LMS J. Comput. Math. 15 (2012) 400–417 © 2012 Authors
doi:10.1112/S1461157012001131

Minimal models for rational functions in a dynamical setting

Nils Bruin and Alexander Molnar

Abstract

We present a practical algorithm to compute models of rational functions with minimal resultant under conjugation by fractional linear transformations. We also report on a search for rational functions of degrees 2 and 3 with rational coefficients that have many integers in a single orbit. We find several minimal quadratic rational functions with eight integers in an orbit and several minimal cubic rational functions with ten integers in an orbit. We also make some elementary observations on possibilities of an analogue of Szpiro's conjecture in a dynamical setting and on the structure of the set of minimal models for a given rational function.

1. *Introduction*

The results in this article are inspired by a conjecture by Silverman.

Conjecture 1.1. For each $d \geqslant 2$ there is a constant C_d such that the following is true. Let $\phi(z) \in \mathbb{Q}(z)$ be a rational function of degree $d \geqslant 2$, such that ϕ^2 is not a polynomial, and for any $\alpha \in \mathbb{Q}$ consider the *orbit* of α under ϕ, being

$$\mathcal{O}_\phi(\alpha) = \{\alpha, \phi(\alpha), \phi(\phi(\alpha)), \dots\}.$$

If ϕ is *minimal* and $\mathcal{O}_\phi(\alpha)$ is infinite as a set then

$$\#\{\beta \in \mathcal{O}_\phi(\alpha) : \beta \in \mathbb{Z}\} \leqslant C_d.$$

The conjecture is a direct translation of a conjecture by Lang, inspired by work by Dem'janenko [4, p. 140], that the number of integral points on an elliptic curve in *minimal* Weierstrass form is bounded above by a constant only depending on the field and the rank of the curve.

Both conjectures are ostensibly false if the *minimal* condition is dropped. Silverman proposes the following definition for minimality of rational functions. Let $f, g \in \mathbb{Z}[z]$ be polynomials such that $\phi(z) = f(z)/g(z)$ and such that the coefficients of f, g do not have a divisor in common. If $\deg(f) = \deg(g)$, see Section 2 for the full definition, we define

$$\mathrm{Res}(\phi) = |\mathrm{res}(f, g)|.$$

We have that the group of fractional linear transformations $\mathrm{PGL}_2(\mathbb{Q}) = \{z \mapsto (az + b)/(cz + d) : a, b, c, d \in \mathbb{Q} \text{ and } ad - bc \neq 0\}$ acts by conjugation on $\mathbb{Q}(z)$, that is, if $A \in \mathrm{PGL}_2(\mathbb{Q})$ then $\phi^A = A^{-1} \circ \phi \circ A$. Silverman considers the subgroup $\mathrm{Aff}_2(\mathbb{Q}) = \{z \mapsto az + b : a, b \in \mathbb{Q} \text{ and } a \neq 0\}$ and defines a rational function to be *affine minimal* if

$$\mathrm{Res}(\phi) = \min\{\mathrm{Res}(\phi^A) : A \in \mathrm{Aff}_2(\mathbb{Q})\}$$

and phrases Conjecture 1.1 in terms of it. Because $\mathbb{Z}$ is a Dedekind domain, this yields the same notion as full $\mathrm{PGL}_2(\mathbb{Q})$-minimality (see Proposition 2.10).

Received 2 May 2012; revised 30 May 2012.

2010 Mathematics Subject Classification 37P05 (primary), 11S82 (secondary).

Research of first author supported by NSERC.

In order to enable the gathering of experimental evidence for the conjecture, one obviously needs a procedure to decide if a given rational function $\phi(z)$ is (affine) minimal, analogous to Tate's algorithm [**13**] to compute minimal models of elliptic curves. The main contribution of this article is Algorithm 4.1, an explicit, practical procedure that, given a rational function ϕ, tests whether it is minimal and, if not, computes a fractional linear transformation A such that ϕ^A is minimal. The procedure we describe applies to rational functions ϕ over any field K that is the field of fractions of a principal ideal domain R. We also provide an implementation of the algorithm for rational functions over $\mathbb{Q}$ in the computer algebra system Magma [**2**], see [**3**].

We apply the algorithm as part of a search for minimal rational functions over $\mathbb{Q}$ of degrees 2 and 3 with many integers in their orbits. We do this by prescribing an initial orbit consisting of small integers and interpolating the rational function ϕ through the prescribed values. We can then test if there are any more integers in the early part of the orbit and test if ϕ is minimal. A systematic search of possible initial orbits yielded, among other results,

$$\frac{86z^2 - 1068z - 338}{z^2 + 7z - 338} \quad \text{with } \mathcal{O}_\phi(0) = [0, 1, 4, 11, 12, 7, 15, -374, \dots]$$

and

$$\frac{7z^3 - 41z^2 - 216z + 180}{2z^3 - z^2 - 21z + 90} \quad \text{with } \mathcal{O}_\phi(0) = [0, 2, -6, 6, -3, 3, -9, 5, -5, 8, \dots].$$

These are orbits with at least eight, respectively ten, integers in them, which is two more than one can prescribe using interpolation in either case. In particular we see that for Conjecture 1.1 we would need at least $C_2 \geqslant 8$ and $C_3 \geqslant 10$. See Section 7 and [**3**] for the complete results of our search.

As an easy corollary of the construction of our algorithm, we see that if $f, g \in \mathbb{Z}[z]$ are monic polynomials with no roots in common and $2\deg(g) < \deg(f) + 1$ then $\phi(z) = f(z)/g(z)$ is minimal (see Remark 3.4). As a consequence, from

$$\phi(z) = \frac{z^d + p^r}{z},$$

we see that powers of primes occurring in resultants of minimal rational maps can be arbitrarily large. That means that a possible dynamical analogue of Szpiro's conjecture would require a more refined concept of conductor and/or of resultant than the most naive guesses, see Section 5.

Finally, we note that the set of minimal rational maps is the union of $\mathrm{PGL}_2(\mathbb{Z})$-orbits. We show that, at least for functions of odd degree, the set may consist of more than a single orbit (see Example 6.1). We make some remarks about the general structure in Section 6. These remarks help us in providing Example 6.4 of a rational function over $\mathbb{Q}(\sqrt{-5})$ that does admit a minimal model but not via an affine transformation, thus providing an example that our algorithm is fundamentally restricted to principal ideal domains.

A significant part of the results in this paper come from the MSc Thesis of the second author [**6**].

2. *Preliminaries*

Let K be a field. Our main objects of study are rational morphisms

$$\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$$

of degree $d \geqslant 2$, defined over K. We follow the definitions and notation from [**10**] and write $\mathrm{Rat}_d(K)$ for the space of such rational morphisms. By choosing homogeneous coordinates $(X : Y)$ on $\mathbb{P}^1$ we can represent a morphism ϕ by two homogeneous degree d polynomials $F, G \in K[X, Y]$ such that

$$\phi(X : Y) = (F(X, Y) : G(X, Y)).$$

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

We write

$$F(X,Y) = f_d X^d + f_{d-1} X^{d-1} Y + \cdots + f_0 Y^d$$

and

$$G(X,Y) = g_d X^d + g_{d-1} X^{d-1} Y + \cdots + g_0 Y^d.$$

It is often convenient to work with an affine coordinate $z = X/Y$ instead and write $f(z) = F(z,1)$ and $g(z) = G(z,1)$, so that we have

$$\phi(z) = \frac{f(z)}{g(z)}.$$

Rational morphisms ϕ defined over K correspond to rational points on a quasi-projective variety Rat_d in the sense that the projective point $(f_d : \ldots : f_0 : g_d : \ldots : g_0) \in \mathbb{P}^{2d+2}(K)$ completely determines ϕ. Let Res_d be the resultant of F, G as degree d forms. This is a bihomogeneous polynomial of bidegree (d,d) in $f_0, \ldots, f_d$ and $g_0, \ldots, g_d$. In order for ϕ to be of degree d we need that $\mathrm{Res}_d(F,G)$ does not vanish. Therefore, the variety Rat_d is the complement in $\mathbb{P}^{2d+2}$ of the hypersurface $\mathrm{Res}_d = 0$.

The automorphism group of $\mathbb{P}^1$ is PGL_2. It has a natural right-action on Rat_d via conjugation: for any $A \in \mathrm{PGL}_2$ we have $\phi^A = A^{-1} \circ \phi \circ A$. Rational maps in the same PGL_2-orbit obviously have the same dynamical properties, so the appropriate moduli space for dynamical purposes is

$$\mathcal{M}_d = \mathrm{Rat}_d \,/\, \mathrm{PGL}_2.$$

Remark 2.1. See [10, Section 4.4] for a discussion on its structure as an algebraic variety. In general, there may be rational points on $\mathcal{M}_d$ that do not have a rational point on Rat_d above them. These are rational morphisms for which the field of moduli is not equal to the field of definition. See [10, Section 4.10] and [9].

For our purposes it is more convenient to make a step in the other direction and consider the affine cone over Rat_d. Given a rational morphism $\phi = (F : G)$, we say $[F,G]$ is a *model* for ϕ. Similarly, in affine coordinates, we have $\phi = f/g$ and we also write $[f,g]$ for the model of ϕ, which encodes exactly the same information.

We also say it is a model for $[\phi]$, where $[\phi]$ is the class of ϕ in $\mathcal{M}_d$. Naturally, if $[F,G]$ is a model for ϕ and λ is a non-zero scalar, then $[\lambda F, \lambda G]$ is also a model for ϕ. We write M_d for the space of models. The embedding

$$\begin{aligned} M_d &\to \mathbb{A}^{2d+2} \\ [F,G] &\mapsto (f_d, \ldots, f_0, g_d, \ldots, g_0) \end{aligned}$$

identifies M_d with the affine open $\{\mathrm{Res}_d \neq 0\} \subset \mathbb{A}^{2d+2}$. We follow [10, 4.11] and lift the action of PGL_2 on Rat_d to an action of GL_2 on M_d in a way that avoids division. For $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ we consider the *classical adjoint*

$$A^{\mathrm{adj}} = \det(A)\, A^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}.$$

Note that $[F,G] \in M_d$ and $A \in \mathrm{GL}_2$ can be interpreted as morphisms $\mathbb{A}^2 \to \mathbb{A}^2$, so we can let A act on M_d by defining

$$[F,G]^A = [F_A, G_A] = A^{\mathrm{adj}} \circ [F,G] \circ A,$$

where

$$\begin{aligned} F_A(X,Y) &= \delta F(\alpha X + \beta Y, \gamma X + \delta Y) - \beta G(\alpha X + \beta Y, \gamma X + \delta Y) \\ G_A(X,Y) &= -\gamma F(\alpha X + \beta Y, \gamma X + \delta Y) + \alpha G(\alpha X + \beta Y, \gamma X + \delta Y). \end{aligned}$$

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

It is easy to check that this action descends to the action of PGL_2 on Rat_d we considered earlier. We now have an action of $\mathbb{G}_{\mathrm{m}} \times \mathrm{GL}_2$ on M_d given by

$$[F, G]^{(\lambda, A)} = [\lambda F_A, \lambda G_A] \quad \text{where } (\lambda, A) \in \mathbb{G}_{\mathrm{m}} \times \mathrm{GL}_2.$$

Furthermore, the compatibility with Rat_d gives us that $M_d/(\mathbb{G}_{\mathrm{m}} \times \mathrm{GL}_2) = \mathcal{M}_d$.

The main advantage of considering M_d rather than Rat_d is that Res_d can be interpreted as a function on M_d. It is a covariant of the group we are considering.

PROPOSITION 2.2. *Let $[F, G] \in M_d$ and let $(\lambda, A) \in \mathbb{G}_{\mathrm{m}} \times \mathrm{GL}_2$. Then*

$$\mathrm{Res}_d(\lambda F_A, \lambda G_A) = \lambda^{2d} \det(A)^{d^2+d} \mathrm{Res}(F, G).$$

Proof. See the proof of [**10**, Proposition 4.95]. □

REMARK 2.3. Note that $\mathrm{Res}_d(F, G)$ is not equal to the univariate polynomial resultant $\mathrm{res}(f, g)$ if either $d_f = \deg_z(f)$ or $d_g = \deg_z(g)$ is smaller than d. We have the relation

$$\mathrm{Res}_d(F, G) = f_d^{d-d_g}((-1)^d g_d)^{d-d_f} \mathrm{res}(f, g).$$

Now consider a field K that is the field of fractions of an integral domain R. Let $[F, G] \in M_d(K)$ be a model of a rational morphism $\phi \in \mathrm{Rat}_d(K)$, and hence also a model of the isomorphism class $[\phi] \in \mathcal{M}_d(K)$. We say that $[F, G]$ is a model *over* R if $F, G \in R[X, Y]$. By clearing denominators, one can always obtain a model over R from a model over K. Note that if $[F, G]$ is a model over R then $[F, G] \in \mathbb{A}^{2d+2}(R)$, but that $[F, G]$ is an R-integral point on M_d only if $\mathrm{Res}_d(F, G)$ is a unit in R.

2.1. *Minimal models*

DEFINITION 2.4. Let R be an integral domain with field of fractions K. Let $\phi \in \mathrm{Rat}_d(K)$. We define the *resultant* of ϕ to be the R-ideal generated by the resultants of the models of ϕ over R, that is,

$$\mathrm{Res}_R(\phi) = (\mathrm{Res}_d(F, G) : [F, G] \in M_d(K) \text{ and a model of } \phi \text{ over } R)R.$$

Similarly, we define the *resultant* of $[\phi] \in \mathcal{M}_d(K)$ to be the R-ideal generated by the resultants of its models over R, that is,

$$\mathrm{Res}_R([\phi]) = (\mathrm{Res}_d(F, G) : [F, G] \in M_d(K) \text{ and a model of } [\phi] \text{ over } R)R.$$

REMARK 2.5. We do not concern ourselves with the resultants of classes in $\mathcal{M}_d(K)$ that do not admit models over K.

DEFINITION 2.6. We say that $[F, G] \in M_d(K) \cap \mathbb{A}^{2d+2}(R)$ is an *R-minimal* model if $[F, G]$ is a model of $[\phi]$ with a resultant that generates the ideal $\mathrm{Res}_R([\phi])$, that is,

$$\mathrm{Res}_R([\phi]) = \mathrm{Res}_d(F, G)R.$$

DEFINITION 2.7. We write $\mathrm{Aff}_2 \subset \mathrm{GL}_2$ for the algebraic subgroup of matrices that induce automorphisms of $\mathbb{P}^1$ that leave $\infty = (1 : 0)$ invariant, that is,

$$\mathrm{Aff}_2(R) = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \in \mathrm{GL}_2(R) \right\}.$$

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

The name is motivated by the fact that a matrix in Aff_2 induces an affine transformation $z \mapsto (1/\delta)(\alpha z + \beta)$. We define $\mathcal{M}_{d,1} = M_d/(\mathbb{G}_m \times \mathrm{Aff}_2)$. For a rational map $\phi \in \mathrm{Rat}_d(K)$ we write $[\phi]_1 \in \mathcal{M}_{d,1}(K)$. We say that $[F, G] \in M_d(K)$ is a *model* for $[\phi]_1$ if $[F/G]_1 = [\phi]_1$ (that is, if there is an affine transformation that conjugates one into the other). We define

$$\mathrm{Res}_R([\phi]_1) = (\mathrm{Res}_d(F, G) : [F, G] \in M_d(K) \text{ and a model of } [\phi]_1 \text{ over } R)R.$$

Definition 2.8. We say that $[F, G] \in M_d(K) \cap \mathbb{A}^{2d+2}(R)$ is an *R-affine minimal* model if $[F, G]$ is a model of $[\phi]_1$ with a resultant that generates $\mathrm{Res}_R([\phi]_1)$, that is,

$$\mathrm{Res}_R([\phi]_1) = \mathrm{Res}_d(F, G)R.$$

Proposition 2.9. *Let R be a principal ideal domain with field of fractions K. Then*

$$\mathrm{GL}_2(K) = \mathrm{Aff}_2(K)\,\mathrm{SL}_2(R) \quad \textit{and} \quad \mathrm{GL}_2(K) = \mathrm{SL}_2(R)\,\mathrm{Aff}_2(K).$$

Proof. Let $B = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. In order to establish the first claim we exhibit a matrix $C \in \mathrm{SL}_2(R)$ such that $BC \in \mathrm{Aff}_2(K)$. If $\gamma = 0$ we can take C to be the identity matrix. Otherwise, there are coprimes $a, c \in R$ such that $\delta/\gamma = -a/c$. It follows that $a\gamma + c\delta = 0$ and that there are $b, d \in R$ such that $ad - bc = 1$. We can take $C = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R)$. The second claim follows by an analogous argument. □

Proposition 2.10. *Let R be a Dedekind domain with field of fractions K. Then for any $\phi \in \mathrm{Rat}_d(K)$ we have $\mathrm{Res}_R([\phi]) = \mathrm{Res}_R([\phi]_1)$. In particular, a model $[F, G]$ for ϕ is R-affine minimal if and only if it is R-minimal.*

Proof. First note that Proposition 2.2 establishes that Res_d is invariant under SL_2, so Proposition 2.9 immediately gives the result for principal ideal domains R.

If R is a Dedekind domain, it is straightforward to check that a model is R-(affine) minimal if and only if it is $R_{\mathfrak{p}}$-(affine) minimal for all localizations $R_{\mathfrak{p}}$ at primes $\mathfrak{p}$. Furthermore, for Dedekind domains, the localizations $R_{\mathfrak{p}}$ are principal ideal domains, so locally, minimality and affine minimality coincide. More explicitly, one checks that $\mathrm{Res}_{R_{\mathfrak{p}}}([\phi]) = \mathrm{Res}_R([\phi])R_{\mathfrak{p}}$ and that $\mathrm{Res}_{R_{\mathfrak{p}}}([\phi]_1) = \mathrm{Res}_R([\phi]_1)R_{\mathfrak{p}}$ and that $I, J \subset R$ are equal if and only if for all primes $\mathfrak{p}$ we have $IR_{\mathfrak{p}} = JR_{\mathfrak{p}}$. □

Remark 2.11. Silverman [**10**, Proposition 4.100] shows that if R is a Dedekind domain with a non-trivial class group, then not every class $[\phi]$ admits an R-minimal model. As we will see in Corollary 2.13, if R is a principal ideal domain, then any class admits an R-minimal model. In fact, Proposition 2.9 implies that such a model can be obtained from any given model via an affine transformation.

Note that Proposition 2.10 does *not* imply this in general: if R has a non-trivial ideal class group, then it is possible to have a rational function ϕ such that $[\phi]$ admits an R-minimal model, but $[\phi]_1$ does not admit an R-affine minimal model. See Example 6.4.

2.2. *Minimal models over discrete valuation rings*

We now restrict to the case where R is a discrete valuation ring, with maximal ideal $\mathfrak{p}$, field of fractions K and valuation $v\colon K \to \mathbb{Z} \cup \{\infty\}$. We write

$$v\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \min(v(\alpha), \ldots, v(\delta))$$

as well as

$$v\left(\sum_{i=0}^{d} f_i z^i\right) = \min(f_0, \ldots, f_d) \quad \text{and} \quad v([F, G]) = \min(v(F), v(G)).$$

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

With these definitions it is easy to check that for $[F, G] \in M_d(K)$ and $(\lambda, A) \in (\mathbb{G}_m \times \mathrm{GL}_2)(K)$, there is a bound B such that for any (λ', A') such that $v(\lambda - \lambda') > B$ and $v(A - A') > B$, we have $v(\mathrm{Res}_d(\lambda F_A, \lambda G_A)) = v(\mathrm{Res}_d(\lambda' F_{A'}, \lambda' G_{A'}))$.

PROPOSITION 2.12. *Let R be a discrete valuation ring with field of fractions K and uniformizer π. Let $\phi \in \mathrm{Rat}_d(K)$ be a rational function given by a model $[F, G] \in M_d(K)$. Then there are $e_1, e_2, e_3 \in \mathbb{Z}$ and $\beta \in K$ such that for any $\beta' \in \beta + \pi^{e_3} R$ we can set*

$$(\lambda, A) = \left(\pi^{e_1}, \begin{pmatrix} \pi^{e_2} & \beta' \\ 0 & 1 \end{pmatrix}\right) \in (\mathbb{G}_m \times \mathrm{GL}_2)(K)$$

and have that $[\lambda F_A, \lambda G_A]$ is an R-minimal model for ϕ.

Proof. Since R is a discrete valuation ring, we know that $\inf\{v(a) : a \in \mathrm{Res}_R([\phi])\}$ is attained in the ideal and the triangle inequality shows it must be attained by the resultant of a model over R. This shows that there is a minimal model. In fact, we can use the same reasoning to assert the existence of an affine minimal model for $[\phi]_1$ and Proposition 2.10 guarantees that this model is also minimal. This shows that we can attain a minimal model by a transformation $(\lambda, A) \in (\mathbb{G}_m \times \mathrm{Aff}_2)(K)$. It remains to prove that we can restrict to a transformation of the shape described.

First note that $(\lambda\delta^{d+1}, \left(\begin{smallmatrix} \alpha/\delta & \beta/\delta \\ 0 & 1 \end{smallmatrix}\right))$ and $(\lambda, \left(\begin{smallmatrix} \alpha & \beta \\ 0 & \delta \end{smallmatrix}\right))$ have the same effect, so we can assume that $\delta = 1$. Next note that transforming by $(\mathbb{G}_m \times \mathrm{GL}_2)(R)$ does not change minimality, so we can assume that λ and α are powers of a given uniformizer.

It remains to show that $v(\mathrm{Res}_d(\lambda F_A, \lambda G_A))$ remains constant under small perturbations of β. Since the resultant is polynomial in β, its valuation is locally constant away from zero and the desired result follows. □

COROLLARY 2.13. *Let R be a principal ideal domain with field of fractions K. Then for any $\phi \in \mathrm{Rat}_d(K)$, the class $[\phi] \in \mathcal{M}_d(K)$ has an R-minimal model $[F, G]$.*

Proof. First let $[F, G]$ be any model of ϕ over R. Since R is a Dedekind domain we have the factorisation $\mathrm{Res}_d(F, G)R = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n}$ into prime ideals. It follows that $[F, R]$ is $R_{\mathfrak{q}}$-minimal for all primes $\mathfrak{q} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$.

We modify $[F, G]$ iteratively to ensure minimality for each index i in the following way. The assumption that R is a principal ideal domain ensures that $\mathfrak{p}_i = \pi_i R$ for some $\pi_i \in R$. We apply Proposition 2.12 to find a transformation (λ, A) such that $[F, G]^{(\lambda, A)}$ is $R_{\mathfrak{p}_i}$-minimal. Since R is dense in the localization $R_{\mathfrak{p}_i}$, we can choose $\beta' \in \pi_i^{e_4} R$ for some $e_4 \in \mathbb{Z}$. This means that $(\lambda, A) \in (\mathbb{G}_m \times \mathrm{GL}_2)(R_{\mathfrak{q}})$ for any prime $\mathfrak{q} \neq \mathfrak{p}_i$ and hence that $[F, G]^{(\lambda, A)}$ is minimal at $\mathfrak{p}_i$ as well as at all primes where $[F, G]$ is already minimal. By iteratively applying such a transformation for each $i = 1, \dots, n$, we obtain a model that is minimal locally at all primes and hence is R-minimal. □

3. *Determining local minimal models*

Let R be a discrete valuation ring with maximal ideal $\mathfrak{p}$, field of fractions K, uniformizer π and valuation $v\colon K \to \mathbb{Z} \cup \{\infty\}$. We write $k = R/\mathfrak{p}$ for the residue field.

Let $\phi \in \mathrm{Rat}_d(K)$ be a rational function given by a model $[F, G]$ over R. In this section we develop a relatively efficient algorithm to compute a transformation

$$(\lambda, A) = \left(\pi^{e_1}, \begin{pmatrix} \pi^{e_2} & \beta \\ 0 & 1 \end{pmatrix}\right) \in (\mathbb{G}_m \times \mathrm{GL}_2)(K) \tag{1}$$

of the form described in Proposition 2.12, such that $[\lambda F_A, \lambda G_A]$ is an R-minimal model of $[\phi] \in \mathcal{M}_d(K)$. We do this by formulating a procedure that finds $e_1, e_2 \in \mathbb{Z}$ and $\beta \in K$, or shows

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

they do not exist, such that $\lambda F_A, \lambda G_A \in R[X,Y]$ and $v(\mathrm{Res}_d(\lambda F_A, \lambda G_A)) < v(\mathrm{Res}_d(F,G))$. First we observe a case where it is particularly easy to recognise that a model is minimal.

LEMMA 3.1. *If d is even and $v(\mathrm{Res}_d(F,G)) < d$ or if d is odd and $v(\mathrm{Res}_d(F,G)) < 2d$ then $[F,G]$ is an R-minimal model for $[\phi]$.*

Proof. Proposition 2.2 shows that transformations can only change the resultant by a factor λ^k, where k is a multiple of $\gcd(2d, d^2+d)$. Since a minimal model has $\mathrm{Res}_d(F,G) \in R$, it must have non-negative valuation. Therefore, if the valuation is already small enough, a transformation cannot reduce it and keep the model over R. □

If we do find such values, we repeat the procedure with the transformed model; otherwise we have shown that the original model is minimal. In light of Proposition 2.2, we need

$$2de_1 + (d^2+d)e_2 < 0.$$

Without loss of generality we can take

$$e_1 = -\min(v(F_A), v(G_A)). \tag{2}$$

We write

$$F_A = \sum f_i' X^i Y^{d-i} \quad \text{and} \quad G_A = \sum g_i' X^i Y^{d-i}.$$

It follows that

$$\begin{aligned} f_j' &= f_j'(e_2,\beta) = \pi^{je_2} \sum_{i=j}^{d} \binom{i}{j} (f_i \beta^{i-j} - g_i \beta^{i-j+1}), \\ g_j' &= g_j'(e_2,\beta) = \pi^{(j+1)e_2} \sum_{i=j}^{d} \binom{i}{j} g_i \beta^{i-j}. \end{aligned} \tag{3}$$

Finding a valuation-reducing transformation amounts to finding $e_2 \in \mathbb{Z}$ and $\beta \in K$ such that

$$v(f_i') > \frac{d+1}{2} e_2 \quad \text{and} \quad v(g_i') > \frac{d+1}{2} e_2 \quad \text{for } i = 0, \dots, d. \tag{4}$$

We proceed by proving lower and upper bounds for e_2 given F, G and then lower bounds on $v(\beta)$ given e_2, F, G.

LEMMA 3.2. *Let $f, g \in R[z]$ be of degrees at most d. Then for any $\beta \in K$ we have*

$$\min(v(f(\beta)), v(g(\beta))) \leqslant v(\mathrm{res}(f,g)).$$

Proof. We first consider the case $v(\beta) \leqslant 0$. The usual properties for resultants (see for example [**10**, Proposition 2.13c]; the proof there is stated for $R = \mathbb{Z}$, but is valid for arbitrary commutative rings) yield polynomials $U(z), V(z) \in R[z]$ of degree at most $d-1$ such that

$$Uf + Vg = z^{2d-1} \,\mathrm{res}(f,g).$$

In particular, we find that

$$v(\mathrm{res}(f,g)) + (2d-1)v(\beta) \geqslant \min(v(U(\beta)) + v(f(\beta)), v(V(\beta)) + v(g(\beta))).$$

Since we have $v(U(\beta)), v(V(\beta)) \geqslant (d-1)v(\beta)$, this yields

$$\min(v(f(\beta)), v(g(\beta))) \leqslant v(\mathrm{res}(f,g)) + dv(\beta) \leqslant v(\mathrm{res}(f,g)).$$

For the case $v(\beta) \geqslant 0$ we use (see again for example [**10**, Proposition 2.13c]) that there are polynomials $U, V \in R[z]$ of degree at most $d-1$ such that

$$Uf + Vg = \mathrm{res}(f,g).$$

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

We have

$$\min(v(U(\beta)) + v(f(\beta)), v(V(\beta)) + v(g(\beta))) \leqslant v(\operatorname{res}(f, g)),$$

and since $v(U(\beta)), v(V(\beta)) \geqslant 0$, the statement follows. □

LEMMA 3.3. *Let $[F, G] \in M_d(K)$ be a model over R. Let $f(z) = F(z, 1)$ and $g(z) = G(z, 1)$. Let d_G be the degree of g. Suppose $e_2 \in \mathbb{Z}$ and $\beta \in K$ provide a solution to (4). Then we have*

$$e_2 > \begin{cases} -\dfrac{2}{2d_G - d + 1} v(g_{d_G}) & \text{if } d_G > \dfrac{1}{2}(d+1), \\ -\dfrac{2}{d-1} v(f_d) & \text{if } d_G < d. \end{cases}$$

Furthermore, we have

$$e_2 < \frac{2}{d-1} v(\operatorname{res}(f - zg, g)) = \begin{cases} \dfrac{2}{d-1} v(\operatorname{res}(f, g)) & \text{if } d_G < d, \\ \dfrac{2}{d-1} (v(\operatorname{res}(f, g)) + v(g_d)) & \text{if } d_G = d. \end{cases}$$

Proof. We use the notation f_i, g_i, f_i', g_i' as defined in (3) and earlier.

We first prove the lower bounds. If $d_G > \frac{1}{2}(d+1)$, we consider $g'_{d_G}(e_2, \beta) = \pi^{(d_G+1)e_2} g_{d_G}$. Its valuation combined with (4) gives the bound stated. If $d_G < d$ we have that $f_d' = \pi^{de_2} f_d$ and that $f_0 \neq 0$. Its valuation combined with (4) yields the bound stated.

For the upper bound, we consider (4) for f_0' and g_0'. They yield

$$v(f(\beta) - \beta g(\beta)) > \frac{d+1}{2} e_2 \quad \text{and} \quad v(g(\beta)) > \frac{d-1}{2} e_2.$$

From Lemma 3.2 we obtain an upper bound on the minimum of the left hand sides of the inequalities, which leads immediately to the upper bound stated in the lemma. It is a straightforward exercise in Sylvester matrices to see that $\operatorname{res}(f - zg, g) = \operatorname{res}(f, g)$ if $\deg(g) < \deg(f)$ and that $\operatorname{res}(f - zg, g) = \pm g_d \operatorname{res}(f, g)$ if $\deg(f) \leqslant \deg(g) = d$. In either case this provides a finite upper bound, because f, g are coprime. □

REMARK 3.4. Note that the argument that provides the lower bound for e_2 if $d_G > \frac{1}{2}(d+1)$ gives the upper bound $e_2 < (2/(d - 1 - 2d_G))v(g_{d_G})$ if $d_G < \frac{1}{2}(d+1)$. In particular, if $f, g \in R[z]$ are monic and $\deg(g) \leqslant \frac{1}{2}\deg(f)$ then we have $v(g_{d_G}) = v(f_d) = 0$ and we see that a solution to (4) would require both $e_2 > 0$ and $e_2 < 0$. It follows that the corresponding model $[F, G]$ is already a minimal model for $[f/g]$.

REMARK 3.5. For obtaining the upper bound on e_2 we considered the inequalities in (4) arising from f_0' and g_0', because those are guaranteed to provide a finite upper bound. However, (4) gives rise to multiple inequalities

$$v\left(\sum_{i=j}^{d} \binom{i}{j} (f_i \beta^{i-j} - g_i \beta^{i-j+1})\right) > \frac{d+1-2j}{2} e_2$$

$$v\left(\sum_{i=j}^{d} \binom{i}{j} g_i \beta^{i-j}\right) > \frac{d-1-2j}{2} e_2,$$

so applying Lemma 3.2 on any pair of them (with $2j < d+1$, respectively $2j < d-1$) potentially yields a sharper upper bound on e_2.

With Lemma 3.3 we have restricted the possible e_2 to a finite set. For each possible e_2, we are left with determining a value $\beta \in K$ that satisfies (4). Note that f_j', g_j' are polynomial in β, so after clearing denominators, we obtain a problem of the following form.

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

PROBLEM 3.6. Given $\{(h_1, c_1), \dots, (h_r, c_r)\}$ with

$$h_1, \dots, h_r \in R[z] \quad \text{and} \quad c_1, \dots, c_r \in \mathbb{R},$$

determine $\beta \in K$ such that

$$v(h_i(\beta)) > c_i \quad \text{for } i = 1, \dots, r,$$

or prove that no such β exists.

LEMMA 3.7. *Let $f = \sum_{i=0}^{n} f_i z^i \in R[z]$ be a polynomial of degree n. Let*

$$B(f, c) = \min\left(\frac{c - v(f_n)}{n}, \min\left\{\frac{v(f_i) - v(f_n)}{n - i} : i = 0, \dots, n-1\right\}\right),$$

then for any $\beta \in K$ such that $v(f(\beta)) > c$ we have $v(\beta) \geqslant B(f, c)$.

Proof. We observe that if $v(f(\beta)) > c$ then we must have $v(f_n\beta^n) > c$ or $v(f_n\beta^n) \geqslant v(f_i\beta^i)$ for some $i = 0, \dots, n-1$. Solving for $v(\beta)$ provides the bound stated. □

Using Lemma 3.7 we see that if β is a solution for Problem 3.6 and $B = \max\{B(h_i, c_i) : i = 1, \dots, r\}$, then $\beta = \pi^{-B}\beta'$ for some $\beta' \in R$, which itself is a solution to the problem

$$V = \begin{cases} \{(\pi^{\deg(h_i)B} h_i(\pi^{-B} z), c_i + B) : i = 1, \dots, r\} & \text{if } B > 0, \\ \{(h_i(\pi^{-B} z), c_i) : i = 1, \dots, r\} & \text{if } B \leqslant 0. \end{cases} \tag{5}$$

Because we have now reduced the problem to find a solution $\beta \in R$, we can use reduction. For $\beta \in R$ we write $\overline{\beta}$ for its residue class in k and for $h \in R[z]$ we write $\overline{h} \in k[z]$ for its coefficient-wise reduction. We obtain the following algorithm.

ALGORITHM 3.8. InequalitySolutions(V)

Input: $V = \{(h_1, c_1), \dots, (h_r, c_r)\} \subset R[z] \times \mathbb{R}$.

Output: An element $\beta \in R$ such that $v(h_i(\beta)) > c_i$ for $i = 1, \dots, r$ or none if no such solution exists.

(1) $V' := \{(\pi^{-v(h_i)} h_i, c_i - v(h_i))$ for those $i = 1, \dots, r$ for which $h_i \neq 0$ and $c_i \geqslant v(h_i)\}$.
(2) `if` $V' = \emptyset$: `return` 0.
(3) $\overline{g} := \gcd(\overline{h'}_i : (h'_i, c'_i) \in V')$.
(4) Let $W \subset R$ be a set of representatives of the roots of $\overline{g}(z)$ in k.
(5) `for` $\beta_0 \in W$:
(6) $\quad V'' := \{(\pi^{-1} h'_i(\beta_0 + \pi z), c'_i - 1) : (h'_i, c'_i) \in V'\}$;
(7) $\quad \beta_1 :=$ InequalitySolutions(V'');
(8) $\quad$ `if` $\beta_1 \neq$ none: `return` $\beta_0 + \pi\beta_1$.
(9) `if` $W = \emptyset$ or $\beta_1 =$ none for all $\beta_0 \in W$: `return` none.

Since the algorithm is recursive, we need to argue it will finish in finite time. The valuation bounds in V'' are decreased by at least 1 from the ones that occur in V. Furthermore, note that any conditions with a negative valuation bound get removed in step (1) and that the algorithm terminates if $V' = \emptyset$. This means that $\max c_i$ is a bound on the recursion depth of the algorithm.

Furthermore, note that the polynomials in V' all have non-zero reduction, so $\overline{g}$ computed in (3) is well defined. That means that W in step (4) is a finite set, so the loop in (5) is finite. This establishes that the algorithm finishes in finite time.

For correctness, first note that in (1) we ensure that the polynomials in V' have integral coefficients and that at least one of them is a unit in R and that all vacuous conditions are

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

removed from V'. If no conditions remain, then any $\beta \in R$ is a valid solution, so if a value is returned in step (2), it is correct.

Furthermore, it is clear that any solution would have to reduce to a root of h_i' in k, for all i. This means that $\beta = \beta_0 + \pi\beta_1$, where β_0 represents such a root and $\beta_1 \in R$, where β_1 satisfies the conditions represented by V''. If we find such a β_1 in step (7), we return the resulting solution in step (8). On the other hand, if we cannot find a suitable β_1 for any of the β_0, we have shown that no solutions exist. Note that the set W can be empty, in which case there are no β_0 to try and none is returned immediately in step (9).

An algorithm to compute an R-minimal model for $[\phi] \in \mathcal{M}_d(K)$ given by a model $[f, g] \in M_d(K)$ is now a matter of bookkeeping.

ALGORITHM 3.9. LocalMinimalModel$(f_{\text{in}}, g_{\text{in}})$

Input: $f_{\text{in}}, g_{\text{in}} \in R[z]$ with $\max(\deg(f_{\text{in}}), \deg(g_{\text{in}})) = d$ and $\phi = f_{\text{in}}/g_{\text{in}} \in \text{Rat}_d(K)$.

Output: $e_{1,\text{tot}}, e_{2,\text{tot}} \in \mathbb{Z}$ and $\beta_{\text{tot}} \in K$ describing a transformation (λ, A) as in equations (1) and (2) and $f, g \in R[z]$ such that $[f, g] = [f_{\text{in}}, g_{\text{in}}]^{(\lambda,A)}$ is a minimal model for $[\phi] \in \mathcal{M}_d(K)$.
If $[f_{\text{in}}, g_{\text{in}}]$ is already minimal then $[f, g] = [f_{\text{in}}, g_{\text{in}}]$ and $(e_1, e_2, \beta) = (0, 0, 0)$.

(1) $e_{1,\text{tot}}, e_{2,\text{tot}}, \beta_{\text{tot}} := 0, 0, 0$ and $f, g := f_{\text{in}}, g_{\text{in}}$.
(2) $e_1 := -\min(v(f), v(g))$; $e_{1,\text{tot}} := e_{1,\text{tot}} + e_1$; $f := \pi^{e_1} f$; $g := \pi^{e_1} g$.
(3) `for` e_2 in the range given by Lemma 3.3:
(4) $\quad V' := \{(f_i', (d+1)/2)\} \cup \{(g_i', (d+1)/2)\}$ as in equation (4);
(5) $\quad$ let V be as in equation (5), where $B := \max\{B(h_i, c_i) : (h_i, c_i) \in V'\}$;
(6) $\quad \beta' :=$ InequalitySolutions(V);
(7) $\quad$ `if` $\beta' \neq$ none:
(8) $\quad\quad \beta := \pi^{-B}\beta'$; $f := f(\pi^{e_2} z + \beta) - \beta g(\pi^{e_2} z + \beta)$; $g := \pi^{e_2} g(\pi^{e_2} z + \beta)$;
(9) $\quad\quad \beta_{\text{tot}} := \beta_{\text{tot}} + \pi^{e_{2,\text{tot}}}\beta$; $e_{2,\text{tot}} := e_{2,\text{tot}} + e_2$;
(10) $\quad\quad$ `goto` step (2).
(11) `return` $(e_{1,\text{tot}}, e_{2,\text{tot}}, \beta_{\text{tot}})$, (f, g).

4. *Determining minimal models over principal ideal domains*

With Algorithm 3.9 in place, we can turn the procedure sketched in the proof of Corollary 2.13 into an algorithm as well. In this section, let R be a principal ideal domain with field of fractions K. For a prime ideal $\mathfrak{p}$ we write $R_{\mathfrak{p}}$ for the localization of R at $\mathfrak{p}$ (we do not need a completion for our purposes). We write $k_{\mathfrak{p}}$ for its residue class field $R/\mathfrak{p}$. As a uniformizer in $R_{\mathfrak{p}}$ we choose a generator $\pi \in R$ of $\mathfrak{p} = \pi R$. Furthermore, when we need representatives of $k_{\mathfrak{p}}$ in $R_{\mathfrak{p}}$, we assume that we take elements from R.

ALGORITHM 4.1. MinimalModel$(f_{\text{in}}, g_{\text{in}})$

Input: $f_{\text{in}}, g_{\text{in}} \in R[z]$ with $\max(\deg(f_{\text{in}}), \deg(g_{\text{in}})) = d$ and $\phi = f_{\text{in}}/g_{\text{in}} \in \text{Rat}_d(K)$.

Output: $\lambda_{\text{tot}}, \alpha_{\text{tot}}, \beta_{\text{tot}} \in K$ and $f, g \in R[z]$ with

$$(\lambda, A) = \left(\lambda, \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}\right)$$

such that $[f, g] = [f_{\text{in}}, g_{\text{in}}]^{(\lambda,A)}$ is an R-minimal model of $[\phi] \in \mathcal{M}_d(K)$. If $[f_{\text{in}}, g_{\text{in}}]$ is already minimal then $[f, g] = [f_{\text{in}}, g_{\text{in}}]$ and $(\lambda_{\text{tot}}, \alpha_{\text{tot}}, \beta_{\text{tot}}) = (1, 1, 0)$.

(1) $f, g := f_{\text{in}}, g_{\text{in}}$.
(2) Compute the prime factorization $\mathfrak{p}_1^{\epsilon_1}, \ldots, \mathfrak{p}_r^{\epsilon_r} = (\text{Res}_d(f, g))R$.

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

(3) `for` $\mathfrak{p} \in \{\mathfrak{p}_i : i = 1, \dots, r \text{ and } \epsilon_i \geqslant d \gcd(2, d+1)\}$:
(4) determine $\pi \in R$ such that $\mathfrak{p} = \pi R$ and choose representatives of $k_{\mathfrak{p}}$ in R;
(5) $(e_1, e_2, \beta), (f, g) := \mathsf{LocalMinimalModel}(f, g)$ with respect to $R_{\mathfrak{p}}$;
(6) $\lambda_{\mathrm{tot}} = \lambda_{\mathrm{tot}} \pi^{e_1}$; $\beta_{\mathrm{tot}} := \beta_{\mathrm{tot}} + \alpha_{\mathrm{tot}} \beta$; $\alpha_{\mathrm{tot}} = \alpha_{\mathrm{tot}} \pi^{e_2}$;
(7) `return` $(\lambda_{\mathrm{tot}}, \alpha_{\mathrm{tot}}, \beta_{\mathrm{tot}}), (f, g)$.

Note that in step (3) we use Lemma 3.1 to reduce the set of primes to consider. Furthermore, in step (4) we take care to choose π and representatives of $k_{\mathfrak{p}}$ such that the transformation computed to ensure $R_{\mathfrak{p}}$-minimality in step (5) does not affect the minimality at any other primes. That means we can simply compose the transformations to obtain one that transforms the given model into an R-minimal one.

5. *A counterexample to some dynamical analogue of Szpiro's conjecture*

In an attempt to formulate a dynamical analogue of Szpiro's conjecture, Silverman suggests the following definition of *conductor* [**10**, Section 4.11].

Definition 5.1. Let R be a Dedekind domain with field of fractions K. For $\phi \in \mathrm{Rat}_d(K)$ we define

$$\mathrm{Cond}_R([\phi]) = \sqrt{\mathrm{Res}_R([\phi])},$$

where $\sqrt{I}$ denotes the *radical ideal* of I.

One analogue of Szpiro's conjecture [**10**, Conjecture 4.97] would predict the existence of a bound n and an ideal $J \subset R$ such that

$$J \,\mathrm{Cond}_R([\phi])^n \subset \mathrm{Res}_R([\phi]) \quad \text{for all } \phi \in \mathrm{Rat}_d(K).$$

If $d \geqslant 3$ and $h(x) \in R[x]$ is a monic polynomial of degree at most $\frac{1}{2}(d-2)$ and $\pi \in R$ such that $J \notin \pi R$, we see that the rational function

$$\phi(x) = \frac{x^d + \pi^{n+1}}{h(x)x}$$

is a counterexample, since the given model is locally minimal at all places of R by Remark 3.4 and therefore globally minimal, but $\mathrm{Res}_d(x^d + \pi^{n+1}, h(x)x)$ is divisible by π^{n+1}. See also [**12**] for counterexamples with $d = 2$ and an in-depth treatment of possible alternative formulations of the concept of *conductor*. The same paper also discusses some approaches to proving that certain models are minimal. In their Section 3 they consider an approach similar to the valuation-based part of Section 3. Indeed, without a systematic method for determining possible values for β (the utility of Algorithm 3.8), they conclude that their methods are likely insufficient in general. However, in their Section 5 they present some methods based on explicit models for the moduli space $\mathcal{M}_d$ and its higher level covers. When these work, they likely provide an elegant alternative to Algorithm 3.9, although for large d such models might be hard to compute.

6. *The structure of the set of minimal models of a map*

Let R be a principal ideal domain with field of fractions K and let $\phi \in \mathrm{Rat}_d(K)$. Proposition 2.13 guarantees the existence of an R-minimal model $[F, G] \in M_d(K)$ for $[\phi]$ and Algorithm 4.1 provides a procedure to compute one, given a sufficiently explicit description of ϕ. In this section we consider the set of all such models

$$\mathrm{Min}_R([\phi]) = \{[F, G] : F, G \in R[X, Y] \text{ and } [F, G] \text{ is an } R\text{-minimal model for } [\phi]\}.$$

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

It is immediate that $\mathrm{Min}_R([\phi])$ is stable under the action of $(\mathbb{G}_m \times \mathrm{GL}_2)(R)$. It can be bigger than a single orbit, as the following example shows.

EXAMPLE 6.1. Let n be a positive integer and suppose that $c \in \mathbb{Z}$ is not $0, \pm 1$. Consider the $\mathbb{Z}$-model $[F, G] = [z^{2n+1} - c^{n+1}, z^n]$. By Remark 3.4, the model is $\mathbb{Z}$-minimal. Conjugation by the transformation

$$(\lambda, A) = \left(c^{-n-1}, \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}\right) \in (\mathbb{G}_m \times \mathrm{GL}_2)(\mathbb{Q})$$

yields the model $[F, G]^{(\lambda, A)} = [c^n z^{2n+1} - 1, z^n]$, which has the same resultant and hence is also minimal. It is straightforward to check that these two models are not in the same $(\mathbb{G}_m \times \mathrm{GL}_2)(\mathbb{Z})$-orbit, for instance by verifying that the set of fixed points of ϕ has a trivial stabilizer in $\mathrm{PGL}_2(\mathbb{Q})$ and noting that the given transformation does *not* map to $\mathrm{PGL}_2(\mathbb{Z})$.

Note that the rational function in Example 6.1 is of degree $2n + 1$, which is odd.

QUESTION 6.2. Does there exist a rational function $\phi \in \mathrm{Rat}_d(\mathbb{Q})$ with d even, such that $\mathrm{Min}_R([\phi])$ consists of a single $(\mathbb{G}_m \times \mathrm{GL}_2)(\mathbb{Z})$-orbit?

If $[\phi]$ admits a minimal model $[F, G]$, we can consider the set of transformations

$$\mathrm{MinTran}_R([F, G]) = \{(\lambda, A) \in (\mathbb{G}_m \times \mathrm{GL}_2)(K) : [F, G]^{(\lambda, A)} \in \mathrm{Min}_R([\phi])\}.$$

As remarked, this set can be decomposed as a union of left cosets of $(\mathbb{G}_m \times \mathrm{GL}_2)(R)$. We make some basic observations on the number of cosets.

PROPOSITION 6.3. *Let R be a discrete valuation ring with field of fractions K and suppose that $[F, G] \in M_d(K)$ is an R-model with $\mathrm{Res}_d(F, G) \in R^\times$. Then*

$$\mathrm{MinTran}_R([F, G]) = (\mathbb{G}_m \times \mathrm{GL}_2)(R).$$

Proof. Let us assume that $[F, G]$ is a model as given and that $(\lambda, A) \in \mathrm{MinTran}_R([F, G])$. We will show that $\lambda \in R^\times$ and $A \in \mathrm{GL}_2(R)$.

First we show that we can assume that the leading coefficients f_d and g_d are units in $R^\times$. We consider the reduction $\overline{F}, \overline{G} \in k[X, Y]$. Our resultant condition implies that $[\overline{F}, \overline{G}] \in M_d(k)$. We write $\overline{\phi}$ for the corresponding rational function. We have $f_d, g_d \in R^\times$ if and only if $\overline{\phi}(\infty) \notin \{0, \infty\}$. Note that $\overline{\phi}$ has at most $d + 1$ fixed points, so if $\#k > d$ then there are points in $P, Q \in \mathbb{P}^1(k)$ such that P is not a fixed point and $\overline{\phi}(P) \neq Q$. We can find a transformation $\overline{T} \in \mathrm{GL}_2(k)$ such that $\overline{T}(\infty) = P$ and $\overline{T}(0) = Q$. We lift $\overline{T}$ to $T \in \mathrm{GL}_2(R)$. It follows that $T^{-1}\phi T$ has the desired property. Since $A \in \mathrm{GL}_2(R)$ if and only if $TA \in \mathrm{GL}_2(R)$, we can restrict to f_d, g_d being units, provided $\#k > d$. However, writing R^{unr} for an unramified extension of R, we have that $\mathrm{GL}_2(R) = \mathrm{GL}_2(R^{\mathrm{unr}}) \cap \mathrm{GL}_2(K)$, so it is sufficient to prove the statement for a sufficiently large unramified extension of R. This means we can assume that $\#k$ is sufficiently large and hence that $f_d, g_d \in R^\times$.

We can adapt the results in Section 3 to determine minimality-preserving transformations by changing the inequalities in (4) to equalities. The argument for Proposition 2.12 allows us to assume that the transformation is of the form

$$(\lambda, A) = \left(\pi^{e_1}, \begin{pmatrix} \pi^{e_2} & \beta \\ 0 & 1 \end{pmatrix}\right) \in (\mathbb{G}_m \times \mathrm{GL}_2)(K).$$

The claim follows if we can show that $e_2 = 0$ and $\beta \in R$, since then obviously $e_1 = 0$. Indeed from Lemma 3.3 we obtain that $e_2 = 0$ and from Lemma 3.7 we find that $\beta \in R$. This proves the proposition. □

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

EXAMPLE 6.4. Let $\alpha = \sqrt{-5}$, let $R = \mathbb{Z}[\alpha]$ and let $K = \mathbb{Q}(\alpha)$. We consider

$$\psi(z) = z^2 \in K(z).$$

Since $\mathrm{Res}_2(z^2, 1) = 1$, we see that ψ is minimal and Proposition 6.3 yields that

$$\mathrm{MinTran}_R([z^2, 1]) \subset \bigcap_{\text{all primes } \mathfrak{p}} (\mathbb{G}_m \times \mathrm{GL}_2)(R_{\mathfrak{p}}) = (\mathbb{G}_m \times \mathrm{GL}_2)(R). \tag{6}$$

We consider

$$M = \begin{pmatrix} 2 & 1 \\ 1+\alpha & 1 \end{pmatrix} \quad \text{and} \quad \phi(z) = M \circ \psi \circ M^{-1} = \frac{2z^2 + (2\alpha - 2)z - \alpha - 1}{3z^2 + (2\alpha - 4)z - \alpha}.$$

We claim that $[\phi]_1$ does not have an R-affine minimal model, whereas of course $[\phi]$ does have the R-minimal model $[z^2, 1]$. This shows that a non-trivial class group for R can prevent us from obtaining affine minimal models even in the presence of a minimal model.

Suppose that $A = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{Aff}_2(K)$ such that $A \circ \phi \circ A^{-1}$ is represented by an R-minimal model. Then $A^{-1}M^{-1} \circ \psi \circ MA$ is represented by an R-minimal model, so (6) yields

$$MA = \begin{pmatrix} 2 & 1 \\ 1+\alpha & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 2a & 2b+d \\ (1+\alpha)a & (1+\alpha)b + d \end{pmatrix} \in \mathrm{GL}_2(R).$$

Since the ideal $\mathfrak{p}_2 = 2R + (1+\alpha)R$ is of norm 2 and non-principal, we see that $2a, (1+\alpha)a \in R$ implies that $a \in R$. But then $\det(MA) \in \mathfrak{p}_2$, which contradicts that $MA \in \mathrm{GL}_2(R)$.

PROPOSITION 6.5. *Let K be a global field and suppose that its ring of integers R is a principal ideal domain. Let $[F, G] \in M_d(K)$ be an R-minimal model for $[\phi] \in \mathcal{M}_d(K)$. Then*

$$\mathrm{MinTran}_R([F, G])$$

is a finite union of left-cosets of $(\mathbb{G}_m \times \mathrm{GL}_2)(R)$.

Proof. We have to establish that a finite union suffices. Let S be the finite set of places where $\mathrm{Res}_d(F, G)$ is not a unit. We write R_S for the ring of S-integers. Since K is a *global* field, we have that all residue fields are finite and hence that $R_S^\times$ is finitely generated. Proposition 2.9 shows that each coset has a representative in $(\mathbb{G}_m \times \mathrm{Aff}_2)(K)$ and Proposition 6.3 shows that we can take the representatives of the form

$$\left(\lambda, \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}\right),$$

where $\lambda = 1/\alpha$ and α is an S-unit. Note that Lemma 3.3 provides us with valuation bounds on α and that the coset represented only depends on the value of α in $R_S^\times / R^\times$. Therefore, we only have to consider finitely many representatives for α.

Similarly, for β we have that Lemma 3.7 provides lower bounds on the valuations of β and that the coset represented only depends on the value of β in $K/\alpha^{-1}R$, which only leaves us with finitely many candidates. □

REMARK 6.6. Note that $R_S^\times / R$ is also finitely generated if the residue fields of R are not finite. We only use that K is global for establishing that finitely many representatives for β suffice. However, note that the lower bounds provided by Lemma 3.7 only give *necessary* conditions. It may well be that the full problem (5) is so restrictive that any solution would lead to one of finitely many cosets regardless of the finiteness of the residue field. One may ask the following concrete question.

QUESTION 6.7. Let k be a field, let $R = k[[t]]$ be the ring of formal power series and let $K = k(\!(t)\!)$ be the corresponding field of Laurent series. Does there exist a minimal model $[F, G] \in M_d(K)$ such that $\mathrm{MinTran}_R([F, G])$ is not a finite union of left cosets of $(\mathbb{G}_m \times \mathrm{GL}_2)(R)$?

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

7. *Orbits of rational functions containing many integer points*

In this section we restrict to $R = \mathbb{Z}$ and $K = \mathbb{Q}$. In order to obtain a concept of integrality on $\mathbb{P}^1(\mathbb{Q})$, we fix a point at infinity and consider $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$. Let $\phi \in \mathbb{Q}(z)$ be a rational map on $\mathbb{P}^1(\mathbb{Q})$. For a point $\alpha \in \mathbb{P}^1(\mathbb{Q})$ we consider the *forward orbit*

$$\mathcal{O}_\phi(\alpha) = \{\alpha, \phi(\alpha), \phi^2(\alpha), \dots\},$$

where $\phi^k = \phi \circ \cdots \circ \phi$ means composition of ϕ with itself. We say that α is a *wandering point* if $\mathcal{O}_\phi(\alpha)$ is an infinite set. In direct analogy with Siegel's theorem that a curve of genus 1 has only finitely many integral points, we have the following theorem.

THEOREM 7.1 ([**8**, Theorem A], [**10**, Theorem 3.43]). *Let $\phi(z) \in \mathbb{Q}(z)$ be a rational map of degree $d \geqslant 2$ such that $\phi^2(z) \notin \mathbb{Q}[z]$. Let $\alpha \in \mathbb{Q}$ be a wandering point for ϕ. Then $\mathcal{O}_\phi(\alpha)$ contains only finitely many integer points.*

The following example shows that, just as elliptic curves can have arbitrarily many integer points (see for instance [**5**]), we can construct rational maps with arbitrarily many integer points in their orbits too.

EXAMPLE 7.2 (See [**10**, Example 3.45]). Let $\phi(z) = (z^2 + z + 1)/(z^2 - z + 1)$. Then $\mathcal{O}_\phi(0) = \{0, 1, 3, 13/7, \dots\}$. We can construct another rational map with more integer points in its orbit by scaling the denominator out. Consider $\psi(z) = 7\phi(z/7)$ with $\mathcal{O}_\psi(0) = \{0, 7, 21, 13, 2163/127, \dots\}$. We can iteratively scale out consecutive denominators and construct rational functions with arbitrarily many integer points in their orbits.

In the example above we have $[\phi] = [\psi] \in \mathcal{M}_2(\mathbb{Q})$. The associated models have

$$\mathrm{Res}_2(z^2 + z + 1, z^2 - z + 1) = 4 \quad \text{and} \quad \mathrm{Res}_2(7x^2 + 49x + 343, x^2 - 7x + 49) = 4 \cdot 7^6,$$

so the function obtained by scaling is not given by a minimal model.

Analogous to a conjecture by Dem'janenko–Lang [**4**, p. 140] on uniform bounds on the number of integral points on minimal Weierstrass models of elliptic curves, Silverman makes the following conjecture.

CONJECTURE 7.3 [**10**, Conjecture 3.47]. For $d \geqslant 2$ there is a constant C_d such that for any rational map $\phi \in \mathrm{Rat}_d(\mathbb{Q})$ such that ϕ^2 is not a polynomial given by a model $[F, G] \in M_d(\mathbb{Q})$ that is $\mathbb{Z}$-minimal for $[\phi] \in \mathcal{M}_d(\mathbb{Q})$ and any wandering point α, we have that $\mathcal{O}_\phi(\alpha)$ contains at most C_d integer points.

Silverman makes a conjecture that is *a priori* stronger by demanding that ϕ is only *affine minimal*, but Proposition 2.10 shows that over $\mathbb{Z}$ this formulation is equivalent. In [**8**] he also mentions an example $\phi(z) = (-54z^2 + 16z + 128)/(z^2 - 41z + 64)$ for which $\mathcal{O}_\phi(0)$ contains at least seven integer values. Unfortunately, $\psi(z) = \phi(8z)/8 = (-54z^2 + 2 + 2)/(8z^2 - 41z + 8)$ has a smaller resultant, so ϕ is not (affine) minimal.

In the same paper Silverman also mentions that it would be interesting to exhibit minimal rational functions of degree 2 with at least eight integer points in an orbit. We describe one approach to finding such functions.

First we remark that a simple interpolation argument shows that a sufficiently long initial part of a wandering orbit determines a rational function of given degree uniquely. Suppose that $\phi(z) = f(z)/g(z)$ is a rational function of degree d with orbit $\{c_0, \dots, c_r, \dots\}$. Then the

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

coefficients $f_d, \dots, f_0, g_d, \dots, g_0$ satisfy the linear system

$$\begin{pmatrix} c_0^d & \dots & 1 & -c_1c_0^d & \dots & -c_1 \\ c_1^d & \dots & 1 & -c_2c_1^d & \dots & -c_2 \\ \vdots & & \vdots & \vdots & & \vdots \\ c_{r-1}^d & \dots & 1 & -c_rc_{r-1}^d & \dots & -c_r \end{pmatrix} \begin{pmatrix} f_d \\ \vdots \\ f_0 \\ g_d \\ \vdots \\ g_0 \end{pmatrix} = 0. \tag{7}$$

Indeed, setting $c_0 = 0$, the affine plane $\mathbb{A}^{2d+1}$ with coordinates $(c_1, \dots, c_{2d+1})$ is birational to Rat_d. There are some obvious loci on which this birationality is not defined. For instance, when $c_i = c_j$ for $i \neq j$ or when a significant part of the orbit already fits a lower degree function, for example $d = 2$ and $(c_1, \dots, c_5) = (1, 3, 7, 15, c_5)$.

In particular, we see that in order for $\{c_0, \dots, c_{2d+1}\}$ to be an orbit of a degree d function, the matrix in (7) must have determinant 0. This leads to a relation

$$N(c_0, \dots, c_{2d+1}) - c_{2d+2}D(c_0, \dots, c_{2d+1}) = 0 \quad \text{with } N, D \in \mathbb{Z}[c_0, \dots, c_{2d+1}].$$

Furthermore, N is of total degree $(d+1)^2$ and D is of total degree $d(d+2)$. Both N and D are of degree $d+1$ in each of $c_1, \dots, c_{2d+1}$ and of degree d in c_0.

A reasonable strategy to find rational maps with an orbit containing many integers is now to set a bound $B > 0$, choose $c_0, \dots, c_{2d+1} \in \{-B, \dots, B\}$ and see for which values we have that $D(c_0, \dots, c_{2d+1})$ divides $N(c_0, \dots, c_{2d+1})$. To reduce the search we can restrict to $c_0 = 0$ and $c_1 > 0$. For each of the found vectors $(0, c_1, \dots, c_{2d+2})$ we check if there is indeed a corresponding degree d rational function and whether the resulting model is minimal using Algorithm 4.1.

For $d = 2$ it turns out that N has 70 monomials and largest coefficient 4 and D has 76 monomials with largest coefficient 3. Since $76 \cdot 3 \cdot 100^8 < 2^{63}$ and $4 \cdot 100^9 < 2^{63}$, we can take $B = 100$ and do the divisibility test with word-sized integers on a 64-bit machine, provided we reduce the terms of N modulo the value of D before adding them. This approach allowed us to test the roughly $1.5 \cdot 10^{11}$ candidates with $c_1 \in \{1, \dots, 100\}$ and $c_2, \dots, c_5 \in \{-100, \dots, 100\}$ in about four days on a 2.33 GHz machine. We used Cython [1] and Sage [11] for the implementation of the computer program. Our findings are summarized in Table 1. A full list of orbits found is available electronically from [3].

In order to prove that the orbit of 0 is indeed infinite we make use of the following result.

THEOREM 7.4 ([10, Theorem 2.21] or [7, Theorem 1.1]). *Let $\phi \in \mathrm{Rat}_d(\mathbb{Q})$ and let $[F, G]$ be a model of ϕ over $\mathbb{Z}$. Let p be a prime not dividing $\mathrm{Res}_d(F, G)$. Then there is an explicit procedure to produce a finite set $M(\phi, p)$ such that for any $\alpha \in \mathbb{P}^1(\mathbb{Q})$ such that α is a periodic point under ϕ, we have that*

$$\phi^k(\alpha) = \alpha \quad \text{for some } k \in \{mp^e : m \in M(\phi, p),\ e \in \{0, 1, \dots\}\}.$$

The construction guarantees that no element of $M(\phi, p)$ is divisible by a prime bigger than $p + 1$.

A consequence of this theorem is that if $p_0 \geqslant 3$ is a prime of good reduction for ϕ, then no primes bigger than p_0 will divide the period of any periodic rational point, so if we take good primes $3 \leqslant p_0 < p_1 < \cdots < p_r$ and compute

$$M = \bigcap_{i=1}^{r} M(\phi, p_i),$$

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

then any point $\alpha \in \mathbb{P}^1(\mathbb{Q})$ periodic under ϕ is a solution to $\phi^k(z) = z$ for some $k \in M$. The nature of the explicit procedure yields that M is likely very small for even small values of $r > 2$, so one can find all rational periodic points by solving a finite and likely small number of polynomial equations. We can find all rational preperiodic points by computing the rational points in the inverse orbits of the periodic points. This is a matter of iteratively solving equations of the form $\phi(z) = \alpha$ for appropriate α. We can check that 0 is a wandering point by verifying it does not occur in the list of preperiodic points we construct above. See [3] for an implementation of this procedure.

For each of the 2190 minimal rational functions for which the initial seven members of the orbit of 0 are integral, we checked whether there are any further integers early in the orbit. We found four functions where the orbit starts with eight integers and a fifth function with eight integers, but not in consecutive spots. See Table 2.

We also used this strategy to find degree 3 rational functions with many integers in the orbit of 0. Using the same approach as for degree 2 functions, we find that we can prescribe orbits $[0, c_1, \ldots, c_7]$ with $c_1 \in \{1, \ldots, 10\}$ and $c_2, \ldots, c_7 \in \{-10, \ldots, 10\}$. Again, we can express $c_8 = N(c_1, \ldots, c_7)/D(c_1, \ldots, c_7)$, where N has total degree 16 and D has total degree 15. Searching through tuples of distinct integers $(c_1, \ldots, c_7)$ in this range such that $D(c_1, \ldots, c_7)$ divides $N(c_1, \ldots, c_7)$ took about 31 h. Again, we check the resulting tuples for minimality, polynomials and preperiodic orbits. Our findings are summarized in Table 3. See [3] for all found orbits.

For each of the 6508 resulting functions we found that 28 functions had a tenth integer in the orbit of 0 and 25 functions had an integer preimage for 0. However, eleven of these are translates of other functions, so we find 42 minimal degree 3 functions with at least ten integers consecutively in an orbit. We also found six examples where a tenth integer point occurred after a non-integral or an infinite value. See [3] for a full list and Table 4 for a small sample.

TABLE 1. *Search results for rational functions of degree* 2 *with many integers in the orbit of* 0.

Size of search space	150 617 612 376
Orbits with a seventh integer point	2 112 933
Orbits corresponding to minimal maps	2 261
Preperiodic orbits	64
Polynomials	7
Non-polynomial, infinite orbits with at least seven integer points in the orbit of 0	2 190

TABLE 2. *Some explicit degree* 2 *functions with eight integers in an orbit.*

$\phi(z)$	$\mathcal{O}_\phi(0)$
$\dfrac{86z^2 - 1068z - 338}{z^2 + 7z - 338}$	$[0, 1, 4, 11, 12, 7, 15, -374, \ldots]$
$\dfrac{-61z^2 - 1279z + 1862}{4z^2 + 114z + 266}$	$[0, 7, -8, -21, -5, -33, -26, -1020, \ldots]$
$\dfrac{25z^2 - 1895z - 8910}{58z^2 - 146z - 990}$	$[0, 9, -10, 2, 12, -5, 1, 10, \ldots]$
$\dfrac{367z^2 - 15104z + 143325}{12z^2 - 469z + 4095}$	$[0, 35, 27, 17, 18, 21, 26, -99, \ldots]$
$\dfrac{12z^2 - 29z - 35}{z^2 + 8z - 35}$	$\left[0, 1, 2, 3, 7, 5, 4, \dfrac{41}{13}, -40, \ldots\right]$

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press

TABLE 3. *Degree 3 functions with many integer points in the orbit of 0.*

Size of search space	195 350 400
Orbits with a ninth integer point	44 563
Orbits belonging to minimal maps	7 631
Orbits corresponding to non-degree 3 maps	3
Degree 3 polynomial orbits	0
Degree 3, preperiodic orbits	913
Degree 3 non-preperiodic, orbits with at least nine integer points in the orbit of 0	6 508

TABLE 4. *Some explicit degree 3 rational functions with ten integers in an orbit.*

$\phi(z)$	$\mathcal{O}_\phi(0)$
$\frac{7z^3-41z^2-216z+180}{2z^3-z^2-21z+90}$	$[0, 2, -6, 6, -3, 3, -9, 5, -5, 8, \dots]$
$\frac{-6z^3-10z^2+29z-3}{z^3-8z-3}$	$[0, 1, -1, -9, -5, -4, -3, 3, \infty, -6, \dots]$
$\frac{35z^3-219z^2+292z+60}{5z^3-18z^2-26z+60}$	$[0, 1, 8, 5, 4, 3, 2, -2, \infty, 7, \dots]$
$\frac{-24z^3+285z^2-825z+252}{z^3+15z^2-142z+126}$	$[0, 2, 5, -3, 9, -2, 7, 1, \infty, -24, \dots]$

Acknowledgements. We are particularly grateful for the generous support of the 2010 Arizona Winter School and in particular Joseph Silverman who carefully prepared lectures and assignments. The work described here drew inspiration from one of the problems he set for the school. We also thank an anonymous referee for inquiring about examples in non-principal domains, which led to a strengthening of Proposition 2.10 and Example 6.4.

References

1. S. BEHNEL, R. BRADSHAW, G. EWING, D. S. SELJEBOTN *et al.*, 'Cython: C-extensions for python', 2009, http://www.cython.org.

2. J. BOSMA, J. CANNON and C. PLAYOUST, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* 24 (1997) no. 3–4, 235–265.

3. N. BRUIN and A. MOLNAR, 'Integers in orbits of rational functions ', 2012, http://www.cecm.sfu.ca/~nbruin/intorbits.

4. S. LANG, *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] 231 (Springer, Berlin, 1978); MR 518817(81b:10009).

5. K. MAHLER, 'On the lattice points on curves of genus 1', *Proc. Lond. Math. Soc., II. Ser.* 39 (1935) 431–466; doi:10.1112/plms/s2-39.1.431.

6. A. MOLNAR, 'Fractional linear minimal models of rational functions', MSc Thesis, Simon Fraser University, 2011.

7. P. MORTON and J. H. SILVERMAN, 'Rational periodic points of rational functions', *Int. Math. Res. Not.* 2 (1994) 97–110; MR 1264933(95b:11066), doi:10.1155/S1073792894000127.

8. J. H. SILVERMAN, 'Integer points, Diophantine approximation, and iteration of rational maps', *Duke Math. J.* 71 (1993) no. 3, 793–829; MR 1240603(95e:11070), doi:10.1215/S0012-7094-93-07129-3.

9. J. H. SILVERMAN, 'The field of definition for dynamical systems on $\mathbf{P}^1$', *Compositio Math.* 98 (1995) no. 3, 269–304; MR 1351830(96j:11090).

10. J. H. SILVERMAN, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics 241 (Springer, New York, 2007), MR 2316407(2008c:11002).

11. W. A. STEIN, 'Sage Mathematics Software (Version 4.7)', The Sage Development Team, 2011, http://www.sagemath.org.

12. L. SZPIRO, M. TEPPER and P. WILLIAMS, 'Resultant and conductor of geometrically semi-stable self maps of the projective line over a number field or function field', Preprint, 2010, http://arxiv.org/abs/1010.5030.

13. J. TATE, 'Algorithm for determining the type of a singular fiber in an elliptic pencil', *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Mathematics 476 (Springer, Berlin, 1975) 33–52; MR 0393039(52#13850).

Nils Bruin
Department of Mathematics
Simon Fraser University
8888 University Drive, Burnaby
BC V5A 1S6
Canada

nbruin@sfu.ca

Alexander Molnar
Mathematics and Statistics
Queen's University
Jeffery Hall, University Avenue
Kingston, ON K7L 3N6
Canada

a.molnar@queensu.ca

https://doi.org/10.1112/S1461157012001131 Published online by Cambridge University Press