ON THE REDUCTION THEORY OF BINARY FORMS

MICHAEL STOLL AND JOHN E. CREMONA

1. Introduction

In [4], a reduction theory for binary forms of degrees three and four with integer coefficients was developed in detail, the motivation in the case of quartics being to improve 2-descent algorithms for elliptic curves over $\mathbb{Q}$. In this paper we extend some of these results to forms of higher degree. One application of this is to the study of hyperelliptic curves, which are given by affine equations of the form

$$Y^2 = f(X)\,,$$

where $f(X)$ is a polynomial of degree $n \geq 5$; we will show how to reduce such an equation to one with smaller coefficients, via a unimodular transformation, in a systematic and (in a certain sense) optimal way. This is often useful, since the construction of such equations often results in polynomials with extremely large coefficients. For example, see [14], where rather *ad hoc* methods are used for reduction.

The goals of a reduction theory for binary forms (or for the corresponding polynomials) are two-fold, corresponding to two basic problems: first, given such a form defined over $\mathbb{R}$, find an equivalent one (with respect to integral unimodular transformations) with 'smaller' coefficients; second, for forms defined over $\mathbb{Z}$, enumerate (up to equivalence) all forms with a given discriminant, or a given set of invariants. Both these problems were studied for cubics and quartics over $\mathbb{Z}$ in [4]; in this paper we only consider the first, but for forms of arbitrary degree. The methods we use are inspired by Julia's treatise [9]: we observe, however, that Julia's results are only explicit for degrees three and four.

The basic principle behind reduction in any set S on which the modular group $\mathrm{SL}(2,\mathbb{Z})$ acts (on the right), is to associate to each element $s \in S$ a covariant point $z(s)$ in the upper half-plane $\mathcal{H}$. Here, covariance means that for each $g \in \mathrm{SL}(2,\mathbb{Z})$ we have

$$z(s \cdot g) = g^{-1}(z(s))\,,$$

where $\mathrm{SL}(2,\mathbb{Z})$ acts on $\mathcal{H}$ in the usual way (on the left) via fractional linear transformations. Each $\mathrm{SL}(2,\mathbb{Z})$-orbit in $\mathcal{H}$ has a representative in the standard fundamental region $\mathcal{F}$ defined as follows:

$$\mathcal{F} = \{z \in \mathcal{H} : |z| \geq 1,\ -\tfrac{1}{2} \leq \mathrm{Re}(z) \leq \tfrac{1}{2}\}\,;$$

the representative in $\mathcal{F}$ is unique except if it is on the boundary of $\mathcal{F}$, when there are up to two representatives. We define $s \in S$ to be *reduced* if and only

Date: November 21, 2002.

if $z(s) \in \mathcal{F}$. Note that there may be more than one way of defining the system of covariant points $s \mapsto z(s)$, in which case there will be more than one notion of 'reduced' for the set S. In such situations other considerations will determine which is best. In particular, this happens when S is the set of real binary forms of fixed degree n, where either $n \geq 5$, or $3 \leq n \leq 4$ and we fix a signature which is neither totally real nor totally imaginary.

When S is the set of binary forms of fixed degree, the action of $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ on $F(X,Z)$ is by substitution: $(F \cdot g)(X,Z) = F(aX + bZ, cX + dZ)$.

An alternate viewpoint is to associate to each $s \in S$ a positive definite real quadratic form $Q(s)$ which is $\mathrm{SL}(2,\mathbb{Z})$-covariant, instead of a point $z(s) \in \mathcal{H}$. There is no essential difference, since each such form Q has a unique root in the upper half-plane, and conversely each point $z \in \mathcal{H}$ is the root of a positive definite real quadratic, unique up to multiplication by a positive constant. In this paper we will use both the language of covariant points and that of covariant quadratics, and make use of the hyperbolic geometry of $\mathcal{H}$ in some of our arguments.

The paper is organised as follows. After setting up some notation, we take up Gaston Julia's thesis [9], where he introduces an approach to reducing real (and also complex) forms of arbitrary degrees greater than two, which builds on earlier work of Hermite. Julia develops some of the theory in general, but only gives complete and explicit details for degrees three and four. We extend this to the general case, and show how this approach leads to a reduction algorithm. We then give some examples for the application of this algorithm, and finish with some additional results for forms with only real roots.

We are grateful to David Masser and the referee for pointing out to us that in A. Baker's paper [1], bounds are obtained for the coefficients of an integer quartic in terms of its invariants, using a reduction method. The method used by Baker is based on precisely the same covariant quadratics as in [4] and here, and one can check that the bounds on the leading coefficient obtained in [1] are almost the same as those in [4]. The former point is not so surprising, given the uniqueness of the covariant quadratic which we prove (see Proposition 3.4 below). However, we note that in [4] a slightly improved bound is obtained for real quartics with exactly two real roots (compare inequality (49) in [4], which agrees precisely with Baker, to the improved inequalities (57) and (58)). Baker's paper refers to Hermite [6], but not to either Julia [9] or Birch and Swinnerton-Dyer [3].

In this paper we do not give explicit results on the bounds on the coefficients of reduced forms. We defer this to a sequel [12], in which we will discuss the question of whether the forms which are reduced, in the sense defined here, are in some sense the "smallest" representatives of their $\mathrm{SL}(2,\mathbb{Z})$-orbit.

We thank the referee for suggesting to us to relate our results to the notions of stable and semi-stable forms.

2. Notation and Basics

In the following, it is is useful to consider the upper half-plane $\mathcal{H}$ to be a vertical cross-section of hyperbolic 3-space or upper half-space $\mathcal{H}_3$. If we coordinatise $\mathcal{H}_3$

as

$$\mathcal{H}_3 = \{(z, u) \mid z \in \mathbb{C}, u \in \mathbb{R}_+\},$$

then $\mathcal{H} = \{(t, u) \mid t \in \mathbb{R}\}$, where we identify $(t, u) \in \mathcal{H}_3$ with $t + iu \in \mathcal{H}$. The action of $\mathrm{SL}(2, \mathbb{R})$ on $\mathcal{H}$ is then compatible with the action of $\mathrm{SL}(2, \mathbb{C})$ on $\mathcal{H}_3$. This enlarged viewpoint was already used by Julia (following Hermite, Humbert, Bianchi and others), and allows the unification of several cases which otherwise have to be treated separately. In addition, this is the appropriate context in which to consider the reduction of complex (as opposed to real) forms, which is necessary in developing a reduction theory over number fields which are not totally real.

In this case, positive definite quadratic forms are replaced by positive definite Hermitian forms; the correspondence between them and points in $\mathcal{H}_3$ is as follows. A positive definite Hermitian form can be expressed as

$$Q(X, Z) = a\,|X|^2 + b\,X\bar{Z} + \bar{b}\,\bar{X}Z + c\,|Z|^2 = a(|X - t\,Z|^2 + u^2\,|Z|^2)$$

with $a, c, u > 0$ and $b, t \in \mathbb{C}$. The corresponding point in $\mathcal{H}_3$ is then (t, u).

In order to be able to treat the real and the complex cases in parallel later on, we set $\mathcal{H}_{\mathbb{R}} = \mathcal{H}$ and $\mathcal{H}_{\mathbb{C}} = \mathcal{H}_3$. The symbol $\mathbb{K}$ will stand for either $\mathbb{R}$ or $\mathbb{C}$. Let $\mathbb{K}[X, Z]_n$ be the space of forms of degree n in two variables with coefficients in $\mathbb{K}$, and let $\mathbb{K}[X, Z]'_n$ denote the subset of forms without repeated factors. If $\mathbb{K} = \mathbb{R}$, we also use the notations $\mathbb{R}[X, Z]_{r,s}$ and $\mathbb{R}[X, Z]'_{r,s}$ for the space of forms and the subset of squarefree forms of signature (r, s), respectively.

To define a suitable covariant map $F \mapsto z(F)$ for binary forms F, we can forget that we are primarily interested in the action of $\mathrm{SL}(2, \mathbb{Z})$ on forms with integral coefficients, and consider $\mathrm{SL}(2, \mathbb{K})$, acting on forms with coefficients in $\mathbb{K}$ (of fixed degree, and maybe fixed signature when $\mathbb{K} = \mathbb{R}$). Then we will require the stronger property that z be covariant with respect to the action of $\mathrm{SL}(2, \mathbb{K})$.

We further denote by $H(\mathbb{R})$ the set of positive definite binary quadratic forms and by $H(\mathbb{C})$ the set of positive definite binary Hermitian forms. Note that $H(\mathbb{R})$ is naturally embedded in $H(\mathbb{C})$ by

$$a\,X^2 + 2b\,XZ + c\,Z^2 \mapsto a\,|X|^2 + b\,X\bar{Z} + b\,\bar{X}Z + c\,|Z|^2$$

(where $a, b, c \in \mathbb{R}$). We denote the canonical map $H(\mathbb{K}) \longrightarrow \mathcal{H}_{\mathbb{K}}$ by z (see above for its definition). The maps for $\mathbb{K} = \mathbb{R}$ and $\mathbb{K} = \mathbb{C}$ are compatible, so we can use the same name for both of them. There is an action of $\mathrm{SL}(2, \mathbb{C})$ on $H(\mathbb{C})$, defined by

$$Q(X, Z) \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = Q(aX + bZ, cX + dZ);$$

then $z : H(\mathbb{C}) \to \mathcal{H}_{\mathbb{C}}$ is covariant with respect to this action and the usual one on $\mathcal{H}_{\mathbb{C}}$. The analogous action of $\mathrm{SL}(2, \mathbb{R})$ on $H(\mathbb{R})$ is compatible with this action.

Furthermore, for our purposes, we define the *discriminant* of the form $Q \in H(\mathbb{C})$, with coefficients (a, b, c) as above, (with $a, c \in \mathbb{R}_{>0}$ and $b \in \mathbb{C}$), by

$$\operatorname{disc} Q = 4\,(ac - |b|^2) \in \mathbb{R}_{>0}.$$

Then $z(Q) = (t, u)$ with $t = -\bar{b}/a$ and $u = \operatorname{disc}(Q)^{1/2}/(2a)$. It is easily seen that the discriminant is invariant under the $\mathrm{SL}(2, \mathbb{C})$-action. The same definition applies also to forms $Q \in H(\mathbb{R})$, which are characterised by $b \in \mathbb{R}$, and in this case the discriminant is the negative of the usual discriminant. (We use the negative here for notational convenience, since it is positive for positive definite forms.)

To summarise, we want to find an $\mathrm{SL}(2, \mathbb{K})$-covariant map

$$z : \mathbb{K}[X, Z]'_n \longrightarrow \mathcal{H}_{\mathbb{K}} \quad (\text{or} \longrightarrow H(\mathbb{K}))$$

that is computable (in a practical sense), and has the property that a form F is 'small' if its image $z(F)$ is in the fundamental domain $\mathcal{F}$.

In the complex case, the map z should also be compatible with complex conjugation (acting on $\mathcal{H}_{\mathbb{C}}$ through the first coordinate). This implies that the restriction of the complex map to real polynomials has image in $\mathcal{H}_{\mathbb{R}} \subset \mathcal{H}_{\mathbb{C}}$ and thus also provides a suitable solution for the problem over $\mathbb{R}$.

We will use throughout the convention of using uppercase letters for binary forms $F(X, Z)$ of a given degree, and lowercase letters for the dehomogenised polynomials $f(X) = F(X, 1)$.

3. Julia's approach

In his thesis [9], Gaston Julia deals with the problem of how to define a good notion of being reduced for binary forms over $\mathbb{R}$ of degree larger than two, building on earlier work of Hermite [6], [7]. His approach (cast in slightly more modern language) is as follows. Let

$$F(X, Z) = a_0 X^n + a_1 X^{n-1} Z + a_2 X^{n-2} Z^2 + \cdots + a_n Z^n$$

be a binary form of degree n; we suppose[1] that $a_0 \neq 0$. Then we can write

$$F(X, Z) = a_0 (X - \alpha_1 Z)(X - \alpha_2 Z) \dots (X - \alpha_n Z)$$

with some complex numbers α_j. To obtain a representative point in the upper half-plane, we construct a positive definite quadratic form

$$Q(X, Z) = \sum_{j=1}^{n} t_j (X - \alpha_j\, Z)(X - \bar{\alpha}_j\, Z)\,,$$

where the t_j are positive real numbers that have to be determined.[2] Julia shows that the set of possible representative points is the convex hull (in hyperbolic geometry) of the roots α_j that lie in the upper half-plane or on the real axis. If we act on F by some element from $\mathrm{SL}(2, \mathbb{R})$, and simultaneously perform an appropriate operation on the t_j, then the resulting Q will be the result of acting on the original Q by the same substitution. Julia notes that the expression (first introduced by Hermite in [6])

$$\theta_0 = \frac{a_0^2\, (\mathrm{disc}(Q))^{n/2}}{t_1 t_2 \dots t_n}$$

is then an *invariant*. Furthermore, the leading coefficient of a form that has its representative point in the fundamental domain $\mathcal{F}$ can be bounded in terms of θ_0

[1] This is not an essential restriction (the relevant quantities can be obtained by a suitable limiting process when $a_0 = 0$), but serves to simplify the exposition.

[2] Julia uses t_j^2 and u_j^2 to denote the positive real numbers t_j.

(and the same is true for the other coefficients if a_0^2 is bounded below, as when we are considering forms with integral coefficients). Therefore he chooses the representative point that belongs to the quadratic Q that makes θ_0 minimal. We will see below that this gives indeed a well-defined point (i.e., there is a unique Q that minimises θ_0; Julia proves existence but not uniqueness). This then implies that this point (or the quadratic Q) is a *covariant* (under $\mathrm{SL}(2,\mathbb{R})$) of F, hence can be used to define a reduction theory.

Julia has solved the optimisation problem for degrees three and four. His results coincide with those obtained by one of us [4] by a different method. In [4] the problem is approached from a different direction, by looking for positive definite quadratic covariants of the given form. We now show why the results are necessarily the same (at least in the purely real and purely complex cases in degrees three and four). The reason is that the presence of sufficiently many symmetries forces a unique covariant.

Lemma 3.1. *Let G be a group acting on two sets A and B. Suppose that for all $a \in A$, the stabiliser G_a of a in G has a unique fixed point $z(a) \in B$. Then $z : A \to B$ is the unique G-equivariant map from A to B.*

Proof: For definiteness, let us assume that G acts on the right on both sets. Let $a \in A$ and $g \in G$; then $G_{a \cdot g} = g^{-1} G_a g$, and therefore, $z(a) \cdot g$ is fixed by $G_{a \cdot g}$, whence $z(a \cdot g) = z(a) \cdot g$. So z is indeed equivariant. Now let $f : A \to B$ be any equivariant map, and let $a \in A$. Then for all $g \in G_a$, we have $f(a) \cdot g = f(a \cdot g) = f(a)$, hence $f(a)$ is fixed by G_a, so $f(a) = z(a)$ and $f = z$. □

We can apply this to forms of degrees three and four, represented by the (unordered) set of their roots.

Lemma 3.2.

(1) *A set of three distinct points on the real line has exactly one* $\mathrm{SL}(2,\mathbb{R})$-*covariant point in the upper half-plane.*
(2) *A set of four distinct points on the real line has exactly one* $\mathrm{SL}(2,\mathbb{R})$-*covariant point in the upper half-plane.*
(3) *A set of two distinct points in the upper half-plane has exactly one* $\mathrm{SL}(2,\mathbb{R})$-*covariant point in the upper half-plane.*

Proof: We use the Poincaré disk model for the hyperbolic plane. In each case, we show that the stabiliser in $\mathrm{SL}(2,\mathbb{R})$ of the given configuration has a unique fixed point in $\mathcal{H}$. The claim then follows from Lemma 3.1.

(1) Since $\mathrm{SL}(2,\mathbb{R})$ acts transitively on sets of three real points, we can move the points such that they become the vertices of an equilateral triangle on the boundary of the disk. This shows that the set of three points has a stabiliser of order three (given by rotations of the disk) with a unique fixed point.

(2) The group $\mathrm{SL}(2,\mathbb{R})$ preserves the cyclic ordering of the four points. Hence the two diagonals of the ideal quadrilateral formed by the points are covariant, and so is their point of intersection. Conversely, we can move this intersection point to become the centre of the Poincaré disk; then the four points must be at the corners of a rectangle. This shows that the set of four points is stabilised by the

rotation by π around the centre, which is the unique fixed point.
(3) A similar argument as in part (2) shows that the midpoint of the geodesic segment connecting the two points is the unique fixed point of the stabiliser. □

The lemma implies that to a real form of degree three with three real roots, or a real form of degree four with either four real roots or two pairs of conjugate complex roots, we can assign one and only one covariant point in the upper half-plane. Hence the methods of Julia in [9] and Cremona in [4] must obtain the same result in these cases. For all real cubics and quartics, Julia's covariant quadratic may be expressed as follows (with $n = 3$ or $n = 4$):

$$Q_0(F)(X,Z) = \sum_{j=1}^{n} \frac{1}{|f'(\alpha_j)|^{2/(n-2)}}(X - \alpha_j Z)(X - \bar{\alpha}_j Z)$$

(where, as usual, $f(X) = F(X,1)$); in fact, this expression gives a covariant for all degrees $n \geq 3$.

Lemma 3.3. *Q_0 is positive definite and a covariant of F for all $n \geq 3$.*

Proof: Positive definiteness is clear. Covariance with respect to translations is obvious, and covariance with respect to the inversion $(X,Z) \mapsto (Z,-X)$ follows from an easy calculation. □

For complex forms F, we define $Q_0(F) \in H(\mathbb{C})$ by

$$Q_0(F)(X,Z) = \sum_{j=1}^{n} \frac{|X - \alpha_j Z|^2}{|f'(\alpha_j)|^{2/(n-2)}};$$

then the same conclusions hold.

It follows from the uniqueness lemma that, for purely real cubics and purely real or purely complex quartics, Q_0 is the unique covariant quadratic (up to a scaling factor) and its root in the upper half-plane is the unique covariant point.

The lack of uniqueness in the mixed cases for degrees three and four is apparent in the literature; for real cubics with a single real root, Matthews [10] and Belabas [2] use the unique root in the upper half-plane as representative point, while both Julia and Cremona in [4] use a different choice, defined below, which depends on all three roots. Other choices are also possible. Similarly with mixed quartics, where Birch and Swinnerton-Dyer in [3] also use as covariant point the unique root in the upper half-plane.

However, if we enlarge our perspective (again following Julia) by considering the hyperbolic plane as embedded in hyperbolic three-space, so that we have an action of $\mathrm{SL}(2,\mathbb{C})$ on complex forms, we find similar uniqueness results for general forms of degrees three and four. Since $\mathrm{SL}(2,\mathbb{C})$ acts transitively on triples of points in $\mathbb{P}^1(\mathbb{C})$, the set consisting of the three roots of a form of degree three has stabiliser isomorphic to the symmetric group S_3, which fixes a unique point in $\mathcal{H}_3$. Similarly, the set of roots of a form of degree four has a Klein four group as stabiliser (coming from the symmetries of the cross-ratio), which again fixes a unique point in $\mathcal{H}_3$. If the given form has real coefficients, then this covariant point lies in the 'real' hyperbolic plane; it is again given by $Q_0(F)$ as above.

This enlarged perspective therefore eliminates the non-uniqueness of the covariant point in $\mathcal{H}$ for real forms F of degrees three and four in the "mixed" cases. While in these cases there is not a unique $\mathrm{SL}(2,\mathbb{R})$-covariant point in $\mathcal{H}$, there *is* a unique $\mathrm{SL}(2,\mathbb{C})$-covariant point $z(F)$ in $\mathcal{H}_3$, which lies in $\mathcal{H}$. It is certainly a good idea to profit from the inherent symmetry of the situation by treating real and complex roots on an equal footing, all the more since this allows us to also set up a reduction theory for complex forms with respect to a subgroup of $\mathrm{SL}(2,\mathbb{C})$, e.g., $\mathrm{SL}(2,\mathbb{Z}[i])$. It therefore seems reasonable that this covariant $z(F)$ should be the best one to use for reduction.

We summarize the conclusions for degrees three and four as follows, denoting by $z_0(F)$ the root $z(Q_0(F))$ of $Q_0(F)$ in $\mathcal{H}_\mathbb{C}$.

Proposition 3.4. *Let $n = 3$ or $n = 4$. There is a unique* $\mathrm{SL}(2,\mathbb{C})$*-covariant map*

$$z : \mathbb{C}[X,Z]'_n \longrightarrow \mathcal{H}_\mathbb{C} \quad (\textit{or} \longrightarrow H(\mathbb{C}))$$

given by $F \mapsto z_0(F)$ (or $\mapsto Q_0(F)$). This map is compatible with complex conjugation, and hence restricts to an $\mathrm{SL}(2,\mathbb{R})$*-covariant map*

$$z : \mathbb{R}[X,Z]'_n \longrightarrow \mathcal{H}_\mathbb{R} \quad (\textit{or} \longrightarrow H(\mathbb{R}))$$

which, for real forms of pure signature, is the unique such covariant map.

For forms of degree five and higher, the stabiliser of the set of roots is usually trivial, and symmetry does not help to fix a covariant. In this case, we fix it by solving Julia's optimisation problem. As it turns out (see Corollary 5.4 below), this solution can also be characterised by a nice geometric property. This fact provides some additional justification for considering Julia's covariant as the 'best' one.

The root $z_0(F)$ of $Q_0(F)$ in $\mathcal{H}$ is a covariant for *any* real form F with distinct roots. This means that we can use it to define a reduction theory — we call a form F *Q_0-reduced* if $z_0(F)$ is in the usual fundamental domain $\mathcal{F}$, and we can Q_0-reduce a form by moving $z_0(F)$ into the fundamental domain by the action of $\mathrm{SL}(2,\mathbb{Z})$. The advantage of this definition is that it is easily implemented, since $Q_0(F)$ is easy to write down. But it does not give optimal results in general. In particular, it is *not* Julia's covariant if the degree is five or more. (See Section 6 below for an example.)

4. Implementing Julia's approach

We consider real and complex forms in parallel.

Definition 4.1. A nonzero binary form F of degree n is called *stable*, if none of its factors (or roots) has multiplicity $\geq n/2$. (In particular, we must have $n \geq 3$.)

The name derives from the fact that these are exactly the forms that are stable with respect to the action of $\mathrm{SL}(2,\mathbb{K})$ in the sense of Mumford's Geometric Invariant Theory, compare [11].

Recall our notation:

$$F(X,Z) = a_0X^n + a_1X^{n-1}Z + a_2X^{n-2}Z^2 + \cdots + a_nZ^n \in \mathbb{K}[X,Z]_n$$

is a real or complex binary form of degree n; we suppose that $a_0 \neq 0$. Then we have

$$F(X,Z) = a_0(X - \alpha_1 Z)(X - \alpha_2 Z) \dots (X - \alpha_n Z)$$

with some complex numbers α_j. Unless otherwise specified, we suppose that F is stable.

The notation used in the following refers to Hermitian forms (i.e., the case $\mathbb{K} = \mathbb{C}$). When $\mathbb{K} = \mathbb{R}$, a term like $|X - \alpha\, Z|^2$ is to be read as $(X - \alpha\, Z)(X - \bar{\alpha}\, Z)$, corresponding to the embedding $H(\mathbb{R}) \to H(\mathbb{C})$.

We consider the positive definite form

$$Q(X,Z) = \sum_{j=1}^{n} t_j |X - \alpha_j\, Z|^2 \in H(\mathbb{K}) \,,$$

where the t_j are positive real numbers, and we want to choose them in such a way as to minimise the quantity θ, where[3]

$$\theta = \frac{|a_0|^2 (\operatorname{disc} Q)^{n/2}}{n^n\, t_1 t_2 \dots t_n} \,.$$

(Recall that with our definition of $\operatorname{disc} Q$, it is a positive real number.)

If we write $Q(X,Z) = s(|X - t\, Z|^2 + u^2\, |Z|^2)$ with $s, u > 0$ and $t \in \mathbb{K}$, we then find

$$\begin{aligned} s &= \sum_{j=1}^{n} t_j \;; \\ st &= \sum_{j=1}^{n} \alpha_j\, t_j \;; \\ s(|t|^2 + u^2) &= \sum_{j=1}^{n} |\alpha_j|^2\, t_j \;; \\ \tfrac{1}{4} \operatorname{disc} Q = s^2 u^2 &= \sum_{j<k} |\alpha_j - \alpha_k|^2\, t_j t_k \,. \end{aligned} \tag{4.1}$$

To deduce the fourth equation from the first three (which are obvious from the definition of Q), write

$$\begin{aligned} 2s^2u^2 &= s(|t|^2 + u^2) \cdot s + s \cdot s(|t|^2 + u^2) - st \cdot s\bar{t} - s\bar{t} \cdot st \\ &= \sum_{j,k=1}^{n} (\alpha_j \bar{\alpha}_j + \alpha_k \bar{\alpha}_k - \alpha_j \bar{\alpha}_k - \bar{\alpha}_j \alpha_k) t_j t_k \\ &= \sum_{j,k=1}^{n} (\alpha_j - \alpha_k)(\bar{\alpha}_j - \bar{\alpha}_k) t_j t_k = \sum_{j,k=1}^{n} |\alpha_j - \alpha_k|^2 t_j t_k = 2 \sum_{j<k} |\alpha_j - \alpha_k|^2 t_j t_k \,. \end{aligned}$$

Now minimising θ is equivalent to minimising $\operatorname{disc} Q$ under the side condition that $t_1 t_2 \dots t_n$ is constant (equal to 1, say). Let V_0 denote the subspace of $\mathbb{R}^n$ given

[3]Our θ differs by a factor of $(2/n)^n$ from Julia's θ_0.

by $\sum_j x_j = 0$. Writing $t_j = \exp(x_j)$ where $x_j \in \mathbb{R}$, we then have to minimise

$$D(x) = \sum_{j<k} |\alpha_j - \alpha_k|^2 \exp(x_j + x_k)$$

on V_0. Now we have the following lemma.

Lemma 4.2. *If F is stable, then D is strictly convex from below on $\mathbb{R}^n$. If x varies in V_0 in such a way that $|x|$ tends to infinity, then $D(x)$ tends to infinity as well. In other words, the set $\{x \in V_0 \mid D(x) \leq C\}$ is compact.*

Hence D has a unique minimum on V_0, and the minimising point is the only critical point of D in V_0.

Proof: For the first claim, consider a point $x \in \mathbb{R}^n$ and a line through it, parametrised as $y = x + \lambda u$, where $0 \neq u \in \mathbb{R}^n$. Then

$$\frac{d^2}{d\lambda^2} D(x + \lambda u)\big|_{\lambda=0} = \sum_{j<k} |\alpha_j - \alpha_k|^2 (u_j + u_k)^2 \exp(x_j + x_k) \geq 0\,.$$

If this expression vanishes, we must have $u_j + u_k = 0$ for all pairs (j, k) such that $\alpha_j \neq \alpha_k$. This implies the contradiction $u = 0$, since there are at least three distinct zeroes α_j. Hence the second derivative of D is positive definite, implying strict convexity. This already implies that there is at most one critical point for $D|_{V_0}$.

For the second claim, take some x in V_0 and assume that $x_j + x_k \leq C$ for all pairs (j, k) such that $\alpha_j \neq \alpha_k$ (this is equivalent to saying that D is bounded). We fix j and let $I = \{k \mid \alpha_j = \alpha_k\}$ and $J = \{k \mid \alpha_j \neq \alpha_k\}$; we set $d = \#I$. We now add these inequalities over all $k \in J$; this gives

$$(n-d)C \geq (n-d)x_j + \sum_{k\in J} x_k = (n-d)x_j - \sum_{k\in I} x_k\,. \tag{4.2}$$

Adding this now for all $j \in I$, we obtain

$$d(n-d)C \geq (n-d)\sum_{j\in I} x_j - d\sum_{k\in I} x_k = (n-2d)\sum_{j\in I} x_j\,.$$

Since $2d < n$ by assumption (F is stable), we then have

$$\sum_{j\in I} x_j \leq \frac{d(n-d)}{n-2d}\,C\,.$$

Using this in inequality (4.2), we get

$$x_j \leq \frac{n-d}{n-2d}\,C\,,$$

so all x_j are bounded from above. Because $\sum_{j=1}^n x_j = 0$, they have to be bounded from below, too.

The statement in the second paragraph is then clear. □

The preceding lemma guarantees us a *unique solution* to our minimisation problem. Since θ is an invariant, this implies that the (unique) minimising $Q \in H(\mathbb{K})$ is a *covariant* of F under $\mathrm{SL}(2, \mathbb{K})$. This allows us to define a reduction theory.

We let $z(F) = z(Q)$ be the point in the upper half-plane or half-space associated to Q; then $z(F)$ is also a covariant of F, as explained in the introduction.

Definition 4.3. A stable form $F(X,Z) \in \mathbb{R}[X,Z]$ is called *reduced* if $z(F)$ lies in the standard fundamental domain $\mathcal{F}$ of $\mathrm{SL}(2,\mathbb{Z})$, where $z(F)$ is the root in the upper half-plane $\mathcal{H}$ of the unique quadratic covariant $Q(X,Z)$ which minimises θ.

The covariance of $z(F)$ implies the following result.

Proposition 4.4. *Each* $\mathrm{SL}(2,\mathbb{Z})$*-orbit of stable real binary forms contains at least one reduced form* F*.*

There will usually be exactly one reduced form in each orbit (up to sign when the degree is odd), unless $z(F)$ is on the boundary of the fundamental domain, when there may be two.

In order to find a reduced form in the orbit of a given form F, we can proceed as follows. Find $z(F)$; then use the usual algorithm to find $S = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}(2,\mathbb{Z})$ such that $S \cdot z(F) \in \mathcal{F}$. Then $F \cdot S^{-1} = F(dX - bZ, -cX + aZ)$ is reduced.

For complex forms F and a suitable subgroup Γ of $\mathrm{SL}(2,\mathbb{C})$, for example $\Gamma = \mathrm{SL}(2,\mathcal{O}_K)$ for the ring of integers $\mathcal{O}_K$ in an imaginary quadratic field K, we can make a similar definition (given a fundamental domain for the action of Γ on $\mathcal{H}_{\mathbb{C}}$).

More generally, if we want to set up a reduction theory for binary forms over an arbitrary number field K, we consider the action of $\mathrm{SL}(2,\mathcal{O}_K)$ on a product $\mathcal{H}_{\mathbb{R}}^{r_1} \times \mathcal{H}_{\mathbb{C}}^{r_2}$ (where K has r_1 real and r_2 pairs of conjugate complex embeddings) through the various embeddings σ of K in $\mathbb{R}$ or $\mathbb{C}$. Given a stable form $F \in K[X,Z]$, we obtain a tuple of covariants

$$z(F) = (z(F^\sigma))_\sigma \in \mathcal{H}_{\mathbb{R}}^{r_1} \times \mathcal{H}_{\mathbb{C}}^{r_2}\,.$$

We call F *reduced* if $z(F)$ is in a fixed fundamental domain for the action of $\mathrm{SL}(2,\mathcal{O}_K)$.

To make reduction of a real or complex form practical, we need some means of actually finding $z(F)$, or equivalently, the minimising quadratic or Hermitian form Q.

The first step is to write down the conditions for a critical point of D on V_0. They are

$$\sum_{k=1}^{n} |\alpha_j - \alpha_k|^2 \exp(x_j + x_k) = \lambda \quad \text{for all } j\,,$$

where λ is a Lagrange multiplier. Going back to our original variables, this means

$$t_j \sum_{k=1}^{n} |\alpha_j - \alpha_k|^2\, t_k = \lambda \quad \text{for all } j\,. \tag{4.3}$$

Using the formulas (4.1), we find that

$$\sum_{k=1}^{n} |\alpha_j - \alpha_k|^2\, t_k = s(|t - \alpha_j|^2 + u^2)\,.$$

Summing equations (4.3) over j, we obtain $2s^2u^2 = n\lambda$. Hence a set of minimising values of t_j must satisfy

$$t_j = \frac{2}{n}\,\frac{s\,u^2}{|t-\alpha_j|^2+u^2}\,. \tag{4.4}$$

This shows that we can assume without loss of generality that $s = 1$. From $s = 1 = \sum_j t_j$ and $st = t = \sum_j \alpha_j t_j$, we deduce that the following two equations must hold.

$$\begin{aligned} \sum_{j=1}^{n} \frac{u^2}{|t-\alpha_j|^2+u^2} &= \frac{n}{2} \\ \sum_{j=1}^{n} \frac{t-\alpha_j}{|t-\alpha_j|^2+u^2} &= 0 \end{aligned} \tag{4.5}$$

In the real case $\mathbb{K} = \mathbb{R}$, we can replace α_j in the numerator of the second equation by $\operatorname{Re}(\alpha_j)$ by combining the terms corresponding to conjugate roots.

Conversely, suppose that these two equations are satisfied for some $t \in \mathbb{K}$ and $u > 0$. We can then define positive t_j by formula (4.4) with $s = 1$. It is easily checked that we then have

$$\sum_{j=1}^{n} t_j|X-\alpha_j\,Z|^2 = |X-t\,Z|^2 + u^2\,|Z|^2$$

and that equations (4.3) are also satisfied with $\lambda = 2u^2/n$. Hence every solution to (4.5) gives rise to a critical point of D, which then must be *the unique minimising point*. We have therefore proved the first part of following result. For the statement, we consider $\mathcal{H} = \mathcal{H}_{\mathbb{R}}$ as embedded into $\mathcal{H}_{\mathbb{C}}$ by $t + ui \mapsto (t,u)$ as described in Section 2.

Proposition 4.5. *For a stable form F, the representative point $z(F) \in \mathcal{H}_{\mathbb{K}}$ is given as $z(F) = (t,u)$, where (t,u) is the unique solution (in $\mathbb{K} \times \mathbb{R}_+$) of the system* (4.5).

If F is a complex form and $z(F) = (t,u)$, then $z(\bar{F}) = (\bar{t},u)$. In particular, if F is a real form, then $z(F)$ does not depend on whether we consider F to be real or complex.

Proof: We only have to prove the second part. But this simply follows by conjugating the system of equations (4.5) for F, leading to the corresponding system for $\bar{F}$, but with $\bar{t}$ instead of t. This then implies that for a real form F, considered as a complex form, $z(F) = (t,u)$ must have $t \in \mathbb{R}$ and hence is the same as $z(F)$ for F considered as a real form (justifying the use of z for both maps). □

We can use this proposition to find $z(F)$ numerically, by performing a search for a solution of (4.5). From a practical point of view, the main point of this result is that it reduces the original optimisation problem in the n variables t_j to a new optimisation problem in only two (or three) real variables t and u (or $\operatorname{Re}(t)$, $\operatorname{Im}(t)$ and u if $\mathbb{K} = \mathbb{C}$).

5. A geometric criterion

In the following, we will always consider $z(F)$ as a point in $\mathcal{H}_{\mathbb{C}}$; if F is real, this is done via the embedding of $\mathcal{H}_{\mathbb{R}}$ in $\mathcal{H}_{\mathbb{C}}$.

There is another nice description of $z(F)$. We introduce the following expression in two variables $t \in \mathbb{K}$ and $u \in \mathbb{R}_+$ associated to the form F.

$$\widetilde{F}(t,u) = |a_0|^2 \prod_{j=1}^{n} (|t-\alpha_j|^2 + u^2)\,.$$

Then it is easily verified that we obtain equations (4.5) by setting the logarithmic partial derivatives of $\widetilde{F}(t,u)/u^n$ (considered as a function of three real variables when $\mathbb{K} = \mathbb{C}$) equal to zero. Hence:

Proposition 5.1. *The representative point $z(F)$ of a stable form F is given as $z(F) = (t,u) \in \mathcal{H}_{\mathbb{K}}$, where (t,u) is the unique minimising point (in $\mathbb{K} \times \mathbb{R}_+$) of the function*

$$(t,u) \longmapsto \frac{\widetilde{F}(t,u)}{u^n}\,.$$

Moreover, the minimal value of θ is given by

$$\theta = \theta(F) = \min_{(t,u)} \frac{\widetilde{F}(t,u)}{u^n}\,.$$

If F is a real form that splits over $\mathbb{R}$, then we have $\widetilde{F}(t,u) = |F(t+ui,1)|^2$, and hence $z(F)$ is the unique minimising point in the upper half-plane of

$$z \longmapsto |F(z,1)| \cdot \operatorname{Im}(z)^{-n/2}\,.$$

Proof: It is easily seen that $\widetilde{F}(t,u)/u^n$ tends to infinity as $u \to 0$ or $u \to \infty$ or $|t| \to \infty$, hence there exists a (global) minimum. By the results of the preceding section, this is then the unique critical point.

It remains to prove the assertion about θ. This follows from $\operatorname{disc} Q = 4\,u^2$, equations (4.4) and the definition of $\widetilde{F}$. □

We can use this to extend the definition of θ to arbitrary forms F by letting

$$\theta(F) = \inf_{(t,u)} \frac{\widetilde{F}(t,u)}{u^n}\,.$$

A form is called *semi-stable* if all its roots have multiplicity $\leq n/2$. This definition again follows Mumford's GIT.

Proposition 5.2. *A form F is semi-stable if and only if $\theta(F) > 0$.*

Proof: We always have that $\widetilde{F}(t,u)/u^n$ tends to infinity if u or $|t|$ tend to infinity. Now suppose t stays away from all roots $\alpha_k \neq \alpha_j$ for some fixed j. Then we see easily that $\widetilde{F}(t,u)/u^n \geq C\,u^{2d-n}$ where d is the multiplicity of the root α_j. So for semistable F, $\widetilde{F}(t,u)/u^n$ is bounded from below by a positive constant.

On the other hand, when F is not semi-stable, we have a root α of multiplicity $d > n/2$, and then $\widetilde{F}(\alpha,u)/u^n$ tends to zero as u tends to zero, so $\theta(F) = 0$. □

If there are two roots of multiplicity $n/2$, then F is a power of a quadratic form, and there is no reasonable choice of $z(F)$ (any point on the geodesic joining the two roots could be taken). The exception is when $\mathbb{K} = \mathbb{R}$ and the quadratic form is positive definite; then there is a unique point of intersection of the geodesic with $\mathcal{H}_\mathbb{R} \subset \mathcal{H}_\mathbb{C}$, which can serve as $z(F)$. If there is a unique root of maximal multiplicity $d \geq n/2$, then the only reasonable choice for $z(F)$ would be that root; of course this $z(F)$ is no longer in the upper half-space, so we cannot use it for reduction purposes.

Note also that if F is not semi-stable, then the coefficients of F can be made arbitrarily small using suitable elements of $\mathrm{SL}(2, \mathbb{K})$, i.e., F is a "nullform" in the sense of Hilbert [8].

To obtain a nice geometric description, we consider again the upper half-space $\mathcal{H}_3$, and we view the roots α_j of F as lying on the 'floor' or boundary of $\mathcal{H}_3$, identified with $\mathbb{P}^1(\mathbb{C})$. Then an individual factor in the definition of $\widetilde{F}$ is the squared (Euclidean) distance from (t, u) to the root α, whereas

$$\log \frac{|t-\alpha|^2 + u^2}{u}$$

measures the hyperbolic distance between (t, u) and $\alpha \in \mathbb{C}$, up to some arbitrary additive constant. More precisely, the difference of these distances for two points lying on a geodesic with α as a limit point is the same as their (oriented) hyperbolic distance. Furthermore, the points with the same 'distance' from α lie on a horosphere at α. So we have the following interpretation.

Proposition 5.3. *The representative point $z(F)$ is the unique point in upper half-space such that the sum of its distances from all the roots of F is minimal.*

Note that these distances are not preserved by the action of $\mathrm{SL}(2, \mathbb{C})$ — the additive constant changes. If we add $2 \log |a_0|$, then the sum of the distances becomes invariant (if we act on F by $S \in \mathrm{SL}(2, \mathbb{C})$ and on (t, u) by S^{-1}).

We can imagine a point in upper half-space that is drawn toward each of the roots by a force of equal magnitude in an attempt to minimise the total distance to the roots. The total distance will be at a minimum when the forces are in an equilibrium. This gives the following.

Corollary 5.4. *The point $z(F)$ is characterised by the property that the unit tangent vectors at $z(F)$ in the directions of the roots of F add up to zero.*

PROOF: Up to a sign, the sum of unit tangent vectors mentioned in the statement is the gradient of $\log(\widetilde{F}(t, u)/u^n)$. □

This property is obvious in the low degree cases $n = 3$ and $n = 4$; and it is this property that gives the correct generalisation to higher degrees.

There is a slightly more elegant way of formulating Proposition 5.1. In order to achieve this, we define the *resultant* of a binary form F and a Hermitian form Q by the rules

$$\mathrm{Res}(aX - bZ, Q) = Q(b, a) \quad \text{and} \quad \mathrm{Res}(F_1 F_2, Q) = \mathrm{Res}(F_1, Q)\,\mathrm{Res}(F_2, Q)\,.$$

This is inspired by some of the properties of the usual resultant of two binary forms. Then it is easily seen that

$$\frac{\widetilde{F}(t,u)}{u^n} = \frac{2^n \operatorname{Res}(F,Q)}{(\operatorname{disc} Q)^{n/2}}$$

for $Q \in H(\mathbb{C})$, if $z(Q) = (t,u)$. Hence the following holds.

Corollary 5.5. *For $F \in \mathbb{C}[X,Z]_n$, we have*

$$\theta(F) = \inf_{Q \in H(\mathbb{C})} \frac{2^n \operatorname{Res}(F,Q)}{(\operatorname{disc} Q)^{n/2}}\,.$$

When F is stable, then the infimum is a minimum and is attained at a unique form Q, up to scaling, and we have $z(F) = z(Q)$.

A simple consequence of this is that $\theta(F_1F_2) \ge \theta(F_1)\theta(F_2)$, with equality if and only if $z(F_1) = z(F_2)$ (provided that both are defined).

6. The reduction algorithm and examples

We are now considering only real forms F, with covariant point $z(F) \in \mathcal{H}$. We want to find a reduced form in the orbit of F under $\mathrm{SL}(2,\mathbb{Z})$.

Given the definition of the covariant point $z(F)$ associated to each form F, the procedure to reduce F is standard; we recall it here and make some remarks of a practical nature.

Let F be a binary form of degree $n \ge 3$ with integral coefficients; we want to find a reduced form that is $\mathrm{SL}(2,\mathbb{Z})$–equivalent to it. We proceed as follows. First find $z := z(F)$. Repeat the following steps while z is outside the usual fundamental domain $\mathcal{F}$ for $\mathrm{SL}(2,\mathbb{Z})$.

1. Let m be the integer nearest to $\operatorname{Re}(z)$ and set $F(X,Z) := F(X+mZ,Z)$ and $z := z - m$.
2. If $|z| < 1$, then set $F(X,Z) := F(Z,-X)$ and $z := -1/z$.

After finitely many passes through the loop, z will be in $\mathcal{F}$, and F will be reduced.

For a practical implementation, a few remarks are useful.

Firstly, it may be a good idea to use $z_0(F)$ as given by $Q_0(F)$ instead of $z(F)$ to start with, since it is much more easily (and speedily) computed. When $z_0(F)$ is in $\mathcal{F}$, we expect that in most cases $z(F)$ will not be very far away from $\mathcal{F}$. This should make numerical methods easier to apply than when $z(F)$ is very close to the real axis. Furthermore, only a few extra steps will be necessary to move $z(F)$ into $\mathcal{F}$, so we will probably gain more than we lose by this slightly devious way of performing the reduction.

Secondly, in order to compute $z_0(F)$ or $z(F)$, we know of no better way than first to find all the complex roots of $F(X,1)$ numerically. The resulting value of z will have finite precision, and this precision will decrease during the computation. Therefore it seems advisable to recompute $z := z(F)$ (or $z_0(F)$) from time to time.

Thirdly, some care should be taken with the condition for leaving the loop. If taken literally, infinite looping can result from rounding errors when z is near the boundary of $\mathcal{F}$.

We now proceed to give some examples that demonstrate how to use our approach to obtain smaller models for hyperelliptic curves over $\mathbb{Q}$. Such a hyperelliptic curve can be given by an affine equation of the form

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

where $f(x)$ is a square-free polynomial with integral coefficients of degree $d \geq 5$ (we are excluding curves of genus less than 2; the genus of the curve above is $g = \lfloor (d-1)/2 \rfloor$). In order to obtain a smooth projective model, we write $f(x) = F(x,1)$ with a form $F(x,z)$ of *even* degree $n = 2\lceil d/2 \rceil = 2g+2$. The equation

$$y^2 = F(x,z)$$

then gives a smooth projective model of the curve, embedded in a weighted projective plane $\mathbb{P}^2_g$ (where x and z have weight 1 and y has weight $g+1$). Equivalently, we can glue together the two affine models

$$y^2 = F(x,1) \qquad \text{and} \qquad w^2 = F(1,z)$$

with the identifications $xz = 1$, $y = wx^{g+1}$. The modular group $\mathrm{SL}(2,\mathbb{Z})$ acts on $\mathbb{P}^2_g$ through its action on x and z; so we can use it to find a better model by reducing the form F. In the examples below, we will make extensive use of our convention $f(x) = F(x,1)$ (similarly for F_j and f_j).

The first example is taken from H.-J. Weber's thesis [14], in which he considers certain hyperelliptic curves with modular Jacobians. Weber tries to simplify the models he obtains by a trial-and-error approach. One of his final models is given by

$$\begin{aligned} y^2 = f(x) = 19x^8 - 262x^7 + 1507x^6 - 4784x^5 + 9202x^4 - 10962x^3 \\ + 7844x^2 - 3040x + 475\,. \end{aligned}$$

(See [14] or [15, p. 284].) Let us follow the algorithm as applied to F in some detail. For the first reduction steps, we use $z_0(F)$. The roots of f are

$$\begin{gathered} 0.42798171, \quad 1.30152156, \quad 1.31947230, \quad 4.31651243, \\ 1.69098301 \pm 0.72287100\,i, \quad 1.52100984 \pm 0.12866975\,i\,. \end{gathered}$$

From the roots, we compute $Q_0(F)$ and its root

$$z = z_0(F) = 1.38323301 + 0.31233552\,i\,.$$

The integer m in the algorithm is 1, so we do a shift and replace f with

$$\begin{aligned} f_1(x) &= f(x+1) \\ &= 19x^8 - 110x^7 + 205x^6 - 180x^5 + 47x^4 + 40x^3 - 35x^2 + 10x - 1 \end{aligned}$$

and z with $z_1 = z - 1 = 0.38323301 + 0.31233552\,i$. Since we have $|z_1| < 1$, we invert f_1 to get

$$\begin{aligned} f_2(x) &= x^8 f_1(-1/x) \\ &= -x^8 - 10x^7 - 35x^6 - 40x^5 + 47x^4 + 180x^3 + 205x^2 + 110x + 19 \end{aligned}$$

and set $z_2 = -1/z_1 = -1.56792167 + 1.27785869\,i$. In the next pass through the loop, $m = -2$, so

$$f_3(x) = f_2(x-2) = -x^8 + 6x^7 - 7x^6 - 12x^5 + 27x^4 - 4x^3 - 19x^2 + 10x - 5$$

and $z_3 = z_2 + 2 = 0.43207833 + 1.27785869\,i$. Since $z_3 \in \mathcal{F}$, we see that F_3 is Q_0-reduced. Now we use Julia's covariant $z(F)$. We find the roots of f_3 and use some numerical method to compute

$$z_4 = z(F_3) = 0.64189877 + 1.18525166\,i\,.$$

This is not in $\mathcal{F}$, and $m = 1$ in our algorithm. Hence we set

$$f_5(x) = f_3(x+1) = -x^8 - 2x^7 + 7x^6 + 16x^5 + 2x^4 - 2x^3 + 4x^2 - 5$$

and $z_5 = z(F_5) = z_4 - 1 = -0.35810123 + 1.18525166\,i \in \mathcal{F}$, so F_5 is reduced.

To summarise, our algorithm produces after the first step (using $z_0(F)$) the model

$$y^2 = -x^8 + 6x^7 - 7x^6 - 12x^5 + 27x^4 - 4x^3 - 19x^2 + 10x - 5\,,$$

and after the second step (using $z(F)$)

$$y^2 = -x^8 - 2x^7 + 7x^6 + 16x^5 + 2x^4 - 2x^3 + 4x^2 - 5\,.$$

Incidentally, the fact that these two are distinct justifies our claim that $z_0(F)$ is in general not Julia's $z(F)$.

Another example is related to work by X. Wang.[4] This time, it concerns a genus 2 curve, and the initial model is

$$y^2 = x^6 + 30x^5 + 371x^4 + 2422x^3 + 8813x^2 + 16968x + 13524\,.$$

After Q_0-reduction, we obtain

$$y^2 = x^6 - 4x^4 + 2x^3 + 8x^2 - 12x + 9\,,$$

and finally

$$y^2 = x^6 + 6x^5 + 11x^4 + 6x^3 + 5x^2 + 4\,.$$

Here is a third example that shows that the Q_0-reduced and the reduced form do not always differ by a shift. Consider

$$f(x) = 6x^6 + 8x^5 - 10x^4 - 4x^3 + 10x^2 - 6x + 5\,.$$

This is Q_0-reduced ($z_0(F)$ is near i, and slightly above the unit circle), but in order to find the reduced representative, we have to invert (since $z(F)$ is also near i, but slightly below the unit circle).

[4] Wang's work is described in [13]. The curve in the example is the curve of level 147; the model was communicated by Wang to the authors of [5].

7. More specific results in the totally real case

In this section, we make $z(F)$ rather explicit for totally real forms F, i.e., real forms that split into linear factors over $\mathbb{R}$. The result is as follows.

Proposition 7.1. *Let $F(X,Z)$ be a totally real form of degree $n \geq 3$ with distinct roots. Then $z(F)$ is the unique root in the upper half-plane of $G(X,1)$, where*

$$G(X,Z) = \frac{X\,F_X(-F_Z(X,Z),F_X(X,Z)) + Z\,F_Z(-F_Z(X,Z),F_X(X,Z))}{n\,F(X,Z)}$$

is a binary form of degree $(n-1)(n-2)$. (Here, F_X and F_Z denote partial derivatives).

Proof: Note that $G(X,Z)$ is indeed a polynomial. To see this, let

$$\widetilde{G}(X,Z) = X\,F_X(-F_Z(X,Z),F_X(X,Z)) + Z\,F_Z(-F_Z(X,Z),F_X(X,Z))$$

be the numerator of G. Let a be a root of F, so that $F(X,Z) = (X-aZ)H(X,Z)$. Then

$$\begin{aligned} F_X(U,V) &= H(U,V) + (U-aV)H_X(U,V) \\ F_Z(U,V) &= -aH(U,V) + (U-aV)H_Z(U,V)\,, \end{aligned}$$

so

$$\begin{aligned} &XF_X(U,V) + ZF_Z(U,V) \\ &\qquad = (X-aZ)H(U,V) + (U-aV)(XH_X(U,V) + ZH_Z(U,V))\,. \end{aligned}$$

The first term on the right is a multiple of $X - aZ$ for any U,V; so is the second when $U = -F_Z(X,Z)$ and $V = F_X(X,Z)$, since $nF = XF_X + ZF_Z$ implies $0 = aF_X(a,1) + F_Z(a,1)$, so $U - aV = -(F_Z + aF_X)$ is zero at $(a,1)$. Hence each linear factor of F divides $\widetilde{G}$, and since F has no repeated factors, $G = \widetilde{G}/(nF)$ is a polynomial.

The proof will now be in two steps. The first step is to show that $z(F)$ really is a root of $G(X,1)$. The second step is to show that $G(X,1)$, which is a polynomial of degree $(n-1)(n-2)$, has at least $n(n-3)$ real roots, leaving $z(F), \bar{z}(F)$ as the only possible pair of complex conjugate roots.

For the first step, recall that $z(F)$ is the point $z = t+iu$ in the upper half-plane minimising

$$\frac{\widetilde{F}(t,u)}{u^n} = \frac{f(z)f(\bar{z})}{(\operatorname{Im} z)^n}$$

(with the usual convention $f(z) = F(z,1)$; this equality is only valid when all the roots of f are real). Taking $z = t+iu$ and $\bar{z} = t-iu$ as new variables, the necessary conditions for the minimum can be written (after some simplification) as

$$(z-\bar{z})f'(z) = n\,f(z) \qquad \text{and} \qquad (z-\bar{z})f'(\bar{z}) = -n\,f(\bar{z})\,.$$

We can solve the first of these two equations for $\bar{z}$, obtaining

$$\bar{z} = z - n\frac{f(z)}{f'(z)} =: \lambda(z)\,;$$

then we substitute this expression for $\bar{z}$ in the second equation. We get

$$f(z)\, f'\Bigl(z - n\frac{f(z)}{f'(z)}\Bigr) + f'(z)\, f\Bigl(z - n\frac{f(z)}{f'(z)}\Bigr) = 0\,. \tag{7.1}$$

Multiplying this by $f'(z)^{n-1}$ and re-writing the expression in terms of the homogeneous polynomial F (note that $f'(z) \neq 0$; otherwise $f(z)$ would have to vanish also, but f was assumed to be squarefree), we get

$$\begin{aligned}
0 &= F(z,1)\, F_X(z\, F_X(z,1) - n\, F(z,1), F_X(z,1)) \\
&\quad + F(z\, F_X(z,1) - n\, F(z,1), F_X(z,1)) \\
&= F(z,1)\, F_X(-F_Z(z,1), F_X(z,1)) \\
&\quad + \tfrac{1}{n}\bigl(-F_Z(z,1)\, F_X(-F_Z(z,1), F_X(z,1)) + F_X(z,1)\, F_Z(-F_Z(z,1), F_X(z,1))\bigr) \\
&= \tfrac{1}{n} F_X(z,1)\bigl(z\, F_X(-F_Z(z,1), F_X(z,1)) + F_Z(-F_Z(z,1), F_X(z,1))\bigr)\,.
\end{aligned}$$

(We have again used the well-known relation $XF_X + ZF_Z = nF$.) This shows that $G(z(F),1) = 0$.

For the second step, we again use that if $f(x) \neq 0$, then

$$\frac{f'(\lambda(x))}{f(\lambda(x))} = -\frac{f'(x)}{f(x)} \tag{7.2}$$

implies that $G(x,1) = 0$. We want to show that between any two consecutive zeroes of f (considered as lying on the circle $\mathbb{P}^1(\mathbb{R})$), there are at least $n-3$ real zeroes of $G(x,1)$. Since G is easily seen to be a covariant of F, we can assume that the two consecutive roots we are considering are 0 and 1. The rational function f'/f has simple poles (with residue 1) at each of the roots of f and is monotonically decreasing (as can be seen from the partial fraction decomposition). Hence the right hand side of our equation grows monotonically from $-\infty$ to $+\infty$ in the open interval $(0,1)$. On the other hand, the function $\lambda(x) = x - nf(x)/f'(x)$ approaches zero from below when x approaches zero from above, it approaches 1 from above when x approaches 1 from below, and it has a unique (simple) pole of positive residue in the open interval $(0,1)$. This shows that when x goes from 0 to 1, the value of $\lambda(x)$ goes from 0 through $-\infty = \infty$ (on $\mathbb{P}^1(\mathbb{R})$) to 1. The function f'/f has $n-2$ simple poles outside the closed interval $[0,1]$, hence $(f'/f)(\lambda(x))$ has (at least) $n-2$ simple poles in the open interval $(0,1)$. Between any two consecutive of these poles, there must be a value of x satisfying equation (7.2). This shows that there are at least $n-3$ zeroes of $G(x,1)$ between two consecutive zeroes of f. Hence $G(x,1)$ has at least $n(n-3)$ real zeroes, as was to be shown. $\square$

When $n = 2$ one may quickly check that $G(X,Z)$ is identically zero. When $n = 3$, $G(X,Z)$ is the Hessian of F. Explicitly, if

$$F(X,Z) = aX^3 + bX^2Z + cXZ^2 + dZ^3\,,$$

then

$$G(X,Z) = (3ac - b^2)X^2 + (9ad - bc)XZ + (3bd - c^2)Z^2\,.$$

(This is minus the Hessian covariant as given in [4].)

When $n = 4$, $G(X,Z)$ is (up to a constant factor) the sextic covariant of F denoted g_6 in [4]. In both these cases it was noted in [4] that the unique root of $G(X,Z)$ in the upper half-plane was the appropriate covariant point with which to reduce a cubic or quartic with all its roots real.

In the special cases of degrees three and four, we can express $\theta(F)$ explicitly as a root of a monic polynomial having rational invariants of F as its coefficients. Let $\Delta = \mathrm{disc}(F)$. Then if F is a binary cubic form splitting over $\mathbb{R}$, we have that $\theta(F)$ is the largest root of

$$T_3(x) = 3^3\,x^2 - 2^6\,\Delta$$

(cf.[9, p.51]; note that Julia's value of θ is $(3/2)^3$ times our value). If F is a binary quartic form splitting over $\mathbb{R}$, then $\theta(F)$ is the largest root of

$$T_4(x) = x^3 - 2I\,x^2 + I^2\,x - \Delta = x(x-I)^2 - \Delta\,,$$

where $I = 12\,a_0a_4 - 3\,a_1a_3 + a_2^2$ is the usual invariant. From this, we can easily deduce that $I < \theta(F) < \frac{4}{3}I$, noting that $T_4(0) < 0$, $T_4(\frac{1}{3}I) > 0$, $T_4(I) < 0$ and $T_4(\frac{4}{3}I) > 0$.

It would be interesting to investigate whether similar equations and inequalities are satisfied by θ in the higher degree cases.

References

[1] A. Baker: *The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$*, J. London Math. Soc. **43**, 1–9 (1967).

[2] K. Belabas: *A fast algorithm to compute cubic fields*, Math. Comp. **66**, 1213–1237 (1997).

[3] B.J. Birch and H.P.F. Swinnerton-Dyer: *Notes on elliptic curves, I*, J. reine angew. Math. **212**, 7–25 (1963).

[4] J.E. Cremona: *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. **2**, 64-94 (1999).

[5] E.V. Flynn, F. Leprévost, E.F. Schaefer, W.A. Stein, M. Stoll and J.L. Wetherell: *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. Comp. **70**, 1675–1697 (2001).

[6] C. Hermite: *Note sur la réduction des fonctions homogènes à coefficients entiers et à deux indéterminées*, J. reine angew. Math. **36** (1848), also in: Œuvres de Charles Hermite, publiés par Émile Picard, Tome I, Gauthier-Villars, Paris (1905), p. 84–93.

[7] C. Hermite: *Sur l'introduction des variables continues dans la théorie des nombres*, J. reine angew. Math. **41** (1850), also in: Œuvres de Charles Hermite, publiés par Émile Picard, Tome I, Gauthier-Villars, Paris (1905), p. 164–192, Sections V and VI.

[8] D. Hilbert: *Theory of algebraic invariants*, Cambridge University Press (1993).

[9] G. Julia: *Étude sur les formes binaires non quadratiques à indéterminées réelles ou complexes*, Mémoires de l'Académie des Sciences de l'Institut de France **55**, 1–296 (1917). Also in Julia's Œuvres, vol. 5.

[10] G.-B. Matthews: *On the reduction and classification of binary cubics which have a negative discriminant*, Proc. London Math. Soc. **10**, 128–138 (1912).

[11] D. Mumford, J. Fogarty and F. Kirwan: *Geometric invariant theory*, 3rd enl. ed., Erg. Math. Grenzgeb. 2. Folge, vol. 34. Berlin: Springer-Verlag (1993).

[12] M. Stoll: *On the reduction theory of binary forms, II*, in preparation.

[13] X. Wang: *2-dimensional simple factors of $J_0(N)$*, Manuscripta Math. **87**, 179–197 (1995).

[14] H.-J. Weber: *Algorithmische Konstruktion hyperelliptischer Kurven mit kryptographischer Relevanz und einem Endomorphismenring echt größer als* $\mathbb{Z}$, Dissertation, Essen University (1996).

[15] H.-J. Weber: *Hyperelliptic simple factors of* $J_0(N)$ *with dimension at least 3*, Exp. Math. **6**:4, 273–287 (1997).

School of Engineering and Science, International University Bremen, P.O.Box 750561, 28725 Bremen, Germany.

E-mail address: m.stoll@iu-bremen.de

School of Mathematical Sciences, University of Nottingham, University Park, Nottingham NG7 2RD, UK.

E-mail address: John.Cremona@nottingham.ac.uk