LANDEN TRANSFORMS AS FAMILIES OF (COMMUTING) RATIONAL SELF-MAPS OF PROJECTIVE SPACE

MICHAEL JOYCE[1,a], SHU KAWAGUCHI[2,b] AND JOSEPH H. SILVERMAN[3,c]

[1]Department of Mathematics, Tulane University, New Orleans, LA 70118, USA.

[a]E-mail: mjoyce3@tulane.edu

[2]Department of Mathematics, Faculty of Science, Kyoto University, Kyoto, 606-8502, Japan.

[b]E-mail: kawaguch@math.kyoto-u.ac.jp

[3]Mathematics Department, Box 1917 Brown University, Providence, RI 02912, USA.

[c]E-mail: jhs@math.brown.edu

Abstract

The classical (m, k)-Landen transform $\mathfrak{F}_{m,k}$ is a self-map of the field of rational functions $\mathbb{C}(z)$ obtained by forming a weighted average of a rational function over twists by m'th roots of unity. Identifying the set of rational maps of degree d with an affine open subset of $\mathbb{P}^{2d+1}$, we prove that $\mathfrak{F}_{m,0}$ induces a dominant rational self-map $\mathfrak{R}_{d,m,0}$ of $\mathbb{P}^{2d+1}$ of algebraic degree m, and for $1 \leq k < m$, the transform $\mathfrak{F}_{m,k}$ induces a dominant rational self-map $\mathfrak{R}_{d,m,k}$ of algebraic degree m of a certain hyperplane in $\mathbb{P}^{2d+1}$. We show in all cases that $\mathfrak{R}_{d,m,k}$ extends nicely to $\mathbb{P}^{2d+1}_{\mathbb{Z}}$, and that $\{\mathfrak{R}_{d,m,0} : m \geq 0\}$ is a commuting family of maps.

1. Introduction

The Landen transform, also known as Gauss' arithmetic-geometric mean, is a self-map of the space of rational functions in one variable. The purpose of this note is to study the generalized Landen transform from the viewpoint of arithmetic geometry and arithmetic dynamics. We defer until Section 2 a

discussion of the history and historical applications of the Landen transform, and devote this introduction to describing our main results.

The following proposition characterizes the generalized Landen transform.

Proposition 1. *Let $m \geq 1$ and $0 \leq k < m$ be integers, let K be a field in which $m \neq 0$, and let ζ_m be a primitive m'th root of unity in an extension field of K. Then for each rational function $\varphi(z) \in K(z)$ there is a unique rational function $\mathfrak{F}_{m,k}(\varphi)(z) \in K(z)$, called the (m, k)-Landen transform of φ, characterized by the formula*

$$\mathfrak{F}_{m,k}(\varphi)(w^m) = \frac{1}{mw^k} \sum_{t=0}^{m-1} \zeta_m^{-kt} \varphi(\zeta_m^t w). \tag{1.1}$$

As a warm-up for our main result, we give the elementary proof of Proposition 1 in Section 2; see Proposition 12.

We denote the space of rational functions of degree d by Rat_d, and we identify Rat_d with an affine open subset of $\mathbb{P}^{2d+1}$ by assigning the degree d rational function

$$\varphi_{\boldsymbol{a},\boldsymbol{b}}(z) := \frac{a_0 z^d + a_1 z^{d-1} + a_2 z^{d-2} + \cdots + a_d}{b_0 z^d + b_1 z^{d-1} + b_2 z^{d-2} + \cdots + b_d}$$

to the point

$$[\boldsymbol{a}, \boldsymbol{b}] := [a_0, a_1, \ldots, a_d, b_0, b_1, \ldots, b_d] \in \mathbb{P}^{2d+1}.$$

In this way Rat_d is an affine scheme over $\mathbb{Z}$, and for any field K, we may view $K(z)$ as a disjoint union

$$K(z) = \bigcup_{d=0}^{\infty} \mathrm{Rat}_d(K) \subset \bigcup_{d=0}^{\infty} \mathbb{P}^{2d+1}(K). \tag{1.2}$$

However, we note that in general, the degree of $\mathfrak{F}_{m,k}(\varphi)(z)$ may be strictly smaller than the degree of $\varphi(z)$, so the Landen transform $\mathfrak{F}_{m,k} : K(z) \to K(z)$ does not respect the disjoint union decomposition (1.2). For example, if $\varphi(z)$ is a polynomial, then $\deg \mathfrak{F}_{m,k}(\varphi)(z) \leq \frac{1}{m} \deg \varphi(z)$; see Section 7. Our main result describes the rational self-maps of $\mathbb{P}_{\mathbb{Z}}^{2d+1}$ induced by the action of $\mathfrak{F}_{m,k}$ on a Zariski open subset of Rat_d.

Theorem 2. *Let $m \geq 1$ and $0 \leq k < m$ be integers.*

(a) *For each $d \geq 1$ there is a unique rational map*

$$\mathfrak{R}_{d,m,k} : \mathbb{P}_{\mathbb{Z}}^{2d+1} \dashrightarrow \mathbb{P}_{\mathbb{Z}}^{2d+1}$$

with the property that for all fields K in which $m \neq 0$ and for all degree d rational functions $\varphi_{\boldsymbol{a},\boldsymbol{b}}(z) \in \operatorname{Rat}_d(K) \subset K(z)$ whose (m,k)-Landen transform satisfies

$$\deg_z \mathfrak{F}_{m,k}(\varphi_{\boldsymbol{a},\boldsymbol{b}})(z) = d,$$

we have

$$\mathfrak{F}_{m,k}(\varphi_{\boldsymbol{a},\boldsymbol{b}})(z) = \mathfrak{R}_{d,m,k}\big([\boldsymbol{a},\boldsymbol{b}]\big).$$

(b) *The indeterminacy locus of $\mathfrak{R}_{d,m,k}$ is the linear subspace*

$$\mathcal{Z}(\mathfrak{R}_{d,m,k}) = \big\{[\boldsymbol{a},\boldsymbol{b}] \in \mathbb{P}_{\mathbb{Z}}^{2d+1} : \boldsymbol{b} = \boldsymbol{0}\big\} \cong \mathbb{P}^d,$$

and the rational map $\mathfrak{R}_{d,m,k}$ induces a morphism

$$\mathfrak{R}_{d,m,k} : \mathbb{P}_{\mathbb{Z}}^{2d+1} \smallsetminus \mathcal{Z}(\mathfrak{R}_{d,m,k}) \longrightarrow \mathbb{P}_{\mathbb{Z}}^{2d+1} \smallsetminus \mathcal{Z}(\mathfrak{R}_{d,m,k}).$$

(c) *The map $\mathfrak{R}_{d,m,0} : \mathbb{P}_{\mathbb{Z}}^{2d+1} \dashrightarrow \mathbb{P}_{\mathbb{Z}}^{2d+1}$ is a dominant rational map of algebraic degree m.*

(d) *For $1 \leq k < m$, the image of the rational map $\mathfrak{R}_{d,m,k}$ is the hyperplane*

$$\big\{[\boldsymbol{a},\boldsymbol{b}] \in \mathbb{P}_{\mathbb{Z}}^{2d+1} : a_0 = 0\big\} \cong \mathbb{P}_{\mathbb{Z}}^{2d}. \tag{1.3}$$

For all $0 \leq k < m$, the map $\mathfrak{R}_{d,m,k}$ induces a dominant rational map of algebraic degree m from the hyperplane (1.3) to itself.

Example 3. We consider the case $d = 2$ and $m = 2$. Using the calculation given later in Example 13, we find that $\mathfrak{R}_{2,2,0}$ and $\mathfrak{R}_{2,2,1}$ are degree 2 rational maps $\mathbb{P}^5 \dashrightarrow \mathbb{P}^5$ given by the formulæ

$$\mathfrak{R}_{2,2,0} = [b_0 a_0,\ b_2 a_0 - b_1 a_1 + b_0 a_2,\ b_2 a_2,\ b_0^2,\ 2b_2 b_0 - b_1^2,\ b_2^2],$$
$$\mathfrak{R}_{2,2,1} = [0,\ -b_1 a_0 + b_0 a_1,\ b_2 a_1 - b_1 a_2,\ b_0^2,\ 2b_2 b_0 - b_1^2,\ b_2^2].$$

As predicted by Theorem 2(b), both $\mathfrak{R}_{2,2,0}$ and $\mathfrak{R}_{2,2,1}$ have indeterminacy locus equal to the 2-dimensional linear subspace $\{[\boldsymbol{a}, \boldsymbol{0}]\} \subset \mathbb{P}^5$. One can check that it requires more than simply blowing up $\mathbb{P}^5$ along this subspace in order to make $\mathfrak{R}_{2,2,0}$ and $\mathfrak{R}_{2,2,1}$ into morphisms.

Taking $k = 0$ leads to interesting families of commuting maps. (See Proposition 16 for general composition properties of $\mathfrak{R}_{m,k,d}$.)

Corollary 4. *Fix a degree d. Then*

$$\{\mathfrak{R}_{d,m,0} : m = 1, 2, 3, \ldots\}$$

is a set of commuting dominant *rational endomorphisms of* $\mathbb{P}^{2d+1}_{\mathbb{Z}}$ *of algebraic degree m. More precisely, dehomogenizing and specializing, the maps* $\mathfrak{R}_{d,m,0}$ *induce commuting dominant polynomial endomorphisms of the affine linear subspaces*

$$\{[\boldsymbol{a}, \boldsymbol{b}] \in \mathbb{P}^{2d+1} : b_0 \neq 0\} \cong \mathbb{A}^{2d+1}$$

and

$$\{[\boldsymbol{a}, \boldsymbol{b}] \in \mathbb{P}^{2d+1} : a_0 = 0 \text{ and } b_0 \neq 0\} \cong \mathbb{A}^{2d}.$$

Remark 5. The classification of commuting rational maps in one variable was solved by Ritt [22] in the 1920s. More recently, there has been some work on classifying commuting *endomorphisms* of $\mathbb{P}^n$ [10, 11], as well as various papers, including [1, 9], that study higher dimensional Lattès maps, and work on commuting birational self-maps of $\mathbb{P}^2$ (and more generally of a compact Kähler surface) [7]. But there seem to be few non-trivial examples known of commuting *rational* (non-birational) self-maps of $\mathbb{P}^n$, and as far as we are aware, the family of commuting Landen maps described in Corollary 4 has not previously been studied.

Remark 6. If we treat rational maps of degree $d-1$ as degenerate maps of degree d, we obtain a natural embedding

$$\iota_{d-1,d} : \mathbb{P}^{2d-1} \longrightarrow \mathbb{P}^{2d+1},$$
$$[a_0, \ldots, a_{d-1}, b_0, \ldots, b_{d-1}] \longmapsto [0, a_0, \ldots, a_{d-1}, 0, b_0, \ldots, b_{d-1}].$$

Then the maps in Theorem 2 fit together via

$$\mathfrak{R}_{d,m,k} \circ \iota_{d-1,d} = \iota_{d-1,d} \circ \mathfrak{R}_{d-1,m,k}.$$

Remark 7. Since $\mathbb{P}_{\mathbb{Z}}^{2d+1}$ is smooth, the rational function $\mathfrak{R}_{d,m,k}$ is defined off of a codimension 2 subscheme. (Theorem 2(b) says that in fact, the indeterminacy locus has codimension $d+1$.) In particular, $\mathfrak{R}_{d,m,k}$ induces a rational map on every special fiber $\mathbb{P}_{\mathbb{F}_p}^{2d+1} \dashrightarrow \mathbb{P}_{\mathbb{F}_p}^{2d+1}$, even if $p \mid m$, despite the $\frac{1}{m}$ factor appearing in the formula (1.1) defining $\mathfrak{F}_{m,k}$.

Remark 8. It follows from Proposition 16 and Theorem 2(c) that

$$\deg \mathfrak{R}_{d,m,0}^r = \deg \mathfrak{R}_{d,m^r,0} = m^r = (\deg \mathfrak{R}_{d,m,0})^r,$$

so $\mathfrak{R}_{d,m,0}$ is algebraically stable, and its dynamical degree is m. And similarly for the restriction of $\mathfrak{R}_{d,m,k}$ to the hyperplane (1.3).

Question 9. There are many further natural questions that one might ask about the Landon maps described in this paper, including for example:

(1) Is there a birational covering $X \to \mathbb{P}_{\mathbb{Q}}^{2d+1}$ such that $\mathfrak{R}_{d,m,0}$ extends to a self-morphism of X, and similarly for $\mathfrak{R}_{d,m,k}$ on the appropriate hyperplane in $\mathbb{P}_{\mathbb{Q}}^{2d+1}$? And the same question over $\mathbb{Z}$.
(2) Does $\mathfrak{R}_{d,m,k}$ preserve a pencil?
(3) Is $\mathfrak{R}_{d,m,k}$ birationally conjugate to a higher-dimensional Lattès map?

We conclude the introduction by summarizing the contents of this article. Section 2 briefly describes some of the history and uses of the Landen transformation. Section 3 illustrates the Landen transform by giving explicit formulas for $\mathfrak{F}_{m,k}(\varphi)$ when φ has degree 2 and 3 and m equals 2 and 3. Sections 4 and 5 give, respectively, the effect of $\mathfrak{F}_{m,k}$ on formal Laurent series and an elementary composition formula for $\mathfrak{F}_{m,k}$. In Section 6 we prove a key proposition that writes $\mathfrak{F}_{m,k}(\varphi)(z)$ as a quotient of polynomials $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)/H_{\boldsymbol{b},m}(z)$ whose coefficients are $\mathbb{Z}$-integral polynomials in the coefficients of φ, and we describe various properties of $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)$ and $H_{\boldsymbol{b},m}(z)$. This material is used in Section 7 to prove our main result (Theorem 2). We conclude in Section 8 by showing that the coefficients of the denominator $H_{\boldsymbol{b},m}(z)$ of the Landen transformation induces a morphism $\mathbb{P}^d \to \mathbb{P}^d$ that is birationally conjugate to the m'th power map.

Acknowledgment

2. History and Applications

Let K be a field that is not of characteristic 2. The classical Landen transformation is the map $\mathfrak{F} = \mathfrak{F}_{2,1}$ on the space of rational functions $K(z)$ given by the formula

$$\mathfrak{F}(\varphi)(z) = \frac{\varphi(\sqrt{z}) - \varphi(-\sqrt{z})}{2\sqrt{z}}.$$

When $K = \mathbb{R}$ or $\mathbb{C}$, the Landen transformation can be used to numerically compute the integral $\int_0^\infty \varphi(z)\,dz$ for certain choices of the rational function φ. More precisely, for appropriate φ one shows that

$$\int_0^\infty \varphi(z)\,dz = \int_0^\infty \mathfrak{F}(\varphi)(z)\,dz$$

and then studies the dynamics of $\mathfrak{F}$, i.e., the behavior of the orbit $(\mathfrak{F}^n(\varphi))_{n \geq 1}$ of the rational map φ under iteration of the transformation $\mathfrak{F}$. See [2, 3, 4, 5, 8, 13, 16, 17, 19, 21] for work in this area, as well as [18] for a survey of the theory of Landen transformations.

The origins of the subject go back to Landen's work [14, 15] on iterative methods to compute certain integrals. The method was rediscovered and extended by Gauss [12] and is often referred to as Gauss's Arithmetic-Geometric Mean (AGM) method.

The authors of [3] also point to a related transformation

$$\mathfrak{C}(\varphi)(z) = \mathfrak{F}_{2,0}(\varphi)(z) = \frac{\varphi(\sqrt{z}) + \varphi(-\sqrt{z})}{2}$$

whose dynamics is analyzed in [6], and they indicate that there are natural generalizations to higher degree transformations that they plan to study in a future work. These higher degree transformations are the maps $\mathfrak{F}_{m,k}$ described in Proposition 1.

Remark 10. The formula (1.1) for $\mathfrak{F}_{m,k}$ is given in [20], where the author determines a basis for the set of rational functions $\varphi(z) \in \mathbb{C}(z)$ that are fixed by $\mathfrak{F}_{m,k}$.

Remark 11. We observe that if we view $K(z)$ as a K-vector space, then $\mathfrak{F}_{m,k}$ is clearly a K-linear transformation of $K(z)$. However, when we view $K(z)$ as a field, the action of $\mathfrak{F}_{m,k}$ is more complicated.

Proposition 12. *Let $m \geq 1$ and $k \in \mathbb{Z}$. Then for all $\varphi(z) \in K(z)$, the expression* (1.1)

$$\frac{1}{mw^k} \sum_{t=0}^{m-1} \zeta_m^{-kt} \varphi(\zeta_m^t w) \tag{2.1}$$

appearing in Proposition 1 is in $K(w^m)$. Further, it is independent of the choice of a particular primitive m^{th} root of unity ζ_m.

Proof. Let $\bar{K}/K$ be an algebraic closure of K. The field extension $\bar{K}(w)/\bar{K}(w^m)$ is a Kummer extension whose Galois group is cyclic and generated by the automorphism $w \to \zeta w$. (As always, we are assuming that m is prime to the characteristic of K.) But it is easy to check that the expression (2.1) is invariant under the substitution $w \to \zeta w$. Hence it is in $\bar{K}(w^m)$, and indeed in $K(\zeta_m)(w^m)$. Next we observe that (2.1) is also invariant under an element σ in the Galois group of $K(\zeta_m)(w^m)/K(w^m)$, since the effect of such an element is to send ζ_m to ζ_m^j for some j satisfying $\gcd(j, m) = 1$, so it simply rearranges the terms in the sum. This proves that (2.1) is in $K(w^m)$, and also shows that (2.1) does not depend on the choice of ζ_m. $\square$

3. Examples

We compute some examples of Landen transforms for generic rational maps of degrees 2 and 3, i.e., we give explicit formulas for the rational maps $\mathfrak{R}_{d,m,k} : \mathbb{P}^{2d+1} \dashrightarrow \mathbb{P}^{2d+1}$ for small values of d, m, k.

Example 13. Consider the generic rational map of degree 2,

$$\varphi(z) = \frac{a_0 z^2 + a_1 z + a_2}{b_0 z^2 + b_1 z + b_2}.$$

A simple calculation shows that the two transformations $\mathfrak{F}_{2,0}$ and $\mathfrak{F}_{2,1}$ are given by

$$\mathfrak{F}_{2,0}(\varphi)(z) = \frac{b_0 a_0 z^2 + (b_2 a_0 - b_1 a_1 + b_0 a_2)z + b_2 a_2}{b_0^2 z^2 + (2b_2 b_0 - b_1^2)z + b_2^2},$$

$$\mathfrak{F}_{2,1}(\varphi)(z) = \frac{(-b_1 a_0 + b_0 a_1)z + b_2 a_1 - b_1 a_2}{b_0^2 z^2 + (2b_2 b_0 - b_1^2)z + b_2^2},$$

and

$$\mathfrak{F}_{3,0}(\varphi)(z) = \frac{b_0^2 a_0 z^2 + (-b_2 b_1 a_0 - b_2 b_0 a_1 + b_1^2 a_1 - b_1 b_0 a_2)z + b_2^2 a_2}{b_0^3 z^2 + (-3b_2 b_1 b_0 + b_1^3)z + b_2^3},$$

$$\mathfrak{F}_{3,1}(\varphi)(z) = \frac{(-b_2 b_0 a_0 + b_1^2 a_0 - b_1 b_0 a_1 + b_0^2 a_2)z + (b_2^2 a_1 - b_2 b_1 a_2)}{b_0^3 z^2 + (-3b_2 b_1 b_0 + b_1^3)z + b_2^3},$$

$$\mathfrak{F}_{3,2}(\varphi)(z) = \frac{(-b_1 b_0 a_0 + b_0^2 a_1)z + (b_2^2 a_0 - b_2 b_1 a_1 - b_2 b_0 a_2 + b_1^2 a_2)}{b_0^3 z^2 + (-3b_2 b_1 b_0 + b_1^3)z + b_2^3}.$$

Example 14. Similarly, for a generic rational map of degree 3,

$$\varphi(z) = \frac{a_0 z^3 + a_1 z^2 + a_2 z + a_3}{b_0 z^3 + b_1 z^2 + b_2 x + b_3},$$

the first few Landen transforms act by

$$\mathfrak{F}_{2,0} = \frac{b_0 a_0 z^3 + (b_2 a_0 - b_1 a_1 + b_0 a_2)z^2 + (-b_3 a_1 + b_2 a_2 - a_3 b_1)z - b_3 a_3}{b_0^2 z^3 + (2b_2 b_0 - b_1^2)z^2 + (-2b_3 b_1 + b_2^2)z - b_3^2},$$

$$\mathfrak{F}_{2,1} = \frac{(-b_1 a_0 + b_0 a_1)z^2 + (-b_3 a_0 + b_2 a_1 - b_1 a_2 + a_3 b_0)z + (-b_3 a_2 + a_3 b_2)}{b_0^2 z^3 + (2b_2 b_0 - b_1^2)z^2 + (-2b_3 b_1 + b_2^2)z - b_3^2},$$

and

$$\mathfrak{F}_{3,0} = \frac{\begin{array}{c}b_0^2 a_0 z^3 + (2b_3 b_0 a_0 - b_2 b_1 a_0 - b_2 b_0 a_1 + b_1^2 a_1 - b_1 b_0 a_2 + b_0^2 a_3)z^2 \\ + (b_3^2 a_0 - b_3 b_2 a_1 - b_3 b_1 a_2 + b_2^2 a_2 + 2b_3 b_0 a_3 - b_2 b_1 a_3)z + b_3^2 a_3\end{array}}{b_0^3 z^3 + (3b_3 b_0^2 - 3b_2 b_1 b_0 + b_1^3)z^2 + (3b_3^2 b_0 - 3b_3 b_2 b_1 + b_2^3)z + b_3^3},$$

$$\mathfrak{F}_{3,1} = \frac{\begin{array}{c}(-b_2 b_0 a_0 + b_1^2 a_0 - b_1 b_0 a_1 + b_0^2 a_2)z^2 \\ + (-b_3 b_2 a_0 - b_3 b_1 a_1 + b_2^2 a_1 + 2b_3 b_0 a_2 - b_2 b_1 a_2 - b_2 b_0 a_3 + b_1^2 a_3)z + b_2^2 a_2 - b_3 b_2 a_3\end{array}}{b_0^3 z^3 + (3b_3 b_0^2 - 3b_2 b_1 b_0 + b_1^3)z^2 + (3b_3^2 b_0 - 3b_3 b_2 b_1 + b_2^3)z + b_3^3},$$

$$\mathfrak{F}_{3,2} = \frac{\begin{array}{c}(-b_1 b_0 a_0 + b_0^2 a_1)z^2 + (-b_3 b_1 a_0 + b_2^2 a_0 + 2b_3 b_0 a_1 - b_2 b_1 a_1 - b_2 b_0 a_2 + b_1^2 a_2 - b_1 b_0 a_3)z \\ + b_3^2 a_1 - b_3 b_2 a_2 - b_3 b_1 a_3 + b_2^2 a_3\end{array}}{b_0^3 z^3 + (3b_3 b_0^2 - 3b_2 b_1 b_0 + b_1^3)z^2 + (3b_3^2 b_0 - 3b_3 b_2 b_1 + b_2^3)z + b_3^3}.$$

4. The Effect of $\mathfrak{F}_{m,k}$ on Laurent Series

An elementary calculation reveals the effect of $\mathfrak{F}_{m,k}$ on a Laurent series around 0, and in particular on the series associated to a rational function.

Proposition 15. *Let*

$$\varphi(z) = \sum_{n\in\mathbb{Z}} a_n z^n$$

be a (formal) Laurent series. Then

$$\mathfrak{F}_{m,k}(\varphi)(z) = \sum_{j\in\mathbb{Z}} a_{mj+k} z^j.$$

Proof. We compute

$$\mathfrak{F}_{m,k}(\varphi)(w^m) = \frac{1}{mw^k} \sum_{t=0}^{m-1} \zeta_m^{-kt} \varphi(\zeta_m^t w) = \frac{1}{mw^k} \sum_{t=0}^{m-1} \zeta_m^{-kt} \sum_{n\in\mathbb{Z}} a_n (\zeta_m^t w)^n$$

$$= \sum_{n\in\mathbb{Z}} a_n w^{n-k} \left(\frac{1}{m} \sum_{t=0}^{m-1} \zeta_m^{(n-k)t} \right) = \sum_{\substack{n\in\mathbb{Z} \\ n\equiv k \ (\text{mod } m)}} a_n w^{n-k}.$$

This completes the proof of Proposition 15.   □

5. Composition of $\mathfrak{F}_{m,k}$ Operators

The transformations $\mathfrak{F}_{m,k}$ and $\mathfrak{F}_{n,\ell}$ do not generally commute, but they do if $k(n-1) = \ell(m-1)$. In particular, if $k = \ell = 0$, then they commute for all values of m and n. The next elementary result gives a general composition formula.

Proposition 16. *For all $m, n \geq 1$ and all $k, \ell \in \mathbb{Z}$,*

$$\mathfrak{F}_{m,k} \circ \mathfrak{F}_{n,\ell} = \mathfrak{F}_{mn,kn+\ell}.$$

In particular, the r'th iterate of $\mathfrak{F}_{m,k}$ is given by

$$\mathfrak{F}_{m,k}^r = \mathfrak{F}_{m^r,(m^{r-1}+m^{r-2}+\cdots+m+1)k}.$$

Proof. This is easy to prove directly from the definition of $\mathfrak{F}_{m,k}$, but as pointed out by the referee, it is even easier to use Proposition 15. Thus

taking $\varphi(z) = \sum_{i \in \mathbb{Z}} a_i z^i$, we find that

$$\mathfrak{F}_{m,k}\big(\mathfrak{F}_{n,\ell}(\varphi)\big) = \mathfrak{F}_{m,k}\Big(\sum_{i \in \mathbb{Z}} a_{ni+\ell} z^i\Big) = \sum_{j \in \mathbb{Z}} a_{n(mj+k)+\ell} z^j = \mathfrak{F}_{mn,kn+\ell}(\phi).$$

This proves the first formula, and the second follows by induction. $\qquad\square$

Proposition 16 allows us to describe the monoid of $\mathfrak{F}_{m,k}$ operators in terms of a matrix monoid.

Corollary 17. *Let M be the monoid of integral matrices*

$$M = \left\{ \begin{pmatrix} m & 0 \\ k & 1 \end{pmatrix} : m, k \in \mathbb{Z},\ m \geq 1 \right\}$$

under matrix multiplication. Then the map

$$M \longrightarrow \{\mathfrak{F}_{m,k} : m, k \in \mathbb{Z},\ m \geq 1\}, \qquad \begin{pmatrix} m & 0 \\ k & 1 \end{pmatrix} \longmapsto \mathfrak{F}_{m,k}, \qquad (5.1)$$

is a monoid isomorphism.

Proof. The map (5.1) is clearly surjective, while Proposition 16 and the matrix multiplication $\begin{pmatrix} m & 0 \\ k & 1 \end{pmatrix}\begin{pmatrix} n & 0 \\ \ell & 1 \end{pmatrix} = \begin{pmatrix} mn & 0 \\ kn+\ell & 1 \end{pmatrix}$ shows that (5.1) is a monoid homomorphism. For injectivity, we suppose that $\mathfrak{F}_{m,k} = \mathfrak{F}_{n,\ell}$. Proposition 15 tells us that $\mathfrak{F}_{m,k}(z^d)$ is equal to $z^{(d-k)/m}$ if $d \equiv k \pmod{m}$, and equal to 0 otherwise. Taking $d = k + me$, our assumption that $\mathfrak{F}_{m,k} = \mathfrak{F}_{n,\ell}$ implies that

$$z^e = \mathfrak{F}_{m,k}(z^{me+k}) = \mathfrak{F}_{n,\ell}(z^{me+k}) = z^{(me+k-\ell)/n},$$

where necessarily n divides $me + k - \ell$. Equating the exponents, we have

$$(n - m)e = k - \ell \quad \text{for all } e \in \mathbb{Z}.$$

The right-hand side is independent of e, and hence we must have $n = m$ and $k = \ell$, which concludes the proof that (5.1) is injective. $\qquad\square$

6. Writing $\mathfrak{F}_{m,k}$ as a Quotient of Integral Polynomials

Our primary goal in this section is to write $\mathfrak{F}_{m,k}(\varphi)$, for a generic rational function φ of degree d, as a quotient of $\mathbb{Z}$-integral polynomials in z and the

coefficients of φ. We recall from the introduction that we are identifying the space Rat_d of rational functions of degree d with an affine open subset of $\mathbb{P}^{2d+1}$. More precisely, for a $(d+1)$-tuple $\boldsymbol{a} = [a_0, \ldots, a_d]$, we let

$$F_{\boldsymbol{a}}(X,Y) = a_0 X^d + a_1 X^{d-1}Y + a_2 X^{d-2}Y^2 + \cdots + a_d Y^d,$$

and we associate to each point $[\boldsymbol{a}, \boldsymbol{b}] \in \mathbb{P}^{2d+1}$ the rational map

$$\varphi_{\boldsymbol{a},\boldsymbol{b}} : \mathbb{P}^1 \longrightarrow \mathbb{P}^1, \qquad \varphi_{\boldsymbol{a},\boldsymbol{b}}\big([X,Y]\big) = \big[F_{\boldsymbol{a}}(X,Y), F_{\boldsymbol{b}}(X,Y)\big].$$

Then Rat_d is the complement of the resultant hypersurface

$$\mathrm{Rat}_d = \big\{ [\boldsymbol{a}, \boldsymbol{b}] \in \mathbb{P}^{2d+1} : \mathrm{Res}(F_{\boldsymbol{a}}, F_{\boldsymbol{b}}) \neq 0 \big\}.$$

In order to emphasize this inclusion, we let

$$\overline{\mathrm{Rat}}_d \cong \mathbb{P}^{2d+1}.$$

Points $[\boldsymbol{a}, \boldsymbol{b}] \in \overline{\mathrm{Rat}}_d \smallsetminus \mathrm{Rat}_d$ correspond to rational maps $\varphi_{\boldsymbol{a},\boldsymbol{b}}$ of lower degree, but we note that different points in $\overline{\mathrm{Rat}}_d \smallsetminus \mathrm{Rat}_d$ may correspond to the the same rational map. (For a discussion of Rat_d and its various extensions, quotients, and compactifications, see for example [23, Section 4.3] or [24].)

It is often convenient to dehomogenize $z = X/Y$, so by abuse of notation we will write

$$\varphi_{\boldsymbol{a},\boldsymbol{b}}(z) = \frac{F_{\boldsymbol{a}}(z)}{F_{\boldsymbol{b}}(z)} = \frac{F_{\boldsymbol{a}}(z,1)}{F_{\boldsymbol{b}}(z,1)}$$

for the associated rational function and its dehomogenized numerator and denominator.

Proposition 18. *Let $m \geq 1$ and $0 \leq k < m$.*

(a) *There are unique polynomials*

$$G_{\boldsymbol{a},\boldsymbol{b},m,k}(z) \in \mathbb{Z}[\boldsymbol{a}, \boldsymbol{b}, z] \quad \text{and} \quad H_{\boldsymbol{b},m}(z) \in \mathbb{Z}[\boldsymbol{b}, z]$$

satisfying

$$G_{\boldsymbol{a},\boldsymbol{b},m,k}(w^m) = \frac{1}{mw^k} \sum_{t=0}^{m-1} \zeta_m^{-kt} F_{\boldsymbol{a}}(\zeta_m^t w) \prod_{s \neq t} F_{\boldsymbol{b}}(\zeta_m^s w), \qquad (6.1)$$

$$H_{\boldsymbol{b},m}(w^m) = \prod_{t=0}^{m-1} F_{\boldsymbol{b}}(\zeta_m^t w). \tag{6.2}$$

(b) Let $\varphi_{\boldsymbol{a},\boldsymbol{b}}(z) = F_{\boldsymbol{a}}(z)/F_{\boldsymbol{b}}(z)$. Then

$$\mathfrak{F}_{m,k}(\varphi_{\boldsymbol{a},\boldsymbol{b}})(z) = \frac{G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)}{H_{\boldsymbol{b},m}(z)}.$$

(c) The polynomials $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)$ and $H_{\boldsymbol{b},m}$ have the following homogeneity properties:

   (i) The z-coefficients of $H_{\boldsymbol{b},m}(z)$, considered as elements of $\mathbb{Z}[\boldsymbol{b}]$, are homogeneous of degree m.

   (ii) The z-coefficients of $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)$, considered as elements of $\mathbb{Z}[\boldsymbol{a},\boldsymbol{b}]$, are bi-homogeneous of bi-degree $(1, m-1)$.

   (iii) If we make $\mathbb{Z}[\boldsymbol{a},\boldsymbol{b},z]$ into a graded $\mathbb{Z}$-algebra by assigning weights

$$\mathrm{wt}(z) = m \quad and \quad \mathrm{wt}(a_i) = \mathrm{wt}(b_i) = i, \tag{6.3}$$

then $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)$ and $H_{\boldsymbol{b},m}(z)$ are weight homogeneous with weights

$$\mathrm{wt}(G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)) = md - k \quad and \quad \mathrm{wt}(H_{\boldsymbol{b},m}(z)) = md.$$

(d) The polynomials $G_{\boldsymbol{a},\boldsymbol{b},m,0}(z)$ and $H_{\boldsymbol{b},m}(z)$ have the form

$$G_{\boldsymbol{a},\boldsymbol{b},m,0}(z) = (-1)^{(m+1)d} a_0 b_0^{m-1} z^d + O(z^{d-1}),$$
$$G_{\boldsymbol{a},\boldsymbol{b},m,k}(z) = O(z^{d-1}) \quad for\ 1 \le k < m,$$
$$H_{\boldsymbol{b},m}(z) = (-1)^{(m+1)d} b_0^m z^d + O(z^{d-1}).$$

In particular, both $G_{\boldsymbol{a},\boldsymbol{b},m,0}(z)$ and $H_{\boldsymbol{b},m}(z)$ have z-degree d, while $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)$ has z-degree strictly smaller than d for $1 \le k < m$; cf. Remark 21.

(e) Let

$$F_{\boldsymbol{b}}(z) = b_0 \prod_{i=1}^{d}(z - \beta_i)$$

be the factorization of $F_{\boldsymbol{b}}(z)$ in some integral extension of $\mathbb{Z}[\boldsymbol{b}, z]$. Then

$$H_{\boldsymbol{b},m}(z) = (-1)^{(m+1)d} b_0^m \prod_{i=1}^{d} (z - \beta_i^m).$$

(f) *We have*

$$\mathrm{Res}(G_{\boldsymbol{a},\boldsymbol{b},m,k}, H_{\boldsymbol{b},m}) = (-1)^{d(m-k+1)} b_0^{m-1} b_d^{m-1-k} \, \mathrm{Res}(F_{\boldsymbol{a}}, F_{\boldsymbol{b}}) \frac{\mathrm{Disc}(H_{\boldsymbol{b},m})}{\mathrm{Disc}(F_{\boldsymbol{b}})}.$$
(6.4)

(g) *We have*

$$\frac{\mathrm{Disc}(H_{\boldsymbol{b},m})}{\mathrm{Disc}(F_{\boldsymbol{b}})} \in \mathbb{Z}[b_0, \ldots, b_d],$$

i.e., the polynomial $\mathrm{Disc}(F_{\boldsymbol{b}})$ divides the polynomial $\mathrm{Disc}(H_{\boldsymbol{b},m})$ in $\mathbb{Z}[\boldsymbol{b}]$.

(h) *Let $\beta_1, \ldots, \beta_d$ be the roots of $F_{\boldsymbol{b}}(z)$ as in (e), and assume that $m \geq 2$. The quotient $\mathrm{Disc}(H_{\boldsymbol{b},m})/\mathrm{Disc}(F_{\boldsymbol{b}})$ vanishes if and only if there is a pair of indices $i \neq j$ such that either:*
    (i) $\beta_i = \beta_j = 0$.
    (ii) $\beta_i \neq \beta_j$ *and* $\beta_i^m = \beta_j^m$.

Remark 19. Note that the resultant formula (6.4) implicitly assumes that $F_{\boldsymbol{a}}$ and $F_{\boldsymbol{b}}$ have degree d. In other words, they should first be homogenenized to be polynomials of degree d, then the polynomials $G_{\boldsymbol{a},\boldsymbol{b},m,k}$ and $H_{\boldsymbol{b},m}$ are also homogeneous of degree d and the resultant is calculated accordingly. With this convention, we see that

$$\deg_z\big(\mathfrak{F}_{m,k}(\varphi_{\boldsymbol{a},\boldsymbol{b}})\big) = \deg_z(\varphi_{\boldsymbol{a},\boldsymbol{b}}) \quad \Longleftrightarrow \quad \mathrm{Res}(G_{\boldsymbol{a},\boldsymbol{b},m,k}, H_{\boldsymbol{b},m}) \neq 0.$$

Thus Proposition 18(f) can be used to answer the question of whether the operator $\mathfrak{F}_{m,k}$ preserves the degree of $\varphi(z)$.

Example 20. We illustrate Proposition 18 for $d = 2$ and $m = 2$. We have

$$G_{\boldsymbol{a},\boldsymbol{b},2,0} = b_0 a_0 z^2 + (b_2 a_0 - b_1 a_1 + b_0 a_2)z + b_2 a_2,$$
$$G_{\boldsymbol{a},\boldsymbol{b},2,1} = (-b_1 a_0 + b_0 a_1)z + b_2 a_1 - b_1 a_2,$$
$$H_{\boldsymbol{b},2} = b_0^2 z^2 + (2b_2 b_0 - b_1^2)z + b_2^2,$$

from Example 13. The resultant of the quadratic polynomials $F_{\boldsymbol{a}}$ and $F_{\boldsymbol{b}}$ is given by a well-known formula [25, §27], while

$$\mathrm{Disc}(H_{\boldsymbol{b},2}) = b_1^2(-4b_2b_0 + b_1^2) = b_1^2 \, \mathrm{Disc}(F_{\boldsymbol{b}}).$$

Then formulas for $\mathrm{Res}(G_{\boldsymbol{a},\boldsymbol{b},2,0}, H_{\boldsymbol{b},2})$ and $\mathrm{Res}(G_{\boldsymbol{a},\boldsymbol{b},2,1}, H_{\boldsymbol{b},2})$ can be derived using Proposition 18(f).

Remark 21. It is possible to compute some of the other monomials appearing in $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)$ and $H_{\boldsymbol{b},m}$ by evaluating more complicated sums and products of powers of roots of unity. For example, as an element of $\mathbb{Z}[\boldsymbol{a}, \boldsymbol{b}, z]$, the polynomial $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)$ contains the monomials

$$(-1)^{(m+1)d} a_{m-k} b_0^{m-1} z^{d-1} \quad \text{and} \quad (-1)^{(m+1)d+1} a_{m-k-1} b_0^{m-2} b_1 z^{d-1}.$$

In particular, if $1 \le k < m$, then $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)$ has z-degree equal to $d-1$. We omit the proof.

Since it will come up frequently, we record here the elementary fact

$$\prod_{t=0}^{m-1} \zeta_m^t = (-1)^{m+1}. \tag{6.5}$$

Proof.[Proof of Proposition 18] For the moment, we let

$$g(w) = \frac{1}{mw^k} \sum_{t=0}^{m-1} \zeta_m^{-kt} F_{\boldsymbol{a}}(\zeta_m^t w) \prod_{s \ne t} F_{\boldsymbol{b}}(\zeta_m^s w), \quad h(w) = \prod_{t=0}^{m-1} F_{\boldsymbol{b}}(\zeta_m^t w).$$

Then the identity

$$\mathfrak{F}_{m,k}(\varphi_{\boldsymbol{a},\boldsymbol{b}})(w^m) = \frac{g(w)}{h(w)}$$

follows directly from the definition (1.1) of $\mathfrak{F}_{m,k}$ by putting the terms in the sum over a common denominator.

We note that the coefficients of $g(w)$, viewed as a polynomial in $\boldsymbol{b}$ and w, are $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$-invariant, hence are in $\mathbb{Z}(\zeta_m) \cap \mathbb{Q} = \mathbb{Z}$. Further, we clearly have $h(\zeta_m w) = h(w)$, so h is a polynomial in w^m. This proves that $h(w) \in \mathbb{Z}[\boldsymbol{b}, w^m]$.

Next we observe that $\varphi_{\boldsymbol{a},\boldsymbol{b}}(z)$ can be expanded as a power series

$$\varphi_{\boldsymbol{a},\boldsymbol{b}}(z) \in \mathbb{Z}[b_d^{-1}, \boldsymbol{b}, \boldsymbol{a}][[z]].$$

It follows from Proposition 15 that

$$\mathfrak{F}_{m,k}(\varphi_{\boldsymbol{a},\boldsymbol{b}})(z) \in \mathbb{Z}[b_d^{-1}, \boldsymbol{b}, \boldsymbol{a}][[z]],$$

and hence that

$$g(w) = h(w) \cdot \mathfrak{F}_{m,k}(\varphi_{\boldsymbol{a},\boldsymbol{b}})(w^m) \in \mathbb{Z}[b_d^{-1}, \boldsymbol{b}, \boldsymbol{a}][[w^m]].$$

On the other hand, the definition of g shows the coefficients of $mw^k g(w)$ are $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$-invariant and in $\mathbb{Z}[\zeta_m]$, so we find that that $g(w) \in (mw^k)^{-1}\mathbb{Z}[\boldsymbol{a}, \boldsymbol{b}, w]$. Hence

$$g(w) \in \mathbb{Z}[b_d^{-1}, \boldsymbol{b}, \boldsymbol{a}][[w^m]] \cap (mw^k)^{-1}\mathbb{Z}[\boldsymbol{a}, \boldsymbol{b}, w] = \mathbb{Z}[\boldsymbol{a}, \boldsymbol{b}, w^m].$$

This proves that there are polynomials $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z) \in \mathbb{Z}[\boldsymbol{a}, \boldsymbol{b}, z]$ and $H_{\boldsymbol{b},m}(z) \in \mathbb{Z}[\boldsymbol{b}, z]$ satisfying

$$G_{\boldsymbol{a},\boldsymbol{b},m,k}(w^m) = g(w), \quad H_{\boldsymbol{b},m}(w^m) = h(w), \quad \text{and}$$
$$\mathfrak{F}_{m,k}(\varphi_{\boldsymbol{a},\boldsymbol{b}})(z) = G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)/H_{\boldsymbol{b},m}(z).$$

Since the uniqueness is clear from the defining formulas (6.1) and (6.2), this completes the proof of (a) and (b).

We next consider the homogeneity properties described in (c). We know from (a) that the z-coefficients of $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)$ and $H_{\boldsymbol{b},m}(z)$ are in $\mathbb{Z}[\boldsymbol{a}, \boldsymbol{b}]$ and $\mathbb{Z}[\boldsymbol{b}]$, respectively. It is clear from the formula (6.1) for $G_{\boldsymbol{a},\boldsymbol{b},m,k}$ that it is a $\mathbb{Q}(\zeta_m)$-linear combination of monomials of the form

$$M_{\boldsymbol{j}}(\boldsymbol{a}, \boldsymbol{b}, w) = w^{-k} a_{j_1} w^{d-j_1} b_{j_2} w^{d-j_2} b_{j_3} w^{d-j_3} \cdots b_{j_m} w^{d-j_m}$$
$$= a_{j_1} b_{j_2} \cdots b_{j_m} w^{md-k-j_1-\cdots-j_m}.$$

The $(\boldsymbol{a}, \boldsymbol{b})$ coefficients of these monomials are clearly bi-homogeneous of bi-degree $(1, m-1)$ in the variables $(\boldsymbol{a}, \boldsymbol{b})$. Further, using the weights described by (6.3), so in particular $\deg(w) = \frac{1}{m}\deg(z) = 1$, we have

$$\mathrm{wt}\big(M_{\boldsymbol{j}}(\boldsymbol{a}, \boldsymbol{b}, w)\big) = md - k.$$

This completes the proof that $G_{\boldsymbol{a},\boldsymbol{b},m,k}$ has the indicated bi-degree and weight. The proof for $H_{\boldsymbol{b},m}$ is similar, but easier, so we leave it for the reader.

We turn to (d). We will make frequent use of (6.5) without further comment. The highest degree term of $H_{\boldsymbol{b},m}(w^m)$ is

$$\prod_{t=0}^{m-1} b_0(\zeta_m^t w)^d = (-1)^{(m+1)d} b_0^d w^{md},$$

so $H_{\boldsymbol{b},m}(z)$ has the indicated form. Similarly, the highest degree term of $G_{\boldsymbol{a},\boldsymbol{b},m,k}(w^m)$ is

$$\frac{1}{mw^k} \sum_{t=0}^{m-1} \zeta_m^{-kt} a_0(\zeta_m^t w)^d \prod_{s\neq t} b_0(\zeta_m^s w)^d$$

$$= \frac{a_0 b_0^{m-1} w^{md-k}}{m} \sum_{t=0}^{m-1} \zeta_m^{-kt} \prod_{s=0}^{m-1} \zeta_m^{ds} = \begin{cases} (-1)^{(m+1)d} a_0 b_0^{m-1} w^{md} & \text{if } k = 0, \\ 0 & \text{if } 1 \leq k < m. \end{cases}$$

Hence $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)$ also has the indicated form. This completes the proof of (d).

For (e) we compute

$$H_{\boldsymbol{b},m}(w^m) = \prod_{t=0}^{m-1} F_{\boldsymbol{b}}(\zeta_m^t w) = \prod_{t=0}^{m-1} \left(b_0 \prod_{i=1}^{d} (\zeta_m^t w - \beta_i) \right)$$

$$= b_0^m \prod_{i=1}^{d} \prod_{t=0}^{m-1} (\zeta_m^t w - \beta_i) = b_0^m \prod_{i=1}^{d} \left((-1)^m (\beta_i^m - w^m) \right)$$

$$= (-1)^{(m+1)d} b_0^m \prod_{i=1}^{d} (w^m - \beta_i^m).$$

To prove (f), we use the fact that for any polynomials we have

$$\text{Res}(f(w^m), g(w^m)) = \text{Res}(f(w), g(w))^m.$$

So we compute the resultant of $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)$ and $H_{\boldsymbol{b},m}(z)$ with respect to the w variable and then take the mth root. We use various elementary formulas

such as

$$
\mathrm{Res}\big(f(\alpha z), g(\alpha z)\big) = \alpha^{(\deg f)(\deg g)} \, \mathrm{Res}\big(f(z), g(z)\big),
$$
$$
\mathrm{Res}\big(Af(z), Bg(z)\big) = A^{\deg g} B^{\deg f} \, \mathrm{Res}\big(f(z), g(z)\big),
$$
$$
\mathrm{Res}\big(f(z), f'(z)\big) = (-1)^{(n^2-n)/2} a_0 \, \mathrm{Disc}\big(f(z)\big), \quad \text{where } n = \deg(f).
$$

Then

$$
\mathrm{Res}\big(G_{\boldsymbol{a},\boldsymbol{b},m,k}(w), H_{\boldsymbol{b},m}(w)\big)^m
$$
$$
= \mathrm{Res}\big(G_{\boldsymbol{a},\boldsymbol{b},m,k}(w^m), H_{\boldsymbol{b},m}(w^m)\big)
$$
$$
= \mathrm{Res}\left(\frac{1}{mw^k} \sum_{t=0}^{m-1} \zeta_m^{-kt} F_{\boldsymbol{a}}(\zeta_m^t w) \prod_{s\neq t} F_{\boldsymbol{b}}(\zeta_m^s w), \; \prod_{r=0}^{m-1} F_{\boldsymbol{b}}(\zeta_m^r w) \right)
$$
$$
= \prod_{r=0}^{m-1} \mathrm{Res}\left(\frac{1}{mw^k} \sum_{t=0}^{m-1} \zeta_m^{-kt} F_{\boldsymbol{a}}(\zeta_m^t w) \prod_{s\neq t} F_{\boldsymbol{b}}(\zeta_m^s w), \; F_{\boldsymbol{b}}(\zeta_m^r w) \right)
$$
$$
= \prod_{r=0}^{m-1} \mathrm{Res}\left(\frac{1}{mw^k} \zeta_m^{-kr} F_{\boldsymbol{a}}(\zeta_m^r w) \prod_{s\neq r} F_{\boldsymbol{b}}(\zeta_m^s w), \; F_{\boldsymbol{b}}(\zeta_m^r w) \right)
$$
$$
= \prod_{r=0}^{m-1} \frac{\mathrm{Res}\big(\zeta_m^{-kr} F_{\boldsymbol{a}}(\zeta_m^r w), F_{\boldsymbol{b}}(\zeta_m^r w)\big)}{\mathrm{Res}\big(mw^k, F_{\boldsymbol{b}}(\zeta_m^r w)\big)}
$$
$$
\times \prod_{r=0}^{m-1} \prod_{s\neq r} \mathrm{Res}\big(F_{\boldsymbol{b}}(\zeta_m^s w), F_{\boldsymbol{b}}(\zeta_m^r w)\big)
$$
$$
= \prod_{r=0}^{m-1} (\zeta_m^{-kr})^d (\zeta_m^r)^{d^2} \frac{\mathrm{Res}\big(F_{\boldsymbol{a}}(w), F_{\boldsymbol{b}}(w)\big)}{m^d b_d^k}
$$
$$
\times \prod_{r=0}^{m-1} \prod_{s\neq r} (\zeta_m^s)^{d^2} \, \mathrm{Res}\big(F_{\boldsymbol{b}}(w), F_{\boldsymbol{b}}(\zeta_m^{r-s} w)\big)
$$
$$
= \pm \left(\mathrm{Res}\big(F_{\boldsymbol{a}}(w), F_{\boldsymbol{b}}(w)\big) \, m^{-d} b_d^{-k} \right)^m \left(\prod_{r=1}^{m-1} \mathrm{Res}\big(F_{\boldsymbol{b}}(w), F_{\boldsymbol{b}}(\zeta_m^r w)\big) \right)^m.
$$

Taking m^{th} roots yields

$$
\mathrm{Res}\big(G_{\boldsymbol{a},\boldsymbol{b},m,k}(w), H_{\boldsymbol{b},m}(w)\big)
$$
$$
= \xi \, \mathrm{Res}\big(F_{\boldsymbol{a}}(w), F_{\boldsymbol{b}}(w)\big) \, m^{-d} b_d^{-k} \prod_{r=1}^{m-1} \mathrm{Res}\big(F_{\boldsymbol{b}}(w), F_{\boldsymbol{b}}(\zeta_m^r w)\big) \qquad (6.6)
$$

for some $\xi \in \boldsymbol{\mu}_{2m}$, and aside from evaluating ξ, it only remains to deal with the final product.

As in (e), we factor $F_{\boldsymbol{b}}$ as $F_{\boldsymbol{b}}(z) = b_0 \prod_{i=1}^{d}(z - \beta_i)$. Then

$$
\prod_{r=1}^{m-1} \operatorname{Res}\left(F_{\boldsymbol{b}}(w), F_{\boldsymbol{b}}(\zeta_m^r w)\right)
$$

$$
= \prod_{r=1}^{m-1}\left(b_0^{2d}\zeta_m^{rd}\prod_{i,j=1}^{d}(\beta_i - \zeta_m^{-r}\beta_j)\right)
$$

$$
= \pm b_0^{2d(m-1)}\left(\prod_{i=1}^{d}\beta_i^{m-1}\prod_{r=1}^{m-1}(1 - \zeta_m^{-r})^d\right)\left(\prod_{i\neq j}\prod_{r=1}^{m-1}(\beta_i - \zeta_m^{-r}\beta_j)\right)
$$

$$
= \pm b_0^{(2d-1)(m-1)}b_d^{m-1}m^d\left(\prod_{i\neq j}\prod_{r=1}^{m-1}(\beta_i - \zeta_m^{-r}\beta_j)\right)
$$

$$
= \pm b_0^{(2d-1)(m-1)}b_d^{m-1}m^d\left(\prod_{i\neq j}\frac{\prod_{r=0}^{m-1}(\beta_i - \zeta_m^{-r}\beta_j)}{\beta_i - \beta_j}\right)
$$

$$
= \pm b_0^{(2d-1)(m-1)}b_d^{m-1}m^d\prod_{i\neq j}\frac{\beta_i^m - \beta_j^m}{\beta_i - \beta_j}
$$

$$
= \pm b_0^{m-1}b_d^{m-1}m^d\frac{\operatorname{Disc}(H_{\boldsymbol{b},m})}{\operatorname{Disc}(F_{\boldsymbol{b}})},
$$

where the last equality uses the formulas

$$
\operatorname{Disc}(F_{\boldsymbol{b}}) = \pm b_0^{2d-2}\prod_{i\neq j}(\beta_i - \beta_j), \tag{6.7}
$$

$$
\operatorname{Disc}(H_{\boldsymbol{b},m}) = \pm b_0^{m(2d-2)}\prod_{i\neq j}(\beta_i^m - \beta_j^m), \tag{6.8}
$$

the latter of which follows from (e). Hence

$$
\prod_{r=1}^{m-1}\operatorname{Res}\left(F_{\boldsymbol{b}}(w), F_{\boldsymbol{b}}(\zeta_m^r w)\right) = \pm b_0^{m-1}b_d^{m-1}m^d\frac{\operatorname{Disc}(H_{\boldsymbol{b},m})}{\operatorname{Disc}(F_{\boldsymbol{b}})}.
$$

Substituting this into (6.6) gives

$$
\operatorname{Res}(G_{\boldsymbol{a},\boldsymbol{b},m,k}, H_{\boldsymbol{b},m}) = \xi \operatorname{Res}(F_{\boldsymbol{a}}, F_{\boldsymbol{b}})b_0^{m-1}b_d^{m-1-k}\frac{\operatorname{Disc}(H_{\boldsymbol{b},m})}{\operatorname{Disc}(F_{\boldsymbol{b}})}. \tag{6.9}
$$

In order to complete the proof of (f), it remains to evaluate ξ. Since (6.9) is an identity in $\mathbb{Z}[\boldsymbol{a}, \boldsymbol{b}]$, we see that $\xi \in \{\pm 1\}$, and it suffices to compute ξ for a single pair $[\boldsymbol{a}, \boldsymbol{b}] \in \mathbb{Z}$ such that $\mathrm{Res}(G_{\boldsymbol{a}, \boldsymbol{b}, m, k}, H_{\boldsymbol{b}, m}) \neq 0$. We only sketch the proof, since for our applications, it suffices to know that ξ is a root of unity. Taking $F_{\boldsymbol{a}}(z) = z^d$ and $F_{\boldsymbol{b}}(z) = (z-1)^d$, an easy calculation shows that the right-hand side of (6.9) equals $\xi(-1)^{d(m-k)} m^{d(d-1)}$, while a slightly more complicated calculation shows that the left-hand side of (6.9) equals $(-1)^d m^{d(d-1)}$. Hence $\xi = (-1)^{d(m-k+1)}$.

For (g), we use (6.7) and (6.8) to write

$$\frac{\mathrm{Disc}(H_{\boldsymbol{b}, m})}{\mathrm{Disc}(F_{\boldsymbol{b}})} = \pm b_0^{(m-1)(2d-2)} \prod_{i \neq j} \sum_{k=0}^{m-1} \beta_i^k \beta_j^{m-1-k}. \tag{6.10}$$

The product of sums is symmetric in $\beta_1, \ldots, \beta_d$, so $\mathrm{Disc}(H_{\boldsymbol{b}, m}) / \mathrm{Disc}(F_{\boldsymbol{b}})$ is in $\mathbb{Z}[\boldsymbol{b}, b_0^{-1}]$. On the other hand, we know that $\mathrm{Disc}(F_{\boldsymbol{b}})$ is in $\mathbb{Z}[\boldsymbol{b}]$ and that it is irreducible in $\mathbb{C}[\boldsymbol{b}]$; see [25, §28]. In particular, it is not divisible by b_0, so $\mathrm{Disc}(H_{\boldsymbol{b}, m}) / \mathrm{Disc}(F_{\boldsymbol{b}})$ is in $\mathbb{Z}[\boldsymbol{b}]$. Alternatively, we can see that $\mathrm{Disc}(F_{\boldsymbol{b}})$ is not divisible by b_0 in $\mathbb{Z}[\boldsymbol{b}]$ directly from the formula

$$\mathrm{Disc}(b_0 z^d + b_1 z^{d-1} + b_d) = b_d^{d-2}(d^d b_d b_0^{d-1} - (-1)^d (d-1)^{d-1} b_1^d)$$

for the discriminant of a trinomial. This gives (g).

Finally, we see that (h) follows immediately from (6.10) provided that we can show that $\mathrm{Disc}(H_{\boldsymbol{b}, m}) / \mathrm{Disc}(F_{\boldsymbol{b}})$ does not vanish when $b_0 = 0$. We will show that $\mathrm{Disc}(H_{\boldsymbol{b}, m})$ is not in the ideal of $\mathbb{Z}[\boldsymbol{b}]$ generated by b_0. It is convenient to work in the ring

$$R = \mathbb{Z}[b_d^{-1}, \gamma_1, \gamma_2, \ldots, \gamma_d] \quad \text{with } \gamma_i = \beta_i^{-1}.$$

We note that $\gamma_1, \ldots, \gamma_d$ satisfy

$$z^d F_{\boldsymbol{b}}(z^{-1}) = b_0 + b_1 z + \cdots + b_d z^d = b_d \prod_{i=1}^{d} (z - \gamma_i),$$

so in particular $\gamma_1, \ldots, \gamma_d$ are algebraically independent and integral over $\mathbb{Z}[b_d^{-1}, \boldsymbol{b}]$. Further,

$$b_0 = (-1)^d b_d \gamma_1 \gamma_2 \cdots \gamma_d, \quad \text{so as ideals we have} \quad b_0 R = \gamma_1 \gamma_2 \cdots \gamma_d R.$$

Rewriting the formula (6.8) for $\mathrm{Disc}(H_{\boldsymbol{b},m})$ in terms of $\gamma_1, \ldots, \gamma_d$ yields

$$\mathrm{Disc}(H_{\boldsymbol{b},m}) = \pm b_d^{m(2d-2)} \prod_{i \neq j}(\gamma_i^m - \gamma_j^m).$$

Since $b_d \in R^*$, we are reduced to the following assertion.

$$\text{Claim:} \quad \prod_{i \neq j}(\gamma_i^m - \gamma_j^m) \notin \gamma_1 \gamma_2 \cdots \gamma_d R. \tag{6.11}$$

In the product (6.11) we consider the monomial

$$(\gamma_1^m)^{2(d-1)}(\gamma_2^m)^{2(d-2)}(\gamma_3^m)^{2(d-3)} \cdots (\gamma_{d-2}^m)^{2 \cdot 2}(\gamma_{d-1}^m)^{2 \cdot 1}(\gamma_d^m)^{2 \cdot 0}. \tag{6.12}$$

There is a *unique* way to choose a term in each binomial in the product (6.11) to get this monomial, since to get $(\gamma_1^m)^{2(d-1)}$ we need to take γ_1^m in every term $\gamma_i^m - \gamma_j^m$ in which either i or j is 1; then to get $(\gamma_2^m)^{2(d-2)}$ we need to take γ_2^m in every remaining term $\gamma_i^m - \gamma_j^m$ in which either i or j is 2; etc. Hence the product on the left-hand side of (6.11) contains a monomial (6.12) that is not in the ideal $\gamma_1 \gamma_2 \cdots \gamma_d R$. (Notice that the monomial (6.12) is not a multiple of γ_d.) This completes the proof that $\mathrm{Disc}(H_{\boldsymbol{b},m})$ is not in the ideal $b_0 \mathbb{Z}[\boldsymbol{b}]$. □

7. The Operator $\mathfrak{F}_{m,k}$ as a Rational Map

In this section we show that $\mathfrak{F}_{m,k}$ induces a rational map on the projective space $\overline{\mathrm{Rat}}_d \cong \mathbb{P}^{2d+1}$, and in particular, we prove Theorem 2 stated in the introduction.

It is natural to ask whether the $\mathfrak{F}_{m,k}$ operators preserve the degree of the rational map φ. The answer is clearly no. For example, if $\varphi(z) = \sum a_i z^i \in K[z]$ is a polynomial of degree d, then Proposition 15 tells us that

$$\mathfrak{F}_{m,k}(\varphi)(z) = \sum_{j=0}^{\lfloor (d-k)/m \rfloor} a_{k+jm} z^j,$$

so

$$\deg\big(\mathfrak{F}_{m,k}(\varphi)\big) \leq \left\lfloor \frac{\deg(\varphi) - k}{m} \right\rfloor \leq \frac{1}{m} \deg(\varphi).$$

We start by describing a large class of degree d rational maps whose degree is preserved by $\mathfrak{F}_{m,k}$.

Definition 22. Let $F(X,Y) \in K[X,Y]$ be a homogeneous polynomial of degree d, and let $m \geq 1$. We say that F is *m-nondegenerate* if $F(z,1)$ has degree d and if the roots $\gamma_1, \ldots, \gamma_d$ of $F(z,1)$ in $\bar{K}$ are nonzero and have the property that for all $i \neq j$,

$$\text{either } \gamma_i = \gamma_j \text{ or } \gamma_i^m \neq \gamma_j^m.$$

If F is m-nondegenerate for all $m \geq 2$, we say simply that F is *nondegenerate*.

Definition 23. We set

$$\text{Rat}_d^{m\text{-nondeg}} = \{\varphi_{\boldsymbol{a},\boldsymbol{b}} \in \text{Rat}_d : F_{\boldsymbol{b}} \text{ is } m\text{-nondegenerate}\}.$$

Corollary 24. *Let $m \geq 2$ and $0 \leq k < m$.*

(a) *Identifying Rat_d as a subset of $\mathbb{P}^{2d+1}$, the set $\text{Rat}_d^{m\text{-nondeg}}$ is the complement of a hypersurface of $\mathbb{P}^{2d+1}$.*

(b) *All $\varphi_{\boldsymbol{a},\boldsymbol{b}} \in \text{Rat}_d^{m\text{-nondeg}}$ satisfy*

$$\deg_z\big(\mathfrak{F}_{m,k}(\varphi_{\boldsymbol{a},\boldsymbol{b}})\big) = d.$$

Proof. (a) Indeed, we see from Proposition 18(e,g,h) that $F(z) = F_{\boldsymbol{b}}(z)$ is m-nondegenerate if and only if $b_0 b_d \neq 0$ and $\text{Disc}(H_{\boldsymbol{b},m})/\text{Disc}(F_{\boldsymbol{b}}) \neq 0$. But Proposition 18(g) tells us that $\text{Disc}(H_{\boldsymbol{b},m})/\text{Disc}(F_{\boldsymbol{b}}) \in \mathbb{Z}[\boldsymbol{b}]$, so $\text{Rat}_d^{m\text{-nondeg}}$ is the complement of the hypersurface defined by

$$b_0 b_d \, \text{Disc}(H_{\boldsymbol{b},m})/\text{Disc}(F_{\boldsymbol{b}}) = 0.$$

(b) This is immediate from Proposition 18(f,h) and the definition of m-nondegeneratcy. We note that the nondegeneracy includes the condition that $b_0 b_d \neq 0$, which is needed due to the $b_0^{m-1} b_d^{m-1-k}$ factor in (6.4), although for $k = m-1$, there are maps with $b_d = 0$ satisfying $\deg_z\big(\mathfrak{F}_{m,k}(\varphi_{\boldsymbol{a},\boldsymbol{b}})\big)$ $= d$. $\qquad\square$

7.1. Proof of Theorem 2(a,b)

Proposition 18 tells us that $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)$ and $H_{\boldsymbol{b},m}(z)$ are of degree at

most d in z, and that their z-coefficients are homogeneous polynomials of degree m in $\mathbb{Z}[\boldsymbol{a}, \boldsymbol{b}]$. We write

$$G_{\boldsymbol{a},\boldsymbol{b},m,k}(z) = \sum_{i=0}^{d} G_{m,k,i}(\boldsymbol{a},\boldsymbol{b})z^{d-i} \quad \text{and} \quad H_{\boldsymbol{b},m}(z) = \sum_{i=0}^{d} H_{m,i}(\boldsymbol{b})z^{d-i}.$$

More precisely, Proposition 18(d) tells us that

$$H_{m,0} = (-1)^{d(m+1)} b_0^m,$$
$$G_{m,0,0} = (-1)^{d(m+1)} a_0 b_0^{m-1},$$
$$G_{m,k,0} = 0 \quad \text{for } 1 \le k < m.$$

Further, the formula $\mathfrak{F}_{m,k}(\varphi_{\boldsymbol{a},\boldsymbol{b}})(z) = G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)/H_{\boldsymbol{b},m}(z)$ in Proposition 18(b) implies that the rational map $\mathfrak{R}_{d,m,k} : \mathbb{P}^{2d+1} \dashrightarrow \mathbb{P}^{2d+1}$ is given by

$$\mathfrak{R}_{d,m,k} = [G_{m,k,0}, \ldots, G_{m,k,d}, H_{m,0}, \ldots, H_{m,d}]. \tag{7.1}$$

Hence $\mathfrak{R}_{d,m,k}$ is a rational map of degree at most m. We are next going to show that

$$G_{m,k,0}, \ldots, G_{m,k,d}, H_{m,0}, \ldots, H_{m,d}$$

have no nontrivial common factor in the polynomial ring $\mathbb{Z}[\boldsymbol{a}, \boldsymbol{b}]$, which will complete the proof that $\mathfrak{R}_{d,m,k}$ has degree exactly equal to m.

Let

$$W = \left\{ [\boldsymbol{a}, \boldsymbol{b}] \in \mathbb{P}^{2d+1} : \begin{array}{l} G_{m,k,0}(\boldsymbol{a},\boldsymbol{b}) = \cdots = G_{m,k,d}(\boldsymbol{a},\boldsymbol{b}) = 0 \\ H_{m,0}(\boldsymbol{b}) = \cdots = H_{m,d}(\boldsymbol{b}) = 0 \end{array} \right\},$$

so (7.1) tells us that $Z(\mathfrak{R}_{d,m,k}) \subset W$. We first observe that if $\boldsymbol{b} = 0$, then the formulas for $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)$ and $H_{\boldsymbol{b},m}(z)$ given in Proposition 18 imply that $G_{\boldsymbol{a},\boldsymbol{b},m,k}(z)$ and $H_{\boldsymbol{b},m}(z)$ are both identically 0, which shows that $\{\boldsymbol{b} = \boldsymbol{0}\} \subset W$. Conversely, let $[\boldsymbol{a}, \boldsymbol{b}] \in W$. In particular, every coefficient of $H_{\boldsymbol{b},m}(z)$ vanishes. Since $H_{\boldsymbol{b},m}(w^m) = \prod F_{\boldsymbol{b}}(\zeta_m^t w)$ by definition, it follows that there is some t such that $F_{\boldsymbol{b}}(\zeta_m^t w) = 0$ as a polynomial in w, which in turn implies that $\boldsymbol{b} = \boldsymbol{0}$. This gives the other inclusion, so we have proven that

$$W = \left\{ [\boldsymbol{a}, \boldsymbol{b}] \in \mathbb{P}^{2d+1} : \boldsymbol{b} = \boldsymbol{0} \right\}.$$

Suppose now that $\deg \mathfrak{R}_{d,m,k} < m$. As noted earlier, this implies that $G_{m,k,0}, \ldots, G_{m,k,d}, H_{m,0}, \ldots, H_{m,d}$ have a nontrivial common factor $u(\boldsymbol{a}, \boldsymbol{b}) \in \mathbb{Z}[\boldsymbol{a}, \boldsymbol{b}]$. But then W contains the subvariety $\{u = 0\}$, which has dimension $2d$, contradicting the fact that

$$\dim W = \dim\{\boldsymbol{b} = \boldsymbol{0}\} = d.$$

This shows that $\deg \mathfrak{R}_{d,m,k} = m$, which completes the proof of Theorem 2(a), while simultaneously proving that

$$\mathcal{Z}(\mathfrak{R}_{d,m,k}) = W = \big\{ [\boldsymbol{a}, \boldsymbol{b}] \in \mathbb{P}^{2d+1} : \boldsymbol{b} = \boldsymbol{0} \big\}.$$

Finally, let $[\boldsymbol{a}, \boldsymbol{b}] \in \mathbb{P}^{2d+1} \smallsetminus \mathcal{Z}(\mathfrak{R}_{d,m,k})$. Then

$$\mathfrak{R}_{d,m,k}(\boldsymbol{a}, \boldsymbol{b}) \in \mathcal{Z}(\mathfrak{R}_{d,m,k})$$

$$\Longleftrightarrow \quad H_{\boldsymbol{b},m}(z) = 0 \text{ as a } z\text{-polynomial},$$

$$\Longleftrightarrow \quad H_{\boldsymbol{b},m}(w^m) = \prod_{t=0}^{m-1} F_{\boldsymbol{b}}(\zeta_m^t w) = 0 \text{ as a } w\text{-polynomial},$$

$$\Longleftrightarrow \quad F_{\boldsymbol{b}}(\zeta_m^t w) = 0 \text{ as a } w\text{-polynomial, for some } t,$$

$$\Longleftrightarrow \quad \boldsymbol{b} = \boldsymbol{0}$$

$$\Longleftrightarrow \quad [\boldsymbol{a}, \boldsymbol{b}] \in \mathcal{Z}(\mathfrak{R}_{d,m,k}). \tag{7.2}$$

This completes the proof of Theorem 2(b).

7.2. Computation of a Jacobian matrix

The proof of the remaining parts of Theorem 2 is more complicated and requires some preliminary results.

The rational map $\mathfrak{R}_{d,m,k}(\boldsymbol{a}, \boldsymbol{b})$ is given by a list of $2d + 2$ homogeneous polynomials of degree m. We write

$$\mathcal{J}_{d,m,k}(\boldsymbol{a}, \boldsymbol{b}) = \operatorname{Jac} \mathfrak{R}_{d,m,k}(\boldsymbol{a}, \boldsymbol{b})$$

for the associated Jacobian matrix. We note that since $G_{\boldsymbol{a},\boldsymbol{b},m,k}$ has degree 1 in $\boldsymbol{a}$ and $H_{\boldsymbol{b},m}$ is independent of $\boldsymbol{a}$ and k, the matrix $\mathcal{J}_{d,m,k}$ has block form

$$\mathcal{J}_{d,m,k}(\boldsymbol{a}, \boldsymbol{b}) = \begin{pmatrix} A_{d,m,k}(\boldsymbol{b}) & \boldsymbol{0} \\ C_{d,m,k}(\boldsymbol{a}, \boldsymbol{b}) & D_{d,m}(\boldsymbol{b}) \end{pmatrix}, \tag{7.3}$$

In particular, the Jacobian determinant

$$\det \mathcal{J}_{d,m,k} = (\det A_{d,m,k})(\det D_{d,m}) \in \mathbb{Z}[\boldsymbol{b}] \tag{7.4}$$

is independent of $\boldsymbol{a}$.

Lemma 1. *With notation as in (7.3), in the case that $k = 0$ we have*

$$D_{d,m} = mA_{d,m,0}.$$

Proof. With our usual identification of $z = w^m$, we have by definition that the (i,j)'th entry of $A_{d,m,0}$ is the coefficient of z^{d-j} in the partial derivative

$$\frac{\partial G_{\boldsymbol{a},\boldsymbol{b},d,m,0}(z)}{\partial a_i} = \frac{\partial}{\partial a_i}\left(\frac{1}{m}\sum_{t=0}^{m-1} F_{\boldsymbol{a}}(\zeta_m^t w)\prod_{s\neq t} F_{\boldsymbol{b}}(\zeta_m^s w)\right)$$

$$= \frac{1}{m}\sum_{t=0}^{m-1}(\zeta_m^t w)^{d-i}\prod_{s\neq t} F_{\boldsymbol{b}}(\zeta_m^s w).$$

Similarly, the (i,j)'th entry of $D_{d,m}$ is the coefficient of z^{d-j} in the partial derivative

$$\frac{\partial H_{\boldsymbol{b},d,m}(z)}{\partial b_i} = \frac{\partial}{\partial b_i}\left(\prod_{t=0}^{m-1} F_{\boldsymbol{b}}(\zeta_m^t w)\right) = \sum_{t=0}^{m-1}(\zeta_m^t w)^{d-i}\prod_{s\neq t} F_{\boldsymbol{b}}(\zeta_m^s w).$$

Comparing these formulas shows that $D_{d,m} = mA_{d,m,0}$. $\qquad\square$

Example 25. We illustrate Lemma 1 and the block form (7.3) of $\mathcal{J}_{d,m,k}$ by computing

$$\mathcal{J}_{2,2,0} = \left(\begin{array}{ccc|ccc} b_0 & b_2 & 0 & 0 & 0 & 0 \\ 0 & -b_1 & 0 & 0 & 0 & 0 \\ 0 & b_0 & b_2 & 0 & 0 & 0 \\ \hline a_0 & a_2 & 0 & 2b_0 & 2b_2 & 0 \\ 0 & -a_1 & 0 & 0 & -2b_1 & 0 \\ 0 & a_0 & a_2 & 0 & 2b_0 & 2b_2 \end{array}\right)$$

The next lemma, which includes a somewhat complicated calculation, is the key to showing that the matrix $A_{d,m,0}$ is generically non-singular in all characteristics.

Lemma 2. *Write the entries of the matrix* $A_{d,m,k}(\boldsymbol{b})$ *as*

$$A_{d,m,k}(\boldsymbol{b}) = \big(\alpha_{d,m,k}(\boldsymbol{b})_{i,j}\big)_{0\leq i,j\leq d}.$$

(a) *Then* $\alpha_{d,m,k}(\boldsymbol{b})_{i,j} \in \mathbb{Z}[\boldsymbol{b}]$ *is homogeneous for both degree and weight, and satisfies*

$$\deg \alpha_{d,m,k}(\boldsymbol{b})_{i,j} = m - 1,$$
$$\operatorname{wt} \alpha_{d,m,k}(\boldsymbol{b})_{i,j} = mj - i - k.$$

(b) $\det A_{d,m,k}(\boldsymbol{b}) \in \mathbb{Z}[\boldsymbol{b}]$ *is homogeneous for both degree and weight, and satisfies*

$$\deg \det A_{d,m,k} = (m - 1)(d + 1),$$
$$\operatorname{wt} \det A_{d,m,k} = \frac{1}{2}(m - 1)(d^2 + d) - k(d + 1).$$

(c) *Let* $I_j \subset \mathbb{Z}[\boldsymbol{b}]$ *be the ideal generated by* $b_0, b_1, \ldots, b_{j-1}$, *where by convention we set* $I_0 = (0)$. *Then*

$$\alpha_{d,m,0}(\boldsymbol{b})_{i,j} \equiv 0 \pmod{I_j} \quad \text{for all } i > j,$$

and for $i = j$, *we have*

$$\alpha_{d,m,0}(\boldsymbol{b})_{j,j} \equiv (-1)^{(m+1)(d-j)} b_j^{m-1} \pmod{I_j}.$$

(d) *When* $\det A_{d,m,0}(\boldsymbol{b})$ *is written as a polynomial in* $\mathbb{Z}[\boldsymbol{b}]$, *it includes the monomial*

$$(-1)^{(m+1)(d^2+d)/2}(b_0 b_1 \cdots b_d)^{m-1}.$$

(Note that (c) *and* (d) *refer to the case that* $k = 0$. *For* $1 \leq k < m$, *see Lemma 3.)*

Proof. The (i, j)'th entry of $A_{d,m,k}$ is equal to the coefficient of z^{d-j} in the partial derivative

$$\frac{\partial G_{\boldsymbol{a},\boldsymbol{b},d,m,k}(z)}{\partial a_i} = \frac{1}{mw^k} \sum_{t=0}^{m-1} \zeta_m^{-kt} (\zeta_m^t w)^{d-i} \prod_{s\neq t} F_{\boldsymbol{b}}(\zeta_m^s w). \qquad (7.5)$$

A typical monomial in the right-hand side of (7.5) is a $\mathbb{Z}[\zeta_m]$-multiple of

$$w^{-k}w^{d-i}b_{u_1}w^{d-u_1}\cdots b_{u_{m-1}}w^{d-u_{m-1}} = b_{u_1}\cdots b_{u_{m-1}}w^{md-i-k-u_1-\cdots-u_{m-1}}.$$

This quantity will be a multiple of $z^{d-j} = w^{m(d-j)}$ if and only if

$$md - i - k - (u_1 + \cdots + u_{m-1}) = m(d-j).$$

Hence $\alpha_{d,m,k}(\boldsymbol{b})_{i,j}$ is a sum of monomials whose $\boldsymbol{b}$-degree is $m-1$ and whose $\boldsymbol{b}$-weight is

$$\text{wt}(b_{u_1}\cdots b_{u_{m-1}}) = u_1 + \cdots + u_{m-1} = mj - i - k.$$

This completes the proof of (a).

For (b), we see that each monomial in $\det A_{d,m,k}$ is a product of $d+1$ homogeneous polynomials of degree $m-1$, which shows that $\det A_{d,m,k}$ is homogeneous of degree $(m-1)(d+1)$. Further, if $\pi \in \mathcal{S}_{d+1}$ is any permutatation, then $\det A_{d,m,k}$ is a linear combination of terms having weight

$$\text{wt}\left(\prod_{i=0}^{d}\alpha_{d,m,k}(\boldsymbol{b})_{i,\pi(i)}\right) = \sum_{i=0}^{d}\text{wt}\,\alpha_{d,m,k}(\boldsymbol{b})_{i,\pi(i)}$$

$$= \sum_{i=0}^{d}\big(m\pi(i) - i - k\big)$$

$$= (m-1)d(d+1)/2 - k(d+1).$$

This completes the proof of (b).

The weight and degree formulas from (a) say that $\alpha_{d,m,0}(\boldsymbol{b})_{i,j}$ is a linear combination of terms of the form

$$b_0^{e_0}b_1^{e_1}\cdots b_d^{e_d} \quad \text{with} \quad \sum_{t=0}^{d}e_t = m - 1 \quad \text{and} \quad \sum_{t=0}^{d}te_t = mj - i.$$

Suppose that

$$\alpha_{d,m,0}(\boldsymbol{b})_{i,j} \not\equiv 0 \pmod{I_j}.$$

This means that $\alpha_{d,m,0}(\boldsymbol{b})_{i,j}$ includes a monomial having $e_0 = \cdots = e_{j-1} = 0$,

i.e., a monomial of the form

$$b_j^{e_j} \cdots b_d^{e_d} \quad \text{with} \quad \sum_{t=j}^{d} e_t = m - 1 \quad \text{and} \quad \sum_{t=j}^{d} t e_t = mj - i.$$

This leads to the inequality

$$mj - i = \sum_{t=j}^{d} t e_t \geq \sum_{t=j}^{d} j e_t = j(m - 1), \tag{7.6}$$

which implies that $i \leq j$. We have thus shown that

$$\alpha_{d,m,0}(\boldsymbol{b})_{i,j} \not\equiv 0 \pmod{I_j} \implies i \leq j. \tag{7.7}$$

The contrapositive of (7.7) is the first part of (c).

For the second part, we suppose that

$$\alpha_{d,m,0}(\boldsymbol{b})_{i,j} \not\equiv 0 \pmod{I_j} \quad \text{and} \quad i = j.$$

Then $mj - i = j(m - 1)$, so the middle inequality in (7.6) is an equality. Hence

$$0 = \sum_{t=j}^{d} t e_t - \sum_{t=j}^{d} j e_t = \sum_{t=j}^{d} (t - j) e_t.$$

Every term $(t - j)e_t$ is non-negative, so we must have $(t - j)e_t = 0$ for all $j \leq t \leq d$, which implies that $e_t = 0$ for all $j + 1 \leq t \leq d$. It follows that the only monomial appearing in $\alpha_{d,m,0}(\boldsymbol{b})_{i,j}$ that is not in I_j has the form $b_j^{e_j}$, and by degree considerations we must have $e_j = m - 1$. This proves that

$$\alpha_{d,m,0}(\boldsymbol{b})_{j,j} \equiv \gamma b_j^{m-1} \pmod{I_j} \quad \text{for some constant } \gamma \in \mathbb{Z}[\zeta_m].$$

In order to complete the proof of the second part of (c), it remains to compute the constant γ.

We are looking for the coefficient of $b_j^{m-1} w^{m(d-j)}$ in the expression (note that $k = 0$ by assumption)

$$\frac{1}{m} \sum_{t=0}^{m-1} (\zeta_m^t w)^{d-j} \prod_{s \neq t} F_{\boldsymbol{b}}(\zeta_m^s w).$$

The only way to get b_j^{m-1} is to take the $b_j(\zeta_m^s w)^{d-j}$ term in each $F_{\boldsymbol{b}}(\zeta_m^s w)$ appearing in the product. This gives

$$\frac{1}{m} \sum_{t=0}^{m-1} (\zeta_m^t w)^{d-j} \prod_{s \neq t} b_j(\zeta_m^s w)^{d-j}$$

$$= \frac{1}{m} b_j^{m-1} w^{m(d-j)} \sum_{t=0}^{m-1} \zeta_m^{(d-j)t} \prod_{s \neq t} \zeta_m^{(d-j)s}$$

$$= \frac{1}{m} b_j^{m-1} w^{m(d-j)} \sum_{t=0}^{m-1} (-1)^{(m+1)(d-j)} \quad \text{from 6.5,}$$

$$= (-1)^{(m+1)(d-j)} b_j^{m-1} w^{m(d-j)}.$$

This proves that $\gamma = (-1)^{(m+1)(d-j)}$, which completes the proof of (c).

Using (c), we see that the entries of the matrix $A_{d,m,k}(\boldsymbol{b})$ have the form

$$\begin{pmatrix} \pm b_0^{m-1} & * & * & * & \cdots & * \\ I_0 & \pm b_1^{m-1} + I_1 & * & * & \cdots & * \\ I_0 & I_1 & \pm b_2^{m-1} + I_2 & * & \cdots & * \\ I_0 & I_1 & I_2 & \pm b_3^{m-1} + I_3 & \cdots & * \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ I_0 & I_1 & I_2 & I_3 & \cdots & \pm b_d^{m-1} + I_d \end{pmatrix},$$

where we write I_j to indicate an element of the ideal I_j, and where stars indicate arbitrary elements of $\mathbb{Z}[\boldsymbol{b}]$.

We now consider how we might obtain the monomial $(b_0 b_1 \ldots b_d)^{m-1}$ in the expansion of $\det A_{d,m,k}(\boldsymbol{b})$. Since $I_0 = (0)$, the only nonzero entry in the first column is the top entry of $\pm b_0^{m-1}$, so we expand on that element and delete the first row and column. But we've now used up all of our allowable factors of b_0, so when we take the determinant of the remaining $d \times d$ submatrix, we're not allowed to use any monomials containing a b_0. Equivalently, we might as well set $b_0 = 0$ before taking the determinant of the $d \times d$ submatrix. When we do this, since $I_1 = (b_0)$, the only nonzero entry in the first column (of the submatrix) is the top entry, which is $\pm b_1^{m-1}$. Expanding on this entry and deleting the top row and column, we've now accumulated a factor of $(b_0 b_1)^{m-1}$, which uses up all of the allowable factors of b_0 and b_1. This means that we can set $b_0 = b_1 = 0$ before taking the determinant of the

remaining $(d-1) \times (d-1)$ submatrix. Since $I_2 = (b_0, b_1)$, the first column of the $(d-1) \times (d-1)$ submatrix is zero except for the top entry of $\pm b_2^{m-1}$. Continuing in this fashion, we see that the monomial $(b_0 b_1 \ldots b_d)^{m-1}$ appears in the expansion of $\det A_{d,m,k}(\boldsymbol{b})$ with coefficient ± 1.

This would suffice for most purposes, but we can use the explicit formula for the sign in (c) to exactly determine the coefficient. Thus $\det A_{d,m,k}(\boldsymbol{b})$ contains the monomial $(-1)^{\mu}(b_0 b_1 \ldots b_d)^{m-1}$ with

$$\mu \equiv \sum_{j=0}^{d} (m+1)(d-j) = (m+1)\frac{d^2+d}{2} \pmod{2}.$$

This completes the proof of Lemma 2. $\qquad\qquad\qquad\qquad\square$

7.3. Proof of Theorem 2(c)

Our goal is to prove that the rational map $\mathfrak{R}_{d,m,0} : \mathbb{P}_{\mathbb{Z}}^{2d+1} \dashrightarrow \mathbb{P}_{\mathbb{Z}}^{2d+1}$ is dominant. We observe that Lemma 2(d) and the elementary Jacobian formula (7.4) imply that the Jacobian determinant of the rational map $\mathfrak{R}_{d,m,0}$, considered as a homogeneous polynomial in $\mathbb{Z}[\boldsymbol{b}]$, includes a monomial of the form

$$m^{d+1}(b_0 b_1 \ldots b_d)^{2m-2}.$$

It follows that

$$\det \mathcal{J}_{d,m,k}(\boldsymbol{a}, \boldsymbol{b}) \neq 0 \quad \text{in } \mathbb{Z}[m^{-1}][\boldsymbol{b}].$$

This proves that $\mathfrak{R}_{d,m,0}$ is a dominant rational map provided that m is invertible, i.e., as long as we're not working in characteristic p for some prime p dividing m. In particular, it proves that $\mathfrak{R}_{d,m,0}$ is a dominant rational self-map of $\mathbb{P}_{\mathbb{Q}}^{2d+1}$.

However, for characteristics p dividing m, this tangent space argument will not work. Indeed, we will soon see that the map $\mathfrak{R}_{d,m,0}$ is inseparable over $\mathbb{F}_p$. So we proceed as follows. Theorem 2(b) says that the indeterminacy locus of $\mathfrak{R}_{d,m,k}$ is the set

$$\mathcal{Z} = \mathcal{Z}(\mathfrak{R}_{d,m,k}) = \{[\boldsymbol{a}, \boldsymbol{b}] \in \mathbb{P}^{2d+1} : \boldsymbol{b} = \boldsymbol{0}\},$$

and that $\mathfrak{R}_{d,m,k}$ induces a *morphism*

$$\mathfrak{R}_{d,m,k} : \mathbb{P}_{\mathbb{Z}}^{2d+1} \smallsetminus \mathcal{Z} \longrightarrow \mathbb{P}_{\mathbb{Z}}^{2d+1} \smallsetminus \mathcal{Z}.$$

We note that $\mathcal{Z}$ is independent of m and k, so compositions of various $\mathfrak{R}_{d,m,k}$ for a fixed d and different m and k give well-defined rational self-maps of $\mathbb{P}_{\mathbb{Z}}^{2d+1}$, since they are self-morphisms of the Zariski dense subset $\mathbb{P}_{\mathbb{Z}}^{2d+1} \smallsetminus \mathcal{Z}$. Contained within this set is the Zariski dense set on which $\mathfrak{R}_{d,m,k}$ agrees with the Landen transform $\mathfrak{F}_{m,k}$ (cf. Corollary 24(a)), so the composition formula in Proposition 16 implies the analogous formula

$$\mathfrak{R}_{d,m,k} \circ \mathfrak{R}_{d,n,\ell} = \mathfrak{R}_{d,mn,kn+\ell}. \tag{7.8}$$

The composition formula (7.8) is valid as rational self-maps of $\mathbb{P}_{\mathbb{Z}}^{2d+1}$. Taking $k = \ell = 0$ in (7.8) and applying it repeatedly, we see that if m has a factorization $m = p_1 p_2 \cdots p_r$ as a product of (not necessarily distinct) primes, then

$$\mathfrak{R}_{d,m,0} = \mathfrak{R}_{d,p_1,0} \circ \mathfrak{R}_{d,p_2,0} \circ \cdots \circ \mathfrak{R}_{d,p_r,0}. \tag{7.9}$$

Hence in order to prove that $\mathfrak{R}_{d,m,0}$ is a dominant rational self-map of $\mathbb{P}_{\mathbb{Z}}^{2d+1}$, it suffices to consider the case that $m = p$ is prime. Further, since we have already proven that $\mathfrak{R}_{d,p,0}$ is dominant over $\mathbb{Z}[p^{-1}]$, it suffices to prove that the reduction modulo p,

$$\tilde{\mathfrak{R}}_{d,p,0} : \mathbb{P}_{\mathbb{F}_p}^{2d+1} \dashrightarrow \mathbb{P}_{\mathbb{F}_p}^{2d+1},$$

is dominant.

In order to analyze $\tilde{\mathfrak{R}}_{d,p,0}$, it is convenient to write $\mathbb{F}_p$ as the quotient field

$$\mathbb{F}_p = \frac{\mathbb{Z}[\zeta_p]}{\mathfrak{p}} \quad \text{with } \mathfrak{p} \text{ the ideal } \mathfrak{p} = (1 - \zeta_p)\mathbb{Z}[\zeta_p].$$

Then using the fact that $\zeta_p \equiv 1 \pmod{\mathfrak{p}}$, we see that

$$H_{\boldsymbol{b},p}(w^p) = \prod_{t=0}^{p-1} F_{\boldsymbol{b}}(\zeta_p^t w) \equiv F_{\boldsymbol{b}}(w)^p \equiv F_{\boldsymbol{b}^p}(w^p) \pmod{\mathfrak{p}},$$

where we write $\boldsymbol{b}^p$ for the p-power Frobenius map applied to the coordinates of $\boldsymbol{b}$. This proves that the last $d + 1$ coordinate functions of $\tilde{\mathfrak{R}}_{d,p,0}(\boldsymbol{a}, \boldsymbol{b})$

are $b_0^p, \ldots, b_d^p$, i.e., $\tilde{\mathfrak{R}}_{d,p,0}$ has the form

$$\tilde{\mathfrak{R}}_{d,p,0}(\boldsymbol{a}, \boldsymbol{b}) = [\tilde{G}_{\boldsymbol{a},\boldsymbol{b},p,0}, b_0^p, b_1^p, \ldots, b_d^p],$$

where we write $\tilde{G}_{\boldsymbol{a},\boldsymbol{b},p,0}$ for the list of z-coefficients of $G_{\boldsymbol{a},\boldsymbol{b},p,0}(z)$, reduced modulo $\mathfrak{p}$.

Viewing $\mathbb{P}^{2d+1}$ as $(\mathbb{A}^{2d+2} \smallsetminus 0)/\mathbb{G}_m$, we lift the rational map $\tilde{\mathfrak{R}}_{d,p,0}$ to a morphism

$$R : \mathbb{A}_{\mathbb{F}_p}^{2d+2} \longrightarrow \mathbb{A}_{\mathbb{F}_p}^{2d+2}, \qquad (\boldsymbol{a}, \boldsymbol{b}) \longmapsto (\tilde{G}_{\boldsymbol{a},\boldsymbol{b},p,0}, b_0^p, b_d^p).$$

It suffices to prove that R is dominant. We write R as a composition $R = T \circ S$ with

$$S : \mathbb{A}_{\mathbb{F}_p}^{2d+2} \longrightarrow \mathbb{A}_{\mathbb{F}_p}^{2d+2} \qquad\qquad T : \mathbb{A}_{\mathbb{F}_p}^{2d+2} \longrightarrow \mathbb{A}_{\mathbb{F}_p}^{2d+2}$$
$$(\boldsymbol{x}, \boldsymbol{y}) \longmapsto (\tilde{G}_{\boldsymbol{x},\boldsymbol{y},p,0}, \boldsymbol{y}) \qquad\qquad (\boldsymbol{x}, \boldsymbol{y}) \longmapsto (\boldsymbol{x}, \boldsymbol{y}^p)$$

Lemma 2(d) tells us that S is dominant, and it is clear that T is dominant, hence R is also dominant. This completes the proof that $\tilde{\mathfrak{R}}_{d,p,0}$ is dominant, and with it the proof of Theorem 2(c).

Remark 26. Theorem 2 describes the algebraic degree of the rational map $\mathfrak{R}_{d,m,k}$, where in general, the algebraic degree of a rational map $\varphi : \mathbb{P}^N \dashrightarrow \mathbb{P}^N$ of projective space is the integer d satisfying $\varphi^* \mathcal{O}_{\mathbb{P}^N}(1) = \mathcal{O}_{\mathbb{P}^N}(d)$. It is also of interest to compute the separable and inseparable degrees of dominant rational maps $\varphi : X \dashrightarrow Y$ of equidimensional varieties. By definition, these are the separable and inseparable degrees of the associated extension $K(X)/\varphi^* K(Y)$ of function fields. (Over $\mathbb{C}$, the separable degree is equal to the topological degree of φ, i.e., $\#\varphi^{-1}(y)$ for a generic point $y \in Y(\mathbb{C})$.) The proof of Theorem 2(c) shows that in characteristic 0, the induced map $\mathfrak{R}_{d,m,0} : \mathbb{P}_{\mathbb{Q}}^{2d+1} \dashrightarrow \mathbb{P}_{\mathbb{Q}}^{2d+1}$ has (separable) degree m^d, while in characteristic p, we factor $m = p^e n$ with $p \nmid n$, and then $\mathfrak{R}_{d,m,0} : \mathbb{P}_{\mathbb{F}_p}^{2d+1} \dashrightarrow \mathbb{P}_{\mathbb{F}_p}^{2d+1}$ has separable degree n^d and inseparable degree p^{ed}. The same statements are true for $\mathfrak{R}_{d,m,k}$ as self-maps of $\{a_0 = 0\} \cong \mathbb{P}^{2d}$.

7.4. Proof of Theorem 2(d)

The proof of (d) is similar to (c), but longer and computationally more complicated, so we only give an outline and leave the details to the reader.

We use a prime to denote restriction to the hyperplane $\{a_0 = 0\}$ in $\mathbb{P}^{2d+1}$. So for example $\mathfrak{R}'_{d,m,k}$ is the restriction of $\mathfrak{R}_{d,m,k}$ to $\{a_0 = 0\}$, and $\mathcal{J}'_{d,m,k}(\boldsymbol{a}, \boldsymbol{b})$ is the Jacobian matrix of $\mathfrak{R}'_{d,m,k}$. We observe that $\mathcal{J}'_{d,m,k}(\boldsymbol{a}, \boldsymbol{b})$ is obtained from $\mathcal{J}_{d,m,k}(\boldsymbol{a}, \boldsymbol{b})$ by deleting the first column and the first row of $\mathcal{J}_{d,m,k}(\boldsymbol{a}, \boldsymbol{b})$, and then setting $a_0 = 0$. Looking at the block form (7.3) of $\mathcal{J}_{d,m,k}(\boldsymbol{a}, \boldsymbol{b})$, we see that $\mathcal{J}'_{d,m,k}(\boldsymbol{a}, \boldsymbol{b})$ has the form

$$\mathcal{J}'_{d,m,k}(\boldsymbol{a}, \boldsymbol{b}) = \begin{pmatrix} A'_{d,m,k}(\boldsymbol{b}) & \mathbf{0} \\ C'_{d,m,k}(\boldsymbol{a}, \boldsymbol{b}) & D_{d,m}(\boldsymbol{b}) \end{pmatrix}, \tag{7.10}$$

where $A'_{d,m,k}$ is the d-by-d matrix obtained by deleting the first column and row of $A_{d,m,k}$, and $D_{d,m}$ is the $(d+1)$-by-$(d+1)$ matrix already appearing in $\mathcal{J}_{d,m,k}$.

We note that Lemmas 1 and 2(d) tell us that $\det D_{d,m}(\boldsymbol{b})$ includes the monomial

$$m^{d+1}(-1)^{(m+1)(d^2+d)/2}(b_0 b_1 \cdots b_d)^{m-1}. \tag{7.11}$$

We recall Lemma 2(c,d) gives various formulas when $k = 0$. The next result gives analogous formulas for $1 \le k < m$.

Lemma 3. *Let $1 \le k < m$, and write the entries of the matrix $A'_{d,m,k}$ as $A'_{d,m,k}(\boldsymbol{b}) = \left(\alpha'_{d,m,k}(\boldsymbol{b})_{i,j}\right)$.*

(a) *For $1 \le j \le d$, we write $I'_j \subset \mathbb{Z}[\boldsymbol{b}]$ for the ideal generated by*

$$b_0, b_1, \dots, b_{j-2}, b_{j-1}^{k+1}.$$

Then

$$\alpha'_{d,m,k}(\boldsymbol{b})_{i,j} \equiv 0 \pmod{I'_j} \quad \text{for all } i > j,$$
$$\alpha'_{d,m,k}(\boldsymbol{b})_{j,j} \equiv (-1)^{(m+1)(d-j)+k} b_{j-1}^k b_j^{m-1-k} \pmod{I'_j}.$$

(b) *When $\det A'_{d,m,k}(\boldsymbol{b})$ is written as a polynomial in $\mathbb{Z}[\boldsymbol{b}]$, it includes the monomial*

$$(-1)^{(m+1)(d^2-d)/2+dk} b_0^k (b_1 b_2 \cdots b_{d-1})^{m-1} b_d^{m-1-k}.$$

Proof. We omit the proof of Lemma 3, which is similar to the proof of Lemma 2(c,d). □

Resuming the proof of Theorem 2(d), we note that (7.10), (7.11), and Lemma 3(b) imply that

$$\det \mathcal{J}_{d,m,k}(\boldsymbol{a}, \boldsymbol{b}) = \det A'_{d,m,k}(\boldsymbol{b}) \det D_{d,m}(\boldsymbol{b})$$

has a monomial term of the form

$$m^{d+1}(-1)^{(m+1)d^2+dk} b_0^{m-1+k}(b_1 b_2 \cdots b_{d-1})^{2m-2} b_d^{2m-2-k}.$$

In particular, we conclude that $\mathfrak{R}'_{d,m,k}$ is a dominant rational self-map of $\mathbb{P}^{2d}$ over $\mathbb{Z}[m^{-1}]$.

The next step of the proof is to note that that the restriction of $\mathfrak{R}_{d,m,0}$ to $\mathbb{P}^{2d} = \{a_0 = 0\} \subset \mathbb{P}^{2d+1}$ gives a map $\mathfrak{R}'_{d,m,0}$ from $\{a_0 = 0\}$ to itself. This follows from the fact that $G_{\boldsymbol{a},\boldsymbol{b},m,0} = \pm a_0 b_0^{m-1} z^d + O(z^{d-1})$. We claim that $\mathfrak{R}'_{d,m,0}$ is a dominant rational map over $\mathbb{Z}$. To see this, we first perform a Jacobian calculation for $\mathfrak{R}'_{d,m,0}$ similar to those already done to check that $\mathfrak{R}'_{d,m,0}$ is a dominant rational map over $\mathbb{Z}[m^{-1}]$. We then decompose $\mathfrak{R}'_{d,m,0}$ as a composition of maps $\mathfrak{R}'_{d,p,0}$ with p prime, cf. (7.9), so it suffices to show that $\mathfrak{R}'_{d,p,0}$ is dominant over $\mathbb{F}_p$. The proof of this last assertion is similar to the final step in the proof of Theorem 2(c) earlier in this section.

Finally, writing $m = np$ with p prime and using the decomposition $\mathfrak{R}'_{d,m,k} = \mathfrak{R}'_{d,n,0} \circ \mathfrak{R}'_{d,p,k}$, we are reduced to showing that $\mathfrak{R}'_{d,p,k}$ is dominant over $\mathbb{F}_p$. But we know from Lemma 3(b) that $\det A'_{d,m,k}(\boldsymbol{b})$ includes a monomial whose coefficient is ± 1, while the matrix $D_{d,m}(\boldsymbol{b})$ does not depend on k, so the argument used at the end of the proof of Theorem 2(c) earlier in this section can be used, *mutatis mutandis*, to complete the proof of Theorem 2(d).

Remark 27. Let $A'_{d,m,k}(\boldsymbol{b})$ be the d-by-d matrix described in (7.10), i.e., the matrix obtained by deleting the first column and row of $A_{d,m,k}(\boldsymbol{b})$. For $k = 0$, we have

$$\det A_{d,m,0}(\boldsymbol{b}) = (-b_0)^{m-1} \det A'_{d,m,0}(\boldsymbol{b}),$$

since only the first entry of the first column of $A_{d,m,0}(\boldsymbol{b})$ is nonzero. It appears from examples that the following formula is true:

$$b_d^k \det A'_{d,m,k}(\boldsymbol{b}) \stackrel{?}{=} (-1)^{(d+1)k} b_0^k \det A'_{d,m,0}(\boldsymbol{b}). \tag{7.12}$$

We also remark that an easy calculation shows that if $1 \leq m \leq d+1$, then the top d rows of $A_{d,m,k+1}$ are equal to the bottom d rows of $A_{d,m,k}$, while the last row of $A_{d,m,k+1}$ is equal to the $(d+1-m)$'th row of $A_{d,m,k}$ shifted one place to the right. But this relation between $A_{d,m,k}$ and $A_{d,m,k+1}$ is not sufficient to explain (7.12).

8. The map on $\mathbb{P}^d$ induced by $H_{\boldsymbol{b},m}$

In this section we discuss the map on $\mathbb{P}^d$ induced by using only the denominator of the Landen transform. We write the function $H_{\boldsymbol{b},m}(z)$ defined by the formula (6.2) in Proposition 18 as

$$H_{\boldsymbol{b},m}(z) = \sum_{i=0}^{d} H_{m,i}(\boldsymbol{b})z^{d-i},$$

and we use the z-coefficients of $H_{\boldsymbol{b},m}(z)$ to define a map

$$h_m : \mathbb{P}^d \longrightarrow \mathbb{P}^d, \quad h_m(\boldsymbol{b}) = \left[H_{m,0}(\boldsymbol{b}), \ldots, H_{m,d}(\boldsymbol{b}) \right].$$

Thus h_m is the map formed using the final $d+1$ coordinate functions of the rational map $\mathfrak{R}_{d,m,k}$ described in Theorem 2(a). We start with an easy fact.

Proposition 28. *The map h_m is a morphism.*

Proof. The computation (7.2) done during the course of proving Theorem 2(b) shows that

$$H_{m,0}(\boldsymbol{b}) = \cdots = H_{m,d}(\boldsymbol{b}) = 0 \iff \boldsymbol{b} = \boldsymbol{0},$$

so $\mathcal{Z}(h_m) = \emptyset$. $\qquad\square$

More interesting is the fact that h_m is closely related to the m'th-power map. In order to describe the exact relationship, we dehomogenize by setting $b_0 = 1$. Since $H_{m,0}(\boldsymbol{b}) = (-1)^{(m+1)d}b_0^d$, this has the effect of restricting h_m to an affine morphism (which by abuse of notation we also call h_m) given by

$$h_m : \mathbb{A}^d \longrightarrow \mathbb{A}^d,$$
$$h_m(\boldsymbol{b}) = \left((-1)^{(m+1)d} H_{m,1}(\boldsymbol{b}), \ldots, (-1)^{(m+1)d} H_{m,d}(\boldsymbol{b}) \right), \qquad (7.13)$$

where again by abuse of notation, we now use affine coordinates $\boldsymbol{b} = (b_1, \ldots, b_d)$. We let

$$\pi_m : \mathbb{A}^d \longrightarrow \mathbb{A}^d, \quad \pi_m(x_1, \ldots, x_d) = (x_1^m, \ldots, x_d^m),$$

be the m-power map, and we let

$$\sigma_d : \mathbb{A}^d \to \mathbb{A}^d, \quad \sigma_d(\boldsymbol{x}) = \big(-\sigma_d^1(\boldsymbol{x}), \sigma_d^2(\boldsymbol{x}), \ldots, (-1)^d \sigma_d^d(\boldsymbol{x})\big),$$

be the map defined by the elementary symmetric functions, taken with alternating sign. So for example, when $d = 3$ we have

$$\sigma_3(x_1, x_2, x_3) = \big(-x_1 - x_2 - x_3, x_1 x_2 + x_1 x_3 + x_2 x_3, -x_1 x_2 x_3\big).$$

It is well known that σ_d induces an isomorphism that takes the quotient of $\mathbb{A}^d$ by the action of the symmetric group $\mathcal{S}_d$ on $(x_1, \ldots, x_d)$ to $\mathbb{A}^d$. We denote this isomorphism by

$$\bar{\sigma}_d : \mathbb{A}^d / \mathcal{S}_d \xrightarrow{\sim} \mathbb{A}^d.$$

Proposition 29. *With notation as described in this section, we have*

$$h_m = \bar{\sigma}_d \circ \pi_m \circ \bar{\sigma}_d^{-1} \quad \text{as self-maps of } \mathbb{A}^d.$$

Proof. In order to relate h_m to π_m, it is convenient to let $u_1, \ldots, u_d$ be the z-roots of $F_{\boldsymbol{b}}(z) = 0$ in some integral closure of $\mathbb{Z}[b_1, \ldots, b_d]$. (Remember that we have set $b_0 = 1$.) In other words,

$$b_i = (-1)^i \sigma_d^i(u_1, \ldots, u_d) \quad \text{and} \quad F_{\boldsymbol{b}}(z) = \prod_{s=1}^{d} (z - u_s).$$

This allows us to compute

$$\sum_{i=0}^{d} H_{m,i}(\boldsymbol{b}) w^{m(d-i)} = H_{\boldsymbol{b},m}(w^m) = \prod_{t=0}^{m-1} F_{\boldsymbol{b}}(\zeta_m^t w) = \prod_{t=0}^{m-1} \prod_{s=1}^{d} (\zeta_m^t w - u_s)$$

$$= \prod_{s=1}^{d} \prod_{t=0}^{m-1} (\zeta_m^t w - u_s) = \prod_{s=1}^{d} (-1)^{m+1} (w^m - u_s^m)$$

$$= (-1)^{d(m+1)} \sum_{i=0}^{d} (-1)^i \sigma_d^i(u_1^m, \ldots, u_d^m) w^{m(d-i)}$$

$$= (-1)^{d(m+1)} \sum_{i=0}^{d} (-1)^i \sigma_d^i \circ \pi_m(u_1, \ldots, u_d) w^{m(d-i)}.$$

Hence for $1 \leq i \leq d$ we have

$$H_{m,i}(\boldsymbol{b}) = (-1)^{d(m+1)} (-1)^i \sigma_d^i \circ \pi_m(u_1, \ldots, u_d).$$

Combining the $H_{m,i}$ to form h_m as in (7.13), we obtain

$$h_m(\boldsymbol{b}) = \bar{\sigma}_d \circ \pi_m(u_1, \ldots, u_d).$$

However, by construction $(u_1, \ldots, u_d)$ satisfies

$$\bar{\sigma}_d(u_1, \ldots, u_d) = \boldsymbol{b},$$

which gives the desired formula

$$h_m = \bar{\sigma}_d \circ \pi_m \circ \bar{\sigma}_d^{-1}.$$

This completes the proof of Proposition 29. $\square$

Remark 30. Although the equality in Proposition 29 is only valid on the affine set $\{b_0 \neq 0\}$, we note that on the excluded hyperplane $b_0 = 0$, the definition of h_m is given via a product of polynomials of degree $d-1$. This allows us to completely describe h_m on $\mathbb{P}^d$ via a natural decomposition. More precisely, we decompose $\mathbb{P}^d$ as a disjoint union

$$\mathbb{P}^d = \bigcup_{n=0}^{d} \{b_0 = \cdots = b_{n-1} = 0 \text{ and } b_n \neq 0\} = \bigcup_{n=0}^{d} \mathbb{A}^n.$$

Then Proposition 29 applied to each affine piece implies that the restriction of $h_m : \mathbb{P}^d \to \mathbb{P}^d$ to $\mathbb{A}^n$ satisfies

$$h_m|_{\mathbb{A}^n} = \bar{\sigma}_n \circ \pi_m \circ \bar{\sigma}_n^{-1}.$$

Remark 31. In some situations it may be more convenient to view $\mathfrak{R}_{d,m,k}$ itself as a map of affine space by dehomogenizing with $b_0 = 1$. We write

$\mathfrak{R}'_{d,m,k}$ for the resulting polynomial map

$$\mathfrak{R}'_{d,m,k} : \mathbb{A}_{\mathbb{Z}}^{2d+1} \longrightarrow \mathbb{A}_{\mathbb{Z}}^{2d+1},$$

where we identify

$$\mathbb{A}_{\mathbb{Z}}^{2d+1} \xrightarrow{\ \sim\ } \mathbb{P}_{\mathbb{Z}}^{2d+1} \smallsetminus \{b_0 = 0\}.$$

We observe that there are a number of vector subspaces of $\mathbb{A}_{\mathbb{Z}}^{2d+1}$ that the morphism $\mathfrak{R}'_{d,m,k}$ leaves invariant, including for example

$$U_i = \{a_0 = a_1 = \cdots = a_i = 0\} \quad \text{for } 0 \le i \le d,$$
$$V_i = \{a_d = a_{d-1} = \cdots = a_{d-i} = 0\} \quad \text{for } 0 \le i \le d,$$
$$W_i = \{b_d = b_{d-1} = \cdots = b_{d-i} = 0\} \quad \text{for } 0 \le i < d.$$

(Note that for $1 \le k < m$, we have $\mathfrak{R}'_{d,m,k}(\mathbb{A}_{\mathbb{Z}}^{2d+1}) = U_0$.)

Writing $\boldsymbol{a}$ as a column vector and letting $A_{d,m,k}(\boldsymbol{b})$ be the matrix appearing in the Jacobian, see (7.3), we see that $\mathfrak{R}'_{d,m,k}$ takes the form

$$\mathfrak{R}'_{d,m,k}(\boldsymbol{a}, \boldsymbol{b}) = \big(A_{d,m,k}(\boldsymbol{b})\boldsymbol{a}, h_m(\boldsymbol{b})\big).$$

With this notation, the composition law for the Landon transform described in Proposition 16 becomes the matrix formula

$$A_{d,m,k}\big(h_m(\boldsymbol{b})\big) A_{d,n,\ell}(\boldsymbol{b}) = A_{d,mn,kn+\ell}(\boldsymbol{b}).$$

References

1. F. Berteloot and J.-J. Loeb, Une caractérisation géométrique des exemples de Lattès de $\mathbb{P}^k$, *Bull. Soc. Math. France*, **129**(2001), No.2, 175-188.

2. G. Boros, M. Joyce, and V. H. Moll, A transformation of rational functions, *Elem. Math.*, **58**(2003), No.2, 73-83.

3. G. Boros, J. Little, V. Moll, E. Mosteig, and R. Stanley, A map on the space of rational functions, *Rocky Mountain J. Math.*, **35**(2005), No.6, 1861-1880.

4. G. Boros and V. H. Moll, A rational Landen transformation. The case of degree six. In *Analysis, geometry, number theory: the mathematics of Leon Ehrenpreis* (*Philadelphia, PA, 1998*), volume 251 of *Contemp. Math.*, pages 83–91. Amer. Math. Soc., Providence, RI, 2000.

5. G. Boros and V. H. Moll, Landen transformations and the integration of rational functions. *Math. Comp.*, **71**(2002), No.238, 649-668 (electronic).

6. S. Briscoe, L. Jiminez, D. Manna, L. Medina, and V. Moll, The dynamics of a trans-
    formation on the space of rational maps. in preparation.

7. S. Cantat, Sur les groupes de transformations birationnelles des surfaces. *Ann. of
    Math. (2)*, 174(1):299–340, 2011.

8. M. Chamberland and V. H. Moll, Dynamics of the degree six Landen transformation.
    Discrete Contin. Dyn. Syst., **15**(2006), No.3, 905-919.

9. T.-C. Dinh, Sur les applications de Lattès de $\mathbb{P}^k$, *J. Math. Pures Appl. (9)*, **80**(2001),
    No.6, 577-592.

10. T.-C. Dinh, Sur les endomorphismes polynomiaux permutables de $\mathbb{C}^2$, *Ann. Inst.
    Fourier* (*Grenoble*), **51**(2001), No.2, 431-459.

11. T.-C. Dinh and N. Sibony, Sur les endomorphismes holomorphes permutables de $\mathbb{P}^k$,
    Math. Ann., **324**(2002), No.1, 33-70.

12. C. F. Gauß, Arithmetische Geometrisches Mittel, 1799, *Werke. Band III*, pages 361–
    432. Konigliche Gesellschaft der Wissenschaft, Gottingen. Reprinted by Georg Olms
    Verlag, Hildesheim, 1973.

13. J. Hubbard and V. Moll, A geometric view of rational Landen transformations, *Bull.
    London Math. Soc.*, **35**(2003), No.3, 293-301.

14. J. Landen, A disquisition concerning certain fluents, which are assignable by the arcs
    of the conic sections; wherein are investigated some new and useful theorems for
    computing such fluents, *Philos. Trans. Royal Soc. London*, **61**(1771), 298-309.

15. J. Landen, An investigation of a general theorem for finding the length of any arc of
    any conic hyperbola, by means of two elliptic arcs, with some other new and useful
    theorems deduced therefrom, *Philos. Trans. Royal Soc. London*, **65**(1775), 283-289.

16. D. Manna and V. H. Moll. Rational Landen transformations on $\mathbb{R}$. *Math. Comp.*,
    76(2007), No.260, 2023-2043 (electronic).

17. D. Manna and V. H. Moll, A simple example of a new class of Landen transformations,
    Amer. Math. Monthly, **114**(2007), No.3, 232-241.

18. D. V. Manna and V. H. Moll, Landen survey. In *Probability, geometry and integrable
    systems*, volume 55 of *Math. Sci. Res. Inst. Publ.*, pages 287–319. Cambridge Univ.
    Press, Cambridge, 2008.

19. V. H. Moll, S. Robins and K. Soodhalter, The action of Hecke operators on hyperge-
    ometric functions, *J. Aust. Math. Soc.*, **89**(2010), No.1, 51-74.

20. E. Mosteig, Fixed points of maps on the space of rational functions, *Online J. Anal.
    Comb.*, (1):Art. 2, 9 pp. (electronic), 2006.

21. C. E. Rhodes, Questions, Discussions, and Notes: A Geometric Interpretation of Lan-
    den's Transformation, *Amer. Math. Monthly*, **39**(1932), No.10, 594-596.

22. J. F. Ritt, Permutable rational functions, *Trans. Amer. Math. Soc.*, **25**(1923), No.3,
    399-448.

23. J. H. Silverman, *The Arithmetic of Dynamical Systems*, volume 241 of *Graduate Texts
    in Mathematics*. Springer, New York, 2007.

24. J. H. Silverman, *Moduli Spaces and Arithmetic Dynamics*, volume 30 of *CRM Mono-
    graph Series*. American Mathematical Society, Providence, RI, 2012.

25. B. van der Waerden, *Algebra*, Frederick Ungar Publ. Co., New York, 7th edition, 1970.