So by tripling the result from Theorem VIII.7 we have that there are

$$\frac{3n(n-2)}{8}$$

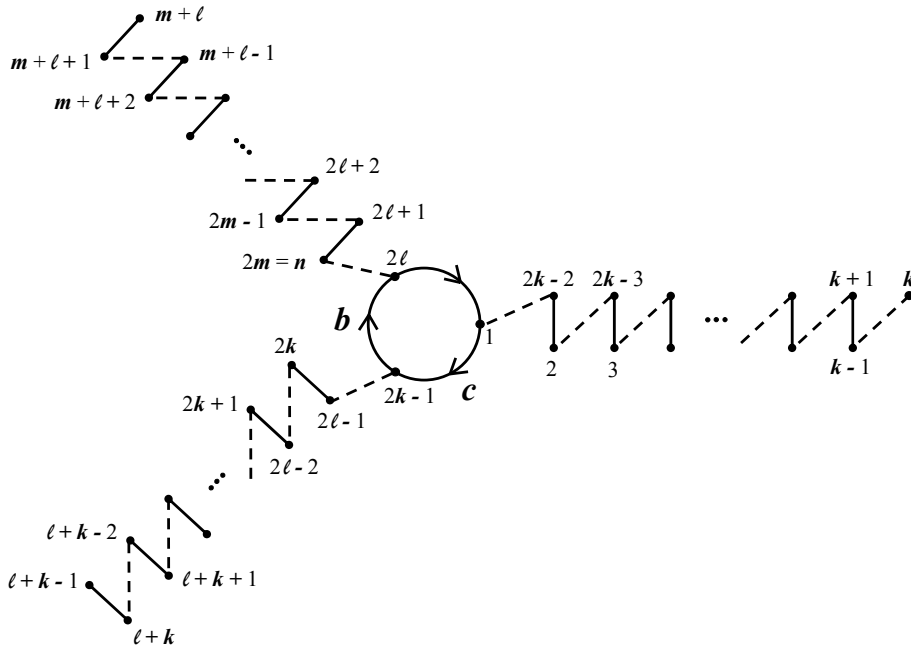


Figure 8.13: The Second Graph with a 3-cycle in Theorem VIII.11

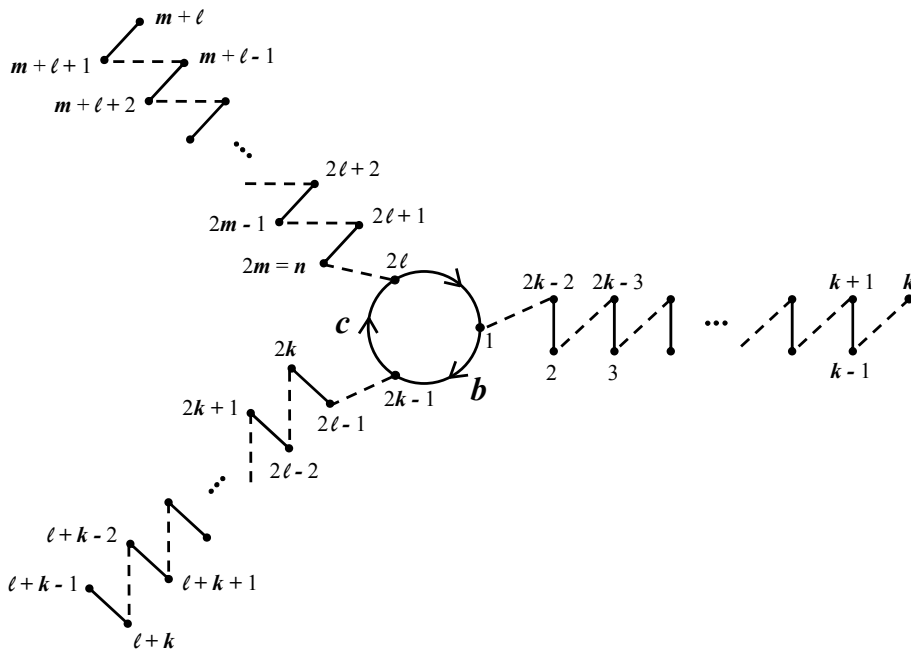


Figure 8.14: The Third Graph with a 3-cycle in Theorem VIII.11

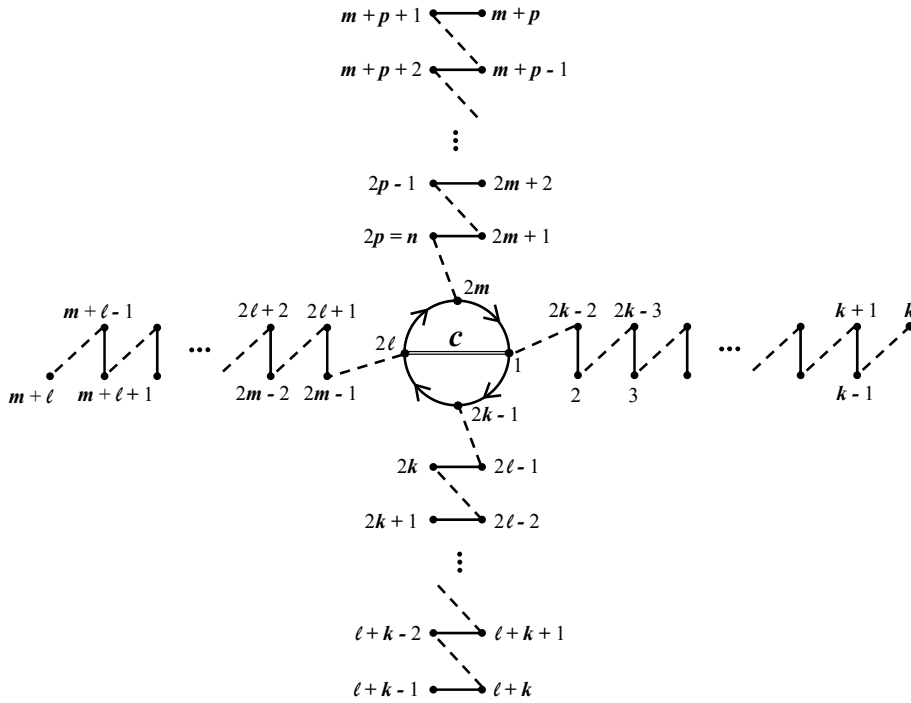


Figure 8.15: The First Graph with a 4-cycle in Theorem VIII.11

possible cases in these three graphs combined.

Finally, when bc is a 4-cycle with $\frac{n-6}{2}$ 2-cycles, there are four possible graphs. We are allowed to assume without loss of generality that the vertex 1 is one of the vertices in the 4-cycle whose branch has a fixed point at the end. However, the graphs differ on whether $2k - 1$ or $2l - 1$ is the other vertex of the 4-cycle whose branch has a fixed point at the end, and whether or not c acts on 1 or acts on $2k - 1$.

The combination of the two graphs which have c acting on 1 are identical to Theorem VIII.8. Likewise, the combination of the other two graphs (where c does

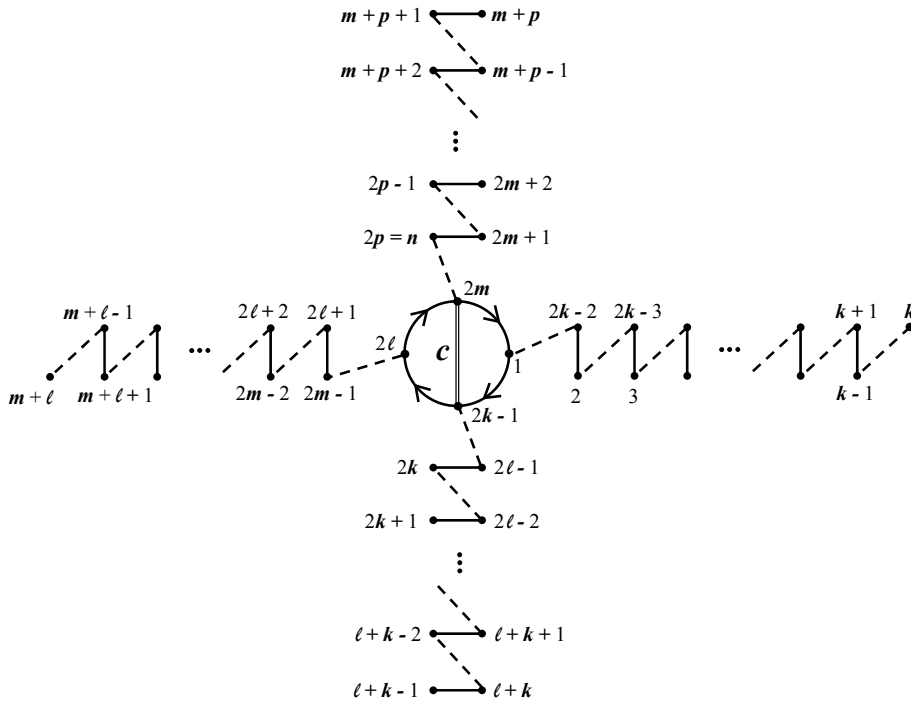


Figure 8.16: The Second Graph with a 4-cycle in Theorem VIII.11

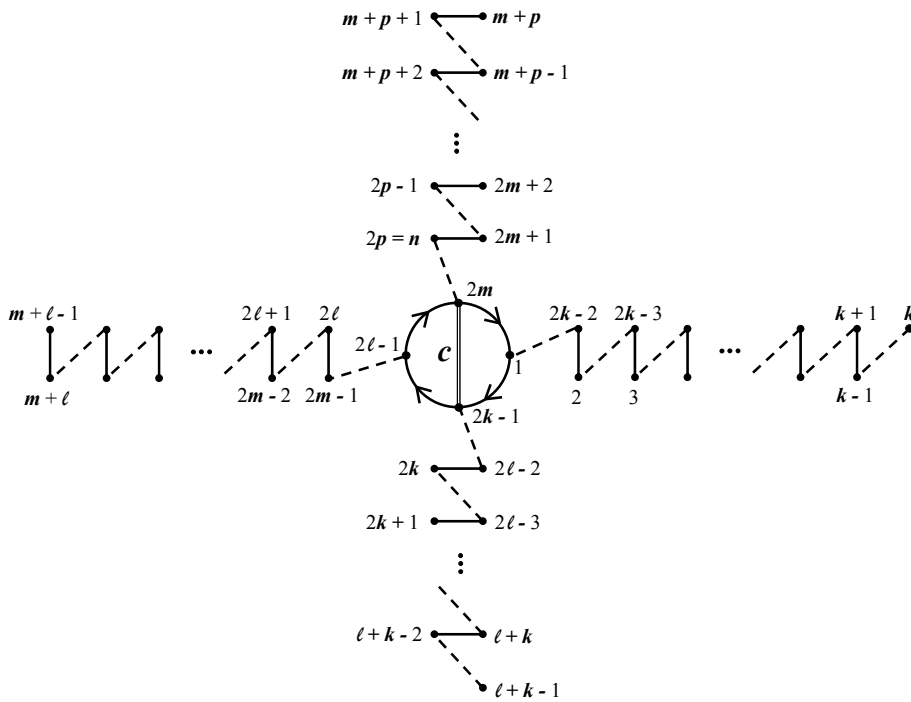


Figure 8.17: The Third Graph with a 4-cycle in Theorem VIII.11

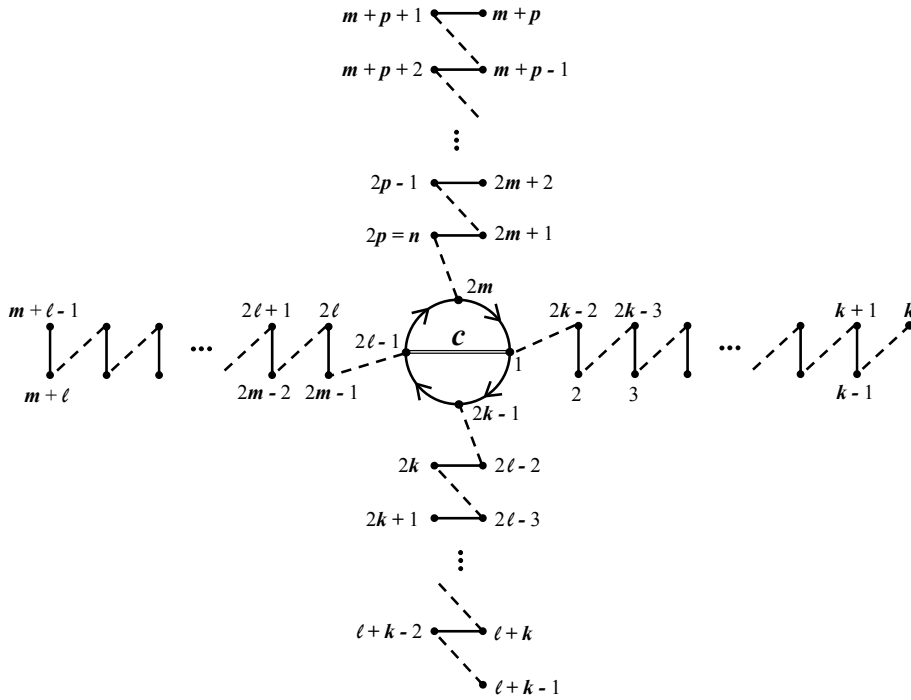


Figure 8.18: The Fourth Graph with a 4-cycle in Theorem VIII.11

not act on 1) are identical to Theorem VIII.8. So all together we double the result from Theorem VIII.8 and have that there are

$$\begin{aligned} & \frac{3}{32}n^3 - \frac{3}{4}n^2 + 3n - \frac{287}{24} \text{ if } n \equiv 0 \pmod{4} \\ & \frac{3}{32}n^3 - \frac{3}{4}n^2 + \frac{25}{8}n - \frac{287}{24} \text{ if } n \equiv 2 \pmod{4} \end{aligned}$$

possibilities with bc containing a 4-cycle. By summing over all these results, we have the stated count. □

8.7 Multiplicity Results Counting Indecomposable Polynomials

We now briefly address how to modify the above calculations to count the number of equivalence classes of indecomposable polynomials having a given ramification type.

Definition VIII.15. The two *trivial partitions* of a finite set $\{1, 2, \dots, n\}$ are the partition $\{1, 2, \dots, n\}$, and the partition $\{1\}, \{2\}, \dots, \{n\}$.

Definition VIII.16. A subgroup $G \subset S_n$ is *primitive* if there is no non-trivial partition Λ of $\{1, 2, \dots, n\}$ such that for all $g \in G$ for all $B \in \Lambda$, it holds that $g(B) \in \Lambda$.

Theorem VIII.17. For $f \in \mathbb{K}[X]$, $f(X)$ is indecomposable over \mathbb{K} if and only if $\text{Gal}(f(X) - T/\mathbb{K}(T))$ is primitive.

Lemma VIII.18. Let Λ be a non-trivial partition of $\{1, 2, 3, \dots, n\}$ such that for all $B \in \Lambda$ it holds that $(1 \ 2 \ \dots \ n)(B) \in \Lambda$. Then Λ is the partition into the residue classes modulo d for some integer d which divides n .

Proof. Let $B \in \Lambda$ be the set containing 1. If there are no other elements in B , then Λ must be a trivial partition. Assume that $\{a\} \in \Lambda$. Then since the action $\{1, 2, 3, \dots, n\}$ preserves Λ it must be that $\{a + 1\} \in \Lambda$. So by induction, if $\{1\} \in \Lambda$ then Λ is trivial.

We therefore know there is a smallest element of B which is greater than 1. Denote this element a . It must be that $a - 1$ actions by $(1, 2, 3, \dots, n)$ map B to itself (since it maps 1 to a) and so it must be that B also contains $2a - 1$. We continue by induction, and see that B contains the set $\{k(a - 1) + 1 \pmod{n} \mid k \in \mathbb{Z}\}$. However, the only way that this set is not all of $\{1, 2, \dots, n\}$ is if $a - 1$ divides n , and so the set B is the set of elements which are congruent to 1 modulo $a - 1$. We again see that since Λ is preserved by the action $(1, 2, 3, \dots, n)$ it must be that the other sets in Λ are the other residue classes modulo $a - 1$. \square

We will now show how these results apply by modifying the calculation from Theorem VIII.4 to only consider equivalence classes of indecomposable polynomials.

Example VIII.19. We wish to count equivalence classes of $(a, b) \in S_n^2$ with ab an n -cycle such that there are no non-trivial partitions of $\{1, 2, 3, \dots, n\}$ such that

a , b , and $(1\ 2\ 3\ \dots\ n)$ preserve the partition. Since $\{1, 2, 3, \dots, n\}$ only preserves congruences modulo p , we need only concern ourselves when a and b preserve modulo p congruences (for any prime p dividing n).

The element a was shown to be the product of the cycles

$$\begin{aligned} a = & (1, 2k + 1, 2\ell + 2, 2m + 3)(2, 2k - 2)(3, 2k - 3) \cdots (k - 1, k + 1) \\ & (2k, 2\ell - 1) \cdots (\ell + k - 1, \ell + k)(2\ell + 1, 2m - 2) \cdots (m + \ell - 1, m + \ell) \\ & (2m, 2r + 1) \cdots (m + r, m + r + 1), \end{aligned}$$

and the element b was shown to be the product of the cycles

$$\begin{aligned} b = & (1, 2k - 2)(2, 2k - 3) \cdots (k - 1, k) \\ & (2k - 1, 2\ell - 1) \cdots (\ell + k - 2, \ell + k) \\ & (2\ell, 2m - 2) \cdots (m + \ell - 2, m + \ell) \\ & (2m - 1, 2r + 1) \cdots (m + r - 1, m + r + 1) \end{aligned}$$

for any integers k, ℓ, m , and r satisfying

$$2 \leq k \leq \ell < m \leq \frac{n+1}{2}, \text{ and } r = \frac{n-1}{2}.$$

The congruences arising from these cases are

$$k \equiv m \pmod{p} \text{ and } \ell \equiv \frac{1}{2} \pmod{p}.$$

So we need to eliminate the cases from our count when both of these occur. For any integer k , there are $\left\lfloor \frac{\frac{n+1}{2} - k}{p} \right\rfloor$ options for m , and given k and m which are congruent modulo p there are $\frac{m-k}{p}$ options for ℓ .

After doing this count for each prime dividing n , it would be necessary to use inclusion–exclusion to count the total number of cases which are eliminated over all primes dividing n .

CHAPTER IX

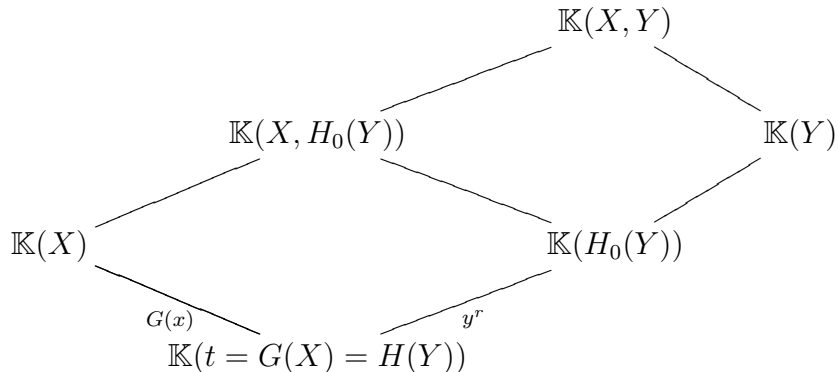
Powers of Non-Linear Polynomials

In this chapter we present our results in the classification of irreducible curves of genus 0 defined by $G(X) - H(Y)$ in the case when $H(Y) = H_0(Y)^r$, with $r > 1$ and $\deg(H_0(Y)) > 1$. As usual, \mathbb{K} is an algebraically closed field of characteristic zero.

Lemma IX.1. *Let $G(X)$ and $H(Y)$ be polynomials with coefficients in $\overline{\mathbb{Q}}$ such that $H(Y) - G(X)$ is irreducible, and $H(Y) = H_0(Y)^r$ with $r > 1$. If the curve $\mathcal{C}: H(Y) = G(X)$ is genus 0 then $G(X)$ is in one of the following infinite families:*

1. $(X - x_0)^a F(X)^r$, for any positive integer a which is coprime to r , any constant x_0 , and any polynomial $F(X) \in \mathbb{K}[X]$;
2. $(X - x_1)^a (X - x_2)^{r-a} F(X)^r$, for any integer $1 \leq a < r$ which is coprime to r , any constants $x_1 \neq x_2$, and any polynomial $F(X) \in \mathbb{K}[X]$.

Proof. We have the following diagram of function fields of curves:



Note however that the function field $\mathbb{K}(X, H_0(Y))$ is associated to a genus 0 curve (since $\mathbb{K}(X, Y)$ is associated to a genus 0 curve). Also note that the curve is defined by $Y^r = G(X)$. Therefore by Theorem III.1 we know that $G(X)$ must be in one of these infinite families. \square

Lemma IX.2. *Let $G(X)$ and $H(Y)$ be polynomials with coefficients in $\overline{\mathbb{Q}}$ such that $H(Y) = H_0(Y)^r$ with $r > 0$, and $H_0(Y)$ not equivalent to a power of a smaller degree polynomial and $G(X) = (X - x_1)^a F(X)^r$ with $(a, r) = 1$. Then $G(X) - H(Y)$ defines an irreducible curve of genus zero if and only if $(G(X), H(Y))$ is equivalent to a pair of polynomials in the collection \mathcal{T}_1 (defined below).*

Definition IX.3. We let \mathcal{T}_1 be the following collection of infinite families and sporadic examples of pairs of polynomials:

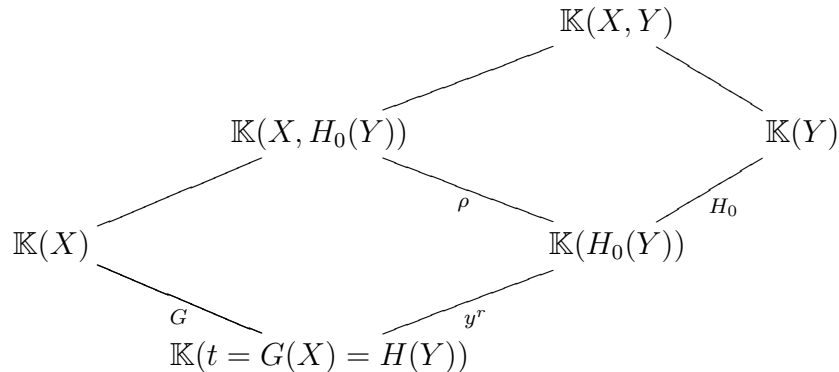
1. $G(X) = (X - x_1)^s$, for any $x_1 \in \mathbb{K}$ and $(r, s) = 1$:
 - (a) $H(Y) = [(Y - y_1)^a F(Y)^s]^r$ with $(a, s) = 1$ and $y_1 \in \mathbb{K}$ and any non-constant polynomial $F(Y)$;
 - (b) $H(Y) = [(Y - y_1)^a (Y - y_2)^{s-a} F(Y)^s]^r$ with $(a, s) = 1$ and y_1 and y_2 non-equal constants, and any polynomial $F(Y)$.
2. $G(X) = (X - x_1)^3 (X - x_2)$ for any distinct constants x_1 and x_2 . While $H(Y) = H_0(Y)^3$ such that the only branch point besides zero is the other branch point of $G(X)$ and has ramification structure $[2^3, 1^6]$.
3. $G(X) = (X - x_1)^4 (X - x_2)$ for any distinct constants x_1 and x_2 . While $H(Y) = H_0(Y)^2$ such that the only branch point besides zero is the other branch point of $G(X)$ and has ramification structure $[2^2, 1^6]$, while over the branch point of zero $H(Y)$ has ramification $[4^2, 2]$.

4. $G(X) = (X - x - 1)(X - x_2)^2(X - x_3)^2$ and has exactly one other branch point. The other branch point has ramification $[3, 1^2]$. While $H(Y) = H_0(Y)^2$ such that the only non-zero branch point is the same point as the other branch point of $G(X)$. The ramification of $H(Y)$ over this point is $[3^2, 1^4]$ while its ramification over zero is $[2^5]$.

5. $G(X) = (X - x - 1)(X - x_2)^2(X - x_3)^2$ and has exactly one other branch point of with the same ramification. $H(Y) = H_0(Y)^2$ with the same branch points as $G(X)$ such that $H(Y)$ has one of the two following ramification structures:
 - (a) ramification $[4^2, 2]$ over zero and ramification $[2^2, 1^6]$ over the other point;
 - (b) ramification $[4, 2^3]$ over zero and ramification $[2^3, 1^4]$ over the other point.

6. $G(X)$ is linearly equivalent to an odd degree Chebyshev polynomial with a branch point over zero, and
 - (a) $H(Y) = H_0(Y)^2$ and has only one non-zero branch point (the same one as $G(X)$) with ramification $[2^{\frac{2-4}{2}}, 1^4]$;
 - (b) $H_0(Y)$ is in \mathcal{R}_1 with both branch points of $H_0(Y)$ mapping to the branch non-zero branch point of $G(X)$ under Y^2 .

Proof of Lemma IX.2. We have the following diagram of function fields of curves:



Note that under the stated assumptions that $\gcd(\deg(G(X)), r) = 1$. Therefore, the rational function ρ is totally ramified over infinity, and so ρ is a polynomial.

Since we also assume that $H_0(Y)$ is not equivalent to a power of a smaller degree polynomial, we know that (ρ, H_0) is equivalent to one of the pairs classified in the previous chapters. Therefore, ρ can have at most three branch points.

Furthermore, for every branch point of $G(X)$ which is not zero, there are r branch points of ρ which have identical ramification structures, and so if $G(X)$ is not cyclic, then r is at most three.

If $G(X)$ is cyclic, then $\rho = G(X) = (X - x_1)^s$. We then apply Lemma III.1 and observe that $H(Y)$ must be one of the two possibilities in the definition of \mathcal{R}_1 which pair with X^s .

If $G(X)$ is not cyclic then it necessarily has at least one non-zero branch point. If it has two non-zero branch points, then ρ must have at least four finite branch points which is impossible by Theorem IV.1.

If $G(X)$ is not cyclic and $r = 3$, then ρ has three finite branch points with identical ramification structures. Furthermore, this ramification structure is identical to the ramification structure of $G(X)$ over its finite non-zero branch point. By Corollary IV.2 the only possible ramification structure of ρ is if each branch point has ramification structure $[2, 1^2]$. This then corresponds to case (2) of \mathcal{T}_1 .

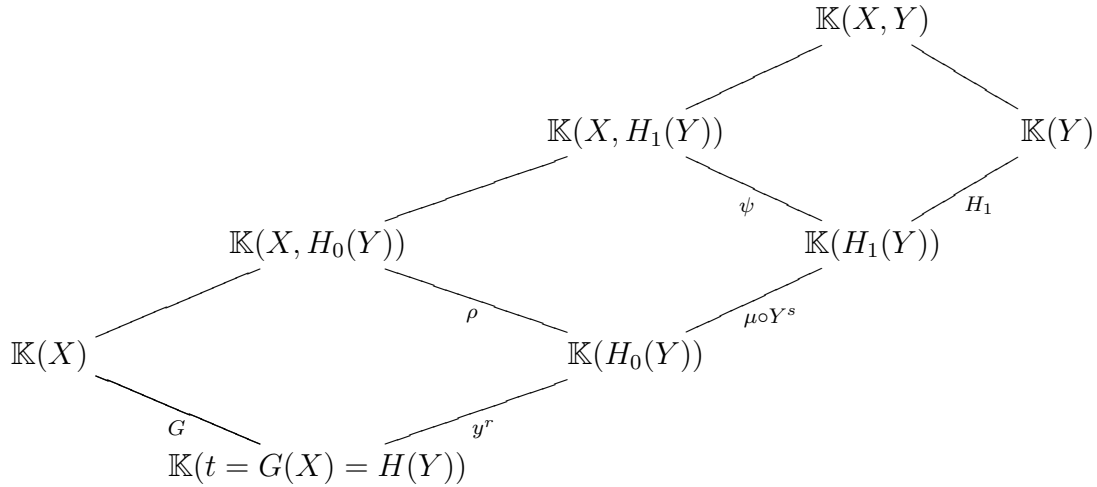
If $G(X)$ is non-cyclic and $r = 2$, then ρ has two identical branch points. If it has a third branch point over zero then again by Corollary IV.2 (and the fact that the degree of ρ must not be even) we see that the only possibility is if over zero ρ has ramification $[2^2, 1]$ and over the other two points it has ramification $[2, 1^3]$. The necessary ramification for $H_0(Y)$ leads to the polynomials being in case (3) of \mathcal{T}_1 .

If $G(X)$ is non-cyclic and $r = 2$, then ρ has two identical branch points. If it

has no other branch points, then we need only check all possibilities from Chapter V where a polynomial has two identical branch points and the other polynomial is not a power of a smaller degree polynomial. The remaining cases in \mathcal{T}_1 come from these possibilities. □

Lemma IX.4. *Let $G(X)$ and $H(Y)$ be polynomials with complex coefficients such that $G(X) - H(Y)$ is irreducible. Additionally, assume that $H(Y) = H_0(Y)^r$ with $r > 0$, and $H_0(Y) = \mu \circ Y^s \circ H_1(Y)$ for any non-constant polynomial $H_1(Y)$, and linear polynomial μ with $\mu(0) \neq 0$. If $G(X) = (X - x_1)^a \overline{G}(X)^r$ with $(a, r) = 1$ and $\deg(\overline{G}(X)) \geq 1$ then $\min(r, s) = 2$, and $r + s \leq 5$.*

Proof. We have the following diagram of function fields of curves:



Also note that from Theorem III.1 it must be that $\mu^{-1} \circ \rho$ is equal to either $(X - x_1)^a F(X)^s$ or $(X - x_1)^a (X - x_2)^{s-a} F(X)^s$ for $(a, s) = 1$. However, ρ must have identical ramification over $r - 1$ other finite points because of how it was constructed. Furthermore, we can assume that $m = \deg(G(X)) = \deg(\rho(X)) > 1$, since this trivial case has been handled.

First assume that $s \geq 2$ with $r \geq 3$ and $\mu^{-1} \circ \rho = (X - x_1)^a F(X)^s$ or $s > 3$ and $\mu^{-1} \circ \rho = (X - x_1)^a (X - x_2)^{s-a} F(X)^s$. We proceed by induction on the degree of

$F(X)$ to show that neither case can happen. We have that whatever the ramification $\mu^{-1} \circ \rho$ has over zero, it has identical ramification over $r - 1$ other points (and is totally ramified over infinity). It cannot be that $\deg(F(X)) = 0$. If it were then letting C_1, \dots, C_R be the ramification multi-sets of $\rho(X)$ we have by Lemma II.7:

$$(9.1) \quad \sum_{i=1}^R \sum_{\alpha \in C_i} [\alpha - 1] = m - 1.$$

However, when $\deg(F(X)) = 0$ and $\mu^{-1} \circ \rho = (X - x_1)^a$ the left side is at least $r(a - 1) = r(m - 1)$ because there are $r - 1$ finite branch points of ρ with identical ramification. Since r is assumed to be at least 2 the left side is greater than the right. Likewise, if $\mu^{-1} \circ \rho = (X - x_1)^a(X - x_2)^{s-a}$ then $m = s > 3$ and the left side is at least $r(s - 2) = r(m - 2)$ (again because ramification over non-zero points occurs identically over $r - 1$ other finite branch points) which is bigger than $m - 1$.

We proceed by induction. We have proven neither case can happen when the degree of $F(X) = 0$. As the degree of $F(X)$ increases by 1 the right side of equation (9.1) increases by s . However the number of points over zero of $\mu^{-1} \circ \rho$ increases by at most 1. Thus the left side of equation (9.1) increases by at least $r(s - 1)$. Since $r \geq 2$ and $s \geq 2$ this is at least s . Therefore it cannot be that $\mu^{-1} \circ \rho = (X - x_1)^a F(X)^s$ nor can it be that $\mu^{-1} \circ \rho = (X - x_1)^a(X - x_2)^{s-a} F(X)^s$ when $s > 3$.

The only cases remaining are $\mu^{-1} \circ \rho = (X - x_1)^a(X - x_2)^{s-a} F(X)^s$ with $s \in \{2, 3\}$. When $s = 3$, we claim that $r = 2$. We again proceed by induction. Assume that $r > 2$ and $\deg(F(X)) = 0$. Then in equation (9.1) the left side is at least $r(s - 2) = r$ and the right side is equal to $s - 1 = 2$. Thus equality cannot hold. Furthermore, when the degree of $F(X)$ increases by 1 the right side increases by $s = 3$ and the left side increases by at least $r(s - 1) = 2r \geq 6$.

Finally we show that if $s = 2$ that $r \leq 3$. We again proceed by contradiction, if $s = 2$ and $r \geq 3$ then $\mu^{-1} \circ \rho$ is $(X - x_1)(X - x_2)F(X)^2$. We again prove this by

induction with the base case that $\deg(F(X)) = 1$. In the case that $s = 2$ and $r \geq 3$ the right side of equation (9.1) is equal to 3 and the left side is at least $r(m - 3) \geq 3$. As the degree of $F(X)$ increases by 1 the right side of the equation increases by $s = 2$, but the left side increases by at least $r(s - 1) \geq 3$. Finally, the case that $\deg(F(X)) = 0$ implies that $\deg(G(X)) = 2$. This can only occur if $r = 2$, or if $G(X) = (X - x_0)^2$. We have assumed that this latter case cannot occur. \square

We conclude this chapter by proving two generalizations of Theorem IV.1 (see Theorem IX.7 and Theorem IX.14) for rational functions, and apply the result to prove Proposition IX.5 and Theorem IX.6.

Proposition IX.5. *Let $G(X)$ and $H(Y)$ be polynomials with complex coefficients such that $G(X) - H(Y)$ is irreducible. Additionally, assume that $H(Y) = H_0(Y)^r$ with $r > 0$ and $H_0(Y)$ not equivalent to a power of a smaller degree polynomial, and $G(X) = (X - x_1)^a(X - x_2)^{r-a}F(X)^r$ with $(a, r) = 1$. If $r \geq 3$ then it must be that $G(X)$ has only one non-zero finite branch point, and it must be that $H(Y)$ has at most three finite branch points.*

Theorem IX.6. *Let $G(X)$ and $H(Y)$ be polynomials with complex coefficients such that $G(X) - H(Y)$ is irreducible. Additionally, assume that $H(Y) = H_0(Y)^r$ with $r > 0$ and $H_0(Y)$ not equivalent to a power of a smaller degree polynomial, and $G(X) = (X - x_1)^a(X - x_2)^{r-a}F(X)^r$ with $(a, r) = 1$, and with $n|m$. Then it cannot be that $r \geq 4$.*

Theorem IX.7. *Let $H_0(Y)$ be a polynomial with complex coefficients which has at least two finite branch points and is not equivalent to a power of a smaller degree polynomial. Let $\rho(X)$ be a rational function with r points mapping to infinity—all of which have the same ramification.*

If $\rho(X) - H_0(Y)$ is irreducible, and the curve $\mathcal{C}: \rho(X) = H_0(Y)$ is genus 0, then $\rho(X)$ can have at most $r + 2$ finite branch points.

The proof of this Theorem will proceed in an identical manner to the proof of Theorem IV.1. We will let m be the degree of $\rho(X)$, and we let there be r points that ρ maps to infinity, each of ramification $\frac{m}{r}$. We will let n be such that $\deg(H_0(Y)) = \frac{n}{r}$. We will still let $d = \gcd(m, n) \geq r$.

We let ρ have S finite branch points. For each $1 \leq i \leq S$ we have the following definitions: Let A_i be the multi-set of ramification indices of ρ over the i^{th} branch point. We let ω_i be an element of A_i such that for all $\alpha \in A_i$ we have $\omega_i \geq \alpha$. We also let N_i be the number of elements in B_i (the ramification of $H_0(Y)$ over the corresponding point) which are not divisible by ω_i . Finally we let $t_i := \sum_{\beta \in B_i} [\omega_i - \gcd(\omega_i, \beta)] - (\omega_i - 1)$.

We also have the following generalizations of Lemmas II.9 and II.10.

Lemma IX.8. *Let $\rho(X)$ and $H_0(Y)$ be as in Theorem IX.7. Then*

$$\sum_{i=1}^S \sum_{\alpha \in A_i} \sum_{\beta \in B_i} [\alpha - (\alpha, \beta)] = m + d - 2.$$

Lemma IX.9. *Let $\rho(X)$ and $H_0(Y)$ be as in Theorem IX.7. Then*

$$\sum_{i=1}^S \sum_{\alpha \in A_i} \left(\sum_{\beta \in B_i} [\alpha - (\alpha, \beta)] - (\alpha - 1) \right) = d - r.$$

Lemma IX.10. *Assume that $\rho(X)$ and $H_0(Y)$ are as in Theorem IX.7, Fix a finite branch point of $\rho(X)$ with A_i the multi-set of ramification indices of $\rho(X)$ over the point, and B_i the multi-set of ramification indices of $H_0(Y)$ over the same point. Then for any $\alpha \in A_i$ we have*

$$\sum_{\beta \in B_i} [\alpha - \gcd(\alpha, \beta)] - (\alpha - 1) \geq 0,$$

with equality if and only if there is exactly one element of B_i not divisible by α .

The proof of this Lemma is identical to that of Lemma IV.6.

Lemma IX.11. *Assume that $\rho(X)$ and $H_0(Y)$ are as in Theorem IX.7. Then*

$$N_i \leq t_i + 1.$$

with equality if and only if $N_i = 1$ or $\omega_i = 2$.

Again, the proof is identical to the proof of Lemma IV.7.

Lemma IX.12. *Assume that $\rho(X)$ and $H_0(Y)$ are as in Theorem IX.7. Then*

$$\sum_{i=1}^S N_i \leq S + d - r,$$

with equality if and only if for all $1 \leq i \leq S$

- *if $N_i > 1$ then $\omega_i = 2$, and*
- *For all $\alpha \in A_i \setminus \{\omega_i\}$ we have that $\sum_{\beta \in B_i} [\alpha - \gcd(\alpha, \beta)] = \alpha - 1$.*

The proof of this is identical to the proof of Lemma IV.8, except we must reference Lemma IX.9 for the bound of the sum.

Lemma IX.13. *Assume that $\rho(X)$ and $H_0(Y)$ are as in Theorem IX.7. Then*

$$(S - 2) \frac{n}{r} \leq \sum_{i=1}^S (N_i) - 2,$$

with equality if and only if

- $\omega_i = 2$ (for all $1 \leq i \leq S$) and,
- for all $1 \leq i \leq S$ every element of B_i which is not divisible by ω_i is equal to 1, and
- for all $1 \leq i \leq S$ every element of B_i which is divisible by ω_i is equal to ω_i , and
- every branch point of $H(Y)$ is a branch point of $G(X)$.

The proof of this Lemma is identical to the proof of Lemma IV.9 with $\frac{n}{r}$ the degree of the polynomial.

Proof of Theorem IX.7. By Lemmas IX.12 and IX.13 we have that

$$(S-2)\frac{n}{r} \leq \sum_{i=1}^S (N_i) - 2 \leq S + d - r - 2$$

$$\frac{n}{r} \leq \frac{S + d - r - 2}{S - 2}.$$

By definition we have that $r \geq 2$ and $d \leq n$, and d is divisible by r (so in particular $d - r$ is non-negative). □

Theorem IX.14. *Let $\rho(X)$ be a rational function which maps $r \geq 2$ points to infinity. Additionally, let ρ be such that for any finite branch point of ρ , the ramification indices over that point are coprime. Let $H_0(Y)$ be a polynomial such that $\rho(X) - H_0(Y)$ defines an irreducible curve of genus 0. Then $H_0(Y)$ has at most two finite branch points.*

We will let m be the degree of ρ and n be such that $\frac{n}{r}$ is the degree of $H_0(Y)$. As usual, $d = \gcd(m, n)$.

Note that the sum of the ramification induced by H_0 over the r points which ρ maps to infinity is $m - d$. So we still have that

$$\sum_{i=1}^R \sum_{\beta \in B_i} \sum_{\alpha \in A_i} [\beta - (\alpha, \beta)] = n + d + 2g - 2.$$

We again denote B_1, \dots, B_S as the ramification indices of the S finite branch points of H_0 , and ω_i a largest element of B_i . We also denote N_i the number of elements of the corresponding set of ramification indices of ρ which are not divisible by ω_i and $t_i := \sum_{\alpha \in A_i} [\omega_i - (\alpha, \omega_i)] - (\omega_i - 1)$.

The following Lemma is proved identically to Lemma IV.8.

Lemma IX.15. *Assume that $\rho(X)$ and $H(Y)$ are as in Theorem IX.14. Then*

$$\sum_{i=1}^S N_i \leq S + d - 1,$$

with equality if and only if for all $1 \leq i \leq S$

- *if $N_i > 1$ then $\omega_i = 2$, and*
- *For all $\beta \in B_i \setminus \{\omega_i\}$ we have that $\sum_{\alpha \in A_i} [\beta - \gcd(\alpha, \beta)] = \alpha - 1$.*

The following Lemma is proved identically to Lemma IV.9.

Lemma IX.16. *Assume that $\rho(X)$ and $H(Y)$ are as in Theorem IX.14. Then*

$$(S - 2)m \leq \sum_{i=1}^S (N_i) - 2r,$$

with equality if and only if

- *$\omega_i = 2$ (for all $1 \leq i \leq S$) and,*
- *for all $1 \leq i \leq S$ every element of A_i which is not divisible by ω_i is equal to 1,*
and
- *for all $1 \leq i \leq S$ every element of A_i which is divisible by ω_i is equal to ω_i , and*
- *every branch point of $\rho(X)$ is a branch point of $H(Y)$.*

Proof of Theorem IX.14. Combining the results of the previous two Lemmas we have

$$(S - 2)m \leq \sum_{i=1}^S (N_i) - 2r \leq S + d - 1 - 2r.$$

Solving for m gives

$$d \leq m \leq \frac{S + d - 2 - 2r}{S - 2}.$$

When $S \geq 3$ it is clear that when $r \geq 2$ the inequality cannot hold (since the right side will be less than d). Furthermore, for any fixed r , as S increases the right side

of the equation can only decrease when $d > 1$ and remains constant when $d = 1$. Therefore this inequality never holds when $S \geq 3$. \square

Proof of Proposition IX.5. By Theorem IX.7 we know that ρ has at most $r + 2$ finite branch points. Furthermore, for every non-zero finite branch point of $G(X)$ there are r finite branch points of ρ , and if zero is a branch point of $G(X)$ with any ramification that doesn't divide r then zero is a branch point of ρ . Additionally, $G(X)$ must have ramification coprime to r over zero (since $r > 2$) and must have at least one finite non-zero branch point. Therefore ρ must have at least $r + 1$ finite branch points, and since $r > 2$ it cannot have $r + 2$ finite branch points, and so it has exactly $r + 1$ finite branch points.

By the structure of $G(X)$ we know that the multi-set of its ramification over zero is coprime, so the multi-set of ramification of ρ over zero is coprime. Additionally, $G(X)$ has exactly one other finite branch point, and this point cannot have ramification which is all divisible by an integer greater than 1. This is because if A_1 is the multi-set of ramification indices over zero, and A_2 is the multi-set of ramification indices over the other finite branch point (and all elements of A_2 are divisible by an integer $s > 1$) then

$$\begin{aligned} m - 1 &= \sum_{\alpha \in A_1} [\alpha - 1] + \sum_{\alpha \in A_2} [\alpha - 1] \leq \\ &\leq \left(m - \frac{m}{r} - 1\right) + \left(m - \frac{m}{s}\right) \\ &\leq 2m - \left[\frac{m}{r} + \frac{m}{s} + 1\right]. \end{aligned}$$

Since $r > 2$ we have $\left[\frac{m}{r} - \frac{m}{s} - 1\right] < m + 1$, and so this cannot occur.

Since the r finite non-zero branch points of ρ have the same multi-set of ramification indices as the non-zero finite branch point of $G(X)$ we can apply Theorem IX.14. Therefore, $H_0(Y)$ has exactly two finite branch points, and so $H(Y)$ can have

2 or 3 finite branch points. It has two finite branch points either if a branch point of H_0 is zero, or if Y^r maps both branch points of H_0 to the same point. \square

Proof of Theorem IX.6. By Proposition IX.5, we now know that $G(X)$ has two finite branch points (one of which is zero) and $H(Y)$ has two or three finite branch points (one of which is zero). We first analyze the case that $H(Y)$ and $G(X)$ each have two finite branch points.

We first assume that the non-zero finite branch points of $H(Y)$ and $G(X)$ are not the same. Recall from Lemma V.3 that $|B_1| + |B_2| = n$. Since all ramification of $H(Y)$ over zero is divisible by r it must be that $|B_1| \leq \frac{n}{r}$. We also have that,

$$\sum_{\beta \in B_2} [\beta - 1] = n - |B_2| = |B_1| - 1.$$

If $G(X)$ does not have the same other branch point as $H(Y)$ then $A_2 = [1^m]$ and

$$\sum_{\alpha \in A_2} \sum_{\beta \in B_2} [\beta - (\alpha, \beta)] = m(|B_1| - 1).$$

If $|B_1|$ were equal to 1 then $H(Y)$ would be cyclic, so $|B_1|$ is at least two. If it were bigger than two then $m(|B_1| - 1)$ would be bigger than $2n - 2$ (since n divides m) which is a contradiction.

We also have that there are two elements of A_1 which are coprime to r So the sum

$$\sum_{\beta \in B_1} \sum_{\substack{\alpha \in A_1 \\ (\alpha, r) = 1}} [\beta - (\alpha, \beta)] = 2n - 4.$$

However this leads to the contradiction that

$$\sum_{i=1}^2 \sum_{\beta \in B_i} \sum_{\alpha \in A_i} [\beta - (\beta, \alpha)] > 2n - 2,$$

since $m > 2$. So if $H(Y)$ and $G(X)$ each have two finite branch points, then the must be the same.

It remains to analyze possible multi-sets A_1 and B_1 (for $G(X)$ and $H(Y)$ respectively over zero) and A_2 and B_2 (for $G(X)$ and $H(Y)$ respectively over the other finite branch point) which satisfy the previous conditions and

$$\sum_{i=1}^2 \sum_{\alpha \in A_i} \sum_{\beta \in B_i} [\beta - (\alpha, \beta)] \leq 2n - 2.$$

We will now show, however, that

$$\sum_{\alpha \in A_1} \sum_{\beta \in B_1} [\beta - (\alpha, \beta)] \geq 2n - \frac{2n}{r},$$

and

$$\sum_{\alpha \in A_2} \sum_{\beta \in B_2} [\beta - (\alpha, \beta)] \geq (|B_1| - 1) \left(m - \frac{2m}{r} \right).$$

Since $|B_1| \geq 2$ and $m - \frac{2m}{r} \geq \frac{2n}{r}$, the sum of these two equations is bigger than $2n - 2$, so there must be a contradiction.

Since $|A_1|$ is at most $\frac{m}{r} + 1$ (this occurs when every element of A_1 is between 1 and r) we have that $|A_2|$ is at least $m - \frac{m}{r}$. Since $\sum_{\alpha \in A_2} \alpha = m$ we have that there are at least $m - \frac{2m}{r}$ (which is positive because $r > 2$) elements of A_2 equal to 1.

Furthermore the sum $\sum_{\beta \in B_2} [\beta - 1]$ is equal to $n - |B_2| = |B_1| - 1$. So we have that

$$\begin{aligned} \sum_{\beta \in B_2} \sum_{\alpha \in A_2} [\beta - (\alpha, \beta)] &\geq \sum_{\beta \in B_2} \sum_{\substack{\alpha \in A_2 \\ \alpha=1}} [\beta - (\alpha, \beta)] \\ &\geq (|B_1| - 1) \left(m - \frac{2m}{r} \right). \end{aligned}$$

When every element of A_1 is between 1 and r and every element of B_1 is equal to r we have

$$\sum_{\alpha \in A_1} \sum_{\beta \in B-1} [\beta - (\alpha, \beta)] = 2n - 2|B_1| = 2n - \frac{2n}{r}.$$

Furthermore it is clear that

$$\sum_{\substack{\alpha \in A_1 \\ r|\alpha}} \sum_{\beta \in B_1} [\beta - (\alpha, \beta)] \geq 0.$$

We also have that there are exactly two elements of A_1 coprime to r (they are also coprime to each other). Let a be the value of the larger such element. Then

$$\sum_{\substack{\alpha \in A_1 \\ (\alpha, r)=1}} \sum_{\beta \in B_1} [\beta] = 2n,$$

and

$$\sum_{\substack{\alpha \in A_1 \\ (\alpha, r)=1}} \sum_{\beta \in B_1} [(\alpha, \beta)] \leq (a+1)|B_1|.$$

However this requires that every element of B_1 is divisible by a and so $B_1 \leq \frac{n}{ar}$. So

we have that

$$\sum_{\alpha \in A_1} \sum_{\beta \in B_1} [\beta - (\alpha, \beta)] \geq 2n - \frac{n}{r} - |B_1|.$$

Since $|B_1| \leq \frac{n}{r}$ this is at least $2n - \frac{2n}{r}$.

Finally, if $H(Y)$ has three branch points, then we still have that

$$\sum_{\alpha \in A_1} \sum_{\beta \in B_1} [\beta - (\alpha, \beta)] \geq 2n - \frac{2n}{r}.$$

However for the branch point of $H(Y)$ which is not a branch point of $G(X)$ we have

$$\sum_{\alpha \in A_3} \sum_{\beta \in B_3} [\beta - (\alpha, \beta)] \geq m > \frac{2n}{r}.$$

This again leads to the contradiction that

$$\sum_{i=1}^R \sum_{\alpha \in A_i} \sum_{\beta \in B_i} [\beta - (\alpha, \beta)] > 2n - 2.$$

□

APPENDIX

APPENDIX A

Code for Exhaust in Chapter V

Below is an example of one of the pieces of magma code used in the exhausts in Chapter V:

```

Z := Integers();
parityn := 1; // parity of n
paritydiff := 1; // difference of parity for n and m
maxvaln := 16; // max n
maxvalm := 17; // max m value
kshift := -1; // k = (m- shift)/2
lshift := -2; // l = (n-shift)/2

for a in [1..14] do
for b in [1..12] do
if a + b ge 3 then
maxvaln := Ceiling((4*a*b + 2*a + 2*b)/(a+b-2));
//the proven upper bound of the exhaust
maxvalm := maxvaln;

```

```

kshift := b;
lshift := a;

for n in [3..maxvaln] do
for m in [n..maxvalm] do
if IsOdd(a) eq IsOdd(n) then
if IsOdd(b) eq IsOdd(m) then
d := GCD(m,n);
k := Z!((m-kshift)/2);
l := Z!((n-lshift)/2);
if k gt 1 then
if l gt 1 then
if k lt m then
if l lt n then
A1 := Partitions(m,k); A2 := Partitions(m,m+1-k); B1:= Partitions(n,l);
B2 := Partitions(n,n+1-l);
// constructs the sets of partitions of the desired sizes.
for a1 in A1 do J := #a1;
// we now exhaust over all the possible partitions, and check that the
// GCD of the elements is 1 (otherwise it is not a power-free polynomial)
gd := GCD(a1[1],a1[2]);
if k gt 2 then
for j in [3..k] do
gd := GCD(gd,a1[j]);
end for;

```

```

    end if;
if gd eq 1 then
    for a2 in A2 do
        J := #a2;
        gd := GCD(a2[1],a2[2]);
        if k lt m-1 then
            for j in [3..m-k+1] do
                gd := GCD(gd,a2[j]);
            end for;
        end if;
        if gd eq 1 then
            for b1 in B1 do
                J := #b1;
                gd := GCD(b1[1],b1[2]);
                if l gt 2 then
                    for j in [3..l] do
                        gd := GCD(gd,b1[j]);
                    end for;
                end if;
                if gd eq 1 then
                    for b2 in B2 do
                        J := #b2;
                        gd := GCD(b2[1],b2[2]);
                        if l lt n-1 then
                            for j in [3..n-l+1] do

```

```

    gd := GCD(gd,b2[j]);
  end for;
end if;
if gd eq 1 then
  ram := n-d;
  for b in b1 do for a in a1 do//here we use the ramification to calculate the
    //genus of the curve, as in the Riemann-Hurwitz calculation
    ram := ram + b - GCD(a,b);
  end for;end for;
  for b in b2 do for a in a2 do
    ram := ram + b - GCD(a,b);
  end for;end for;
  if ram eq 2*n - 2 then
    "a1 = ",a1," a2= ",a2," b1= ",b1," b2= ",b2;"\n";
  end if;
end if;

end for;

end if;

end for; end if;

end for; end if;

end for;

end if; end if;

end if; end if;

end if; end if;

```


end for; end for;

end if;

end for; end for;

BIBLIOGRAPHY

BIBLIOGRAPHY

- [1] R. M. Avanzi and U. M. Zannier. Genus one curves defined by separated variable polynomials and a polynomial Pell equation. *Acta Arith.* **99** (2001), 227–256.
- [2] R. M. Avanzi and U. M. Zannier. The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$. *Compositio Math.* **139** (2003), 263–295.
- [3] F. Beukers, T. N. Shorey and R. Tijdeman. Irreducibility of polynomials and arithmetic progressions with equal products of terms. *Number Theory in Progress (Proc. Internat. Conf. in Number Theory in Honor of A. Schinzel, Zakopane, 1997)*, de Gruyter, 1999.
- [4] Y. F. Bilu and R. F. Tichy. The Diophantine equation $f(x) = g(y)$. *Acta Arith.* **95** (2000), 261–288.
- [5] E. Brieskorn and H. Knörrer. *Plane Algebraic Curves*. Birkhäuser Verlag, Basel, 1986.
- [6] P. Cassou-Noguès and J.-M. Couveignes. Factorisations explicites de $g(y) - h(z)$. *Acta Arith.* **87** (1999), 291–317.
- [7] H. Davenport, D. J. Lewis, and A. Schinzel. Equations of the form $f(x) = g(y)$. *Quart. J. Math. Oxford Ser. (2)* **12** (1961), 304–312.
- [8] A. Ehrenfeucht. A criterion of absolute irreducibility of polynomials. *Prace Mat.* **2** (1956), 167–169. (in Polish)
- [9] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.* **73** (1983), 349–366.
- [10] W. Feit. On symmetric balanced incomplete block designs with doubly transitive automorphism groups. *J. Combinatorial Theory Ser. A* **14** (1973), 221–247.
- [11] W. Feit. Some consequences of the classification of finite simple groups. In *The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979)*, volume 37 of *Proc. Sympos. Pure Math.*, pages 175–181. Amer. Math. Soc., Providence, RI, 1980.
- [12] G. Fischer. *Plane Algebraic Curves*, volume 15 of *Student Mathematical Library*. American Math. Soc., Providence, 2001.
- [13] M. Fried. The field of definition of function fields and a problem in the reducibility of polynomials in two variables. *Illinois J. Math.* **17** (1973), 128–146.
- [14] M. Fried. Extension of constants, rigidity, and the Chowla–Zassenhaus conjecture. *Finite Fields Appl.* **1** (1995), 326–359.
- [15] H. W. Lenstra Solving the Pell equation, *Notices of the Amer. Math. Soc.* **49** (2002), 182–192, 2002.
- [16] P. Müller. Primitive monodromy groups of polynomials. In *Recent developments in the inverse Galois problem (Seattle, WA, 1993)*, volume 186 of *Contemp. Math.*, pages 385–401. Amer. Math. Soc., Providence, RI, 1995.

- [17] P. Müller and M. Zieve. On Ritt's polynomial decomposition theorems. arXiv:0807.3578
- [18] J. F. Ritt. Prime and composite polynomials. *Trans. Amer. Math. Soc.* **23** (1922), 51–66.
- [19] A. Schinzel. *Selected Topics on Polynomials*. University of Michigan Press, Ann Arbor, Mich., 1982.
- [20] C. L. Siegel. Über einige Anwendungen diophantischer Approximation, Abh. Preuss. Akad. Wiss. Phys.-Math. Kl. **1** (1929), 41–69.
- [21] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.
- [22] H. Stichtenoth. *Algebraic Function Fields and Codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.
- [23] H. Völklein. *Groups as Galois groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996.