Reduction of binary forms over imaginary quadratic fields

John Cremona
University of Warwick, UK

Plan of the talk

- Review of reduction of real binary forms
  - ⋆ Applications of reduction of integral cubics and quartics

- Reduction of complex binary forms
  - ⋆ Applications of reduction of cubics and quartics over imaginary quadratic fields

I. Real Binary Forms
Real Binary Quadratic Forms

$$\mathrm{BQF}(\mathbb{R}) = \{f(X,Y) = aX^2 + bXY + cY^2 \mid a,b,c \in \mathbb{R}\} \subset \mathbb{R}[X,Y]$$

Notation: $f = [a,b,c]$, $\Delta = b^2 - 4ac$.

f is positive definite iff $a > 0$, $\Delta < 0$ since

$$4af(X,Y) = (2aX + bY)^2 - \Delta Y^2.$$

$$\mathrm{BQF}(\mathbb{R})_+ = \{f \in \mathrm{BQF}(\mathbb{R}) \mid f \text{ is positive definite}\}$$

The Upper Half Plane

$$\mathcal{H}_2 = \{z \in \mathbb{C} \mid \Im(z) > 0\} = \{x + yi \mid x \in \mathbb{R}, y \in \mathbb{R}_{>0}\}.$$

"Root map":

$$\mathrm{BQF}(\mathbb{R})_+ \longrightarrow \mathcal{H}_2$$

via

$$f = [a, b, c] \mapsto z = \frac{-b + \sqrt{\Delta}}{2a} = x + yi$$

with $x = -b/2a$, $y = \sqrt{|\Delta|}/2a$, $|z|^2 = x^2 + y^2 = c/a$.
Inverse: $z = x + yi \mapsto [1, -2x, x^2 + y^2]$.
Bijection:

$$\mathrm{BQF}(\mathbb{R})_+/\mathbb{R}_{>0} \longleftrightarrow \mathcal{H}_2.$$

Group actions

$G = \mathrm{SL}(2,\mathbb{R})$ acts on $\mathrm{BQF}(\mathbb{R})_+$ on the right via

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : f(X,Y) \mapsto f^M(X,Y) = f(aX+bY, cX+dY)$$

preserving Δ; new leading coefficient is $f^M(1,0) = f(a,c) > 0$.
G acts transitively on $\mathcal{H}_2$ on the left via

$$M : z \mapsto M(z) = \frac{az+b}{cz+d},$$

or

$$(x,y) \mapsto \left(\frac{(ax+b)(cx+d)+acy^2}{(cx+d)^2+c^2y^2}, \frac{y}{(cx+d)^2+c^2y^2} \right)$$

The root map is G-equivariant: $z(f) = M(z(f^M))$ since the root of f^M is $M^{-1}(z)$.

Discrete subgroups, integral points and reduction

$\Gamma = \mathrm{SL}(2,\mathbb{Z}) \leq G$, discrete subgroup acting on $\mathrm{BQF}(\mathbb{R})_+$ and on $\mathcal{H}_2$.
Γ preserves $\mathrm{BQF}(\mathbb{Z})_+$, the integral forms in $\mathrm{BQF}(\mathbb{R})_+$. Γ has the usual fundamental region in $\mathcal{H}_2$:

$$\mathcal{F} = \{z \in \mathcal{H}_2 \mid -\frac{1}{2} \leq x < \frac{1}{2}, |z| > 1 \quad \text{or} \quad -\frac{1}{2} \leq x \leq 0, |z| = 1\}$$

$f \in \mathrm{BQF}(\mathbb{R})_+$ is *reduced* iff $z(f) \in \mathcal{F}$, i.e. $f = [a,b,c]$ with

$$-a < b \leq a < c \qquad \text{or} \qquad 0 \leq b \leq a = c.$$

$z \in \mathcal{F} \implies y \geq \sqrt{3}/2$, hence

$$f \quad \text{reduced} \implies \frac{\sqrt{|\Delta|}}{2a} \geq \sqrt{3}/2 \implies 0 < a \leq 3^{-\frac{1}{2}}|\Delta|^{\frac{1}{2}}.$$

Reduction in other sets

If S is any other set on which G acts, then to define "reduced" for elements of S we just need a G-equivariant map $\chi : S \to \mathrm{BQF}(\mathbb{R})_+$ (or $S \to \mathcal{H}_2$) and define $s \in S$ to be reduced iff $\chi(s)$ is.

There may be more than one such "covariant" map χ, in which case there will be rival notions of "reduced" for elements of S. We can ask:

- Is there a covariant χ?
- If so, is it unique?
- Is it "useful" (e.g. are reduced elements "small"?)
- If S has an integral structure, do we have a finiteness result?

Reduction of higher degree forms

Let $\mathbb{R}[X,Y]_n$ denote the set of real binary forms of degree $n \geq 3$. G acts on this just as for binary forms, and Γ acts on the integral forms $\mathbb{Z}[X,Y]_n$.

There is at least one covariant for every $n \geq 3$: write

$$g(X,Y) = \sum_{i=0}^{n} a_i X^i Y^{n-i} = a_n \prod_{i=1}^{n} (X - \alpha_i Y)$$

where $a_i \in \mathbb{R}$, $a_n \neq 0$ (for simplicity) and we assume that the roots $\alpha_i \in \mathbb{C}$ are distinct. Define

$$\chi(g) = \sum_{i=1}^{n} |g'(\alpha_i)|^{\frac{2}{2-n}} \left|X - \alpha_i Y\right|^2 .$$

Here if $\alpha_i \in \mathbb{R}$ then $\left|X - \alpha_i Y\right|^2 = (X - \alpha_i Y)^2$, while if $\alpha_i \in \mathbb{C} \setminus \mathbb{R}$ then $\left|X - \alpha_i Y\right|^2 = (X - \alpha_i Y)(X - \overline{\alpha_i} Y)$, this term appearing *twice* since $\overline{\alpha_i}$ is also a root.

Reduction of higher degree forms (contd.)

Lemma: $\chi(g)$ is covariant.

For $n = 3, 4$ this covariant appears in the work of Julia (1917) though with separate definitions for each signature. This unified expression is due to Stoll (c.f. JEC & Stoll, Crelle 2003).

- Unique? Yes for $n = 3, 4$ and unmixed signature, otherwise not (but see below).
- Useful? Certainly (see next page).
- Optimal? Not when $n \geq 5$: see JEC & Stoll op.cit. for a more complicated refinement.

Application I: enumeration of cubic fields

(Davenport-Heilbronn, Belabas)

To find all cubic number fields with discriminant Δ we enumerate integral cubic forms

$$g(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3 \in \mathbb{Z}[X,Y], \qquad \operatorname{disc}(g) = \Delta.$$

Set $P = b^2 - 3ac$ (leading coefficient of Hessian $H(g)$). If $\Delta > 0$ then $\chi(g) = H(g)$ (up to a constant factor), and

$$g \quad \text{reduced} \implies |a| \le \frac{2}{3\sqrt{3}}\Delta^{\frac{1}{4}} \qquad \text{and} \qquad 0 < P \le \Delta^{\frac{1}{2}}.$$

If $\Delta < 0$ then $\chi(g)$ differs from the covariant used by D-H & B. We obtain[1]

$$g \quad \text{reduced} \implies |a| \le \frac{2\sqrt{2}}{3\sqrt{3}}|\Delta|^{\frac{1}{4}} \qquad \text{and} \qquad |P| \le 2^{1/3}|\Delta|^{\frac{1}{2}}.$$

[1] D-H had constant $2/3^{3/4} = 0.877$ instead of $2\sqrt{2}/3\sqrt{3} = 0.544$

Application II: Two-descent on elliptic curves

- Birch and Swinnerton-Dyer showed how to do two-descent on elliptic curves over $\mathbb{Q}$ by searching for all integral binary quartics $g(X, Y)$ with given invariants.

- The search uses bounds derived from reduction theory as above.

- This is implemented in my program `mwrank`.

- In 1997 I reworked the reduction theory and obtained better bounds in the mixed signature case, by using $\chi(g)$ instead of an alternative.

II. Complex Binary Forms
Complex Binary Hermitian Forms

We replace positive definite real binary quadratic forms with positive definite complex binary Hermitian forms:

$$\mathrm{BHF}(\mathbb{C})_+ = \{aZ_1\overline{Z_1} + b\overline{Z_1}Z_2 + \bar{b}Z_1\overline{Z_2} + cZ_2\overline{Z_2} \mid a, c \in \mathbb{R}_{>0}, b \in \mathbb{C}, \Delta = |b|^2 - ac < 0\}$$

Notation: $F = [a, b, c]$.
Note: $aF(Z_1, Z_2) = |aZ_1 + bZ_2|^2 - \Delta|Z_2|^2$ so these forms take positive *real* values.

Hyperbolic 3-space

We replace the upper half-plane $\mathcal{H}_2$ with hyperbolic 3-space:

$$\mathcal{H}_3 = \mathbb{C} \times \mathbb{R}_{>0} = \{(z,t) \mid z \in \mathbb{C}, t \in \mathbb{R}_{>0}\} = \{q = z + tj \in \mathbb{H}\},$$

also called quaternionic upper half-space.
"Root map":

$$\mathrm{BHF}(\mathbb{C})_+ \to \mathcal{H}_3$$

$$F = [a,b,c] \mapsto q = z + tj \quad \text{with} \quad (z,t) = \left(\frac{-b}{a}, \frac{\sqrt{|\Delta|}}{a}\right)$$

Note: $F(Z_1, Z_2) = a|Z_1 - qZ_2|^2 = a|Z_1 - Z_2 q|^2$.
Inverse map: $q = (z,t) \mapsto [1, -z, |z|^2 + t^2]$.
Bijection:

$$\mathrm{BHF}(\mathbb{C})_+/\mathbb{R}_{>0} \longleftrightarrow \mathcal{H}_3.$$

Group actions

$G = \mathrm{SL}(2, \mathbb{C})$ acts on $\mathrm{BHF}(\mathbb{C})_+$ on the right via

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : F(Z_1, Z_2) \mapsto F^M(Z_1, Z_2) = f(aZ_1 + bZ_2, cZ_1 + dZ_2)$$

preserving Δ; new leading coefficient is $f^M(1, 0) = f(a, c) > 0$.
G acts transitively on $\mathcal{H}_3$ on the left via

$$M : q \mapsto M(q) = (aq + b)(cq + d)^{-1},$$

or

$$(z, t) \mapsto \left(\frac{(az + b)\overline{(cz + d)} + a\bar{c}t^2}{|cz + d|^2 + |c|^2t^2}, \frac{t}{|cz + d|^2 + |c|^2t^2} \right)$$

The root map is G-equivariant as before: best checked using the quaternion notation!

Discrete subgroups and integral points

For analogues of $\mathrm{SL}(2,\mathbb{Z}) \subset \mathrm{SL}(2,\mathbb{R})$ and $\mathrm{BQF}(\mathbb{Z})_+ \subset \mathrm{BQF}(\mathbb{R})_+$ we need a discrete subring of $\mathbb{C}$. Classically, Julia and others just took "integral complex numbers" to be Gaussian integers $\mathbb{Z}[i]$. We will take the ring of integers $\mathcal{O} = \mathcal{O}_K$ in any imaginary quadratic field $K \subset \mathbb{C}$.

The "Bianchi group" $\Gamma = \mathrm{SL}(2,\mathcal{O})$ acts on $\mathrm{BHF}(\mathcal{O})_+$, preserving discriminants, and also (discretely) on $\mathcal{H}_3$. The latter action has a fundamental region $\mathcal{F} = \mathcal{F}_K$, depending on K, shaped like a hyperbolic polyhedron. For small $\mathrm{disc}(K)$ this was determined by Bianchi and others in the 19th century.

The cases $h_K = 1$ and $h_K > 1$ are significantly different.

When $h_K = 1$: the only cusp in $\mathcal{F}$ is at infinity, and there exists $t_K > 0$ such that $(z,t) \in \mathcal{F} \implies t \geq t_K$.

e.g. $t^2_{\sqrt{-1}} = \frac{1}{2}$, $t^2_{\sqrt{-2}} = \frac{1}{4}$.

When $h_K > 1$: $\mathcal{F}$ contains other cusps on $\{t = 0\}$, and no such t_K exists.

Reduction of Hermitian forms

Assume $h_K = 1$. Define $F \in \mathrm{BHF}(\mathbb{C})_+$ to be *reduced* when $q(F) \in \mathcal{F}$. Then

$$F = [a, b, c] \quad \text{reduced} \implies \frac{\sqrt{|\Delta|}}{a} \geq t_K > 0 \implies 0 < a \leq t_K^{-1}\sqrt{|\Delta|}.$$

As over $\mathbb{Z}$ this allows us to enumerate the *finite* set of reduced integral forms $F \in \mathrm{BHF}(\mathcal{O})_+$ with given (integer) discriminant Δ: take the above bound on $a \in \mathbb{Z}$, take $b \in \mathcal{O}$ with $-b/a$ in the projection of $\mathcal{F}$ to $\mathbb{C}$, and solve for c.

When $h_K > 1$, obtaining bounds is harder. $\mathcal{F}$ contains points (z, t) with arbitrarily small t, and hence there is no upper bound for the leading coefficient a of a reduced form with given discriminant. The book of Elstrodt, Mennicke and Grunewald shows how to get around this, but we have not seen this done explicitly.

Reduction of higher degree forms

We assume that $h_K = 1$ from now on.

Can we reduce binary forms $g(X,Y) \in \mathbb{C}[X,Y]_n$ with respect to $\Gamma = \mathrm{SL}(2, \mathcal{O}_K)$?
Again we need a covariant, $i.e.$ G-equivariant map $\chi : \mathbb{C}[X,Y]_n \to \mathrm{BHF}(\mathbb{C})_+$ or $\chi : \mathbb{C}[X,Y]_n \to \mathcal{H}_3$.
The *same* formula for $\chi(g)$ does the job! Define

$$\chi(g) = \sum_{i=1}^{n} |g'(\alpha_i)|^{\frac{2}{2-n}} \left|Z_1 - \alpha_i Z_2\right|^2 .$$

Now the α_i are the (complex) roots of g, and each $\left|Z_1 - \alpha_i Z_2\right|^2$ is a binary Hermitian form, $[1, -\alpha_i, |\alpha_i|^2]$.
Proof of covariance is as before.

A uniqueness result

Theorem [JEC & Stoll]

1. For $n = 3$ and $n = 4$, χ is the unique covariant map $\mathbb{C}[X,Y]_n \longrightarrow \mathrm{BHF}(\mathbb{C})_+$ (or $\mathbb{C}[X,Y]_n \to \mathcal{H}_3$);

2. χ is compatible with complex conjugation, hence restricts to a covariant map $\mathbb{R}[X,Y]_n \to \mathrm{BQF}(\mathbb{R})_+$ (or $\mathbb{R}[X,Y]_n \to \mathcal{H}_2$);

3. For real forms of pure signature, χ is the unique such covariant.

Here $\mathcal{H}_2$ embeds in $\mathcal{H}_3$ via $x + yi \mapsto x + yj$.

Application : reduction of forms over $\mathcal{O}_K$

As above, let $\mathcal{O}_K$ be an imaginary quadratic rings of integers of class number 1.

Proposition [Womack] Let $g \in \mathbb{C}[X,Y]_n$ with leading coefficient $a_0 = g(1,0)$ and discriminant Δ. Write $\chi(g) = [a,b,c]$. Then

$$a \geq n|\Delta|^{-2/n(n-2)}|a_0|^{2/n}.$$

Now when g is reduced we also have upper bounds for a in terms of $\mathrm{disc}(\chi(g))$, which may be expressed in terms of invariants of g. Hence we can bound the leading coefficient of a reduced form in terms of its invariants..

$n = 3$: Here we have $a \geq 3|\Delta|^{-2/3}|a_0|^{2/3}$ and $\mathrm{disc}(\chi(g)) = -3|\Delta|$; hence $a \leq t_K^{-1}\sqrt{|\mathrm{disc}(\chi(g))|}$ implies, for a reduced cubic in $\mathcal{O}_K[X,Y]$:

$$|a_0| \leq 3^{-3/4} t_K^{-3/2} |\Delta|^{1/4}.$$

Application : reduction of cubics (contd.)

We now apply the same to the cubic covariant of g, which is reduced when g is (by uniqueness). It has discriminant $3^6\Delta^3$ and its leading coefficient U satisfies the syzygy $U^2 + 27\Delta a_0^2 = P^2$ (where P is as before the leading coefficient of the Hessian). We obtain

$$|U| \leq 3^{3/4} t_K^{-3/2} |\Delta|^{3/4}, \qquad \text{and hence} \qquad |P| \leq 3^{3/4}(1 + 3^{3/2}) t_K^{-3/2} |\Delta|^{3/4}.$$

Since the unit group is finite this gives us a finite set of (a_0, P) pairs for fixed Δ, and hence we may enumerate all reduced cubics.

A similar approach should allow the enumeration of quartics in $\mathcal{O}_K[X, Y]_4$ with given invariants I, J, but the details have not been worked out (in the imaginary quadratic case) since alternative methods of 2-descent (applicable to general number fields) seem more effective.

Other number fields

Let K be a number fields with r_1 real embeddings and $2r_2$ pairs of complex embeddings. Then $\mathrm{SL}(2, \mathcal{O}_K)$ acts discretely on

$$\mathcal{H}_2^{r_1} \times \mathcal{H}_3^{r_2}.$$

It should be possible to develop a theory of reduction based on a fundamental region for this action, though the details would be complicated.

For real quadratic fields $(r_1, r_2) = (2, 0)$ with class number one this was done for quartics by P. Serf, leading to an implementation of 2-descent in these cases. The bounds depend critically on the size of the fundamental unit of K; even in the simplest cases the resulting program was rather slow.

It remains to be seen whether a practical reduction theory can be made to work efficiently for more general fields.