# Numerical computation of endomorphism rings of Jacobians

Nils Bruin (Simon Fraser University), Jeroen Sijsling (Ulm),
Alexandre Zotine (Simon Fraser University)

July 16, 2018, Madison

# Setting

- $k \subset \mathbb{C}$ a number field
- $C$ a proper smooth absolutely irreducible curve over $k$ of genus $g$, represented by an affine plane model:

$$\tilde{C} : f(x,y) = 0 \text{ where } f(x,y) \in k[x,y].$$

# Setting

- $k \subset \mathbb{C}$ a number field
- $C$ a proper smooth absolutely irreducible curve over $k$ of genus $g$, represented by an affine plane model:

$$\tilde{C} : f(x,y) = 0 \text{ where } f(x,y) \in k[x,y].$$

**Analytic Jacobian:**

$$J(\mathbb{C}) \cong \mathrm{H}^0(C_{\mathbb{C}}, \Omega^1_C)^* / \mathrm{H}_1(C(\mathbb{C}), \mathbb{Z}) \cong \mathbb{C}^g / \Omega \mathbb{Z}^{2g},$$

# Setting

- $k \subset \mathbb{C}$ a number field
- $C$ a proper smooth absolutely irreducible curve over $k$ of genus $g$, represented by an affine plane model:

$$\tilde{C} : f(x,y) = 0 \text{ where } f(x,y) \in k[x,y].$$

**Analytic Jacobian:**

$$J(\mathbb{C}) \cong \mathrm{H}^0(C_{\mathbb{C}}, \Omega^1_C)^* / \mathrm{H}_1(C(\mathbb{C}), \mathbb{Z}) \cong \mathbb{C}^g / \Omega \mathbb{Z}^{2g},$$

- Basis for $\mathrm{H}^0(C_{\mathbb{C}}, \Omega^1_C)$: $\omega_1, \dots, \omega_g$
- Basis for $\mathrm{H}_1(C(\mathbb{C}), \mathbb{Z})$: $\alpha_1, \dots, \alpha_g, \beta_1, \dots, \beta_g$
- Period matrix: $\Omega = \left( \int_{\alpha_j} \omega_i \middle| \int_{\beta_j} \omega_i \right)_{i,j}$

**Goal:** Numerically compute $\Omega$ and read off properties of $C$.

# Previous work

**Design criterion:** Applications need lots of digits. Machine precision (53 bits) is not enough.
**Other work:**

**Deconinck-van Hoeij (2001):** General case (Maple)

**van Wamelen (2006):** Hyperelliptic curves (Magma)

**Molin-Neurohr (2017):** Superelliptic curves (C/Arb)

**Neurohr (2018):** General implementation (in Magma?)

# Previous work

**Design criterion:** Applications need lots of digits. Machine precision (53 bits) is not enough.

**Other work:**

**Deconinck-van Hoeij (2001):** General case (Maple)

**van Wamelen (2006):** Hyperelliptic curves (Magma)

**Molin-Neurohr (2017):** Superelliptic curves (C/Arb)

**Neurohr (2018):** General implementation (in Magma?)

**Our contributions:**

- Use *certified* homotopy continuation
- Simple way of getting homology generators
- Flexible implementation that is easy to improve and adapt (in Sage)
- Compute automorphisms of $C$ via Torelli theorem

# Basis for $\mathrm{H}^0(C_{\mathbb{C}}, \Omega^1_C)$

$\mathrm{H}^0(C_{\mathbb{C}}, \Omega^1_C) = \mathrm{H}^0(C, \Omega^1_C) \otimes \mathbb{C}$ contains the *regular differentials* on $C$ (i.e., the ones that have no poles)

- If $\tilde{C} \colon f(x,y) = 0$ with $\deg(f) = n$ then

$$\mathrm{H}^0(C, \Omega^1_C) \subset \left\{ \frac{h\,dx}{\partial_y f(x,y)} : \deg(h) \leq n-3 \right\}.$$

- Singularities impose linear conditions on $h$.
- If singularities are in $\{(1:0:0),(0:1:0),(0:0:1)\}$, conditions are easy to write down
- Otherwise, *adjoint ideal* gives required information
- Algebraic process, implemented in Singular.

**Result:** Basis $\omega_1, \ldots, \omega_g$, where

$$\omega_i = \frac{h_i(x,y)\,dx}{\partial_y f(x,y)} \text{ with } h_i \in k[x,y]$$

# Basis for $\mathrm{H}_1(C(\mathbb{C}), \mathbb{Z})$

- $\mathrm{H}_1(C(\mathbb{C}), \mathbb{Z})$ consists of *cycles* modulo equivalence

# Basis for $\mathrm{H}_1(C(\mathbb{C}), \mathbb{Z})$

- $\mathrm{H}_1(C(\mathbb{C}), \mathbb{Z})$ consists of *cycles* modulo equivalence
- $C(\mathbb{C})$ is a compact Riemann surface, so $\mathrm{H}_1(C(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}^{2g}$
- Generated by classes of generators of the fundamental group

# Basis for $\mathrm{H}_1(C(\mathbb{C}),\mathbb{Z})$

- $\mathrm{H}_1(C(\mathbb{C}),\mathbb{Z})$ consists of *cycles* modulo equivalence
- $C(\mathbb{C})$ is a compact Riemann surface, so $\mathrm{H}_1(C(\mathbb{C}),\mathbb{Z}) \simeq \mathbb{Z}^{2g}$
- Generated by classes of generators of the fundamental group
- $C(\mathbb{C})$ is an oriented topological surface, so $\mathrm{H}_1(C(\mathbb{C}),\mathbb{Z})$ comes with a non-degenerate alternating intersection pairing.

# Basis for $\mathrm{H}_1(C(\mathbb{C}),\mathbb{Z})$

- $\mathrm{H}_1(C(\mathbb{C}),\mathbb{Z})$ consists of *cycles* modulo equivalence
- $C(\mathbb{C})$ is a compact Riemann surface, so $\mathrm{H}_1(C(\mathbb{C}),\mathbb{Z}) \simeq \mathbb{Z}^{2g}$
- Generated by classes of generators of the fundamental group
- $C(\mathbb{C})$ is an oriented topological surface, so $\mathrm{H}_1(C(\mathbb{C}),\mathbb{Z})$ comes with a non-degenerate alternating intersection pairing.

**Strategy:**

- Determine loops on $C(\mathbb{C})$ that generate fundamental group
- Compute their intersection pairing matrix
- Use $\mathbb{Z}$-linear algebra to get a basis for $\mathrm{H}_1(C(\mathbb{C}),\mathbb{Z})$.

**One solution:** Tretkoff-Tretkoff (1984) – rather opaque algorithm.

# Lifting homotopy

Consider finite cover $\tilde{C} \to \mathbb{C}; \;\; (x,y) \mapsto x$ of degree $n = \deg_y(f)$.
Unramified outside

$$S = \{x \in \mathbb{C} : \mathrm{disc}_y f(x,y) = 0\}$$

# Lifting homotopy

Consider finite cover $\tilde{C} \to \mathbb{C};\ (x,y) \mapsto x$ of degree $n = \deg_y(f)$. Unramified outside

$$S = \{x \in \mathbb{C} : \mathrm{disc}_y f(x,y) = 0\}$$

- Determine a connected plane graph $(V,E)$ in $\mathbb{C} - S$ for which a cycle basis generates the fundamental group of $\mathbb{C} - S$

# Lifting homotopy

Consider finite cover $\tilde{C} \to \mathbb{C}; \;\; (x,y) \mapsto x$ of degree $n = \deg_y(f)$. Unramified outside

$$S = \{x \in \mathbb{C} : \mathrm{disc}_y f(x,y) = 0\}$$

- Determine a connected plane graph $(V,E)$ in $\mathbb{C} - S$ for which a cycle basis generates the fundamental group of $\mathbb{C} - S$
- Lift graph to $(\tilde{V}, \tilde{E})$ on $\tilde{C} - x^{-1}(S)$.

# Lifting homotopy

Consider finite cover $\tilde{C} \to \mathbb{C};\ (x,y) \mapsto x$ of degree $n = \deg_y(f)$. Unramified outside

$$S = \{x \in \mathbb{C} : \mathrm{disc}_y f(x,y) = 0\}$$

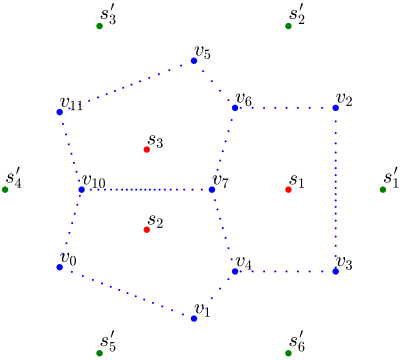
- Determine a connected plane graph $(V,E)$ in $\mathbb{C} - S$ for which a cycle basis generates the fundamental group of $\mathbb{C} - S$
- Lift graph to $(\tilde{V},\tilde{E})$ on $\tilde{C} - x^{-1}(S)$.
- A cycle basis of $(\tilde{V},\tilde{E})$ generates the fundamental group of $\tilde{C} - x^{-1}(S)$ and hence of $C$.

# Using Voronoi decomposition

**Example:** $\tilde{C}: y^2 = x^3 - x - 1$

$$S = \{s_1, s_2, s_3\}$$

Take (bounded) Voronoi cells:



# Lifting edges

## Lifting vertices and edges

- Lift $v$ to $C$ to $v^{(i)} = (x_v, y_v^{(i)})$ by solving $f(x_v, y_v^{(i)}) = 0$.
- Given edge $e = (v, w)$, parametrize $x(t) = (1-t)x_v + tx_w$.
- Let $y^{(i)}(t)$ be the continuous function determined by $y^{(i)}(0) = y_v^{(i)}$ and $f(x(t), y^{(i)}(t)) = 0$
- Then $e^{(i)} = \{(x(t), y^{(i)}(t) : t \in [0,1]\}$ is a lift of $e$ to $\tilde{C}$.

# Lifting edges

**Lifting vertices and edges**

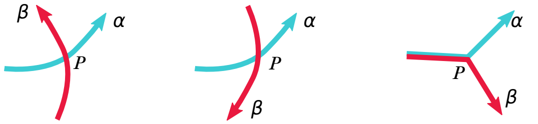
- Lift $v$ to $C$ to $v^{(i)} = (x_v, y_v^{(i)})$ by solving $f(x_v, y_v^{(i)}) = 0$.
- Given edge $e = (v, w)$, parametrize $x(t) = (1-t)x_v + tx_w$.
- Let $y^{(i)}(t)$ be the continuous function determined by $y^{(i)}(0) = y_v^{(i)}$ and $f(x(t), y^{(i)}(t)) = 0$
- Then $e^{(i)} = \{(x(t), y^{(i)}(t) : t \in [0,1]\}$ is a lift of $e$ to $\tilde{C}$.

**Certified continuation:**

- For $t_0$, set $\varepsilon = \frac{1}{3} \min_{i \neq j} |y^{(i)}(t_0) - y^{(j)}(t_0)|$
- (Kranich 2015): Compute explicit $\delta > 0$ such that for $t_0 \leq t_1 < t_0 + \delta$ we have $|y^{(i)}(t_1) - y^{(i)}(t_0)| < \varepsilon$
- Store sequence of points along $e^{(i)}$ from which $(x(t), y(t))$ can be reliably interpolated.

# Intersection pairing

- Cycle basis $\gamma_1, \ldots, \gamma_r$ for $(\tilde{V}, \tilde{E})$ gives us generators for $\mathrm{H}_1(C(\mathbb{C}), \mathbb{Z})$.
- Orientation gives us a signed intersection pairing:




$$\langle \alpha, \beta \rangle_P = 1 \qquad \langle \alpha, \beta \rangle_P = -1 \qquad \langle \alpha, \beta \rangle_P = -\tfrac{1}{2}$$

- There is a basis $\alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g$ such that the Gram matrix for the pairing is

$$\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$$

- An algorithm of Frobenius allows us to find such a basis.

# Computing period matrices

- Cycles $\alpha_i, \beta_i$ represented as $\mathbb{Z}$-linear combinations of edges $e_{vw}^{(k)}$:

$$\int_{e_{vw}^{(k)}} \omega_i = |w - v| \int_{t=0}^{1} \frac{h_i(x(t), y(t))}{\partial_y f(x(t), y(t))} dt$$

- Integral is well-suited for computation using a high-order method, such as Gauss-Legendre.
- Presently heuristic adaptive integration method
- *Future*: Johansen's ARB/ACB library now provides numerical integration with guaranteed error bounds and has a good interface in Sage.

# Application: Homomorphisms

Suppose $C_1, C_2$ are curves with Jacobians $J_1, J_2$, with bases for differentials and homology

- Consider a homomorphism $\phi\colon J_1 \to J_2$.
- $T = T_\phi\colon\ \mathrm{H}^0(C_1, \Omega^1_{C_1})^* \to \mathrm{H}^0(C_2, \Omega^1_{C_2})^*$ $\qquad T_\phi \in M_{g_2,g_1}(\mathbb{C})$
- $R = R_\phi\colon\ \mathrm{H}_1(C_1, \mathbb{Z}) \to \mathrm{H}_1(C_2, \mathbb{Z})$ $\qquad R_\phi \in M_{2g_2,2g_1}(\mathbb{Z})$

# Application: Homomorphisms

Suppose $C_1, C_2$ are curves with Jacobians $J_1, J_2$, with bases for differentials and homology

- Consider a homomorphism $\phi : J_1 \to J_2$.
- $T = T_\phi : \mathrm{H}^0(C_1, \Omega^1_{C_1})^* \to \mathrm{H}^0(C_2, \Omega^1_{C_2})^*$ $\quad T_\phi \in M_{g_2, g_1}(\mathbb{C})$
- $R = R_\phi : \mathrm{H}_1(C_1, \mathbb{Z}) \to \mathrm{H}_1(C_2, \mathbb{Z})$ $\quad R_\phi \in M_{2g_2, 2g_1}(\mathbb{Z})$

**Lemma:** *If* $\Omega_i = (I_{g_i} | \tau_i)$ *then*

$$R = \begin{pmatrix} D & B \\ C & A \end{pmatrix}, \text{ where } D, B, C, A \in M_{g_2, g_1}(\mathbb{Z}).$$

*and* $T = D + \tau_2 C$, *with* $B + \tau_2 A = (D + \tau_2 C)\tau_1$.

**Result:** $2g_1g_2$ equations with real coefficients in $4g_1g_2$ integer variables, so LLL can find small integer solutions.

# Application: Idempotents and automorphisms

Suppose we have a $\mathbb{Z}$-basis $B_1, \ldots, B_r$ for $\mathrm{End}(J) = \mathrm{Hom}(J, J)$.

- We can determine idempotents in $\mathrm{End}(J)$, which give isogeny factors.
- We can determine units.
- If symplectic structure is taken into account, we get a *finite* group of symplectic automorphisms. The Torelli theorem relates this to $\mathrm{Aut}(C)$.

Via action on tangent space, we get action of automorphisms on canonical model of $C$. We can verify automorphisms algebraically this way.

Similarly, numerically found endomorphisms can be certified: [Costa-Mascot-Sijsling-Voight, 2016]

# Example: genus 3 curves

(from Sutherland):

$$C_1 : \ -x^2y^2 - xy^3 + x^3 + 2x^2y + 2xy^2 - x^2 - y = 0$$
$$C_2 : y^2 + (x^4 + x^3 + x^2 + 1)y = x^7 - 8x^5 - 4x^4 + 18x^3 - 3x^2 - 16x + 8$$

We find a homomorphism (on homology):

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}$$

# Example: non-galois cover

Consider

$$C\colon 4x^6 - 54x^5y - 729x^4 + 108x^3y^3 + 39366x^2 - 54xy^5 - 531441 = 0.$$

From idempotent computations we see for

$$D_2\colon y^2 = -16x^5 - 40x^4 + 32x^3 + 88x^2 - 32x - 23.$$

there is a degree $3$ map $C \to D_2$, but $\mathrm{Aut}(C) = \mathbb{Z}/2$.

**Construction:** From action of idempotent on tangent space, we can construct a projection from canonical model of $C$ to construct $D_2$.

# Example: Prym varieties

Construction of W.P. Milne (1923) associates to a genus $4$ curve (e.g.):

$$C: x^2+xy+y^2+3xz+z^2-yw+w^2 = xyz+xyw+xzw+yzw = 0$$

a plane quartic:

$$\begin{aligned} F:\ 5s^4 + 28s^3t + 28s^3 + 47s^2t^2 + 76s^2t + 44s^2 + 34st^3 + 82st^2 \\ +66st + 18s + 16t^4 + 34t^3 + 32t^2 + 18t + 1 = 0. \end{aligned}$$

# Example: Prym varieties

Construction of W.P. Milne (1923) associates to a genus 4 curve (e.g.):

$$C\colon x^2+xy+y^2+3xz+z^2-yw+w^2 = xyz+xyw+xzw+yzw = 0$$

a plane quartic:

$$F\colon 5s^4+28s^3t+28s^3+47s^2t^2+76s^2t+44s^2+34st^3+82st^2 \\ +66st+18s+16t^4+34t^3+32t^2+18t+1=0.$$

Unramified double cover of $C$:

$$\tilde{D}\colon u^4v^4-3u^4v^2+u^4-u^3v^3-2u^3v+u^2v^2-u^2+3uv^3 \\ +2uv+v^4+v^2+1=0.$$

Numerical computation: $\mathrm{Jac}(\tilde{D}) \simeq \mathrm{Jac}(F)\times\mathrm{Jac}(C)$. (consisten with $\mathrm{Jac}(F)$ being the Prym variety of $\tilde{D}\to C$.

# Example usage

```
sage:  E=EllipticCurve([0,1])
sage:  S=E.riemann_surface(prec=100)
sage:  A=S.symplectic_isomorphisms()
sage:  A=S.symplectic_isomorphisms(); A
[
[ 0 -1]  [ 1 1]  [1 0]  [ 0 1]  [-1 -1]  [-1 0]
[ 1 1], [-1 0], [0 1], [-1 -1], [ 1 0], [ 0 -1]
]
sage:  TA=S.tangent_representation_algebraic(A); TA
[[a], [-a + 1], [1], [-a], [a - 1], [-1]]
sage:  parent(TA[0])
Full MatrixSpace of 1 by 1 dense matrices over Number
Field in a with defining polynomial y^2 - y + 1
```