London Mathematical Society ISSN 1461–1570

REDUCTION OF BINARY CUBIC AND QUARTIC FORMS

J. E. CREMONA

Abstract

A reduction theory is developed for binary forms (homogeneous polynomials) of degrees three and four with integer coefficients. The resulting coefficient bounds simplify and improve on those in the literature, particularly in the case of negative discriminant. Applications include systematic enumeration of cubic number fields, and 2-descent on elliptic curves defined over $\mathbb{Q}$. Remarks are given concerning the extension of these results to forms defined over number fields.

1. *Introduction*

Reduction theory for polynomials has a long history and numerous applications, some of which have grown considerably in importance in recent years with the growth of algorithmic and computational methods in mathematics. It is therefore quite surprising to find that even for the case of binary forms of degree three and four with integral coefficients, the results in the existing literature, which are widely used, can be improved. The two basic problems which we will address for forms $f(X, Y)$ in $\mathbb{Z}[X, Y]$ of some fixed degree n are as follows (precise definitions will be given later).

1. Given f, find a unimodular transform of f which is as 'small' as possible.
2. Given a fixed value of the discriminant Δ, or alternatively fixed values for a complete set of invariants, find all forms f with these invariants up to unimodular equivalence.

It is these two problems for which we will present solutions in degrees three and four. Our definition of a *reduced form* differs from ones in common use in the case of negative discriminant for both cubics and quartics. We will show that it agrees with the definition in Julia's treatise [**12**], though this fact is not obvious. Moreover, our definition is better than Julia's for computational purposes, and leads to good bounds on the coefficients of a reduced form.

The applications we have in mind are in two areas of number theory: the systematic tabulation of cubic and quartic algebraic number fields with given discriminant, or given bound on the discriminant; and 2-descent on elliptic curves. In the second application, the bounds we obtain below for quartics have led to considerable improvements in the running times of our program `mwrank`, which implements 2-descent on elliptic curves defined over $\mathbb{Q}$ (as described in [**8**], for example), compared with the bounds given in [**8**] and originally in [**3**]. For the first application in the cubic case, see the papers [**1**] and [**2**] of Belabas. The quartic case seems to be considerably more difficult.

In this paper we will often restrict to considering forms whose coefficients are rational integers, although a large part of the algebra applies to forms defined over arbitrary fields of characteristic 0. In future we hope to extend this to general number fields; real quadratic

Received 29 June 1998, revised 23 April 1999; *published 10 June 1999*.
1991 Mathematics Subject Classification 11C, 12Y, 11Y

fields have already been treated in [**14**] and [**9**]. Some remarks on the extension to number fields are made in the final section of the paper.

We will use a small amount of classical invariant theory in this paper, in the style of Hilbert's lecture notes [**11**], or Elliott's book [**10**], from which we obtained the term 'semi-invariant' which we use repeatedly. The modern term for these is apparently 'U-invariants'; however, we have made no attempt to couch our exposition in the language of modern invariant theory. We have not seen any systematic treatment of the 'algebraic covariants' which we use extensively. The article [**7**] contains all the invariant theory that is needed, together with an explanation of the connection with 2-descent on elliptic curves.

Our results for cubics may also be compared with bounds (due to Mordell and Davenport) which come from the Geometry of Numbers, as in Cassels' book [**4**, Chapter 2]. We will make such comparisons in detail below.

After reviewing the basic ideas underlying the reduction of real binary forms in Section 2, together with a brief summary of Julia's approach to reduction, we proceed to the two main sections of the paper, concerning the reduction of cubics (Section 3) and quartics (Section 4).

2. *Reduction: basic concepts*

Let K be a field, and n a positive integer. A *binary form* of degree n over K is a homogeneous polynomial in $K[X, Y]$ of degree n. The group $\mathrm{GL}(2, K)$ acts on $K[X, Y]$ via 'linear substitutions':

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}: \quad f(X, Y) \mapsto f(\alpha X + \beta Y, \gamma X + \delta Y).$$

This action clearly preserves the degree, and so restricts to an action on the set of forms of degree n, which is a K-vector space of dimension $n + 1$. We will mainly be concerned with the action of the subgroup $\mathrm{SL}(2, K)$ of unimodular matrices; moreover, for our applications we will also wish to restrict to forms with integral coefficients: for example, when $K = \mathbb{Q}$ or a number field the coefficients will lie in the ring of integers $\mathcal{O}_K$ and we will only consider transformations in $\mathrm{SL}(2, \mathcal{O}_K)$ or $\mathrm{GL}(2, \mathcal{O}_K)$.

It will be convenient at times to pass from a form $f(X, Y) = \sum_{i=0}^{n} a_i X^i Y^{n-i}$ to the corresponding inhomogeneous polynomial

$$f(X) = f(X, 1) = \sum_{i=0}^{n} a_i X^i \in K[X];$$

the group action then becomes

$$f(X) \mapsto (\gamma X + \delta)^n f\left(\frac{\alpha X + \beta}{\gamma X + \delta}\right).$$

The ingredients for a reduction theory for such polynomials or forms consist of the following: a definition of a suitable notion of a *reduced form*, such that every form is equivalent to (at least one) reduced form; together with algorithms for reducing a given form, and for enumerating all reduced forms up to equivalence. For example, we will see in Section 3 below a definition of 'reduced' for real cubics (which will depend on the sign of the discriminant), an algorithm for reducing any given cubic in $\mathbb{R}[X]$, and bounds on the coefficients of a reduced cubic in terms of the discriminant. This enables us to list easily all reduced cubics with integer coefficients and given discriminant.

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

2.1. *Reduction of positive definite quadratics*

Where the field of definition is a subfield of the real numbers, our definition of reduction will consist of associating, to a given polynomial $f(X)$, a quadratic with real coefficients which is positive definite and a covariant of f, and then decreeing that f is reduced if and only if this quadratic is reduced in the classical sense. The bounds we thereby obtain on the coefficients of f will come, directly or indirectly, from the well-known inequalities satisfied by the coefficients of a reduced positive definite quadratic. Hence we start by recalling the necessary facts for such quadratics.

Let $f(X, Y) = aX^2 + bXY + cY^2 \in \mathbb{R}[X, Y]$ be a real quadratic form, with discriminant $\Delta = b^2 - 4ac$. We say that f is *positive definite* if $a > 0$ and $\Delta < 0$; then $f(x, y) > 0$ for all $(x, y) \in \mathbb{R}^2 - \{(0, 0)\}$, and the roots of f (by which we mean the roots of the polynomial $f(X, 1)$) have the form $z, \overline{z}$ where $z = (-b + i\sqrt{|\Delta|})/2a$ is in the upper half-plane.

The transform of a positive definite quadratic $f(X, Y)$ by a real matrix

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

with positive determinant is also positive definite. The root z in the upper half-plane transforms via M^{-1} into $(\delta z - \beta)/(\alpha - \gamma z)$, which is also in the upper half-plane, since $\mathrm{Im}(M^{-1}(z)) = \det(M)^{-1}\,\mathrm{Im}(z)/|\alpha - \gamma z|^2$.

Definition 1. The form $f(X, Y)$ is *reduced* if the following inequalities hold:

$$|b| \leqslant a \leqslant c. \tag{1}$$

Equivalently, f is reduced if its root z in the upper half-plane lies in the standard fundamental region for the action of the modular group $\Gamma = \mathrm{SL}(2, \mathbb{Z})$:

$$|\,\mathrm{Re}(z)| \leqslant \frac{1}{2} \quad \text{and} \quad |z| \geqslant 1. \tag{2}$$

Each positive definite form is equivalent to a reduced form. The reduced form is unique unless one of the inequalities in (1) or (2) is an equality, in which case there will be two equivalent reduced forms (differing only in the sign of b). This non-uniqueness, which could of course be avoided by insisting that $b \geqslant 0$ when either equality holds, will not be at all important in the sequel.

To reduce a given form, we may choose to operate directly on the coefficients (a, b, c) or on the root z. In either case, we repeatedly *translate* by an integer k and *invert*. Operating on the coefficients, these steps are:

Step 1. **Reduce** b modulo $2a$: replace (a, b, c) by $(a, b', c') = (a, b + 2ka, ak^2 + bk + c)$, where k is the nearest integer to $-b/2a$.

Step 2. **Interchange** a and c if $a > c$: replace (a, b, c) by $(a', b', c') = (c, -b, a)$.

After a finite number of steps the resulting form will be reduced. In the second case, we operate directly on the root z, again using the translations $z \mapsto z - k$ and inversion $z \mapsto -1/z$. In either case, we keep track of the elementary transformations used in the reduction, so that at the end we can give the unimodular transformation

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

which reduces f, as well as the reduced form itself; indeed, often we will only need this transformation.

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

From the inequalities (1) we can easily deduce that

$$0 < a \leqslant \sqrt{|\Delta|/3}; \tag{3}$$

geometrically, this states that the imaginary part of the root z is at least $\sqrt{3}/2$. To find all integer quadratics with given negative integer discriminant Δ, we then merely have to search the region $0 \leqslant |b| \leqslant a \leqslant \sqrt{|\Delta|/3}$, finally testing whether $c = (b^2 - \Delta)/4a$ is integral.

2.2. *Julia's method of reduction*

We now give a very brief summary of Julia's reduction method as it applies to cubics and quartics defined over $\mathbb{R}$. For more details, see [12].

Let $g(X) \in \mathbb{R}[X]$ be a polynomial of degree $n \geqslant 3$ with nonzero leading coefficient a and nonzero discriminant Δ. Let the real roots of g be α_i for $1 \leqslant i \leqslant r$ and the pairs of complex (that is, non-real) roots be $\beta_j, \overline{\beta_j}$ for $1 \leqslant j \leqslant s$, where $r + 2s = n$. Julia considers positive definite quadratics of the form

$$\varphi(X) = \sum_{i=1}^{r} t_i^2 (X - \alpha_i)^2 + \sum_{j=1}^{s} 2u_j^2 (X - \beta_j)(X - \overline{\beta_j}), \tag{4}$$

for suitably chosen 'variables' t_i and u_j, defining g to be reduced if and only if φ is. From this he derives upper bounds on the absolute value of the leading coefficient and roots of a reduced polynomial g, all expressed in terms of the quantity

$$\theta = \frac{a^2 \operatorname{disc}(\varphi)^{n/2}}{\prod_{i=1}^{r} t_i^2 \prod_{j=1}^{s} u_j^4}.$$

For each signature (r, s) Julia then seeks to minimize θ by suitable choice of the coefficients t_i, u_j. In each case, he obtains a specific positive definite quadratic $\varphi(X)$ attached to $g(X)$, and defines $g(X)$ to be reduced if and only if $\varphi(X)$ is. From his discussion, it is clear that Julia regards the quadratic $\varphi(X)$ to be 'optimal', though no precise claim (or definition of optimality) is stated. The fact that these 'optimal' $\varphi(X)$ are indeed covariants of g is proved after the optimization, by entirely geometric considerations.

The coefficients t_i, u_j for Julia's optimal φ are defined in terms of the roots of g; in most cases, Julia states that it is therefore necessary to know these roots before reducing a given polynomial g. One feature of our reduction scheme is that we can often avoid this explicit dependence on the roots, which is certainly a computational convenience, since otherwise effective reduction requires computation of the roots of g to high precision. We will obtain expressions for φ which are defined over a subfield of the splitting field of g.

Our approach is to find quadratic covariants of cubic and quartic polynomials directly, and define reduction in terms of them. It will turn out that our covariants are in each case the same as Julia's, up to an unimportant constant factor. We will also derive bounds for the coefficients of reduced cubics and quartics which are in certain cases better than Julia's bounds, and thus result in greater efficiency in our applications.

For later reference, we now describe Julia's quadratic covariants for each of the possible signatures of cubic and quartic polynomials. We express each one both in the form Julia gives, involving modulus signs in some cases, and where necessary in an alternative form (without the modulus signs) which we will use later.

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

2.2.1. Signature (3,0): real cubics with three real roots

A real cubic with positive discriminant $\Delta > 0$ has three real roots α_1, α_2, α_3. We set $t_1^2 = (\alpha_2 - \alpha_3)^2$, with t_2^2 and t_3^2 defined symmetrically, obtaining

$$\varphi(X) = (\alpha_2 - \alpha_3)^2(X - \alpha_1)^2 + (\alpha_3 - \alpha_1)^2(X - \alpha_2)^2 + (\alpha_1 - \alpha_2)^2(X - \alpha_3)^2.$$

As Julia remarks, up to a constant factor $\varphi(X)$ is just the 'forme d'Eisenstein' or Hessian of g. This is an easy exercise in symmetric polynomials (or see Section 3 below). If $g(X) = aX^3 + bX^2 + cX + d$, then (up to a constant factor)

$$\varphi(X) = (b^2 - 3ac)X^2 + (bc - 9ad)X + (c^2 - 3bd).$$

This is the only case where we can reduce g using a rational covariant quadratic (defined over the field containing the coefficients of g).

2.2.2. Signature (1,1): real cubics with one real root

A real cubic with negative discriminant $\Delta < 0$ has one real root α and two non-real roots β, $\overline{\beta}$. We take

$$t^2 = \left|\beta - \overline{\beta}\right|^2 \qquad \text{and} \qquad u^2 = (\alpha - \beta)(\alpha - \overline{\beta}) = |\alpha - \beta|^2.$$

Then

$$\begin{aligned}\varphi(X) &= t^2(X - \alpha)^2 + 2u^2(X - \beta)(X - \overline{\beta}) \\ &= -\left(\beta - \overline{\beta}\right)^2(X - \alpha)^2 + 2(\alpha - \beta)(\alpha - \overline{\beta})(X - \beta)(X - \overline{\beta}).\end{aligned}$$

2.2.3. Signature (4,0): real quartics with four real roots

A real quartic with positive discriminant $\Delta > 0$ has either four or no real roots; these can be distinguished using certain seminvariants, as explained in Section 4 below. When there are four real roots α_i, we order these so that $\alpha_1 > \alpha_3 > \alpha_2 > \alpha_4$, and take $t_i^2 = |g'(\alpha_i)^{-1}|$ for $1 \leqslant i \leqslant 4$, to obtain

$$\begin{aligned}\varphi(X) &= g'(\alpha_1)^{-1}(X - \alpha_1)^2 + g'(\alpha_2)^{-1}(X - \alpha_2)^2 \\ &\quad - g'(\alpha_3)^{-1}(X - \alpha_3)^2 - g'(\alpha_4)^{-1}(X - \alpha_4)^2 \\ &= 2(g'(\alpha_1)^{-1}(X - \alpha_1)^2 + g'(\alpha_2)^{-1}(X - \alpha_2)^2).\end{aligned} \tag{5}$$

2.2.4. Signature (0,2): real quartics with no real roots

Here one takes $2u_1^2 = |\beta_2 - \overline{\beta_2}|$ and $2u_2^2 = |\beta_1 - \overline{\beta_1}|$, so that

$$\begin{aligned}\varphi(X) &= |\beta_2 - \overline{\beta_2}|(X - \beta_1)(X - \overline{\beta_1}) + |\beta_1 - \overline{\beta_1}|(X - \beta_2)(X - \overline{\beta_2}) \\ &= -i(\beta_2 - \overline{\beta_2})(X - \beta_1)(X - \overline{\beta_1}) - i(\beta_1 - \overline{\beta_1})(X - \beta_2)(X - \overline{\beta_2}).\end{aligned}$$

2.2.5. Signature (2,1): real quartics with two real roots

Real quartics with negative discriminant $\Delta < 0$ have exactly two real roots. Denote these as α_1, α_2 with $\alpha_1 > \alpha_2$, and the non-real roots as β, $\overline{\beta}$. Set

$$\begin{aligned}t_1^2 &= \left|\beta - \overline{\beta}\right| |\alpha_2 - \beta|^2, \\ t_2^2 &= \left|\beta - \overline{\beta}\right| |\alpha_1 - \beta|^2, \\ 2u^2 &= |\alpha_1 - \alpha_2|\,|\alpha_1 - \beta|\,|\alpha_2 - \beta|,\end{aligned} \tag{6}$$

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

and assume that $\mathrm{Im}(\beta) > 0$. Then

$$\begin{aligned}\varphi(X) &= t_1^2(X-\alpha_1)^2 + t_2^2(X-\alpha_2)^2 + 2u^2(X-\beta)(X-\overline{\beta}) \qquad (7)\\ &= |\beta-\overline{\beta}||\overline{\beta}-\alpha_2||\alpha_2-\beta|(X-\alpha_1)^2\\ &\quad +|\beta-\overline{\beta}||\overline{\beta}-\alpha_1||\alpha_1-\beta|(X-\alpha_2)^2\\ &\quad +|\alpha_1-\alpha_2||\alpha_2-\beta||\beta-\alpha_1|(X-\beta)(X-\overline{\beta})\\ &= -i(\beta-\overline{\beta})(\alpha_2-\beta)(\alpha_2-\overline{\beta})(X-\alpha_1)^2\\ &\quad -i(\beta-\overline{\beta})(\alpha_1-\beta)(\alpha_1-\overline{\beta})(X-\alpha_2)^2\\ &\quad +(\alpha_1-\alpha_2)\sqrt{(\alpha_2-\beta)(\alpha_2-\overline{\beta})(\alpha_1-\beta)(\alpha_1-\overline{\beta})}(X-\beta)(X-\overline{\beta}).\end{aligned}$$

3. *Reduction of cubics*

3.1. *Invariants and covariants*

Let

$$g(X) = aX^3 + bX^2 + cX + d$$

be a cubic. We now regard the coefficients a, b, c, d as indeterminates, and the results and formulas which we obtain in this subsection will be valid over arbitrary fields whose characteristic is neither 2 nor 3. So let K_0 denote a prime field other than $\mathbb{F}_2$ or $\mathbb{F}_3$ and set $K = K_0(a, b, c, d)$, so that $g \in K[X]$. We will call K_0 and K the *constant field* and the *coefficient field* respectively.

3.1.1. Rational covariants

First we consider 'rational' invariants and covariants of g, which lie in K and $K[X]$ respectively. The only invariant of g is the discriminant

$$\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

(Strictly speaking, all invariants are constant multiples of powers of Δ.)

There are two seminvariants, in addition to Δ and the leading coefficient a, namely P and U where

$$P = b^2 - 3ac \qquad \text{and} \qquad U = 2b^3 + 27a^2d - 9abc.$$

Each seminvariant is the leading coefficient of a covariant of g: it is said to be the 'source' of the covariant (see [7]; the terminology is from [10]). The discriminant is a covariant of degree 0, and a is the source of g itself. P is the source of the Hessian covariant:

$$H(X) = (b^2 - 3ac)X^2 + (bc - 9ad)X + (c^2 - 3bd).$$

Finally, U is the source of a cubic covariant:

$$\begin{aligned}G(X) &= 3g(X)H'(X) - 2g'(X)H(X)\\ &= (2b^3 + 27a^2d - 9abc)X^3 + 3(b^2c + 9abd - 6ac^2)X^2\\ &\quad -3(bc^2 + 9acd - 6b^2d)X - (2c^3 + 27ad^2 - 9bcd).\end{aligned}$$

The seminvariants are related by the following syzygy:

$$4P^3 = U^2 + 27\Delta a^2, \qquad (8)$$

which extends to a syzygy between the covariants:

$$4H(X)^3 = G(X)^2 + 27\Delta g(X)^2. \qquad (9)$$

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

The Hessian and cubic covariants have the following discriminants:

$$\operatorname{disc}(H) = -3\Delta,$$
$$\operatorname{disc}(G) = 729\Delta^3.$$

Note that these are determined up to a constant multiple by the fact that they are clearly also invariants of g, hence powers of Δ, and the exponent is determined by their degree in the coefficients of g.

Finally, we may form the covariants of the cubic covariant $G(X)$; again, these are determined up to a scalar multiple by consideration of degrees:

$$H_G(X) = 27\Delta H(X),$$
$$G_G(X) = -729\Delta^2 g(X).$$

Note that the relation between $g(X)$ and $G(X)$ is almost symmetric; this will have interesting implications later.

3.1.2. Algebraic covariants

When we consider the reduction of real cubics with negative discriminant, and later when we consider quartics, we will need to make use of covariants whose coefficients are algebraic over the coefficient field $K = K_0(a, b, c, d)$. In the classical literature such covariants are called 'irrational covariants', but we prefer to call them 'algebraic covariants'. In almost all cases, the coefficients will lie in the splitting field of $g(X)$ over K; as with Julia's quadratic covariants given above, in the case of quartics with negative discriminant we need to make a further extension.

Our philosophy will to be use covariants which are defined over as small a field extension of K as possible, both for simplicity and for reasons of computational efficiency. For cubics, we only need to extend the coefficient field K by adjoining a root of the cubic.

Let α be a root of $g(X)$ in some algebraic closure of K, so that $K(\alpha)$ is an extension of K of degree 3. If $C(X) \in K(\alpha)[X]$ is an algebraic covariant of degree d, then its norm in $K[X]$ will be a rational covariant of degree $3d$, and hence can be expressed as a polynomial in the basic covariants g, H and G (not uniquely, on account of the syzygy relating these three). For example, if $C(X)$ is quadratic then its norm must be a K-linear combination of g^2, H^3 and G^2, and even a K_0-linear combination of Δg^2, H^3 and G^2 since its coefficients must be isobaric as polynomials in a, b, c, d. Using the syzygy this may be expressed uniquely as a linear combination of Δg^2 and G^2, say.

We apply this idea to the quadratic $\varphi(X)$ which Julia considers for real cubics with negative discriminant (signature $(1, 1)$) defined above in Subsection 2.2.2. Express $\varphi(X)$ in terms of the single root α, and scale for convenience, to obtain

$$J_2(X) = a^2\varphi(X) = h_0X^2 + h_1X + h_2; \tag{10}$$

a straightforward calculation with symmetric polynomials shows that

$$\begin{aligned} h_0 &= 9a^2\alpha^2 + 6ab\alpha + 6ac - b^2, \\ h_1 &= 6ab\alpha^2 + 6(b^2 - ac)\alpha + 2bc, \\ h_2 &= 3ac\alpha^2 + 3(bc - 3ad)\alpha + 2c^2 - 3bd. \end{aligned} \tag{11}$$

Let $S(X)$ be the norm of $J_2(X)$ from $K(\alpha)[X]$ to $K[X]$; a calculation shows that

$$S(X) = \operatorname{norm}(J_2(X)) = G^2 - 2H^3 = 2H^3 - 27\Delta g^2 = \frac{1}{2}(G^2 - 27\Delta g^2)$$

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

$$= J_2(X)J_4(X) \in K[X],$$

where $J_4(X) \in K(\alpha)[X]$ has degree 4. This purely symbolic calculation shows that the degree 6 rational covariant $S(X)$ factorizes over $K(\alpha)$ as the product of two algebraic covariants $J_2(X)$ and $J_4(X)$. Moreover, since $J_2(X)$ is a factor of the covariant $S(X)$, it follows immediately that $J_2(X)$ is itself a covariant of $g(X)$. We may also check that $J_2(X)$ and $J_4(X)$ are irreducible over $K(\alpha)$; the Maple package was used for this and all the algebraic computations in this paper.

We note for future reference that

$$\operatorname{disc}(J_2(X)) = 12\Delta = -4\operatorname{disc}(H(X)).$$

In the case of real cubics, this will mean that either $H(X)$ or $J_2(X)$ will be positive definite and can be used for reduction.

We will also later need to consider the J_2-covariant of the cubic $G(X)$. We first observe that $G(X)$ itself factorizes over $K(\alpha)$; in fact, $G(\alpha') = 0$ where

$$\alpha' = \frac{3d/\alpha + c}{3a\alpha + b}.$$

One can use this to compute the J_2-covariant of G directly, obtaining $-27\Delta J_2(X)$. However it is more elegant, and requires considerably less calculation, to proceed as follows.

Starting from the sextic covariant $S(X)$ of g, to compute the corresponding covariant for G we replace g, Δ, H by G, $729\Delta^3$ and $27\Delta H$ respectively, to obtain

$$2(27\Delta H)^3 - 27(729\Delta^3)G^2 = -3^9\Delta^3(G^2 - 2H^3) = -3^9\Delta^3 S.$$

Hence, up to a constant factor, $S(X) = G^2 - 2H^3$ is invariant under the transformation $g \mapsto G$. Since $J_2(X)$ is the unique quadratic factor of this sextic defined over $K(\alpha)[X]$ it follows that the J_2-covariant of G is indeed $-27\Delta J_2(X)$.

3.2. *Reduction of real cubics with $\Delta > 0$*

This is the simplest case. Let $g(X)$ be a real cubic with $\Delta > 0$ and three real roots α_1, α_2 and α_3. The Hessian $H(X)$ is real with negative discriminant -3Δ. Moreover, the leading coefficient of $H(X)$ is $P = b^2 - 3ac = \frac{1}{2}a^2\sum_{i<j}(\alpha_i - \alpha_j)^2$, and hence $P > 0$. Hence $H(X)$ is positive definite, and we make the following definition (following Hermite).

Definition 2. A real cubic with positive discriminant is *reduced* if and only if its Hessian is reduced in the usual sense.

We now find that the property of being reduced coincides for $g(X)$, its Hessian $H(X)$, and its cubic covariant $G(X)$.

Proposition 1. *Let $g(X)$ be a real cubic with positive discriminant. Then $g(X)$ is reduced if and only if its cubic covariant $G(X)$ is also reduced.*

Proof. $G(X)$ has discriminant $729\Delta^3 > 0$ and Hessian $-27\Delta H(X)$, so this is immediate. □

We now show that the seminvariants of a reduced cubic are bounded in terms of the discriminant.

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

Proposition 2. *Every real cubic with positive discriminant* Δ *is* $\mathrm{GL}(2,\mathbb{Z})$*-equivalent to one whose seminvariants are bounded as follows:*

$$0 < |a| \leqslant \frac{2}{3\sqrt{3}}\Delta^{1/4} \tag{12}$$

$$0 < P \leqslant \Delta^{1/2}. \tag{13}$$

Proof. It suffices to bound the seminvariants when $g(X)$ is reduced. Since $H(X)$ is reduced we have

$$0 < P \leqslant \sqrt{\frac{|\operatorname{disc}(H)|}{3}} = \sqrt{\Delta}$$

as required. Now the seminvariant syzygy (8) gives

$$27\Delta a^2 \leqslant 27\Delta a^2 + U^2 = 4P^3 \leqslant 4\Delta^{3/2},$$

so that a is also bounded as stated. Note that we also obtain the bound $0 < U \leqslant 2\Delta^{3/4}$. □

A reduction algorithm based on this definition is easy to implement; for integer cubics, only integer arithmetic is required. Both the translation and inversion steps are simply determined by inspection of the coefficients of the Hessian.

Algorithm 1. *Reduction of a real cubic with positive discriminant*

Input: a cubic $g(X) = aX^3 + bX^2 + cX + d \in \mathbb{R}[X]$ with $\Delta(g) > 0$.
Output: a reduced cubic $\mathrm{GL}(2,\mathbb{Z})$-equivalent to $g(X)$.

1. Let k be the nearest integer to
$$\frac{-(bc - 9ad)}{2(b^2 - 3ac)};$$
if this falls half-way between two integers, either choice will do.
2. Replace $g(X)$ by $g(X + k)$; that is,
$$(a, b, c, d) \leftarrow (a, 3ak + b, 3ak^2 + 2bk + c, g(k)).$$
3. If $b^2 - 3ac \leqslant c^2 - 3bd$ then output $g(X)$; else, replace $g(X)$ by $X^3 g(-1/X)$; that is,
$$(a, b, c, d) \leftarrow (d, -c, b, -a).$$
4. Go to step 1.

Now we turn to the question of listing all cubics with given positive discriminant. Given values of the seminvariants a and P, which must satisfy the syzygy condition that $4P^3 - 27\Delta a^2$ is a square, U^2; the value of U is determined up to sign, and we may easily write down a suitable cubic by setting $b = 0$, $c = -P/(3a)$ and $d = U/(27a^2)$. If we are seeking integral cubics with a given positive integer discriminant Δ, however, it is better to proceed a little differently. Since the unimodular substitution of $X + \alpha$ for X changes the cubic coefficients from $(a, b, \ldots)$ to $(a, b + 3\alpha a, \ldots)$ we may assume that $-3a/2 < b \leqslant 3a/2$ for fixed a; then for fixed a, b the bounds on P give bounds on c. This results in the following algorithm.

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

Algorithm 2. *To list all integer cubics with given positive integer discriminant* Δ*, up to* $\mathrm{GL}(2,\mathbb{Z})$*-equivalence*

Input: a positive integer Δ.
Output: a list of reduced cubics $g(X)$ with discriminant Δ, including exactly one in each $\mathrm{GL}(2,\mathbb{Z})$-orbit.

1. Loop on a: $1 \leqslant a \leqslant \frac{2}{3\sqrt{3}}\Delta^{1/4}$.
2. Loop on b: $-3a/2 < b \leqslant 3a/2$.
3. Loop on c: $(b^2 - \Delta^{1/2})/(3a) < c \leqslant b^2/(3a)$.
4. Set $P = b^2 - 3ac$; test if $4P^3 - 27\Delta a^2$ is a square, say U^2; continue if not.
5. Given U, test if $d = (U - 2b^3 + 9abc)/(27a^2)$ is integral; continue if not.
6. Reduce the cubic with coefficients (a, b, c, d) using Algorithm 1, output the result, and continue.

Note that we may assume that $a > 0$ since $g(-X)$ is $\mathrm{GL}(2,\mathbb{Z})$-equivalent to $g(X)$. Similarly, we do not have to test both signs of U in step 5, since replacing $g(X)$ by $-g(-X)$ changes the signs of b, d and U.

The triple loop on (a, b, c) can be made very efficient by the use of a quadratic sieve based on the seminvariant syzygy (8). Given Δ one precomputes, for each of a set of suitable moduli m, the pairs (a mod m, P mod m) for which $4P^3 - 27\Delta a^2$ is a square modulo m. This can be stored as a 2-dimensional array of $\{0, 1\}$-valued flags $f_m[i, j]$, with indices running from 0 to $m - 1$, such that

$$f_m[i, j] = 1 \Leftrightarrow 4j^3 - 27\Delta i^2 \quad \text{is a square modulo } m.$$

Then we can program the loop in such a way as to skip quickly past triples (a, b, c) for which there exists a modulus m such that $f_m[a \bmod m, (b^2 - 3ac) \bmod m] = 0$.

One can also adapt this procedure to list all integer cubics whose discriminant is positive but less than a given bound. With care, it is possible to ensure that the cubics listed determine distinct cubic number fields. For details of this, see the paper of Belabas [**2**].

Next we give a comparison of the bounds in Proposition 2 with those of Julia in [**12**]. We have already mentioned that Julia's covariant quadratic $\varphi(X)$ is (up to a constant factor) the Hessian $H(X)$ in this case. However, Julia obtains the weaker bound

$$|a| \leqslant \frac{2\sqrt{2}}{3\sqrt{3}}|\Delta|^{1/4}$$

for the leading coefficient of a reduced cubic. The reason for this is that Julia applies the AGM (Arithmetic-Geometric Mean) inequality to the three positive real numbers

$$t_1^2 = (\alpha_2 - \alpha_3)^2, \quad t_2^2 = (\alpha_3 - \alpha_1)^2, \quad t_3^2 = (\alpha_1 - \alpha_2)^2,$$

to give

$$3(t_1^2 t_2^2 t_3^2)^{1/3} \leqslant t_1^2 + t_2^2 + t_3^2.$$

Now, $\mathrm{disc}(\varphi) = 12t_1^2t_2^2t_3^2 = 12a^{-4}\Delta$, and the leading coefficient of $\varphi(X)$ is $t_1^2 + t_2^2 + t_3^2$. Hence the assumption that $\varphi(X)$ is reduced gives the inequality $t_1^2 + t_2^2 + t_3^2 \leqslant 2a^{-2}\Delta^{1/2}$, and one obtains the bound on a stated above. However, the standard AGM inequality is not the best possible for three positive real numbers t_i^2 for which $t_1 + t_2 + t_3 = 0$. It is possible to improve it by a factor of $\sqrt[3]{2}$, as in the following lemma.

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

Lemma 1. *Let t_1, t_2 and t_3 be real numbers such that $t_1 + t_2 + t_3 = 0$. Then*

$$3(2t_1^2t_2^2t_3^2)^{1/3} \leqslant t_1^2 + t_2^2 + t_3^2.$$

Proof. From $t_1 + t_2 + t_3 = 0$ we deduce the identity

$$(t_1^2 + t_2^2 + t_3^2)^3 - 54t_1^2t_2^2t_3^2 = 2(t_1 - t_2)^2(t_2 - t_3)^2(t_3 - t_1)^2$$

from which the result follows. □

Using this lemma instead of the usual AGM inequality we obtain the bound on a of Proposition 2. In fact, one can see that the identity in the proof of the lemma is nothing other than the seminvariant syzygy applied to the cubic $\prod(X - t_i)$.

Finally, we compare our bounds with the results given in [**4**, Section II.5]. A 1943 theorem of Mordell states (in effect) that given a real cubic f with positive discriminant Δ, there is a cubic $\mathrm{GL}(2, \mathbb{Z})$-equivalent to f with leading coefficient a satisfying

$$|a| \leqslant \left(\frac{\Delta}{49}\right)^{1/4},$$

which is best possible since $x^3 + x^2 - 2x - 1$ has $\Delta = 49$. Now the constant appearing here is $1/\sqrt{7} = 0.3780$, which is slightly smaller than the constant $2/3\sqrt{3} = 0.3849$ which appears in our bound (13). However, Mordell's theorem does not state that the equivalent cubic which minimizes the leading coefficient is actually reduced, so that one cannot deduce, as we did above, that the seminvariant P is simultaneously bounded. A related result of Davenport (1945) states that if $f(X, Y)$ is a reduced cubic form with positive discriminant Δ, then

$$\min\{f(1, 0), f(0, 1), f(1, 1), f(1, -1)\} \leqslant \left(\frac{\Delta}{49}\right)^{1/4}$$

which again implies Mordell's theorem, but is not quite sufficient for our purposes.

3.3. *Reduction of real cubics with $\Delta < 0$*

Now the cubic $g(X)$ has a single real root α and complex roots β, $\overline{\beta}$. Since $\mathrm{disc}(H) = -3\Delta > 0$, we cannot use the Hessian for reduction. The approach of Belabas, following Mathews and Berwick [**13**] (which predates Julia [**12**]), and Davenport is to use the positive definite quadratic $(X - \beta)(X - \overline{\beta})$, defining g to be reduced if this quadratic is reduced. Davenport calls this being 'Minkowski-reduced'. This leads to the bound

$$|a| \leqslant \frac{2}{3^{3/4}}|\Delta|^{1/4} \approx 0.877|\Delta|^{1/4}$$

for a Minkowski-reduced cubic (see [**2**]). We will instead follow Julia, giving an alternative definition of reduction using the algebraic quadratic covariant $J_2(X)$ introduced above, from which we will obtain the improved bound

$$|a| \leqslant \frac{2\sqrt{2}}{3\sqrt{3}}|\Delta|^{1/4} \approx 0.544|\Delta|^{1/4}$$

for a Julia-reduced cubic.

As in the previous subsection, we can compare our results with those of Davenport, who showed in 1945 that for a Minkowski-reduced cubic $f(X, Y)$,

$$\min\{f(1, 0), f(0, 1), f(1, 1), f(1, -1)\} \leqslant \left|\frac{\Delta}{23}\right|^{1/4}.$$

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

So every cubic with $\Delta < 0$ is equivalent to one whose leading coefficient satisfies

$$|a| \leqslant \left|\frac{\Delta}{23}\right|^{1/4},$$

which again is best possible since $x^3 - x - 1$ has discriminant -23. The constant here is 0.4566 which is smaller than ours, but again since the form which minimizes the leading coefficient is not necessarily the reduced form, we cannot deduce bounds on the other seminvariants (and hence on the other coefficients) as we need to.

We use the real root α of $g(X)$ to define $J_2(X)$ as in (10) and (11). Since α is real and $\Delta < 0$, we see that $J_2(X)$ is real and positive definite: its discriminant 12Δ is negative, and its leading coefficient is $h_0 = a^2(|\beta - \overline{\beta}|^2 + 2|\alpha - \beta|^2)$, which is positive. (Alternatively, h_0 has norm $\frac{1}{2}(U^2 - 27\Delta a^2) > 0$, and the other two conjugates of h_0 are complex conjugates of each other, and hence their product is positive.)

Hence we make the following definition.

Definition 3. A real cubic $g(X)$ with negative discriminant is *reduced* if and only if the positive definite quadratic $J_2(X)$ is reduced.

Since the cubic covariant $G(X)$ has the same J_2-covariant as $g(X)$, up to a constant factor, and its discriminant $729\Delta^3$ has the same sign as Δ, the following proposition is now immediate.

Proposition 3. *Let $g(X)$ be a real cubic with negative discriminant. Then $g(X)$ is reduced if and only if its cubic covariant $G(X)$ is also reduced.*

Now we are able to derive bounds on the seminvariants of a reduced cubic with negative discriminant.

Proposition 4. *Let $g(X)$ be a real cubic with negative discriminant which is reduced. Then the following inequalities hold:*

$$0 < |a| \leqslant \frac{2\sqrt{2}}{3\sqrt{3}}|\Delta|^{1/4};$$
$$0 < |P| \leqslant 2^{1/3}|\Delta|^{1/2}.$$

Proof. To bound a we follow Julia. Using

$$a^{-2}h_0 = |\beta - \overline{\beta}|^2 + 2|\alpha - \beta|^2$$

and

$$|\Delta| = a^4|\beta - \overline{\beta}|^2|\alpha - \beta|^4,$$

the AGM inequality gives $(a^{-4}|\Delta|)^{1/3} \leqslant \frac{1}{3}a^{-2}h_0$, so that $27a^2|\Delta| \leqslant h_0^3$. On the other hand, since $J_2(X)$ is reduced, we have $3h_0^2 \leqslant |\operatorname{disc}(J_2(X))| = 12|\Delta|$, so that $h_0^2 \leqslant 4|\Delta|$. Combining these gives the stated inequality on a.

Now $G(X)$ is also reduced, by the preceding proposition, so applying what we have just proved to $G(X)$ we obtain

$$U^2 \leqslant \frac{8}{27}\left|729\Delta^3\right|^{1/2} = 8|\Delta|^{3/2}.$$

The syzygy now gives

$$4P^3 = U^2 + 27\Delta a^2 \leqslant U^2$$

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

(since $\Delta < 0$), so we obtain

$$P^3 \leqslant 2|\Delta|^{3/2},$$

which is the upper bound for P. For the lower bound,

$$4P^3 = U^2 + 27\Delta a^2 \geqslant 27\Delta a^2 \geqslant 27\Delta\frac{8}{27}|\Delta|^{1/2} = -8|\Delta|^{3/2},$$

so that $P^3 \geqslant -2|\Delta|^{3/2}$. □

Remark 1. Note that Julia's bound on a is the same in both cases (positive and negative discriminant); we improved the bound by a factor of $\sqrt{2}$ in the positive case, but the same trick does not work in the negative case, as the non-real roots prevent us from applying the improved form of the AGM inequality.

The algorithm for listing all integral cubics with given negative discriminant Δ, up to $\mathrm{GL}(2,\mathbb{Z})$-equivalence, is almost identical to Algorithm 2 for the positive case. We merely have to replace the upper bound on the loop on a by an upper bound on $|a|$ of $((2\sqrt{2})/(3\sqrt{3}))|\Delta|^{1/4}$, and the lower bound on the loop on c by $(b^2 - 2^{1/3}|\Delta|^{1/2})/(3a)$.

To adapt Algorithm 1 requires more work, since we first compute the real root α of the given cubic. Then we define h_0, h_1 and h_2 as in (11). In the translation step we use the nearest integer to $-h_1/2h_0$ as k, and must remember to replace α by $\alpha - k$ as well as changing the coefficients. The inversion step takes place if $h_0 > h_2$, and we then replace α by $-1/\alpha$. If several steps are needed in the reduction, we will gradually lose precision in our (necessarily approximate) value of the real root α. This should be avoided, either by recomputing the root from the new coefficients every few steps, or by refining the root by replacing α by $\alpha - g(\alpha)/g'(\alpha)$.

It is possible to express the reduction criterion in terms which do not require knowing an explicit value for the real root α. The cubic is reduced if and only if $-h_0 \leqslant h_1 \leqslant h_0 \leqslant h_2$, which is if and only if the three quantities $h_2 - h_0$, $h_0 - h_1$ and $h_0 + h_1$ are non-negative. Now each of these quantities has two other conjugates, which are complex conjugates and hence whose product is positive; so an equivalent condition is that the three norms $N(h_2 - h_0)$, $N(h_0 - h_1)$ and $N(h_0 + h_1)$ should be non-negative. These norms are the following polynomials:

$$\begin{aligned}
C_1 = N(h_2 - h_0) = {} & -108b^3a^2d - 3b^4c^2 + 54a^2c^4 + 18b^5d + 243a^2d^2b^2 - 54b^3cad \\
& -162bc^2a^2d - 54a^3c^3 + 486a^3dcb + 3c^4b^2 - 18c^5a \\
& -243d^2a^2c^2 + 54c^3abd + 162d^2ab^2c + 2c^6 - 2b^6 - 729a^4d^2 \\
& +729d^4a^2 + 54b^3d^3 + 18b^4ac - 27a^2b^2c^2 + 108c^3d^2a \\
& -18c^4db + 27d^2c^2b^2 - 486d^3acb - 54d^2b^4;
\end{aligned}$$

$$\begin{aligned}
C_2 = N(h_0 - h_1) = {} & (108b^3a^2d - 12b^4c^2 + 216a^2c^4 \\
& +72b^5d + 972a^2d^2b^2 - 216b^3cad - 648bc^2a^2d + 54a^3c^3 \\
& -486a^3dcb + 2b^6 + 729a^4d^2 - 18b^4ac + 27a^2b^2c^2) \\
& +2(-108d^2b^3a + 45ac^2b^3 + 243a^3c^2d - 135a^2c^3b \\
& -81ab^4d - 729a^3bd^2 - 3b^5c + 8c^3b^3 + 324a^2b^2dc \\
& -36db^4c - 36c^4ba - 108dc^3a^2 + 216db^2ac^2);
\end{aligned}$$

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

$$\begin{aligned} C_3 = N(h_0 + h_1) = (&108b^3a^2d - 12b^4c^2 + 216a^2c^4 \\ &+72b^5d + 972a^2d^2b^2 - 216b^3cad - 648bc^2a^2d + 54a^3c^3 \\ &-486a^3dcb + 2b^6 + 729a^4d^2 - 18b^4ac + 27a^2b^2c^2) \\ &-2(-108d^2b^3a + 45ac^2b^3 + 243a^3c^2d - 135a^2c^3b \\ &-81ab^4d - 729a^3bd^2 - 3b^5c + 8c^3b^3 + 324a^2b^2dc \\ &-36db^4c - 36c^4ba - 108dc^3a^2 + 216db^2ac^2). \end{aligned}$$

Use of these formulas does give us exact integral conditions for an integer cubic to be reduced, and even a possible reduction procedure: invert if $C_1 < 0$, replace $g(X)$ by $g(X+1)$ until $C_3 \geqslant 0$, replace $g(X)$ by $g(X-1)$ until $C_2 \geqslant 0$, then repeat. Apart from the complicated nature of these expressions, however, there is a more serious drawback here: we cannot compute directly from the initial values of C_2 and C_3 the integer value of k such that $g(X+k)$ has positive C_2 and C_3, only its sign. Since in practice we may require a very large value of k, it is clearly most inefficient to carry out the shift in unit steps. (M. Stoll has pointed out to us that one can in fact reduce the number of steps to the order of $\log_2(k)$ by repeatedly doubling the step size until overshooting, and then reversing direction. We leave the details as an exercise to the reader.) Hence it is more efficient in practice to compute the real root α, so that we can compute k directly.

A similar criticism can be applied to the reduction procedure proposed by Mathews in [**13**]: the condition that the covariant $(X-\beta)(X-\overline{\beta})$ is reduced is expressed there as equivalent to the three inequalities

$$\begin{aligned} C_1 &= d(d-b) + a(c-a) \geqslant 0; \\ C_2 &= ad - (a+b)(a+b+c) \leqslant 0; \\ C_3 &= ad + (a-b)(a-b+c) \geqslant 0. \end{aligned}$$

While this is simple to use in practice, we encounter the same drawback when a large shift is required.

Finally, we present some comparisons between the reduction defined here, following Julia, and the reduction of Mathews/Belabas.

Experiment shows that in many cases the only difference between the Julia reduction of an integer cubic and its Mathews reduction is a shift in the variable. For example, cubics of the form $g(X) = X^3 + d$, which have negative discriminant $-27d^2$, are always Julia-reduced, while their Mathews reduction is $g(X+k)$ where $k = [(1+\sqrt[3]{d})/2]$, since we then shift so that the non-real roots have real part less than $1/2$. For instance, the Mathews reduction of $X^3 + 1000$ is $X^3 + 15X^2 + 75X + 1125$.

In [**2**], a report is given of an enumeration of all cubic fields with discriminant less than 10^{11} in absolute value. In the complex case ($\Delta < 0$), the bound on the leading coefficient a used there was

$$\left[\left(\frac{16 \cdot 10^{11}}{27}\right)^{1/4}\right] = 493.$$

By comparison, our bound for a is

$$\left[\left(\frac{64 \cdot 10^{11}}{729}\right)^{1/4}\right] = 306.$$

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

It would be interesting to compare the running time of approximately 25.5 days given in [2] with the time needed using this lower bound. Belabas estimates (as stated in a personal communication to the author) that the difference would not be very great, since most of the running time in his program is accounted for by the small values of a, since for larger values of a the inner loops are very short. Full references to the Davenport (1945) and Mordell (1943) results are given in Cassels' book [4].

4. *Reduction of quartics*

As with cubics, we start by a purely algebraic account of the invariants and covariants of a quartic, including algebraic covariants. See [7] for a brief summary of the relevant classical invariant theory for quartics.

4.1. *Invariants and covariants*

Let

$$g(X) = aX^4 + bX^3 + cX^2 + dX + e \tag{14}$$

be a quartic. As with cubics, we regard the coefficients a, b, c, d, e as indeterminates, and the results and formulas which we obtain in this subsection will be valid over arbitrary fields whose characteristic is neither 2 nor 3. Let K_0 again denote a prime field other than $\mathbb{F}_2$ or $\mathbb{F}_3$ and set $K = K_0(a, b, c, d, e)$, so that $g \in K[X]$.

4.1.1. Rational invariants and covariants

We first consider rational invariants and covariants of g. The invariants form a graded ring, generated by two invariants of weights 4 and 6 which are conventionally denoted I and J:

$$I = 12ae - 3bd + c^2, \tag{15}$$

$$J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3. \tag{16}$$

These are algebraically independent, and every invariant is an isobaric polynomial in I and J. We will denote the invariant $4I^3 - J^2$ by Δ, and refer to it as the discriminant; this is in fact 27 times the usual discriminant Δ_0 of g:

$$\Delta = 4I^3 - J^2 = 27\Delta_0, \tag{17}$$

$$\begin{aligned}\Delta_0 = {} & 256a^3e^3 - 4b^3d^3 - 128a^2c^2e^2 - 192a^2bde^2 - 6ab^2d^2e - 80abc^2de \\ & + 16ac^4e + b^2c^2d^2 - 27(a^2d^4 + b^4e^2) + 2c(9bd + 72ae - 2c^2)(ad^2 + b^2e).\end{aligned} \tag{18}$$

The seminvariants of g (which are just the leading coefficients of covariants) are the invariants I and J, and the leading coefficient a, together with the following:

$$H = 8ac - 3b^2; \tag{19}$$

$$R = b^3 + 8a^2d - 4abc; \tag{20}$$

$$Q = \frac{1}{3}(H^2 - 16a^2I) = 3b^4 - 16ab^2c + 16a^2c^2 + 16a^2bd - 64a^3e. \tag{21}$$

These are denoted $-p$ and r respectively in [7]; the notation for I and J is classical and standard, while H is used in [3]. The seminvariants I, J, a, H, R are related by the following syzygy:

$$H^3 - 48Ia^2H + 64Ja^3 = -27R^2. \tag{22}$$

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

The (non-constant) rational covariants of g are $g(X)$ itself, with leading coefficient a, a quartic covariant $g_4(X)$ with leading coefficient $-H$:

$$g_4(X) = (3b^2 - 8ac)X^4 + 4(bc - 6ad)X^3 + 2(2c^2 - 24ae - 3bd)X^2 + 4(cd - 6be)X + (3d^2 - 8ce), \tag{23}$$

and a sextic covariant $g_6(X)$ with leading coefficient R:

$$\begin{aligned} g_6(X) = {} & (b^3 + 8a^2d - 4abc)X^6 + 2(16a^2e + 2abd - 4ac^2 + b^2c)X^5 \\ & + 5(8abe + b^2d - 4acd)X^4 + 20(b^2e - ad^2)X^3 \\ & - 5(8ade + bd^2 - 4bce)X^2 - 2(16ae^2 + 2bde - 4c^2e + cd^2)X \\ & - (d^3 + 8be^2 - 4cde). \end{aligned} \tag{24}$$

The syzygy between the seminvariants extends to a syzygy between the covariants:

$$g_4^3 - 48Ig^2g_4 - 64Jg^3 = 27g_6^2. \tag{25}$$

All rational covariants are polynomials in I, J, g, g_4 and g_6 with constant coefficients; in particular, there is no rational quadratic covariant of a quartic, as there was for a cubic. We will therefore always need to extend the base field in order to find a suitable quadratic covariant for reduction purposes.

Since $g_4(X)$ is again a quartic, we may look at its invariants and covariants. These are easily identifiable, as they are also covariants of g itself. We summarize the results in Proposition 5, which is trivial to verify using algebraic manipulation. We include some algebraic in- and covariants which will be defined in the next subsection.

Proposition 5. *The invariants, seminvariants and covariants of the quartic covariant $g_4(X)$ are as follows.*

$g(X)$	$g_4(X)$
I	2^4I^2
J	$2^6(2I^3 - J^2)$
Δ	$2^{12}J^2\Delta$
a	$-H$
H	$2^4(4aJ - HI)$
R	2^6JR
$g_4(X)$	$-2^4(I\,g_4(X) + 4J\,g(X))$
$g_6(X)$	$2^6J\,g_6(X)$
φ	$4(\varphi^2 - 2I)$
z	$16(\varphi^2 - 3I)z$
$H(X)$	$4\sqrt{\varphi^2 - 3I}\,H(X)$
$G(X)$	$-16\varphi\sqrt{\varphi^2 - 3I}\,G(X)$

4.1.2. Algebraic invariants and covariants

For fixed I and J, every quartic with these invariants has a splitting field which contains the splitting field of the so-called *resolvent cubic* equation $F(X) = 0$, where

$$F(X) = X^3 - 3IX + J, \tag{26}$$

which has discriminant $27\Delta = 27(4I^3 - J^2)$. We will denote by φ a generic root of $F(X)$, so that $\varphi^3 = 3I\varphi - J$. This quantity φ is an algebraic invariant of g: if g is transformed

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

by a linear substitution of determinant δ, so that I and J are transformed into $\delta^4 I$ and $\delta^6 J$ respectively, then clearly φ is transformed into $\delta^2\varphi$; thus, φ has weight 2.

Note that φ is absolutely invariant under unimodular transformations (with determinant ± 1), and that the cubic resolvent field $K(\varphi)$ is itself invariant. It will therefore be advantageous to use covariants defined over $K(\varphi)$ where possible; we will see, in fact, that this is possible for real quartics with positive discriminant, while reduction of real quartics with negative discriminant will require a further extension of the coefficient field.

We note in passing that there is a close connection between the three values of φ and the four roots of $g(X)$. This is the basis for one classical method of solving quartics by radicals. Denote the roots of $g(X)$ by x_i for $1 \leqslant i \leqslant 4$, and set $z = (4a\varphi - H)/3$. Letting φ run through the three roots of $F(X)$ we obtain three values of z, say z_j for $1 \leqslant j \leqslant 3$. Then we have

$$z_1 = a^2(x_1 + x_2 - x_3 - x_4)^2, \tag{27}$$

with similar expressions for z_2 and z_3, and conversely,

$$4ax_i + b = \pm\sqrt{z_1} \pm \sqrt{z_2} \pm \sqrt{z_3}, \tag{28}$$

where the four values are obtained by taking any choice of signs such that the three square roots multiply to $+R$ as opposed to $-R$. Note that the seminvariant syzygy (22) gives

$$z_1 z_2 z_3 = \prod(4a\varphi - H)/3 = R^2. \tag{29}$$

When $R = 0$, one of the values of φ is rational, and one value of z is zero; then (28) only gives four values.

This quantity z is an algebraic seminvariant, and will appear repeatedly below; its minimal polynomial is

$$\left(\frac{4a}{3}\right)^3 F\left(\frac{3Z + H}{4a}\right) = Z^3 + HZ^2 + QZ - R^2,$$

whose coefficients are rational seminvariants. Moreover, z is the leading coefficient of the algebraic covariant $\frac{1}{3}(g_4(X) + 4\varphi g(X))$, of degree 4. This quartic is in fact the square of a quadratic, a property which characterizes φ as a root of the resolvent cubic. (See [**11**, pp.73–76] for how to use this to give an alternative method of solving quartic equations, noting that Hilbert's notation is not quite the same as ours.)

It is more convenient for us to approach the quadratic algebraic covariants, which we have just seen arise as the square roots of $\frac{1}{3}(g_4(X) + 4\varphi g(X))$, in a different way. If there is a quadratic covariant defined over the cubic resolvent field $K(\varphi)$, then its norm (from $K(\varphi)$ to K) is a rational sextic covariant, and hence must equal $g_6(X)$ up to a constant factor. So we are led to consider the factorization of $g_6(X)$ in $K(\varphi)[X]$. Using Maple, we find the following factorization:

$$g_6(X) = H(X)G(X) = z^{-1}H_1(X)G_1(X), \tag{30}$$

where $H_1(X) = \sqrt{z}H(X)$ and $G_1(X) = \sqrt{z}G(X)$ are irreducible polynomials in $K(\varphi)[X]$ of degrees 2 and 4 respectively. Explicitly,

$$H_1(X) = \frac{1}{36}\left(g_4''(X) + 4g''(X)\varphi + 8(I - \varphi^2)\right) \tag{31}$$

and

$$G_1(X) = \frac{1}{90}\left(20g'(X)\varphi^2 - 5g_4'(X)\varphi + 3g_6''(X) - 40Ig'(X)\right). \tag{32}$$

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

The polynomials $H_1(X)$ and $G_1(X)$ are simpler to use than $H(X)$ and $G(X)$, since they are defined over the cubic extension $K(\varphi)$ instead of the degree 6 extension $K(\sqrt{z})$, but they suffer two disadvantages. First, they are not truly covariant, although we will see that this does not matter greatly in practice. Secondly, it may happen (when $R = 0$) that one value of z is zero, in which case both $H_1(X)$ and $G_1(X)$ are identically zero. In fact, for real quartics with positive discriminant we will see that we can avoid this case, since then $H(X)$ is positive definite for a unique choice of φ which is *not* the value for which $z = (4a\varphi - H)/3 = 0$. Then we could use $H_1(X)$ just as well as $H(X)$ for reduction purposes. But for real quartics with negative discriminant, when we will need to use $G(X)$, the case $z = 0$ can occur and must be allowed for.

An alternative expression for $H(X)$ and its other two conjugates may be obtained by factorizing $g_6(X)$ over the splitting field $K(x_1, x_2, x_3, x_4)$ of $g(X)$. One finds

$$g_6(X) = H^{(1)}(X)H^{(2)}(X)H^{(3)}(X)$$

where $H^{(1)}(X)$ is given by

$$a((x_1 + x_2 - x_3 - x_4)X^2 + 2(x_3x_4 - x_1x_2)X + (x_1x_2(x_3 + x_4) - x_3x_4(x_1 + x_2)))$$

and $H^{(2)}(X)$ and $H^{(3)}(X)$ are defined similarly. Comparing with (27), we see that $H(X)$ has leading coefficient $\sqrt{z}$, and it is easy to verify that $H^{(1)}(X)$ is the same as $H(X)$.

We will occasionally use the notation $H_\varphi(X)$ instead of $H(X)$, in order to make the dependence on φ explicit.

For future reference, we note the following formulas, which are all proved easily by algebraic manipulation.

Proposition 6. *Let φ be a root of $F(X) = X^3 - 3IX + J$, with φ' and φ'' its conjugates. Then the following hold.*

(i) $\varphi^2 - 3I = \varphi'\varphi'' = -J/\varphi$.

(ii) $\varphi^2 - I = \frac{1}{3}(\varphi - \varphi')(\varphi - \varphi'')$.

(iii) $\varphi^2 - 4I = -\frac{1}{3}(\varphi' - \varphi'')^2$.

(iv) $-\Delta = (\varphi^2 - 4I)(\varphi^2 - I)^2$.

(v) $27\Delta = [(\varphi - \varphi')(\varphi' - \varphi'')(\varphi'' - \varphi)]^2$.

The algebraic covariant $H(X)$ has the following properties.

(vi) $H(X)^2 = \frac{1}{3}(g_4(X) + 4\varphi g(X))$.

(vii) $H(X)H^{(2)}(X)H^{(3)}(X) = g_6(X)$.

(viii) *The leading coefficient of $H(X)$ is $\sqrt{z}$.*

(ix) $\operatorname{disc}(H(X)) = \frac{4}{3}(\varphi^2 - I) = \frac{4}{9}(\varphi - \varphi')(\varphi - \varphi'')$.

4.2. *Classification of real quartics*

Let $g(X) = aX^4 + bX^3 + cX^2 + dX + e$ denote a quartic with real coefficients. Following [3], we classify real quartics into three 'types' according to their signature (r_1, r_2), where r_1 is the number of real roots and r_2 is the number of conjugate pairs of non-real complex roots, so that $r_1 + 2r_2 = 4$. These types can be distinguished by the signs of the discriminant Δ and of the seminvariants H and Q. We summarize this in the following proposition, which also serves as the definition of the three types.

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

Proposition 7. *Let $g(X) = aX^4 + bX^3 + cX^2 + dX + e \in \mathbb{R}[X]$ be a real quartic with distinct roots.*

Type 1. *If $\Delta > 0$ and either $H > 0$ or $Q < 0$, then $g(X)$ has no real roots, signature* $(0, 2)$.

Type 2. *If $\Delta > 0$, $H < 0$ and $Q > 0$, then $g(X)$ has* 4 *real roots, signature* $(4, 0)$.

Type 3. *If $\Delta < 0$, then $g(X)$ has* 2 *real roots, signature* $(2, 1)$.

Proof. This is a standard exercise (see [6, Exercise 1 on page 217], but note that the result there is not stated correctly). In the case $\Delta > 0$, all cases are covered, since it is impossible to have either $H = 0$ and $Q > 0$, or $H < 0$ and $Q = 0$. This follows from the following identity:

$$4096a^6\Delta_0 = -27R^4 + 4H^3R^2 - 18R^2HQ + H^2Q^2 - 4Q^3.$$

□

Consider further the case $\Delta > 0$ (Types 1 and 2). Since the resolvent cubic $F(X)$ has discriminant Δ, it has three real roots in this case, which we denote φ_i for $1 \leqslant i \leqslant 3$. We will always order these so that

$$4a\varphi_1 > 4a\varphi_2 > 4a\varphi_3. \tag{33}$$

Since $\prod(H - 4a\varphi) = -27R^2 \leqslant 0$, we can distinguish between Types 1 and 2 according to the interval in which H lies. For Type 1, we have

$$4a\varphi_1 \geqslant H \geqslant 4a\varphi_2 > 4a\varphi_3, \tag{34}$$

(or $z_1 \geqslant 0 \geqslant z_2 > z_3$), while for Type 2 we have

$$4a\varphi_1 > 4a\varphi_2 > 4a\varphi_3 \geqslant H \tag{35}$$

(or $z_1 > z_2 > z_3 \geqslant 0$).

Similarly, when $\Delta < 0$ (Type 3) there is only one real value of φ, and the same syzygy now gives

$$4a\varphi \geqslant H \tag{36}$$

(or $z \geqslant 0$).

Remark 2. For fixed values of the invariants I and J, if $\Delta > 0$ then the real quartics with invariants I and J lie in three orbits under the action of $\mathrm{SL}(2, \mathbb{R})$: Type 1 with $a > 0$ (positive definite), Type 1 with $a < 0$ (negative definite), and Type 2 (indefinite). If $\Delta < 0$ there is just one orbit.

Remark 3. In applications to 2-descent on elliptic curves, we are only interested in quartics $g(X)$ for which the equation $Y^2 = g(X)$ has real solutions. We then ignore quartics of Type 1 with $a < 0$, and $\mathrm{SL}(2, \mathbb{R})$ acts transitively on the remaining quartics of each relevant type.

4.3. *Reduction of real quartics with $\Delta > 0$*

For real quartics with positive discriminant, we will be able to use the algebraic covariant quadratic $H_\varphi(X)$ for reduction, provided that we can choose the value of φ so that $H_\varphi(X)$ is definite. We are able to treat simultaneously here both the relevant types of quartic (Types 1 and 2), in contrast with Julia [12] and Birch and Swinnerton-Dyer [3], who deal with these quite separately.

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

Let φ denote any of the three roots of $F(X)$, which are all real, and denote the other two roots by φ' and φ''. As before, we set $z = (4a\varphi - H)/3$. Recall that $H(X) = H_\varphi(X)$ is the quadratic factor of $g_6(X)$ in $K(\sqrt{z})[X]$, with leading coefficient $\sqrt{z}$ and discriminant $\frac{4}{3}(\varphi^2 - I) = \frac{4}{9}(\varphi - \varphi')(\varphi - \varphi'')$.

If $H = 4a\varphi$, then $z = 0$ and $H(X)$ degenerates to a linear polynomial (proportional to $4aX + b$) which is certainly not positive definite.

If $H < 4a\varphi$, so that $z > 0$, then $H(X)$ has a positive leading coefficient, and will have negative discriminant provided that φ lies *between* φ' and φ''. This implies that $g(X)$ must be a Type 2 quartic, with $4a\varphi_1 > 4a\varphi_2 > 4a\varphi_3 > H$ and $\varphi = \varphi_2$.

On the other hand, if $H > 4a\varphi$ then $z < 0$ so that $H(X)$ is not real, but in this case $H_1(X) = \sqrt{z}H(X)$ is real and will be positive definite provided that $(\varphi - \varphi')(\varphi - \varphi'') > 0$. For this, φ must be one of the outer roots. Then $4a\varphi_1 > H > 4a\varphi_2 > 4a\varphi_3$, with $\varphi = \varphi_3$, and $g(X)$ has Type 1.

We have thus proved the following proposition. Observe that in each case, there is a unique choice of φ which gives a positive definite quadratic.

Proposition 8. *Let $g(X)$ be a real quartic with positive discriminant Δ and leading coefficient a. Order the roots φ_i of the resolvent cubic $F(X)$ as before, with $4a\varphi_1 > 4a\varphi_2 > 4a\varphi_3$. Set*

(i) *$\varphi = \varphi_3$, and $h(X) = -H_1(X) = -\sqrt{z}H_\varphi(X)$, if $g(X)$ has Type 1;*

(ii) *$\varphi = \varphi_2$, and $h(X) = H_1(X) = \sqrt{z}H_\varphi(X)$, if $g(X)$ has Type 2.*

Then $h(X)$ is a positive definite real quadratic, which is a covariant of $g(X)$ up to the positive constant factor $\sqrt{|z|}$. It is the unique positive definite quadratic factor of the covariant $g_6(X)$ in each case.

This proposition enables us to define a reduced quartic in the positive discriminant case.

Definition 4. A real quartic $g(X)$ with positive discriminant is *reduced* if and only if the positive definite quadratic $h(X)$, defined in Proposition 8, is reduced.

Before we proceed to derive bounds on the coefficients of a reduced quartic, we record the fact that these covariant quadratics are in fact the same as those used by both Julia in [**12**] and Birch and Swinnerton-Dyer in [**3**] (see Subsection 2.2.4), up to unimportant constant factors. Note that we have been able to give essentially the *same* definition of the covariant quadratic $h(X)$ in these two cases, while the expressions used by the previous authors look totally different for quartics of Types 1 and 2.

Proposition 9. *The positive definite quadratic covariants associated to a real quartic with positive discriminant in Proposition 8 are equal to those defined by Julia and also used by Birch and Swinnerton-Dyer, both for Type 1 and Type 2 quartics. Hence our definition of 'reduced' agrees with theirs in both these cases.*

Proof. This is a straightforward calculation in each case, using the expression for $H(X)$ in terms of the roots of $g(X)$. It is necessary to order the x_i correctly. For Type 1 quartics, one must take the conjugate pairs to be $\{\beta_1, \overline{\beta_1}\} = \{x_1, x_3\}$ and $\{\beta_2, \overline{\beta_2}\} = \{x_2, x_4\}$, while for Type 2 one takes $x_1 > x_3 > x_2 > x_4$. We leave the remaining details to the reader. □

We next observe that, as was the case for cubics, a real quartic $g(X)$ with positive discriminant is reduced if and only if its quartic covariant $g_4(X)$ is also reduced.

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

Proposition 10. *Let $g(X)$ be a real quartic with positive discriminant and nonzero J invariant. Then $g(X)$ is reduced if and only if its quartic covariant $g_4(X)$ is reduced.*

Proof. The condition on the J invariant is included merely because $g_4(X)$ is singular when $J(g) = 0$, since $\Delta(g_4) = 2^{12}J^2\Delta$, and we have only defined the notion of 'reduced' for nonsingular quartics. The same relation shows that $\Delta(g_4) > 0$ when $\Delta > 0$ and $J \neq 0$, so we have defined what it means for g_4 to be reduced.

Above we showed that $g_6(X)$ factorizes over the splitting field of the cubic resolvent $F(X)$ as a product of three real quadratics, exactly one of which is definite. Hence $g_6(X)$ has exactly one pair of complex roots, of which exactly one is in the upper half-plane, and $g(X)$ is reduced if and only if this root lies in the usual fundamental region (2). Since the g_6 covariant of $g_4(X)$ is $2^6 J\, g_6(X)$, the result is now immediate. □

Remark 4. It is not true that $g(X)$ and $g_4(X)$ have the same type. In fact, a rather tedious examination of cases shows that $g_4(X)$ has Type 1 when $g(X)$ has Type 2 or when $g(X)$ has Type 1 and $aJ > 0$, but $g_4(X)$ has Type 2 when $g(X)$ has Type 1 and $aJ < 0$.

We now derive the important inequalities satisfied by a reduced quartic in the positive discriminant case.

Proposition 11. *Let $g(X)$ be a reduced real quartic with positive discriminant Δ, leading coefficient a and seminvariant H. Order the three real roots of the resolvent cubic so that $4a\varphi_1 > 4a\varphi_2 > 4a\varphi_3$.*

(i) *If $g(X)$ has Type 1, then*

$$|a| \leqslant \frac{1}{9}|\varphi_1 - \varphi_3|; \tag{37}$$

$$4a\varphi_2 \leqslant H \leqslant \min\{4a\varphi_1, 4a\varphi_3 + \frac{4}{3}(\varphi_3^2 - I)\}. \tag{38}$$

(ii) *If $g(X)$ has Type 2, then*

$$|a| \leqslant \frac{1}{9}|\varphi_1 - \varphi_2|; \tag{39}$$

$$4a\varphi_2 + \frac{4}{3}(\varphi_2^2 - I) \leqslant H \leqslant 4a\varphi_3. \tag{40}$$

Remark 5. In the Type 1 case, the range of a naturally divides up into two subranges: when $|a| \leqslant \frac{1}{9}|\varphi_2 - \varphi_3|$, the relevant upper bound on H is

$$H \leqslant 4a\varphi_3 + \frac{4}{3}(\varphi_3^2 - I) \quad (\leqslant 4a\varphi_1),$$

while for $\frac{1}{9}|\varphi_2 - \varphi_3| \leqslant |a| \leqslant \frac{1}{9}|\varphi_1 - \varphi_3|$, the relevant upper bound is

$$H \leqslant 4a\varphi_1 \quad (\leqslant 4a\varphi_3 + \frac{4}{3}(\varphi_3^2 - I)).$$

Remark 6. With slightly different notation, these are in fact the same bounds as stated in [3], though this is by no means apparent: our expression (37) for the upper bound on $|a|$ for Type 1 quartics is much simpler than the expression given in [3].

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

Remark 7. In applying these bounds, one must not forget that our convention is to order the roots φ_i differently for positive and negative a. If we instead fix $\varphi_1 > \varphi_2 > \varphi_3$, then the range of a in the Type 2 case becomes

$$\frac{1}{9}(\varphi_3 - \varphi_2) \leqslant a \leqslant \frac{1}{9}(\varphi_1 - \varphi_2). \tag{41}$$

Remark 8. One can attempt to obtain alternative bounds on H by noting that it is (minus) the leading coefficient of $g_4(X)$, so that we may apply the bounds on a to g_4, which is reduced when g is. This is quite delicate, as we have to consider carefully the ordering of the three roots $4(\varphi^2 - 4I)$ of the resolvent cubic of g_4. In the end one obtains bounds which are always weaker (or at least no stronger) than the bounds stated here. We omit the details.

Proof of Proposition 11. First consider the Type 1 case, where $\varphi = \varphi_3$ and $4a\varphi_1 \geqslant H \geqslant 4a\varphi_2 > 4a\varphi_3$. The positive definite quadratic covariant $h(X)$ defined above has leading coefficient $-9z = 3(H - 4a\varphi_3)$ and discriminant $108z(\varphi_3^2 - I) = 36(4a\varphi_3 - H)(\varphi_3^2 - I)$. Applying the basic reduction inequality (3) gives

$$H - 4a\varphi_3 \leqslant \frac{4}{3}(\varphi_3^2 - I),$$

which combined with $4a\varphi_2 \leqslant H \leqslant 4a\varphi_1$ gives the stated bounds on H. Then

$$a(\varphi_2 - \varphi_3) \leqslant \frac{1}{3}(\varphi_3^2 - I) = \frac{1}{9}(\varphi_1 - \varphi_3)(\varphi_2 - \varphi_3),$$

which gives the stated upper bound for $|a|$.

In the Type 2 case, we have $\varphi = \varphi_2$ and $4a\varphi_1 > 4a\varphi_2 > 4a\varphi_3 \geqslant H$. Now $h(X)$ has leading coefficient $9z = 3(4a\varphi_2 - H)$ and discriminant $36(4a\varphi_2 - H)(\varphi_2^2 - I)$, so reduction implies that $H - 4a\varphi_2 \geqslant \frac{4}{3}(\varphi_2^2 - I)$. The bounds on a and H are obtained as before. □

4.4. *Reduction of real quartics with* $\Delta < 0$

We turn to the case of real quartics with negative discriminant (Type 3). Here there is a unique real root φ of the resolvent cubic $F(X)$, using which we may define a real quadratic $H(X)$ over $K(\sqrt{z})$. But now $H \leqslant 4a\varphi$, so that $z \geqslant 0$, and the discriminant of $H(X)$ is $\frac{4}{9}(\varphi - \varphi')(\varphi - \varphi'') = \frac{4}{9}|\varphi - \varphi'|^2 > 0$. So $H(X)$ is indefinite, and cannot be used for reduction.

The approach used by Birch and Swinnerton-Dyer in [3] bears a strong resemblance to the idea used by Mathews for cubics with negative discriminant. They define reduction in terms of the real positive definite quadratic factor $(X - \beta)(X - \overline{\beta})$ of $g(X)$ itself, ignoring the two real roots α_1 and α_2. This leads to the following bounds on the leading coefficient a and seminvariant H of a reduced quartic of Type 3:

$$\left(a - \frac{1}{3}\varphi\right)^2 \leqslant \frac{4}{27}(\varphi^2 - I); \tag{42}$$

$$9a^2 - 2a\varphi + \frac{1}{3}(4I - \varphi^2) \leqslant H \leqslant 4a\varphi. \tag{43}$$

Later, we will compare these bounds with the ones obtained by our alternative definition.

Instead we consider the real quartic factor $G(X)$ of $g_6(X)$ defined over $K(\sqrt{z})$, defined in (32).

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

Proposition 12. *Let g be a real quartic with negative discriminant (Type 3). Then the real algebraic covariant $G(X)$ has Type 1.*

Proof. We can show directly that $G(X)$ has no real roots. A real root α of $G(X)$ would be a root of $g_4(X) + 4\varphi' g(X)$ for one of the complex roots φ' of $F(X)$, and hence by conjugation for both the complex roots. But then α is a common root of $g(X)$ and $g_4(X)$, which is impossible since their resultant is $\frac{1}{9}\Delta^2 \neq 0$.

Alternatively, we see from Lemma 2 below that $\Delta_G > 0$ and $H_G > 0$, from which the result follows by Proposition 7. □

As we have already defined what it means for a Type 1 real quartic to be reduced, we may now make the following definition.

Definition 5. Let g be a real quartic with negative discriminant (Type 3). Then we say that g is *reduced* if and only if its real algebraic covariant $G(X)$ is reduced.

It is not at all clear that this definition will give useful results, or how it compares with earlier alternative definitions of Julia or Birch and Swinnerton-Dyer. In fact it turns out to be equivalent to Julia's definition in [**12**], though we are able to obtain better bounds than Julia from it; and it is certainly different from the definition of Birch and Swinnerton-Dyer, giving considerably better bounds. Obtaining bounds on a and H from our definition, however, will involve some work.

As in all earlier cases, we find that $g(X)$ is again reduced if and only if $g_4(X)$ is reduced.

Proposition 13. *Let g be a real quartic with negative discriminant (Type 3) and nonzero J invariant. Then*

(i) *The quartic covariant $g_4(X)$ also has Type 3;*

(ii) *The quartic covariants $G(X)$ associated to g and g_4 are the same, up to a constant factor;*

(iii) *The quartic g is reduced if and only if g_4 is reduced.*

Proof. The first two parts follow from the explicit formulas given in Proposition 5, and then the last statement is immediate. □

In order to apply the results of the previous section to $G(X)$, we must examine its invariants and covariants. The basic inequalities for a Type 1 quartic, from which we derived the bounds (37) and (38) for a and H stated in Proposition 11, were

$$3(H - 4a\varphi_3) \leqslant 4(\varphi_3^2 - I) \tag{44}$$

and

$$4a\varphi_2 \leqslant H \leqslant 4a\varphi_1. \tag{45}$$

We therefore compute the quantities appearing in these expressions associated to the quartic $G(X)$, obtaining the values shown in Lemma 2. Note that $z = \frac{1}{3}(4a\varphi - H) \geqslant 0$. We also set

$$\Phi = \frac{2}{3}|\varphi - \varphi'|\,|\varphi' - \varphi''|. \tag{46}$$

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

Lemma 2. *Let $g(X)$ be a real quartic with negative discriminant (Type 3). Denote the real root of the resolvent cubic by φ, and the complex conjugate roots by φ', φ''. Then the values of the invariants and seminvariants of $G(X)$ are as follows.*

$g(X)$	$G(X)$
I	$\frac{4}{3}(\varphi^2 - I)(\varphi^2 - 4I) = \frac{4}{27}\lvert\varphi - \varphi'\rvert^2\lvert\varphi' - \varphi''\rvert^2$
J	0
Δ	$2^8 3^{-3}(\varphi^2 - I)^3(\varphi^2 - 4I)^3 = 2^8 3^{-9}\lvert\varphi - \varphi'\rvert^6\,\lvert\varphi' - \varphi''\rvert^6$
a	$\lvert z'\rvert$
H	$4z(\varphi^2 - 4I) = \frac{4}{3}z\lvert\varphi' - \varphi''\rvert^2$
φ_1	Φ
φ_2	0
φ_3	$-\Phi$
$H - 4a\varphi_3$	$\frac{4}{3}\lvert\varphi' - \varphi''\rvert\,(z\lvert\varphi' - \varphi''\rvert + 2\lvert z'\rvert\,\lvert\varphi - \varphi'\rvert)$
$\varphi_3^2 - I$	$2I_G = \frac{8}{3}(\varphi^2 - I)(\varphi^2 - 4I) = \frac{8}{27}\lvert\varphi - \varphi'\rvert^2\lvert\varphi' - \varphi''\rvert^2$

Proof. That the leading coefficient of $G(X)$ is $9R$ is immediate from its definition (32). The values of I_G, J_G, Δ_G and H_G are obtained by direct calculation. These quantities are all positive, except for J_G, which is zero, and H_G, which is zero when $R = 0$ (since then $z = 0$). The cubic resolvent polynomial for $G(X)$ is thus

$$X^3 - 3I_G X + J_G = X(X^2 - 3I_G),$$

whose roots are 0 and $\pm\Phi$, since $\Phi^2 = 3I_G$. The rest is straightforward, using identities we derived earlier. □

Lemma 3. *Let $g(X)$ be a real quartic of Type 3. With the same notation as above, the following inequality holds:*

$$0 \leqslant \lvert\varphi' - \varphi''\rvert(4a\varphi - H) \leqslant 2\lvert\varphi - \varphi'\rvert\,\lvert 4a\varphi' - H\rvert. \tag{47}$$

If g is reduced, then also

$$\lvert\varphi' - \varphi''\rvert(4a\varphi - H) + 2\lvert\varphi - \varphi'\rvert\,\lvert 4a\varphi' - H\rvert \leqslant \frac{8}{9}\lvert\varphi' - \varphi''\rvert\,\lvert\varphi - \varphi'\rvert^2. \tag{48}$$

Proof. These are the inequalities (45) and (44) applied to $G(X)$, using the formulas of the preceding lemma. In fact (47) just comes from the seminvariant syzygy, following directly (since $H \leqslant 4a\varphi$) from the identity

$$4\lvert\varphi - \varphi'\rvert^2\lvert 4a\varphi' - H\rvert^2 - \lvert\varphi' - \varphi''\rvert^2(4a\varphi - H)^2 = 9(H\varphi + 8aI)^2.$$

□

Lemma 4. *Let $g(X)$ be a reduced real quartic of Type 3. Then its leading coefficient a and seminvariant H satisfy the following inequalities.*

$$\lvert a\rvert \leqslant \frac{1}{6\sqrt{3}}(2\sqrt{\varphi^2 - I} + \sqrt{\varphi^2 - 4I}); \tag{49}$$

$$4a\varphi - \frac{4}{3}(\varphi^2 - I) \leqslant H \leqslant 4a\varphi; \tag{50}$$

$$\lvert H + 2a\varphi\rvert \leqslant \frac{2}{3}\sqrt{\varphi^2 - 4I}\sqrt{4(\varphi^2 - I) - 27a^2}. \tag{51}$$

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

Proof. Substitute (47) into (48) to get

$$0 \leqslant 2|\varphi' - \varphi''|(4a\varphi - H) \leqslant \frac{8}{9}|\varphi' - \varphi''|\,|\varphi - \varphi'|^2,$$

so that

$$0 \leqslant 4a\varphi - H \leqslant \frac{4}{9}|\varphi - \varphi'|^2 = \frac{4}{3}(\varphi^2 - I), \tag{52}$$

which is (50). Also, since $4a\varphi - H \geqslant 0$, (48) implies that

$$|H - 4a\varphi'| \leqslant \frac{4}{9}|\varphi - \varphi'|\,|\varphi' - \varphi''|. \tag{53}$$

To ease notation, write $x = |\varphi - \varphi'|$ and $y = |\varphi' - \varphi''|$; these satisfy $0 < y \leqslant 2x$, since by the triangle inequality, $|\varphi' - \varphi''| \leqslant |\varphi' - \varphi| + |\varphi'' - \varphi| = 2\,|\varphi - \varphi'|$ (recall that φ is real, while $\varphi'' = \overline{\varphi'}$). Since $\varphi + \varphi' + \varphi'' = 0$, we have $\varphi' = \frac{1}{2}(-\varphi + yi)$. The identities $x^2 = 3(\varphi^2 - I)$, $y^2 = 3(\varphi^2 - 4I)$ and $4x^2 = 9\varphi^2 + y^2$ will also be used; they follow from Proposition 6.

In this notation, (52) and (53) become

$$0 \leqslant 4a\varphi - H \leqslant \frac{4}{9}x^2, \tag{54}$$

and

$$|H - 4a\varphi'| \leqslant \frac{4}{9}xy. \tag{55}$$

Now $H - 4a\varphi' = (H + 2a\varphi) - 2ayi$, so (55) implies that $4x^2 \geqslant 81a^2$ and then

$$(H + 2a\varphi)^2 \leqslant \frac{4}{81}y^2(4x^2 - 81a^2). \tag{56}$$

This implies (51), using the identities stated above.

Note that this calculation already implies that $|a| \leqslant \frac{2}{9}x$; we now strengthen this to give $|a| \leqslant \frac{1}{18}(2x + y)$, which is (49). Write $u = |z'| = \frac{1}{3}|H - 4a\varphi'|$. Now (48) and (47) become $yz + 2xu \leqslant \frac{8}{27}x^2y$ and $0 \leqslant yz \leqslant 2xu$. Together with $z \geqslant 0$ these determine a triangle in the (z, u) plane with vertices at $(0, 0)$, $(0, \frac{4}{27}xy)$ and $(\frac{4}{27}x^2, \frac{2}{27}xy)$. Using $y \leqslant 2x$ one sees that the maximum value of $z + u$ is attained at the last vertex, so that $z + u \leqslant \frac{2}{27}x(2x + y)$, which implies the desired result $|a| \leqslant \frac{1}{18}(2x + y)$, since

$$4|a|x = |4a(\varphi - \varphi')| \leqslant |4a\varphi - H| + |4a\varphi' - H| = 3(z + u).$$

□

Remark 9. The bound on $|a|$ in the preceding Lemma may be written in the form

$$\frac{1}{18}\sum_{i<j}|\varphi_i - \varphi_j|.$$

This has exactly the same form as the bound we obtained for Type 1 quartics: when $\varphi_1 > \varphi_2 > \varphi_3$ this expression equals $\frac{1}{9}|\varphi_1 - \varphi_3|$, just as in (37). The same is also true for Type 2 reduced quartics, if one compares the form of the bounds given in (41). It was this symmetry which led us to seek to prove the inequality (49), instead of the weaker form

$$|a| \leqslant \frac{1}{9}x + \frac{1}{9}y = \frac{1}{9}|\varphi - \varphi'| + \frac{1}{9}|\varphi' - \varphi''| = \frac{1}{3\sqrt{3}}(\sqrt{\varphi^2 - I} + \sqrt{\varphi^2 - 4I}),$$

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

which is somewhat easier to derive from (48) and (47).

Remark 10. The bounds (42) on a given in [3] determine an interval of length $\frac{4}{9}x$, whereas our bound (49) gives an interval of length $\frac{1}{9}(2x + y)$; the latter is at least as good, since $y \leqslant 2x$.

We now further tighten the bounds just obtained for a and H. The final result is as follows.

Proposition 14. *Let $g(X)$ be a reduced real quartic of Type 3, with (negative) discriminant Δ, leading coefficient a and seminvariant H, and let φ be the real root of the resolvent cubic. Set*

$$A = \frac{1}{6\sqrt{3}}(2\sqrt{\varphi^2 - I} + \sqrt{\varphi^2 - 4I})$$

(which depends only on the invariants I and J), and

$$B_a = \frac{2}{3}\sqrt{\varphi^2 - 4I}\sqrt{4(\varphi^2 - 4I) - 27a^2}$$

(which also depends on a).

If $J < 0$ (equivalently, $\varphi > 0$), then a satisfies

$$-\frac{1}{3\sqrt{3}}\sqrt{\varphi^2 - 4I} \leqslant a \leqslant \min\left\{ A\,,\ \max\left\{ \frac{1}{6}\left(\varphi + \sqrt{\varphi^2 - 4I}\right)\,,\ \frac{2}{9}\frac{(\varphi^2 - I)}{\varphi} \right\} \right\} \tag{57}$$

while if $J > 0$ (equivalently, $\varphi < 0$), then a satisfies

$$\frac{1}{3\sqrt{3}}\sqrt{\varphi^2 - 4I} \geqslant a \geqslant \max\left\{ -A\,,\ \min\left\{ \frac{1}{6}\left(\varphi - \sqrt{\varphi^2 - 4I}\right)\,,\ \frac{2}{9}\frac{(\varphi^2 - I)}{\varphi} \right\} \right\}. \tag{58}$$

If $J = 0$ then $\varphi = 0$ and $I < 0$, and a satisfies

$$|a| \leqslant \frac{2}{3\sqrt{3}}\sqrt{-I}. \tag{59}$$

For each a, H satisfies the inequalities

$$\max\left\{ 4a\varphi - \frac{4}{3}(\varphi^2 - I)\,,\ -2a\varphi - B_a \right\} \leqslant H \leqslant \min\{\, 4a\varphi\,,\ -2a\varphi + B_a \,\}. \tag{60}$$

Proof. The relation between the signs of J and φ follows from $\varphi\varphi'\varphi'' = -J$.

The inequalities (50) and (51) each determine an interval in which H lies, given the value of a. Recall the notation introduced above: $x = |\varphi - \varphi'|$ and $y = |\varphi' - \varphi''|$; then the relevant inequalities on H are (55) and (56). We now impose the conditions that these are not disjoint, in order to further restrict a. First we have

$$-2a\varphi - \frac{2}{9}y\sqrt{4x^2 - 81a^2} \leqslant H \leqslant 4a\varphi$$

(where $4x^2 - 81a^2 \geqslant 0$), so that $-y\sqrt{4x^2 - 81a^2} \leqslant 27a\varphi$. This is trivially satisfied if $a\varphi \geqslant 0$, but if $a\varphi < 0$ it gives $y^2(4x^2 - 81a^2) \geqslant 729a^2\varphi^2$, which simplifies to $y^2 \geqslant 81a^2$ on using the identity $4x^2 = 9\varphi^2 + y^2$. Hence

$$|a| \leqslant \frac{1}{9}y = \frac{1}{3\sqrt{3}}\sqrt{\varphi^2 - 4I}.$$

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

Note that this is always at least as strong as (49), since $y \leqslant 2x$, so we can replace the upper or lower bounds on a when $\varphi < 0$ or $\varphi > 0$ respectively by $\pm\frac{1}{3\sqrt{3}}\sqrt{\varphi^2 - 4I}$.

Secondly, we have

$$4a\varphi - \frac{4}{9}x^2 \leqslant H \leqslant -2a\varphi + \frac{2}{9}y\sqrt{4x^2 - 81a^2},$$

which simplifies to $27a\varphi - 2x^2 \leqslant y\sqrt{4x^2 - 81a^2}$. This time we obtain no further information when $a\varphi < 0$, or even when $a\varphi \leqslant \frac{2}{27}x^2$. But when $a\varphi > \frac{2}{27}x^2$ we have $(27a\varphi - 2x^2)^2 \leqslant y^2(4x^2 - 81a^2)$, which simplifies to

$$(6a - \varphi)^2 \leqslant \frac{1}{3}y^2.$$

Now $4x^2 = 9\varphi^2 + y^2 > 9\varphi^2$, so $\frac{2}{27}x^2 > \frac{1}{6}\varphi^2$; hence the condition $a\varphi > \frac{2}{27}x^2$ implies that $|a| > \frac{1}{6}|\varphi| > 0$. First suppose that $\varphi > 0$; then $a > \varphi/6$, so the extra condition on a is

$$\frac{2}{27}\frac{x^2}{\varphi} < \frac{1}{6}\varphi \leqslant a \leqslant \frac{1}{6}\varphi + \frac{1}{6\sqrt{3}}y.$$

Thus when $\varphi > 0$, an upper bound on positive a is

$$a \leqslant \max\left\{\frac{1}{6}\varphi + \frac{1}{6\sqrt{3}}y\,,\ \frac{2}{27}\frac{x^2}{\varphi}\right\} = \max\left\{\frac{1}{6}\left(\varphi + \sqrt{\varphi^2 - 4I}\right)\,,\ \frac{2}{9}\frac{(\varphi^2 - I)}{\varphi}\right\};$$

the bound $\frac{2}{27}\frac{x^2}{\varphi}$ is stronger (smaller than $\frac{1}{6}\varphi + \frac{1}{6\sqrt{3}}y$) if and only if $I + 2\varphi^2 > 0$.

The analysis for $a < 0$ when $\varphi < 0$ is similar. Finally, the case $\varphi = 0$ is easy, as here we just restate the bound obtained earlier. □

We end this section by sketching a proof that our definition of reduction for quartics with negative discriminant does coincide with Julia's. Note that we have not yet written down explicitly the associated positive definite real quadratic in this case. Ignoring an irrelevant constant factor, this is

$$H_\Phi(X) = G_4''(X) + 4G''(X)\Phi - 16I_G,$$

where $G(X)$ is the quartic defined above, with invariant $I_G = \frac{4}{3}(\varphi^2 - I)(\varphi^2 - 4I)$ and quartic covariant $G_4(X)$, and $\Phi = \sqrt{3I_G}$.

Since Φ^2 has a lower algebraic degree than Φ, it is easier to work with

$$H_\Phi(X)H_{-\Phi}(X) = (G_4''(X) - 16I_G)^2 - 48I_G G''(X)^2.$$

which is a quartic defined over $\mathbb{Q}(a, b, c, d, e)(\varphi)$. We now replace b, c, d, e and φ by their expressions in terms of a and the roots α_1, α_2, β and $\overline{\beta}$ of the original quartic $g(X)$. Computer algebra then shows that the resulting expression is equal, up to a constant factor, to

$$(t_1^2(X - \alpha_1)^2 + t_2^2(X - \alpha_2)^2)^2 - 4u^4(X - \beta)^2(X - \overline{\beta})^2,$$

where t_1^2, t_2^2 and u^2 are as defined in (6). The latter is the product of Julia's quadratic $t_1^2(X - \alpha_1)^2 + t_2^2(X - \alpha_2)^2 + 2u^2(X - \beta)(X - \overline{\beta})$ and the conjugate quadratic $t_1^2(X - \alpha_1)^2 + t_2^2(X - \alpha_2)^2 - 2u^2(X - \beta)(X - \overline{\beta})$. Since on both sides we have a real quartic with a unique positive definite quadratic factor, these quadratic factors must themselves be equal (up to a constant factor). Hence $H_\Phi(X)$ is equal to Julia's quadratic, as claimed.

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

4.5. *Algorithm for reducing real quartics*

The algorithm for reducing a given real quartic $g(X)$ is straightforward. We compute the invariants I and J, the discriminant Δ and the seminvariants H and Q, to determine the type using Proposition 7. We then solve the cubic resolvent equation to find its roots φ.

If $\Delta > 0$ then we choose one of the three real roots φ as in Proposition 8: we take the smallest for Type 1 quartics with $a > 0$, the largest for Type 1 quartics with $a < 0$, and the middle root for Type 2 quartics. (Note that with Type 1 quartics the sign of a will remain constant during reduction, since $g(X)$ has no real roots and so is itself positive or negative definite according to the sign of a.) Given this value of φ, we define the quadratic $H_1(X)$ by (31), ignoring the constant factor, and reduce $H_1(X)$ using the general procedure given in Section 2.1.

If $\Delta < 0$ we find it simplest to use Julia's expression for the positive definite covariant quadratic given above in (6) and (7). This does require us to compute the roots of $g(X)$ before reducing it. However, since we already have the roots of the resolvent cubic, we may easily write down these roots, rather than use a general-purpose procedure. Let φ and φ' denote the real and one of the complex roots of the cubic resolvent, as above. Set $w = \pm\sqrt{z} \in \mathbb{R}$, where as before, $z = \frac{1}{3}(4a\varphi - H) \geqslant 0$, and the sign of w is chosen to agree with the sign of the seminvariant R. Also set $w' = \sqrt{z'} \in \mathbb{C}$, where $z' = \frac{1}{3}(4a\varphi' - H)$. (The choice of sign ensures that $R = ww'\overline{w'} = w|w'|^2$.) Then the real roots of $G(X)$ are

$$\alpha_1, \alpha_2 = \frac{1}{4a}\left(-b - w \pm 2\,\mathrm{Re}(w')\right),$$

and the complex conjugate roots are

$$\beta, \overline{\beta} = \frac{1}{4a}\left(-b + w \pm 2\,\mathrm{Im}(w')i\right).$$

Now the quadratic used for reduction is $t_1^2(X-\alpha_1)^2 + t_2^2(X-\alpha_2)^2 + 2u^2(X-\beta)(X-\overline{\beta})$, where $t_1^2 = |\,\mathrm{Im}(w')||w+w'|^2$, $t_2^2 = |\,\mathrm{Im}(w')||w-w'|^2$, and $u^2 = |\,\mathrm{Re}(w')||w'^2 - w^2|$. (These are $8|a|^3$ times the values given in (6) and (7).)

4.6. *Algorithm for finding all integer quartics with given invariants*

It is clear from much of the discussion in the preceding sections that we regard bounding the seminvariants of a reduced quartic with given invariants as more important than bounding all the coefficients directly, as one might perhaps expect *a priori* would be more natural. The only coefficient that we bound explicitly is the leading coefficient a, which is also seminvariant. In fact this is quite natural, since knowledge of the seminvariants a, H and R (as well as I and J) determines the quartic $g(X)$ up to a translation of the variable X, and hence up to $\mathrm{SL}(2,\mathbb{Z})$-equivalence. We can even ignore the seminvariant R, which is determined up to sign by the seminvariant syzygy (22) given a and H, since the seminvariants of $g(-X)$ are $(a, H, -R)$. Similar remarks apply in the cubic case.

It would appear, therefore, that our search for inequivalent integer quartics with given invariants I, J should consist essentially of a double loop over a (the outer loop) and H (the inner loop). But this approach has one major drawback, that a given integer pair (a, H) does not necessarily come from an integer quartic, since the equation $H = 8ac - 3b^2$ does not necessarily have integer solutions for b and c. Instead, we proceed as follows: the outer loop on a contains an inner loop on b in the range $-2|a| < b \leqslant 2|a|$; for each pair (a, b) we determine bounds on c from the bounds given above on H and use a third loop on c between these bounds. This ensures that all the inequalities are satisfied, and that a, b and c

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

are all integral. (The same method was used in [**3**], for the same reason, though of course with different bounds when $\Delta < 0$.)

Just as with cubics, we can make this triple loop very much more efficient by using a quadratic sieve based on the syzygy (22). For each (a, b, c) triple processed, we compute H, and look up in precomputed tables the values (a mod m, H mod m) for various carefully chosen auxiliary moduli m, so that we only proceed with the triple if the left-hand side of the syzygy has the form $-27R^2$ mod m for each m. Note that although we have a triple loop, the precomputed arrays are indexed by (a, H) and so are only two-dimensional.

Given a triple (a, b, c) which passes the sieve, we test whether the the left-hand side of the syzygy really does have the form $-27R^2$ for some integer R. If so, we use the definition of R in (20) to solve for d (discarding the triple if this value is not integral), and then the definition of I gives the value of the last coefficient e, which again we check to be integral.

This is the procedure we have implemented as part of our program `mwrank` for 2-descent on general elliptic curves defined over $\mathbb{Q}$. For more details of this algorithm, see the description in [**8**, Section 3.6] and also the original paper [**3**]. Note that in [**3**], the syzygy is not used and there is no quadratic sieving. Also, the computation of d and e there is done using the cubic quantities φ_i, which are only known approximately, to a certain precision. This results in a practical problem, of how to decide whether the computed values of d and e are in fact integers when they are close to integers. By contrast, our approach uses exact integer arithmetic throughout, apart from the computation of the bounds on a and H.

4.6.1. Examples

We give here two examples to show how the bounds just obtained improve substantially on those used in [**3**], given above in (42) and (43), which we call the BSD bounds.

Example 1. First consider integer quartics with $I = 3792$ and $J = -591408$. These arise on doing 2-descent on the elliptic curve

$$E: \quad y^2 + y = x^3 - 79x + 342$$

which has rank 5. The discriminant here is $\Delta = -131658746112 = 2^8 3^3 \Delta_E$. The real value of φ is $\varphi = 126.6686$ and the complex values are $\varphi' = -63.3343 + 25.5457i$ and its conjugate. The BSD bound for a leads us to consider the range

$$1 \leqslant a \leqslant 84,$$

and for each a we consider integer values of H satisfying (43). The number of (a, H) pairs satisfying these is 927 806.

Now the bound on $|a|$ given in Lemma 4 in (49) is 24.15; for a in the range $-24 \leqslant a \leqslant 24$, the inequalities (50), (51) on H are incompatible unless $-5 \leqslant a \leqslant 24$. As expected, the refined bounds for a in Proposition 14 give precisely this range for a. The number of (a, H) pairs which satisfy (57), (60) is only 177 176, or approximately one fifth of the earlier number. This leads to a saving of almost 81 percent in the time to find all inequivalent integer quartics with these invariants. The number we find is in fact 58; under the weaker equivalence between quartics which is relevant for classifying homogeneous spaces for a 2-descent, this number reduces to 32 and hence to the conclusion that the curve E has rank 5. (We omit fuller details of the 2-descent, which is described in [**8**].)

Example 2. For an even more impressive example, we consider the invariants $I = 721812$ and $J = -1236714912$, which come from the elliptic curve

$$E: \quad y^2 = x^3 - 240604x + 45804256$$

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press

of rank 7. The BSD bounds give the range $1 \leqslant a \leqslant 1134$ for a, and a total of 2 188 507 643 (a, H) pairs satisfy the BSD inequalities. Using our bounds we find the range $-14 \leqslant a \leqslant 290$ for a, and a total of 77 752 191 (a, H) pairs. The saving here is nearly 96.5%.

5. *Remarks on reduction over number fields*

In extending our results to the reduction of polynomials over number fields, two important matters arise. Firstly, reduction of integer polynomials uses the real embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$. For a number field K, we must use all the real embeddings of K, as well as the complex (non-real) embeddings $K \hookrightarrow \mathbb{C}$ if K is not totally real. Secondly, we must somehow combine the bounds coming from the various embeddings of K to obtain usable bounds, and a finite search region, for the coefficients of reduced polynomials in $\mathcal{O}_K[X]$.

We consider first totally real fields. The only case which has been worked out in detail to date is that of a real quadratic field of class number 1: see [**9**], and [**14**] for fuller details. One finds that the correct approach is not to consider the real embeddings separately, but to work with them simultaneously. The basic reduction theory of Section 2, which was based on the action of the modular group $\mathrm{SL}(2, \mathbb{Z})$ on the upper half-plane $\mathcal{H}$, must be replaced by a theory based on the action of the Hilbert modular group $\mathrm{SL}(2, \mathcal{O}_K)$ on $\mathcal{H}^2$. This leads to bounds on the *norm* of the leading coefficient of a reduced totally positive definite quadratic in $K[X]$, and this is sufficient to produce a finite search region since the action of units can easily be controlled.

For the case of fields which are not totally real, we only consider here an imaginary quadratic field K. Instead of reduction by means of positive definite real quadratics (or equivalently, points in the upper half-plane $\mathcal{H}$), one is led to reduction by means of so-called 'Hermitian quadratics'. These have the form

$$h(z, w) = az\overline{z} + bz\overline{w} + \overline{b}\overline{z}w + cw\overline{w},$$

where a and c are real, b is complex, and we consider z and w to be complex indeterminates. In place of points on the upper half-plane, we have points in hyperbolic 3-space $\mathcal{H}_3$. The modular group $\mathrm{SL}(2, \mathcal{O}_K)$ is here usually called a Bianchi group, and acts both on the set of Hermitian quadratics and on $\mathcal{H}_3$. This theory is quite classical, originating in the late 19th century with the work of Bianchi, Humbert and others. The application to the reduction of polynomials with complex coefficients forms the second part of Julia's treatise [**12**], whose first part we have referred to repeatedly in this paper. In a future paper, we hope to show how to use Julia's methods to find all quartics with given K-integral invariants I and J, up to $\mathrm{SL}(2, \mathcal{O}_K)$-equivalence, over an imaginary quadratic field K of class number 1. This will form part of a planned implementation of an explicit 2-descent algorithm for elliptic curves defined over such fields. It is not yet clear whether the approach via classical invariant theory, which we have exploited in this paper, has an analogue in the complex case. Some preliminary work on such a theory is in progress, but it is too early to tell whether the results will have practical applications to reduction.

Acknowledgements. This work was carried out while the author was visiting Université Bordeaux I during the first six months of 1997, and he would like to thank the members of *A2X* (Laboratoire d'Algorithmique Arithmétique Expérimentale) for their hospitality, and for providing a congenial working environment.

References

1. K. Belabas, 'Computing cubic fields in quasi-linear time', [5] 17–25. 62
2. K. Belabas, 'A fast algorithm to compute cubic fields', *Math. Comp.* 66 (1997) 1213–1237. 62, 71, 72, 75, 76
3. B. J. Birch and H. P. F. Swinnerton-Dyer, 'Notes on elliptic curves I', *J. Reine Angew. Math.* 212 (1963) 7–25. 62, 76, 79, 80, 81, 82, 82, 83, 87, 90, 90, 90, 90
4. J. W. S. Cassels, *An introduction to the geometry of numbers*, Classics in Mathematics (Springer, 1997). 63, 72, 76
5. H. Cohen (ed.), *Algorithmic number theory*, Lecture Notes in Computer Science 1122 (Springer-Verlag, 1996). 92
6. H. Cohen, *A course in computational algebraic number theory*, 3rd corrected printing, Graduate Texts in Mathematics 138 (Springer-Verlag, 1996). 80
7. J. E. Cremona, 'Classical invariants and 2-descent on elliptic curves', *J. Symbolic Comput.*, to appear. 63, 67, 76, 76
8. J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd edn (Cambridge University Press, 1997). 62, 62, 90, 90
9. J. E. Cremona and P. Serf, 'Computing the rank of elliptic curves over real quadratic fields of class number 1', *Math. Comp.* 68 (1999) 1187–1200. 63, 91
10. E. B. Elliott, *An introduction to the algebra of quantics*, 2nd edn (Oxford University Press, 1913). 63, 67
11. D. Hilbert, *Theory of algebraic invariants* (Cambridge University Press, 1993). 63, 78
12. G. Julia, 'Étude sur les formes binaires non quadratiques à indéterminées réelles ou complexes', *Mem. Acad. Sci. l'Inst. France* 55 (1917) 1–293. 62, 65, 71, 72, 80, 81, 84, 91
13. G.-B. Mathews, 'On the reduction and classification of binary cubics which have a negative discriminant', *Proc. London Math. Soc.* (3) 10 (1912) 128–138. 72, 75
14. P. Serf, 'The rank of elliptic curves over real quadratic number fields of class number 1', Ph.D. thesis, Universität des Saarlandes, 1995. 63, 91

J. E. Cremona (John.Cremona@nottingham.ac.uk)

School of Mathematical Sciences
University of Nottingham
University Park
Nottingham
NG7 2RD

https://doi.org/10.1112/S1461157000000073 Published online by Cambridge University Press