Belyi map verification using certified path tracking

Alexandre Guillemot[1][0009−0004−1795−3729] and John Voight[2][0000−0001−7494−8732]

[1] Inria, Université Paris–Saclay, Palaiseau, 91120, France
alexandre.guillemot@inria.fr
[2] School of Mathematics and Statistics, University of Sydney, NSW, 2006, Australia
jvoight@gmail.com

Abstract. We provide an end-to-end workflow to rigorously compute the monodromy of Belyi maps from exact equations over number fields using certified homotopy continuation. We then apply this method at scale to certify the monodromy triples of Belyi maps in the L-functions and Modular Forms Database (LMFDB).

Keywords: Belyi maps, monodromy, certified homotopy continuation, interval arithmetic, numerical algebraic geometry

1 Introduction

Motivation and context

Let X be a smooth projective algebraic curve over $\mathbb{C}$ or equivalently a compact Riemann surface. A Belyi map is a nonconstant map $\varphi\colon X \to \mathbb{P}^1_{\mathbb{C}}$ unramified away from $\{0, 1, \infty\}$. Belyi [5] proved that X can be defined over $\mathbb{Q}^{\mathrm{al}}$ if and only if it admits a Belyi map. Explicit methods for Belyi maps have seen many applications—see Sijsling–Voight [25] for an overview, as well as the more recent work by Roberts [22], Barth–Wenz [1], and Berghaus–Monien–Radchenko [6]. These methods take as input a permutation triple encoding the monodromy around the branch points and return candidate equations over a number field $K \subset \mathbb{C}$. One can certify that the map is indeed a Belyi map with the correct ramification.

In this paper, we tackle rigorously the certification that the monodromy triple of the map indeed coincides with the given input. Algebraic techniques [13, 1] may suffice to compute the monodromy group and the triple when uniquely determined, but do not provide a general approach. On the other hand, monodromy permutations can be computed from the equations using *certified path tracking*: for a parametrized polynomial system F_t, one follows the zeros of F_t along loops in the base. For monodromy, a heuristic approach is not sufficient even with *a posteriori* end point certification, since path jumping or swapping may occur [3, §6.2]. Certified methods instead isolate the tracked zero along the whole path, ensuring correctness.

Previous work

The idea of using certified path tracking or homotopy continuation to rigorously compute the monodromy of Belyi maps is not new. For instance, Schneps [24] and Bruin–Sijsling–Zotine [9, §2C] describe predictor-corrector loops whose certification rely on a step size bound. Deconinck–van Hoeij [10] and Bartholdi–Buff–Graf Von Bothmer–Kröker [2] present approaches that compute fibers above the points of a discretization of the parameter path and connect each consecutive fibers to recover the monodromy permutation. However, implementing these methods to obtain a rigorous result is difficult, as they may consider implicit bounds, that roots of polynomials can be obtained exactly, or assume a model of exact computation over the reals (e.g., the BSS model) for correctness.

Beltrán–Leykin [4] provide the first implemented certified homotopy continuation algorithm in the Turing machine model, using exact arithmetic over the rationals and with generality well beyond Belyi maps. For rigorous numerical computations, other methods rely on interval arithmetic in some way. For the univariate case, see the algorithms and implementations by Marco-Buzunariz–Rodríguez [19], Kranich [18], and Xu–Burr–Yap [27]. The multivariate case is tackled by Guillemot–Lairez [16] and Duff–Lee [11], based on ideas from van der Hoeven [26]. The preprint by Duff–Lee [12] addresses monodromy computations for general complex algebraic branched covers, with an emphasis on practical results and including Belyi maps.

Contribution

Using Algpath [15, 16], a certified path tracking software based on Krawczyk's operator, interval arithmetic, and Taylor models, we rigorously compute the monodromy triples of the 1111 Belyi maps present in the LMFDB [21]. The results prove for the first time the correctness of the monodromy groups and, up to minor issues with permuting the branch points $\{0, 1, \infty\}$, of the monodromy triples attached to all entries in the database. Code is available online [14]. This demonstrates that recent advances make certified homotopy continuation a practical tool to compute the monodromy of finite algebraic maps.

2 Setup

Monodromy representation

Let X be a smooth projective algebraic curve over $\mathbb{C}$ and let $\varphi\colon X \to \mathbb{P}^1_{\mathbb{C}}$ be a Belyi map of degree d. Put $U := \mathbb{P}^1_{\mathbb{C}} \setminus \{0, 1, \infty\}$, so that φ restricts to a topological cover $\varphi^{-1}(U) \to U$ of degree d.

Fix a basepoint $b \in U$ and label the fiber $\varphi^{-1}(b) = \{x_1, \dots, x_d\}$. Analytic continuation along loops in U defines a monodromy representation $\rho\colon \pi_1(U, b) \to S_d$. Choosing standard loops $\gamma_0, \gamma_1, \gamma_\infty$ around $0, 1, \infty$ with $\gamma_0\gamma_1\gamma_\infty = 1$, we obtain permutations $\sigma_0, \sigma_1, \sigma_\infty$ satisfying $\sigma_0\sigma_1\sigma_\infty = 1$, called the monodromy triple of φ, well-defined up to simultaneous conjugation. The subgroup $G =$

$\langle \sigma_0, \sigma_1, \sigma_\infty \rangle \subseteq S_d$ is the (geometric) monodromy group. The cycle structure of σ_s records the ramification above $s \in \{0, 1, \infty\}$.

Analytic continuation via polynomial systems

To compute this triple from equations, let $Y \subseteq \mathbb{C}^n$ be an affine chart cut out by polynomials $g_1, \ldots, g_{n-1}$, and suppose φ is represented on this chart by a rational function p/q. Consider the polynomial system

$$F_t(x, z) = \big(g_1(x), \ldots, g_{n-1}(x),\, p(x) - tq(x),\, q(x)z - 1\big). \tag{1}$$

For each $t \in U$, the regular zeros of F_t are in bijection with the points of $\varphi^{-1}(t)$, since $q(x)z - 1 = 0$ excludes the common vanishing locus of p and q. Over U, these zeros are regular and vary analytically with t, so analytic continuation of zeros of (1) agrees with path lifting for φ.

Therefore, if $\gamma\colon [0,1] \to U$ is a loop based at b and each regular zero of F_b is tracked correctly along γ, then the induced permutation on the zeros of F_b is the monodromy permutation of φ associated to γ. In particular, it is enough to compute the permutations associated to loops around 0 and 1.

3 Monodromy computations using path tracking

We briefly explain the underlying algorithm of Algpath and how it applies to the computation of monodromy permutations.

Data structure for regular zeros of polynomial systems

Let $f\colon \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map. We review Moore's root isolation criterion, based on Krawczyk's operator, and the associated data structure for regular zeros. We denote by B the unit ball for the real ∞-norm on $\mathbb{C}^n$, and by I_n the $n \times n$ identity matrix.

Theorem 2 (Moore's criterion). *Let $\rho \in (0,1)$, $x \in \mathbb{C}^n$, $r > 0$ and $A \in \mathbb{C}^{n\times n}$. Suppose that for all $u, v \in rB$, we have*

$$-Af(x) + (I_n - Adf(x+u))v \in \rho r B. \tag{3}$$

Then there exists a regular zero ζ of f in $x + \rho r B$, and it is the unique zero of f in $x + rB$.

The proof can be found in [23, 16] and relies on Banach's fixed-point theorem.

Definition 4 (Moore boxes). *Let $\rho \in (0,1)$. A ρ-Moore box for f is a triple $(x, r, A) \in \mathbb{C}^n \times \mathbb{R}_> \times \mathbb{C}^{n\times n}$ satisfying (3).*

A Moore box is a ρ-Moore box for some $\rho \in (0,1)$. By Theorem 2, a Moore box represents a unique regular zero of f. Condition (3) is checked effectively by interval arithmetic [20]. Given a ρ-Moore box $m = (x, r, A)$ and $\tau \in (0,1)$, one can refine m to a τ-Moore box with the same associated zero by quasi-Newton iterations and reductions of r [16, Algorithm 2]. Equality of the zeros represented by two Moore boxes is decided by refining both to 1/3-Moore boxes and checking whether the shrunken boxes intersect.

Path tracking algorithm

We focus on the algorithm implemented in Algpath; a precise description is given in [16]. Let $F\colon \mathbb{C} \times \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map. The first argument is the parameter, put in subscript, so that $F_t\colon \mathbb{C}^n \to \mathbb{C}^n$ is the map obtained from F by specialization of the parameter. Let $x \in \mathbb{C}^n$ be a regular zero of F_0, and let $\zeta\colon [0,1] \to \mathbb{C}^n$ be the corresponding solution path. The input zero is given by a Moore box m, and Algpath alternates:

1. correction: refine m to a 1/8-Moore box;
2. prediction: compute $\delta > 0$ such that for all $s \in [t, t+\delta]$, m is a 7/8-Moore box for F_s, then update t to $t+\delta$.

When $t = 1$, the algorithm returns a Moore box for $\zeta(1)$. Guillemot–Lairez [16] prove termination and correctness in a practical computational model, and explain how predictors and Taylor models improve efficiency.

To track a zero of F along a more general path $\gamma\colon [0,1] \to \mathbb{C}$, we precompose F with γ in the t variable. In this article, the parameter paths are piecewise linear loops, and we track each linear piece in turn.

Computing monodromy permutations

Let $F\colon \mathbb{C} \times \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map, let X be the variety of pairs (t,x) such that $F(t,x) = 0$, let p be the projection on the first variable, and denote by $X_t = p^{-1}(t)$ the fiber above $t \in \mathbb{C}$. Suppose that p is dominant and X has dimension 1, so that it is a branched cover, unramified over

$$U := \{t \in \mathbb{C} : X_t \text{ is non-empty and consists of finitely many regular points}\}.$$

Let $\gamma\colon [0,1] \to U$ be a loop based at $b \in U$. To compute the monodromy permutation associated to γ, we first compute the fiber X_b and represent its points by Moore boxes. We then run certified path tracking along γ from each point of the fiber. The resulting ending boxes again represent the points of X_b, and the monodromy permutation is obtained by identifying which starting and ending Moore boxes represent the same zero.

Because a permutation on d points is determined by its action on $d-1$ points, we do all d path tracking runs in parallel and halt whenever $d-1$ runs finish. This improves computational time when one zero is slower to track.

4 Verification of Belyi maps

The method of Klug–Musty–Schiavone–Voight [17], used for the LMFDB [21], computes equations for the Belyi map associated to a given permutation triple σ. Once the equations are computed, it remains to check that the monodromy triple of the equations is simultaneously conjugate to σ. Using Algpath, we perform this check for all Belyi maps present on the LMFDB.

Parametric system building

We explain how to build a parametric system to compute the monodromy of a given Belyi map for each data type encountered on the LMFDB.

Smooth model. In this case, the Belyi map is given by a polynomial $f \in \mathbb{C}[x, y]$ and a bivariate rational function $p/q \in \mathbb{C}(x, y)$. By homogenizing, we obtain a smooth curve $X \subseteq \mathbb{P}^2$, and p/q induces a map $\varphi\colon X \to \mathbb{P}^1$. The system we use to compute the monodromy is

$$f = p - tq = 0. \tag{5}$$

For fixed $t \in \mathbb{C}$, this system captures the fiber $\varphi^{-1}(t)$ together with the points of X on which p and q vanish simultaneously. Adding $qz - 1 = 0$ removes the latter but may greatly slow down path tracking. In practice, we compute starting solutions using the enlarged system and then track (5), excluding the solutions on which q vanishes. More precisely, from a Moore box for the enlarged system with center (x, y, z) we compute a Moore box for (5) centered at (x, y); Theorem 2 ensures that q does not vanish on the associated zero.

Smooth case with curve $\mathbb{P}^1$. Whenever the underlying curve is $\mathbb{P}^1$, the LMFDB provides a rational function $p/q \in \mathbb{C}(x)$ representing a map $\mathbb{P}^1 \to \mathbb{P}^1$. In this case, we compute the monodromy using $p - tq = 0$ after checking that p and q are coprime.

Plane models. Some entries provide, in addition to the smooth model, one polynomial equation $f \in \mathbb{C}[t, x]$ defining a possibly singular curve, and a constant $\lambda \in \mathbb{C}$. If $p\colon V(f) \to \mathbb{C}$ is the projection on the variable t, then λp induces a map from the normalization of $V(f)$ to $\mathbb{P}^1$, and we compute the monodromy by tracking the roots of $f(x, \lambda^{-1}t)$.

Computing the fiber above the base point

To compute the monodromy of a Belyi map, we first need a Moore box for each point in the fiber above the base point for the loops around 0 and 1. We numerically compute the fiber and then certify 1/3-Moore boxes around the resulting approximations. The whole fiber is captured as soon as the number of Moore boxes matches the degree of the map and they represent distinct zeros, which we check using the equality test of Section 3.

In the smooth case where the curve is $\mathbb{P}^1$, or when a plane model is available, this amounts to solving a univariate polynomial with complex coefficients after embedding the equations into $\mathbb{C}$, so we use a standard root finder in SageMath. Otherwise we use `Msolve` [7] on (5), before embedding the equations into $\mathbb{C}$ and treating ν as a variable. This yields fibers, for all embeddings of the number field, which we sort using the ν-coordinate. For each fiber, we also get the unwanted

common locus of p and q over X; to remove it, we discard the points whose evaluation by q is the smallest, until the size of the fiber matches the degree of the map. We choose `Msolve` as it is directly accessible from SageMath and requires no additional setup, but we also experimented with `HomotopyContinuation.jl` [8] and found it to be a suitable alternative for this task.

Dealing with algebraic coefficients

Algpath can handle polynomial systems with rational, floating point, or interval coefficients, whereas the equations defining Belyi maps may have algebraic coefficients. Each LMFDB entry specifies a number field $\mathbb{Q}(\nu)$ by the minimal polynomial m_ν of ν, and the coefficients of the equations are polynomials in ν with rational coefficients. Given an embedding $\mathbb{Q}(\nu) \hookrightarrow \mathbb{C}$, corresponding to a root α of m_ν, we obtain a Belyi map by evaluating at α.

One possibility is to treat ν as an additional variable, add m_ν to the system, and extend each starting zero with α on the ν-coordinate. This ensures termination but introduces a substantial cost, and the closeness of the roots of m_ν may force small Moore boxes and hence small step sizes. In practice, we instead compute a tight interval around α and replace ν by this interval in the system. If the interval is not tight enough, the algorithm may stall, but whenever a run succeeds the result is correct. This performs much better in practice: for the Belyi map with entry 7T7-6.1_5.2_4.2.1-a, adding the number field equation did not finish within 6 days, whereas replacing α by an interval took less than 20 seconds.

Practical results

We compute the triples for all 1111 entries of the LMFDB database. The results can be found online [14]. Using plane models when available, the whole computation takes 1.7 hours of CPU time, of which 1.2 hours correspond to monodromy computations, and the total wall clock time is 30 minutes on 128 threads.

Using the resulting triples, we prove correctness of all monodromy groups in the database. The computations brought to light a few bugs. First, the triples computed using plane models only correspond to the triples on the database up to an S_3-action, coming from post-composition by an automorphism of $\mathbb{P}^1$ that permutes $\{0, 1, \infty\}$. In this case, we check correctness only up to this S_3-action. Second, we found a few mistakes in the embedding values and in the tables matching embeddings and triples. Other than that, all remaining triples were proved correct.

Additionally, we verified the monodromy of the maps provided by Barth–Wenz [1], whose degree ranges from 55 to 280, with the exception of two: the two maps with highest degree (266 and 280) are defined over a non-trivial number field, and while their monodromy group could be verified using algebraic techniques, their monodromy triples remain unverified.

5 Conclusion

We have presented a certified method, implemented in Algpath, for recovering the monodromy of a Belyi map from exact equations over number fields. The method tracks regular solutions of a parametrized polynomial system along loops using interval arithmetic, Krawczyk-based root isolation, and certified homotopy continuation. Finally, we showed that this approach works at scale, certifying the monodromy triples of all Belyi maps currently in the LMFDB.

Acknowledgements

We are grateful to Anton Leykin, Pierre Lairez, and Éric Pichon-Pharabod for useful discussions, as well as to Joshua Perlmutter for his work at initial stages of the project. Guillemot was supported by the European Research Council (ERC) under the European Union's Horizon Europe research and innovation program, grant agreement 101040794 (10000 DIGITS). Voight was supported by a grant from the Simons Foundation (SFI-MPS-Infrastructure-00008650).

References

[1] D. Barth and A. Wenz. "Computation of Belyi Maps with Prescribed Ramification and Applications in Galois Theory". In: *Journal of Algebra* 569 (2021), pp. 616–642.

[2] L. Bartholdi, X. Buff, H.-C. Graf Von Bothmer, and J. Kröker. "Algorithmic Construction of Hurwitz Maps". In: *Experimental Mathematics* 24.1 (2015), pp. 76–92.

[3] C. Beltrán and A. Leykin. "Certified Numerical Homotopy Tracking". In: *Experimental Mathematics* 21.1 (2012), pp. 69–83.

[4] C. Beltrán and A. Leykin. "Robust certified numerical homotopy tracking". In: *Found. Comput. Math.* 13.2 (2013), pp. 253–295.

[5] G. V. Belyi. "On Galois Extensions Of a Maximal Cyclotomic Field". In: *Math. USSR Izv.* 14.2 (1980), p. 247.

[6] D. Berghaus, H. Monien, and D. Radchenko. "On the computation of modular forms on noncongruence subgroups". In: *Math. Comp.* 93.347 (2024), pp. 1399–1425.

[7] J. Berthomieu, C. Eder, and M. Safey El Din. "Msolve: A Library for Solving Polynomial Systems". In: *Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation*. ISSAC '21. New York, NY, USA: Association for Computing Machinery, 2021, pp. 51–58.

[8] P. Breiding and S. Timme. "HomotopyContinuation.Jl: A Package for Homotopy Continuation in Julia". In: *Mathematical Software – ICMS 2018*. Ed. by J. H. Davenport, M. Kauers, G. Labahn, and J. Urban. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018, pp. 458–465.

[9] N. Bruin, J. Sijsling, and A. Zotine. "Numerical computation of endomorphism rings of Jacobians". In: *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*. Vol. 2. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2019, pp. 155–171.

[10] B. Deconinck and M. van Hoeij. "Computing Riemann Matrices of Algebraic Curves". In: *Physica D: Nonlinear Phenomena*. Advances in Nonlinear Mathematics and Science: A Special Issue to Honor Vladimir Zakharov 152–153 (2001), pp. 28–46.

[11] T. Duff and K. Lee. "Certified Homotopy Tracking Using the Krawczyk Method". In: *Proc. ISSAC 2024*. New York, NY, USA: Association for Computing Machinery, 2024, pp. 274–282.

[12] T. Duff and K. Lee. *Certifying Galois/Monodromy Actions via Homotopy Graphs*. 2026. arXiv: 2603.17288 [math].

[13] N. D. Elkies. "The complex polynomials $P(x)$ with $\mathrm{Gal}(P(x) - t) \cong M_{23}$". In: *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*. Vol. 1. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2013, pp. 359–367.

[14] A. Guillemot. *Belyi monodromy*. https://gitlab.inria.fr/aguillem/belyi-monodromy. GitLab repository. Accessed 2026-04-12.

[15] A. Guillemot. "Certified Algebraic Path Tracking with Algpath". In: *ACM Commun. Comput. Algebra* 59.3 (2026), pp. 53–56.

[16] A. Guillemot and P. Lairez. "Validated Numerics for Algebraic Path Tracking". In: *Proc. ISSAC 2024*. New York, NY, USA: Association for Computing Machinery, 2024, pp. 36–45.

[17] M. Klug, M. Musty, S. Schiavone, and J. Voight. "Numerical Calculation of Three-Point Branched Covers of the Projective Line". In: *LMS J. Comput. Math.* 17.1 (2014), pp. 379–430.

[18] S. Kranich. *An Epsilon-Delta Bound for Plane Algebraic Curves and Its Use for Certified Homotopy Continuation of Systems of Plane Algebraic Curves*. 2016. arXiv: 1505.03432 [math].

[19] M. Á. Marco-Buzunariz and M. Rodríguez. "SIROCCO: A Library for Certified Polynomial Root Continuation". In: *Mathematical Software – ICMS 2016*. Ed. by G.-M. Greuel, T. Koch, P. Paule, and A. Sommese. Vol. 9725. Cham: Springer International Publishing, 2016, pp. 191–197.

[20] R. E. Moore, R. B. Kearfott, and M. J. Cloud. *Introduction to Interval Analysis*. Other Titles in Applied Mathematics. Society for Industrial and Applied Mathematics, 2009.

[21] M. Musty, S. Schiavone, J. Sijsling, and J. Voight. "A Database of Belyi Maps". In: *Open Book Series* 2.1 (2019), pp. 375–392.

[22] D. P. Roberts. "Hurwitz–Belyi Maps". In: *Publications mathématiques de Besançon. Algèbre et théorie des nombres* (2018), pp. 25–67.

[23] S. M. Rump. "Solving Algebraic Problems With High Accuracy". In: *A New Approach to Scientific Computation*. Ed. by U. W. Kulisch and W. L. Miranker. Academic Press, 1983, pp. 51–120.

[24] "Dessins d'enfants on the Riemann Sphere". In: *The Grothendieck Theory of Dessins d'Enfants*. Ed. by L. Schneps. London Mathematical Society Lecture Note Series. Cambridge: Cambridge University Press, 1994, pp. 47–78.

[25] J. Sijsling and J. Voight. "On Computing Belyi Maps". In: *Publications mathématiques de Besançon. Algèbre et théorie des nombres* 1 (2015), pp. 73–131.

[26] J. van der Hoeven. *Reliable Homotopy Continuation*. Research Report. LIX, Ecole polytechnique, 2015.

[27] J. Xu, M. Burr, and C. Yap. "An Approach for Certifying Homotopy Continuation Paths: Univariate Case". In: *Proc. ISSAC 2018*. New York, NY, USA: Association for Computing Machinery, 2018, pp. 399–406.