Puiseux Series Solutions with Real or Rational Coefficients of First Order Autonomous AODEs

Sebastian Falkensteiner
Research Institute for Symbolic Computation (RISC), Johannes Kepler University
Linz, Austria
falkensteiner@risc.jku.at

ABSTRACT

Given an autonomous first order algebraic ordinary differential equation $F(y, y') = 0$, we provide algorithms for computing formal Puiseux series solutions of $F(y, y') = 0$ with real or rational coefficients. For this purpose we give necessary and sufficient conditions on the existence of such solutions by combining classical methods from algebraic geometry and the study of an associated differential equation. Since all formal Puiseux series solutions of such differential equations are convergent in a certain neighborhood, the solutions also define real solution functions.

CCS CONCEPTS

• **Mathematics of computing → Ordinary differential equations**; Solvers.

KEYWORDS

Algebraic differential equation, algebraic curve, real solution, formal Puiseux series solution, topological graph.

ACM Reference Format:
Sebastian Falkensteiner. 2022. Puiseux Series Solutions with Real or Rational Coefficients of First Order Autonomous AODEs. In *Proceedings of the 2022 Int'l Symposium on Symbolic and Algebraic Computation (ISSAC '22), July 4–7, 2022, Villeneuve-d'Ascq, France.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3476446.3536185

1 INTRODUCTION

Let $\mathbb{K}$ be a field such that $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$, and let us consider first order autonomous algebraic ODEs (shortly AODEs)

$$F(y, y') = 0 \text{ where } F \in \mathbb{K}[y, p]. \tag{1}$$

In this paper, we are interested in computing the Puiseux series solutions of (1) with coefficients in certain field extension of $\mathbb{K}$, where "computing" means to represent the set of Puiseux series solutions, in one-to-one correspondence, by means of a set of truncations.

Rational and algebraic solutions of (1) have been studied in [11, 12] and [2] by using an algebraic-geometric approach. In the current paper, where Puiseux series solutions are studied, we follow an adapted version of this approach. More precisely, we use the well-known theory on local parametrizations (see e.g. [9]) for deriving an associated differential equation which can be solved, for example, by the Newton polygon method [5]. In the current work, the bounds on local parametrizations presented in [9] are generalized to the non-monic case.

In [6] we have proved that every formal Puiseux series solution of (1) is convergent. Moreover, under the assumption that $\mathbb{K}$ is computable, [6] shows how these solutions can be algorithmically found. Alternatively, one can find several papers in the literature for computing series solutions by means of the construction of the Newton polygon, e.g. [4, 14, 21]. All these works have in common that they are not completely algorithmic and do not have a-priori bounds on the number of terms which have to be determined to ensure that the solution truncations are in one-to-one correspondence with the series solutions. This is a major difference to [6].

Similarly as in the theory of rational parametrizations (see e.g. [20]), the question of finding optimal field extensions of $\mathbb{K}$, where the Puiseux series solutions can be expressed, arises. Furthermore, motivated by the potential applications, the study and determination of the Puiseux series solutions with coefficients in a real field extension of $\mathbb{K}$ turn to be specially interested. Observe that formal Puiseux series with a positive radius of convergence locally define solution functions. Moreover, if the coefficients of the series are real, then the image of the solution function is real as well and hence of major interest in applications. The smoothness of the solution functions can be read off the exponents of the series. Let us note that the classical methods for computing real solution functions such as the Picard-Lindelöf Theorem typically fail for the differential equations treated here. More recently, a theory for analyzing dynamical systems related to the given differential equations, also applicable to AODEs [18], has been developed. At singular curve points, however, the method is, in principle, not algorithmic either.

In [6], the first initial steps for the optimal field extension problem have been achieved. Nevertheless, the problem remains open, in particular, the reality issue. This is where the current paper focuses. Let $\mathbb{L}$ be either $\mathbb{Q}$ or $\mathbb{R}$. So, $\mathbb{K}$ is from now assumed to be real. In this paper, we further analyze the results of necessary field extensions and focus on the solution set to Puiseux series with coefficients in $\mathbb{L}$, called $\mathbb{L}$-*Puiseux series*. For this purpose, several aspects and results of various different areas of mathematics are required. The main contribution of this paper can be seen in the adaptation of these techniques and the results in [6] to the differential problem studied here. We give some new, linking results and show necessary and sufficient conditions for the existence of $\mathbb{L}$-Puiseux series solutions. In addition, we provide algorithms for computing formal Puiseux series solutions of (1) with real or rational coefficients. An implementation of this work is described in [3].

The structure of the paper is as follows. Section 2 is devoted to the preliminary theory on real and algebraic curve points and local

ACM ISBN 978-1-4503-8688-3/22/07…$15.00
https://doi.org/10.1145/3476446.3536185

parametrizations. Rational curve points can be computed when the associated curve has genus zero or one. Real curve points can be represented by the topological graph of the curve. Section 2.2 is devoted to local parametrizations. In particular, rational Puiseux parametrizations are introduced, where the least number of field extensions is necessary for the local description of the algebraic curve. Algorithmically the singular part of the rational Puiseux parametrization is important, which is bounded in Proposition 2.9.

In Section 3 it is shown that every non-constant $\mathbb{L}$-Puiseux series solution defines a place of the associated curve such that its equivalent rational Puiseux parametrization has coefficients in $\mathbb{L}$, which is an effective necessary condition on a place of the curve to contain $\mathbb{L}$-Puiseux series solutions of the original differential equation (see Proposition 3.4 and Corollary 3.5). Sufficient conditions for deciding the existence of $\mathbb{L}$-Puiseux series solutions are given in Theorem 3.7, Theorem 3.8 and, if the curve is of genus zero, in Theorem 3.10. These theorems are new and give an algorithmic procedure for finding $\mathbb{L}$-Puiseux series solutions. Algorithms for computing $\mathbb{L}$-Puiseux series solutions with $\mathbb{L} \in \{\mathbb{R}, \mathbb{Q}\}$ are presented in Section 4 and illustrated by examples.

2 PRELIMINARIES

Let us introduce the type of differential equations treated within this paper. We assume that the coefficients of the equation (1) are rational, so $\mathbb{K} = \mathbb{Q}$, or a number field $\mathbb{K} = \mathbb{Q}(v_1, \ldots, v_m) \subset \mathbb{R}$ where $v_1, \ldots, v_m$ are algebraic numbers. In the latter case, by the primitive element theory (see [24]), we can assume without loss of generality that $m = 1$. Additionally, we assume that F is square-free and has no factor in $\overline{\mathbb{K}}[y]$ or $\overline{\mathbb{K}}[y']$, where $\overline{\mathbb{K}}$ denotes the algebraic closure of $\mathbb{K}$. Let $\mathbb{L}$ be a field extension of $\mathbb{K}$. Associated to the differential equation, we denote by $\mathcal{C}_{\mathbb{L}}(F)$ the algebraic set

$$\mathcal{C}_{\mathbb{L}}(F) = \{(a, b) \in \mathbb{L}_\infty^2 \mid F(a, b) = 0\},$$

where $\mathbb{L}_\infty$ is the one-point compactification of $\mathbb{L}$. Note that for $\mathbb{L} = \mathbb{C}$ we obtain the algebraic curve defined by F and for $\mathbb{L} \subset \mathbb{C}$ the set $\mathcal{C}_{\mathbb{L}}(F)$ could be finite or even empty.

We use the notations $\mathbb{L}[[x]]$ for the ring of formal power series, $\mathbb{L}((x))$ for its fraction field and $\mathbb{L}\langle\langle x \rangle\rangle = \bigcup_{m \geq 1} \mathbb{L}((x^{1/m}))$ for the field of formal Puiseux series (expanded around zero) with coefficients in $\mathbb{L}$. We call the minimal natural number $m \in \mathbb{Z}_{>0}$ such that $y(x)$ belongs to $\mathbb{L}((x^{1/m}))$ the *ramification index* of $y(x)$. Moreover, for non-zero $y(x) = \sum_{j \geq k} a_j \, x^{j/m}$ with $a_{j_0} \neq 0$ we define the *order* of $y(x)$ as j_0/m, denoted by $\mathrm{ord}_x(y(x))$. For $y(x) = 0$ we set $\mathrm{ord}_x(y(x)) = \infty$.

Let us fix $y_0 \in \mathbb{L}_\infty$ and let us seek for $\mathbb{L}$-Puiseux series solutions of (1) with $y(0) = y_0$. Since F is independent of the x-variable, the solutions expanded around zero can be shifted to solutions expanded around any other finite point $x_0 \in \mathbb{L}$. In the case of infinity as expansion point, after the transformation $x = 1/z$ we obtain the (non-autonomous) differential equation $F(y(z), -z^2 y'(z)) = 0$. In order to deal with both cases in a unified way, equations of the type

$$F(y, \epsilon x^h y') = 0, \tag{2}$$

where $h \in \{0, 2\}$, $\epsilon \in \{-1, 1\}$, and its $\mathbb{L}$-Puiseux series solutions expanded around zero are studied. Additionally, if $y(x)$ is a solution of negative order, then $\tilde{y}(x) = 1/y(x)$ is a solution of the numerator of $F(1/y, -x^h y'/y^2) = 0$, which is again of the form (2) and fulfills $\tilde{y}(0) = 0$. Therefore, in the sequel, we assume that $y_0 \in \mathbb{L}$.

A necessary condition on solutions $y(x) \in \mathbb{L}\langle\langle x \rangle\rangle$ of (2) is that $((1-h)x^h y'(x))(0) = p_0$ must fulfill one of the following properties

(1) If $p_0 < \infty$ then $F(y_0, p_0) = 0$;
(2) If $p_0 = \infty$ then the leading coefficient of $F(y, p)$ seen as polynomial in p, denoted by $\mathrm{lc}(F)(y_0)$, is zero.

The condition $p_0 < \infty$ is equivalent to $\mathrm{ord}_x(y(x) - y_0) \geq 1$. The deduction $F(y_0, p_0) = 0$ can be rephrased as $(y_0, p_0) \in \mathcal{C}_{\mathbb{L}(p_0)}(F)$, i.e. (y_0, p_0) is a $\mathbb{L}(p_0)$-rational curve point. This particularly motivates the study of rational and real curve points. In the following, the tuple (y_0, p_0) will be called an *initial tuple* (of $y(x)$ or $F(y, y') = 0$, respectively).

2.1 $\mathbb{L}$-Rational Curve Points

In this section we study the points $\mathcal{C}_{\mathbb{L}}(F)$, called $\mathbb{L}$*-rational curve points*. We focus on $\mathbb{Q}$-rational curve points and $\mathbb{R}$-rational curve points, which are simply called *rational curve points* and *real curve points*, respectively.

We distinguish between two types of curve points $(y_0, p_0) \in \mathcal{C}_{\mathbb{L}}(F)$, namely *critical* and non-critical curve points (see [6]). The first is the finite collection of points obtained precisely in the following way.

- For $p_0 = 0$ find the roots of $F(y, 0) = 0$ in $\mathbb{L}$;
- For $p_0 = \infty$ find the roots of $\mathrm{lc}(F)(y) = 0$ in $\mathbb{L}$;
- The common roots of $F(y, p)$ and its separant $\frac{\partial F}{\partial p}(y, p) = S_F(y, p)$ in $\mathbb{L}^2$.

Curve points with $y_0 = \infty$ correspond to solutions of the differential equation of negative order which are treated separately.

Remark 2.1. *A curve point $(y_0, p_0) \in \mathcal{C}_{\mathbb{L}}(F)$ with $S_F(y_0, p_0) \neq 0$ or $\frac{\partial F}{\partial y}(y_0, p_0) \neq 0$ is called* regular *and non-regular curve points are called* singular. *Singular curve points are critical, in the sense defined above, but critical curve points are not necessarily singular.*

Remark 2.2. *As it is shown in [20, Theorem 5.4], for curves of genus zero, there exists a regular $\mathbb{L}$-rational curve point if and only if there are infinitely many. In particular, $\mathcal{C}_{\mathbb{R}}(F)$ ($\mathcal{C}_{\mathbb{Q}}(F)$) is infinite if and only if there exists a regular real (rational) curve point.*

In the following sections we will give criteria for the existence of infinitely many $\mathbb{L}$-rational curve points when $\mathcal{C}_{\mathbb{C}}(F)$ has positive genus.

Throughout this paper we use a detailed version of Example 15 from [6] to illustrate the notions and results of the current work.

Example 1. *Let us consider*

$$F(y, p) = ((p-1)^2 + y^2)^3 - 4(p-1)^2 y^2 = 0.$$

For $p_0 = 0$ we obtain the curve points $(\alpha, 0)$ with $\alpha^6 + 3\alpha^4 - \alpha^2 + 1 = 0$ which are regular. The common roots of $F(y, p) = 0$ and $S_F(y, p) = 3((p-1)^2 + y^2)^2(2p-2) - 8(p-1)y^2$ are $(0, 1)$, $(\frac{4\beta}{9}, \gamma)$ where $\beta^2 = 3$, and $27\gamma^2 - 54\gamma + 19 = 0$. The only curve point at infinity is (∞, ∞). Thus, the set of critical curve points is given by

$$\mathcal{B} = \{(0, 1), (\alpha, 0), (\frac{4\beta}{9}, \gamma), (\infty, \infty)\}.$$

Rational Curve Points. The solution of equations in rational numbers is the object of diophantine analysis. In the case of one variable, such as $F \in \mathbb{Q}[y,p]$ and $y = y_0 \in \mathbb{Q}$ is given, one can apply the Rational Root Theorem for finding roots $p_0 \in \mathbb{Q}$. In the case where y_0 is not given and F is non-linear, due to the negative answer of Hilbert's tenth problem, it is in general algorithmically impossible to even find one rational curve point. Depending on the genus of the curve, however, all rational curve points can indeed be found (cf. Remark 2.2).

Remark 2.3. *Let us assume that $\mathcal{C}_{\mathbb{C}}(F)$ is a curve of genus zero. Thus, it has a rational parametrization $P(t) \in \mathbb{C}(t)^2$. If the total degree of F is odd, a rational parametrization with only rational coefficients can be found. If F has even total degree there is a birational parametrization $P(t) \in \mathbb{Q}(t)^2$ if and only if $\mathcal{C}_{\mathbb{C}}(F)$ has a rational regular curve point (see [20, Corollary 5.9]). For $P(t) \in \mathbb{Q}(t)^2$, $\mathcal{C}_{\mathbb{Q}}(F) \setminus P(\mathbb{Q})$ is finite and $P(\overline{\mathbb{Q}})$ misses at most one point which is given as the limit point. More details on the surjectivity of P can be found in [19]. The computation of rational parametrizations in an optimal field is algorithmic and presented in [20].*

Remark 2.4. *If $\mathcal{C}_{\mathbb{C}}(F)$ is a smooth curve of genus one and contains a rational point, the curve is called an* elliptic curve*. Elliptic curves are well studied and their rational points form a finitely generated abelian group [23].*

Example. *The algebraic curve $\mathcal{C}_{\mathbb{C}}(F)$ is of genus zero and has the birational parametrization*

$$P(t) = \Big(\frac{8t^2(50400t^4 - 13470t^3 + 1349t^2 - 60t + 1)}{11543176t^6 - 4596840t^5 + 763428t^4 - 67680t^3 + 3378t^2 - 90t + 1}, \frac{8532616t^6 - 3589736t^5 + 628788t^4 - 58688t^3 + 3078t^2 - 86t + 1}{11543176t^6 - 4596840t^5 + 763428t^4 - 67680t^3 + 3378t^2 - 90t + 1}\Big).$$

The rational curve points are $P(\mathbb{Q}) \cup \{p_\infty, (\infty,\infty)\}$ where $p_\infty = \lim_{t\to\infty} P(t) = (\frac{50400}{1442897}, \frac{1066577}{1442897})$.

Topological Graph. The topological graph displays the real curve points $\mathcal{C}_{\mathbb{R}}(F)$ and the real branches of a given curve $\mathcal{C}_{\mathbb{C}}(F)$. In principle, $\mathcal{C}_{\mathbb{R}}(F)$ can either be the empty set, a finite collection of points or an infinite set. If $\mathcal{C}_{\mathbb{R}}(F)$ is finite, its points can be represented by separated boxes with rational endpoints, or a symbolic description can be used. In this case, the real points are singular curve points and can be found by cylindrical algebraic decomposition [1].

If $\mathcal{C}_{\mathbb{R}}(F)$ is infinite, we may speak about a real algebraic curve. The topological graph is commonly used for representing its real branches and singular curve points. There have been many papers addressing the problem of computing the topology of real algebraic plane curves, e.g. [7, 15]. Let us note that most works on this topic assume that the coefficient field is $\mathbb{K} = \mathbb{Q}$, but the reasonings hold for an algebraic extension field $\mathbb{K} = \mathbb{Q}(\nu)$ without problems.

The *topological graph* $\mathcal{G}$ of a real algebraic curve $\mathcal{C}_{\mathbb{R}}(F)$ is a topologically equivalent arrangement of polylines given as a graph such that the edges and vertices fulfill the following.

- The vertices correspond to critical points, isolated points, or ramification points of the curve which are real.
- Every edge corresponds to a real branch of the curve connecting two such curve points.

Here, ramification points are common roots of $F(y,p), S_F(y,p)$ or of $F(y,p), \frac{\partial F}{\partial y}(y,p)$. Differently to most works in the literature, we additionally add the real critical curve points to the vertex set. Adding real curve points to the vertex set does not change the topology. Since the real critical curve points can be found similarly to the singular curve points, the topological graph, as defined here, can still be computed as described in [15, Algorithm 1].

Let us emphasize that the topological graph provides the set of real critical curve points and the number of real curve branches going through a curve point, which is of particular importance for the computation of $\mathbb{R}$-Puiseux series solutions of $F(y,y') = 0$.

Example. *The polynomial $F(y,p)$ defines a real algebraic curve which is represented by the topological graph $\mathcal{G}$ (see Figure 1). The vertices of $\mathcal{G}$ are the real points among the critical curve points $\mathcal{B}$ together with the real solutions of $F(y,p) = 0$, $\frac{\partial F}{\partial y}(y,p) = 0$, namely*

$$\{(0,1), (\frac{4\beta}{9}, \gamma), (\frac{2\sqrt{2}\beta}{9}, \bar{\gamma}), (\infty,\infty)\}$$

where $27\bar{\gamma}^2 - 54\bar{\gamma} + 11 = 0$. The curve point at infinity can be seen as an isolated real curve point.

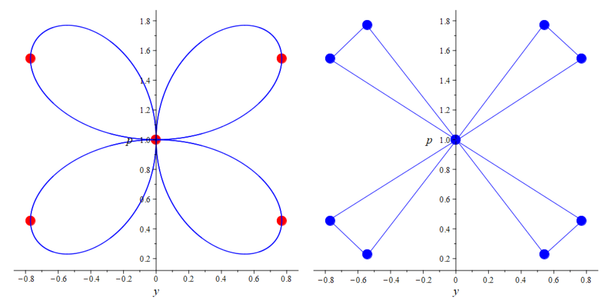

Figure 1: Left: the real part of the curve implicitly defined by $F(y,p)$ with the critical curve points in red; Right: The topological graph $\mathcal{G}$.

Alternatively to the topological graph, since $\mathcal{C}_{\mathbb{C}}(F)$ is of genus zero, the real curve points can be expressed via the rational parametrization as $P(\mathbb{R}) \cup \{p_\infty, (\infty,\infty)\}$.

2.2 Local Parametrizations

In this section we recall some results from [9]. For a more algorithmic point of view we refer to [17]. In Duval's work it is assumed that the given polynomial $F \in \mathbb{K}[y,p]$ is monic (considered as polynomial in p) and absolutely irreducible, i.e. irreducible in $\overline{\mathbb{K}}[y,p]$. As it is just indicated therein, the results similarly hold for square-free F with no factor in $\overline{\mathbb{K}}[y]$ as it is assumed in (1). In Proposition 2.9, we give a proof of the main theorem from [9] for this more general setting.

A *local parametrization* of the curve $\mathcal{C}_{\mathbb{C}}(F)$ is a pair $(a(t), b(t)) \in \mathbb{C}((t))^2 \setminus \mathbb{C}^2$ such that $F(a(t), b(t)) = 0$. The *center* of the parametrization is defined as $(a(0), b(0))$. Two parametrizations $(a_1(t), b_1(t))$, $(a_2(t), b_2(t))$ are *equivalent* if there is some $s(t) \in \mathbb{C}[[t]]$ with $\text{ord}_t(s(t)) = 1$ such that

$$(a_1(s(t)), b_1(s(t))) = (a_2(t), b_2(t)).$$

A local parametrization is said to be *reducible* if it is equivalent to another one in $\mathbb{C}((t^k))^2$ for some $k > 1$. Otherwise, it is called *irreducible*. The equivalence class of an irreducible local parametrization $A(t)$ is called a *place* and denoted by $[A(t)]$. Since equivalent local parametrizations have the same center point we may speak about the center of a place. Additionally, a place *lies above* a point $y_0 \in \mathbb{C}$ if the center of this place is (y_0, p_0) for some $p_0 \in \mathbb{C}_\infty$.

Let $F \in \mathbb{K}[t, p]$ be square-free and $d = \deg_p(F(t, p))$. Due to Puiseux' Theorem, given $y_0 \in \mathbb{K}$, we obtain d-many *Puiseux expansions* $\varphi_1(t), \ldots, \varphi_d(t)$ of F expanded around y_0. The Puiseux expansions are of the form $\varphi(t) = \sum_{j \geq k} c_j (t - y_0)^{j/m}$ with ramification index equal to $m \in \mathbb{Z}_{>0}$ and coefficients $c_j \in \overline{\mathbb{K}}$. *Classical Puiseux parametrizations* are obtained from such a Puiseux expansion $\varphi(t)$ as

$$(y_0 + t^m, \sum_{j \geq k} c_j t^j) \in \mathbb{C}((t))^2.$$

Note that for any equivalent local parametrization $(a(t), b(t))$ the order $\operatorname{ord}_t(a(t) - a(0))$ is equal to the ramification index of φ. Hence, we may speak indistinctly about the ramification index of a local parametrization and of a place.

The Puiseux expansions and its corresponding places can be grouped according to the field extensions they define. Let ζ_{m_i} be a primitive m_i-th root of unity. After the transformation $t = t - y_0$, a monic polynomial $F(t, p)$ can be factored as

$$F = \prod_{i=1}^{\rho} F_i \quad \text{with } F_i \text{ irreducible in } \mathbb{K}[[t]][p]$$

$$F_i = \prod_{j=1}^{f_i} F_{ij} \quad \text{with } F_{ij} \text{ irreducible in } \overline{\mathbb{K}}[[t]][p]$$

$$F_{ij} = \prod_{k=0}^{m_i - 1} (y - \varphi_{ij}(\zeta_{m_i}^k t^{1/m_i})) \quad \text{with } \varphi_{ij} \in \overline{\mathbb{K}}((t))$$

for some $\rho, f_i, m_i \in \mathbb{Z}_{>0}$. The $\varphi_{ijk}(t) = \varphi_{ij}(\zeta_{m_i}^k t^{1/m_i})$ are exactly the Puiseux expansions of F expanded around y_0 and have ramification index m_i. The $\{F_{ij}\}_{1 \leq j \leq f_i}$ have coefficients in a degree f_i extension $\mathbb{L}_i$ of $\mathbb{K}$ and they are conjugated by the action of the Galois group of $\mathbb{L}_i/\mathbb{K}$ (for details on Galois theory see e.g. [8]). We call $\mathbb{L}_i$ the residue field of F_i and f_i its residual degree. It holds that

$$d = \sum_{1 \leq i \leq \rho} m_i f_i. \tag{3}$$

For non-monic $F(t, p)$, the same factorization can be found with an additional factor in F_{ij}.

Definition 2.5. *In the notation from above, a system of* rational Puiseux parametrizations *(over $\mathbb{K}$), lying above $y_0 \in \mathbb{K}$, is a set of non-equivalent irreducible local parametrizations*

$$\{(y_0 + \alpha_i t^{m_i}, b_i(t))\}_{1 \leq i \leq \rho} \subset \mathbb{L}_i((t))^2$$

where $m_i \in \mathbb{Z}_{>0}, \alpha_i \neq 0$.

The criterion that rational Puiseux parametrizations have coefficients in $\mathbb{L}_i$ is usually not fulfilled for classical Puiseux parametrizations where $\alpha_i = 1$. Note that they are in one-to-one correspondence by the reparametrization $s_i(t) = \alpha_i^{-1/m_i} t$.

Remark 2.6. *The field extension $\mathbb{L}_i/\mathbb{K}$ is minimal in the following sense (see [9, Theorem 3 ff.]): For a rational Puiseux parametrization $A(t)$ over $\mathbb{K}$ with residual field $\mathbb{L}_i$ and a local parametrization $B(t) \in [A(t)]$, where $B(t) \in \mathbb{L}_B((t))^2$, it holds that the degree of the field extension $\mathbb{L}_B/\mathbb{K}$ is at least the residual degree f_i.*

Definition 2.7. *The* regularity index *of a Puiseux expansion $\varphi(t) = \sum_{j \geq k} c_j t^{j/m}$ of $F(t, p)$ is defined as the smallest number $R \in \mathbb{Z}_{\geq 0}$, $R \geq m \cdot \operatorname{ord}_t(\varphi(t))$, such that $\varphi(t)$ is the only Puiseux expansion extending the truncation $\tilde{\varphi}(t) = \sum_{j=k}^{R} c_j t^{j/m}$. The truncation $\tilde{\varphi}(t)$ is then called the* singular part *of $\varphi(t)$.*

Correspondingly, the regularity index of a classical Puiseux parametrization $(y_0 + t^m, \varphi(t^m))$ is that of $\varphi(t)$ and its singular part is $(y_0 + t^m, \tilde{\varphi}(t^m))$. The regularity index and singular part of a rational Puiseux parametrization $(y_0 + \alpha t^m, b(t))$ are defined as that of the Puiseux expansion $\varphi(t) = b(\alpha^{-1/m} t^{1/m})$.

The coefficients of a Puiseux expansion $\varphi(t) \in \mathbb{C}\langle\langle t \rangle\rangle$ beyond the singular part $\tilde{\varphi}(t) \in \mathbb{L}(t^{1/m})$ can be computed by the implicit function theorem up to an arbitrary degree [16, Corollaries 5.1, 5.2]. This implies that $\varphi(t) \in \mathbb{L}((t^{1/m}))$. Consequently, the singular part of a classical / rational Puiseux parametrization determines the ramification index and the coefficient field.

Lemma 2.8. *Let $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}\}$. Let $F \in \mathbb{K}[y, p]$ and let $A(t)$ be a rational Puiseux parametrization over $\mathbb{K}$. Then the place $[A(t)]$ contains a local parametrization with coefficients in $\mathbb{K}$ if and only if the coefficients of the singular part of $A(t)$ are in $\mathbb{K}$.*

Proof. Let $\mathbb{L}_A$ be the residual field of $A(t)$ and let $B(t) \in [A(t)]$ be a local parametrization with coefficient field $\mathbb{L}_B = \mathbb{K}$. Since the degree of the field extension $\mathbb{L}_A/\mathbb{K}$ is minimal (see Remark 2.6), it follows that $\mathbb{L}_A = \mathbb{K}$.

The converse direction follows from the fact that $A(t) \in \mathbb{K}((t))^2$ if and only if the singular part of $A(t)$ has coefficients in $\mathbb{K}$. □

Note that a rational Puiseux parametrization $A(t) \in \mathbb{R}((t))^2$ is convergent and gives infinitely many real curve points in a certain neighborhood of zero. In this way, infinitely many real curve points can be found (cf. Remark 2.2).

From an algorithmic point of view, we have to bound the regularity index. This is stated in [9, Lemma 2] for monic polynomials. We generalize this result here.

Proposition 2.9. *Let $F \in \mathbb{K}[t, p]$ be a square-free polynomial. Then the regularity index of every Puiseux expansion of F is bounded by*

$$N = 2(\deg_p(F) - 1) \deg_t(F) \deg_p(F) + 1. \tag{4}$$

Proof. Let $F(t, p) = \sum_{0 \leq i \leq d} a_i(t) p^i$ with $a_d(t) \neq 0$ and $d = \deg_p F$ and $r = \deg_t F$. Let $\nu = \deg_t(a_d)$ and set

$$G(t, z) = t^{\nu(d-1)} F(t, t^{-\nu} z) \in \mathbb{K}[t, z].$$

The leading coefficient of $G(t, z)$, as a polynomial in z, is of order zero and $\deg_p(F) = \deg_z(G)$, $\deg_t(G) \leq \deg_t(F) + \nu(d-1)$. By [9, Lemma 2], we obtain the bound on the regularity index R of Puiseux expansions of $G(t, z)$

$$\begin{aligned} R &\leq 2(\deg_z G - 1) \deg_t G + 1 \\ &\leq 2(\deg_p F - 1)(\deg_t F + \nu(\deg_p F - 1)) + 1 \\ &\leq 2(d-1)rd + 1 = N. \end{aligned}$$

A formal Puiseux series $p(t)$ is a Puiseux expansion of $F(t,p)$ if and only if $z(t) = t^{\nu} p(t)$ is a Puiseux expansion of $G(t,z)$. In particular, $p(t)$ and $z(t)$ have the same regularity index R. Since N is independent of the chosen Puiseux expansion, the statement follows. □

Given $\mathbb{L} \in \{\mathbb{R}, \mathbb{Q}\}$, by Lemma 2.8 and Proposition 2.9, it can be algorithmically checked whether there are local parametrizations lying above a given $y_0 \in \mathbb{K}$ with elements in $\mathbb{L}((t))^2$. Moreover, this also determines the real curve branches lying above y_0 in an alternative way to that introduced for the topological graph.

Example. *For $F(t,p)$ and $y_0 = 0$ we obtain the Puiseux expansions*

$$\varphi_1(t) = 1 - \frac{t^2}{2} - \frac{3t^4}{16} + O(t^6), \varphi_2(t) = 1 + \frac{t^2}{2} + \frac{3t^4}{16} + O(t^6) \in \mathbb{Q}[[t]],$$

$$\varphi_3(t) = 1 + \sqrt{2}i\zeta t^{1/2} + \frac{3\sqrt{2}i\zeta t^{3/2}}{8} + O(t^{5/2}) \in \mathbb{Q}(\sqrt{2}i)[[t^{1/2}]],$$

$$\varphi_4(t) = 1 + \sqrt{2}\zeta t^{1/2} - \frac{3\sqrt{2}\zeta t^{3/2}}{8} + O(t^{5/2}) \in \mathbb{Q}(\sqrt{2})[[t^{1/2}]]$$

where $\zeta \in \{-1,1\}$. This leads to the system of rational Puiseux parametrizations

$$\{(t,\varphi_1(t)),(t,\varphi_2(t)),$$
$$(-2t^2,\varphi_3(-2t^2)) = (-2t^2, 1 - 2t + \frac{3t^3}{2} + O(t^5)),$$
$$(2t^2,\varphi_4(2t^2)) = (2t^2, 1 + 2t - \frac{3t^3}{2} + O(t^5))\} \subset \mathbb{Q}((t))^2.$$

The regularity index of φ_1, φ_2 is two and that of φ_3, φ_4 is one.

3 $\mathbb{L}$-PUISEUX SERIES SOLUTIONS

In this section we use the results from Section 2.1 in order to find $\mathbb{L}$-Puiseux series solutions, that are Puiseux series solutions with coefficients in $\mathbb{L}$, of a given differential equation (1). We focus on the cases where $\mathbb{L} = \mathbb{R}$ and $\mathbb{L} = \mathbb{Q}$.

First we show that it is sufficient to consider differential equations with coefficients in $\mathbb{K}$ in order to find Puiseux series solutions with real coefficients such that our assumptions for (1) are legit.

Lemma 3.1. *Let $F \in \mathbb{C}[y,p]$ be square-free and $y(x) \in \mathbb{R}\langle\langle x\rangle\rangle$ be a non-constant solution of $F(y,y') = 0$. Then F has a factor in $\mathbb{R}[y,p]$.*

Proof. From [6, Theorem 11] we know that $y(x) \in \mathbb{R}\langle\langle x\rangle\rangle$ is convergent in a certain neighborhood U. Hence, there are infinitely many real simple points of $\mathcal{C}_{\mathbb{C}}(F)$ given by $(y(x^n), y'(x^n))$ with $x \in U \cap \mathbb{R}$, where n is the ramification index of $y(x)$. Then, from [20, Lemma 7.3] it follows that F has a real factor. □

Lemma 3.2. *Let $F \in \mathbb{Q}(v)[y,p]$ be square-free with $v \in \mathbb{C}$ algebraic over $\mathbb{Q}$ and let $y(x) \in \mathbb{Q}\langle\langle x\rangle\rangle$ be a non-constant solution of $F(y,y') = 0$. Then F has a factor in $\mathbb{Q}[y,p]$.*

Proof. Similar as in the proof of Lemma 3.1, there are infinitely many simple points in $\mathcal{C}_{\mathbb{Q}}(F)$. Let v be an algebraic number of degree $r+1$. Then, F can be expressed as $F = F_0 + v F_1 + \cdots + v^r F_r$ where $F_i \in \mathbb{Q}[y,p]$. Since F vanishes at infinitely many rational points, $F_0, \ldots, F_r$ vanish also at infinitely many points. Therefore, their greatest common divisor is non-constant and a factor of F in $\mathbb{Q}[y,p]$. □

A necessary condition on an $\mathbb{L}$-Puiseux series solution of $F(y,y') = 0$, as we have already seen in Section 2, is that the initial tuple (y_0,p_0) is an $\mathbb{L}$-rational curve point.

Remark 3.3. *If $(y_0,p_0) \in \mathcal{C}_{\mathbb{L}}(F)$ is a non-critical curve point, by a version of the implicit function theorem [10], there is a (non-constant) formal power series solution $y(x)$ of $F(y,y') = 0$ with coefficients in $\mathbb{L}$. In fact, by [6, Theorem 10], there is no other Puiseux series solution with initial tuple (y_0,p_0).*

In the following we will focus on solutions with initial tuples corresponding to critical curve points. As a side-result we additionally show that the solution at a non-critical curve point is unique. For this purpose we use the approach from [6]. Let $h \in \{0,2\}$. The case $h = 0$ corresponds to Puiseux series solutions expanded around zero and $h = 2$ corresponds to solutions expanded around infinity. Let us recall that a non-constant solution $y(x) \in \mathbb{C}\langle\langle x\rangle\rangle$ with ramification index n defines an irreducible local parametrization $A(t) = (y(t^n), (1-h)t^{hn}y'(t^n)) \in \mathbb{C}((t))^2$, called a *solution parametrization* (corresponding to $y(x)$). The place $[A(t)]$ is then called *solution place*.

A necessary condition on a place $[(a(t),b(t))]$ to be a solution place is that

$$n(1-h) = \mathrm{ord}_t(a(t) - a_0) - \mathrm{ord}_t(b(t)). \tag{5}$$

holds for some $n \in \mathbb{Z}_{>0}$ and $h \in \{0,2\}$. In the affirmative case we call the place $[(a(t),b(t))]$ *order-suitable* (with n and h). For a given order-suitable place $[(a(t),b(t))]$, we have to analyze the reparametrizations given as the solutions of the *associated differential equation*

$$a'(s(t))s'(t) = (1-h)nt^{n(1-h)-1}b(s(t)) \tag{6}$$

for $s(t) \in \mathbb{C}[[t]]$ with $\mathrm{ord}_t(s(t)) = 1$. For $h = 0$ there are exactly n solution parametrizations in a solution place as [6, Theorem 10] shows. For $h = 2$ the associated differential equation (6) has either no solution or a family of solutions $s(t) = \sum_{i\geq 1} \sigma_i t^i \in \mathbb{C}[[t]]$ involving a free parameter σ_n. In both cases all $\mathbb{C}$-Puiseux series solutions can be found.

By restricting the coefficients of the local parametrization and the reparametrization to $\mathbb{L}$, we obtain the following result.

Proposition 3.4. *Let $F \in \mathbb{K}[y,y']$ be a square-free polynomial as in (1), let $(a(t),b(t)) \in \mathbb{L}((t))^2$ be an irreducible local parametrization, order-suitable with $n \in \mathbb{Z}_{>0}$ and $h \in \{0,2\}$, and let $s(t) \in \mathbb{L}[[t]]$ be a solution of the associated differential equation. Then $a(s(x^{(1-h)/n})) \in \mathbb{L}\langle\langle x\rangle\rangle$ is a solution of the differential equation $F(y,y') = 0$.*

Proof. By [6, Proposition 3], since $(a(t),b(t))$ is order-suitable and $s(t)$ is a solution of the associated differential equation, $y(x) = a(s(x^{(1-h)/n}))$ is indeed a solution of $F(y,y') = 0$ and the coefficients of $y(x)$ are in $\mathbb{L}$. □

As a consequence of Proposition 3.4 together with Lemma 2.8 we obtain the following necessary condition on the existence of $\mathbb{L}$-Puiseux series solutions given just in terms of algebraic geometry.

Corollary 3.5. *Let $\mathbb{L} \in \{\mathbb{R}, \mathbb{Q}\}$. Let $y(x) \in \mathbb{L}\langle\langle x\rangle\rangle$ be a non-constant solution of* (1). *Then the solution place corresponding to*

$y(x)$ is represented by a rational Puiseux parametrization such that the coefficients of the singular part are in $\mathbb{L}$.

Based on Proposition 3.4 we can now find $\mathbb{L}$-Puiseux series solutions. An effective method for checking whether the reparametrization $s(t)$ has coefficients in $\mathbb{L}$ is given as follows.

REMARK 3.6. *Let $(a(t) = y_0 + t^k \cdot \sum_{i\geq 0} a_i t^i, b(t) = t^r \cdot \sum_{i\geq 0} b_i t^i) \in \mathbb{L}((t))^2$ be an order-suitable local parametrization with $n = \frac{k-r}{1-h} > 0$ and $a_0 b_0 \neq 0$. The coefficients of the solutions of the associated differential equation $s(t) = \sum_{i\geq 1} \sigma_i t^i$ have the following dependencies. The first coefficient fulfills*

$$a_0\, \sigma_1^{n(1-h)} - (1-h)n\, b_0 = 0.$$

For $h = 0$ and a fixed σ_1, the coefficients σ_i, $i \geq 2$, are uniquely determined and depend on $\sigma_1, a_0, \ldots, a_{i-1}, b_0, \ldots, b_{i-1}$ such that $s(t) \in \mathbb{L}(\sigma_1)[[t]]$. Hence, $s(t) \in \mathbb{L}[[t]]$ if and only if $\sigma_1 \in \mathbb{L}$. For solutions expanded around infinity ($h = 2$), if there exists a solution $s(t)$, it additionally has a free parameter σ_n. By choosing $\sigma_n \in \mathbb{L}$, $s(t)$ has coefficients in $\mathbb{L}$ if and only if $\sigma_1 \in \mathbb{L}$.

Let $\mathbb{L} = \mathbb{R}$. If n is odd, there is always a possible choice for σ_1 in $\mathbb{R}$. If n is even, there are two possible choices if $(1-h)a_0 b_0 > 0$ and no real σ_1 if $(1-h)a_0 b_0 < 0$. For $\mathbb{L} = \mathbb{Q}$ the fraction $\frac{(1-h)n\, b_0}{a_0}$, after canceling out possible common factors, additionally must have squares as numerator and denominator.

Let us note that due to the bound on the field extension f of a rational Puiseux parametrization (see equation (3)) and Remark 3.6, all coefficients of a $\mathbb{C}$-Puiseux series solution of (1) are algebraic over $\mathbb{Q}$ with bounded degree $f + n$.

An open question is whether Proposition 3.4 also gives a sufficient condition. More concretely, for a given order-suitable local parametrization $(a(t), b(t)) \in \mathbb{L}((t))^2$, is there a solution $s(t) \in \mathbb{C}[[t]] \setminus \mathbb{L}[[t]]$ of the associated differential equation such that $(a(s(t)), b(s(t)))$ has coefficients in $\mathbb{L}$? In almost all cases the answer is negative as the following theorems show.

For this purpose, let us define the *order of a place $\mathcal{A}$* centered at a finite point (y_0, p_0) as $\min(\{\mathrm{ord}_t(a(t)), \mathrm{ord}_t(b(t))\})$ where $(y_0 + a(t), p_0 + b(t)) \in \mathcal{A}$ is an arbitrary local parametrization. Note that the order of a place is indeed independent of the representative. Similarly as formula 3, the sum of the orders of places centered at (y_0, p_0) is equal to the multiplicity of $\mathcal{C}_{\mathbb{C}}(F)$ at (y_0, p_0). For more details see [22, page 108ff.].

THEOREM 3.7. *Let $F \in \mathbb{K}[y, y']$ be as in (1), let $\mathbb{L} \in \{\mathbb{R}, \mathbb{Q}\}$ and let $\mathcal{A}$ be an order-suitable place centered at $(y_0, p_0) \in \mathcal{C}_{\mathbb{L}}(F)$ such that one of the following conditions hold*

1. *(y_0, p_0) is finite and the order of $\mathcal{A}$ is one;*
2. *$\mathcal{A}$ is order-suitable with $n = 1$.*

Then there is an $\mathbb{L}$-Puiseux series solution $y(x)$ corresponding to $\mathcal{A}$ if and only if the singular part of the rational Puiseux parametrization $(a(t), b(t)) \in \mathcal{A}$ has coefficients in $\mathbb{L}$, the associated differential equation is solvable and the first coefficient of a solution is in $\mathbb{L}$.

PROOF. Assume that $y(x) = a(s(x^{1/n}))$ is an $\mathbb{L}$-Puiseux series solution. Let $(a(t), b(t)) \in \mathcal{A}$ be a rational Puiseux parametrization. Then there exists a solution $s(t) = \sum_{i\geq 1} \sigma_i t^i \in \mathbb{C}[[t]]$ of (6) such that $y(x) = a(s(x^{1/n}))$. In both cases the components of $(a(t), b(t))$ have non-negative order and, by Corollary 3.5, its coefficients are in $\mathbb{L}$. Due to Lemma 2.8, the latter is the case if and only if its singular part has coefficients in $\mathbb{L}$.
Let us assume that item (1) holds and $\mathrm{ord}_t(a'(t)) = 0$ or $\mathrm{ord}_t(b'(t)) = 0$. If $a'(0) \neq 0$, since $a(t)$ is convergent in a certain neighborhood and due to the inverse function theorem, there exists (locally) an analytic inverse $a^{-1}(t) \in \mathbb{L}[[t]]$ and $s(t) = a^{-1}(y(t^n))$. Since the right hand side has coefficients in $\mathbb{L}$, also $s(t) \in \mathbb{L}[[t]]$. If $b'(0) \neq 0$, by a similar argument, $s(t) = b^{-1}(y'(t^n)) \in \mathbb{L}[[t]]$. In both cases, by Remark 3.6, this is the case if and only if $\sigma_1 \in \mathbb{L}$ and, if $h = 2$, we can additionally choose $\sigma_n \in \mathbb{L}$.
Let us assume that item (2) holds. By Remark 3.6, σ_1 is uniquely determined and in $\mathbb{L}$.

For the reverse implication, by Lemma 2.8, $(a(t), b(t)) \in \mathbb{L}((t))^2$ and, by Remark 3.6, there is a solution $s(t) \in \mathbb{L}[[t]]$ of (6). Then the statement follows from Proposition 3.4. □

THEOREM 3.8. *Let $F \in \mathbb{R}[y, y']$ be as in (1) and let $\mathcal{A}$ be a real order-suitable place with odd $n > 0$, centered at $(y_0, p_0) \in \mathcal{C}_{\mathbb{R}}(F)$. Then there is a non-constant $\mathbb{R}$-Puiseux series solution $y(x)$ of $F(y, y') = 0$.*

PROOF. By Lemma 2.8, there exists a real rational Puiseux parametrization $A(t) = (a(t), b(t)) \in \mathcal{A}$. Since $\mathcal{A}$ is order-suitable, there exists a solution $s(t) = \sum_{i\geq 1} \sigma_i t^i$ of (6) and by Remark 3.6, there is at least one solution with $\sigma_1 \in \mathbb{R}$. Then the statement follows by Theorem 3.7. □

Note that the assumptions in Theorem 3.8 are always fulfilled for regular curve points with $n = 1$. Hence, it generalizes Remark 3.3.

REMARK 3.9. *When finding rational curve points, the case where $\mathcal{C}_{\mathbb{C}}(F)$ is of genus zero is special (see Section 2.1). There exists a birational parametrization $P(t) = (P_1(t), P_2(t))$ with coefficients in an optimal field $\mathbb{L}$ [20]. Let $(y_0, p_0) = P(t_0) \in \mathcal{C}_{\mathbb{L}}(F)$ for some $t_0 \in \mathbb{L}$. Then a local parametrizations centered at a curve point (y_0, p_0) can be found by expanding $P_1(t - t_0), P_2(t - t_0)$ around 0. Assume that its coefficients are in $\mathbb{L} \in \{\mathbb{R}, \mathbb{Q}\}$. Then, by Lemma 2.8, the rational Puiseux parametrizations centered at (y_0, p_0) also has coefficients in $\mathbb{L}$ and the above reasonings hold for $P(t)$ as well, where computations might simplify. We illustrate this in Section 4 by the ongoing example.*

Let us note that, when $\mathcal{C}_{\mathbb{C}}(F)$ is of genus zero, the associated differential equation (6) with $n = 1, h = 0$ is studied in [13] for computing closed-form solutions of $F(y, y') = 0$. The case of rational solutions is covered by [11, 12].

If the given algebraic curve has genus zero, another sufficient condition on verifying the existence of $\mathbb{L}$-Puiseux series solutions than that in Theorem 3.7 can be shown.

THEOREM 3.10. *Let $F \in \mathbb{K}[y, y']$ be as in (1), let $\mathbb{L} \in \{\mathbb{R}, \mathbb{Q}\}$ and let $P(t) = (P_1(t), P_2(t)) \in \mathbb{L}(t)^2$ be a birational parametrization of $\mathcal{C}_{\mathbb{C}}(F)$ with $P(t_0) = (y_0, p_0) \in \mathcal{C}_{\mathbb{L}}(F)$ for some $t_0 \in \mathbb{L}$ and $P(t - t_0)$ is order-suitable. Then there exists a corresponding $\mathbb{L}$-Puiseux series solution of $F(y, y') = 0$ with initial tuple (y_0, p_0) if and only if the associated differential equation (6) is solvable and the first coefficient of a solution is in $\mathbb{L}$.*

PROOF. Assume that $y(x) = a(s(x^{1/n}))$ is an $\mathbb{L}$-Puiseux series solution. Then there exists a solution $s(t) = \sum_{i\geq 1} \sigma_i t^i \in \mathbb{C}[[t]]$

of (6) such that $y(x) = P_1(s(x^{1/n}) - t_0)$. Following the construction of the inverse in [20, Theorem 4.37], it directly follows that the inverse rational parametrization $Q(y, p)$ of $P(t)$ has coefficients in $\mathbb{L}$. Since $P(s(t) - t_0) = (y(t^n), t^{hn}y'(t^n))$, we obtain

$$s(t) = Q(y(t^n), t^{hn}y'(t^n)) + t_0 \in \mathbb{L}[[t]].$$

By Remark 3.6, this is the case if and only if $\sigma_1 \in \mathbb{L}$ and, if $h = 2$, we can additionally choose $\sigma_n \in \mathbb{L}$. The reverse implication follows as in Theorem 3.7. □

4 ALGORITHMS AND EXAMPLES

In this section we outline an algorithm that is derived from the results in the previous sections. We describe an algorithmic method that computes, for a given initial value $y_0 \in \mathbb{K}$, Puiseux series solutions of the differential equation (1) with coefficients in $\mathbb{L} \in \{\mathbb{R}, \mathbb{Q}\}$. For each Puiseux series solution we will provide a solution truncation that can be extended uniquely to an $\mathbb{L}$-Puiseux series solution. The solution truncations are Puiseux polynomials, i.e. elements in $\mathbb{L}[x^{1/n}][x^{-1}]$, where n is the ramification index of the corresponding Puiseux series solution.

The current work is partly implemented in the Maple package `FirstOrderSolve` [3]. The package is available at the online repository https://risc.jku.at/sw/firstordersolve/. Although it is not explicitly mentioned within the documentation, the package already uses rational Puiseux parametrizations because, empirically, computations with rational Puiseux expansions are more efficient than that with classical Puiseux expansions.

Algorithm 1 InitialValueSolve

Input: A first-order AODE $F(y, y') = 0$, where $F \in \mathbb{K}[y, p]$ is square-free with no factor in $\overline{\mathbb{K}}[y]$ or $\overline{\mathbb{K}}[p]$ and an initial tuple $(y(0), y'(0)) = (y_0, p_0) \in C_{\mathbb{L}}(F)$ for a number field $\mathbb{K}$ and $\mathbb{L} \in \{\mathbb{R}, \mathbb{Q}\}$.

Output: A set consisting of $\mathbb{L}$-Puiseux series solutions of $F(y, y') = 0$ fulfilling $(y(0), y'(0)) = (y_0, p_0)$ which are represented by Puiseux polynomials such that there is a one-to-one correspondence between the truncations and the series.

1: If $y_0 = \infty$, apply the following steps to the numerator of $F(1/y, -p/y^2)$.
2: Compute a system of rational Puiseux parametrizations $\mathcal{A}$ centered at (y_0, p_0).
3: For every rational Puiseux parametrization $A(t) = (a(t), b(t)) \in \mathcal{A}$, check whether $A(t)$ is order-suitable (with $n \in \mathbb{Z}_{>0}$, $h \in \{0, 2\}$) and the singular part of $A(t)$ has coefficients in $\mathbb{L}$.
4: In the affirmative case, compute the solution set $\mathcal{S}$ of the associated differential equation (6).
5: Discard the $s(t) \in \mathcal{S}$ where the first coefficient is not in $\mathbb{L}$.
6: Output $a(s(x^{(1-h)/n}))$.

Let us give some remarks on Algorithm 1:

- In every step we compute only the first terms of the series until the singular part is surpassed. A bound for this is given by (4).
- The initial values (y_0, p_0) are algebraic and may be given by their minimal polynomials. Then the further computation is done symbolically. In particular, the coefficients of $A(t)$ may be expressed in terms of y_0, p_0 and the check whether it has real coefficients is performed by cylindrical algebraic decomposition [1].
- There are either no, one or two elements $s(t)$ in $\mathcal{S}$, possibly depending on a free parameter, with coefficients in $\mathbb{L}$ (see Remark 3.6).
- If (y_0, p_0) fulfills the assumptions of Theorem 3.7 or Theorem 3.10, then all $\mathbb{L}$-Puiseux series solutions with initial tuple (y_0, p_0) are found.
- The assumption that $(y_0, p_0) \in C_{\mathbb{L}}(F)$ could be neglected, because if (y_0, p_0) is not a curve point there is no local parametrization centered at it and if y_0 or p_0 is not in $\mathbb{L}_\infty$, the rational Puiseux paramerizations does not have coefficients in $\mathbb{L}$.

Algorithm 2 RealPuiseuxSolve

Input: A first-order AODE $F(y, y') = 0$, where $F \in \mathbb{K}[y, p]$ is square-free with no factor in $\overline{\mathbb{K}}[y]$ or $\overline{\mathbb{K}}[p]$.

Output: A set consisting of $\mathbb{R}$-Puiseux series solutions of $F(y, y') = 0$ (expanded around zero and infinity) represented by their solution truncations: The generic solution by $y_0 + p_0 x$ and the topological graph $\mathcal{G}$ of $C_{\mathbb{R}}(F)$ describing the real curve points (y_0, p_0); and some particular solutions not covered by the generic solution represented as Puiseux polynomials.

1: If $(\infty, \infty) \in C_{\mathbb{R}}(F)$, then perform the transformation $\tilde{y} = 1/y$ and apply Algorithm 1 to the numerator of $F(1/y, -p/y^2)$ and $(y_0, p_0) = (0, 0)$.
2: If $C_{\mathbb{R}}(F)$ is infinite, compute its topological graph $\mathcal{G}$. Otherwise there is no generic real solution.
3: For every critical curve point $(y_0, p_0) \in C_{\mathbb{R}}(F)$, apply Algorithm 1 with $\mathbb{L} = \mathbb{R}$.

If a description of all rational curve points $C_{\mathbb{Q}}(F)$ is given, e.g. by a rational parametrization $P(t) \in \mathbb{Q}(t)^2$, one can find all $\mathbb{Q}$-Puiseux series solutions of $F(y, y') = 0$ similarly as in Algorithm 2.

Example. *Let us illustrate Algorithms 2 and 1 by the concurrent example*

$$F = ((y' - 1)^2 + y^2)^3 - 4(y' - 1)^2 y^2 = 0.$$

The generic solution of $F(y, y') = 0$ is given by $y(x; y_0) = y_0 + p_0 x + O(x^2)$ with $(y_0, p_0) \in C_{\mathbb{R}}(F) \setminus \mathcal{B}$. The set $C_{\mathbb{R}}(F) \setminus \mathcal{B}$ is given by the topological graph $\mathcal{G}$, displayed in Figure 1.

Let us now analyze the real critical curve points in $\mathcal{B}$. In the system of rational Puiseux parametrizations at $(0, 1)$,

$$\{(t, \varphi_1(t)), (t, \varphi_2(t)), (-2t^2, \varphi_3(-2t^2)), (2t^2, \varphi_4(2t^2))\},$$

the first two local parametrizations are order-suitable with $n = 1$ and the latter are order-suitable with $n = 2$. The associated differential equation (6) corresponding to $(2t^2, \varphi_4(2t^2)) \in \mathbb{Q}((t))^2$ has the solutions

$$s_1(t) = \frac{t}{\sqrt{2}} + \frac{t^2}{3} + \frac{\sqrt{2}t^3}{36} - \frac{89t^4}{1080} + O(t^5),$$
$$s_2(t) = \frac{-t}{\sqrt{2}} + \frac{t^2}{3} - \frac{\sqrt{2}t^3}{36} - \frac{89t^4}{1080} + O(t^5)$$

with first coefficients in $\mathbb{Q}(\sqrt{2})$. Therefore,

$$2(s_1(x^{1/2})^2) = x + \tfrac{2\sqrt{2}\,x^{3/2}}{3} + \tfrac{x^2}{3} + O(x^{5/2}),$$
$$2(s_2(x^{1/2})^2) = x - \tfrac{2\sqrt{2}\,x^{3/2}}{3} + \tfrac{x^2}{3} + O(x^{5/2})$$

are $\mathbb{Q}(\sqrt{2})$-Puiseux series solutions of $F(y,y')=0$. Similarly we can find the two $\mathbb{C}$-Puiseux series solutions corresponding to $(-2t^2, \varphi_3(-2t^2))$,

$$x + \tfrac{2\sqrt{2}ix^{3/2}}{3} - \tfrac{x^2}{3} + O(x^{5/2}),\ x - \tfrac{2\sqrt{2}ix^{3/2}}{3} - \tfrac{x^2}{3} + O(x^{5/2}),$$

and the two formal power series solutions with rational coefficients

$$x + \tfrac{x^3}{6} + \tfrac{17x^5}{240} + O(x^6),\ x - \tfrac{x^3}{6} + \tfrac{17x^5}{240} + O(x^6)$$

corresponding to $(t, \varphi_2(t))$ and $(t, \varphi_1(t))$, respectively. Note that in [6, Example 15] we obtained the same solution set, but when using classical Puiseux parametrizations it is in general unclear which of the solutions will be real as it can be seen with the initial tuple $(\frac{4\beta}{9}, \gamma) \in \mathcal{C}_{\mathbb{R}}(F)$. The rational Puiseux parametrizations are

$$(\tfrac{4\beta}{9} + \tfrac{1}{\beta}\, t^2, \gamma - \tfrac{1}{\beta}\, t + O(t^3)).$$

whereas the classical Puiseux parametrizations are purely complex. The solutions of the associated differential equation are

$$s(t) = \pm\sqrt{-\gamma\,\beta}\, t + O(t^2)$$

which are real if and only if $(\beta,\gamma) \in \{(-\sqrt{3}, 1+\frac{2\sqrt{6}}{9}), (-\sqrt{3}, 1-\frac{2\sqrt{6}}{9})\}$. Thus, we obtain four $\mathbb{R}$-Puiseux series solutions with initial value $(\frac{4\beta}{9}, \gamma)$ given by

$$\tfrac{4\beta}{9} + \gamma x \pm \tfrac{2\sqrt{-\gamma\,\beta}}{3\sqrt{3}} x^{3/2} + \left(\tfrac{5\gamma}{32} - \tfrac{143}{864}\right)\beta x^2 + O(x^{5/2}).$$

Finally, there is no solution corresponding to the curve point (∞,∞).

Let us note that all curve points of $\mathcal{C}_{\mathbb{C}}(F)$ are fulfilling the assumptions of Theorem 3.7. Hence, we have indeed found all $\mathbb{R}$-Puiseux series solutions of $F(y,y')=0$.

Let us now demonstrate that these solutions can also be found by using $P(t)$ (see Remark 3.9). The curve point $(0,1)$ is obtained for $t_0 \in \{0, \frac{1}{14}, \frac{1}{15}, \frac{1}{16}\}$. Since $P(t) \in \mathbb{Q}(t)^2$ has $(0,1)$ four times in its image, we could have directly concluded that the rational Puiseux parametrizations of $\mathcal{C}_{\mathbb{C}}(F)$ centered at $(0,1)$ have rational coefficients. Moreover, for $t_0 = 0$, the Taylor expansion is

$$P(t) = (8t^2 + O(t^3), 1 + 4t + O(t^2)).$$

The associated differential can be written in closed-form as

$$P_1'(s(t))\, s'(t) = 2t\, P_2(s(t))$$

and has the solutions $\bar{s}(t) = \pm\frac{1}{2\sqrt{2}} + O(t^2)$. Then,

$$P_1(\bar{s}(x^{1/2})) = x \pm \frac{2\sqrt{2}\,x^{3/2}}{3} + \frac{x^2}{3} + O(x^{5/2})$$

are the $\mathbb{R}$-Puiseux series solutions corresponding to this place.

Since $\mathcal{C}_{\mathbb{Q}}(F)$ is given by $P(\mathbb{Q}) \cup p_\infty$, we can use Algorithm 2 for finding the $\mathbb{Q}$-Puiseux series solutions of $F(y,y')=0$. The generic solution is $y(x;y_0) = y_0 + p_0 x + O(x^2)$ for $(y_0,p_0) \in \mathcal{C}_{\mathbb{Q}}(F) \setminus \mathcal{B}$. By Theorem 3.10, the generic solution and $x \pm \frac{x^3}{6} + O(x^5)$ represent all $\mathbb{Q}$-Puiseux series solutions of $F(y,y')=0$.

Example 2. *Let us consider $F(y,y') = y' + y^3y'^2 + y^2 - 1$ and the critical curve point $(\infty,\infty) \in \mathcal{C}_{\mathbb{C}}(F)$ as initial tuple. The numerator of $F(1/y, -p/y^2)$ is $G(y,p) = p^2 + y^5 - py^5 - y^7$ and has the rational Puiseux parametrization*

$$(a(t), b(t)) = (-t^2, -t^5 + \frac{t^9}{2} + O(t^{10}))$$

centered at $(0,0)$, which is order-suitable with $n=3, h=2$. The associated differential equation $2s'(t) = 3t^{-4}\cdot(-s(t)^4 + \frac{s(t)^8}{2} + O(t^9))$ has the solution

$$s(t) = \frac{s_1 t}{3} + s_4\, t^4 + \frac{s_1^2 t^5}{27} + O(t^6),$$

where $s_4 \in \mathbb{R}$ is a free parameter and $s_1^3 = 2/3$. Then, for $s_1 = \sqrt[3]{2/3}$, we obtain the $\mathbb{R}$-Puiseux series solution (expanded around infinity)

$$(a(s(x^{-1/3})))^{-1} = \frac{-\sqrt[3]{18}\,x^{2/3}}{2} + 3s_4\, x^{-1/3} - \frac{\sqrt[3]{18}^2\, x^{-2/3}}{9} - \frac{x^{-1}}{3} + O(x^{-4/3})$$

of $F(y,y')=0$.

ACKNOWLEDGMENTS

The author would like to thank Rafael Sendra, José Cano and Jose Capco for useful discussions. The author was partially supported by the OeAD project FR 09/2022 and the grant PID2020-113192GB-I00 (Mathematical Visualization: Foundations, Algorithms and Applications) from the Spanish MICINN.

REFERENCES

[1] D.S. Arnon, G.E. Collins, and S. McCallum. 1984. Cylindrical algebraic decomposition I: The basic algorithm. *SIAM J. Comput.* 13, 4 (1984), 865–877.

[2] J.M. Aroca, J. Cano, R. Feng, and X.-S. Gao. 2005. Algebraic General Solutions of Algebraic Ordinary Differential Equations. In *Proceedings of the 2005 international symposium on Symbolic and algebraic computation.* ACM, 29–36.

[3] F. Boulier, J. Cano, S. Falkensteiner, and J.R. Sendra. 2020. Puiseux Series and Algebraic Solutions of First Order Autonomous AODEs–A MAPLE Package. In *Maple Conference.* Springer, 89–103.

[4] A.D. Bruno. 2000. *Power Geometry in Algebraic and Differential Equations.* Elsevier.

[5] J. Cano. 1993. An extension of the Newton-Puiseux polygon construction to give solutions of Pfaffian forms. *Ann. Inst. Fourier (Grenoble)* 43, 1 (1993), 125–142.

[6] Jose Cano, Sebastian Falkensteiner, and J Rafael Sendra. 2022. Existence and convergence of Puiseux series solutions for autonomous first order differential equations. *Journal of Symbolic Computation* 108 (2022), 137–151.

[7] J. Cheng, S. Lazard, L. Peñaranda, M. Pouget, F. Rouillier, and E. Tsigaridas. 2010. On the topology of real algebraic plane curves. *Mathematics in Computer Science* 4, 1 (2010), 113–137.

[8] P.M. Cohn. 2003. *Basic Algebra: Groups, Rings and Fields.* Springer-Verlag London.

[9] D. Duval. 1989. Rational Puiseux Expansion. *Compositio Mathematica* 70, 2 (1989), 119–154.

[10] S. Falkensteiner, Y. Zhang, and N. Thieu Vo. 2022. On Formal Power Series Solutions of Algebraic Ordinary Differential Equations. *Mediterranean Journal of Mathematics* 19, 17 (2022).

[11] R. Feng and X.-S. Gao. 2004. Rational General Solutions of Algebraic Ordinary Differential Equations. In *Proceedings of the 2004 international symposium on Symbolic and algebraic computation.* ACM, 155–162.

[12] R. Feng and X.-S. Gao. 2006. A polynomial time Algorithm for finding rational general solutions of first order autonomous ODEs. *Journal of Symbolic Computation* 41, 7 (2006), 739–762.

[13] G. Grasegger and F. Winkler. 2015. Symbolic Solutions of First-Order Algebraic ODEs. In *Computer algebra and polynomials (Lecture Notes in Computer Science, Vol. 8942)*, J. Gutierrez, J. Schicho, and M. Weimann (Eds.). Springer International Publishing, 94–104. http://dx.doi.org/10.1007/978-3-319-15081-9_5

[14] D.Y. Grigoriev and M. Singer. 1991. Solving Ordinary Differential Equations in Terms of Series with Real Exponents. *Trans. Amer. Math. Soc.* 327, 1 (1991), 329–351.

[15] H. Hong. 1996. An efficient method for analyzing the topology of plane real algebraic curves. *Mathematics and Computers in Simulation* 42, 4-6 (1996), 571–582.

[16] H.T. Kung and J.F. Traub. 1978. All algebraic functions can be computed fast. *Journal of the ACM (JACM)* 25, 2 (1978), 245–260.

[17] A. Poteaux and M. Weimann. 2021. Computing Puiseux series: a fast divide and conquer algorithm. *Annales Henri Lebesgue* 4 (2021), 1061–1102.

[18] W.M. Seiler. 2009. *Involution.* Springer.

[19] J.R. Sendra. 2002. Normal parametrizations of algebraic plane curves. *Journal of Symbolic Computation* 33, 6 (2002), 863–885.

[20] J.R. Sendra, F. Winkler, and S. Pérez-Díaz. 2008. *Rational Algebraic Curves.* Vol. 22. Springer.

[21] J. van der Hoeven. 2006. *Transseries and Real Differential Algebra.* Vol. 1888. Springer.

[22] R.J. Walker. 1950. *Algebraic Curves.* Princeton University Press.

[23] L.C. Washington. 2008. *Elliptic Curves, Number Theory and Cryptography.* Taylor & Francis Group.

[24] F. Winkler. 2012. *Polynomial Algorithms in Computer Algebra.* Springer Science & Business Media.