FUNCTIONAL EQUATIONS IN COMPLEX ANALYSIS AND NUMBER THEORY

FELIX WANG
MIT-PRIMES, 2016

Abstract. We study the following questions:

(1) What are all solutions to $f \circ \hat{f} = g \circ \hat{g}$ with $f, g, \hat{f}, \hat{g} \in \mathbb{C}(X)$ being complex rational functions?

(2) For which rational functions $f(X)$ and $g(X)$ with rational coefficients does the equation $f(a) = g(b)$ have infinitely many solutions with $a, b \in \mathbb{Q}$?

We utilize various algebraic, geometric and analytic results in order to resolve both (1) and a variant of (2) in case the numerator of $f(X) - g(Y)$ is an irreducible polynomial in $\mathbb{C}[X, Y]$. Our results have applications in various mathematical fields, such as complex analysis, number theory, and dynamical systems. Our work resolves a 1973 question of Fried, and makes significant progress on a 1924 question of Ritt and a 1997 question of Lyubich and Minsky. In addition, we prove a quantitative refinement of a 2015 conjecture of Cahn, Jones and Spear.

1. Introduction

Throughout the history of number theory, many mathematicians have studied special cases of the following question:

Question 1.1. *For which rational functions $f, g \in \mathbb{Q}(X)$ does the equation $f(a) = g(b)$ have infinitely many solutions in rational numbers a and b?*

For example, Archimedes studied an instance of the Pell equation $a^2 = db^2 + 1$; we now know that there are infinitely many integers a, b satisfying this equation for any prescribed nonsquare positive integer d [21, p. 184]. More recently, Wiles [39] proved that Fermat's equation $c^n = d^n + e^n$ has no solutions in nonzero integers c, d, e, n with $n > 2$. Upon division by e^n, this result shows that $a^n = b^n + 1$ has no solutions in nonzero rational numbers a, b. Another prominent equation in modern number theory is the Weierstrass equation $Y^2 = X^3 + cX + d$, where c and d are fixed rational numbers such that $4c^3 \neq -27d^2$. This equation defines an elliptic curve, and has infinitely many solutions in rational numbers if and only if the corresponding elliptic curve has positive rank; this rank is the key quantity in the Birch and Swinnerton–Dyer conjecture, which is one of the most important open problems in mathematics [10]. This last example is enlightening, because although there has been progress on describing "how often" such an equation has infinitely many rational solutions [4–6], it seems that there is no hope of finding all pairs (c, d) for which the equation has infinitely many solutions. However, each equation of this form has infinitely many solutions in some algebraic number field K, by which we mean a field which is a finite-dimensional $\mathbb{Q}$-vector space. It is thus natural to modify Question 1.1 as follows:

Question 1.2. *For which rational functions $f, g \in K(X)$, where K is an algebraic number field, does the equation $f(a) = g(b)$ have infinitely many solutions in K?*

We prove the following result:

Theorem 1.3. *For any number field K and any rational functions $f, g \in K(X)$ such that the numerator of $f(X) - g(Y)$ is an irreducible polynomial in $\mathbb{C}[X, Y]$, if the equation $f(a) = g(b)$ has infinitely many solutions in K then one of these holds:*

(1.3.1) *at least one of the extensions $K(X)/K(f(X))$ or $K(X)/K(g(X))$ has Galois closure of genus 0 or 1*

(1.3.2) *$f = \mu \circ X^c(X-1)^d \circ \nu_1$ and $g = \mu \circ \gamma X^c(X-1)^d \circ \nu_2$ for some coprime positive integers c, d, some $\gamma \in K \setminus \{0, 1\}$, and some degree-one $\mu, \nu_1, \nu_2 \in K(X)$*

(1.3.3) $\deg(f), \deg(g) \leq 80$.

Conversely, if (1.3.2) holds then $f(X) - g(Y)$ is irreducible in $\mathbb{C}[X, Y]$ and $f(a) = g(b)$ has infinitely many solutions in K. These conclusions are sometimes satisfied when (1.3.1) holds, but not always. However, for each $f(X) \in K(X)$ such that $K(X)/K(f(X))$ has Galois closure of genus 0 or 1, there exist rational functions $g(X) \in \hat{K}(X)$ of arbitrarily large degree (with coefficients in a number field $\hat{K}$ containing K) for which these conclusions are satisfied over $\hat{K}$. Finally, we have explicitly determined all rational functions f and g satisfying both (1.3.3) and the hypotheses of Theorem 1.3.

Since automorphism groups of function fields of genus 0 or 1 are well-understood, condition (1.3.1) lets us give a precise description of either f or g. For instance, if the Galois closure of $K(X)/K(f(X))$ has genus 0 and $\deg(f) > 60$ then $f(X)$ is either X^m or $X^m + X^{-m}$ or a Chebyshev polynomial $T_m(X)$, up to composition on both sides with degree-one rational functions. Furthermore, when (1.3.1) holds we can describe both $f(X)$ and $g(X)$: for instance, if $f(X) = X^m$ with $m > 6$ then there is some degree-one $\nu \in K(X)$ for which $g \circ \nu$ is $X^c h(X)^m$ with $h \in K(X)$ and c coprime to m.

Most of the previous work on Question 1.1 addresses the much easier problem of determining the polynomials $f, g \in \mathbb{Z}[X]$ for which $f(a) = g(b)$ has infinitely many solutions in integers a, b. This was solved by Bilu and Tichy [7], building on previous work by Davenport, Fried, Lewis, Schinzel, Siegel, and others [13, 16, 37, 38]. It is easy to reduce this question to the case that $f(X) - g(Y)$ is irreducible in $\mathbb{C}[X, Y]$. Question 1.1 for rational solutions has also been studied by several authors. The most general published result was proved by Avanzi and Zannier [2], and addresses the case that f and g are polynomials of coprime degrees. Very recently, Carney et al. extended this to arbitrary polynomials f and g [11, 12]. Our further extension to rational functions (under some hypotheses) requires completely different methods than were used previously.

The second main topic of this paper is functional equations, and specifically the following questions:

Question 1.4. *What are all solutions to $f \circ \hat{f} = g \circ \hat{g}$ in rational functions $f, \hat{f}, g, \hat{g} \in \mathbb{C}(X)$?*

Question 1.5. *What are all solutions to $f \circ \hat{f} = g \circ \hat{g}$ in rational functions $f, g \in \mathbb{C}(X)$ and meromorphic functions $\hat{f}, \hat{g}$ on the complex plane?*

Here a *meromorphic function* is a ratio h_1/h_2 where h_1, h_2 are entire functions with $h_2 \neq 0$, and an *entire function* is a function $\mathbb{C} \to \mathbb{C}$ defined by a single power series $\sum_{i=0}^{\infty} \alpha_i X^i$ with infinite radius of convergence. For instance, e^X is entire, as are all polynomials, and all rational functions are meromorphic. Hence Question 1.4 is a more restricted version of Question 1.5.

We prove the following result:

Theorem 1.6. *For any $f, g \in \mathbb{C}(X)$ such that the numerator of $f(X)-g(Y)$ is an irreducible polynomial in $\mathbb{C}[X,Y]$, if there are nonconstant meromorphic functions $\hat{f}, \hat{g}$ on the complex plane such that $f \circ \hat{f} = g \circ \hat{g}$ then one of these holds:*

(1.6.1) *at least one of the extensions $\mathbb{C}(X)/\mathbb{C}(f(X))$ or $\mathbb{C}(X)/\mathbb{C}(g(X))$ has Galois closure of genus 0 or 1*

(1.6.2) *$f = \mu \circ X^c(X-1)^d \circ \nu_1$ and $g = \mu \circ \gamma X^c(X-1)^d \circ \nu_2$ for some coprime positive integers c, d, some $\gamma \in K \setminus \{0,1\}$, and some degree-one $\mu, \nu_1, \nu_2 \in \mathbb{C}(X)$*

(1.6.3) $\deg(f), \deg(g) \leq 80$.

Conversely, if (1.6.2) holds then the meromorphic functions $\hat{f}, \hat{g}$ satisfying $f \circ \hat{f} = g \circ \hat{g}$ are given by

$$\hat{f} = \nu_1^{-1} \circ \frac{\gamma^b X^c - 1}{\gamma^{a+b} X^{c+d} - 1} \circ h \quad \text{and} \quad \hat{g} = \nu_2^{-1} \circ \frac{\gamma^{a+b} X^{c+d} - \gamma^a X^d}{\gamma^{a+b} X^{c+d} - 1} \circ h$$

where h is meromorphic and a, b are integers such that $bd - ac = 1$. We also know all possibilities for f, g, $\hat{f}$ and $\hat{g}$ when (1.6.3) holds, and to some extent when (1.6.1) holds.

Questions 1.4 and 1.5 are of interest for several reasons. First, Nevanlinna showed that if nonconstant meromorphic functions $\hat{f}, \hat{g}$ satisfy $\hat{f}^{-1}(\alpha) = \hat{g}^{-1}(\alpha)$ for five distinct values of $\alpha \in \mathbb{C}$, then we must have $\hat{f} = \hat{g}$ [27]. Subsequent authors have sought analogous results when the values α are replaced by finite sets of complex numbers, and more generally when there are several pairs of finite sets (S_i, T_i) such that $\hat{f}^{-1}(S_i) = \hat{g}^{-1}(T_i)$. If there are nonconstant rational functions f, g for which $f \circ \hat{f} = g \circ \hat{g}$, then $\hat{f}^{-1}(f^{-1}(U)) = \hat{g}^{-1}(g^{-1}(U))$ for any $U \subset \mathbb{C}$, so in this case there are infinitely many pairs (S_i, T_i) of finite subsets of $\mathbb{C}$ for which $\hat{f}^{-1}(S_i) = \hat{g}^{-1}(T_i)$. Conversely, it is conceivable that such an infinitude of pairs (S_i, T_i) only exists when there exist such rational functions f, g. Thus Question 1.5 is a fundamental question about the distribution of preimages of meromorphic functions. We note that quite special cases of Question 1.5 have themselves been major results, for instance the case that f, g are polynomials and b, d are entire [31]. Furthermore, Theorem 1.6 answers a question of Fried [16, Problem 1]. Question 1.4 was originally studied by Ritt [36]; Theorem 1.6 comprises significant progress towards a solution of both Ritt's question and a question of Lyubich and Minsky [23, p. 83] on laminations in holomorphic dynamics.

In the special case that $f, \hat{f}, g, \hat{g}$ are polynomials, Question 1.4 was solved by Ritt [35]. His result has been used to prove important theorems in algebra [40], algebraic geometry [24], differential equations [8, 33], dynamical systems [3, 18, 19], logic [24], topology [29], transcendental number theory [28], and other topics. Solutions to Questions 1.4 or 1.5 would yield

vast improvements to all of these theorems. Prior to our work, these polynomial results had been extended only slightly, to cases of Question 1.4 which were not too far from the polynomial case; however, we note that already such extensions required significant effort [30,32,41]. Our Theorem 1.6 goes far beyond all these previous results.

This paper is organized as follows. In the next section we show that Theorems 1.3 and 1.6 are consequences of another result (Theorem 2.3), and present several important tools. We use these tools in Section 3 in order to prove Theorem 2.3, and then in Section 4 we refine our three main theorems. In Section 5 we present a dynamical application of our results, and we conclude in Section 6 with a discussion of future avenues of research. Finally, Section 7 contains several acknowledgements to various individuals and organizations that were crucial to the success of this research project.

2. Ramification and genus

In this section we show that the number-theoretic Theorem 1.3 and the analytic Theorem 1.6 are both consequences of a single geometric theorem, and then present several tools we will use to prove this theorem. We begin with some notation.

Definition 2.1 (Ramification Index)**.** *The ramification index $e_f(P)$ of a rational function $f(X)$ at a point $P \in \mathbb{C} \cup \{\infty\}$ is the local degree of $f(X)$ near $X = P$. Concretely, if $P, f(P) \in \mathbb{C}$, then $e_f(P)$ is the multiplicity of $X = P$ as a root of $f(X) - f(P)$, and in other cases $e_f(P)$ can be defined by changing variables to reduce to this case.*

Definition 2.2 (Ramification Multiset)**.** *The ramification multiset $E_f(Q)$ of a rational function f at a point Q is the multiset of all values of $e_f(P)$ for $P \in f^{-1}(Q)$.*

We can now state our main geometric result. Here and elsewhere, the expression $[a^c, b^d, \dots]$ denotes the multiset containing c copies of a, d copies of b, and so on. Also, by the genus of a plane curve we mean the genus of the corresponding function field.

Theorem 2.3 (LCM Theorem)**.** *Let $f, g \in \mathbb{C}(X)$ have degrees $m, n > 0$, respectively. Let $Q_1, \dots, Q_r$ be the points in $\mathbb{C} \cup \{\infty\}$ for which either $E_f(Q_i) \neq [1^m]$ or $E_g(Q_i) \neq [1^n]$. If the numerator of $f(X) - g(Y)$ defines an irreducible curve of genus 0 or 1, then $F_i := E_f(Q_i)$ and $G_i := E_g(Q_i)$ satisfy one of the following:*

(2.3.1) $\sum_{i=1}^{r} (1 - \frac{1}{\operatorname{lcm}(F_i)}) \leq 2$

(2.3.2) $\sum_{i=1}^{r} (1 - \frac{1}{\operatorname{lcm}(G_i)}) \leq 2$

(2.3.3) *$m = n$, $r = 4$, and (after relabeling the Q_i's) we have $F_1 = G_1 = [m]$, $F_2 = G_2 = [c, m-c]$ for some c coprime to m, $F_3 = G_4 = [1^{m-2}, 2]$, and $F_4 = G_3 = [1^m]$*

(2.3.4) $m, n \leq 80$.

Proof that Theorem 2.3 implies Theorems 1.3 and 1.6. By theorems of Faltings [14] and Picard [34], if the hypotheses of Theorem 1.3 or Theorem 1.6 hold then the numerator of $f(X) - g(Y)$ defines a curve of genus 0 or 1, so the hypotheses (and hence the conclusion) of Theorem 2.3 are satisfied. Plainly (2.3.4) implies (1.3.3) and (1.6.3), so we may assume that one of (2.3.1)–(2.3.3) holds. Let $\mathcal{N}$ be the Galois closure of $\mathbb{C}(X)/\mathbb{C}(f(X))$, and let d be the degree of the extension $\mathcal{N}/\mathbb{C}(f(X))$. Then Q_i lies under $\frac{d}{\mathrm{lcm}(F_i)}$ points of $\mathcal{N}$, each of which has ramification index $\mathrm{lcm}(F_i)$ in $\mathcal{N}/\mathbb{C}(f(X))$. Thus, by applying the Riemann–Hurwitz genus formula to the extension $\mathcal{N}/\mathbb{C}(f(X))$, if (2.3.1) (or likewise (2.3.2)) holds then (1.3.1) and (1.6.1) hold. Finally, suppose that (2.3.3) holds. Upon replacing f and g by $f \circ \nu_1$ and $g \circ \nu_2$ for suitable degree-one $\nu_i \in \mathbb{C}(X)$, we may assume that $f(\infty) = Q_1 = g(\infty)$ and $f^{-1}(Q_2) = \{0, 1\} = g^{-1}(Q_2)$ where $e_f(0) = c = e_g(0)$. Upon replacing f and g by $\mu \circ f$ and $\mu \circ g$ for a suitable degree-one $\mu \in \mathbb{C}(X)$, we may assume that $Q_1 = \infty$, $Q_2 = 0$, and the numerator and denominator of f have the same leading coefficient. It follows that $f = X^c(X-1)^{m-c}$ and $g = \gamma X^c(X-1)^{m-c}$ for some $\gamma \in \mathbb{C}^*$, and the reducibility hypothesis ensures that $\gamma \neq 1$. Hence the original f and g satisfy (1.3.2) and (1.6.2). □

Our proof of Theorem 2.3 proceeds by showing that if f, g satisfy the hypotheses of Theorem 2.3 then the multisets $F_i := E_f(Q_i)$ and $G_i := E_g(Q_i)$ satisfy several numerical conditions, and then solving the combinatorial problem of determining all collections of multisets of positive integers which satisfy these conditions. We present these numerical conditions in the remainder of this section, and then prove Theorem 2.3 in the next section.

The first two numerical conditions satisfied by ramification multisets are

$$\sum_{P \in f^{-1}(Q)} e_f(P) = \deg(f) \quad \text{for each } Q \in \mathbb{C} \cup \{\infty\} \tag{2.4}$$

$$\sum_{Q \in \mathbb{C} \cup \{\infty\}} \big(\deg(f) - |E_f(Q)|\big) = 2\deg(f) - 2. \tag{2.5}$$

Equation (2.5) is the Riemann–Hurwitz formula for the function field extension $\mathbb{C}(X)/\mathbb{C}(f(X))$. If $f, g \in \mathbb{C}(X)$ have degrees $m, n > 0$, and the numerator of $f(X) - g(Y)$ is irreducible, then this numerator defines a curve of genus $\mathfrak{g}$ where

$$2\mathfrak{g} - 2 = -2m + \sum_{Q \in \mathbb{C} \cup \{\infty\}} \sum_{a \in E_f(Q)} \sum_{b \in E_g(Q)} \big(a - \gcd(a, b)\big). \tag{2.6}$$

Equation (2.6) is a version of the Riemann–Hurwitz genus formula for the function field extension $\mathbb{C}(X, Y)/\mathbb{C}(Y)$ (where $f(X) = g(Y)$), and was proved by Ritt [35]. In particular,

if $\mathfrak{g} \in \{0,1\}$ then

$$\sum_{Q\in\mathbb{C}\cup\{\infty\}} \sum_{a\in E_f(Q)} \sum_{b\in E_g(Q)} \big(a-\gcd(a,b)\big) \in \{2m-2, 2m\}. \tag{2.7}$$

The next two lemmas give new types of constraints on the F_i's and G_i's which are crucial for our work.

Lemma 2.8. *If all elements of $F_1 \cup F_2$ are even then, for each $i > 2$, the multiset F_i can be written as the union of two submultisets each having sum $\frac{m}{2}$.*

Proof. Upon replacing f by $\mu\circ f$ for some degree-one $\mu \in \mathbb{C}(X)$, we may assume that $Q_1 = 0$ and $Q_2 = \infty$, so by hypothesis $f(X) = h(X)^2$ for some $h \in \mathbb{C}(X)$. Then for $i > 2$ we have $E_f(Q_i) = E_h(\sqrt{Q_i}) \cup E_h(-\sqrt{Q_i})$, which implies the result by (2.4). □

Lemma 2.9. *If the numerator of $f(X) - g(Y)$ is irreducible then both of these hold:*

(2.9.1) *For any distinct i, j we have* $\gcd(F_i \cup F_j \cup G_i \cup G_j) = 1$.

(2.9.2) *For any distinct i, j, k such that $F_i \cup F_j$ and $G_i \cup G_j$ each contain at most two odd indices, we must have* $\gcd(F_k \cup G_k) \le 2$.

Proof. We prove the contrapositive. If (2.9.1) fails then we can replace f and g by $\mu \circ f$ and $\mu \circ g$ for some degree-one $\mu \in \mathbb{C}(X)$, and we may therefore assume that $Q_i = 0$ and $Q_j = \infty$. Since $d := \gcd(F_i \cup F_j \cup G_i \cup G_j)$ divides $\gcd(F_i \cup F_j)$, we can write $f = X^d \circ \hat{f}$ for some $\hat{f} \in \mathbb{C}(X)$, and likewise $g = X^d \circ \hat{g}$. Therefore $f(X) - g(Y) = \prod_{\zeta^d=1}\big(\hat{f}(X) - \zeta\hat{g}(Y)\big)$ is reducible.

Henceforth suppose that (2.9.2) fails. Again we may assume $Q_i = -1$, $Q_j = 1$ and $Q_k = \infty$. First suppose there is an odd prime p which divides $\gcd(F_k \cup G_k)$. Then the degree-p Chebyshev polynomial $T_p(X)$ satisfies $E_{T_p}(Q_i) = E_{T_p}(Q_j) = [1, 2^{(p-1)/2}]$, $E_{T_p}(Q_k) = [p]$, and $E_{T_p}(Q_\ell) = [1^p]$ for $\ell \notin \{i, j, k\}$. Hence

$$\sum_{S\in\mathbb{C}\cup\infty} \sum_{a\in E_{T_p}(S)} \sum_{b\in E_a(S)} \big(a-\gcd(a,b)\big) \le p-1 < 2p-2,$$

so by (2.6) the numerator of $T_p(X) - f(Y)$ must be reducible, since otherwise it would define a curve having negative genus. Then [15, Prop. 2] implies that $f = f_1 \circ f_2$ for some $f_1, f_2 \in \mathbb{C}(X)$ such that the numerators of $T_p(X) - z$ and $f_1(X) - z$ have the same splitting field as one another over $\mathbb{C}(z)$, where z is transcendental over $\mathbb{C}$. Since the splitting field $\mathcal{M}$ of $T_p(X) - z$ over $\mathbb{C}(z)$ is $\mathbb{C}(y)$ where $y^p + y^{-p} = 2z$, the Galois group of $\mathcal{M}/\mathbb{C}(z)$ is dihedral of order $2p$, so that each non-Galois extension of $\mathbb{C}(z)$ contained in $\mathcal{M}$ has the form $\mathbb{C}(x)$ where $T_p(x) = z$. Hence $f_1 = T_p \circ h$ for some $h \in \mathbb{C}(X)$, so $f = T_p \circ \hat{f}_2$ where $\hat{f}_2 := h \circ f_2$.

Likewise $g = T_p \circ g_2$, so that $f(X) - g(Y)$ equals $T_p(f_2(X)) - T_p(g_2(Y))$, whose numerator is reducible since it is divisible by the numerator of $f_2(X) - g_2(Y)$.

The proof is similar but lengthier when $\gcd(F_k \cup G_k)$ is a power of 2, so for the sake of brevity, we simply sketch the argument. The main difference is that the ramification of $T_2(X)$ is slightly different from that of $T_p(X)$ for odd p, so that the above argument does not imply that the numerator of $T_2(X) - f(Y)$ is reducible. However, the above argument does imply that the numerator of either $T_2(X) - f(Y)$ or $T_2(X) + f(Y)$ is reducible, so $f = \pm T_2 \circ f_2$. Similarly, $f = \pm T_4 \circ f_2$ and $g = \pm T_4 \circ g_2$, and since both $T_4(X) - T_4(Y)$ and $T_4(X) + T_4(Y)$ are reducible it follows that the numerator of $f(X) - g(Y)$ is reducible. □

3. Proof of LCM Theorem

In this section we prove Theorem 2.3 when either $n \geq 42m$ or $n \geq m > 150$. This addresses all cases with $n \geq m$ except when $n < 42m \leq 42 \cdot 150$. More intricate (but slightly lengthier) versions of the arguments presented in this section yield a proof of Theorem 2.3 in all cases.

Proposition 3.1 (Fixed m, Large n)**.** *Using the notation and assumptions of Theorem 2.3, if $n \geq 42m$ then (2.3.1) holds.*

Proof. For each i we write $l_i = \operatorname{lcm}(F_i)$, and we let D_i denote the set of proper divisors of l_i. For a given i and for $d \in D_i$ we write $c_{i,d}$ to denote the number of elements $j \in G_i$ for which $\gcd(j, l_i) = d$. Observe that for any given i we must have $n \geq l_i \cdot c_{i,l_i} + \sum_{d \in D_i} d \cdot c_{i,d}$ and therefore

$$\sum_{d \in D_i} c_{i,d} + \frac{n - \sum_{d \in D_i} d \cdot c_{i,d}}{l_i} \geq c_{i,l_i} + \sum_{d \in D_i} c_{i,d} = |G_i|$$

By (2.5), we have

$$2n - 2 \geq \sum_{i=1}^{r} (n - |G_i|) \geq \sum_{i=1}^{r} \left(n - \sum_{d \in D_i} c_{i,d} - \frac{n - \sum_{d \in D_i} d \cdot c_{i,d}}{l_i} \right). \tag{3.2}$$

Furthermore, by (2.7), we have

$$2m \geq \sum_{i=1}^{r} \sum_{d \in D_i} c_{i,d} \sum_{i \in F_i} (i - \gcd(d, i)).$$

We define s to be the greatest positive number such that for all i and all $d \in D_i$

$$\sum_{i \in F_i} (i - \gcd(d, i)) \geq s \left(1 - \frac{d}{l_i} \right).$$

Multiplying (3.2) by s and simplifying a bit yields

$$s \cdot n \left(\sum_{i=1}^{r} \left(1 - \frac{1}{l_i}\right) - 2 \right) \leq 2m - 2s,$$

whence $\sum_{i=1}^{r} \left(1 - \frac{1}{l_i}\right) - 2 < \frac{2m}{ns}$. Additionally, for a given i and $d \in D_i$, note that because $d < l_i$ we must have

$$\frac{\sum_{i \in F_i} (i - \gcd(d,i))}{\left(1 - \frac{d}{l_i}\right)} \geq \frac{\sum_{i \in F_i} (i - \gcd(d,i))}{\frac{1}{2}} \geq \frac{1}{\frac{1}{2}} = 2,$$

and therefore we may assume that $s \geq 2$. Recalling that $\sum_{i=1}^{r} \left(1 - \frac{1}{l_i}\right) - 2 < \frac{2m}{ns}$, we conclude that $\sum_{i=1}^{r} \left(1 - \frac{1}{l_i}\right) < 2 + \frac{m}{n}$. Hence by Lemma 3.3, either $\sum_{i=1}^{r} \left(1 - \frac{1}{l_i}\right) \leq 2$ or $\sum_{i=1}^{r} \left(1 - \frac{1}{l_i}\right) \geq 2 + \frac{1}{42}$. But the latter implies that $\frac{1}{42} < \frac{m}{n}$ or that $n < 42m$, contradicting the assumptions of (2.3), and thus $\sum_{i=1}^{r} \left(1 - \frac{1}{l_i}\right) \leq 2$, so we are done. □

Lemma 3.3. *If $d_1, \ldots, d_q$ is a finite sequence of integers greater than 1, then $S := \sum_{i=1}^{q} \left(1 - \frac{1}{d_i}\right)$ lies in $\{0\} \cup [\frac{1}{2}, 1] \cup [\frac{7}{6}, 2] \cup [2 + \frac{1}{42}, \infty)$. Furthermore, we have $S \leq 2$ if and only if either $q \leq 2$ or the multiset of d_i's is one of the following: $[2^4]$, $[3^3]$, $[2, 4^2]$, $[2, 3, \ell]$ with $2 \leq \ell \leq 6$, or $[2^2, k]$ with $k > 1$.*

Proof. Write D for the multiset of d_i's. Note that $S = 2$ when D is $[2^4]$, $[3^3]$, $[2, 4^2]$, or $[2, 3, 6]$. Since the value of S becomes strictly larger if we either append a 2 to D or increase some element of D by 1, and by starting with each of the above four D's and repeatedly applying these operations we obtain every D with $q > 2$ except $[2, 3, \ell]$ with $\ell < 6$ and $[2^2, k]$ with $k > 1$, this implies the last assertion in the result. Moreover, the smallest value of S larger than 2 must occur when D arises from a single such operation, so the smallest such S is $2 + \frac{1}{42}$ which occurs for $D = [2, 3, 7]$. Likewise, if $D = \emptyset$ or $D = [2^2]$ then $S = 0$ or $S = 1$, so by the same argument the smallest values of S greater than 0 or 1 occur when $D = [2]$ or $D = [2, 3]$, respectively, and are $S = \frac{1}{2}$ and $\frac{7}{6}$. □

In the rest of this section we assume that $150 < m \leq n \leq 42m$. Our next result provides a crucial constraint on the multisets F_i and G_i.

Proposition 3.4. *Suppose that f and g satisfy the hypotheses of Theorem 2.3, and also $150 < m \leq n \leq 42m$. For any i, put $F := E_f(Q_i)$ and $G := E_g(Q_i)$, and let f_a and g_a be the numbers of copies of the integer a in F and G, respectively. For any integer c such that $0 \leq c \leq 6$, one of the following holds:*

(3.4.1) *There is a positive integer $d \leq c$ such that $f_d > \frac{m}{d} - (2d + 3)$.*

(3.4.2) $f_a, g_a \leq 4$ *for* $1 \leq a \leq c$.

Proof. We prove Proposition 3.4 by induction on c. The base case is $c = 0$, where (3.4.2) is vacuously true. For the inductive step it is enough to prove that if $f_a, g_a \leq 4$ for $1 \leq a \leq c-1$ then either $f_c > \frac{m}{c} - (2c+3)$ or $f_c, g_c \leq 4$. By condition (2.7), we have

$$2m \geq g_c \sum_{a=1}^{\infty} f_a \cdot (a - \gcd(a,c)) \geq g_c \sum_{a=c+1}^{\infty} f_a \cdot \frac{a}{2} \geq g_c \cdot \frac{1}{2}\left(m - cf_c - \sum_{a=1}^{c-1} af_a\right),$$

where we used the facts that $m = \sum_a af_a$ and if $a > c$ then $\gcd(a,c) \leq \frac{a}{2}$. The above inequality then implies that

$$4m \geq g_c\left(m - cf_c - \sum_{a=1}^{c-1} af_a\right) \geq g_c\left(m - cf_c - \sum_{a=1}^{c-1} 4a\right) \geq g_c\left(m - cf_c - 2c(c-1)\right). \tag{3.5}$$

Similarly,

$$4n \geq f_c\left(n - cg_c - \sum_{a=1}^{c-1} ag_a\right) \geq f_c\left(n - cg_c - \sum_{a=1}^{c-1} 4a\right) \geq f_c\left(n - cg_c - 2c(c-1)\right). \tag{3.6}$$

Assume that $5 \leq f_c \leq \frac{m}{c} - (2c+3)$; we now show that this leads to a contradiction. Here $m - cf_c - 2c(c-1) > 0$ and $f_c > 0$, so we may combine (3.5) and (3.6) to get

$$\frac{4m}{m - cf_c - 2c(c-1)} \geq g_c \geq \frac{1}{c}\left(n - 2c(c-1) - \frac{4n}{f_c}\right).$$

By clearing denominators we obtain $h(f_c) \geq 0$, where $h(X)$ is the polynomial

$$cX^2\left(n - 2c(c-1)\right) + X\left(4mc - 4nc - \left(m - 2c(c-1)\right)\left(n - 2c(c-1)\right)\right) + 4n\left(m - 2c(c-1)\right).$$

It is easy to check that $h(X)$ is negative when X is either 5 or $\frac{m}{c} - (2c+3)$. Since $h(X)$ has degree at most 2, and the coefficient of X^2 in $h(X)$ is nonnegative, it follows that $h(X)$ is negative for all X with $5 \leq X \leq \frac{m}{c} - (2c+3)$. This yields the contradiction $h(f_c) < 0$, so our assumption was incorrect and thus either $f_c \leq 4$ or $f_c > \frac{m}{c} - (2c+3)$.

If $f_c > \frac{m}{c} - (2c+3)$ then we are done. If $f_c \leq 4$ then (3.5) implies that

$$4m \geq g_c\left(m - cf_c - 2c(c-1)\right) \geq g_c\left(m - 4c - 2c(c-1)\right) = g_c\left(m - 2c(c+1)\right);$$

hence $g_c \leq \frac{4m}{m-2c(c+1)} < 5$, which completes the proof. □

We can improve Proposition 3.4 by strengthening the inequalities used in its proof. In particular, we can replace (3.5) by

$$4m \geq \sum_{j=1}^{c} g_j\left(m - jf_j - \sum_{a=1}^{j-1} af_a\right), \tag{3.7}$$

we can make a similar improvement to (3.6), and also for each fixed c we can improve the inequality $\gcd(a,c) \le \frac{a}{2}$ by using the actual value if $a \le 2c$ and otherwise using the bound $\gcd(a,c) \le c$. Applying these improvements requires the separate treatment of a large number of cases, depending on the values of f_a and g_a for several choices of a, and was done with the assistance of a computer program. This yields the following result.

Proposition 3.8. *Under the hypotheses of Proposition 3.4, if c is an integer with $1 \le c \le 6$ then one of the following holds:*

(3.8.1) *There is a positive integer $d \le c$ such that $f_d > \frac{m-w_d}{d}$, where $w_1 = 5$, $w_2 = 12$, $w_3 = 15$, $w_4 = w_5 = 24$, and $w_6 = 36$*

(3.8.2) *$\sum_{a \le c} f_a \le 4$ and $\sum_{a \le c} g_a \le 4$.*

Propositions 3.4 and 3.8 show that, for each i, either there is some (necessarily unique) integer d_i with $1 \le d_i \le 6$ for which the sum of the elements of F_i different from d_i is bounded by an absolute constant, or else F_i contains a bounded number of elements smaller than 7 (in which case we define $d_i := \infty$). In our proof of Theorem 2.3, we combine this information across all the different points Q_i in order to determine the possibilities for the multiset D consisting of all d_i's greater than 1. We first give a heuristic argument illustrating our approach. If $d_i \le 6$ then $|F_i| \approx \frac{m}{d_i}$, and if $d_i = \infty$ then $|F_i|$ is at most $\frac{m}{7} + c$ for some small constant c. By (2.5), we have $2m - 2 = \sum_{i=1}^{r} (m - |F_i|)$, so that

$$2m - \sum_{i:\ d_i \le 6} m\Big(1 - \frac{1}{d_i}\Big) \approx \sum_{i:\ d_i = \infty} (m - |F_i|), \tag{3.9}$$

where each summand on the right side is between $\frac{6m}{7} - c$ and m. By Lemma 3.3, the quantity $\sum_{i:\ d_i \le 6}(1 - \frac{1}{d_i})$ is either 0 or an element of one of the intervals $[\frac{1}{2}, 1]$ or $[\frac{7}{6}, \infty)$, so the left side of (3.9) is either $2m$ or an element of $[m, \frac{3m}{2}]$ or $(-\infty, \frac{5m}{6}]$. Since the right side of (3.9) is a sum of elements of $[\frac{6m}{7} - c, m]$, the only possibility is that each summand on the right side is approximately m, whence $\sum_{d \in D}(1 - \frac{1}{d}) = 2$. This equation implies that D is one of the multisets

$$[2,2,2,2], [2,4,4], [3,3,3], [2,3,6], [2,2,\infty], [\infty,\infty].$$

Below we prove Theorem 2.3 via a rigorous version of this heuristic argument, first restricting the possibilities for the F_i's and then deducing the desired conclusion. In what follows, we write $f_{i,a}$ for the number of copies of a in the multiset F_i, and we define $g_{i,a}$ analogously. We begin the proof with two lemmas, and then split the case into three cases: $f_{i,1} \le 4$ for at least four i's, $f_{i,1} \le 4$ for at most two i's, and $f_{i,1} \le 4$ for exactly three i's, which cover all possible situations. The first of these three cases loosely corresponds to

$D = [2,2,2,2]$, the second corresponds to $D = [\infty,\infty]$, and the third corresponds to $D = [2,4,4],[3,3,3],[2,3,6],[2,2,\infty]$.

Lemma 3.10. *If $f_{i,2} > \frac{m}{2} - 6$ for $1 \le i \le 4$, then $\bigcup_{i=1}^4 G_i = [1^4, 2^{2n-2}]$ and $G_i = [1^n]$ for $i > 4$. In particular, (2.3.2) holds.*

Proof. Let k be the number of odd elements in $\bigcup_{i=1}^4 G_i$. If $k \ge 5$ then

$$2m-2 \ge \sum_{i=1}^{4}\sum_{a\in F_i}\sum_{b\in G_i}\big(a-\gcd(a,b)\big) \ge \sum_{i=1}^{4}\sum_{\substack{a\in F_i\\ a=2}}\sum_{\substack{b\in G_i\\ b \text{ odd}}} 1 > 5\Big(\frac{m}{2}-6\Big) > 2m-2,$$

a contradiction. Hence $k \le 4$, so by (2.5) we have

$$2n-2 = \sum_{i=1}^{r}\big(n-|G_i|\big) \ge \sum_{i=1}^{4}\big(n-|G_i|\big) \ge 4n - \Big(k + \frac{4n-k}{2}\Big) = \frac{4n-k}{2} \ge 2n-2.$$

Thus this chain of inequalities must consist of equalities; proceeding from left to right, it follows that if $i > 4$ then $|G_i| = n$ (and hence $G_i = [1^n]$); if $i \le 4$ then G_i contains only 1's and 2's; and finally, $k = 4$. This yields the desired conclusion. □

Lemma 3.11. *If $|F_i| = 1$ then $\gcd(F_i, G_i) = m$ or $\sum_{a\in F_i}\sum_{b\in G_i}\big(a-(a,b)\big) \ge \frac{m}{2}$. If $|F_i| = 2$ and $n \le m+4$ then $\gcd(F_i,G_i) = \frac{m}{2}$ or $\sum_{a\in F_i}\sum_{b\in G_i}\big(a-(a,b)\big) \ge \frac{m}{4}$. If $|F_i| = 3$ and $n \le m+4$ then $\gcd(F_i,G_i) \in \{\frac{m}{3},\frac{m}{4},\frac{m}{6}\}$ or $\sum_{a\in F_i}\sum_{b\in G_i}\big(a-(a,b)\big) \ge \frac{m}{6}$.*

Proof. We prove Lemma 3.11 when $|F_i| = 1$ and $F_i = [m]$. If m divides each element of G_i then $\gcd(F_i,G_i) = m$. If G_i contains an element c which is not divisible by m, then $\sum_{a\in F_i}\sum_{b\in G_i}\big(a-(a,b)\big) \ge m-(m,c) \ge \frac{m}{2}$. The proofs of the other two assertions are highly similar. We omit them due to space constraints. □

Proof of Theorem 2.3 when $f_{i,1} \le 4$ for at least four i's. Without loss of generality, we may assume that $f_{i,1} \le 4$ for $1 \le i \le 4$, so that $|F_i| \le 4 + \frac{m-4}{2} = \frac{m}{2}+2$ and $m - |F_i| \ge \frac{m}{2} - 2$ for $1 \le i \le 4$. If $f_{1,1} + f_{1,2} \le 4$ then $|F_1| \le 4 + \frac{m-4}{3} = \frac{m+8}{3}$ and therefore $m - |F_1| \ge \frac{2m-8}{3}$. Then $\sum_{1\le i\le 4}(m-|F_i|) \ge 3(\frac{m}{2}-2) + \frac{2m-8}{3} = \frac{13m}{6} - \frac{26}{3} > 2m-2$, a contradiction. Thus $f_{1,1} + f_{1,2} > 4$, and then by Proposition 3.8 we must have $f_{1,2} > \frac{m}{2} - 6$ and similarly $f_{i,2} > \frac{m}{2} - 6$ for $2 \le i \le 4$. Lemma 3.10 yields the desired conclusion. □

Proof of Theorem 2.3 when at most two i's satisfy $f_{i,1} \le 4$. By Proposition 3.8, if $f_{i,1} > 4$ then $f_{i,1} \ge m-5$, so that $|F_i| \ge m-4$ and therefore $m - |F_i| \le 4$. By (3.6) it follows that $g_{i,1} \ge n - \frac{4n}{f_{i,1}} \ge n - \frac{4n}{m-4}$. Hence there are at most two i's for which $4 < f_{i,1} < m$, since otherwise

$$2m = \sum_{i=1}^{r}\sum_{a\in F_i}\sum_{b\in G_i}\big(a-(a,b)\big) \ge 3\big(n - \frac{4n}{m-4}\big) > 2m.$$

Since each such i satisfies $m - |F_i| \leq 4$, it follows that the sum of the corresponding values of $(m - |F_i|)$ is at most 8, so (2.5) implies that $f_{i,1} \leq 4$ for at least two (hence exactly two) values of i.

We may assume that $f_{i,1} \leq 4$ if and only if $i \leq 2$. Then $g_{i,1} \geq n - \frac{4n}{m-4}$ for $i \geq 3$, so

$$2m \geq \sum_{i\geq 3} g_{i,1} \sum_{a\in F_i}(a-1) \geq \sum_{i\geq 3} g_{i,1}(m - |F_i|) \geq (n - \frac{4n}{m-4}) \sum_{i\geq 3}(m - |F_i|).$$

This implies $\sum_{i\geq 3}(m - |F_i|) \leq \frac{2m}{n-\frac{4n}{m-4}} < 3$ because $n \leq 42m$. If $\sum_{i\geq 3}(m - |F_i|) = 2$, then by (2.5), $2m - 2 = m - |F_1| + m - |F_2| + \sum_{i\geq 3}(m - |F_i|)$ so $|F_1| + |F_2| = 4$. In particular, $1 \leq |F_1| \leq 3$. We must also have

$$\sum_{i=1}^{2} \sum_{a\in F_i} \sum_{b\in G_i} (a - (a, b)) \leq 2m - 2(n - \frac{4n}{m-5}) < 9;$$

this also implies $n \leq m + 4$. If $|F_1| = 1$ and $|F_2| = 3$ then by Lemma 3.11 we can conclude that $\gcd(F_1, G_1) = m$, since $\frac{m}{2} > 9$, and that $\gcd(F_2, G_2) \in \{\frac{m}{3}, \frac{m}{4}, \frac{m}{6}\}$, since $\frac{m}{6} > 9$. Then $\gcd(F_1, F_2, G_1, G_2) > 1$, which contradicts (2.9.1). A similar argument demonstrates that when $|F_1| = |F_2| = 2$ or $|F_1| = 3$ and $|F_2| = 1$, we must again have $\gcd(F_1, F_2, G_1, G_2) > 1$, a contradiction. Thus $\sum_{i\geq 3}(m - |F_i|) \leq 1$, and then by (2.5), $2m - 2 = m - |F_1| + m - |F_2| + \sum_{i\geq 3}(m - |F_i|)$, so $|F_1| + |F_2| \leq 3$. If $|F_1| + |F_2| = 2$, we must have $F_1 = F_2 = [m]$ and then (2.3.1) holds. If $|F_1| + |F_2| = 3$, we can write $F_1 = [m]$ and $F_2 = [c, m - c]$. Now an analysis of the multisets G_i, using (2.5) and (2.7), yields (2.3.3). □

Proof of Theorem 2.3 when exactly three i's satisfy $f_{i,1} \leq 4$. We split this case into four subcases based on how many of the three points satisfy $f_{i,2} > 4$. Three of these four subcases are resolved via the methods used to treat the case when $f_{i,1} \leq 4$ for at least four i's; due to space constraints and the similarity of the cases, we sketch the proofs. The fourth subcase, when exactly two i's satisfy $f_{i,2} > 4$, is more difficult. The full proof of the fourth subcase is too long to be included here, but we provide a detailed outline of the proof so that the reader may understand the motivation and important details.

Proof of First Subcase. The first subcase is when all three points satisfy $f_{i,2} > 4$. We let these three points be F_1, F_2 and F_3; by Proposition 3.8, it must be true that $f_{i,1} \leq 4$ for $1 \leq i \leq 3$. Since we assume that exactly three i's satisfy $f_{i,1} \leq 4$, for $i \geq 4$, we must have $f_{i,1} > 4$. Now by Proposition 3.8, $f_{i,2} > 4$ implies that $f_{i,2} \geq \frac{m-12}{2}$ and hence

$|F_1|, |F_2|, |F_3| \geq \frac{m-12}{2}$. But then by (2.5),

$$2m-2 = \sum_{i=1}^{r}(m-|F_i|) \leq 3m-3\left(\frac{m-12}{2}\right) + \sum_{i\geq 4}(m-|F_i|)$$

Recall that since $f_{i,1} > 4$ for $i \geq 4$, by Proposition 3.8, $f_{i,1} \geq m-5$ and then by (3.6) we must have $g_{i,1} \geq n - \frac{4n}{f_{i,1}} \geq n - \frac{4n}{m-5}$ and hence there are at most two i's for which $4 < f_{i,1} < m$. Moreover, if F_y and F_z satisfy $f_{y,1}, f_{z,1} > 4$ then $(m-|F_y|)+(m-|F_z|) \leq 2$, because otherwise $\sum_{i=1}^{r}\sum_{a\in F_i}\sum_{b\in G_i}\big(a-(a,b)\big)$ would be larger than $2m$, thus contradicting (2.7). In particular, since $f_{i,1} \leq 4$ for $1 \leq i \leq 3$, this implies that the quantity $\sum_{i\geq 4}(m-|F_i|)$ must be at most 2. Hence

$$2m-2 \leq \frac{3m}{2} + 18 + 2$$

which implies that $\frac{m}{2} \leq 22$ or that $m \leq 44$, a contradiction. □

Proof of Second Subcase. The second subcase is when none of the three points satisfies $f_{i,2} > 4$. We let these three points be F_1, F_2 and F_3; we then claim that all three points must satisfy $f_{i,3} > 4$. Indeed, for the sake of contradiction, assume that at least one of the points, say F_1 does not satisfy $f_{i,3} > 4$. The maximum possible size of F_2 and F_3 occurs when they consist of almost entirely 3's and four 1's (because they cannot have more than four 1's by Proposition 3.8) and is therefore equal to $4 + \frac{m-4}{3}$. By similar logic, the maximum possible size of F_1 occurs when F_1 consists of almost entirely 4's and four 1's and therefore equals $4 + \frac{m-4}{4} = \frac{m}{4} + 3$, and hence

$$2m-2 \geq \sum_{i\leq 3}(m-|F_i|) \geq 3m-2\left(4+\frac{m-4}{3}\right) - \frac{m}{4} - 3$$

which implies $\frac{19}{3} \geq \frac{m}{12}$ or $76 \geq m$, a contradiction. Hence all three points must satisfy $f_{i,3} > 4$ and this subcase loosely corresponds to $D = [3,3,3]$. With the knowledge that $f_{i,3} > 4$ for $1 \leq i \leq 3$, we can proceed using the exact same techniques used in Lemma 3.10. That is, we use (2.5) to analyze $\sum_{i\geq 4}^{r}(m-|F_i|)$ and we use (2.7) to relate F_1, F_2 and F_3 to all the F_i with $i \geq 4$; eventually our analysis proves that $\sum_{i\geq 4}^{r}(m-|F_i|) = 0$ and that $F_1 \cup F_2 \cup F_3$ consists entirely of 1's and 3's, a similar result to that of Lemma 3.10, and thus illustrates that (2.3.1) must hold in this subcase. □

Proof of Third Subcase. The third subcase is when exactly one of the three points satisfies $f_{i,2} > 4$; we let F_1 be this point. We then claim that F_2 must satisfy either $f_{2,3} > 4$ or $f_{2,4} > 4$ or $f_{2,6} > 4$. Observe that if $f_{2,5} > 4$ then $4 + \frac{m-4}{5} \geq |F_2| \geq \frac{m-25}{5} + 1 = \frac{m}{5} - 4$; in other words, $|F_2| \approx \frac{m}{5}$. But then $f_{3,k} > 4$ for any $k \in \{3,4,5,6\}$ would result in a

contradiction. Indeed, consider that $f_{3,4} > 4$ implies that $|F_3| \leq \frac{m}{4} + 3$ whence by (2.5)

$$2m - 2 \geq \sum_{i \leq 3} (m - |F_i|) \geq 3m - |F_1| - |F_2| - |F_3|$$

which with a little substitution becomes

$$2m - 2 \geq 3m - \left(4 + \frac{m-4}{2}\right) - \left(4 + \frac{m-4}{5}\right) - \left(\frac{m}{4} + 3\right)$$

or $\frac{m}{20} \leq \frac{31}{5}$ or $m \leq 124$, a contradiction. Similarly, $f_{3,3} > 4$ implies that $|F_3| \geq \frac{m-12}{3} + 1 = \frac{m}{3} - 3$ which can also be seen to contradict (2.5), and analogous arguments demonstrate that $f_{3,k} > 4$ for any $k \in \{3, 4, 5, 6\}$ fails. But if $f_{3,k} > 4$ is false for $3 \leq k \leq 6$ then $|F_3| \leq 4 + \frac{m-4}{7}$, resulting in another contradiction of (2.5). Hence F_2 must satisfy either $f_{2,3} > 4$ or $f_{2,4} > 4$ or $f_{2,6} > 4$. By further analysis with (2.5), if $f_{2,3} > 4$ then $f_{3,6} > 4$, if $f_{2,4} > 4$ then $f_{3,4} > 4$, and if $f_{2,6} > 4$ then $f_{3,3} > 4$; hence this case loosely corresponds to $D = [2, 4, 4]$ if $f_{2,4}, f_{3,4} > 4$ and otherwise it loosely corresponds to $D = [2, 3, 6]$.

When $D = [2, 4, 4]$ and $f_{2,4}, f_{3,4} > 4$, this subcase is easily resolved by the same techniques of Lemma 3.10 and the second subcase (when none of the three points satisfies $f_{i,2} > 4$): simple analysis with (2.5) and (2.7). However, when $D = [2, 3, 6]$ and $f_{2,3} > 4$ and $f_{3,6} > 4$, this subcase is much trickier to resolve. This scenario requires the analysis of thousands of possibilities, for which we use a computer program. We do not have the space to present the computer program, but we will illustrate the methodology of the program by resolving this case with one additional hypothesis: $n \geq 4m$.

First of all, by Proposition 3.8 we must have $f_{1,2} \geq \frac{m}{2} - 6$ and hence by (3.6), $g_{1,2} \geq \frac{1}{2} \cdot (n - \frac{4n}{f_{1,2}} - 4) = \frac{n}{2} - \frac{2n}{f_{1,2}} - 2 \geq \frac{n}{2} - \frac{4n}{m-12} - 2$. Hence if F_1 contains an element greater than 2 then

$$2m \geq \sum_{i=1}^{r} \sum_{a \in F_i} \sum_{b \in G_i} \big(a - (a, b)\big) \geq 2g_{1,2} \geq n - \frac{8n}{m-12} - 4 > 2m$$

where the last step is because $n \geq 4m$. So F_1 cannot contain an element greater than 2, and thus F_1 consists of all 1's and 2's.

Similarly, $g_{i,1} \geq n - \frac{4n}{f_{4,1}}$ for $i \geq 4$ and so F_i cannot contain an element greater than 1 for $i \geq 4$, and therefore $F_4, F_5, \ldots$ are all equal to $[1^m]$. Observe again that by (3.6), $g_{3,2} \geq \frac{1}{3} \cdot (n - 12 - \frac{4n}{f_{3,2}})$ so that the only possible elements of F_2 are 1, 2 and 3. Similarly, $g_{3,6} \geq \frac{1}{6} \cdot (n - 60 - \frac{4n}{f_{3,6}})$ so that the only possible elements of A_3 are 1, 2, 3, 4 and 6. Now, assume for the sake of contradiction that (2.3.1) and (2.3.2) both fail; then either F_2 must have a 2 or F_3 must have a 4 (and both cannot happen, for then $\sum_{i=1}^{r} \sum_{a \in F_i} \sum_{b \in G_i} \big(a - (a, b)\big)$ would be larger than $2m$). Assume henceforth that F_2 has a 2; the case where F_3 has a 4 has a (nearly) identical proof.

By (2.5), $3m - (|F_1| + |F_2| + |F_3|) = 2m - 2$ and therefore $|F_1| + |F_2| + |F_3| = m + 2$. We now let a equal the number of 1's in F_1, b equal the number of 1's in F_2, c equal the number of 1's in F_3, d equal the number of 2's in F_3 and e equal the number of 3's in F_3. We are assuming that F_2 contains a 2, so that F_3 cannot contain a 4. Then, because $|F_1| + |F_2| + |F_3| = m + 2$, we have

$$a + \frac{m-a}{2} + 1 + b + \frac{m-2-b}{3} + c + d + e + \frac{m-c-2d-3e}{6} = m + 2$$

Rearranging yields

$$\frac{a}{2} + \frac{1}{3} + \frac{2b}{3} + \frac{5c + 4d + 3e}{6} = 2$$

and then clearing denominators yields

$$3a + 4b + 5c + 4d + 3e = 10$$

There are 7 solutions for (a, b, c, d, e): $(0, 0, 2, 0, 0)$, $(2, 1, 0, 0, 0)$, $(1, 1, 0, 0, 1)$, $(0, 1, 0, 0, 2)$, $(2, 0, 0, 1, 0)$, $(1, 0, 0, 1, 1)$, and $(0, 0, 0, 1, 2)$. It is easy to verify that all 7 possibilities contradict $2n \geq \sum_{i=1}^{r} \sum_{b \in G_i} \sum_{a \in F_i} \big(b - (b, a)\big)$. For instance, consider $(a, b, c, d, e) = (0, 0, 2, 0, 0)$: since F_2 contains a 2 and F_3 contains two 1's,

$$\sum_{i=1}^{r} \sum_{b \in G_i} \sum_{a \in F_i} \big(b - (b, a)\big) \geq \frac{(3 - (3, 2))}{3} \left(n - 12 - \frac{4n}{f_{2,3}}\right) + \frac{2(6 - (6, 1))}{6} \left(n - 60 - \frac{4n}{f_{3,6}}\right)$$

whence

$$2n \geq \frac{2}{3} \left(n - 12 - \frac{4n}{f_{2,3}}\right) + \frac{5}{3} \left(n - 60 - \frac{4n}{f_{3,6}}\right)$$

or $\frac{n}{3} \leq 72 + 4n(\frac{1}{f_{2,3}} + \frac{1}{f_{3,6}})$, a contradiction since $n \geq 4m > 600$. The other 6 cases result in a similar contradiction, and therefore when $n \geq 4m$, we reach a contradiction.

This concludes our proof of the $f_{1,2} > 4$, $f_{2,3} > 4$, $f_{3,6} > 4$ case when $n \geq 4m$. When we remove the restriction that $n \geq 4m$, the argument remains similar. The only difference is that there are many more cases to analyze, for which we simply write a computer program to run through all possible cases. The program eliminates many possibilities with two key lemmas from Section 2, namely Lemmas 2.8 and 2.9; the program then confirms that all possibilities result in $\sum_{i=1}^{r} \sum_{b \in G_i} \sum_{a \in F_i} \big(b - (b, a)\big)$ being larger than $2n$, and thus shows that the $D = [2, 3, 6]$ case cannot actually occur.

The conclusion of the $D = [2, 3, 6]$ case concludes our proof of the third subcase. □

Proof of Fourth Subcase. The fourth and final subcase is when exactly two of the three points satisfies $f_{i,2} > 4$. We let F_1 and F_2 be these two points, and we observe that by

Proposition 3.8, $|F_1|, |F_2| \geq \frac{m-12}{2} + 1 = \frac{m}{2} - 5$. By (2.5),

$$2m - 2 = \sum_{i=1}^{r} (m - |F_i|) = \sum_{1 \leq i \leq 3} (m - |F_i|) + \sum_{i=4}^{r} (m - |F_i|)$$

But recall that $\sum_{i=4}^{r} (m - |F_i|) \leq 2$ and hence

$$2m - 2 \leq \sum_{1 \leq i \leq 3} (m - |F_i|) + 2 = 3m - |F_1| - |F_2| - |F_3| + 2$$

But since $|F_1|, |F_2| \geq \frac{m}{2} - 5$ this implies that

$$|F_3| \leq m + 4 - |F_1| - |F_2| \leq 2m + 4 - (m - 10) = 14$$

Hence $|F_3|$ is extremely small and so this case loosely corresponds to $D = [2, 2, \infty]$. In particular, it is impossible for $f_{i,k} > 4$ for $3 \leq k \leq 6$. The proof of this case is far more difficult than the proof of the other three subcases, primarily because the small size of F_3 makes it hard to control F_3. We now present an extensive outline of the proof.

We first recall that $|F_3| \leq m+4-|F_1|-|F_2|$; we therefore attempt to bound $|F_3|$ from above by bounding $|F_1|$ and $|F_2|$ from below. To do this, we must utilize our knowledge of F_1 and F_2, and specifically the fact that $f_{1,2}, f_{2,2} > 4$. This implies by (3.6) that $g_{1,2}, g_{2,2} \geq \frac{n-4}{2} - \frac{2n}{\frac{m-12}{2}} = \frac{n-4}{2} - \frac{4n}{m-12}$. Now observe that the presence of any number larger than 2 in either F_1 or F_2 will cause $\sum_{i=1}^{r} \sum_{a \in F_i} \sum_{b \in G_i} \big(a - (a, b)\big)$ to increase tremendously. Indeed, if $a > 2$ and $b = 2$, then $a - (a, b) \geq \max(a - 2, 2)$ and hence $\sum_{i=1}^{r} \sum_{a \in F_i} \sum_{b \in G_i} \big(a - (a, b)\big)$ will increase by at least $\max(a - 2, 2) \left(\frac{n-4}{2} - \frac{4n}{m-12}\right)$. But this quantity is at least roughly n, and since $2m \geq \sum_{i=1}^{r} \sum_{a \in F_i} \sum_{b \in G_i} \big(a - (a, b)\big)$, we can easily establish an upper bound on the number of numbers in $F_1 \cup F_2$ that are larger than 2. Moreover, since $\max(a - 2, 2) \left(\frac{n-4}{2} - \frac{4n}{m-12}\right)$ increases as a increases, we can also establish an upper bound on the sum of all numbers in $F_1 \cup F_2$ that are larger than 2. We therefore possess stringent upper bounds on $\sum_{i \geq 3} f_{2,i}$ and $\sum_{i \geq 3} i \cdot f_{2,i}$ and $\sum_{i \geq 3} f_{3,i}$ and $\sum_{i \geq 3} i \cdot f_{3,i}$. By similar logic in the opposite direction, we establish strict upper bounds on $\sum_{i \geq 3} g_{2,i}$ and $\sum_{i \geq 3} i \cdot g_{2,i}$ and $\sum_{i \geq 3} g_{3,i}$ and $\sum_{i \geq 3} i \cdot g_{3,i}$.

Equipped with these bounds on the larger elements of $F_1 \cup F_2$ and $G_1 \cup G_2$, we achieve lower bounds on $|F_1|, |F_2|, |G_1|$ and $|G_2|$. We therefore arrive at strong upper bounds on $|F_3|$ and $|G_3|$. These bounds are sufficiently strong that there are very few possibilities for F_3 and G_3, and so we write a computer program to generate all of these possibilities. For each potential pair (F_3, G_3), the program generates all possible (F_1, F_2, G_1, G_2). The program then uses these 6 multisets to demonstrate that $F_4, F_5, \ldots$ and $G_4, G_5, \ldots$ must all be equivalent to $[1^m]$ and $[1^n]$, respectively. Finally, the program demonstrates that

either $F_1 \cup F_2$ or $G_1 \cup G_2$ must consist of entirely 1's and 2's, whence either (2.3.1) or (2.3.2) holds. This concludes our outline of the proof of this fourth and final subcase. □

The resolution of these four subcases proves Theorem 2.3 in the case that exactly 3 i's satisfy $f_{i,1} > 4$. We have therefore proved Theorem 2.3 in this section under the hypothesis that $42m \geq n \geq m > 150$. In the next section, we reinterpret and refine our results, and clarify their importance. □

4. Refinements of Our Results

In this section we refine our main results by giving a more precise description of the rational functions f and g satisfying the hypotheses of those results.

More precisely, if f and g satisfy the hypotheses of any of Theorems 1.3, 1.6 or 2.3, then we will show that one of the following occurs, up to changing variables:

(4.0.1) At least one of f or g is on a short list of simple functions (such as X^m), and the other is almost completely determined.

(4.0.2) Both f and g both have degree ≤ 80, and are on an explicit finite (but long) list.

As was noted following Theorem 1.3, conditions (1.3.1) and (1.6.1) imply that at least one of f or g is on a short list of simple functions. One such case is $f = X^m$; here we determine the corresponding functions g in case $m > 6$, by showing that (up to changing variables) $g(X) = X^a h(X)^m$ for some integer a coprime to m and some $h \in \mathbb{C}(X)$.

Proof. By (2.7) we have

$$\sum_{i=1}^{2} \sum_{b \in G_i} \big(m - (m,b)\big) \in \{2m-2, 2m\}.$$

Let D be the multiset of values $\frac{m}{(m,b)}$ where $b \in G_1 \cup G_2$ and $m \nmid b$ so that D is a finite multiset of integers greater than 1 and $\sum_{d \in D}\big(1 - \frac{1}{d}\big) \leq 2$. By Lemma 3.3, either $|D| \leq 2$ or D is one of $[2^4]$, $[3^3]$, $[2, 4^2]$, $[2^2, k]$ with $k > 1$, or $[2, 3, \ell]$ with $2 \leq \ell \leq 6$. By (2.9.1), $\gcd(F_1 \cup F_2 \cup G_1 \cup G_2) = 1$, or $\gcd(m, G_1 \cup G_2) = 1$. Hence the least common multiple of the elements of D must be m, so (since $m > 6$) either $|D| \leq 2$ or $D = [2^2, k]$. If $D = [2^2, k]$, at least one of G_1 and G_2 (say G_1) consists of elements divisible by $\frac{m}{2}$, so $\frac{m}{2}$ divides the sum of the elements in G_1, which is n. Hence $\frac{m}{2}$ also divides the sum of the elements in G_2; since $\frac{m}{2}$ divides all but at most one element of G_2, it must divide all elements of G_2, so $\frac{m}{2} \mid \frac{m}{k}$ and thus $k \mid 2$, contrary to the condition $\operatorname{lcm}(D) = m$. Thus $|D| \leq 2$, so since $\sum_{d \in D}\big(m - \frac{m}{d}\big) \geq 2m - 2$ we must have $D = [m^2]$. By replacing f and g by $f \circ \nu_1$ and $g \circ \nu_2$ for some degree-one $\nu_i \in \mathbb{C}(X)$, we may assume that $f(0) = Q_1$, $f(\infty) = Q_2$, and that

the two points P in $g^{-1}(\{Q_1, Q_2\})$ for which $m \nmid e_g(P)$ are 0 and ∞. By replacing f and g by $\mu \circ f$ and $\mu \circ g$ for some degree-one $\mu \in \mathbb{C}(X)$, we may assume that $Q_1 = 0$, $Q_2 = \infty$, and the numerator and denominator of f have the same leading coefficient. It follows that $f(X) = X^m$ and $g(X) = X^a h(X)^m$ for some a coprime to m and some $h \in \mathbb{C}(X)$. $\square$

If f and g both have degree ≤ 80, then our proof of Theorem 2.3 produces an explicit (but long) list of possibilities for the ramification types of f and g. In order to determine which of these ramification types actually correspond to rational functions f and g for which the numerator of $f(X) - g(Y)$ is irreducible, we used the following result of Hurwitz, which reduces the question to a problem about tuples of elements in a certain finite symmetric group:

Theorem 4.1 (Hurwitz)**.** *For any positive integer m, any multisets $A_1, \dots, A_r$ consisting of positive integers, and any distinct $Q_1, \dots, Q_r \in \mathbb{C} \cup \{\infty\}$, the following are equivalent:*

(4.1.1) *there exists a degree-m rational function $f(X) \in \mathbb{C}(X)$ such that $E_f(Q_i) = A_i$ and $E_f(Q) = [1^m]$ for each $Q \notin \{Q_1, \dots, Q_r\}$*

(4.1.2) *all three of the following hold:*

- $\sum_{a \in A_i} a = m$ *for each i with $1 \leq i \leq r$*
- $\sum_{i=1}^r (m - |A_i|) = 2m - 2$
- *there are elements $g_1, \dots, g_r \in S_m$ such that the multiset of cycle lengths of g_i is A_i, the product $g_1 g_2 \dots g_r$ is the identity permutation, and the subgroup of S_m generated by $g_1, \dots, g_r$ is transitive.*

Theorem 4.1 can be combined with (2.7) and Fried's reducibility theorem [15] in order to give a similar characterization of the ramification types of pairs of rational functions (f, g) for which the numerator of $f(X) - g(Y)$ defines an irreducible curve of genus 0 or 1. Moreover, a refinement of Theorem 4.1 describes the number of functions f satisfying (4.1.1), up to a change of variables. In each case we used various computational methods to produce the required number of rational functions having the prescribed ramification type, thereby determining all low-degree functions satisfying the hypotheses of Theorem 1.3.

Here is one example of rational functions having a prescribed ramification type: one possibility is that the F_i's are $[1, 3], [2^2], [1^2, 2], [1^2, 2]$, and that $F_i = G_i$ for each i. In this case the corresponding rational functions are as follows, up to changing variables. For any complex number t such that $t^2 \neq 0, 1, 3, -3, 9$ and $t^2 - 6t + 3 \neq 0$, we define $u := -\frac{1}{6} \cdot \frac{t^2+3}{t^2-3}$ and $v := \frac{\frac{1}{3}t^2+1}{t^2+6t-3}$. We then define $f := \frac{\left(X^2+X+3+u^2-\frac{1}{12}\right)^2}{X}$ and $g := -\frac{1}{8} \cdot \frac{\left(t^2+6t-3\right)^3}{\left(t^2-3\right)^3} \cdot \frac{\left(X^2+X+3+v^2-\frac{1}{12}\right)^2}{X}$. It turns out that $f(X) - g(Y)$ is irreducible of genus 0, and that there exist $\hat{f}$ and $\hat{g}$ for which

$f \circ \hat{f} = g \circ \hat{g}$. We computed explicit expressions for all such $\hat{f}$ and $\hat{g}$; they are considerably more complicated than the expressions for f and g.

5. A Dynamical Application

In this section, we present an application of our results. Cahn, Jones, and Spear [9] conjectured that for $f, g \in \mathbb{Q}(X)$ with degree at least 2 and $c \in \mathbb{Q}$, the set $\mathcal{A} := \{n \in \mathbb{N} : g^n(c) \in f(\mathbb{Q})\}$ must be the union of finitely many numbers and finitely many one-sided arithmetic progressions, where $g^n(X)$ denotes the n-th iterate of $g(X)$. This conjecture was recently proven by Hyde and Zieve. Using our results, we can refine the result to show that each arithmetic progression has common difference and smallest element being at most $4 + (\deg f)^2$. This application is especially interesting since it involves no irreducibility hypothesis. Due to space constraints, we only sketch the proof.

Sketch of Proof. We may assume that $\mathcal{A}$ is infinite, so that for each n the equation $f(X) = g^n(Y)$ has infinitely many rational solutions, and hence (by Faltings' theorem) the numerator of $f(X) - g^n(Y)$ has an irreducible factor in $\mathbb{C}[X, Y]$ which has rational coefficients and defines a curve of genus 0 or 1. Choose such factors $H_n(X, Y)$ such that $H_{n+1}(X, Y)$ divides the numerator of $H_n(X, g(Y))$ for every n. For simplicity we assume that $H_n(X, Y) = 0$ has genus 0 for every n, so that its zeroes can be parametrized as $(X, Y) = (a_n(t), b_n(t))$ for some $a_n, b_n \in \mathbb{Q}(X)$, whence the equation $b_n(X) = g^m(Y)$ has infinitely many rational solutions for all $n, m \in \mathbb{N}$.

Crucially $\deg(b_{n+m}) \leq \deg(b_n)$, with equality holding precisely when $b_n(X) - g^m(Y)$ is irreducible. By our results, if $b_n(X) - g^m(Y)$ is irreducible then we obtain strong constraints on b_n and g^m. If this irreducibility happened for several consecutive values of m, then we can combine the constraints on b_n and g^m in order to show (using Fried's reducibility theorem [15]) that $b_n(X) - g^m(Y)$ would be irreducible for every m. It follows that if $\deg(b_{n+m}) < \deg(b_n)$ for some m then this must occur for some small m, which via a short argument implies that the smallest element of each arithmetic progression is small. Similar arguments bound the common difference of each arithmetic progression, and yield the result when some $H_n(X, Y) = 0$ has genus 1. □

6. Conclusion

In this paper, we use combinatorial and algebraic methods to prove a geometric result, Theorem 2.3, that describes the ramification of large-degree complex rational functions f and g for which the numerator of $f(X) - g(Y)$ defines an irreducible curve of genus 0 or 1. We deduce two consequences: the number theoretic Theorem 1.3 addressing rational functions

$f, g \in \mathbb{Q}(X)$ for which $f(\mathbb{Q}) \cap g(\mathbb{Q})$ is infinite, and the analytic Theorem 1.6 regarding the functional equation $f \circ \hat{f} = g \circ \hat{g}$ with $f, g \in \mathbb{C}(X)$ and $\hat{f}, \hat{g}$ meromorphic on $\mathbb{C}$. The results illustrate that the rational functions satisfying any of these conditions are unexpectedly nice: it must be the case that either the Galois closure of $\mathbb{C}(X)/\mathbb{C}(f(X))$ has genus 0 or 1 (in which case all corresponding functions are understood), or the analogous condition holds for g, or that there is a change of variables turning the equation $f(X) = g(Y)$ into the special equation $X^c(X-1)^d = \gamma Y^c(Y-1)^d$, or that the ramification types of f and g are confined to an explicit list. Our results resolve a 1973 question of Fried, and (under an irreducibility hypothesis) resolve a 1924 question of Ritt and a 1997 question of Lyubich and Minsky. In addition, we obtain a quantitative refinement of a 2015 conjecture by Cahn, Jones and Spear.

In the future, we will attempt to remove the irreducibility hypothesis from our main results. As was illustrated in Section 5, the irreducible case can often serve as the base case for an inductive approach to tackle the reducible case. We hope to achieve a result in the reducible case by such an inductive approach, combining the reducibility result from [15] with refinements of the group-theoretic results in [1, 17, 20, 22, 26].

7. Acknowledgements

I would like to acknowledge several individuals and organizations whose support has been invaluable in conducting this research project. First and foremost, I want to thank Professor Michael E. Zieve from the University of Michigan for suggesting this project and mentoring me for almost the past two years. Professor Zieve's role has been incredibly influential; his ever-present guidance has helped me throughout this project, and he deserves immense credit for much of my mathematical achievement and inspiration. Thao Do from MIT also played a critical role in connecting me to this research question and in mentoring me for the first year of the project. I would like to thank the MIT-PRIMES program for providing me the opportunity of conducting valuable and groundbreaking mathematical research with wonderful mentors; in particular, Tanya Khovanova and several other leaders at MIT-PRIMES were instrumental in guiding me throughout the strenous process. I also wish to acknowledge the immense contributions of my parents, and their never-ending stream of support and encouragement.

References

[1] M. Aschbacher, *On conjectures of Guralnick and Thompson*, J. Algebra **135** (1990), 277–343.

[2] 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.

[3] M. Baker and L. De Marco, *Special curves and postcritically finite polynomials*, Forum Math. Pi **1** (2013), e3, 35 pp.

[4] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Annals of Math. **181** (2015), 191–242.

[5] M. Bhargava and A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank* 0, Annals of Math. **181** (2015), 587–621.

[6] M. Bhargava, C. Skinner and W. Zhang, *A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture*, arXiv:1407.1826 (2014).

[7] Y. F. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), 261–288.

[8] M. Briskin, N. Roytvarf and Y. Yomdin, *Center conditions at infinity for Abel differential equations*, Annals of Math. (2) **172** (2010), 437–483.

[9] J. Cahn, R. Jones and J. Spear, *Powers in orbits of rational functions: cases of an arithmetic dynamical Mordell-Lang conjecture*, arXiv:1512.03085 (2015).

[10] J. Carlson, A. Jaffe and A. Wiles (eds.), The Millennium Prize Problems, Clay Mathematics Institute, Cambridge, MA (2006).

[11] A. Carney, T. Do, J. Hallett, Y. Jiang, B. L. Weiss, E. Wells and M. E. Zieve, *Diophantine equations with separated variables, I: the irreducible case*, preprint (2015).

[12] A. Carney, J. Hallett, Q. Sun, B. L. Weiss, Y. Xia and M. E. Zieve, *Diophantine equations with separated variables, II: the reducible case*, preprint (2015).

[13] H. Davenport, D. J. Lewis and A. Schinzel, *Equations of the form $f(x) = g(y)$*, Quart. J. Math. Oxford (2) **12** (1961), 304–312.

[14] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[15] 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.

[16] M. D. Fried, *On a theorem of Ritt and related Diophantine problems*, J. Reine Angew. Math. **264** (1973), 40–55.

[17] D. Frohardt and K. Magaard, *Composition factors of monodromy groups*, Annals of Math. **154** (2001), 327–345.

[18] D. Ghioca, T. J. Tucker and M. E. Zieve, *Intersections of polynomial orbits, and a dynamical Mordell–Lang conjecture*, Invent. Math. **171** (2008), 463–483.

[19] D. Ghioca, T. J. Tucker and M. E. Zieve, *Linear relations between polynomial orbits*, Duke Math. J. **161** (2012), 1379–1410.

[20] R. M. Guralnick and J. G. Thompson, *Finite groups of genus zero*, J. Algebra **131** (1990), 303–341.

[21] H. W. Lenstra, Jr., *Solving the Pell equation*, Notices of the Amer. Math. Soc **49** (2002), 182–192.

[22] M. Liebeck and A. Shalev, *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc. **12** (1999), 266–314.

[23] M. Lyubich and Y. Minsky, *Laminations in holomorphic dynamics*, J. Diff. Geom. **47** (1997), 17–94.

[24] A. Medvedev and T. Scanlon, *Invariant varieties for polynomial dynamical systems*, Annals of Math. **179** (2014), 81–177.

[25] J. Milnor, *On Lattès maps*, in: Dynamics on the Riemann sphere, pages 9–43. Eur. Math. Soc., Zürich, 2006.

[26] D. Neftin and M. E. Zieve, *Monodromy groups of minimal covers*, preprint (2016).

[27] R. Nevanlinna, *Einige Eindeutigkeitssätze in der Theorie der Meromorphen Funktionen*, Acta Math. **48** (1926), 367–391.

[28] K. D. Nguyen, *Algebraic independence of local conjugacies and related questions in polynomial dynamics*, Proc. Amer. Math. Soc. **143** (2015), 1491–1499.

[29] F. Pakovich, *On polynomials sharing preimages of compact sets, and related questions*, Geom. Funct. Anal. **18** (2008), 163–183.

[30] F. Pakovich, *Prime and composite Laurent polynomials*, Bull. des Sci. Math. **133** (2009), 693–732.

[31] F. Pakovich, *On the equation $P(f) = Q(g)$ where P, Q are polynomials and f, g are entire functions*, Amer. J. Math. **132** (2010), 1591–1607.

[32] F. Pakovich, *Algebraic curves $P(x) - Q(y) = 0$ and functional equations*, Complex Var. Elliptic Equ. **56** (2011), 199–213.

[33] F. Pakovich and M. Muzychuk, *Solution of the polynomial moment problem*, Proc. London Math. Soc. (3) **99** (2009), 633–657.

[34] E. Picard, *Démonstration d'un théorème général sur les fonctions uniformes liées par une relation algébrique*, Acta Math. **11** (1887), 1–12.

[35] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51–66.

[36] J. F. Ritt, *Permutable rational functions*, Trans. Amer. Math. Soc. **25** (1923), 399–448.

[37] A. Schinzel, Selected Topics on Polynomials, The Univ. of Michigan Press, Ann Arbor, 1982.

[38] C. L. Siegel, *The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$*, J. London Math. Soc. **1** (1926), 66–68.

[39] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **142** (1995), 443–551.

[40] U. Zannier, *On a functional equation relating a Laurent series $f(x)$ to $f(x^m)$*, Aequat. Math. **55** (1998), 15–43.

[41] M. E. Zieve, *Decompositions of Laurent polynomials*, arXiv:0710.1902 (2007).