Reduction of binary forms

John Cremona

University of Nottingham, UK

(joint work with Michael Stoll)

The Problem

Let $F(X,Z) \in \mathbb{Z}[X,Z]$ be homogeneous of degree $2g+2$ and without multiple factors; then

$$y^2 = F(x,1)$$

defines a *hyperelliptic curve* C over $\mathbb{Q}$ of genus g.
NB $F(x,1)$ has degree either $2g+2$ or $2g+1$

Problem 1.
Find a 'better' equation for C (with 'smaller' coefficients)!

Since isomorphisms between hyperelliptic curves come from automorphisms of $\mathbb{P}^1$, this means the following.

Problem 2.
Find $a,b,c,d,e \in \mathbb{Q}$ with $ad \neq bc$ and $e \neq 0$ such that

$$F_1(X,Z) = e^2\, F(aX+bZ, cX+dZ)$$

has integral coefficients, 'smaller' than those of F.

Two Subproblems

The problem of reducing F splits into two subproblems.

Subproblem 1 (p-adic reduction).
Minimise p-adic valuations of the invariants
(or of the discriminant) of F.

Subproblem 2 (reduction over $\mathbb{Z}$).
Reduce F using unimodular transformations
($a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$, $e = 1$).

For $g = 1$, Subproblem 1 is related to Tate's algorithm.

For $g > 1$ there exists an algorithm for Subproblem 1, see
Q. Liu: *Modèles entiers des courbes hyperelliptiques* … ,
Trans. Amer. Math. Soc. **348**, 4577–4610 (1996).

We will focus on Subproblem 2 in this talk.

Positive Definite Quadratic Forms

Since Gauss, a positive definite quadratic form

$$F(X,Z) = a\,X^2 + b\,XZ + c\,Z^2$$

$$(a,b,c \in \mathbb{R}; \quad \Delta = b^2 - 4ac < 0; \quad a,c < 0)$$

is called *reduced*, if its 'zero' $z(F) \in \mathcal{H}$
is in the usual fundamental domain $\mathcal{F}$ of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathcal{H}$.
($\mathcal{H}$ is the upper half-plane; $F(z(F),1) = 0$)

Since the map $F \mapsto z(F)$ is $\mathrm{SL}(2,\mathbb{R})$-*covariant:*

$$z(F \circ \gamma) = \gamma^{-1} \cdot z(F) \quad \text{for } \gamma \in \mathrm{SL}(2,\mathbb{R}),$$

we can reduce F by finding $\gamma \in \mathrm{SL}(2,\mathbb{Z})$ such that

$$\gamma \cdot z(F) \in \mathcal{F}\,;$$

then $F \circ \gamma^{-1}$ is reduced.

Thus, each $SL(2,\mathbb{Z})$-orbit of forms has a unique reduced representative,
and the coefficients of the reduced form are the smallest in the orbit (in a precise sense).

Positive Definite Hermitian Forms

$$F(X,Z) = a\,|X|^2 + b\,\overline{X}Z + \overline{b}\,X\,\overline{Z} + c\,|Z|^2$$

$$(a, c \in \mathbb{R}, b \in \mathbb{C}; \quad \Delta = |b|^2 - 4ac < 0; \quad a, c > 0)$$

$$F(X,Z) = a\left|X + \frac{b}{a}Z\right|^2 - \frac{\Delta}{a}|Z|^2$$

We say that F has "root"

$$z(F) = \left(\frac{-b}{a}, \frac{\sqrt{|\Delta|}}{a}\right) \in \mathcal{H}^3$$

where $\mathcal{H}^3$ is hyperbolic 3-space ("upper half-space"):

$$\mathcal{H}^3 = \{(z,t) \mid z \in \mathbb{C}, t \in \mathbb{R}_{>0}\}.$$

The map $F \mapsto z(F)$ is $\mathrm{SL}(2,\mathbb{C})$-*covariant:*

$$z(F \circ \gamma) = \gamma^{-1} \cdot z(F) \quad \text{for } \gamma \in \mathrm{SL}(2,\mathbb{C}).$$

We can define a notion of being "reduced" if we fix a discrete subgroup Γ of $\mathrm{SL}(2,\mathbb{C})$ and require $z(F)$ to lie in a specific fundamental domain for Γ.

The Basic Idea

We generalise to forms of higher degree.

Let $\mathbb{R}[X, Z]'_n$ denote the set of forms of degree n without multiple factors.

Aim.
Define an $\mathrm{SL}(2, \mathbb{R})$-covariant map

$$\mathbb{R}[X, Z]'_n \longrightarrow \mathcal{H}\,, \qquad F \longmapsto z(F)$$

such that F is 'small' when $z(F) \in \mathcal{F}$.

Then we call F *reduced* if $z(F) \in \mathcal{F}$.

We can reduce a given F by the same algorithm as that used for positive definite quadratic forms.

We also want to extend this to complex coefficients:

$$\mathbb{C}[X, Z]'_n \longrightarrow \mathcal{H}^3\,, \qquad F \longmapsto z(F)$$

should be $\mathrm{SL}(2, \mathbb{C})$-covariant.

Real and Complex covariant maps

Real case: We need an $\mathrm{SL}(2,\mathbb{R})$-covariant map:

$$\mathbb{R}[X,Z]'_n \longrightarrow \{\text{PDBQF}\} \longrightarrow \mathcal{H}$$

$$F \mapsto Q(F), \qquad Q \mapsto z(Q)$$

Complex case: We need an $\mathrm{SL}(2,\mathbb{C})$-covariant map:

$$\mathbb{C}[X,Z]'_n \longrightarrow \{\text{PDHQF}\} \longrightarrow \mathcal{H}^3$$

$$F \mapsto Q(F), \qquad Q \mapsto z(Q)$$

These should be compatible with the inclusions

$$\begin{aligned} \mathbb{R}[X,Z]'_n &\hookrightarrow \mathbb{C}[X,Z]'_n \\ \{\text{PDBQF}\} &\hookrightarrow \{\text{PDHQF}\} \\ \mathcal{H} &\hookrightarrow \mathcal{H}^3 \\ x+yi &\mapsto (z,t) = (x,y) \end{aligned}$$

Degrees 3 and 4

For geometric reasons, there is a *unique* such map for forms of degrees 3 and 4.

Any set of 3 or 4 distinct points in $\mathbb{C}$ has a non-trivial stabiliser in $\mathrm{SL}(2, \mathbb{C})$, and this stabiliser has a unique fixed point in $\mathcal{H}^3$.

$z(F)$ must be the point associated to the roots of F in this way.

A formula for real forms F.

$$z_0(F) = z(Q_0(F)), \quad \text{where}$$

$$Q_0(F)(X, Z) = \sum_{\alpha : f(\alpha)=0} \frac{1}{|f'(\alpha)|^{2/(n-2)}} (X - \alpha Z)(X - \bar{\alpha} Z)$$

(We use the convention $f(x) = F(x, 1)$, and $n = \deg F$.)

Note.

This defines a covariant map on real forms of *any* degree $n > 2$.

So we can use this to define

$$F \text{ is } Q_0\text{-reduced} \iff z_0(F) \in \mathcal{F}.$$

Higher Degrees — Julia's Approach

For degrees $n \geq 5$, there are many covariant maps $F \mapsto z(F)$.

How do we find a good one?

Gaston Julia (1917) suggests to take

$$z(F) = z(Q(F)), \quad \text{where}$$
$$Q(F)(X,Z) = \sum_{\alpha : f(\alpha)=0} t_\alpha (X - \alpha Z)(X - \bar{\alpha} Z)$$

with suitable $t_\alpha > 0$.

(The possible $z(F) \in \mathcal{H}$ then form the interior of the convex hull of the roots α.)

When $z(F) \in \mathcal{F}$, then the coefficients of F can be bounded in terms of

$$\theta = \frac{F(1,0)^2 |\operatorname{disc} Q(F)|^{n/2}}{\prod_\alpha t_\alpha}.$$

So we want to choose t_α such that θ is minimised.

Minimising θ

Let

$$F(X,Z) = a_0 \prod_{j=1}^{n} (X - \alpha_j Z)\,.$$

Then

$$\theta = \frac{a_0^2 \left(\sum_{j<k} |\alpha_j - \alpha_k|^2 t_j t_k\right)^{n/2}}{\prod_{j=1}^{n} t_j}\,.$$

We can prove that (for $n \geq 3$) this is strictly convex from below on $V = \{(t_1,\ldots,t_n) | t_j > 0, t_1 \ldots t_n = 1\}$ and approaches infinity when one of the $t_j \to \infty$.

Conclusion.
θ has a unique critical point on V, and it provides a global minimum.

Conclusion.
The map $F \mapsto z(F) = z(Q(F))$, where $Q(F)$ is defined using the minimsing t_j, is covariant.

We define

$$F \text{ is reduced} \iff z(F) \in \mathcal{F}\,.$$

Another Description

Define

$$\tilde{F}(t,u) = \frac{a_0^2 \prod_j ((t-\alpha_j)(t-\bar{\alpha}_j)+u^2)}{u^n}$$

for $t \in \mathbb{R}$, $u > 0$.

If (t,u) is a critical point of $\tilde{F}$, then setting

$$t_j = \frac{u^2}{(t-\alpha_j)(t-\bar{\alpha}_j)+u^2}$$

gives a critical point of θ and 'vice versa'.

Conclusion.
$z(F) = t + iu$, where (t,u) is the unique critical point of $\tilde{F}$; at this point, $\tilde{F}$ has a global minimum, which is θ (up to a factor of n^n).

We can use this to find $z(F)$ numerically for any given F.

A Geometric Interpretation

When $t \in \mathbb{C}$, $u > 0$ and $\alpha \in \mathbb{C}$, then

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

is a measure for the hyperbolic distance of $(t, u) \in \mathcal{H}^3$ from the boundary point α (up to an additive constant).

So $\log \tilde{F}(t, u)$ measures the sum of the distances of (t, u) from the roots of F.

Conclusion.
$z(F) = t + iu$, where $(t, u) \in \mathcal{H}^3$ is the point minimising the sum of the distances to the roots of F.

Conclusion.
This point (t, u) is characterised by the fact that the sum of the unit tangent vectors pointing towards the roots of F vanishes.

(This is easy to see when the degree is 3 or 4.)

The Reduction Algorithm

Input: $F = a_0X^n + a_1X^{n-1}Z + \cdots + a_nZ^n \in \mathbb{Z}[X,Z]'_n$

Output: A reduced form $\mathrm{SL}(2,\mathbb{Z})$-equivalent to F.

1. Compute $z = z(F)$.
2. While $z \notin \mathcal{F}$ do

   2.1. Let $m = \mathrm{Round}(\mathrm{Re}(z))$.

   2.2. Set $F(X,Z) = F(X+mZ,Z)$, $z = z - m$.

   2.3. If $|z| < 1$, then set $F(X,Z) = F(Z,-X)$, $z = -1/z$.

Remarks.

- We can use this with $z_0(F)$ in place of $z(F)$.
  (Faster, since $z_0(F)$ is computed more easily.)
- Be careful with exit condition to avoid infinite looping.
- Re-compute $z(F)$ from time to time to compensate precision loss.

Example

$$C : y^2 = 19x^8 - 262x^7 + 1507x^6 - 4784x^5 + 9202x^4 - 10962x^3 + 7844x^2 - 3040x + 475$$

(Taken from H.-J. Weber's thesis (Essen, 1996).)

For the first reduction steps, we use $z_0(F)$. The roots of f are

$$0.42798171, \quad 1.30152156, \quad 1.31947230, \quad 4.31651243,$$
$$1.69098301 \pm 0.72287100\,i, \quad 1.52100984 \pm 0.12866975\,i\,.$$

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

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

$m = 1$, so we do a shift and replace f with

$$f_1(x) = f(x+1) = 19x^8 - 110x^7 + 205x^6 - 180x^5 + 47x^4 + 40x^3 - 35x^2 + 10x - 1$$

and z with $z_1 = z - 1 = 0.38323301 + 0.31233552\,i$.

$|z_1| < 1$, so we invert f_1 to get

$$f_2(x) = x^8 f_1(-1/x) = -x^8 - 10x^7 - 35x^6 - 40x^5 + 47x^4 + 180x^3 + 205x^2 + 110x + 19$$

and set $z_2 = -1/z_1 = -1.56792167 + 1.27785869\,i$.

Example, continued

Now $m = -2$, so

$$\begin{aligned} f_3(x) &= f_2(x-2) \\ &= -x^8 + 6x^7 - 7x^6 - 12x^5 + 27x^4 - 4x^3 - 19x^2 + 10x - 5 \end{aligned}$$

and $z_3 = z_2 + 2 = 0.43207833 + 1.27785869\, i \in \mathcal{F}$,
so F_3 is Q_0-reduced.

Now we use Julia's covariant $z(F)$. We find the roots of f_3 and use some numerical method to compute

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

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

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

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