# Reducing models for branched covers of the projective line

John Voight
University of Sydney

joint work with
Ciaran Schembri and Sam Schiavone

Arithmetic, Geometry, Cryptography and Coding Theory
CIRM, Luminy
9 June 2025

# Motivation

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

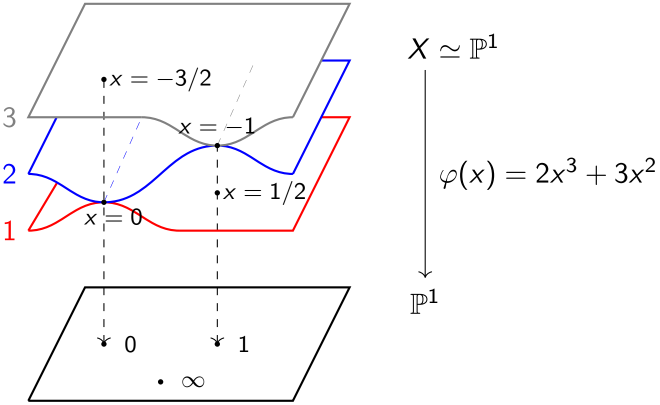
$$\varphi(x) = \frac{\frac{8676\sqrt{-6}+56137}{8688}x^7 + \frac{6920140\sqrt{-6}+5383305}{1381392}x^6}{\begin{aligned} & x^7 + \frac{201651\sqrt{-6}+153613}{47965}x^6 + \frac{90228166\sqrt{-6}-323404767}{10168580}x^5 \\ & - \frac{2051197711\sqrt{-6}+5182860568}{215573896}x^4 + \frac{3078070363644\sqrt{-6}-851257957203}{91403331904}x^3 \\ & + \frac{556948888943428\sqrt{-6}-593744287985961}{4844376590912}x^2 \\ & + \frac{29295834562711316\sqrt{-6}+51072269883081183}{1283759796591680}x \\ & + \frac{3410272680217874724\sqrt{-6}-2427837788491257163}{68039269219359040} \end{aligned}}$$

$$\begin{aligned} X\colon\ & 3x^6(x-\sqrt{-6}+1)t + \\ & \sqrt{-6}\big((-4\sqrt{-6}-3)x^3 + (3\sqrt{-6}-3)x^2 + \\ & (-2\sqrt{-6}+9)x + \sqrt{-6}-3\big) = 0 \end{aligned}$$

$$\begin{aligned} \varphi\colon X &\to \mathbb{P}^1 \\ (t,x) &\mapsto t \end{aligned}$$

# Belyi maps

We are interested in finite branched covers $\varphi\colon X \to \mathbb{P}^1$; when $\varphi$ is unramified away from $\{0, 1, \infty\}$, we call $\varphi$ a **Belyi map**.




Grothendieck in his *Esquisse* studied the action of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \,|\, \mathbb{Q})$ on Belyi maps. LMFDB!

# Minimization and reduction

## Problem

*Given a model $\varphi \colon X \to Y$ of a map of schemes over a number field $K$, find a reduced model with smaller size.*

There is also *minimization*, where one seeks a model which minimizes an invariant (for example, the absolute discriminant). These often go together.

This is an important but hard problem in general!

- Elliptic curves $E \hookrightarrow \mathbb{P}^2$ (Tate's algorithm for minimal Weierstrass model)
- Point clusters $X \hookrightarrow \mathbb{P}^n$ (Stoll)
- Binary forms and cyclic covers $X \to \mathbb{P}^1$ (Stoll–Cremona, Hutz–Stoll)
- $n$-covers of elliptic curves (Cremona–Fisher–Stoll, Fisher)
- Curves over $\mathbb{Q}$ (van Hoeij–Novocin)
- Hypersurfaces $X \hookrightarrow \mathbb{P}^n$ (Elsenhans–Stoll)

This work: try reducing/minimizing the map $\varphi$.

# Algorithm overview

- Input: model for a map of curves $\varphi\colon X \to \mathbb{P}^1$
- Output: a reduced model

Steps:

1. Create a small (singular) plane model
2. Rescale the coefficients of the plane model
3. Rinse and repeat, return the smallest one

# Step 1: (singular) plane models

The map $\varphi\colon X \to \mathbb{P}^1$ describes a function field extension $K(\mathbb{P}^1) = K(t) \hookrightarrow K(X)$. We look for small functions $x \in K(X)$ such that $K(X) = K(t,x)$. Then there is an equation $X\colon f(t,x) = 0$ and $\varphi(t,x) = t$ (computed using elimination theory).

Small functions may come from anywhere! Gonal maps, over finite fields, ...

**Idea**

*If the map is small then its ramification points should be small—and there's nothing smaller than zero and $\infty$!*

- Let $W \leq \operatorname{Div} X$ be the subgroup of $K$-rational divisors supported within the set of ramification points on $\varphi$.
- For $d \geq 0$, let $W_d := W \cap \operatorname{Div}^d(K)$ be those divisors $D = D_0 - D_\infty$ with $\max(\deg D_0, \deg D_\infty) = d$.
- Using Riemann–Roch, find $D \in W_d$ such that $\dim_K L(D) = 1$, so $x \in L(D)$ is unique up to rescaling (by $K^\times$).

# Step 2: toric reduction

Working more generally now, let

$$f(x) = \sum_{\nu} a_\nu x^\nu \in K[x] = K[x_1, \ldots, x_n]$$

and consider the rescaling action of $(K^\times)^{n+1}$ by

$$(b, c) \cdot f(x) = (b_1, \ldots, b_n, c) \cdot f(x_1, \ldots, x_n) := cf(b_1 x_1, \ldots, b_n x_n).$$

We want to find $(b, c) \in (K^\times)^{n+1}$ such that $(b, c) \cdot f \in \mathbb{Z}_K[x]$ is minimized.

**Idea**

*Work locally: for all places $v$, minimize valuations/absolute values of the coefficients.*

# Step 2: nonarchimedean toric reduction

Starting with $f(x) = \sum_\nu a_\nu x^\nu$ we compute that

$$(b, c) \cdot f(x) = \sum_\nu (a_\nu b^\nu c) x^\nu.$$

Since we want the smallest equation, for each prime $\mathfrak{p}$ we want to minimize

$$\sum_\nu \operatorname{ord}_\mathfrak{p}(a_\nu b^\nu c), \quad \text{subject to } \operatorname{ord}_\mathfrak{p}(a_\nu b^\nu c) \geq 0 \text{ for all } \nu.$$

Writing

$$b_i \mathbb{Z}_K = \mathfrak{p}^{z_i}, \qquad c\mathbb{Z}_K = \mathfrak{p}^w$$

we want to minimize

$$\left(\sum_\nu \nu\right) \cdot z + w, \quad \text{subject to } \nu \cdot b + w \geq -\operatorname{ord}_\mathfrak{p}(a_\nu) \text{ for all } \nu.$$

This is an *integer linear program* which can be solved efficiently!

# Step 2: nonarchimedean toric reduction, example

Consider $p = 2$ and

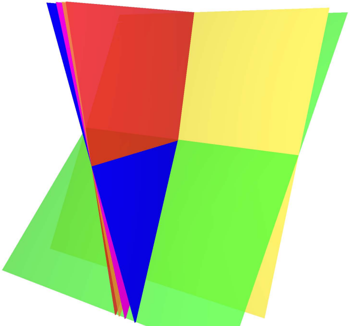
$$f(x_1, x_2) = -256x_1^2 + 256x_1 + x_2^6 - 12x_2^5 + 48x_2^4 - 64x_2^3.$$

We rescale by $2^w f(2^{z_1}x_1, 2^{z_2}x_2)$, with

$$\nu = (2,0), (1,0), (0,6), (0,5), (0,4), (0,3)$$

$$\mathrm{ord}_2(a_\nu) = 8, 8, 0, 2, 4, 6$$

We want to minimize $3x_1 + 18x_2 + 6w$ subject to:



$$2z_1 + 0z_2 + w \geq -8$$

$$1z_1 + 0z_2 + w \geq -8$$

$$0z_1 + 6z_2 + w \geq 0$$

$$0z_1 + 5z_2 + w \geq -2$$

$$0z_1 + 4z_2 + w \geq -4$$

$$0z_1 + 3z_2 + w \geq -6$$

# Step 2: nonarchimedean toric reduction, example

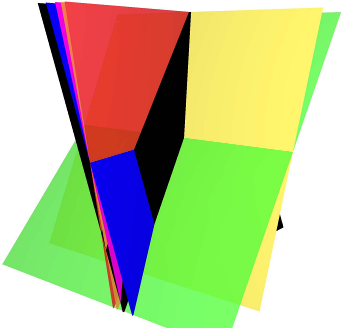
Consider $p = 2$ and

$$f(x_1, x_2) = -256x_1^2 + 256x_1 + x_2^6 - 12x_2^5 + 48x_2^4 - 64x_2^3.$$

We rescale by $2^w f(2^{z_1}x_1, 2^{z_2}x_2)$, with

$$\nu = (2,0), (1,0), (0,6), (0,5), (0,4), (0,3)$$
$$\mathrm{ord}_2(a_\nu) = 8, 8, 0, 2, 4, 6$$

We want to minimize $3x_1 + 18x_2 + 6w$ subject to:



$$2z_1 + 0z_2 + w \geq -8$$
$$1z_1 + 0z_2 + w \geq -8$$
$$0z_1 + 6z_2 + w \geq 0$$
$$0z_1 + 5z_2 + w \geq -2$$
$$0z_1 + 4z_2 + w \geq -4$$
$$0z_1 + 3z_2 + w \geq -6$$

# Step 2: nonarchimedean toric reduction, example

Consider $p = 2$ and

$$f(x_1, x_2) = -256x_1^2 + 256x_1 + x_2^6 - 12x_2^5 + 48x_2^4 - 64x_2^3.$$

We rescale by $2^w f(2^{z_1}x_1, 2^{z_2}x_2)$, with

$$\begin{aligned} \nu &= (2,0),(1,0),(0,6),(0,5),(0,4),(0,3) \\ \mathrm{ord}_2(a_\nu) &= 8,8,0,2,4,6 \end{aligned}$$

The minimum of $3x_1 + 18x_2 + 6w$ in the feasible domain occurs at the vertex

$$(z, w) = (4, 2, -12) \quad \leftrightarrow \quad (b, c) = (2^4, 2^2, 2^{-12})$$

giving the reduction

$$(b, c) \cdot f(x) = -16x_1^2 + x_1 + x_2^6 - 3x_2^5 + 3x_2^4 - x_2^3.$$

# Step 2: nonarchimedean toric reduction, class number issues

**Idea**

*Even if $h(\mathbb{Z}_K) > 1$, principal elements lie in a finite index sublattice.*

Let $S$ be a set of primes (containing the support of the coefficients). We repeat with

$$b_i \mathbb{Z}_K = \prod_{\mathfrak{p} \in S}, \qquad c\mathbb{Z}_K = \mathfrak{p}^{w_\mathfrak{p}}$$

and we now want to minimize

$$\sum_{\mathfrak{p} \in S} \log \mathrm{Nm}(\mathfrak{p}) \left( \left( \sum_{\nu} \nu \right) \cdot z_\mathfrak{p} + w_\mathfrak{p} \right)$$

subject to

$$\nu \cdot z_\mathfrak{p} + w_\mathfrak{p} \geq -\operatorname{ord}_\mathfrak{p}(a_\nu) \quad \text{for all } \nu \text{ and all } \mathfrak{p}$$
$$\sum_{\mathfrak{p} \in S} z_\mathfrak{p} \equiv \sum_{\mathfrak{p} \in S} w_\mathfrak{p} \equiv 0 \pmod{h(\mathbb{Z}_K)}.$$

This is still a linear program (just over a sublattice)!

# Step 2: archimedean toric reduction, setup

For the archimedean places, we proceed similarly but now with a norm coming from the log Minkowski embedding

$$\lambda\colon K^\times \hookrightarrow \mathbb{R}^m.$$

As a measure of "small", we take the $L_2$-norm $\|\ \|$ on $\mathbb{R}^m$ (and restrict to $K^\times$).

Our action is now restricted to $(\mathbb{Z}_K^\times)^{n+1}$ on $K[x]$. The set $\lambda(ua)$ is constrained lattice points in a hyperplane; the minimal norm in this plane is obtained by

$$\underline{a} = \frac{\log(|\operatorname{Nm}(a)|)}{m} \cdot (1, \dots, 1).$$

Accordingly, to minimize a coefficient $a$ means finding $u \in (\mathbb{Z}_K^\times)^{n+1}$ which minimizes

$$\|\lambda(ua) - \underline{a}\| = \|\lambda(u) - (\underline{a} - \lambda(a))\|.$$

# Step 2: archimedean toric reduction, program

We look to minimize

$$\sum_{\nu} \|\lambda(b^{\nu} c) - (\underline{a_{\nu}} - \lambda(a_{\nu}))\|$$

with $(b, c) \in (\mathbb{Z}_K^{\times})^{n+1}$.

## Idea

*Minimizing sums of distances give a semidefinite integer quadratic program.*

Writing $(b, c)$ in terms of a basis of units and expanding out, we need to solve:

$$\text{minimize } z^{\mathsf{T}} Q z + (c')^{\mathsf{T}} z, \quad \text{for } z \in \mathbb{Z}^{m-1},$$

where $Q \in \mathrm{M}_{m-1}(\mathbb{R})_{\mathrm{sym}, \geq 0}$ is positive semidefinite.

The standard approach to solve this: first do so over the reals using a Cholesky decomposition $Q = B^{\mathsf{T}} B$, and then find a closest vector.

# Step 2: archimedean toric reduction, example

Consider the polynomial

$$f(x_1, x_2) = (338\sqrt{2} - 478)x_1 x_2 + 5x_2^3.$$

We have $\mathbb{Z}_K^\times/\{\pm 1\} = \langle 1 - \sqrt{2}\rangle = \langle \epsilon \rangle$, and

$$f(x_1, x_2) = -2\epsilon^7 x_1 x_2 + 5x_2^3.$$

We have $(b, c) = (\epsilon^{z_1}, \epsilon^{z_2}, \epsilon^{z_3})$ (for convenience), and the function to minimize is:

$$\begin{aligned}
&\left\| \begin{pmatrix} -5.48 \\ 6.86 \end{pmatrix} + (z_1 + z_2 + z_3) \begin{pmatrix} -0.88 \\ 0.88 \end{pmatrix} \right\| + \left\| \begin{pmatrix} 1.61 \\ 1.61 \end{pmatrix} + (3z_2 + z_3) \begin{pmatrix} -0.88 \\ 0.88 \end{pmatrix} \right\| \\
&\doteq 1.55z_1^2 + 3.11z_1z_2 + 3.11z_1z_3 + 21.75z_1 + 15.54z_2^2 + 12.43z_2z_3 + 21.75z_2 \\
&\qquad + 3.11z_3^2 + 21.75z_3
\end{aligned}$$

# Step 2: archimedean toric reduction, example

We are reducing the polynomial

$$f(x_1, x_2) = (338\sqrt{2} - 478)x_1x_2 + 5x_2^3.$$

We minimize a quadratic polynomial, written as $\frac{1}{2}z^TQz + (c')^Tz$ where

$$Q = \begin{pmatrix} 3.11 & 3.11 & 3.11 \\ 3.11 & 31.1 & 12.4 \\ 3.11 & 12.4 & 6.21 \end{pmatrix}, \quad c' = \begin{pmatrix} 21.8 \\ 21.8 \\ 21.8 \end{pmatrix}.$$

We find a minimum at $z = (-5, 1, -3)$ (both a real and integer solution). We reduce $f(x_1, x_2)$ to get

$$\epsilon^{-3}f(\epsilon^{-5}x_1, \epsilon^1x_2) = -2x_1x_2 + 5x_2^3.$$

# Conclusion

- We described an algorithm for reduction of a branched cover of the projective line $\varphi \colon X \to \mathbb{P}^1$.
- The two steps: find small plane model, then rescale the equation (reducing via a torus action).
- We ran this algorithm on the 1111 Belyi maps in the LMFDB, sometimes with dramatic reduction.
- Next step: write the coefficients in a number field with respect to an LLL-reduced basis (instead of a power basis).
- The toric reduction works in principle for any variety.