

# JOURNAL de Théorie des Nombres de BORDEAUX

*anciennement Séminaire de Théorie des Nombres de Bordeaux*

Huy DANG, Soumyadip DAS, Kostas KARAGIANNIS, Andrew OBUS  
et Vaidehee THATTE

**Local Oort groups and the isolated differential data criterion**

Tome 34, n° 1 (2022), p. 251-269.

<https://doi.org/10.5802/jtnb.1200>

© Les auteurs, 2022.

 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/>

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux »  
(<http://jtnb.centre-mersenne.org/>) implique l'accord avec les conditions générales  
d'utilisation (<http://jtnb.centre-mersenne.org/legal/>).



*Le Journal de Théorie des Nombres de Bordeaux est membre du  
Centre Mersenne pour l'édition scientifique ouverte  
<http://www.centre-mersenne.org/>*

# Local Oort groups and the isolated differential data criterion

par HUY DANG, SOUMYADIP DAS, KOSTAS KARAGIANNIS,  
ANDREW OBUS et VAIDEHEE THATTE

RÉSUMÉ. Il est conjecturé que si  $k$  est un corps algébriquement clos de caractéristique  $p > 0$ , alors tout  $G$ -revêtement ramifié de courbes projectives lisses sur  $k$  pour lequel l’obstruction « KGB » s’annule et tel qu’un  $p$ -sous-groupe de Sylow de  $G$  est cyclique peut être relevé en caractéristique 0. Obus a démontré que cette conjecture est vraie si l’on suppose l’existence de certaines formes différentielles méromorphes sur  $\mathbb{P}_k^1$  dont les propriétés sont déterminées par la filtration de ramification du revêtement. Nous présentons ici un algorithme plus efficace pour calculer ces formes. En conséquence, nous pouvons prouver que tous les  $D_{25}$ -revêtements et tous les  $D_{27}$ -revêtements se relèvent en caractéristique zéro.

ABSTRACT. It is conjectured that if  $k$  is an algebraically closed field of characteristic  $p > 0$ , then any branched  $G$ -cover of smooth projective  $k$ -curves where the “KGB” obstruction vanishes and where a  $p$ -Sylow subgroup of  $G$  is cyclic lifts to characteristic 0. Obus has shown that this conjecture holds given the existence of certain meromorphic differential forms on  $\mathbb{P}_k^1$  with behavior determined by the ramification data of the cover. We give a more efficient procedure to compute these forms than was previously known. As a consequence, we show that all  $D_{25}$ -covers and  $D_{27}$ -covers lift to characteristic zero.

## 1. Introduction

This paper concerns the *local lifting problem*, which is stated as follows:

**Problem 1.1** (The local lifting problem). *Let  $k$  be an algebraically closed field of characteristic  $p$  and  $G$  a finite group. Let  $k[[z]]/k[[t]]$  be a  $G$ -Galois extension (that is,  $G$  acts on  $k[[z]]$  by  $k$ -automorphisms with fixed ring  $k[[t]]$ ). Does this extension lift to characteristic zero? That is, does there exist a DVR  $R$  of characteristic zero with residue field  $k$  and a  $G$ -Galois extension  $R[[Z]]/R[[S]]$  that reduces to  $k[[z]]/k[[s]]$ ?*

---

Manuscrit reçu le 22 septembre 2020, accepté le 5 juin 2021.

2010 *Mathematics Subject Classification.* 14H37, 12F10, 13B05.

*Mots-clefs.* local lifting problem, local Oort group, differential data, Vandermonde determinant.

The fourth author was supported by the National Science Foundation under Grant Numbers DMS-1641020 and DMS-1900396, as well as by a PSC-CUNY Award, jointly funded by The Professional Staff Congress and The City University of New York.

Let us give some brief context (for more details, see the expositions [14, 17]). The local lifting problem is motivated by the *global lifting problem*, which asks whether a characteristic  $p$  curve with a finite group of automorphisms (or, equivalently, a Galois branched cover of curves) lifts to characteristic zero. In fact, solving the global lifting problem is equivalent to solving the local lifting problem for each extension coming from the complete local ring of a ramification point on the cover. For tame covers, this reduces to the local lifting problem when  $G$  is cyclic and prime to  $p$ , which is more or less trivial by the Kummer theory, and gives an alternate proof of one of the main results of SGA1 ([11, XIII, Corollaire 2.1]). For more on this *local-global principle*, see [17, Section 3], or see the papers [9, 10, 2] for the original proofs.

We will refer to a  $G$ -Galois extension  $k[[z]]/k[[t]]$  for  $k$  an algebraically closed field of characteristic  $p$  as a *local  $G$ -extension*. Basic ramification theory shows that any group  $G$  that occurs as the Galois group of a local extension is of the form  $P \times \mathbb{Z}/m$ , with  $P$  a  $p$ -group and  $p \nmid m$ . In [7], Chinburg, Guralnick, and Harbater ask, given a prime  $p$ , for which groups  $G$  (of the form  $P \times \mathbb{Z}/m$ ) is it true that all local  $G$ -actions (over all algebraically closed fields of characteristic  $p$ ) lift to characteristic zero? Such a group is called a *local Oort group* (for  $p$ ). Due to various obstructions (The *Bertin obstruction* of [1], the *KGB obstruction* of [7], and the *Hurwitz tree obstruction* of [5]), the list of possible local Oort groups is quite limited. In particular, the following proposition is a consequence of [7, Theorem 1.2] and [5].

**Proposition 1.2.** *If a group  $G$  is a local Oort group for  $p$ , then  $G$  is either cyclic, dihedral of order  $2p^n$ , or the alternating group  $A_4$  (with  $p = 2$ ).*

Cyclic groups are known to be local Oort (this is the so-called *Oort conjecture*, proven by Obus–Wewers and Pop in [19, 21]). Obus proved that  $A_4$  is local Oort in [15] (this was also independently known to Pop and Bouw). This leaves the case of dihedral groups.

Dihedral groups of order  $2p$  are known to be local Oort for  $p$  odd due to Bouw–Wewers ([3]) and for  $p = 2$  due to Pagot ([20]). The group  $D_9$  is local Oort by [16], and the group  $D_4$  is local Oort by [24]. No other dihedral groups are known to be local Oort. Our main theorem is:

**Theorem 1.3.** *The groups  $D_{25}$  and  $D_{27}$  are local Oort.*

In fact, the paper [16] states a more general conjecture for groups with cyclic  $p$ -Sylow subgroup. The conjecture below is a combination of Conjecture 1.9, Proposition 1.6, and Remark 1.7 of [16].

**Conjecture 1.4.** *Let  $G \cong \mathbb{Z}/p^n \rtimes \mathbb{Z}/m$  be non-abelian with  $p \nmid m$ , and let  $k[[z]]/k[[t]]$  be a local  $G$ -extension whose  $\mathbb{Z}/p^n$ -subextension has ramification*

jumps  $(u_1, \dots, u_n)$  for the upper numbering ([23, IV]) that are congruent to  $-1 \pmod{m}$ . Then  $k[[z]]/k[[t]]$  lifts to characteristic zero.

*Remark 1.5.* By [16, Remark 1.7] (see also [18, Remark 1.10]), for a local  $G$ -extension to satisfy the hypotheses of Conjecture 1.4, it is necessary that  $G$  be center-free. That is, the conjugation action of  $\mathbb{Z}/m$  on  $\mathbb{Z}/p^n$  is faithful.

*Remark 1.6.* If the congruence condition of Conjecture 1.4 is *not* satisfied, then it is known that the local  $G$ -extension does *not* lift to characteristic zero (see [16, Proposition 1.6]).

*Remark 1.7.* If  $m = 2$  (so that  $G$  is dihedral), then the  $u_i$  are *always* odd, so Conjecture 1.4 asserts that  $D_{p^n}$  is local Oort for odd  $p$  as a special case.

In [16], Conjecture 1.4 was reduced to showing that the so-called *isolated differential data criterion* holds in sufficiently many cases. Saving the details for Section 2, we say now that this criterion is about finding a meromorphic differential form on  $\mathbb{P}_k^1$  with prescribed poles that transforms in a particular way under the Cartier operator, and which is “isolated” in the sense that small deformations of the differential form do not satisfy these criteria. In fact, constructing the differential form can be reduced to constructing a certain polynomial  $f \in k[x]$ , and the isolatedness criterion is stated in terms of the invertibility of a Vandermonde-like determinant arising from the roots of  $f$ . One of the key intermediate results of this paper is Corollary 4.7, which rewrites this criterion in terms of the *coefficients* of  $f$ . This allows us to write an algorithm to verify the *existence* of a satisfactory  $f$  entirely in terms of Gröbner bases (even if we cannot write the solution explicitly). In particular, this existence criterion is necessary for us to prove that  $D_{27}$  is local Oort.

**1.1. Outline of the paper.** In Section 2 we discuss the isolated differential data criterion and its relation to the local lifting problem for dihedral groups, introduced in [16]. The criterion is defined in two steps: in Definition 2.1 we state the differential data criterion, which is about the existence of a meromorphic differential form on  $\mathbb{P}_k^1$  with pre-specified behavior under the Cartier operator, while the notion of isolatedness is made specific in Definition 2.3. The main result of this section is Proposition 2.4 which essentially reduces the local lifting problem to verifying that the isolated differential data criterion holds for finitely many cases.

The meromorphic differential form of Definition 2.1 is uniquely determined by a polynomial  $f \in k[t]$ . In the two subsequent sections, we reformulate each of the two conditions that make up the isolated differential data criterion so as to be expressed in terms of the vanishing or non-vanishing of certain polynomials in the coefficients of  $f$ . In particular, Section 3 deals with the differential data criterion, ignoring the isolatedness conditions. Its

main result is Proposition 3.1, which says that the differential data criterion is equivalent to a system of equations in the coefficients of  $f$ , which involve multinomials obtained by the expansion of the polynomial  $f^{p-1}$ .

In Section 4 we discuss the isolatedness condition and translate it to a condition in terms of the coefficients of  $f$  rather than its roots. Our result makes use of Heineman’s work on generalized Vandermonde matrices and their determinants. The main result of this section is Corollary 4.7 in which we prove that the isolatedness condition is equivalent to the invertibility of a matrix whose entries are uniquely determined by the coefficients of  $f$ .

The main results of the two previous sections are combined in Section 5 in two different manners: Remark 5.1 describes an approach which requires first solving the system of Proposition 3.1 then checking whether the respective matrix defined in Corollary 4.7 is invertible. The difficulty of explicitly solving the system of Proposition 3.1 motivates the existence criterion of Proposition 5.2, the main result of this section, in which we prove that the isolated differential data criterion holds if and only if an ideal uniquely determined by the equations of Proposition 3.1 and Corollary 4.7 is not the unit ideal.

Finally, in Section 6 we use our results to prove that  $D_{25}$  and  $D_{27}$  are local Oort groups. In fact, the small size of the input data allows us to explicitly realize the isolated differential data criterion as in Remark 5.1 for all  $D_{25}$  cases and all but two  $D_{27}$  cases. In these two cases, we must rely on the existence criterion of Proposition 5.2.

**Acknowledgements.** This project was conceived at the AMS Mathematics Research Community “Explicit methods in Arithmetic Geometry in Characteristic  $p$ ” in June 2019, and we thank the AMS and the organizers of that workshop. In particular, we thank Drew Sutherland and Sachi Hashimoto for fruitful conversations during the workshop. The second author would like to thank Indian Statistical Institute for partial travel support for the aforementioned workshop. Additionally, we thank the anonymous referee for their comments and insightful remarks, and Christelle Vincent, for translating the abstract into French.

## 2. The isolated differential data criterion

In this section, we briefly review the notion of the isolated differential data criterion following [16, Section 1.4]. Let  $p$  be a prime number and  $k$  be an algebraically closed field of characteristic  $p$ . We start by recalling the definition of the *Cartier operator*  $\mathcal{C}$ , introduced by Cartier in [6]. This  $p$ -linear operator, acting on meromorphic differentials forms  $\Omega_{k(t)/k}^1$ , is defined as follows. Any  $\omega \in \Omega_{k(t)/k}^1$  can be written as  $\omega = (f_0^p + f_1^p t + \cdots + f_{p-1}^p t^{p-1}) dt$

for some  $f_i \in k(t)$ . Then

$$\begin{aligned}\mathcal{C} : \Omega_{k(t)/k}^1 &\longrightarrow \Omega_{k(t)/k}^1, \\ \omega &\longmapsto f_{p-1} dt.\end{aligned}$$

For any  $f \in k(t)$  and  $\omega \in \Omega_{k(t)/k}^1$ , the operator  $\mathcal{C}$  satisfies the following.

$$(2.1) \quad \mathcal{C}(f^p \omega) = f \mathcal{C}(\omega);$$

$$(2.2) \quad \mathcal{C}(\omega_1 + \omega_2) = \mathcal{C}(\omega_1) + \mathcal{C}(\omega_2);$$

$$(2.3) \quad \mathcal{C}(df) = 0;$$

$$(2.4) \quad \mathcal{C}(df/f) = df/f;$$

$$(2.5) \quad \mathcal{C}(f^{p-1} df) = df;.$$

We note that  $\mathcal{C}$  extends to an operator on any completion of  $k(t)$  with the same properties. For more details on the above definition and the properties, the reader may refer to [13, Section A.4].

**Definition 2.1.** *Let  $p$  be a prime number and  $k$  be an algebraically closed field of characteristic  $p$ . Let  $m > 1$  be an integer dividing  $p-1$ , and  $\tilde{u}$  be a positive integer such that  $\tilde{u} \equiv -1 \pmod{m}$ . Let  $N \in \{\tilde{u}(p-1), \tilde{u}(p-1)-m\}$ . Define  $u$  by  $\tilde{u} = up^\nu$ ,  $p \nmid u$ . We say that the differential data criterion is satisfied for the quadruple  $(p, m, \tilde{u}, N)$  (with respect to the field  $k$ ) if there exists a polynomial  $f(t) \in k[t^m]$  of degree  $N$  such that the meromorphic differential form  $\omega := \frac{dt}{f(t)t^{\tilde{u}+1}} \in \Omega_{k(t)/k}^1$  satisfies*

$$(2.6) \quad \mathcal{C}(\omega) = \omega + ut^{-\tilde{u}-1} dt,$$

where  $\mathcal{C}$  is the Cartier operator on  $\Omega_{k(t)/k}^1$ .

If the differential data criterion is realized by a meromorphic differential form  $\omega$  (or equivalently, for an element  $f(t) \in k[t^m]$ ), we will say that  $\omega$  (or  $f(t)$ ) is a *solution* to the differential data criterion for  $(p, m, \tilde{u}, N)$ .

**Lemma 2.2.** *If  $f(t)$  is a solution to the differential data criterion for  $(p, m, \tilde{u}, N)$ , then  $f(t)$  is separable and is not divisible by  $t$ .*

*Proof.* If  $\alpha$  is a root of  $f(t)$ , then by Equation (2.6), the order of the pole of  $\mathcal{C}(\omega)$  at  $t = \alpha$  is the same as that of  $\omega$ . From the basic properties of the Cartier operator on the completion  $k((t-\alpha))$  of  $k(t)$  (see Equations (2.1)–(2.5)), the order of this pole is 1. Since  $\tilde{u} \geq 1$ , this is a contradiction for  $\alpha = 0$ . If  $\alpha \neq 0$ , this shows that  $\alpha$  has multiplicity one as a root of  $f(t)$ .  $\square$

From Equations (2.1)–(2.5) it follows that if  $\omega$  is a solution to the differential data criterion for the quadruple  $(p, m, \tilde{u}, N)$ , then  $\omega$  must be of the form

$$(2.7) \quad \omega = dg/g - u \sum_{i=0}^{\nu} t^{-up^i-1} dt$$

for some rational function  $g \in k(t)$ . Since  $g$  appears only in the term  $dg/g$ , it is well defined up to multiplication by  $p^{\text{th}}$  powers. Also note that  $\omega$  has a zero of order  $N + \tilde{u} - 1$  at  $t = \infty$ .

**Definition 2.3.** *Let  $p, m, \tilde{u}, N$  be as in Definition 2.1. Let  $\omega$  be a solution to the differential data criterion for  $(p, m, \tilde{u}, N)$  where  $\omega = dg/g - u \sum_{i=0}^{\nu} t^{-up^i-1} dt$  (cf. Equation (2.7)). We say that the isolated differential data criterion holds for  $(p, m, \tilde{u}, N)$  if no infinitesimal deformation<sup>1</sup>  $\tilde{g}$  of  $g$  gives rise to a differential form  $\tilde{\omega} = d\tilde{g}/\tilde{g} - u \sum_{i=0}^{\nu} t^{-up^i-1} dt$  having a zero of order at least  $N + \tilde{u} - 1$  at  $t = \infty$ .*

Let  $f(t)$  be a solution to the differential data criterion for  $(p, m, \tilde{u}, N)$  and write  $x_1, \dots, x_{N/m}$  for a set of representatives, one from each distinct  $\mu_m$ -orbit of roots of  $f(t)$ . By [16, Definition 7.23, Remark 7.24], the solution  $f(t)$  is isolated if the Vandermonde-like matrix  $(x_j^{q-1})_{q \in S, 1 \leq j \leq N/m}$  is invertible, where  $S$  is the set

$$S := \{1 \leq q \leq N + \tilde{u} - 1 \mid q \equiv -1 \pmod{m}, p \nmid q\}.$$

Now let  $p$  be an odd prime, and  $G \cong \mathbb{Z}/p^n \rtimes \mathbb{Z}/m$  be non-abelian with  $p \nmid m$ . When  $n = 1$ , it was shown in [3, 4] that Conjecture 1.4 holds. For the rest of this paper we assume  $n \geq 2$ . By [16, Remark 1.16], Conjecture 1.4 is reduced to showing that the isolated differential data criterion holds for certain finitely many quadruples  $(p, m, \tilde{u}, N)$ . Using the same argument, the following result shows that it is sufficient to check even fewer quadruples.

**Proposition 2.4.** *Let  $p$  be an odd prime, and  $m$  be a positive integer dividing  $p - 1$ . Let  $n \geq 2$ . Suppose that for each  $m - 1 \leq \tilde{u} \leq (p^{n-2} + \dots + 1)(mp - 1)$  with  $p^{n-1} \nmid \tilde{u}$  and  $\tilde{u} \equiv -1 \pmod{m}$ , the isolated differential data criterion holds for the quadruples  $(p, m, \tilde{u}, (p-1)\tilde{u})$  and  $(p, m, \tilde{u}, (p-1)\tilde{u} - m)$ . Then Conjecture 1.4 holds for all non-abelian groups  $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$ .*

*Proof.* By Remark 1.5, Conjecture 1.4 is vacuous unless  $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$  is center-free. So we may assume this is true. In particular,  $m|(p - 1)$ . By [16, Proposition 1.11], it suffices to prove Conjecture 1.4 for  $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$ -extensions whose  $\mathbb{Z}/p^n$ -subextension has upper ramification breaks  $(u_1, \dots, u_n)$  with  $u_1 < mp$  and  $pu_{i-1} \leq u_i < pu_{i-1} + mp$  for all  $1 < i \leq n$ . By [22, Lemma 19], we note that  $p^{n-1} \nmid u_i$  for any  $1 \leq i < n$ . Let  $L/k[\![s]\!]$  be such an extension. Set  $u_0 = 0$ . By [16, Proposition 1.14], if for each  $1 < i \leq n$ , both  $u_i \equiv -1 \pmod{m}$  and  $pu_{i-1} \leq u_i \leq pu_{i-1} + mp - 1$ , and

---

<sup>1</sup>An “infinitesimal deformation” of  $g$  here refers to replacing each zero/pole  $\bar{x}_j \in k$  of  $g$  with  $\bar{x}_j + \epsilon c_j \in k[\epsilon]/\epsilon^2$ , see [16, Eq. 7.16]. The set of zeros and poles of  $g$  in [16, Eq. 7.16] is the same as the set of zeros of  $f$ , so by Lemma 2.2, all calculations can be done inside the ring  $(k[\epsilon]/\epsilon^2)[\![t^{-1}]\!]$ .

also the isolated differential data criterion holds for  $(p, m, u_{i-1}, N)$  where

$$N = \begin{cases} (p-1)u_{i-1}, & \text{if } u_i = pu_{i-1} \text{ and} \\ (p-1)u_{i-1} - m, & \text{otherwise,} \end{cases}$$

then the extension  $L/k[\![s]\!]$  lifts to characteristic 0. This inductive criterion on  $u_i$  means  $u_1 \leq mp-1$  and for  $i \geq 2$ , we have  $u_{i-1} \leq (p^{i-2} + \dots + 1) \times (mp-1)$ . By our hypotheses, these conditions are satisfied and the extension  $L/k[\![s]\!]$  lifts.  $\square$

*Remark 2.5.* Note that the upper bound on  $\tilde{u}$  in Proposition 2.4 is stronger than the bound  $\tilde{u} \leq m(p^{n-1} + \dots + p)$  listed in [16, Remark 1.16].

In the next sections, we reduce the isolated differential data criterion for each quadruple into an equivalent statement about the existence of solutions to a system of multivariate polynomial equations, which is much easier to implement computationally.

### 3. The multinomial coefficient approach

Throughout this section, let  $p$  be an odd prime and  $k$  be an algebraically closed field of characteristic  $p$ . Let  $(p, m, \tilde{u}, N)$  be a quadruple satisfying the condition of Definition 2.1. Our first result shows that the differential data criterion can be formulated in terms of the existence of a solution to a system of polynomial equations with coefficients in  $k$ , hence can be studied using computational techniques. For any polynomial  $f(t) \in k[t^m]$  of degree  $N$  with  $m|N$ , we write

$$(3.1) \quad f = f(t) = \sum_{i=0}^{N/m} a_{mi} t^{mi} \in k[t^m].$$

**Proposition 3.1.** *A polynomial  $f(t) = \sum_{i=0}^{N/m} a_{mi} t^{mi}$  is a solution to the differential data criterion for  $(p, m, \tilde{u}, N)$  if and only if the coefficients  $a_{mi}$  satisfy the following system of equations for  $0 \leq i \leq N/m$ .*

$$(3.2) \quad \begin{cases} a_0 = -u^{-1} \\ u a_{mi}^p = c_{pmi-\tilde{u}(p-1)}, & \text{for } \lceil \tilde{u} - \tilde{u}/p \rceil \leq mi \leq N \\ a_{mi} = 0, & \text{otherwise} \\ a_N \neq 0, & \end{cases}$$

where for  $0 \leq j \leq (p-1)N/m$ , the  $c_{mj}$ 's are given by

$$(3.3) \quad c_{mj} = \sum_{\substack{(s_0, \dots, s_{N/m}) \in \mathbb{N}^{N/m+1} \\ s_0 + s_1 + \dots + s_{N/m} = p-1 \\ ms_1 + 2ms_2 + \dots + Ns_{N/m} = mj}} \binom{p-1}{s_0, \dots, s_{N/m}} \prod_{i=0}^{N/m} a_{mi}^{s_i} \in k[\{a_{mi}\}_{0 \leq i \leq N/m}].$$

*Proof.* Note that the coefficient of  $t^{mj}$  in the expansion of the  $(p-1)$ -th power of  $f(t)$  is  $c_{mj}$  given by Equation (3.3) and so,

$$f^{p-1} = \sum_{j=0}^{(p-1)N/m} c_{mj} t^{mj} \in k[t^m].$$

By Definition 2.1,  $(p, m, \tilde{u}, N)$  satisfies the differential data criterion if and only if there exists a polynomial  $f \in k[t^m]$  such that

$$\mathcal{C} \left( \frac{1}{t^{\tilde{u}+1} f} dt \right) = \frac{1+uf}{t^{\tilde{u}+1} f} dt.$$

This is equivalent to

$$\mathcal{C} \left( t^{(p-1)(\tilde{u}+1)} f^{p-1} dt \right) = (1+uf) dt.$$

Substituting the explicit forms of  $f$  and  $f^{p-1}$ , we have

$$\mathcal{C} \left( \sum_{j=0}^{(p-1)N/m} c_{mj} t^{mj+\tilde{u}(p-1)} t^{p-1} dt \right) = \left( 1 + u \sum_{i=0}^{N/m} a_{mi} t^{mi} \right) dt.$$

From Equations (2.1) and (2.5), we have that  $\mathcal{C}$  is an additive map that sends any differential form  $g^p t^{p-1} dt$  to  $g dt$ , and which kills any term  $ct^b dt$  where  $b \not\equiv -1 \pmod{p}$ . So the above equation is equivalent to

$$\sum_{\substack{0 \leq j \leq (p-1)N/m \\ p|(mj+\tilde{u}(p-1))}} c_{mj} t^{mj+\tilde{u}(p-1)} = \left( 1 + u \sum_{i=0}^{N/m} a_{mi} t^{mi} \right)^p = 1 + u \sum_{i=0}^{N/m} a_{mi}^p t^{pmi}.$$

Since the least exponent of the left hand side is  $\tilde{u}(p-1)$ , we obtain  $1+ua_0^p = 0$  and  $a_{mi} = 0$  when  $pmi < \tilde{u}(p-1)$  or equivalently, when  $mi < \tilde{u} - \tilde{u}/p$ . For  $mi \geq \lceil \tilde{u} - \tilde{u}/p \rceil$  we get  $ua_{mi}^p = c_{mj}$  exactly when  $mj + \tilde{u}(p-1) = pmi$ , i.e.  $ua_{mi}^p = c_{pmi-\tilde{u}(p-1)}$ . The result follows.  $\square$

*Remark 3.2.* Note that each of the  $c_{pmi-\tilde{u}(p-1)}$  is a homogeneous polynomial of degree  $p-1$  in the variables  $a_0, a_{\lceil \tilde{u} - \tilde{u}/p \rceil}, \dots, a_N$ .

*Example 3.3.* By Proposition 3.1, the quadruple  $(3, 2, 5, 10)$  satisfies the differential data criterion if there exists a polynomial  $f(t) = a_0 + a_2 t^2 + a_4 t^4 + a_6 t^6 + a_8 t^8 + a_{10} t^{10}$  whose coefficients satisfy the following system of polynomial equations

$$\begin{cases} a_0 = -5^{-1} = 1, \\ 5a_6^3 = -a_8, \\ 5a_8^3 = -a_6 a_8, \\ 5a_{10}^3 = a_{10}^2, \\ a_2 = a_4 = 0, \\ a_{10} \neq 0. \end{cases}$$

By a direct computation, one can show that the only solutions to this system are  $f(t) = 2t^{10} + 1$  and  $f(t) = 2t^{10} + t^8 + t^6 + 1$ .

#### 4. Test for isolatedness

In this section, the notation  $(g(i, j))_{i,j}$  means the matrix whose  $ij^{\text{th}}$  entry is  $g(i, j)$ . Suppose  $f(t)$  is a solution to the differential data criterion for a quadruple  $(p, m, u, N)$ . As in Equation (3.1), write  $f(t) = \sum_{i=0}^{N/m} a_{mi} t^{mi}$ . By Lemma 2.2,  $f$  is separable and does not have 0 as a root. So let  $x_1, \dots, x_{N/m}$  be a list consisting of one representative from each  $\mu_m$ -orbit of the roots of  $f(t)$ . As was mentioned in Section 2,  $f$  realizes the isolated differential data criterion if and only if the matrix

$$M := (x_j^{q-1})_{q,j}$$

is invertible, where  $1 \leq j \leq N/m$  and the  $q$  ranges over all numbers from 1 to  $N + \tilde{u} - 1$  that are congruent to  $-1 \pmod{m}$  and are not divisible by  $p$ . In fact, since  $\tilde{u} \equiv -1 \pmod{m}$  and  $m \mid N$ , the largest value of  $q$  is  $N + \tilde{u} - m$ . This matrix is always square ([16, Remark 7.20]), and  $x_{i_1}/x_{i_2} \notin \mu_m$  whenever  $i_1 \neq i_2$ .

In Corollary 4.7 below, we give a criterion for the isolatedness in terms of the *coefficients* of  $f$ , rather than its roots. Indeed, one simply needs to check that a matrix made from coefficients of  $f$  is invertible. Since this criterion does not require computing roots of polynomials, it is computationally easier to verify.

The starting point is a classical formula of Heineman ([12]) computing generalized Vandermonde determinants, where a *generalized Vandermonde matrix* is a square matrix of the form  $(z_j^{b_i})_{i,j}$  where the  $b_j$  are integers, but are not necessarily equal to  $i - 1$ . The *principal Vandermonde* associated to a generalized Vandermonde matrix is the determinant of the matrix given by  $(z_j^{i-1})_{i,j}$ , i.e., the standard Vandermonde determinant associated to the entries  $z_1, \dots, z_j$ .

Since none of the  $x_j$  is zero, we can form a new matrix  $M'$  by dividing the  $j^{\text{th}}$  column of  $M$  by  $x_j^{m-1}$ , and  $M'$  is invertible if and only if  $M$  is. Now, if we let  $y_j = x_j^m$ ,  $M'$  can be expressed as follows:

$$(4.1) \quad M' = (y_j^r)_{r,j},$$

where  $1 \leq j \leq N/m$  as before and the  $r$  range from 0 to  $(N + \tilde{u} - 2m + 1)/m$ , skipping all values of  $r$  such that  $p \mid (mr + m - 1)$ . Since the  $x_j$  lie in different  $\mu_m$ -orbits, the  $y_j$  are pairwise distinct. Thus  $M'$  is a generalized Vandermonde matrix whose corresponding “principal Vandermonde” (in the language of [12]) is nonzero. So it suffices to give a criterion for when the quotient of  $\det(M')$  by this principal Vandermonde is 0.

**Lemma 4.1.** *Let  $r_1, \dots, r_{N/m}$  be the values of  $r$  in the matrix  $M'$  from (4.1) in ascending order. Let  $\epsilon$  be such that  $N = (p-1)\tilde{u} - \epsilon m$  (so  $\epsilon \in \{0, 1\}$ ).*

- (i) *We have  $r_{N/m} - N/m + 1 = (\tilde{u} - m + 1)/m$ .*
- (ii) *There are exactly  $p-1-\epsilon$  values of  $i$  such that  $r_i - i + 1 = (\tilde{u} + m - 1)/m$ .*

*Proof.* For (i), it suffices to show that  $r_{N/m} = (N + \tilde{u} - 2m + 1)/m$ . By the construction of  $M'$ , we need to only show that  $p \nmid (N + \tilde{u} - m)$ . Since  $N + \tilde{u} = p\tilde{u} - \epsilon m$ , one needs only to show that  $p$  does not divide  $(\epsilon + 1)m$ . This holds because  $p \nmid m$  and  $p > 2 \geq \epsilon + 1$ .

To prove (ii), note that (i) implies  $mr_{N/m} + m - 1 = N + \tilde{u} - m = p\tilde{u} - (1 + \epsilon)m$ , so the largest value of  $r$  less than  $r_{N/m}$  such that  $p \mid (mr + m - 1)$  is that for which  $mr + m - 1 = p\tilde{u} - pm$ . So  $r_i - i + 1 = (\tilde{u} - m + 1)/m$  exactly when  $mr_i + m - 1 \geq p\tilde{u} - (p-1)m$ . Since  $N = (p-1)\tilde{u} - \epsilon m$ , this is exactly when  $r_i \geq (N + \tilde{u} - (p-\epsilon)m + 1)/m$ . By (i),  $r_{N/m} - (N + \tilde{u} - (p-\epsilon)m + 1)/m = p - 2 - \epsilon$ . We have proven the second assertion.  $\square$

*Remark 4.2.* Note that, for each element  $j$  of  $\{1, 2, \dots, (\tilde{u} - m + 1)/m - 1\}$ , there are exactly  $p-1$  values of  $i$  such that  $r_i - (i-1) = j$ . Intuitively, we have  $r_i - (i-1) = 0$  for  $i = 1, 2, \dots$  until we “jump” over an  $r$  such that  $p \mid (mr + m - 1)$ . Then  $r_i - (i-1) = 1$  for the next  $p-1$  values of  $i$ , until we jump over another such  $r$ . Then  $r_i - (i-1) = 2$  for the next  $p-1$  values of  $i$ , etc. By Lemma 4.1, the largest value of  $r_i - (i-1)$  occurs only  $p-1-\epsilon$  times, as opposed to  $p-1$  times.

Echoing the notation of [12], we write  $V_i$  for the determinant of the matrix obtained by writing  $(N/m + 1) \times N/m$  matrix

$$(y_j^r)_{r,j}$$

with  $j$  ranging from 1 to  $N/m$  and  $r$  ranging from 0 to  $N/m$ , and then removing the  $(N/m - i)$ th row. Note that  $V_0$  is the principal Vandermondean, and is thus non-zero. We have the following proposition.

**Proposition 4.3** ([12, Theorem I]). *For all  $i$ , the ratio  $V_i/V_0$  equals the  $i^{\text{th}}$  elementary symmetric function in the  $y_j$ .*

In particular, since the  $y_j$  are the roots of the polynomial  $\sum_{i=0}^{N/m} a_{mi}t^{mi}$ , we can write

$$(4.2) \quad V_i = (-1)^i a_{N-mi}/a_N.$$

Following [12], for all  $\ell, n \in \mathbb{N}$ , define  $D_\ell^n$  to be the  $\ell \times \ell$  matrix given by the upper-left hand corner of the infinite matrix below:

$$\left( \begin{array}{ccccccc} V_1 & V_2 & V_3 & \cdots & V_n & 0 & 0 & \cdots & \cdots & \cdots \\ V_0 & V_1 & V_2 & \cdots & \cdots & V_n & 0 & 0 & \cdots & \cdots \\ 0 & V_0 & V_1 & \cdots & \cdots & \cdots & V_n & 0 & 0 & \cdots \\ 0 & 0 & V_0 & V_1 & \cdots & \cdots & \cdots & V_n & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \cdots & \cdots & \cdots \end{array} \right)$$

For a sequence of non-negative integers  $l \geq t_1 \geq t_2 \geq \cdots \geq t_s$ , we define

$$D_\ell^n\{t_1, t_2, \dots, t_s\}$$

to be the  $\ell \times \ell$  matrix formed as follows:

- (1) Start with  $D_\ell^n$ .
- (2) Increase the subscripts of the  $V_i$  in rows 1 through  $t_s$  by  $s$ , in rows  $t_s + 1$  through  $t_{s-1}$  by  $s - 1$ , in rows  $t_{s-1} + 1$  through  $t_{s-2}$  by  $s - 2$ , etc.

Here  $V_i$  is defined to be 0 whenever  $i > n$ , and a zero that precedes a  $V_0$  should be replaced by  $V_0$  whenever the subscripts in its row are increased by 1 (effectively, each increase by 1 “moves the row to the left”).

*Example 4.4.* The matrix  $D_4^{18}\{4, 4, 4, 3, 3, 3, 2, 2, 2, 2, 1, 1, 1, 1\}$  is equal to

$$\left( \begin{array}{cccc} V_{16} & V_{17} & V_{18} & 0 \\ V_{11} & V_{12} & V_{13} & V_{14} \\ V_6 & V_7 & V_8 & V_9 \\ V_1 & V_2 & V_3 & V_4 \end{array} \right).$$

We write  $|n_1, n_2, \dots, n_\ell|$  for the determinant of the generalized Vandermonde matrix given by  $(y_j^{n_i})$ . The main result of [12] implies the following proposition.

**Proposition 4.5** (cf. [12, Theorem IV]). *For any  $n \geq s \in \mathbb{N}$ , and any natural numbers  $t_1 \geq t_2 \geq \cdots \geq t_s$ , the generalized Vandermonde  $n \times n$  determinant  $|t_1, t_2, \dots, t_s, n-s-1, n-s-2, \dots, 1, 0|$  is, up to sign and multiples of the principal Vandermonde  $V_0$ , equal to the determinant of*

$$D_{t_1-n+1}^n\{t_2-n+2, t_3-n+3, \dots, t_s-n+s\}.$$

**Proposition 4.6.** *Let  $r_1, r_2, \dots, r_{N/m}$  be the values of  $r$  in the matrix  $M'$  from (4.1) in ascending order. Assume  $\tilde{u} + 1 > m$ . Then the generalized Vandermonde determinant  $|r_n, r_{n-1}, \dots, r_1|$  is, up to sign and multiples of*

the principal Vandermondian  $V_0$ , equal to the determinant of

$$(4.3) \quad D_{(\tilde{u}-m+1)/m}^{N/m} \left\{ \underbrace{\frac{\tilde{u}-m+1}{m}, \dots, \frac{\tilde{u}-m+1}{m}}_{p-2-\epsilon \text{ times}}, \underbrace{\frac{\tilde{u}-2m+1}{m}, \dots, \frac{\tilde{u}-2m+1}{m}}_{p-1 \text{ times}}, \dots, \underbrace{2, \dots, 2}_{p-1 \text{ times}}, \underbrace{1, \dots, 1}_{p-1 \text{ times}} \right\}.$$

*Proof.* By the construction of  $M'$ , the  $r_i$  are the whole numbers from 0 to  $(N + \tilde{u} - m + 1)/m$  in increasing order, skipping all  $r$  such that  $p \mid (mr + m - 1)$ . Let  $n = N/m$ . In the language of Proposition 4.5, we have  $r_{n+1-i} = t_i$ , so  $t_2 - n + 2 = r_{n-1} - (n-1) + 1$ ,  $t_3 - n + 3 = r_{n-2} - (n-2) + 1$ , and so forth. By Lemma 4.1(ii) and Remark 4.2, there are exactly  $p-2-\epsilon$  values of  $i$  (other than  $i = n$ ) such that  $r_i - i + 1 = (\tilde{u} + m - 1)/m$ , and  $p-1$  values of  $i$  such that  $r_i - i + 1 = j$  for each  $j$  between 1 and  $(\tilde{u} + m - 1)/m - 1$ . The proposition now follows from Proposition 4.5,  $\square$

**Corollary 4.7** (Isolatedness criterion). *Suppose  $f = \sum_{i=0}^{N/m} a_{mi} t^{mi} \in k[t]$  is a solution to the differential data criterion for  $(p, m, \tilde{u}, N)$ . If  $\tilde{u} + 1 = m$ , then  $f$  is automatically a solution to the isolated differential data criterion.*

*If  $\tilde{u} + 1 > m$ , then  $f$  is a solution to the isolated differential data criterion if and only if the matrix  $A$  is invertible, where  $A$  is the square matrix of size  $(\tilde{u} + 1 - m)/m$  whose  $ij$ th entry is*

$$a_{(p-1)(m-1)-m(j-1)+pm(i-1)}.$$

*Here, we set  $a_i = 0$  for all  $i < 0$  and  $i > N$ .*

*Proof.* Let  $n = N/m$ , and let  $\epsilon$  be defined as in Lemma 4.1. We have that  $f$  is a solution to the isolated differential data criterion if and only if the matrix  $M'$  from Equation (4.1) is invertible. In the language of generalized Vandermonde determinants, the determinant of  $M'$  up to sign is  $|r_n, r_{n-1}, \dots, r_1 = 0|$ , where the  $r_i$  are as in Proposition 4.6. Note that, by Lemma 4.1(i),  $r_n - n + 1 = (\tilde{u} - m + 1)/m$ . So if  $\tilde{u} + 1 = m$ , then  $r_n = n - 1$  and the matrix  $M'$  is itself Vandermonde, and thus invertible.

Now consider  $\tilde{u} + 1 > m$ . By Proposition 4.6,  $\det M'$  is, up to sign and multiples of the principal Vandermondian, equal to the determinant of  $B$ , where  $B$  is the matrix from Equation (4.3). This means that we start with the matrix  $D_{(\tilde{u}-m+1)/m}^n$ , move the indices in the first row up by  $(p-1)(\tilde{u}-m+1)/m - 1 - \epsilon$ , move the indices in the second row up by  $(p-1)(\tilde{u}-2m+1)/m - 1 - \epsilon$ , move the indices in the third row up by  $(p-1)(\tilde{u}-3m+1)/m - 1 - \epsilon$ , etc. So the first row of  $B$  begins with  $V_\alpha$ ,

where  $\alpha = (p-1)(\tilde{u} - m + 1)/m - \epsilon$ , the second row begins with  $V_{\alpha-p}$ , the third begins with  $V_{\alpha-2p}$ , etc., and the indices on the respective  $V_{(\cdot)}$  increase by 1 as we move from left to right along any row. We need to show that  $B$  is invertible if and only if the matrix  $A$  from the statement of the corollary is invertible.

By Equation (4.2),  $V_\alpha = (-1)^\alpha a_{N-m\alpha}/a_N$ . Since  $N = (p-1)\tilde{u} - m\epsilon$ , we have that for  $\alpha = (p-1)(\tilde{u} - m + 1)/m - \epsilon$ , the entry  $V_\alpha$  equals  $(-1)^\alpha a_{(p-1)(m-1)}/a_N$ . So this is the top left entry of  $B$ . Each step to the right increases the index of  $V_{(\cdot)}$  by 1, which, by Equation (4.2), decreases the corresponding index of  $a_{(\cdot)}$  by  $m$  and changes the sign. Similarly, each step down decreases the index of  $V_{(\cdot)}$  by  $p$ , which increases the corresponding index of  $a_{(\cdot)}$  by  $pm$  and changes the sign. So the  $ij$ th entry of  $B$  is  $(-1)^{i+j+\alpha}(a_{(p-1)(m-1)-m(j-1)+pm(i-1)})/a_N$ . Multiplying the odd-numbered rows and columns of  $B$  by  $-1$ , and then multiplying every entry by  $(-1)^\alpha$ , we obtain the matrix  $B'$  whose  $ij$ th entry is  $a_{(p-1)(m-1)-m(j-1)+pm(i-1)}/a_N$ . Clearly,  $B$  is invertible if and only if  $B'$  is. Since  $a_N B' = A$  and  $a_N \neq 0$ , we see that  $B'$  is invertible if and only if  $A$  is, and we are done.  $\square$

*Example 4.8.* Suppose  $(p, m, \tilde{u}, N) = (5, 2, 9, 36)$ . A solution  $f$  is isolated if the matrix  $B := D_4^{18}\{4, 4, 4, 3, 3, 3, 2, 2, 2, 2, 1, 1, 1, 1\}$  is invertible. We saw in Example 4.4 that

$$B = \begin{pmatrix} V_{16} & V_{17} & V_{18} & 0 \\ V_{11} & V_{12} & V_{13} & V_{14} \\ V_6 & V_7 & V_8 & V_9 \\ V_1 & V_2 & V_3 & V_4 \end{pmatrix}.$$

By Equation (4.2), up to factors of  $a_N = a_{36} \neq 0$ , this matrix is equal to

$$\begin{pmatrix} a_4 & a_2 & a_0 & 0 \\ a_{14} & a_{12} & a_{10} & a_8 \\ a_{24} & a_{22} & a_{20} & a_{18} \\ a_{34} & a_{32} & a_{30} & a_{28} \end{pmatrix}$$

which is the matrix  $A$  from Corollary 4.7.

*Remark 4.9.* Suppose  $A$  is the matrix from Corollary 4.7. Here are some observations about  $\det A$  which could potentially be helpful for future computations concerning the isolated differential data criterion.

- (i) Each term of  $\det A$  is a monomial of degree  $(\tilde{u} - m + 1)/m$  in the  $a_i$ . If the *weight* of a monomial  $c \prod_{\ell=1}^L a_{i_\ell}$  is defined to be  $\sum_{\ell=1}^L i_\ell$ ,

then the weight of each term of  $\det A$  equals

$$\sum_{\ell=1}^{(\tilde{u}-m+1)/m} ((m-1)(p-1) + (\ell-1)(p-1)m) = \frac{(p-1)(\tilde{u}-m+1)(\tilde{u}-1)}{2m}.$$

In Example 4.8, the weight of each term is 64.

(ii) The indices of the  $a_i$  jump by  $pm$  in every row and by  $\tilde{u} - 2m + 1$  from the first entry in a row to the last one. Thus if  $\tilde{u} - 2m + 1 < pm$ , no  $a_i$  appears more than once in  $A$ . In order to prove Conjecture 1.4 when the  $p$ -Sylow subgroup of  $G$  has order  $p^2$ , one need only show the isolated differential data criterion holds for  $(p, m, \tilde{u}, N)$  with  $\tilde{u} < pm$  (Proposition 2.4). In particular,  $\tilde{u} - 2m + 1 < pm$ , so we may assume in this case that no term of  $\det A$  has a repeated factor of  $a_i$ .

*Example 4.10.* Recall from Example 3.3 that the only functions that satisfy differential data criterion are  $2t^{10} + 1$  and  $2t^{10} + t^8 + t^6 + 1$ . Moreover, by Corollary 4.7, the matrix  $A$  associated to that quadruple is

$$A = \begin{pmatrix} a_2 & a_0 \\ a_8 & a_6 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ a_8 & a_6 \end{pmatrix}.$$

The determinant of the matrix is  $-a_8$ . Hence, only  $2t^{10} + t^8 + t^6 + 1$  verifies the isolated differential data criterion.

## 5. Gröbner basis computation setup

Recall that a quadruple  $(p, m, \tilde{u}, N)$  satisfies the isolated differential data criterion if there exist elements  $a_i \in k$ ,  $0 \leq i \leq N$  that satisfy the conditions of Proposition 3.1 and Corollary 4.7. Using the notation of the former, we define an ideal  $I = (g_0, g_m, g_{2m}, \dots, g_N) \in k[a_0, \dots, a_N]$  where

$$(5.1) \quad \begin{cases} g_0 := a_0 + u^{-1} \\ g_{mi} := ua_{mi}^p - c_{pmi-\tilde{u}(p-1)}, & \text{for } \lceil \tilde{u} - \tilde{u}/p \rceil \leq mi \leq N \\ g_{mi} := a_{mi}, & \text{otherwise} \end{cases}$$

while, in the notation of the latter, we write  $h$  for the determinant of the matrix with entries  $a_{(p-1)(m-1)-m(j-1)+pm(i-1)}$  from Corollary 4.7, which is also a polynomial in  $k[a_0, \dots, a_N]$ .

*Remark 5.1.* Proposition 3.1 and Corollary 4.7 can be combined to provide a method to verify whether a given quadruple  $(p, m, \tilde{u}, N)$  satisfies the isolated differential data criterion: first we find a  $k$ -rational point  $(a_0, \dots, a_N)$  in the affine variety  $V(I) \subseteq \mathbb{A}^N$  with  $a_N \neq 0$ , then we compute the determinant  $h(a_0, \dots, a_N)$  and verify it is non-zero. This approach was illustrated

in Example 3.3 and Example 4.10, where we verified that the quadruple  $(3, 2, 5, 10)$  satisfies the isolated differential data criterion.

The obvious disadvantage of the above method is that it seems difficult to find an explicit formula for such a  $k$ -rational point for a general quadruple  $(p, m, \tilde{u}, N)$ . Our alternative computational approach can be summarized as follows:

**Proposition 5.2.** *There exists a solution to the isolated differential data criterion for a quadruple  $(p, m, \tilde{u}, N)$  if and only if the ideal*

$$J = (g_0, g_m, g_{2m}, \dots, g_N, 1 - ya_Nh) \subseteq k[a_0, a_m, a_{2m}, \dots, a_N, y]$$

*is not the unit ideal. This is equivalent to  $1$  not being in the reduced Gröbner basis of  $J$  with respect to any term order.*

*Proof.* By Proposition 3.1, the quadruple  $(p, m, \tilde{u}, N)$  satisfies the differential data criterion if and only if there exists a solution to the system (3.2), i.e., if  $g_0 = g_m = \dots = g_N = 0$  and  $a_N \neq 0$ . Furthermore, such a solution is isolated if and only if the matrix  $A$  of Corollary 4.7 is invertible, i.e. if and only if  $h \neq 0$ . As  $k$  is algebraically closed, it follows from Hilbert's Nullstellensatz that this happens if and only if neither  $a_N$  nor  $h$  lies in the radical of  $(g_0, g_m, \dots, g_N)$ . By [8, Section 15, Corollary 35], this is equivalent to  $(g_0, g_m, \dots, g_N, 1 - ya_Nh)$  not being the unit ideal in  $k[a_0, \dots, a_N, y]$ .  $\square$

*Example 5.3.* Consider the quadruple  $(3, 2, 5, 10)$  of Example 3.3 and Example 4.10. To apply Proposition 5.2, we consider the ideal

$$\begin{aligned} J = (a_0 - 1, 2a_6^3 + a_8, 2a_8^3 + a_6a_8, 2a_{10}^3 - a_{10}^2, a_2, a_4, 1 - ya_{10}a_8) \\ \subseteq k[a_0, a_2, a_4, a_6, a_8, a_{10}], \end{aligned}$$

then compute the Gröbner Basis

$$\mathcal{G} = \{y^3 - a_6, a_6^2 - y, a_6a_8 - y^2, a_8^2 - a_6, a_6y - a_8, a_8y - 1, a_{10} + 1\}$$

corresponding to the (degrevlex) monomial ordering  $y > a_{10} > \dots > a_0$ , and finally verify that  $1 \notin \mathcal{G}$ .

*Remark 5.4.* Ignoring the line  $a_N \neq 0$ , the system of equations (3.2) is a system of  $N/m + 1$  equations in the  $N/m + 1$  variables  $a_0, a_m, a_{2m}, \dots, a_N$  over the algebraically closed field  $k$ . It is thus reasonable to expect a solution. In fact, the solution space, if it exists, is always zero-dimensional. This fact is not used in the sequel, so we only sketch the proof: If there were a positive-dimensional solution space, then the solution space of the corresponding homogenized system (say using a variable  $x$ ) would non-trivially intersect the hyperplane at infinity given by  $x = 0$ . Since the  $c_j$  all have degree  $p - 1$  in the  $a_i$  by Remark 3.2, one sees that  $x = 0$  would imply that  $a_i = 0$  for all  $i$ , a contradiction.

## 6. Computational Results

In this section we prove that  $D_{25}$  and  $D_{27}$  are local Oort groups.

**6.1.  $D_{25}$ .** Since  $D_{25} \cong \mathbb{Z}/5^2 \rtimes \mathbb{Z}/2$ , we have that  $p = 5$ ,  $m = 2$ ,  $n = 2$  and so, by Proposition 2.4, it suffices to verify that the isolated differential data criterion is satisfied for the quadruples  $(5, 2, \tilde{u}, N)$  where  $\tilde{u} < 10$ ,  $\tilde{u} \equiv -1 \pmod{2}$ ,  $5 \nmid \tilde{u}$  and  $N \in \{4\tilde{u}, 4\tilde{u} - 2\}$ . We thus have that  $D_{25}$  is local Oort group if the isolated differential data criterion is satisfied for the quadruples  $(5, 2, \tilde{u}, N)$  where

$$(6.1) \quad (\tilde{u}, N) \in \{(1, 2), (1, 4), (3, 10), (3, 12), (7, 26), (7, 28), (9, 34), (9, 36)\}.$$

To verify the isolated differential data criterion for the above quadruples, we use Remark 5.1. For each pair  $(\tilde{u}, N)$  listed in (6.1), we consider the system of equations

$$\begin{cases} a_0 = -u^{-1} \\ ua_{2i}^5 = c_{10i-4\tilde{u}}, & \text{for } \lceil \tilde{u} - \tilde{u}/5 \rceil \leq 2i \leq N \\ a_{2i} = 0, & \text{otherwise,} \end{cases}$$

where the polynomials  $c_{10i-4\tilde{u}}$  are defined in Equation (3.3). We note that  $\tilde{u}$  is not divisible by  $p$  in any of the cases and so,  $\tilde{u} = u$ . The small size of these input allows us to explicitly solve the system.<sup>2</sup> For each solution obtained, we compute the determinant of the square matrix of size  $(\tilde{u} - 1)/2$  whose  $ij^{\text{th}}$  entry is  $a_{4-2(j-1)+10(i-1)}$ , as in Corollary 4.7. In the table below, we indicate one isolated solution per pair  $(\tilde{u}, N)$ , noting that, in some cases, we have found more than one. (In the following table,  $\alpha$  satisfies  $\alpha^2 = 3$  in  $\overline{\mathbb{F}}_5$ .)

$(\tilde{u}, N)$	Solution to the Isolated Differential Data Criterion
(1,2)	$t^2 + 4$
(1,4)	$t^4 + 4$
(3,10)	$2t^{10} + 3t^8 + t^4 + 3$
(3,12)	$2t^{12} + t^8 + 4t^4 + 3$
(7,26)	$2t^{26} + 2t^{24} + 4t^{20} + 2t^{16} + t^{12} + t^8 + 2$
(7,28)	$3t^{28} + t^{26} + 2t^{24} + 3t^{16} + 2t^{12} + 2t^8 + 2$
(9,34)	$4t^{34} + t^{32} + 3t^{30} + 2t^{28} + 4t^{26} + 4t^{22} + t^{18} + 3t^{16} + 2t^{14} + 3t^{12} + 2t^{10} + 1$
(9,36)	$4t^{36} + (\alpha - 1)t^{32} + (3\alpha + 1)t^{28} + 2t^{24} + 4t^{20} + 3\alpha t^{16} + t^{12} + 1$

<sup>2</sup>The solutions are calculated by hand from the Gröbner basis of the system, which is calculated using the program `sage_GB_calculation_according_to_paper.txt`. They can be checked using the program `sage_poly_checking_validity_and_isolatedness.txt`. Both programs are bundled with the arXiv version of this paper (<https://arxiv.org/abs/1912.12797>).

**6.2.  $D_{27}$ .** Since  $D_{27} \cong \mathbb{Z}/3^3 \rtimes \mathbb{Z}/2$ , we have that  $p = 3$ ,  $m = 2$ ,  $n = 3$ . By Proposition 2.4, it suffices to verify that the isolated differential data criterion is satisfied for the quadruples  $(3, 2, \tilde{u}, N)$  where  $\tilde{u} \leq 20$ ,  $\tilde{u} \equiv -1 \pmod{2}$ ,  $9 \nmid \tilde{u}$  and  $N \in \{2\tilde{u}, 2\tilde{u} - 2\}$ . So,  $D_{27}$  is local Oort group if the isolated differential data criterion is satisfied for the quadruples  $(3, 2, \tilde{u}, N)$  where

$$(6.2) \quad (\tilde{u}, N) \in \left\{ \begin{array}{l} (3, 4), (3, 6), (5, 8), (5, 10), (7, 12), (7, 14), \\ (15, 28), (15, 30), (17, 32), (17, 34), (19, 36), (19, 38) \end{array} \right\}.$$

We again use Remark 5.1 to verify the isolated differential data criterion for the above quadruples. For each pair  $(\tilde{u}, N)$  in the list (6.2), we consider the system of equations

$$\begin{cases} a_0 = -u^{-1} \\ ua_{2i}^3 = c_{6i-2\tilde{u}}, & \text{for } \lceil \tilde{u} - \tilde{u}/3 \rceil \leq 2i \leq N \\ a_{2i} = 0, & \text{otherwise,} \end{cases}$$

where the polynomials  $c_{6i-2\tilde{u}}$  are defined in Equation (3.3). We note that when  $\tilde{u}$  is divisible by  $p$ , we have  $u = \tilde{u}/3$ . Here we can explicitly compute solutions except when  $(\tilde{u}, N) = (17, 34)$  or  $(19, 36)$ .<sup>3</sup> In all but these two cases, we compute the determinant of the square matrix of size  $(\tilde{u} - 1)/2$  whose  $ij^{\text{th}}$  entry is  $a_{2-2(j-1)+6(i-1)}$ , as in Corollary 4.7. As with  $D_{25}$ , we indicate one solution to the isolated differential criterion per pair in the table below (in which  $\beta$  satisfies  $\beta^2 = 2$ ).

For  $(17, 34)$  and  $(19, 36)$ , we instead use the criterion of Proposition 5.2 to verify that an isolated solution exists.<sup>4</sup>

$(\tilde{u}, N)$	Solution to the Isolated Differential Data Criterion
(3,4)	$\beta t^4 + t^2 + 2$
(3,6)	$t^6 + 2t^4 + t^2 + 2$
(5,8)	$t^8 + t^6 + 1$
(5,10)	$2t^{10} + t^8 + t^6 + 1$
(7,12)	$\beta t^{12} + t^{10} + t^8 + 2$
(7,14)	$t^{14} + t^{12} + t^{10} + t^8 + 2$
(15,28)	$\beta t^{28} + 2t^{26} + 2t^{24} + 2t^{18} + 2t^{16} + 2t^{10} + 1$
(15,30)	$2t^{30} + 2t^{28} + t^{24} + t^{20} + t^{18} + t^{16} + 2t^{10} + 1$
(17,32)	$t^{32} + t^{30} + t^{28} + t^{26} + t^{24} + t^{22} + t^{20} + t^{18} + 1$
(17,34)	Solution exists due to Proposition 5.2
(19,36)	Solution exists due to Proposition 5.2
(19,38)	$t^{38} + t^{36} + t^{34} + t^{32} + t^{30} + t^{28} + t^{26} + t^{24} + t^{22} + t^{20} + 2$

<sup>3</sup>Again, we use the program `sage_GB_calculation_according_to_paper.txt` to compute the Gröbner bases and check using `sage_poly_checking_validity_and_isolatedness.txt`.

<sup>4</sup>This is verified by the program `sage_existence_iso_sol_check.txt`, also available at <https://arxiv.org/abs/1912.12797>.

## References

- [1] J. BERTIN, “Obstructions locales au relèvement de revêtements galoisiens de courbes lisses”, *C. R. Math. Acad. Sci. Paris* **326** (1998), no. 1, p. 55-58.
- [2] J. BERTIN & A. MÉZARD, “Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques”, *Invent. Math.* **141** (2000), no. 1, p. 195-238.
- [3] I. I. BOUW & S. WEWERS, “The local lifting problem for dihedral groups”, *Duke Math. J.* **134** (2006), no. 3, p. 421-452.
- [4] I. I. BOUW, S. WEWERS & L. ZAPPONI, “Deformation data, Belyi maps, and the local lifting problem”, *Trans. Am. Math. Soc.* **361** (2009), no. 12, p. 6645-6659.
- [5] L. H. BREWIS & S. WEWERS, “Artin characters, Hurwitz trees and the lifting problem”, *Math. Ann.* **345** (2009), no. 3, p. 711-730.
- [6] P. CARTIER, “Une nouvelle opération sur les formes différentielles”, *C. R. Acad. Sci. Paris* **244** (1957), p. 426-428.
- [7] T. CHINBURG, R. GURALNICK & D. HARBATER, “The local lifting problem for actions of finite groups on curves”, *Ann. Sci. Éc. Norm. Supér.* **44** (2011), no. 4, p. 537-605.
- [8] D. S. DUMMIT & R. M. FOOTE, *Abstract algebra*, third ed., John Wiley & Sons, 2004, xii+932 pages.
- [9] M. A. GARUTI, “Prolongement de revêtements galoisiens en géométrie rigide”, *Compos. Math.* **104** (1996), no. 3, p. 305-331.
- [10] B. GREEN & M. MATIGNON, “Liftings of Galois covers of smooth curves”, *Compos. Math.* **113** (1998), no. 3, p. 237-272.
- [11] A. GROTHENDIECK (ed.), *Séminaire de géométrie algébrique du Bois Marie 1960–61. Revêtements étalés et groupe fondamental (SGA 1)*, Documents Mathématiques, vol. 3, Société Mathématique de France, 2003, xviii+327 pages.
- [12] E. R. HEINEMAN, “Generalized Vandermonde determinants”, *Trans. Am. Math. Soc.* **31** (1929), no. 3, p. 464-476.
- [13] S. LANG, *Elliptic functions*, second ed., Graduate Texts in Mathematics, vol. 112, Springer, 1987, With an appendix by J. Tate, xii+326 pages.
- [14] A. OBUS, “The (local) lifting problem for curves”, in *Galois-Teichmüller theory and arithmetic geometry*, Advanced Studies in Pure Mathematics, vol. 63, Mathematical Society of Japan, 2012, p. 359-412.
- [15] ———, “The local lifting problem for  $A_4$ ”, *Algebra Number Theory* **10** (2016), no. 8, p. 1683-1693.
- [16] ———, “A generalization of the Oort conjecture”, *Comment. Math. Helv.* **92** (2017), no. 3, p. 551-620.
- [17] ———, “Lifting of curves with automorphisms”, in *Open Problems in Arithmetic Algebraic Geometry*, Advanced Lectures in Mathematics (ALM), vol. 46, International Press, 2019, p. 9-59.
- [18] A. OBUS & R. J. PRIES, “Wild tame-by-cyclic extensions”, *J. Pure Appl. Algebra* **214** (2010), no. 5, p. 565-573.
- [19] A. OBUS & S. WEWERS, “Cyclic extensions and the local lifting problem”, *Ann. Math.* **180** (2014), no. 1, p. 233-284.
- [20] G. PAGOT, “Relèvement en caractéristique zéro d’actions de groupes abéliens de type  $(p, \dots, p)$ ”, PhD Thesis, Université Bordeaux I (France), 2002, available at <http://www.math.u-bordeaux1.fr/~mmatigno/Pagot-These.pdf>.
- [21] F. POP, “The Oort conjecture on lifting covers of curves”, *Ann. Math.* **180** (2014), no. 1, p. 285-322.
- [22] R. J. PRIES, “Wildly ramified covers with large genus”, *J. Number Theory* **119** (2006), no. 2, p. 194-209.
- [23] J.-P. SERRE, *Corps locaux*, 2nd ed., Publications de l’Institut de Mathématique de l’Université de Nancago, vol. 8, Hermann, 1968, 245 pages.
- [24] B. WEAVER, “The local lifting problem for  $D_4$ ”, *Isr. J. Math.* **228** (2018), no. 2, p. 587-626.

Huy DANG

Institute of Mathematics

Vietnam Academy of Science and Technology

18 Hoang Quoc Viet Road

Cau Giay District

Hanoi 10307, Vietnam

*E-mail:* hqd4bz@virginia.edu

Soumyadip DAS

Tata Institute of Fundamental Research

Homi Bhabha Road, Colaba

Mumbai 400005, India

*E-mail:* dass@math.tifr.res.in

Kostas KARAGIANNIS

Aristotle University of Thessaloniki

Department of Mathematics

School of Sciences

54124 Thessaloniki, Greece

*E-mail:* kkaragia@math.auth.gr

Andrew OBUS

Baruch College

1 Bernard Baruch Way

New York, NY 10010, USA

*E-mail:* andrewabus@gmail.com

Vaidehee THATTE

Binghamton University

Binghamton

New York 13902-6000, USA

*E-mail:* thatte@math.binghamton.edu