

JOURNAL

de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux


Matthew RADOSEVICH et John VOIGHT

Computing Euclidean Belyi maps

Tome 35, n° 2 (2023), p. 543-565.

<https://doi.org/10.5802/jtnb.1256>

© Les auteurs, 2023.

 Cet article est mis à disposition selon les termes de la licence
CREATIVE COMMONS ATTRIBUTION – PAS DE MODIFICATION 4.0 FRANCE.
<http://creativecommons.org/licenses/by-nd/4.0/fr/>



*Le Journal de Théorie des Nombres de Bordeaux est membre du
Centre Mersenne pour l'édition scientifique ouverte*

<http://www.centre-mersenne.org/>

e-ISSN : 2118-8572

Computing Euclidean Belyi maps

par MATTHEW RADOSEVICH et JOHN VOIGHT

RÉSUMÉ. Nous exposons un algorithme explicite pour calculer les revêtements ramifiés en trois points de la droite projective complexe lorsque le groupe de triangles uniformisant est euclidien.

ABSTRACT. We exhibit an explicit algorithm to compute three-point branched covers of the complex projective line when the uniformizing triangle group is Euclidean.

1. Introduction

1.1. Motivation. Grothendieck in his *Esquisse d'un Programme* [5] described an action of the absolute Galois group $\text{Gal}(\mathbb{Q}^{\text{al}} | \mathbb{Q})$ of the rational numbers on the sets of Belyi maps and dessins d'enfants, linking combinatorics, topology, geometry, and arithmetic in a deep and surprising way. Computational aspects of this program remain of significant interest: for a survey, see Sijssling–Voight [12]. A common thread underlying these approaches is to realize a Belyi map via uniformization as $\varphi: \Gamma \backslash \mathcal{H} \rightarrow \Delta \backslash \mathcal{H}$ where \mathcal{H} is one of the three classical geometries (the sphere, the Euclidean plane, or the hyperbolic plane), and $\Gamma \leq \Delta$ is a finite-index subgroup of a triangle group. The case where \mathcal{H} is spherical is truly classical, corresponding to certain triangulations of the Platonic solids. In the hyperbolic case, complex analytic methods can be employed to convert this geometric description into an algebraic one [1, 6, 9, 10]. What remains is the case of Euclidean triangle groups, those arising from the familiar regular triangular tessellations of the Euclidean plane. In this paper, we fill this gap: we compute Euclidean Belyi maps explicitly from maps of complex tori, forming a bridge between the classical and the general.

1.2. Main result. A Belyi map over \mathbb{C} is a morphism $\varphi: X \rightarrow \mathbb{P}_{\mathbb{C}}^1$ of nice (projective, nonsingular, integral) curves over \mathbb{C} that is unramified away from $\{0, 1, \infty\}$. By the Riemann existence theorem, we may equivalently work with such a map of compact Riemann surfaces. Famously, Belyi [2, 3] proved that a curve X over \mathbb{C} can be defined over the algebraic numbers \mathbb{Q}^{al} if and only if X admits a Belyi map.

Manuscrit reçu le 26 avril 2022, révisé le 1^{er} février 2023, accepté le 26 janvier 2023.

2020 *Mathematics Subject Classification.* 11G32, 11Y40.

Mots-clefs. Belyi maps, elliptic curves.

Voight was supported by a Simons Collaboration grant (550029).

Belyi maps admit a tidy combinatorial description, something we take as the input to our algorithm. A **permutation triple** of degree d is a triple $(\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$ of permutations on d elements such that $\sigma_\infty \sigma_1 \sigma_0 = 1$. A permutation triple is **transitive** if it generates a transitive subgroup of S_d . The monodromy around $0, 1, \infty$ of a Belyi map of degree d gives a permutation triple of degree d , giving a bijection between isomorphism classes of Belyi maps of degree d and transitive permutation triples up to simultaneous conjugation. Lifting paths, one can compute (by numerical approximation) the permutation triple attached to a Belyi map; in this paper, we consider the harder, converse computational task.

Let σ be a transitive permutation triple of degree d and let a, b, c be the orders of $\sigma_0, \sigma_1, \sigma_\infty$, respectively. By the theory of covering spaces, the permutation triple σ defines a homomorphism $\pi: \Delta(a, b, c) \rightarrow S_d$ and thereby a subgroup $\Gamma \leq \Delta(a, b, c)$ of index d (see Section 2). The quotient $\Gamma \backslash \mathcal{H}$ can be given the natural structure of a Riemann surface $X(\Gamma)$, and the further quotient to $\Delta \backslash \mathcal{H}$ defines a Belyi map $\varphi: X(\Gamma) \rightarrow X(\Delta) \simeq \mathbb{P}_{\mathbb{C}}^1$. By the theorem of Belyi, the map φ can be defined over the field of algebraic numbers \mathbb{Q}^{al} .

We say that σ (and its corresponding map φ) is **Euclidean** if $1/a + 1/b + 1/c = 1$, in which case the attached triangle group $\Delta(a, b, c)$ is a group of symmetries of the Euclidean plane, whence (a, b, c) is equal to $(3, 3, 3)$, $(2, 3, 6)$, or $(2, 4, 4)$. Our main result provides an algorithmic way to compute algebraic equations for φ given σ .

Theorem 1.2.1. *There exists an explicit algorithm that, given as input a transitive, Euclidean permutation triple σ , produces as output a model for the Belyi map φ associated to σ over \mathbb{Q}^{al} .*

The algorithm in Theorem 1.2.1 is specified in Algorithm 3.5.1. We implemented the algorithm in the computer algebra system **Magma** [4]: the running time is quite favorable. We computed a database of Euclidean Belyi maps with this implementation (see Section 4) which we will upload to the LMFDB [7]. Our code is available as part of a Belyi maps package available online (<https://github.com/michaelmusty/Belyi>).

Remark 1.2.2. It would be interesting to estimate the running time of our algorithm by estimating the heights of intermediate computations and the precision required in Step 4 of Algorithm 3.2.5.

1.3. Proof sketch. We now briefly indicate the idea behind the proof of Theorem 1.2.1. We first convert the permutation triple σ into an explicit description of the group $\Gamma \leq \Delta$. Next, we write $\Gamma \simeq T(\Gamma) \rtimes R(\Gamma)$ as a semi-direct product, where $T(\Gamma)$ consists of the subgroup of translations in Γ and $R(\Gamma)$ is generated by rotation around a particular point, which we can find explicitly. The quotients $E(\Gamma) := T(\Gamma) \backslash \mathbb{C}$ and $E(\Delta) := T(\Delta) \backslash \mathbb{C}$

define elliptic curves. We then have the following commutative diagram, which we call the *master diagram*:

$$(1.3.1) \quad \begin{array}{ccc} E(\Gamma) & \xrightarrow{\beta} & X(\Gamma) \\ \psi \downarrow & & \downarrow \varphi \\ E(\Delta) & \xrightarrow{\alpha} & X(\Delta) \simeq \mathbb{P}^1 \end{array}$$

To find the Belyi map φ , our strategy is to compute the other three maps in our diagram, filling in φ by commutativity (“descending ψ along α ”). The bottom map α depends only on a, b, c and the choice of origin, giving six possibilities. The map ψ is an isogeny of elliptic curves, which we compute from the inclusion of lattices implied by $T(\Gamma) \leq T(\Delta)$ by applying formulas of Vélu. The top map β is computed by looking at the fixed field of $\mathbb{C}(E(\Gamma))$ under the finite subgroup of automorphisms corresponding to the rotations $R(\Gamma)$ (taking care to ensure these rotations act by automorphisms at the origin). The final step, to fill in φ to make the diagram commute, is obtained via explicit substitution.

1.4. Contents. After reviewing background in Section 2, we exhibit in Section 3 the main algorithm (Algorithm 3.5.1) in pseudocode and then prove the main result (Theorem 1.2.1). In Section 4 we describe an implementation in the **Magma** computer algebra system and then present some computed examples.

Acknowledgements. The authors would like to thank Sam Schiavone and Jeroen Sijsling for discussions and the anonymous referee for feedback.

2. Group theory and geometry

In this section, we begin by developing some preliminary input coming from group theory and geometry.

2.1. Transitive permutation representations. First, a few basic facts and conventions. In this article, the symmetric group S_d acts on the right on $\{1, \dots, d\}$, written in exponentiated form: e.g., if $\tau = (123)$ and $\mu = (23)$ then $1^{\tau\mu} = (1^\tau)^\mu = 2^\mu = 3$.

Recall that if G is a group, a (finite) permutation representation of G is a group homomorphism $\pi: G \rightarrow S_d$ for some $d \geq 1$, and we say that π is transitive if its image is a transitive subgroup of S_d . A transitive permutation triple σ defines a transitive permutation representation by $\pi(\delta_s) = \sigma_s$ for $s = a, b, c$, and conversely.

Let $\pi: \Delta \rightarrow S_d$ be a transitive permutation representation. Let

$$(2.1.1) \quad \Gamma := \{\delta \in \Delta : 1^{\pi(\delta)} = 1\}.$$

be the preimage of the stabilizer of 1 under π . (The stabilizer of $k \in \{1, \dots, d\}$ is conjugate to Γ in Δ .) Then $[\Delta : \Gamma] = d$. Conversely, given $\Gamma \leq \Delta$ of index d , the action of Δ on the cosets of Γ gives a transitive permutation representation $\pi: \Delta \rightarrow S_d$, and this correspondence is bijective.

2.2. Euclidean triangle groups. We refer to Magnus [8, §II.4] for classical background on Euclidean triangle groups; we briefly summarize some classical facts. Let T^* be a triangle in the Euclidean plane \mathbb{C} with angles π/a , π/b , and π/c at the vertices v_a , v_b , and v_c labeled clockwise, with $a, b, c \in \mathbb{Z}_{\geq 2}$. Then in fact there are only three possibilities, namely

$$(a, b, c) = (3, 3, 3), (2, 3, 6), (2, 4, 4)$$

corresponding to the solutions to $1/a + 1/b + 1/c = 1$; the corresponding tessellations of the Euclidean plane by triangles are sketched in Figure 2.2.1, with alternating triangles colored white and black.

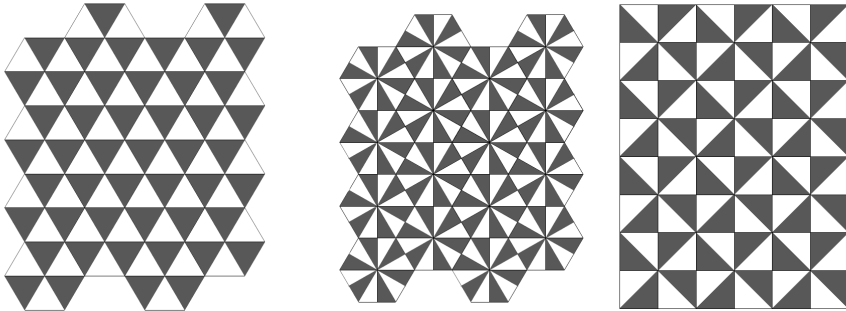


Figure 2.2.1: Tessellations for $\Delta(3, 3, 3)$, $\Delta(2, 3, 6)$, and $\Delta(2, 4, 4)$

The group generated by the reflections in the sides of T^* generates a discrete group of isometries acting properly on \mathbb{C} , with fundamental domain T^* . The further subgroup of orientation-preserving isometries $\Delta(a, b, c)$ has index 2, described as follows. For $s \in \{a, b, c\}$, let δ_s be the counterclockwise rotation about v_s by an angle of $2\pi/s$.

Proposition 2.2.2. *The following statements hold.*

(a) *There is a presentation*

$$\Delta = \Delta(a, b, c) \simeq \langle \delta_a, \delta_b, \delta_c \mid \delta_a^a = \delta_b^b = \delta_c^c = \delta_c \delta_b \delta_a = 1 \rangle.$$

(b) *There is a unique group homomorphism*

$$(2.2.3) \quad \rho: \Delta \rightarrow \frac{1}{c}\mathbb{Z}/\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/c\mathbb{Z}$$

such that

$$\delta_a, \delta_b, \delta_c \mapsto 1/a, 1/b, 1/c \mapsto c/a, c/b, 1.$$

(c) We have $\ker \rho = T(\Delta)$ where $T(\Delta) \trianglelefteq \Delta$ is the subgroup of translations, giving a split exact sequence

$$(2.2.4) \quad 1 \rightarrow T(\Delta) \rightarrow \Delta \xrightarrow{\rho} \mathbb{Z}/c\mathbb{Z} \rightarrow 1;$$

in particular,

$$\Delta = T(\Delta)\langle \delta_c \rangle \simeq \mathbb{Z}^2 \rtimes \mathbb{Z}/c\mathbb{Z}.$$

Proof. See Magnus [8, Thm. 2.5] for a proof of part (a) using the Reidemeister–Schreier method.

For part (b), we check that the relations in Δ are satisfied: indeed, we have $\rho(\delta_s^s) = s(c/s) \equiv 0 \pmod{c}$, and $\rho(\delta_c\delta_b\delta_a) = c(1/a + 1/b + 1/c) \equiv 0 \pmod{c}$. Alternatively, we define a group homomorphism first by taking the quotient by the commutator subgroup to surject onto $(\mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z} \oplus \mathbb{Z}/c\mathbb{Z})/\langle(1, 1, 1)\rangle$, then map to $\mathbb{Z}/c\mathbb{Z}$ via $(x, y, z) \mapsto x(c/a) + y(c/b) + z$.

Since it will be of some importance to us, we prove part (c) two ways. First, we compute algebraically. We treat the case $\Delta = \Delta(2, 3, 6)$, the other two being similar. Without loss of generality, we may suppose that $v_c = 0$ and $v_b = 1$. Then $v_a = (\zeta_6 + 1)/2$, where $\zeta_6 = \exp(2\pi i/6)$. The translations in Δ are precisely those that translate by the Δ orbit of $v_c = 0$, so $T(\Delta)$ is generated by $z \mapsto z + (\zeta_6 + 1) = z + 2v_a$ and $z \mapsto z + \sqrt{3}i = z + (2\zeta_6 - 1)$. We then compute directly that

$$\delta_a(z) = -z + (\zeta_6 + 1)$$

is the composition of the rotation $z \mapsto -z = \zeta_6^3 z$ in $\langle \delta_c \rangle$ followed by the translation $z \mapsto z + (\zeta_6 + 1)$ in $T(\Delta)$. Since $\delta_b = \delta_c^{-1}\delta_a^{-1}$, we conclude that $\Delta = T(\Delta)\langle \delta_c \rangle$. In particular, every transformation $\delta \in \Delta$ is of the form $\delta(z) = \zeta_6^i z + \beta$ for $i \in \mathbb{Z}/c\mathbb{Z}$ and with $z \mapsto z + \beta$ in $T(\Delta)$; and written this way, $\rho(\delta) = i \pmod{c}$, so indeed $\ker \rho = T(\Delta)$. (We may also verify independently that $T(\Delta)$ is normal in Δ : if $\tau(z) = z + \beta \in T(\Delta)$ then

$$(2.2.5) \quad (\delta_c^{-1}\tau\delta_c)(z) = z + \zeta_6^{-1}\beta = z + \delta_c^{-1}(\beta)$$

is again translation by a point in the Δ orbit of v_c , so $\delta_c^{-1}\tau\delta_c \in T(\Delta)$.) Finally, since $T(\Delta) \simeq \mathbb{Z}^2$ is generated freely by two translations, it follows that $\Delta \simeq \mathbb{Z}^2 \rtimes \mathbb{Z}/c\mathbb{Z}$ as claimed.

We may also argue geometrically, as follows. Intuitively, each transformation δ_s rotates the plane by the corresponding interior angle $2\pi/s = (c/s)(2\pi/c)$, composition accumulates this rotation in an abelian way, and the resulting transformation is a translation if and only if the total amount of rotation sums to a multiple of 2π . In other words, every element of Δ is

obtained by first rotation by a power of δ_c to put E into one of c positions, then translation of E : see Figure 2.2.6.

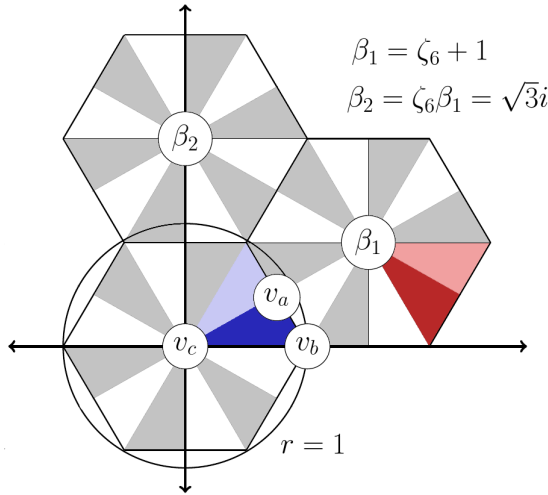


Figure 2.2.6: Geometric proof of Proposition 2.2.2(b)–(c)

More precisely, around v_c there is a central hexagon or square E consisting of c pairs of white and black triangles. Let $\delta \in \Delta$. Then $\delta(E)$ is another hexagon or square in the tessellation, with center $\delta(v_c)$. It is geometrically evident (and can be verified in a straightforward manner) that there is a unique translation $\tau_\delta \in T(\Delta)$ mapping $\delta(v_c)$ to v_c , so the composition fixes v_c and maps E to itself. But again visibly, the stabilizer of E in Δ is precisely $\langle \delta_c \rangle$. This association thereby defines a surjective group homomorphism $\Delta \rightarrow \langle \delta_c \rangle$ with kernel $T(\Delta)$, as claimed. Figure 2.2.6 gives the transformation taking T^* (blue) to T' (red) by first rotating about v_c by $5\pi/3$ (applying δ_c^5) then translating by $z \mapsto z + \beta_1$, an element of $T(\Delta)$. \square

Corollary 2.2.7. *The group $T(\Delta)$ is generated by*

$$(2.2.8) \quad (\omega_1, \omega_2) := \begin{cases} (\delta_a \delta_c^2, \delta_b \delta_c^2), & \text{if } (a, b, c) = (3, 3, 3); \\ (\delta_a \delta_c^3, \delta_b \delta_c^4), & \text{if } (a, b, c) = (2, 3, 6); \\ (\delta_a \delta_c^2, \delta_b \delta_c^3), & \text{if } (a, b, c) = (2, 4, 4). \end{cases}$$

Proof. In each case, ω_1 and ω_2 are in the kernel of the homomorphism ρ described in Proposition 2.2.2, and thus $\omega_1, \omega_2 \in T(\Delta)$. From Figure 2.2.1, it is straightforward to verify that the $\langle \omega_1, \omega_2 \rangle$ orbit of v_c is the same as the $T(\Delta)$ orbit of v_c , so $T(\Delta) = \langle \omega_1, \omega_2 \rangle$. \square

Visibly from Figure 2.2.1 we have $\Delta(3, 3, 3) \trianglelefteq \Delta(2, 3, 6)$ with index 2 (halving a fundamental triangle), and $T(\Delta(3, 3, 3)) = T(\Delta(2, 3, 6))$. Attached to each translation subgroup is the orbit of 0

$$(2.2.9) \quad \Lambda_\Delta := T(\Delta) \cdot 0$$

which defines a lattice $\Lambda_\Delta \simeq \mathbb{Z}^2$. We write

$$(2.2.10) \quad \begin{aligned} \Lambda_\square &:= \Lambda_{\Delta(2,4,4)} = \mathbb{Z}[i] \\ \Lambda_\circ &:= \Lambda_{\Delta(3,3,3)} = \Lambda_{\Delta(2,3,6)} = \mathbb{Z}[\zeta_6] \end{aligned}$$

Remark 2.2.11. More precisely, we work with these lattices up to homothety, rescaling by an element of \mathbb{C}^\times ; to obtain elliptic curves defined over \mathbb{Q} (see Section 3.1), we must rescale by a real number (which can be given explicitly as a real period).

2.3. Fundamental domains. In this section, we describe fundamental domains for the groups under consideration. A fundamental domain for the action of Δ is obtained from any pair of one shaded triangle and one unshaded triangle which we may take to share an edge. This gives a region where all the interior points are distinct under the identification $\Delta \circlearrowleft \mathbb{C}$. Furthermore, we can divide the four sides of the quadrilateral into two pairs of consecutive sides identified under the quotient by Δ as in Figure 2.3.1, so that $X(\Delta)$ has genus 0.

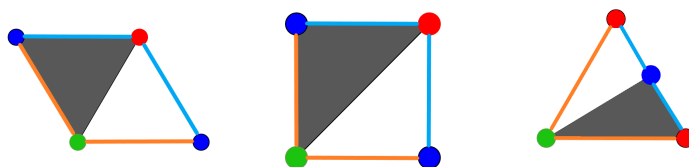


Figure 2.3.1: Fundamental domains for Δ , like colors identified

Since $T(\Delta)$ is generated by two noncollinear translations, we can take as its fundamental domain the parallelogram determined from two sides sharing a vertex at the origin. Opposite edges are identified while consecutive edges are distinct as in Figure 2.3.2, so the fundamental region is equivalent to a torus (genus 1). Similar statements hold for $T(\Gamma)$.

Finally, a fundamental domain for Γ is constructed in the usual manner: we choose coset representatives $\Delta = \bigsqcup_{i=1}^d \gamma_i \Gamma$, and then for $D(\Delta)$ the fundamental domain for Δ we have the fundamental domain $D(\Gamma) = \bigcup_{i=1}^d \gamma_i D(\Delta)$.

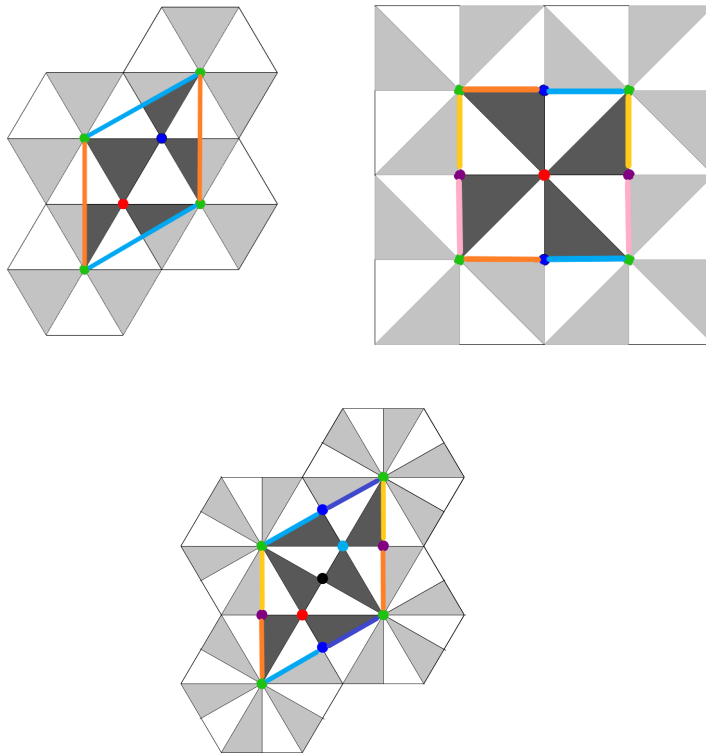


Figure 2.3.2: Fundamental domains for $T(\Delta)$, like colors identified

We now consider the genus of the surface $X(\Gamma) := \Gamma \backslash \mathbb{C}$. Given a permutation $\tau \in S_d$, let $k(\tau)$ be the number of disjoint cycles in τ and define its excess as $e(\tau) := d - k(\tau)$. Then by the Riemann–Hurwitz formula, the genus of $X(\Gamma)$ is equal to [12, (1.5)]

$$(2.3.3) \quad g(X(\Gamma)) = 1 - d + \frac{e(\sigma_0) + e(\sigma_1) + e(\sigma_\infty)}{2}.$$

Lemma 2.3.4. *We have $g(X(\Gamma)) \leq 1$, with equality if and only if for all $s \in \{a, b, c\}$, every cycle in σ_s has length s .*

Proof. For $s \in \{a, b, c\}$ since the cycle decomposition of σ_s can contain no cycle of length greater than s , we have $k(\sigma_s) \geq d/s$, so

$$e(\sigma_a) + e(\sigma_b) + e(\sigma_c) \leq 3d - \left(\frac{d}{a} + \frac{d}{b} + \frac{d}{c} \right) = 3d - d = 2d$$

with equality if and only if all cycles in σ_s are length s . Substituting this into (2.3.3), the result follows. \square

Remark 2.3.5. We will see later, in Corollary 2.5.7, that $g(X(\Gamma)) = 1$ if and only if $\Gamma = T(\Gamma)$.

2.4. Translation subgroups. Let

$$(2.4.1) \quad T(\Gamma) := \Gamma \cap T(\Delta) = \ker \rho|_{\Gamma}$$

be the subgroup of translations in Γ ; then $T(\Gamma) \trianglelefteq \Gamma$, as $T(\Delta) \trianglelefteq \Delta$ by Proposition 2.2.2. Writing $E(\Gamma) := T(\Gamma) \backslash \mathbb{C}$ and similarly for Δ , the containments of these four groups give quotient maps which fit into the diagram (1.3.1).

We again have a lattice

$$(2.4.2) \quad \Lambda_{\Gamma} := T(\Gamma) \cdot 0$$

with $\Lambda_{\Gamma} \leq \Lambda_{\Delta}$ a subgroup of finite index. When no confusion can arise, we will identify translation maps by the corresponding lattice element. We define

$$(2.4.3) \quad N := [T(\Delta) : T(\Gamma)].$$

In the following algorithm, we compute a convenient basis for $T(\Gamma)$.

Algorithm 2.4.4. This algorithm takes as input σ and outputs a basis η_1, η_2 for $T(\Gamma)$ and $N = [T(\Delta) : T(\Gamma)]$.

1. Let π be the transitive permutation representation attached to σ , and for $i = 1, 2$, let ω_i be as in Corollary 2.2.7 (a basis for $T(\Delta)$).
2. Let τ_1 be the cycle containing 1 in $\pi(\omega_1)$ and let τ_2 be the cycle containing 1 in $\pi(\omega_2^{-1})$. For $i = 1, 2$, let ℓ_i be the length of τ_i .
3. Compute

$$V := \{(b_1, b_2) : 0 \leq b_i \leq \ell_i \text{ for } i = 1, 2 \text{ and } 1^{\tau_1^{b_1}} = 1^{\tau_2^{b_2}}\}.$$

4. Let A be the matrix whose rows are the elements of V . Reduce A to Hermite normal form (HNF) and take its first two row vectors (n_1, n_2) and $(0, m_2)$.
5. Return $\eta_1 = \omega_1^{n_1} \omega_2^{n_2}$ and $\eta_2 = \omega_2^{m_2}$ and $N = n_1 m_2$.

Proof of correctness. Since ω_1 and ω_2 commute, any $\eta \in T(\Delta)$ is of the form $\eta = \omega_1^{a_1} \omega_2^{a_2}$ for some $(a_1, a_2) \in \mathbb{Z}^2$. By definition, such $\eta \in T(\Gamma)$ if and only if $1^{(\pi_1(\omega_1)^{a_1} \pi_2(\omega_2)^{a_2})} = 1$, or equivalently when $1^{\tau_1^{a_1}} = 1^{\tau_2^{a_2}}$. Since τ_i has order ℓ_i , we only need to consider $0 \leq a_i \leq \ell_i$ for $i = 1, 2$. The \mathbb{Z} -span of V therefore gives all pairs (a_1, a_2) such that $\eta = \omega_1^{a_1} \omega_2^{a_2}$ is in $T(\Gamma)$. Since only row operations are performed in computing the Hermite normal form, the \mathbb{Z} -span does not change, hence η_1, η_2 computed in Step 5 generate $T(\Gamma)$. Finally, we have

$$N = [T(\Delta) : T(\Gamma)] = \det \begin{pmatrix} n_1 & n_2 \\ 0 & m_2 \end{pmatrix} = n_1 m_2. \quad \square$$

2.5. Rotation index. In this section, we study rotations in Γ . Restricting the exact sequence (2.2.4) we obtain

$$1 \rightarrow T(\Gamma) \rightarrow \Gamma \rightarrow R(\Gamma) \rightarrow 1$$

where $R(\Gamma) := \rho(\Gamma) \leq \mathbb{Z}/c\mathbb{Z}$. Evidently, $R(\Gamma)$ is a cyclic group with order dividing c .

Definition 2.5.1. The rotation index of Γ is $r(\Gamma) := [\Gamma : T(\Gamma)] = \#R(\Gamma)$.

Lemma 2.5.2. *We have*

$$r(\Gamma) = \frac{cN}{d}$$

where $N = [T(\Delta) : T(\Gamma)]$.

Proof. From

$$[\Delta : T(\Gamma)] = [\Delta : \Gamma][\Gamma : T(\Gamma)] = [\Delta : T(\Delta)][T(\Delta) : T(\Gamma)]$$

we conclude $dr(\Gamma) = cN$. □

In Proposition 2.2.2(c) we split the exact sequence using δ_c . Indeed, the analogous sequence for Γ above is again split, but not necessarily by a power of δ_c : instead, $R(\Gamma)$ is generated by a rotation about some vertex (an element in the Δ orbit of v_a, v_b , or v_c), as follows.

Lemma 2.5.3. *There exists a vertex v_O whose stabilizer $\gamma_O \in \Gamma$ has $\rho(\gamma_O)$ a generator of $R(\Gamma)$, giving a split exact sequence*

$$1 \rightarrow T(\Gamma) \rightarrow \Gamma \rightarrow \langle \gamma_O \rangle \rightarrow 1$$

so in particular $\Gamma = T(\Gamma)\langle \gamma_O \rangle \simeq \mathbb{Z}^2 \rtimes \mathbb{Z}/r(\Gamma)\mathbb{Z}$.

Proof. Every element of Δ is either a translation (and fixes no point) or fixes a unique point ($z \mapsto uz + v$ fixes $z = v/(1 - u)$ if $u \neq 1$), necessarily a vertex as every nonidentity element of finite order in Δ is conjugate to one of the generators $\delta_a, \delta_b, \delta_c$. So let $\gamma_O \in \Gamma$ be any element which maps to a generator of $R(\Gamma)$ under ρ , well-defined up to a translation in $T(\Gamma)$. If γ_O is a translation, which is to say $\gamma_O \in T(\Gamma)$, then $R(\Gamma)$ is trivial: hence $\Gamma = T(\Gamma)$, and we may take v_O to be any vertex (each having trivial stabilizer under Γ).

Otherwise, γ_O fixes a vertex v_O with the claimed properties; the splitting follows immediately, just as we saw in the geometric proof of Proposition 2.2.2(c). □

Definition 2.5.4. A vertex v_O whose stabilizer generates $R(\Gamma)$ is called a vertex of maximum rotation.

With Lemma 2.5.3, we can be more precise about the possible vertices of maximal rotation.

Corollary 2.5.5. *The vertices of maximal rotation, up to translation by $T(\Gamma)$, are in bijection with the union of the sets of cycles τ in σ_s with length $s/r(\Gamma)$ for $s \in \{a, b, c\}$.*

Proof. Under the quotient map $\Gamma \backslash \mathbb{C} \rightarrow \Delta \backslash \mathbb{C}$, for $s \in \{a, b, c\}$, the preimages of the vertex v_s are in bijection with the cycles in σ_s and the stabilizer of a vertex with cycle τ has order $s/\ell(\tau)$ where $\ell(\tau)$ is the length of τ . Such a vertex has maximal rotation if and only if $s/\ell(\tau) = r(\Gamma)$. \square

Because a permutation triple which is simultaneously conjugate to σ gives an isomorphic Belyi map (with differently labelled sheets), we may suppose without loss of generality that one of v_a, v_b, v_c is a vertex of maximal rotation: after simultaneous conjugation, we just insist that 1 belongs to a cycle as in Corollary 2.5.5. This “preprocessing” step is given as follows.

Algorithm 2.5.6. This algorithm takes as input a Euclidean permutation triple σ and gives as output the rotation index $r(\Gamma)$ and a simultaneously conjugate triple σ' and $s \in \{a, b, c\}$ such that one of v_a, v_b, v_c is a vertex of maximal rotation

1. Compute N using Algorithm 2.4.4 and $r(\Gamma) = cN/d$.
2. By trying all possibilities, find a cycle τ in σ_s with $s \in \{a, b, c\}$ with length $\ell(\tau) = s/r(\Gamma)$.
3. For any $i \in \tau$, return $r(\Gamma)$ and the simultaneous conjugation of σ by $(1\ i)$.

Proof. In Step 1, the rotation index is computed correctly by Lemma 2.5.2. Step 2 will succeed by 2.5.5. By choice of Γ as the stabilizer of 1, we conclude that v_s is a vertex of maximal rotation. \square

From here forward, we may suppose without loss of generality that this “preprocessing” step has been applied.

We now see the exact circumstances when $g(X(\Gamma)) = 1$.

Corollary 2.5.7. *We have $g(X(\Gamma)) = 1$ if and only if $r(\Gamma) = 1$ if and only if $\Gamma = T(\Gamma)$.*

Proof. By Corollary 2.5.5, we have $r(\Gamma) = 1$ if and only if for all $s \in \{a, b, c\}$, every cycle in σ_s has length s ; the result then follows from Lemma 2.3.4. \square

3. Equations

From the subgroup $\Gamma \leq \Delta$ of index d , in the previous section we defined the translation subgroups $T(\Gamma) \leq T(\Delta)$ whose quotients fit into the commutative diagram (1.3.1). We now calculate equations for these curves and the maps between them. As a basic reference, we refer to Silverman [13, 14].

3.1. Fixed maps. We begin with the bottom map $\alpha: E(\Delta) \rightarrow X(\Delta) \simeq \mathbb{P}^1$, which depends only on Δ (with the choice of the origin at v_c). From Proposition 2.2.2(c), the map α is the quotient by a cyclic group of rotations of order c at a vertex v_c , which we may take as the origin of the elliptic curve $E(\Delta)$. Accordingly, these rotations act by automorphisms of the elliptic curve $E(\Delta)$, and so their equations are well-known [13, §II.2] (see also Lemma 3.3.2 below). Define the elliptic curves

$$(3.1.1) \quad E_{\circlearrowleft}: y^2 = x^3 + 1 \quad E_{\square}: y^2 = x^3 - x$$

over \mathbb{Q} , the automorphisms

$$(3.1.2) \quad \begin{array}{lll} \delta_3: E_{\circlearrowleft} \rightarrow E_{\circlearrowleft} & \delta_4: E_{\square} \rightarrow E_{\square} & \delta_6: E_{\circlearrowleft} \rightarrow E_{\circlearrowleft} \\ (x, y) \mapsto (\zeta_3 x, y) & (x, y) \mapsto (-x, iy) & (x, y) \mapsto (\zeta_3^{-1} x, -y). \end{array}$$

and the quotient maps

$$(3.1.3) \quad \begin{array}{lll} \alpha_3: E_{\circlearrowleft} \rightarrow \mathbb{P}^1 & \alpha_4: E_{\square} \rightarrow \mathbb{P}^1 & \alpha_6: E_{\circlearrowleft} \rightarrow \mathbb{P}^1 \\ (x, y) \mapsto \frac{y+1}{2} & (x, y) \mapsto x^2 & (x, y) \mapsto y^2. \end{array}$$

We recall the lattices defined in (2.2.10). After homothety, the Weierstrass map $z \mapsto (\wp(z), \wp'(z)/2)$ gives an analytic isomorphism from the complex elliptic curve $\mathbb{C}/\Lambda_{\square}$ to $E_{\square}(\mathbb{C})$. Moreover, the rotation δ_4 acts by $(x, y) \mapsto (-x, iy)$ (gently abusing notation), and the quotient map $E(\Delta) \rightarrow X(\Delta)$ is given by α_4 in these coordinates. Similar statements hold for the two \circlearrowleft cases.

Lemma 3.1.4. *The maps α_c for $c = 3, 4, 6$ are Euclidean Belyi maps of degree c .*

Proof. For α_4 , the set of preimages under $(x, y) \mapsto x^2 = t$ has cardinality four unless $t = 0, \infty$ or $y = 0$, in which case $t = x^2 = 0, 1$, giving ramification type $(2, 4, 4)$. Similarly for α_6 , we have six preimages under $(x, y) \mapsto y^2 = t$ unless $t = 0, \infty$ or $y^2 - 1 = x^3 = 0$, in which case $t = y^2 = 1$, giving ramification $(2, 3, 6)$.

For α_3 , the map $(x, y) \mapsto y$ is ramified above $\{\pm 1, \infty\}$ with ramification $(3, 3, 3)$, so to get ramification at $\{0, 1, \infty\}$ we simply postcompose with the Möbius transformation $y \mapsto (y + 1)/2$. □

3.2. Isogeny. We now turn to the isogeny $\psi: E(\Gamma) \rightarrow E(\Delta)$ in (1.3.1).

We first show how to work explicitly with torsion on $E(\Delta)$ using exact arithmetic. To handle the three cases uniformly, let $j = i$ or $j = \zeta_6$, so that $\Lambda = \Lambda_{\Delta} = \mathbb{Z}[j]$, let $K := \mathbb{Q}(j) \subseteq \mathbb{C}$, and let $E = E_{\square}$ or $E = E_{\circlearrowleft}$.

Lemma 3.2.1. *For all $a + bj \in \mathbb{Z}[j]$, there exists an effectively computable rational function $m_{a+bj}(x) \in K(x)$ such that $x([a + bj]P) = m_{a+bj}(x(P))$ for all $P \in E(\mathbb{Q}^{\text{al}})$.*

Proof. When $b = 0$, the lemma is established as part of the theory of division polynomials: see Silverman [14, Exercise 3.7 (d)]. When $b \neq 0$, we may similarly calculate using the explicit description of the action of j given in (3.1.2): we still know that $x([a + bj]P)$ is a rational function in $x(P)$, since $x([a + bj](-P)) = x(-[a + bj]P) = x([a + bj]P)$. \square

For an integer $N \geq 1$, the torsion group

$$E[N] \simeq \frac{1}{N}\Lambda/\Lambda \simeq \mathbb{Z}[j]/N\mathbb{Z}[j]$$

is a cyclic $\mathbb{Z}[j]$ -module; we use the symbol $P \in E[N]$ to denote a generator of $E[N]$ as a $\mathbb{Z}[j]$ -module.

Algorithm 3.2.2. This algorithm takes as input $N \in \mathbb{Z}_{\geq 1}$ and returns as output a number field L and the set

$$\{(a + bj, x([a + bj]P)) : a, b \in \mathbb{Z}/N\mathbb{Z}\} \subseteq \mathbb{Z}[j]/N\mathbb{Z}[j] \times L$$

for a generator P .

1. Compute the N -division polynomial $f_N(x) \in \mathbb{Q}[x]$ for E .
2. For each proper divisor $D \mid N$, compute the D -division polynomial $f_D(x) \in \mathbb{Q}[x]$ for $E(\Delta)$ and divide $f_N(x)$ by $\gcd(f_D(x), f_N(x))$ recursively.
3. Let $g_N(x)$ be an irreducible factor of $f_N(x)$ over $K[x]$ and let $L := K(\theta)$ with θ a root of $g_N(x)$.
4. Return the values

$$\{(a + bj, m_{a+bj}(\theta)) : a, b \in \mathbb{Z}/N\mathbb{Z}\}.$$

Remark 3.2.3. As an alternative to Step 4 (in place of computing the rational functions), at the cost of enlarging L to include the y -coordinate (if $E: y^2 = f(x)$, we just need $\sqrt{f(\theta)}$), we can just compute directly using the group law on E .

Proof of correctness. In Step 1, we form the polynomial whose roots are the x -coordinates of the N -torsion points, by definition of the division polynomial. In Step 2, we remove all roots whose order is a proper divisor of N ; so any remaining root will be the x -coordinate of a point with exact order N . Some such point P generates $E[N]$ as a $\mathbb{Z}[j]$ module. By Lemma 3.2.1, in Step 3 any irreducible factor of $f_N(x)$ is a splitting field for $f_N(x)$ over K , so if $g_N(\theta) = 0$ then $x(E[N]) \subseteq K(\theta)$. The output of Step 4 is correct by Lemma 3.2.1. \square

Next, we recall Section 2.4, where we defined $N := [T(\Delta) : T(\Gamma)]$ and computed in Algorithm 2.4.4 a basis for Λ_Γ . Since $N\Lambda_\Delta \subseteq \Lambda_\Gamma$, we have an isogeny

$$(3.2.4) \quad \begin{aligned} \widehat{\psi}: E(\Delta) &\rightarrow E(\Gamma) \\ z &\mapsto Nz \end{aligned}$$

dual to our desired isogeny ψ . From this setup, we compute an equation for ψ using Vélú’s formulas, as in the following algorithm.

Algorithm 3.2.5. This algorithm takes as input a basis

$$(3.2.6) \quad \begin{aligned} \eta_1 &= n_1\omega_1 + n_2\omega_2 \\ \eta_2 &= m_2\omega_2 \end{aligned}$$

for $\Lambda_\Gamma \leq \Lambda_\Delta = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ and gives as output a model for the isogeny $\psi: E(\Gamma) \rightarrow E(\Delta)$.

1. Let $p_1 := (0, \lceil n_1/2 \rceil)$. If m_2 is odd, let $p_2 := (\lfloor m_2/2 \rfloor, n_1)$. If m_2 is even, let $p_2 := (m_2/2, \lfloor n_1/2 \rfloor)$.
2. Let

$$C := \{(t_1, t_2) \in \mathbb{Z}/m_2\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z} : p_1 \leq (t_1, t_2) \leq p_2\}$$

where \leq here indicates the dictionary order.

3. Let

$$K := \left\{ \frac{1}{N}(t_1n_1, t_1n_2 + t_2m_2) : (t_1, t_2) \in C \right\}.$$

4. Compute

$$X := \{\wp_\Lambda(a_i\omega_1 + b_i\omega_2) : (a_i, b_i) \in K\} \subseteq \mathbb{C}$$

to enough precision to distinguish their values.

5. Call Algorithm 3.2.2 with output W_L . Embed $L \hookrightarrow \mathbb{C}$, and let $X_L \subseteq L$ be the set of x -coordinates in W_L whose embedding into \mathbb{C} matches a value in X .
6. Let

$$p(x) := \prod_{k \in X_L} (x - k) \in L[x].$$

Let K' be the subfield of L generated (over \mathbb{Q}) by the coefficients of $p(x)$.

7. Using Vélú’s formulas [15], compute the isogeny $\widehat{\psi}: E \rightarrow E'$ with kernel $p(x) \in K'[x]$ and E' defined over K' .
8. Return the dual isogeny $\psi: E' \rightarrow E$.

Proof of correctness. Algorithm 2.4.4 gives $\eta_1 = n_1\omega_1 + n_2\omega_2$ and $\eta_2 = m_2\omega_2$, so $\Lambda_\Gamma \subseteq \Lambda_\Delta$. Note also that $N\omega_1 = m_2\eta_1 - n_2\eta_2$ and $N\omega_2 = n_1\eta_2$, so $N\Lambda_\Delta \subseteq \Lambda_\Gamma$.

Let $f_N(x)$ be the N -division polynomial. We determine the x -coordinates of the points in $\ker \widehat{\psi}$ from among the roots of f_N . Since $z \in (1/N)\Lambda_\Gamma$ if and only if $Nz \in \Lambda_\Gamma$, it follows that $\ker(\widehat{\psi}) = (1/N)\Lambda_\Gamma/\Lambda_\Delta \simeq \Lambda_\Gamma/N\Lambda_\Delta$ and

$$\#\ker(\widehat{\psi}) = \#(\Lambda_\Gamma/N\Lambda_\Delta) = \det \begin{pmatrix} m_2 & -n_2 \\ 0 & n_1 \end{pmatrix} = n_1m_2 = N.$$

To list representatives for $\Lambda_\Gamma/N\Lambda_\Delta$, we proceed as follows: if we identify ordered pairs (a, b) with coordinates relative to the basis $\{\eta_1, \eta_2\}$ for Λ_Γ (i.e., (a, b) indicates the point $a\eta_1 + b\eta_2$), then (a_1, b_1) and (a_2, b_2) are equivalent modulo $N\Lambda_\Delta$ if and only if $a_1 - a_2 = im_2$ and $b_1 - b_2 = jn_1 - in_2$ for some $i, j \in \mathbb{Z}$. So the set

$$(3.2.7) \quad \{t_1\eta_1 + t_2\eta_2 : 0 \leq t_1 < m_2, 0 \leq t_2 < n_1\}$$

with N elements gives a complete set of coset representatives for $\Lambda_\Gamma/N\Lambda_\Delta$. It follows then that the set

$$(3.2.8) \quad \begin{aligned} A &:= \{\frac{1}{N}(t_1\eta_1 + t_2\eta_2) : 0 \leq t_1 < m_2, 0 \leq t_2 < n_1\} \\ &= \{\frac{1}{N}t_1(n_1\omega_1 + n_2\omega_2) + \frac{1}{N}t_2(m_2\omega_2) : 0 \leq t_1 < m_2, 0 \leq t_2 < n_1\} \\ &= \{\frac{1}{N}xn_1\omega_1 + \frac{1}{N}(t_1n_2 + t_2m_2)\omega_2 : 0 \leq t_1 < m_2, 0 \leq t_2 < n_1\} \end{aligned}$$

gives a complete set of coset representatives for $(1/N)\Lambda_\Gamma/\Lambda_\Delta$.

We use the Weierstrass \wp -function to map the points in the set $z \in A$ to points $P = (\wp(z), \wp'(z)/2) \in E(\mathbb{C})$ on the algebraic model E . On this model, since $x(-Q) = x(Q)$ for all Q we only need one representative in A up to inverses. Points in A corresponding to the pairs (t_1, t_2) and (t'_1, t'_2) give inverses on $E(\mathbb{C})$ if and only if $m_2 \mid (t_1 + t'_1)$ and $n_1 \mid (t_2 + t'_2)$. Forming the set C in Step 2 then avoids redundancies so that no points in the set K are inverse to each other.

The algebraic recognition in Steps 4 and 5 follow since the values are the distinct x -coordinates of N -torsion points. With an equation for E and the polynomial representing the kernel of the isogeny $\hat{\psi}: E \rightarrow E'$, we can use Vélú's formula to calculate $\hat{\psi}$ explicitly. Taking the dual to $\hat{\psi}$ gives the desired isogeny ψ . □

Remark 3.2.9. If n_1 and m_2 above are coprime, then $\ker(\hat{\psi}) \cong \mathbb{Z}/m_2\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z} \cong \mathbb{Z}/N\mathbb{Z}$ with $N = n_1m_2$ is cyclic. So, in algorithm 3.2.2, we need only compute the set of values $\{m_a(x(P)) : a \in \mathbb{Z}/N\mathbb{Z}\}$ for a generating point P of $\ker(\hat{\psi})$. Then, we may take those values as the roots of the kernel polynomial $p(x)$ in Step 6 of algorithm 3.2.5. As the computation of the rational maps $m_{a+bj}(x)$ can be costly, this is a useful simplification. If n_1 and m_2 are not coprime, let $k := \gcd(n_1, m_2)$. Then, we may factor $\psi = [k] \circ \psi'$ where $[k]: E(\Delta) \rightarrow E(\Delta)$ is the multiplication by k map and $\psi': E(\Gamma) \rightarrow E(\Delta)$ is the isogeny with cyclic kernel obtained as described above replacing n_1 with n_1/k and m_2 with m_2/k .

3.3. Descent using automorphisms. Returning to our master diagram (1.3.1), we now consider the top map $\beta: E(\Gamma) \rightarrow X(\Gamma)$ having computed in the previous section an equation for ψ and $E(\Gamma)$ over a number field K' . To do so, we apply a bit of Galois theory. Associated to our master diagram is

the following diagram of inclusions of function fields (see e.g. Silverman [14, §II.2]):

$$(3.3.1) \quad \begin{array}{ccc} \mathbb{C}(E(\Gamma)) & & \\ \psi^* \downarrow & \searrow^{\beta^*} & \mathbb{C}(X(\Gamma)) \\ \mathbb{C}(E(\Delta)) & & \downarrow^{\varphi^*} \\ & \searrow^{\alpha^*} & \mathbb{C}(X(\Delta)) \end{array}$$

We recall our explicit equations from Section 3.1 and the automorphisms (3.1.2). The inclusion α^* realizes $\mathbb{C}(X(\Delta))$ as the fixed field under $\langle \delta_c^* \rangle$. For example, for $c = 4$ we have

$$\mathbb{C}(E_{\square}) = \mathbb{C}(x, y)$$

with $y^2 = x^3 - x$, and so with $\delta_4(x, y) = (-x, iy)$ we have

$$\mathbb{C}(E_{\square})^{\langle \delta_4^* \rangle} = \mathbb{C}(x^2, y^4) = \mathbb{C}(x^2) \subseteq \mathbb{C}(E_{\square})$$

because $y^4 = x^6 - 2x^4 + x^2 \in \mathbb{C}(x^2)$.

By Lemma 2.5.3, there exists a vertex of maximal rotation (Definition 2.5.4) for Γ . At the end of Section 2, we argued that up to isomorphism (without loss of generality) we may suppose that this vertex is one of v_a, v_b, v_c . We have $\deg \beta = r(\Gamma) \in \{1, 2, 3, 4, 6\}$ equal to the rotation index.

If $r(\Gamma) = 1$, then $E(\Gamma) = X(\Gamma)$ and β is the identity. So we may suppose that $r(\Gamma) > 1$.

First suppose that $v_c = 0$ is a vertex of maximal rotation under a subgroup of rotations generated by a power of δ_c . Then the quotient map β is again by a subgroup of automorphisms of $E(\Gamma)$ over K' as an elliptic curve, so is given in the same well-known manner as in Section 3.1.

Lemma 3.3.2. *Suppose v_c is a vertex of maximal rotation with $r(\Gamma) > 1$. Then $X(\Gamma) \simeq \mathbb{P}^1$, and the following statements hold.*

- (a) *If $r(\Gamma) = 3, 6$, then $E(\Gamma)$ has an equation of the form $y^2 = x^3 + B$ for some nonzero $B \in K'$, and $\beta: E(\Gamma) \rightarrow X(\Gamma)$ can be taken to be $(x, y) \mapsto y, y^2$, respectively.*
- (b) *If $r(\Gamma) = 4$, then $E(\Gamma): y^2 = x^3 + Ax$ for some nonzero $A \in K'$, and $\beta(x, y) = x^2$.*
- (c) *If $r(\Gamma) = 2$, then $\beta(x, y) = x$.*

Proof. We may suppose that $E(\Gamma)$ has a Weierstrass equation $y^2 = x^3 + Ax + B$. Any automorphism of E is of the form $(x, y) \mapsto (u^{-2}x, u^{-3}y)$

for some $u \in \mathbb{C}^\times$ with $u^{-4}A = A$ and $u^{-6}B = B$. Considering the cases $r(\Gamma) = 3, 4, 6$ gives $A = 0$ or $B = 0$ as in (a) and (b). We compute the maps in (a)–(c) by considering the fixed subfields under these automorphisms, as above. \square

Suppose now that our vertex v_O of maximum rotation is either v_a or v_b , with rotations generated by an element δ_O (generating the coset representatives of $\Gamma/T(\Gamma)$). In this case, δ_O need not induce an automorphism of $E(\Gamma)$, because as a rotation of the plane δ_O need not take the lattice corresponding to $T(\Gamma)$ back to itself. However, we may simply translate, as in the following lemma.

Lemma 3.3.3. *Let $Q_O := (\wp(v_O), \wp'(v_O)/2) \in E(\Gamma)$ be the image of v_O . Let $E(\Gamma)'$ denote the elliptic curve whose underlying curve is $E(\Gamma)$ but with origin Q_O . Then we have an isomorphism*

$$(3.3.4) \quad \begin{aligned} \tau_{-Q_O}: E(\Gamma) &\rightarrow E(\Gamma)' \\ P &\mapsto P - Q_O \end{aligned}$$

of elliptic curves, and δ_O induces an automorphism of the elliptic curve $E(\Gamma)'$ under τ_{-Q_O} .

Proof. The translation isomorphism moves Q_O to the origin on $E(\Gamma)'$; thus the action induced by δ_O is bijective and fixes the origin on $E(\Gamma)'$, so gives an automorphism of $E(\Gamma)'$ as an elliptic curve. \square

Thus to compute the map $\beta: E(\Gamma) \rightarrow X(\Gamma)$, by the lemma we first compose with the isomorphism $\tau_{-Q_O}: E(\Gamma) \rightarrow E(\Gamma)'$ to reduce to the previous case. But rather than compute the point $Q_O \in E(\Gamma)$ and the translation map, we find it computationally more convenient to translate by the point $P_O := (\wp(v_O), \wp'(v_O)/2) \in E(\Delta)$ on the base curve.

Writing $E(\Delta)'$ for the elliptic curve $E(\Delta)$ having origin P_O , we have the following diagram:

$$(3.3.5) \quad \begin{array}{ccccc} & & E(\Gamma)' & & \\ & \nearrow \tau_{-Q_O} & \downarrow \psi & \searrow \beta' & \\ E(\Gamma) & & & \searrow \beta & X(\Gamma) \\ & \downarrow \psi & & & \downarrow \varphi \\ & & E(\Delta)' & & X(\Delta) \\ & \nearrow \tau_{-P_O} & \searrow \alpha' & & \\ E(\Delta) & & & \searrow \alpha & \end{array}$$

The diagram is commutative because $\psi(Q_O) = P_O$, both points corresponding to v_O under the complex uniformization. Note that the map $\psi: E(\Gamma)' \rightarrow E(\Delta)'$ has the same defining equation as the map $E(\Gamma) \rightarrow E(\Delta)$, and still defines a finite map of curves—it just loses the property of being a homomorphism.

In this way, we have “aligned” $E(\Delta)'$ with $E(\Gamma)'$, and we can more simply repeat the steps above with $E(\Delta)'$ in place of $E(\Delta)$ at the cost of computing translation maps $\tau_{P_O}: E(\Delta) \rightarrow E(\Delta)'$ with P_O the image of either v_a or v_b , giving a few more fixed maps α' , which can be computed by composing α with translation (computed using the group law).

Lemma 3.3.6. *The following statements hold, with $E(\Delta)' = E(\Delta)$ as in (3.1.1).*

(a) *If $c = 6$ and $v_O = v_a = v_2$, then we have*

$$\alpha': E(\Delta)' \rightarrow \mathbb{P}^1$$

$$(x, y) \mapsto \frac{(9\zeta_6 - 9)x^2 + 9\zeta_6x + 9}{x^3 + (3\zeta_6 - 3)x^2 - 3\zeta_6x + 1} = 9\zeta_6^2 \frac{(x - \zeta_6)(x + 1)}{(x + \zeta_6^2)^3}$$

(b) *If $c = 6$ and $v_O = v_b = v_3$, then we have*

$$\alpha': E(\Delta)' \rightarrow \mathbb{P}^1$$

$$(x, y) \mapsto \frac{x^6 + 8x^3y + 8x^3 + 16y^2 + 32y + 16}{x^6}$$

(c) *If $c = 4$ and $v_O = v_a = v_2$, then we have*

$$\alpha': E(\Delta)' \rightarrow \mathbb{P}^1$$

$$(x, y) \mapsto \frac{(x + 1)^2}{(x - 1)^2}$$

In Case (a), we may need to extend the field of definition K' to include ζ_6 . In the remaining cases, we have taken $v_O = v_c$ without loss of generality, so the maps (3.1.3) may be used. After having made this reduction, we drop the superscripts (the underlying curves have the same equations) and proceed to the final step.

3.4. The Belyi map. With three of the four maps in our master diagram determined, we complete the computation of $\varphi: X(\Gamma) \rightarrow X(\Delta)$ by filling in the map in the master diagram from the other three sides, using commutativity. To do this, we again apply Galois theory, referring to the field diagram (3.3.1).

Let $\xi := \alpha \circ \psi: E(\Gamma) \rightarrow X(\Delta)$, a map represented by a rational function $\xi(x, y) \in K'(x, y)$ where $E' = E(\Gamma): y^2 = f'(x)$ is the defining equation of E' . By commutativity, we have $\xi = \varphi \circ \beta$. If $r(\Gamma) = 1$, then β is the identity map so $\varphi = \xi$. So we may suppose that $r(\Gamma) > 1$.

The monomial map $\beta: E(\Gamma) \rightarrow X(\Gamma)$ is described by Lemma 3.3.2, corresponding to the cyclic field extension $\mathbb{C}(E(\Gamma)) \supseteq \mathbb{C}(X(\Gamma))$, given explicitly by $\beta(x, y) = y^2, x^2, y, x$. In particular, $\varphi \in \mathbb{C}(X(\Gamma))$ lies in this fixed field, and we need to solve

$$\xi(x, y) = \varphi(\beta(x, y))$$

given ξ and β explicitly for φ . Accordingly, we can write $\xi(x, y)$ as a rational function in the monomial $\beta(x, y)$, using the relation $y^2 = f'(x)$ if necessary, replacing every instance of $\beta(x, y)$ in $\xi(x, y)$ with a new variable u . Then $\varphi(u) \in K'(u)$ defines the map $\varphi: X(\Gamma) \simeq \mathbb{P}^1 \rightarrow \mathbb{P}^1$.

Remark 3.4.1. We have seen that Euclidean Belyi maps can be understood as descending an isogeny along a fixed quotient map; this is encoded in our master diagram. Our effort has been to take as input a permutation triple and then to compute the master diagram (associated isogeny and then its descent). One can also cut this in the middle, working directly with the master diagram by specifying a pair (K, H) where $K \leq \mathbb{Z}[j]/N\mathbb{Z}[j] \simeq (\mathbb{Z}/N\mathbb{Z})^2$ is a subgroup containing an element of order N and $H \leq \langle j \rangle$ is a subgroup with $H \neq \{\pm 1\}$ and $HK = K$. This data defines an isogeny to $E(\Delta)$ dual to the one provided by the torsion subgroup, and the descent is along the subgroup of automorphisms, with H stabilizing this kernel.

3.5. Proof of main result. To finish, we put all of the pieces together.

Algorithm 3.5.1. *This algorithm takes as input a Euclidean, transitive permutation triple $\sigma = (\sigma_a, \sigma_b, \sigma_c) \in S_d^3$ corresponding to a homomorphism $\pi: \Delta \rightarrow S_d$ with $\pi(\delta_s) = \sigma_s$ for $s = a, b, c$; it gives as output a model for the corresponding Belyi map from $X(\Gamma)$ to \mathbb{P}^1 .*

1. *Apply the preprocessing step by calling Algorithm 2.5.6, with vertex of maximal rotation v_O .*
2. *Depending on the case of (a, b, c) and v_O , look up β using Lemma 3.3.2 and the map $\alpha: E(\Delta) \rightarrow \mathbb{P}^1$ using Lemma 3.3.6 (referring back to 3.1.3).*
3. *Call Algorithm 2.4.4 to compute a basis η_1, η_2 for $T(\Gamma)$ and $N = [T(\Delta) : T(\Gamma)]$.*
4. *Call Algorithm 3.2.2 to compute $\psi: E(\Gamma) \rightarrow E(\Delta)$.*
5. *Compute the composition $\xi := \alpha \circ \psi$.*
6. *From $\xi = \varphi \circ \beta$, compute $\varphi: X(\Gamma) \rightarrow \mathbb{P}^1$ by substitution. Return φ .*

Theorem 3.5.2. *Algorithm 3.5.1 terminates with correct output.*

Proof. Correctness follows from our master diagram (1.3.1) and the correctness of each step, provided by the proof of correctness of the algorithm used except for Step 6, which is justified in Section 3.4. □

Remark 3.5.3. In the above, we assumed throughout a Euclidean triangle group Δ with three generators δ_a, δ_b , and δ_c with orders a, b , and c respectively and satisfying $\delta_c \delta_b \delta_a = 1$. These three generators corresponded to rotations around the three vertices of a designated triangle in the corresponding tessellation of the plane. We took as input to our algorithm the set of all permutation triples $\sigma = (\sigma_a, \sigma_b, \sigma_c)$ such that $\pi: \Delta \rightarrow S_n$ taking δ_i to σ_i described a group homomorphism with transitive image. In some contexts, we might prefer to work with the relation $\delta_a \delta_b \delta_c = 1$. The change amounts to a relabeling of vertices so that v_a, v_b , and v_c follow each other counterclockwise around a chosen triangle.

Accordingly, given a permutation triple σ' with $\sigma'_a \sigma'_b \sigma'_c = 1$, we just take inverses $\sigma_s := (\sigma'_s)^{-1}$ to obtain $\sigma_c \sigma_b \sigma_a = 1$, and we call our algorithm above with this inverted input.

4. Examples and data

We conclude with some examples computed using an implementation of Algorithm 3.5.1.

4.1. Description of implementation. We implemented Algorithm 3.5.1 using the *Magma* computer algebra system [4]. In particular, we used the existing implementation of Vélú's formula in calculating our isogeny ψ and the implementation of division polynomials. The construction of these isogenies is the most time intensive step in our calculation, as in general it involves working in a number field of possibly large degree. Even with this step, most of our example computations take no more than a few seconds to finish. Some examples in prime degree took as long as 30 minutes; an example in degree 100 took only 7 seconds.

Remark 4.1.1. Returning to Remark 2.2.11, we see that *Magma* provides two periods for E that span its associated lattice, so we are careful to generate our basis vectors for $T(\Gamma)$ and to deal with lattice coordinate points relative to the lattice *Magma* uses in its computations. As we only need worry about this for our two canonical elliptic curves, we can see which lattice *Magma* uses, compare it to our own lattices described above, and convert coordinates between the two by a simple change of basis operation.

4.2. Belyi maps obtained from triples. We give here some examples to illustrate Algorithm 3.5.1. We list the final Belyi maps from $\varphi: X(\Gamma) \rightarrow \mathbb{P}^1$ and provide factorizations of the numerator, denominator, and their difference in the case of genus zero maps, confirming the correspondence between ramification at $0, \infty$, and 1 respectively and the cycle structure of σ . (We provide monic factorizations, ignoring leading coefficients.)

Example 4.2.1. Given the permutation triple $\sigma := ((243), (134), (123))$, we will illustrate the steps in our algorithm and determine the corresponding Belyi map. First, we call Algorithm 2.5.6 and conjugate σ by the transposition (14) to obtain $((213), (431), (423))$ where v_c is then the vertex of maximal rotation. Since this conjugate triple gives an isomorphic Belyi map, we will redefine $\sigma := ((213), (431), (423))$. Since $\omega_1 := \delta_b \delta_c^2$ and $\omega_2 := \delta_b^2 \delta_c$ span the translations in $T(\Delta)$ by Corollary 2.2.7, we take $\sigma_1 = \pi(\omega_1) = (13)(24)$ and $\sigma_2 = \pi(\omega_2) = (14)(23)$ and call Algorithm 2.4.4. We find our basis vectors for $T(\Gamma)$ are $\eta_1 = \omega_1^2$ and $\eta_2 = \omega_2^2$ so $n_1 = 2, n_2 = 0, m_1 = 0$, and $m_2 = 2$.

We obtain the rotation index

$$r = \frac{cn_1m_2}{d} = \frac{3(2)(2)}{4} = 3$$

and take $N = [T(\Delta) : T(\Gamma)] = n_1m_2 = 4$, so the points in $T(\Delta) \setminus \mathbb{C}$ in the kernel of the multiplication by N map from $T(\Delta) \setminus \mathbb{C}$ to $T(\Gamma) \setminus \mathbb{C}$ are

$$A = \{(0, 0), (1/2, 0), (0, 1/2), (1/2, 1/2)\}$$

with coordinates relative to ω_1 and ω_2 , while the points whose images on $E(\Delta)$ have distinct x -coordinates are $K := \{(1/2, 0), (0, 1/2), (1/2, 1/2)\}$ as in Step 3 of Algorithm 3.2.5. Letting k_1, k_2 , and k_3 be the x -coordinates of the images of these three points on $E(\Delta)$, we obtain the kernel polynomial

$$p(x) = (x - k_1)(x - k_2)(x - k_3) = x^3 + 1$$

which we input to Vélú's formula and take the dual to obtain the isogeny $\psi: E(\Gamma) \rightarrow E(\Delta)$ given by

$$\psi(x, y) = \left(\frac{(1/16)x^4 - 32x}{x^3 + 64}, \frac{(1/64)x^6y + 20x^3y - 512y}{x^6 + 128x^3 + 4096} \right)$$

and see that $E(\Gamma)$ is given by the equation $y^2 = x^3 + 64$.

Since we are in the $\Delta(3, 3, 3)$ case, our map $\alpha: E(\Delta) \rightarrow \mathbb{P}_{\mathbb{C}}^1$ is given by $\alpha(x, y) = (y + 1)/2$, so the composition $\xi = \alpha \circ \psi: E(\Gamma) \rightarrow \mathbb{P}_{\mathbb{C}}^1$ is given by

$$\begin{aligned} \xi(x, y) &= \alpha \left(\frac{(1/16)x^4 - 32x}{x^3 + 64}, \frac{(1/64)x^6y + 20x^3y - 512y}{x^6 + 128x^3 + 4096} \right) \\ &= \frac{(1/128)x^6y + (1/2)x^6 + 10x^3y + 64x^3 - 256y + 2048}{x^6 + 128x^3 + 4096} \end{aligned}$$

Finally, since $r = 6$, the map $\beta: E(\Gamma) \rightarrow X(\Gamma)$ has $\beta(x, y) = y$. So, we wish to rewrite ξ in terms of only y . Since points on $E(\Gamma)$ satisfy $x^3 = y^2 - 64$, we may replace each instance of x^3 in ξ with $y^2 - 64$; we obtain a rational function in y , which gives our final Belyi map

$$\varphi(x) = \frac{(1/128)x^4 + (1/2)x^3 + 9x^2 - 864}{x^3}$$

Let $N(x)$ and $D(x)$ be the numerator and denominator of φ respectively. Note that the preimages under φ of $0, \infty$, and 1 respectively are the roots of N, D , and $N - D$. To confirm the ramification of φ , we note that up to a constant multiple we have the factorizations

$$\begin{aligned} N(x) &= (x - 8)(x + 24)^3 \\ D(x) &= x^3 \\ N(x) - D(x) &= (x + 8)(x - 24)^3 \end{aligned}$$

where the repeated factors confirm the ramification, and we note the direct correspondence between the powers of the factors and the cycle structure of σ .

Example 4.2.2. Given $\sigma := ((14)(25)(36), (135), (145236))$, we determine that $X(\Gamma)$ has genus 0 and the corresponding Belyi map $\varphi: X(\Gamma) \rightarrow \mathbb{P}^1_{\mathbb{C}}$ is given by

$$\varphi(x) = \frac{x^6 + 162x^5 + 7047x^4 + 43740x^3 + 413343x^2 + 1062882x + 4782969}{x^6 - 54x^5 + 1215x^4 - 14580x^3 + 98415x^2 - 354294x + 531441}$$

with numerator, denominator, and difference given by

$$\begin{aligned} N(x) &= (x^3 + 81x^2 + 243x + 2187)^2 \\ D(x) &= (x - 9)^6 \\ N(x) - D(x) &= (x^2 + 27)(x + 9)^3 \end{aligned}$$

Example 4.2.3. Now given $\sigma := ((19)(28)(37)(46), (16)(29103)(4587), (1254)(38)(67109))$ we obtain

$$\varphi(x) = \frac{1/625x^{10} + 1/125(8i + 44)x^8 + 1/25(264i + 702)x^6 + 1/5(2872i + 4796)x^4 + (10296i + 11753)x^2}{x^8 + 1/5(152i - 164)x^6 + 1/25(-18696i + 1422)x^4 + 1/125(547048i + 434764)x^2 + 1/625(-1476984i - 9653287)}$$

with numerator $x^2(x^2 + 10i + 55)^4$, denominator $(x^2 + 1/5(38i - 41))^4$, and difference

$$(x - 4i + 3)(x + 4i - 3)(x^2 + (-2i + 14)x - 24i - 7)^2(x^2 + (2i - 14)x - 24i - 7)^2$$

where $i^2 = -1$.

Remark 4.2.4. Unfortunately, our algorithms do not automatically descend the Belyi map to a minimal field of definition (if such a field exists). For example, for the permutation triple $\sigma := ((14), (126)(345), (162435))$ we find the map

$$\varphi(x) = 36(\zeta_6 - 1) \frac{(x - 2)(x - 2\zeta - 1)^2(x^2 + 2x - 11)}{(x + 2z - 3)^6}$$

defined over $\mathbb{Q}(\zeta_6)$; however, it can be shown that the Belyi map descends to \mathbb{Q} , given more simply by $\varphi(x) = 9(3x^6 - 3x^4 + x^2)$. We refer to Sijsling–Voight [12, §6] and Musty–Schiaivone–Sijsling–Voight [11, §4] for further discussion.

References

- [1] D. BARTH & A. WENZ, “Computation of Belyi maps with prescribed ramification and applications in Galois theory”, *J. Algebra* **569** (2021), p. 616–642.
- [2] G. V. BELYĬ, “Galois extensions of a maximal cyclotomic field”, *Math. USSR, Izv.* **14** (1980), no. 2, p. 247–256.
- [3] ———, “A new proof of the three-point theorem”, *Sb. Math.* **193** (2002), no. 3–4, p. 329–332.
- [4] W. BOSMA, J. CANNON & C. PLAYOUST, “The Magma algebra system. I. The user language”, *J. Symb. Comput.* **24** (1997), no. 3–4, p. 235–265.
- [5] A. GROTHENDIECK, “Sketch of a programme (translation into English)”, in *Geometric Galois Actions. 1. Around Grothendieck’s Esquisse d’un Programme* (L. Schneps & P. Lochak, eds.), London Mathematical Society Lecture Note Series, vol. 242, Cambridge University Press, 1997, p. 243–283.
- [6] M. KLUG, M. MUSTY, S. SCHIAVONE & J. VOIGHT, “Numerical calculation of three-point covers of the projective line”, *LMS J. Comput. Math.* **17** (2014), no. 1, p. 379–430.
- [7] THE LMFDB COLLABORATION, “The L-functions and Modular Forms Database”, <http://www.lmfdb.org>, accessed 27 May 2020.
- [8] W. MAGNUS, *Noneuclidean tessellations and their groups*, Pure and Applied Mathematics, vol. 61, Academic Press Inc., 1974.
- [9] H. MONIEN, “The sporadic group J_2 , Hauptmodul and Belyi map”, <https://arxiv.org/abs/1703.05200>, 2017.
- [10] ———, “The sporadic group Co_3 , Hauptmodul and Belyi map”, <https://arxiv.org/abs/1802.06923>, 2018.
- [11] M. MUSTY, S. SCHIAVONE, J. SIJSLING & J. VOIGHT, “A database of Belyi maps”, in *Proceedings of the Thirteenth Algorithmic Number Theory Symposium (ANTS-XIII)* (R. Scheidler & J. Sorenson, eds.), The Open Book Series, vol. 2, Mathematical Sciences Publishers, p. 375–392.
- [12] J. SIJSLING & J. VOIGHT, “On computing Belyi maps”, *Publ. Math. Besançon, Algèbre Théorie Nombres* **2014** (2014), no. 1, p. 73–131.
- [13] J. SILVERMAN, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer, 1994.
- [14] ———, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer, 2009.
- [15] J. VÉLU, “Isogénies entre courbes elliptiques”, *C. R. Acad. Sci. Paris* **273** (1971), p. 238–241.

Matthew RADOSEVICH
 Department of Mathematics
 Dartmouth College
 6188 Kemeny Hall
 Hanover, NH 03755, USA
E-mail: matt.j.radosevich@gmail.com

John VOIGHT
 Department of Mathematics
 Dartmouth College
 6188 Kemeny Hall
 Hanover, NH 03755, USA
E-mail: jvoight@gmail.com
URL: <http://www.math.dartmouth.edu/~jvoight/>