

University of Groningen

Aspects of algorithmic algebra

Vidunas, Raimundas

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version

Publisher's PDF, also known as Version of record

Publication date:
1999

[Link to publication in University of Groningen/UMCG research database](#)

Citation for published version (APA):

Vidunas, R. (1999). *Aspects of algorithmic algebra: differential equations and splines*. s.n.

Copyright

Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license. More information can be found on the University of Groningen website: <https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment>.

Take-down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): <http://www.rug.nl/research/portal>. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

Chapter 2

Second order differential equations with one singular point

The goal of this chapter is to describe the set of polynomials $r \in C[x]$ such that the linear differential equation $y'' = ry$ has Liouvillian solutions, where C is an algebraically closed field of characteristic 0. It is known that the differential equation has Liouvillian solutions only if the degree of r is even. Using differential Galois theory we show that the set of such polynomials of degree $2n$ can be represented by a countable set of algebraic varieties of dimension $n + 1$. Some properties of these algebraic varieties are proved. This chapter is the publication [61].

2.1 Introduction

Let C be an algebraically closed field of characteristic 0, and $K = C(x)$ — the differential field of rational functions with the usual derivation. We consider the second order homogeneous linear differential equation

$$y'' = ry, \quad \text{with } r \in C[x], r \notin C \tag{2.1}$$

which has only one singular point, at infinity. One can ask whether this equation has solutions which can be written in “closed form”. Joseph Liouville has studied this problem in 1841. He has built “closed form” solutions (*fonction finie explicite*) from rational functions by means of exponentials, logarithms and algebraic extensions. Liouville showed that the possible “closed form” for solutions of (2.1) is $y = F \exp(\int v dx)$, where v and F are polynomials. He also showed that they exist if and only if r can be written as $r = u' + u^2$, where $u = v + \frac{F'}{F}$. If r is of this form, Liouville has verified that the second independent solution cannot be of “closed form”, but observes that the second solution is obtained from rational functions by means of four operations: “exponentials,

logarithms, algebraic expressions and indefinite integrals". Nowadays the functions obtained with those operations are called Liouvillian functions. The aim of this chapter is to describe the set of differential equations (2.1) which have Liouvillian solutions.

To decide whether an equation of form (2.1) has Liouvillian solutions one can use the Kovacic algorithm [37], which solves this problem for general second order linear differential equations over $C(x)$. In the special case $r \in C[x]$ this algorithm and the method of Liouville are very similar. We look at the situation from the differential Galois theory point of view.

The possible differential Galois groups for (2.1) are listed in [57]. If $\deg r > 0$ then there are two possibilities: the differential Galois group is conjugated either to $Sl(2, C)$ or to the Borel group

$$\mathbb{B} = \left\{ \begin{pmatrix} c & b \\ 0 & c^{-1} \end{pmatrix} \mid c \in C^*, b \in C \right\}.$$

In the first case there are no (non-zero) Liouvillian solutions. In the second case all solutions of (2.1) are Liouvillian. This case occurs if and only if the associated Riccati equation

$$u' + u^2 = r, \quad (r \in C[x], r \notin C). \quad (2.2)$$

has a solution in $C(x)$. Hence the equation (2.1) has Liouvillian solutions if and only if the Riccati equation (2.2) has a solution $u \in C(x)$. From the structure of the Borel group it also follows that the Riccati equation has at most one rational solution.

Therefore our problem can be reformulated as to describe the set of Riccati equations (2.2) which have a rational solution. We use the following properties of these solutions.

Proposition 2.1.1 *Let $u \in C(x)$ be a rational solution of the Riccati equation $u' + u^2 = r$ with $r \in C[x]$. Then:*

- (i) *The degree of r is even $2n$.*
- (ii) *u has the form $u = v + \frac{F'}{F}$, where $v \in C[x]$ is of degree n , $F \in C[x]$ is monic and with non-zero discriminant.*
- (iii) *The polynomials v, F, r satisfy*

$$F'' + 2vF' + (v' + v^2 - r)F = 0. \quad (2.3)$$

For the proof we refer to [37, 57]. They also give the following algorithm for finding a possible solution of the Riccati equation (2.2). First we look for a formal solution $u_\infty \in C((x^{-1}))$ of it. If the degree of r is even $2n$, there are two solutions $u_\infty = a_n x^n + a_{n-1} x^{n-1} + \dots$ of the Riccati equation. Their truncations $a_n x^n + \dots + a_0$ differ by a sign. We need to compute the coefficients $a_n, a_{n-1}, \dots, a_{-1}$ of both solutions. From a possible global solution $u = v + \frac{F'}{F}$ we see that $v = \pm(a_n x^n + a_{n-1} x^{n-1} + \dots + a_0)$, and v is determined (up to a sign) by the condition that $v^2 - r$ has degree $\leq n - 1$. The coefficient a_{-1} must be the degree of F . If this coefficient of both solutions is not an integer ≥ 0 , then a solution $u \in C(x)$ of (2.2) does not exist. Otherwise at most one solution has $a_{-1} \geq 0$. In this case we set the possible degree $d = a_{-1}$ of F . The equation (2.3) can be seen as a set of linear equations in d coefficients of F . Now the existence

of F is solved by linear algebra. We note that this algorithm is essentially present in [39]. However, Liouville did not try to characterize the polynomials r of even degree for which the Riccati equation (2.2) has a rational solution. This was done by H.P. Rehm [47] in the case $\deg r = 2$.

We handle our problem using categorical language. This will help us not only to define required objects more properly, but also consider their smoothness and irreducibility efficiently. Let \mathcal{R}_C denote the category of commutative C -algebras with 1. We consider functors $\mathcal{S}_{n,d}$ from \mathcal{R}_C to the category of sets, which associates to a ring $R \in \mathcal{R}_C$ the set of triples (v, F, r) of polynomials in $R[x]$, such that v and r are of degrees n and $2n$ respectively, their leading coefficients are invertible in R ; F is monic of degree d with invertible discriminant, and such that the rational expression $u = v + \frac{F'}{F} \in R[x, \frac{1}{F}]$ formally satisfies the Riccati equation $u' + u^2 = r$. In the next section we will see that this functor is *representable*, that means there exists a C -algebra $R_{n,d} \in \mathcal{R}_C$ such that $\mathcal{S}_{n,d}(R) \cong \text{Mor}_C(R_{n,d}, R)$. In explicit terms, there is a “universal” ring $R_{n,d}$ with an element $(v_{n,d}, F_{n,d}, r_{n,d}) \in \mathcal{S}_{n,d}(R_{n,d})$ such that $v_{n,d} + \frac{F'_{n,d}}{F_{n,d}}$ is a solution of the “universal” Riccati equation $u' + u^2 = r_{n,d}$, and any other Riccati equation $u' + u^2 = r$ in a C -algebra R with a solution of the same form is obtained by a unique homomorphism $R_{n,d} \rightarrow R$ and induced “specialization” of the universal triple $(v_{n,d}, F_{n,d}, r_{n,d})$. The representing objects are unique by the general nonsense, see [40].

Having constructed the universal ring $R_{n,d}$, which represents $\mathcal{S}_{n,d}$, we define an affine scheme $\mathbf{S}_{n,d} = \text{Spec } R_{n,d}$. We will see that $\mathbf{S}_{n,d}$ is reduced, smooth, of dimension $n + 1$. Its irreducibility will be proved for $d \leq 2$ and $n \geq d - 1$. Geometric points $R_{n,d} \rightarrow C$ of $\mathbf{S}_{n,d}$ classify Riccati equations (2.2) which have a rational solution as follows. Let \mathbf{V}_k denote the affine space of polynomials in $C[x]$ of degree k . It is a Zariski open subset of \mathbb{A}^{k+1} with coordinate ring $\cong C[a_k, \dots, a_0, a_k^{-1}]$. We define a morphism $\pi_r : \mathbf{S}_{n,d} \rightarrow \mathbf{V}_{2n}$ by $(v, F, r) \mapsto r$. Explicitly it is given by the coefficients of $r_{n,d}$. The image of π_r set-theoretically is a set of polynomials $r \in C[x]$ of degree $2n$, such that the Riccati equation $u' + u^2 = r$ has a rational solution $u \in C(x)$. For fixed n the set of all such polynomials degree $2n$ is the union of images $\pi_r(\mathbf{S}_{n,d})$ for various d . Since a Riccati equation (2.2) has at most one rational solution for a fixed r of positive degree, and π_r is a closed immersion (as we will see), we have the following result:

Theorem 2.1.2 *The set of polynomials r of degree $2n > 0$ such that the linear differential equation (2.2) has Liouvillian solutions, is isomorphic (set-theoretically) to the disjoint union $\coprod_{d \geq 0} \pi_r(\mathbf{S}_{n,d})$ of Zariski closed subsets in \mathbf{V}_{2n} .*

The other main results of this chapter concern the geometry of the affine schemes $\mathbf{S}_{n,d}$. They are summarized below. Additionally, the case $n = 2$ is considered more thoroughly in section 4. For convenience, let \mathbf{F}_d be the Zariski open set of monic polynomials of degree d with non-zero discriminant in the affine space \mathbb{A}^d of all monic polynomials of degree d . We also consider the morphisms $\pi_v : \mathbf{S}_{n,d} \rightarrow \mathbf{V}_n$ and $\pi_F : \mathbf{S}_{n,d} \rightarrow \mathbf{F}_d$ defined by $(v, F, r) \mapsto v$ and $(v, F, r) \mapsto F$ respectively (analogous to $\pi_r : \mathbf{S}_{n,d} \rightarrow \mathbf{V}_{2n}$).

Theorem 2.1.3 *Let $n > 0, d \geq 0$ be integers. Let $R_{n,d}$ represent the functor $\mathcal{S}_{n,d}$, and let $\mathbf{S}_{n,d} = \text{Spec } R_{n,d}$, the morphisms π_r, π_v and π_F be as above. Then:*

- (i) $\mathbf{S}_{n,d}$ is reduced, smooth, a complete intersection, of dimension $n + 1$.
- (ii) The morphism $\pi_r : \mathbf{S}_{n,d} \rightarrow \mathbf{V}_{2n}$ is a closed immersion.
- (iii) The morphism $\pi_v : \mathbf{S}_{n,d} \rightarrow \mathbf{V}_n$ is a finite morphism of degree $\binom{n+d-1}{d}$.
- (iv) If $n \geq d$, then the morphism $\pi_F : \mathbf{S}_{n,d} \rightarrow \mathbf{F}_d$ is surjective; in this case $\mathbf{S}_{n,d}$ is isomorphic to $\mathbf{F}_d \times \mathbf{V}_{n-d}$.
- (v) If $n < d$, then π_F gives an isomorphism of $\mathbf{S}_{n,d}$ with a locally closed subscheme of \mathbf{F}_d ; the collection of images $\pi_F(\mathbf{S}_{n,d})$ for $1 \leq n \leq d - 1$ forms a disjoint covering (stratification) of \mathbf{F}_d .
- (vi) $\mathbf{S}_{n,d}$ is irreducible if $n \leq 2$ or $n \geq d - 2$.

These results do not immediately give a better algorithm for solving equation (2.1). However, similar investigations for differential equations with more singular points may help us to improve some steps of the Kovacic algorithm [37], where efficient choices of local solutions need to be made. In this chapter one can see the complexity of solving differential equations with parameters.

The chapter is organized as follows. In the next section we construct the representing ring $R_{n,d}$ and prove the statement (ii). Here we also introduce a useful two-dimensional algebraic group, which corresponds to affine changes of the indeterminate x , and acts on $\mathbf{S}_{n,d}$ and related schemes. In section 3 we look at the morphism π_F and prove parts (iv) and (v) of the proposition above. The required properties (including irreducibility) of $\mathbf{S}_{n,d}$ with $n \geq d - 1$ then follow directly. For $n < d - 1$ we prove the statement (i), characterize the Zariski closure of $\pi_F(\mathbf{S}_{k,d})$ in \mathbf{F}_d , and prove irreducibility of $\mathbf{S}_{d-2,d}$. The fourth section is devoted to the case $n = 2$, main results being summarized in theorem 2.4.1. Also some arithmetical properties of $\mathbf{S}_{2,d}$ will be mentioned. In the last section the statement (iii) is proved using Gröbner bases.

2.2 Functors associated to the problem

Most of the algebraic schemes in this chapter are defined and considered in terms of functors associated to them. For instance, the “obvious” affine spaces \mathbf{V}_k and \mathbf{F}_d can be precisely defined as follows. The first one is the spectrum of the representing ring of the functor \mathcal{V}_k , which assigns to a ring $R \in \mathcal{R}_C$ the set of polynomials in $R[x]$ of degree k with invertible leading coefficient. In a similar way \mathbf{F}_d is associated to the functor $\mathcal{R}_C \rightarrow (\text{Sets})$, which assigns to a ring R the set of monic polynomials in $R[x]$ with invertible discriminant. The morphism $\pi_r : \mathbf{S}_{n,d} \rightarrow \mathbf{V}_{2n}$ is intrinsically defined by the natural transformation $\mathcal{S}_{n,d} \rightarrow \mathcal{V}_{2n}$ with $\mathcal{S}_{n,d}(R) \rightarrow \mathcal{V}_{2n}(R)$ given by $(v, F, r) \rightarrow r$ for a ring $R \in \mathcal{R}_C$. The morphisms π_v and π_F are defined in a similar way. When we write the coordinate ring of \mathbf{V}_k as $C[a_k, \dots, a_0, a_k^{-1}]$, the universal polynomial in $\mathcal{V}_k(\mathcal{O}(\mathbf{V}_k))$ is assumed to be $a_k x^k + \dots + a_0$. The coordinate ring of \mathbf{F}_d is isomorphic to $C[p_1, \dots, p_d, \Delta^{-1}]$, where Δ is the discriminant of the universal polynomial $x^d + p_1 x^{d-1} + \dots + p_d$ for the functor of \mathbf{F}_d . Note the difference in the enumeration of coefficients of the universal polynomials of these two functors. All functors (except one on Artinian local rings) defined in this chapter are covariant, from \mathcal{R}_C to the category of sets, and representable.

Now our problem. From now on the integers $n > 0, d \geq 0$ are fixed. Our basic equation is (2.3), where F, v and r could be polynomials over any ring $R \in \mathcal{R}_C$:

$$F'' + 2vF' + (v' + v^2 - r)F = 0. \quad (2.4)$$

It is equivalent to the condition that $(v, F, r) \in \mathcal{S}_{n,d}(R)$. The functor $\mathcal{S}_{n,d}$ is representable as follows. Let R_u be the ring

$$R_u = C[b_{2n}, \dots, b_0, b_{2n}^{-1}, a_n, \dots, a_0, a_n^{-1}, p_1, \dots, p_d, \Delta^{-1}] \cong \mathcal{O}(\mathbf{V}_{2n}) \otimes \mathcal{O}(\mathbf{V}_n) \otimes \mathcal{O}(\mathbf{F}_d)$$

and let $r = b_{2n}x^{2n} + \dots + b_0$, $v = a_nx^n + \dots + a_0$, $F = x^d + p_1x^{d-1} + \dots + p_d$ be polynomials in $R_u[x]$. Then the functor $\mathcal{S}_{n,d}$ is represented straightaway by the ring $R_{n,d} = R_u/(T_{2n+d}, \dots, T_0)$, where the T_k 's are the coefficients of the left-hand side of (2.4) as a polynomial in $R_u[x]$:

$$F'' + 2vF' + (v' + v^2 - r)F = \sum_{j=0}^{2n+d} T_j x^j, \quad (T_j \in R_u). \quad (2.5)$$

By this construction the scheme $\mathbf{S}_{n,d} = \text{Spec } R_{n,d}$ is realized as a closed subscheme of $\mathbf{V}_{2n} \times \mathbf{V}_n \times \mathbf{F}_d$. The universal polynomials $v_{n,d}, F_{n,d}, r_{n,d}$ are homomorphic images of v, F, r by canonical surjection $R_u[x] \rightarrow R_{n,d}[x]$.

Proposition 2.2.1 *The morphism $\pi_r : \mathbf{S}_{n,d} \rightarrow \mathbf{V}_{2n}$ is a closed immersion.*

Proof. Let R_u^0 be the ring $C[a_n, \dots, a_0, a_n^{-1}, b_{2n}, \dots, b_0, b_{2n}^{-1}]$. Let $H_{2n}, \dots, H_0 \in R_u^0$ be the coefficients of the polynomial $v' + v^2 - r \in R_u^0[x]$ to the indeterminate x , so that $v' + v^2 - r = \sum_{j=0}^{2n} H_j x^j$. Finally, let $\tilde{H}_{n+d-1}, \dots, \tilde{H}_0 \in R_u$ be defined by

$$F'' + 2vF' + (H_{n-1}x^{n-1} + \dots + H_1x + H_0)F = \sum_{j=0}^{n+d-1} \tilde{H}_j x^j. \quad (2.6)$$

It is easy to see that $\mathbf{S}_{n,d}$ is also defined by the ideal $(H_{2n}, \dots, H_n, \tilde{H}_{n+d-1}, \dots, \tilde{H}_0)$ in R_u , because $T_{n+d+k} = H_{n+k} + \sum_{i=1}^{\min(d, n-k)} p_i H_{n+k+i}$ when $0 \leq k \leq n$, and any other T_j is a similar combination of \tilde{H}_j and polynomials H_n, \dots, H_{2n} .

We factor π_r as $\mathbf{S}_{n,d} \rightarrow \text{Spec } A \rightarrow \text{Spec } B \rightarrow \mathbf{V}_{2n}$, where

$$\begin{aligned} A &= R_u/(T_{2n+d}, \dots, T_{n-1}) \cong R_u/(H_{2n}, \dots, H_n, \tilde{H}_{n+d-1}, \dots, \tilde{H}_{n-1}), \\ B &= R_u^0/(H_{2n}, \dots, H_n, \tilde{H}_{n+d-1}). \end{aligned}$$

Note that $\tilde{H}_{n+d-1} = H_{n-1} + 2da_n$, thus the ring B is correctly defined.

The first morphism $\mathbf{S}_{n,d} \rightarrow \text{Spec } A$ is clearly a closed immersion.

The ring A represents the functor \mathcal{A} , which assigns to a C -algebra $R \in \mathcal{R}_C$ the set of triples (v, F, r) in $R[x]$ such that (again) the degrees of v, r and F are $n, 2n, d$; F is monic; the discriminant of F and the leading coefficients of v and r are invertible; and the degree of $F'' + 2vF' + (v' + v^2 - r)F$ is $\leq n - 2$. Analogously, the ring B represents a functor \mathcal{B} , which assigns to a ring $R \in \mathcal{R}_C$ the set of pairs (v, r) of polynomials in

$R[x]$ of degrees $n, 2n$, with invertible leading coefficients, and such that the degree of $2dvx^{d-1} + (v' + v^2 - r)x^d$ is $\leq n + d - 2$. We now show that the map $(F, v, r) \mapsto (v, r)$ defines a bijection $\mathcal{A}(R) \rightarrow \mathcal{B}(R)$ for any C -algebra R . Indeed, the condition that the degree of $F'' + 2vF' + (v' + v^2 - r)F$ is $\leq n + d - 2$ implies that the degree of $2dvx^{d-1} + (v' + v^2 - r)x^d$ is $\leq n + d - 2$. On the other hand, let a pair $(v, r) \in \mathcal{B}(R)$ be given. Then the degree of $(v' + v^2 - r)$ is $\leq n - 1$, and polynomials $(x^k)'' + 2v(x^k)' + (v' + v^2 - r)x^k$ have degree $n + k - 1$ for $k = 0, \dots, d - 1$, and degree $\leq n + d - 2$ for $k = d$. Hence there is a unique monic F of degree d such that the degree of $F'' + 2vF' + (v' + v^2 - r)F$ is $\leq n - 2$. From Yoneda lemma (see [40]) it follows that rings A and B are isomorphic, hence $\text{Spec } A \rightarrow \text{Spec } B$ is an isomorphism.

The morphism $\text{Spec } B \rightarrow \mathbf{V}_{2n}$ is a closed immersion if and only if the homomorphism of coordinate rings $\psi : C[b_{2n}, \dots, b_0, b_{2n}^{-1}] \rightarrow B$ is surjective. Let $\tilde{a}_k = a_k/a_n \in B$ for $0 \leq k < n$. Then $a_k a_l = \tilde{a}_k \tilde{a}_l b_{2n}$ for any $0 \leq k, l < n$ since $H_{2n} = a_n^2 - b_{2n} = 0$. We can rewrite the elements H_{2n-1}, \dots, H_n in the ideal as

$$H_{2n-1} = 2b_{2n}\tilde{a}_{n-1} - b_{2n-1}, \quad H_{2n-2} = 2b_{2n}\tilde{a}_{n-2} + b_{2n}\tilde{a}_{n-1}^2 - b_{2n-2}, \quad \dots,$$

$$H_n = 2b_{2n}\tilde{a}_0 + b_{2n}(\tilde{a}_1\tilde{a}_{n-1} + \tilde{a}_2\tilde{a}_{n-2} + \dots + \tilde{a}_{n-1}\tilde{a}_1) - b_n.$$

Now it is easy to see that \tilde{a}_k 's are in the image of ψ . Consider $r - v^2$ as a polynomial in $B[x]$. It is equal to $b_{2n}x^{2n} + \dots + b_0 - b_{2n}(x^n + \tilde{a}_{n-1}x^{n-1} + \dots + \tilde{a}_0)^2$. Therefore, all its coefficients lie in the image of ψ . Let \tilde{b}_{n-1} be the preimage of the coefficient to x^{n-1} in $r - v^2$. Then $\tilde{H}_{n+d-1} = (n + 2d)a_n - \tilde{b}_{n-1}$. It shows that $a_n \in \text{Im } \psi$, and immediately all $a_k = \tilde{a}_k a_n$ are in the image of ψ . Thus ψ is surjective and $\text{Spec } B \rightarrow \mathbf{V}_{2n}$ is a closed immersion. Note incidentally that the image of $\text{Spec } B \rightarrow \mathbf{V}_{2n}$ is a hypersurface in \mathbf{V}_{2n} given by

$$\tilde{b}_{n-1}^2 - (n + 2d)^2 b_{2n} = 0. \quad (2.7)$$

One can obtain this equation by eliminating a_n from H_{2n} and \tilde{H}_{n+d-1} .

The morphism $\mathbf{S}_{n,d} \rightarrow \mathbf{V}_{2n}$ is a closed immersion as a composition of closed immersions. \square

Example 2.1 In the case $n = 1$ the two morphisms in $\mathbf{S}_{1,d} \rightarrow \text{Spec } A \rightarrow \text{Spec } B$ of the last proof are isomorphisms. Thus $\mathbf{S}_{1,d}$ is isomorphic to the image of $\text{Spec } B \rightarrow \mathbf{V}_2$. The last part of the proof also gives a single equation which defines $\pi_r(\mathbf{S}_{1,d})$:

$$(b_1^2 - 4b_2b_0)^2 = 16(2d + 1)^2 b_2^3. \quad (2.8)$$

This was known to H.P. Rehm, see [47].

When $n = 1$ the morphism $\pi_v : \mathbf{S}_{1,d} \rightarrow \mathbf{V}_1$ turns out to be an isomorphism. To define the inverse morphism we introduce the following notation which will often be used later. For a C -algebra $R \in \mathcal{R}_C$ and non-negative integer k let W_R^k denote the free R -module of polynomials in $R[x]$ of degree $\leq k$.

To prove that $\pi_v : \mathbf{S}_{1,d} \rightarrow \mathbf{V}_1$ is an isomorphism we show that functors $\mathbf{S}_{1,d}$ and \mathcal{V}_1 are equivalent. Let $v = a_1x + a_0 \in \mathcal{V}_1(R)$ for a C -algebra $R \in \mathcal{R}_C$. Then $F'' + 2(a_1x + a_0)F' + (v' + v^2 - r)F = 0$ implies $v' + v^2 - r = -2da_1$. Let $L : W_R^d \rightarrow W_R^{d-1}$ be a linear map defined by $f \mapsto f'' + 2(a_1x + a_0)f' - 2da_1f$. Then $L(x^k)$ is of degree k with the leading coefficient $2(k - d)a_1$ being invertible for $0 \leq k < d$, hence these

$L(x^k)$'s form a basis for W_R^{d-1} . Thus we can express uniquely $L(x^d) \in W_R^{d-1}$ linearly in $L(x^k)$'s with $k < d$, and this linear dependence relation gives the desired F . It has invertible discriminant, because otherwise there would be a morphism $R \rightarrow C$ such that F with specialized coefficients in $C[x]$ has zero discriminant and satisfies (2.3) for some $v, r \in C[x]$, which is impossible. Thus, given $v \in \mathcal{V}_1(R)$ there exists unique $F \in \mathcal{F}_d(R)$ and $r \in \mathcal{V}_2(R)$ so that $(v, F, r) \in \mathcal{S}_{1,d}(R)$.

In [47] such F was computed explicitly for $v = a_1x \in C[x]$. In fact one needs to find a suitable linear dependence relation between $L(x^k) = k(k-1)x^{k-2} - 2(d-k)a_1x^k$. For instance $(\frac{x}{2}, F, \frac{x^2}{4} + d + \frac{1}{2})$ is an element of $\mathcal{S}_{1,d}(C)$, where

$$F = x^d + \sum_{k=1}^{\lfloor d/2 \rfloor} \frac{d!}{2^k k! (d-2k)!} x^{d-2k}. \quad (2.9)$$

An interesting observation is that if F of degree d is of this form, then the derivative of F is (up to constant d) again the polynomial of the same form of degree $d-1$.

All other elements of $\mathcal{S}_{1,d}(C)$ can be obtained from the mentioned triple by a transformation $x \mapsto \beta x + \gamma$ ($\beta \in C^*, \gamma \in C$) which changes the indeterminate x into $\beta x + \gamma$. Here we describe the action of these transformations in general situation.

We will use changes of the indeterminate x which transform a differential equation (2.1) with a single pole at infinity to an equation of the same kind again. Solutions of transformed equations are closely related. Specifically, one can check that if a function $y(x)$ satisfies the differential equation $y'' = r(x)y$, then for any $\beta \in C^*, \gamma \in C$ the function $y(\beta x + \gamma)$ satisfies $y'' = \beta^2 r(\beta x + \gamma)y$. A rational solution $u(x) \in C(x)$ of the Riccati equation $u' + u^2 = r(x)$ is then transformed to $\beta u(\beta x + \gamma) \in C(x)$. These transformations may be identified with automorphisms of the affine line \mathbb{A}^1 . They form a two-dimensional algebraic group \mathbf{G} which acts on our schemes $\mathbf{S}_{n,d}$. An element of \mathbf{G} will be denoted by $x \mapsto \beta x + \gamma$ with $\beta \in C^*, \gamma \in C$. It acts on a triple $(v, F, r) \in \mathcal{S}_{n,d}(C)$ as follows:

$$v(x) \mapsto \beta v(\beta x + \gamma), \quad F(x) \mapsto F(\beta x + \gamma)/\beta^d, \quad r(x) \mapsto \beta^2 r(\beta x + \gamma). \quad (2.10)$$

The algebraic group \mathbf{G} is generated by affine translations $x \mapsto x + \gamma$ and actions $x \mapsto \beta x$ of \mathbb{G}_m . A normal subgroup of transformations $x \mapsto x + \gamma$ is isomorphic to the additive group \mathbb{G}_a . It is not reductive, but a universal categorical quotient $\mathbf{S}_{n,d}/\mathbb{G}_a$ exists, namely it is isomorphic to the closed subscheme $\mathbf{S}_{n,d}^0$ of $\mathbf{S}_{n,d}$ defined by $a_{n-1} = 0$. (Alternatively, it is isomorphic to the subscheme of $\mathbf{S}_{n,d}$ defined by $p_1 = 0$.) Since $\mathbf{G}/\mathbb{G}_a \cong \mathbb{G}_m$ is a reductive algebraic group, it follows that a geometric quotient $\mathbf{S}_{n,d}/\mathbf{G}$ in the sense of [44] exists and is isomorphic to $\mathbf{S}_{n,d}^0/\mathbb{G}_m$.

In particular, the action of the multiplicative group \mathbb{G}_m will be important for us while proving irreducibility of some $\mathbf{S}_{n,d}$'s. It acts on the coordinate functions of $\mathbf{S}_{n,d}$ as follows:

$$a_k \mapsto \beta^{k+1} a_k, \quad p_k \mapsto p_k/\beta^k, \quad b_k \mapsto \beta^{k+2} b_k. \quad (2.11)$$

Accordingly, we introduce a grading on the coordinate rings of $\mathbf{S}_{n,d}$ and related schemes by setting degree of p_k (for $k \leq d$) to be equal to $-k$, of a_k (for $k \leq n$) — to $k+1$,

etc. We can think of the quotient $\mathbf{S}_{n,d}/\mathbf{G}$ as a subvariety of the corresponding weighted projective space — the quotient of $\mathbb{A}^{n+1} \times \mathbb{A}^d \times \mathbb{A}^{2n+1}$ by the action (2.11) of \mathbb{G}_m .

An important practical problem is the computation of a simple set of equations defining $\mathbf{S}_{n,d}$ in some coordinates. First one can easily divide out $\mathbf{S}_{n,d}$ by the algebraic group \mathbf{G} without any essential loss of information. By setting $a_{n-1} = 0$ (then $b_{2n-1} = 0$ as well) or $p_1 = 0$ in equations of $\mathbf{S}_{n,d}$ we obtain the quotient $\mathbf{S}_{n,d}/\mathbb{G}_a$. The action of \mathbb{G}_m on it allow us to set $a_n = 1$ or $b_{2n} = 1$ for example, so the dimension of our varieties is effectively reduced by 2. The polynomials $H_{2n}, \dots, H_n, \tilde{H}_{n+d-1}, \dots, \tilde{H}_0$ introduced in the proof of proposition 2.2.1 are surely better as generators of the ideal in R_u defining $\mathbf{S}_{n,d}$ than the original T_j 's in (2.5). Moreover, these polynomials are linear in p_1, \dots, p_d , so one can easily eliminate them. It was mentioned that \tilde{H}_{n+d-1} does not contain these variables. To eliminate them completely one can consider the linear map $L : W_{R_u^0}^d \rightarrow W_{R_u^0}^{n+d-1}$ defined by $f \mapsto f'' + 2vf' + (v' + v^2 - r)f$, and take maximal minors of its matrix. It might seem useful to eliminate coefficients a_i of v as well, because our goal is to recognize when for given r there are Liouvillian solutions of the differential equation (2.1). However, the obtained equations for b_i 's are very messy; the equation (2.7) is one of the simpler ones we can get. A better chance to get a fruitful insight into geometry of $\mathbf{S}_{n,d}$ is to introduce coefficients of $v' + v^2 - r$ as variables. It is useful to note that the leading term of $v' + v^2 - r$ must be $-2da_n x^{n-1}$ (this can be easily seen from (2.4)). The coefficients b_i of r are then essentially eliminated. This approach is useful when n is small, as it is demonstrated in section 2.4.

Another source of useful equations for $\mathbf{S}_{n,d}$ is lemma (2.3.1). Its corollary 2.3.2 gives us an easy parametrization of $\mathbf{S}_{n,d}$ when $n \geq d$. However, the examples in section 2.4 show that not all $\mathbf{S}_{n,d}$ are unirational. If $n = d - 1$ then $\mathbf{S}_{n,d}$ is isomorphic to an open subvariety in \mathbf{F}_d . If $n = d - 2$ then $\mathbf{S}_{n,d}$ is isomorphic to an open set of a hypersurface in \mathbf{F}_d given by a single equation $E_{d-1,d} = 0$ introduced in section 2.3. When $n - d > 1$ but small, we can use equations $E_{j,d} = 0$ quite effectively to describe our varieties, but it is better to use generators of the ideal I_F in $C[p_1, \dots, p_d]$ defined in the second half of the section 2.3. They have smaller degree and define the Zariski closure of $\pi_F(\mathbf{S}_{n,d})$ inside $\text{Spec } C[p_1, \dots, p_d]$.

2.3 Smoothness and irreducibility

We start by proving a simple lemma, which allows us however to prove easily parts (iv) and (v) of the main theorem 2.1.3. The properties of $\mathbf{S}_{n,d}$ stated in parts (i) and (vi) of the same theorem follow then immediately for $n \geq d$. The same lemma helps us a lot in proving the same statements for $n < d$. For a fixed polynomial $F \in \mathcal{F}_d(R)$ ($R \in \mathcal{R}_C$) it describes completely the set of all triples $(v, F, r) \in \mathcal{S}_{n,d}(R)$ over all n with the given F . In this way we obtain complete knowledge about the morphism $\pi_F : \mathbf{S}_{n,d} \rightarrow \mathbf{F}_d$. The equation (2.4) is used there again.

For convenience, we set $\tilde{r} = r - v' - v^2$. Note that the degree of \tilde{r} is at most $(\deg v - 1)$. Also recall the notation W_R^k .

Lemma 2.3.1 *Let R_0 be a C -algebra in \mathcal{R}_C , let $F \in R_0[x]$ be of degree $d \geq 2$ and such that its discriminant Δ is not a zero divisor in R_0 . Let $R = R_0[\Delta^{-1}]$. Then the equation*

$$F'' + 2vF' - \tilde{r}F = 0 \quad (2.12)$$

has a unique solution (v_0, \tilde{r}_0) with $v_0 \in R[x]$ of degree $\leq d - 1$, and $\tilde{r}_0 \in R[x]$ of degree $\leq d - 2$. Moreover, $\Delta \cdot v_0 \in R_0 \subset R$.

All solutions of (2.12) in R are of form

$$v = v_0 + qF, \quad \tilde{r} = \tilde{r}_0 + 2qF', \quad (2.13)$$

where $q \in R[x]$ is a polynomial.

Proof. Consider a linear map $\rho : W_R^{d-1} \times W_R^{d-2} \rightarrow W_R^{2d-2}$ defined by $\rho : (f, g) \mapsto fF' + gF$. We fix a basis $x^k, \dots, x, 1$ for the spaces W_R^k , $k = d - 1, d - 2$ or $2d - 2$. Then the matrix of this linear transformation is the transpose of the Sylvester matrix for polynomials (F', F) . Its determinant is Δ . Hence ρ is invertible, and for any polynomial $h \in W_R^{2d-2}$ (in particular, for $-F''$) there exist unique polynomials $f_0 \in W_R^{d-1}, g_0 \in W_R^{d-2}$ such that $f_0F' + g_0F = h$. Thus required $v_0F' + \tilde{r}_0F = -F''$ exists and is unique. The statement about $\Delta \cdot v_0$ follows from the Cramer's rule. For any other solution (v, \tilde{r}) of (2.12) we have $2(v - v_0)F' = (\tilde{r} - \tilde{r}_0)F$, and since $\gcd(F, F') = 1$, F divides $v - v_0$, F' divides $\tilde{r} - \tilde{r}_0$, and $\frac{v-v_0}{F} = \frac{\tilde{r}-\tilde{r}_0}{2F'} = q \in R[x]$. \square

The lemma 2.3.1 motivates us to define a map of sets $\varphi : \mathcal{F}_d(R) \rightarrow W_R^{d-1}$, which maps $F \in \mathcal{F}_d(R)$ to the corresponding $v_0 \in W_R^{d-1}$. In particular, for the universal polynomial $F = x^d + p_1x^{d-1} + \dots + p_d$ of \mathbf{F}_d we write

$$\varphi(F) = \frac{1}{\Delta}(E_{d,d-1}x^{d-1} + \dots + E_{d,1}x + E_{d,0}). \quad (2.14)$$

According to a statement in the last proposition, we have $E_{d,k} \in C[p_1, \dots, p_d]$ for all $k \leq d - 1$.

Remark 2.2 For a polynomial $F \in \mathcal{F}_d(C)$ we can compute $\varphi(F)$ by solving an extrapolation problem: at the d roots α_k ($1 \leq k \leq d$) of F the value of v should be $-F''(\alpha_k)/2F'(\alpha_k)$, according to (2.12). These values determine $\varphi(F)$ uniquely.

The next corollary is the part (iv) of the theorem 2.1.3. It immediately implies that $\mathbf{S}_{n,d}$ is smooth, reduced and irreducible, a complete intersection, of dimension $n + 1$ when $n \geq d$.

Corollary 2.3.2 *For $n \geq d$ there is an isomorphism $\mathbf{S}_{n,d} \rightarrow \mathbf{F}_d \times \mathbf{V}_{n-d}$.*

Proof. We can prove, that the associated functors $\mathcal{R}_C \rightarrow (\text{Sets})$ are equivalent, and then use Yoneda lemma, see [40]. Let $R \in \mathcal{R}_C$. Given a pair $(F, q) \in \mathcal{F}_d(R) \times \mathcal{V}_{n-d}(R)$ we construct $(v, F, r) \in \mathbf{S}_{n,d}(R)$ by $v = \varphi(F) + qF$ and r being uniquely determined by v and F . On the other hand, if $(v, F, r) \in \mathbf{S}_{n,d}(R)$ then F should divide $v - \varphi(F)$ because of (2.13), and then we can set $q = (v - \varphi(F))/F$ for the corresponding $(F, q) \in \mathcal{F}_d(R) \times \mathcal{V}_{n-d}(R)$. \square

In the case $n < d$ the map $\pi_F : \mathcal{S}_{n,d}(R) \rightarrow \mathcal{F}_d(R)$ is injective for any $R \in \mathcal{R}_{n,d}$, because given $F \in \mathcal{F}_d(R)$ we have at most one triple $(v, F, r) \in \mathcal{S}_{n,d}$ with $\deg v = n < d$ by the lemma 2.3.1. The possible one has $v = \varphi(F)$. Let us consider a functor $\mathcal{P}_{n,d}$, which associates to a C -algebra $R \in \mathcal{R}_C$ the set of monic polynomials F of degree d with invertible discriminant such that $\varphi(F)$ is of degree $\leq n$. It is equivalent to the requirement that F'' could be expressed as $-2vF' + \tilde{r}F$ with $\deg v \leq n$. Then $\mathcal{S}_{n,d}(R)$ is isomorphic to the subset of $\mathcal{P}_{n,d}(R) \setminus \mathcal{P}_{n-1,d}(R)$ of F 's such that $\varphi(F)$ has invertible leading coefficient. The functor $\mathcal{P}_{n,d}$ is representable by an affine scheme $\mathbf{P}_{n,d}$ with coordinate ring

$$\mathcal{O}(\mathbf{P}_{n,d}) \cong C[p_1, \dots, p_d, \Delta^{-1}]/(E_{d,d-1}, \dots, E_{d,n+1}), \quad (2.15)$$

where $E_{d,d-1}, \dots, E_{d,0}$ are defined by (2.14). Of course, $\mathbf{P}_{d-1,d} \cong \mathbf{F}_d$. We also define $\mathbf{P}_{n,d}^*$ to be an open subset of $\mathbf{P}_{n,d}$ defined by $E_{d,n} \neq 0$. Then $\mathbf{P}_{n,d}^* = \mathbf{P}_{n,d} \setminus \mathbf{P}_{n-1,d}$ (for $n < d$) and the coordinate ring of $\mathbf{P}_{n,d}^*$ is $\mathcal{O}(\mathbf{P}_{n,d})[E_{d,n}^{-1}]$. It is easy to see that $\mathbf{S}_{n,d}$ is isomorphic to $\mathbf{P}_{n,d}^*$ because these two schemes represent equivalent functors.

This construction shows part (v) of the main theorem 2.1.3, because $\mathbf{P}_{n,d}^* \cong \mathbf{S}_{n,d}$ is an open subset of the closed subscheme $\mathbf{P}_{n,d}$ of \mathbf{F}_d , and the disjoint union of the $\mathbf{P}_{n,d}^*$'s covers all \mathbf{F}_d .

It is clear that $\mathbf{P}_{d-1,d}^* \cong \mathbf{S}_{d-1,d}$ is an open subset of \mathbf{F}_d , hence it is automatically smooth, reduced and irreducible, a complete intersection, of dimension d .

We assume $n < d - 1$ for the rest of this section. We prove that $\mathbf{S}_{n,d}$ is smooth, reduced, of dimension $n+1$ and a complete intersection in this case. Also the irreducibility of $\mathbf{S}_{n,d}$ for $n = 2$ (in the next section) and $n = d - 2$ is proved.

The smoothness of $\mathbf{S}_{n,d}$ is proved by considering the tangent spaces at points of $\mathcal{S}_{n,d}(C)$. Computations of them are based on the lemma 2.11 in [49]. For a point $Q = (v, F, r)$ in $\mathcal{S}_{n,d}(C)$ let $\mathcal{S}_{n,d}^Q$ be a functor on local Artinian rings $R \in \mathcal{R}_C$ with residue field C so that $\mathcal{S}_{n,d}^Q(R)$ is the set of those elements of $\mathcal{S}_{n,d}(R)$ which are mapped to Q by the induced $\mathcal{S}_{n,d}(R) \rightarrow \mathcal{S}_{n,d}(C)$. Then the tangent space T_Q of $\mathbf{S}_{n,d}$ at the point Q is isomorphic to $\mathcal{S}_{n,d}^Q(C[\varepsilon])$ as a C -linear space. Here $C[\varepsilon]$ is the ring of dual numbers, $\varepsilon^2 = 0$ as usual.

Proposition 2.3.3 $\mathbf{S}_{n,d}$ is smooth, of dimension $n + 1$.

Proof. Let $Q = (v, F, r)$ be a point on $\mathcal{S}_{n,d}(C)$, let \mathcal{O}_Q be a local ring of $\mathbf{S}_{n,d}$ at Q . It is isomorphic to a quotient of a regular d -dimensional local ring by $d - n - 1$ elements, namely to the localization of $C[p_1, \dots, p_d]/(E_{d,d-1}, \dots, E_{d,n+1})$. Hence \mathcal{O}_Q has the Krull dimension at least $n+1$. We show that the dimension of the tangent space is $\leq n+1$. This will imply that \mathcal{O}_Q is a regular local ring of dimension $n+1$.

We identify the tangent space T_Q with a subspace of W_C^{d-1} of polynomials G of degree $\leq d-1$ such that $F + \varepsilon G$ defines an element of $\mathcal{S}_{n,d}^Q(C[\varepsilon])$. Note that if $(v + \varepsilon w, F + \varepsilon G, r + \varepsilon s) \in \mathcal{S}_{n,d}^Q(C[\varepsilon])$ then

$$G'' + 2vG' + (v' + v^2 - r)G = (-2w)F' + (s - w' - 2vw)F \quad (2.16)$$

with $\deg w \leq n$. In general, for any $G \in W_C^{d-1}$ the polynomial on left-hand side of (2.16) is of degree $\leq n+d-1$. We can express it as $AF' + BF$ with $\deg A \leq d-1$, $\deg B \leq d-2$, because this is possible for any polynomial of degree $\leq 2d-2$ by the isomorphism $W_C^{d-1} \times W_C^d \rightarrow W_C^{2d-2}$ defined by $(f, g) \rightarrow fF' + gF$ (as in the proof of the lemma 2.3.1). Moreover, such an expression is unique and depends linearly on $G \in W_C^{d-1}$. Define a linear map $L : W_C^{d-1} \rightarrow W_C^{d-1}$ which sends a polynomial $G \in W_C^{d-1}$ to the unique A of degree $\leq d-1$ in the expression $G'' + 2vG' + (v' + v^2 - r)G = AF' + BF$. If $\deg L(G) \leq n$ we easily construct an element of $\mathcal{S}_{n,d}^Q(C[\varepsilon])$ from $F + \varepsilon G$. Thus the tangent space T_Q is isomorphic to the subspace of W_C^{d-1} of polynomials G for which $\deg L(G) \leq n$.

The next step of the proof is to construct polynomials G_1, \dots, G_{d-n-1} of degree $\leq d-1$ so that $\deg L(G_m) = n+m$ for $m = 1, \dots, d-n-1$. The polynomial G_m can be expressed as $G_m = eF' + fF$ with $\deg e = m+1$ and $\deg f = m$. We want to choose polynomials e and f so that $\deg G_m \leq d-1$. Write $e = x^{m+1} + e_m x^m + \dots + e_0$, $f = -dx^m + f_{m-1}x^{m-1} + \dots + f_0$, so that the coefficient to x^{d-1+i} in $eF' + fF$ is of form

$$de_i + f_{i-1} + (\text{linear terms in } e_{i+1}, \dots, e_m, f_i, \dots, f_{m-1}).$$

From here it is easy to see, that coefficients $e_m, \dots, e_0, f_{m-1}, \dots, f_0$ can be chosen so that $\deg G_m \leq d-1$. Further, straightforward computation yields

$$G_m'' + 2vG_m' + (v' + v^2 - r)G_m = (e'' + 2f' - (2ve)')F' + (\dots)F,$$

Since $\deg(e'' + 2f' - (2ve)') = n+m < d$, we have $L(G_m) = e'' + 2f' - (2ve)'$.

The obtained polynomials G_m ($1 \leq m \leq n-d-1$) are such that $L(G_m)$ have different degrees and these degrees are greater than n . Thus they are linearly independent and generate a subspace of W_C^d of dimension $(d-n-1)$ which has only the zero vector in common with T_Q . Hence the dimension of T_Q is less or equal to $d - (d-n-1) = n+1$.

The upper bound for the dimension of T_Q implies that the local ring \mathcal{O}_Q is regular of dimension $n+1$ for every point $Q \in \mathbf{S}_{n,d}$. This means that $\mathbf{S}_{n,d}$ is smooth and has dimension $n+1$. \square

Corollary 2.3.4 $\mathbf{P}_{n,d}$ is smooth, of dimension $n+1$.

Proof. Let $Q \in \mathbf{P}_{n,d}$, let \mathcal{O}_Q be the local ring of $\mathbf{P}_{n,d}$ at Q . Its dimension is $\geq n+1$. Q is a smooth point on some $\mathbf{P}_{m,d}^*$ with $m \leq n$. Let \mathcal{O}_Q^* be the regular local ring of $\mathbf{P}_{m,d}^*$ at Q . Its dimension is $m+1$. The elements $E_{d,n}, \dots, E_{d,m+1}$ of \mathcal{O}_Q generate the kernel of $\mathcal{O}_Q \rightarrow \mathcal{O}_Q^*$. Hence the dimensions of the local rings differ at most by $n-m$. Thus \mathcal{O}_Q is a regular local ring of dimension $n+1$, and $\mathbf{P}_{n,d}$ is smooth of the same dimension. \square

Corollary 2.3.5 $\mathbf{S}_{n,d}$ and $\mathbf{P}_{n,d}$ are complete intersections.

Proof. $\mathbf{P}_{n,d}$ is defined by $n-d-1$ equations $E_{d,d-1}, \dots, E_{d,n+1}$ in a d -dimensional regular affine space \mathbf{F}_d . On the other hand, the dimension of $\mathbf{P}_{n,d}$ is $n+1 = d - (n-d-1)$, thus it is a complete intersection. $\mathbf{S}_{n,d}$ is also a complete intersection as open set of $\mathbf{P}_{n,d}$. \square

The last aim of this section is to prove that $\mathbf{P}_{d-2,d}$ is irreducible. The main ingredient in the proof of its irreducibility is to show that its Zariski closure in $\text{Spec } C[p_1, \dots, p_d]$ is regular in codimension 1. The same actually holds for the Zariski closure of $\mathbf{P}_{n,d}$ in $\text{Spec } C[p_1, \dots, p_d]$ for any $n < d - 1$. We prove the more general regularity statement because the special case $n = d - 2$ is not much simpler. For the rest of this section, let $\bar{\mathbf{P}}_{n,d}$ denote the Zariski closure of $\mathbf{P}_{n,d}$ in $\text{Spec } C[p_1, \dots, p_d]$.

To characterize the Zariski closure $\bar{\mathbf{P}}_{n,d}$ consider a new functor $\mathcal{Q}_{n,d}$, which associates to a C -algebra $R \in \mathcal{R}_C$ the set of monic polynomials $F \in R[x]$ of degree d with the following property. Given F let $\rho_F : W_R^0 \times W_R^n \times W_R^{n-1} \rightarrow W_R^{d+n-1}$ be a linear map given by $(c, f, g) \mapsto cF'' + fF' + gF$. Then $F \in \mathcal{Q}_{n,d}(R)$ if and only if the initial Fitting ideal (see [38]) of ρ_F is the zero ideal in R . More explicitly we can write down a matrix M of the transformation ρ_F in the bases $(1, x, \dots, x^k)$ for the involved W_R^k . Then we require that all maximal minors (they are determinants of square submatrices of M of maximal size) of the matrix M vanish. The functor $\mathcal{Q}_{n,d}$ is representable by the ring $C[p_1, \dots, p_d]/I_F$, where I_F is the initial Fitting ideal of ρ_F with $F = x^d + p_1x^{d-1} + \dots + p_d \in C[p_1, \dots, p_d, x]$ being the universal monic polynomial of degree d . Let $\bar{\mathbf{P}}_{n,d} = \text{Spec } C[p_1, \dots, p_d]/I_F$. If M is the matrix of ρ_F for the universal F , then its maximal minors generate I_F .

Remark 2.3 The mentioned maximal minors have smaller degree in p_1, \dots, p_d than polynomials $E_{d-1,d}, \dots, E_{n+1,d}$, thus they could be easier to use for computations with $\mathbf{P}_{n,d}$ and $\mathbf{S}_{n,d}$'s. Note also that polynomials $E_{d,j}$'s do not define the Zariski closure of $\mathbf{P}_{n,d}$ in $\text{Spec } C[p_1, \dots, p_d]$ in general because the sequence $E_{d,d-1}, \dots, E_{d,2}$ usually is not regular in $C[p_1, \dots, p_d]$, thus they define also components of higher dimensions on the hypersurface $\Delta = 0$. For example, take $d = 4$. It can be shown that $\text{Spec } C[p_1, \dots, p_4]/(E_{4,3}, E_{4,2})$ contains a 3-dimensional variety of polynomials, which are squares of monic quadratic polynomials. Therefore equations $E_{d,k} = 0$ do not define the Zariski closure $\bar{\mathbf{P}}_{n,d}$.

It is easy to see that the closed points of $\mathbf{P}_{n,d}$ are exactly the points on $\bar{\mathbf{P}}_{n,d}$ which correspond to polynomials with non-zero discriminant, because if $F \in \mathcal{F}_d(C)$ then ρ_F has non-zero kernel exactly when the expression $F'' = -2vF' + \tilde{r}F$ with $\deg v \leq n$ exists. It is true in general that for any $R \in \mathcal{R}_C$ we have $\mathcal{P}_{n,d}(R) = \mathcal{Q}_{n,d}(R) \cap \mathcal{F}_d(R)$. To show that the set on the left-hand side is a subset of $\mathcal{P}_{n,d}(R)$ one needs the linear algebra lemma below. The submatrix M' in the current situation is the matrix of $W_R^n \times W_R^{n-1} \rightarrow W_R^{d+n-1}$ defined by $(f, g) \mapsto fF' + gF$. (Its maximal minors generate the unit ideal because otherwise there would be a specialization $R \rightarrow C$ such that the induced map $W_C^n \times W_C^{n-1} \rightarrow W_C^{d+n-1}$ would be singular in contradiction with the assumption that the discriminant of $F \in R[x]$ is invertible.) By the lemma below, the first column of M is a linear combination of columns of M' , or in other words, we can express $F'' = -2vF' + \tilde{r}F$.

Lemma 2.3.6 *Let M be a matrix over a ring R (commutative, with 1) of size $n \times (m+1)$ with $m < n$, and let M' be the submatrix of M of size $n \times m$ formed by the last m columns. Suppose that all maximal minors of M are 0, and that maximal minors of M' generate the unit ideal in R . Then the first column of M is a linear combination of the columns*

of M' .

Proof. Choose any m rows in M . Consider the linear combination of columns of M where the coefficient to the j th column is the minor formed by the chosen rows and all but the j th column. If the i th row is among the chosen ones, then the i th component of this linear combination is zero as it is the determinant of a matrix with two equal rows. Otherwise the i th component is also zero because it is equal (up to sign) to the maximal minor of M formed by the chosen and the i th rows. Thus the considered linear combination gives a linear dependence relation between columns of M , and its coefficient to the first column is the maximal minor of M' formed by the chosen rows. Since maximal minors of M' generate the unit ideal in R , the claim of the lemma follows. \square

Our next claim is that $\mathcal{Q}_{n,d}(C) \setminus \mathcal{P}_{n,d}(C)$ is the set of monic polynomials in $C[x]$ of degree d which have $\leq n$ distinct roots. Indeed, if $F \in \mathcal{Q}_{n,d}(C)$ but not in $\mathcal{P}_{n,d}(C)$ then it has zero discriminant, hence it is impossible to express $F'' = -2vF' + \tilde{r}F$ for any $v \in C[x]$. Then there should be v, \tilde{r} with $\deg v \leq n$ such that $-2vF' + \tilde{r}F = 0$, which implies that F has $\leq n$ distinct roots. It is easy to see that $\mathcal{Q}_{n,d}(C) \setminus \mathcal{P}_{n,d}(C)$ set-theoretically is the union of several algebraic varieties in $\text{Spec } C[p_1, \dots, p_d]$, namely for each solution of equations $k_1 + \dots + k_j = n$, $k_1 + 2k_2 + \dots + jk_j = d$ in non-negative integers we have a “subvariety” of $\mathcal{Q}_{n,d}(C) \setminus \mathcal{P}_{n,d}(C)$ parametrized by polynomials of the form $Q_{k_1} Q_{k_2}^2 \dots Q_{k_j}^j$, where Q_i must be monic of degree i . The following lemma is an important step in proving that $\bar{\mathbf{P}}_{n,d}$ is regular in codimension 1.

Lemma 2.3.7 $\bar{\mathbf{P}}_{n,d}$ is smooth at the points $F \in \mathcal{Q}_{n,d}(C) \setminus \mathcal{P}_{n,d}(C)$ such that the polynomial F of degree d has exactly n roots.

Proof. We need to show that $\bar{\mathbf{P}}_{n,d}$ has dimension $n + 1$ at these points, precisely as on the open subset $\mathbf{P}_{n,d}$. Take a point $F \in \mathcal{Q}_{n,d}(C) \setminus \mathcal{P}_{n,d}(C)$ and write $F = (x - \alpha_1)^{m_1} \dots (x - \alpha_n)^{m_n}$ with distinct $\alpha_1, \dots, \alpha_n \in C$. We need to know the dimension of the image of ρ_F . Note that polynomials $F, xF, \dots, x^{n-1}F, F', xF', \dots, x^n F'$ generate the subspace of $\text{Im } \rho_F \in W_C^{d+n-1}$ consisting of polynomials which are divisible by $\gcd(F, F') = \prod_{j=1}^n (x - \alpha_j)^{m_j-1}$. The dimension of this subspace is $2n$, and $F'' \in \text{Im } \rho_F$ does not lie in it. Hence the dimension of the image of ρ_F is $2n + 1$. We may conclude that the kernel of ρ_F is one-dimensional. This kernel is generated by the element $(0, v, \tilde{r}) \in W_C^0 \times W_C^n \times W_C^{n-1}$ with $v = (x - \alpha_1) \dots (x - \alpha_n)$. Let M_F be the matrix of ρ_F in the basis $1, x, \dots, x^k$ for the involved W_C^k .

Similarly as in the proposition 2.3.3 we identify the tangent space T_F at F with a subspace of polynomials G in W_C^{d-1} such that $F + \varepsilon G$ is in $\mathcal{Q}_{n,d}(C[\varepsilon])$. First we show that if $G \in T_F$ then we can express $vG' + \tilde{r}G$ as

$$vG' + \tilde{r}G = cF'' + wF' + sF \quad \text{for some } c \in C, w, s \in W_C^n. \quad (2.17)$$

Let $M_{F+\varepsilon G}$ be the matrix of $\rho_{F+\varepsilon G}$ in the similar basis as for M_F . Taking any $2n + 1$ rows of $M_{F+\varepsilon G}$ we can form an element of the kernel of $\rho_{F+\varepsilon G}$ whose components are determinants of $(2n + 1) \times (2n + 1)$ submatrices containing chosen rows, exactly in the same manner as in the proof of the lemma 2.3.6. Note that there is a $(2n + 1) \times (2n + 1)$ submatrix of $M_{F+\varepsilon G}$ whose determinant is a unit in $C[\varepsilon]$, because $M_{F+\varepsilon G}$ specializes

due to $\varepsilon \mapsto 0$ to the matrix M_F of rank $2n+1$. It follows that there is an element of form $(-\varepsilon s, v - \varepsilon w, \tilde{r} - \varepsilon s) \in W_{C[\varepsilon]}^0 \times W_{C[\varepsilon]}^n \times W_{C[\varepsilon]}^{n-1}$ in the kernel of $\rho_{F+\varepsilon G}$ which specializes to $(0, v, \tilde{r})$. From this element we easily form the expression (2.17).

Let T_F^0 be the subspace of T_F of polynomials G such that the expression (2.17) is possible with $c = 0$. Note that the right-hand side of (2.17) is divisible by the greatest common divisor of F and F' . If $G \in T_F$ then $\gcd(F, F')$ must also divide $vG' + \tilde{r}G$. We claim that this is possible only if $\gcd(F, F')$ divides G . Indeed, consider G and $vG' + \tilde{r}G$ locally at a root α_j of F with multiplicity $m_j \geq 2$. Suppose that $G = (x - \alpha_j)^k \tilde{G}$ with $k \geq 0$ and \tilde{G} not divisible by $x - \alpha_j$. Since

$$v = (x - \alpha_j) + \star(x - \alpha_j)^2 \quad \text{and} \quad \tilde{r} = -m_j + \star(x - \alpha_j)$$

(because of $vF' + \tilde{r}F = 0$), we have that $vG' + \tilde{r}G = (x - \alpha_j)^k(k - m_j + \star(x - \alpha_j))$. But α_j is a root of $\gcd(F, F')$ with multiplicity $m_j - 1$, thus $k \geq m_j - 1$. Therefore $\gcd(F, F')$ divides $vG' + \tilde{r}G$ only if it divides G .

It follows that T_F^0 is a subspace of W_C^{d-1} of polynomials which are divisible by $\gcd(F, F')$ of degree $n - d$. Hence $\dim T_F \leq n$. On the other hand, polynomials $G_i = F/(x - \alpha_i)$ for $i = 1, \dots, n$ are elements of T_Q because $F + \varepsilon m_i G_i$ can be factored over $C[\varepsilon]$ precisely like F but with the factor $(x - \alpha_i + \varepsilon)^{k_i}$ instead of $(x - \alpha_i)^{k_i}$. Hence the expression (2.17) can be derived from $vF' + \tilde{r}F$ with α_i replaced by $\alpha_i - \varepsilon$. One can check that the polynomials G_i are linearly independent by considering their orders of vanishing at roots of F . Therefore $\dim T_F^0 = n$.

Further, there exist $G_0 \in T_F \setminus T_F^0$. One can take

$$G_0 = - \sum_j \frac{m_j(m_j - 1)}{2} \frac{\gcd(F, F')}{x - \alpha_j} \notin T_F^0.$$

Considering the expression $vG_0' + \tilde{r}G_0 - F''$ locally at every root α_j of F with $m_j \geq 2$ it is easy to see that this expression is divisible by $\gcd(F, F')$, thus we can express it as $wF' + sF$ for some $w, s \in W_C^n$, thus $G_0 \in T_F$. Finally, $\dim T_F = \dim T_F^0 + 1$ because for $G \in T_F$ there exist a linear combination $G - cG_0$ (with $c \in C$) which lies in T_F^0 . Hence the dimension of T_F is $n + 1$. \square

As a result we have that $\bar{\mathbf{P}}_{n,d}$ can be singular only at points of $\mathcal{Q}_{n,d}(C)$ which correspond to polynomials F with $\leq n - 1$ roots. These points form a subscheme of codimension ≥ 2 . As a conclusion, $\bar{\mathbf{P}}_{n,d}$ is regular in codimension 1. Also we see that the constructed $\bar{\mathbf{P}}_{n,d}$ is indeed a Zariski closure of $\mathbf{P}_{n,d}$ in $\text{Spec } C[p_1, \dots, p_d]$ at least set-theoretically, if we mind possible embedded components in codimension ≥ 2 . If $\mathbf{P}_{n,d}$ is an irreducible variety, it is normal.

Now we are ready to prove the irreducibility of $\bar{\mathbf{P}}_{d-2,d}$. It implies immediately the irreducibility of $\mathbf{P}_{d-2,d}$ and $\mathbf{S}_{d-2,d}$.

Proposition 2.3.8 $\bar{\mathbf{P}}_{d-2,d}$ is irreducible.

Proof. We may consider the irreducibility of the geometric quotient $\bar{\mathbf{P}}_{d-2,d}/\mathbf{G}$. It is isomorphic to $\bar{\mathbf{P}}_{d-2,d}^0/\mathbf{G}_m$, where $\bar{\mathbf{P}}_{d-2,d}^0$ is the closed subvariety of $\bar{\mathbf{P}}_{d-2,d}$ defined by $p_1 = 0$ and is a quotient of $\bar{\mathbf{P}}_{d-2,d}$ by the non-reductive group \mathbb{G}_a . The quotient

$\bar{\mathbf{P}}_{d-2,d}/\mathbf{G}$ is regular in codimension 1, because so is $\bar{\mathbf{P}}_{d-2,d}$ and taking a quotient by an algebraic group does not add singularities in codimension 1, see [44]. Explicitly $\bar{\mathbf{P}}_{d-2,d}/\mathbf{G} \cong \text{Proj } C[p_1, \dots, p_d]/(E_{d,d-1}, p_1)$, where we set $\deg p_i = i$ (it differs by a sign from $\deg p_i$ defined by the action (2.11) of \mathbb{G}_m). We have $\bar{\mathbf{P}}_{d-2,d}/\mathbf{G}$ naturally embedded into the weighted projective space $\mathbb{P}(2, 3, \dots, d) = \text{Proj } C[p_2, \dots, p_d]$, with $\deg p_i = i$ again according to the action of \mathbb{G}_m . A weighted projective space is singular in general as the example of $\mathbb{P}(2, 3, 4)$ shows (see the next section), but it is normal and it is a quotient of the usual projective space \mathbb{P}^{d-2} by a finite group, see [22]. If $\bar{\mathbf{P}}_{d-2,d}/\mathbf{G}$ is reducible then the irreducible components are hypersurfaces in $\mathbb{P}(2, 3, \dots, d)$. They must intersect in codimension 1 because their preimages in \mathbb{P}^{d-2} by the finite covering $\mathbb{P}^{d-2} \rightarrow \mathbb{P}(2, 3, \dots, d)$ intersect in this way. On the other hand these hypersurface should intersect in the singular locus of $\bar{\mathbf{P}}_{d-2,d}/\mathbf{G}$ which has codimension ≥ 2 . This contradiction implies the irreducibility of $\bar{\mathbf{P}}_{d-2,d}/\mathbf{G}$ and $\bar{\mathbf{P}}_{d-2,d}$. \square

Example 2.4 Consider the variety $\mathbf{P}_{3,5} = \pi_F(\mathbf{S}_{3,5})$. We may set $p_1 = 0$ in the equation $E_{5,4} = 0$ defining the Zariski closure $\bar{\mathbf{P}}_{3,5}$. Then the equation $E_{5,4} = 0$ written in \mathbb{G}_m -invariant coordinates $z = p_4/p_2^2, w = p_3^2/p_2^3, t = p_5/p_2p_3$ is

$$54w^2 + 6250t^3w - 5625t^2w + 2250tzw - 315zw + 825tw + 8w \\ - 800z^3 + 2000tz^2 + 280z^2 - 900tz - 36z + 108t = 0.$$

It defines a hypersurface in \mathbb{P}^3 birationally isomorphic to $\mathbf{S}_{3,5}/\mathbf{G}$. This equation also defines an elliptic curve over the function field $C(t)$. Some transformations into a canonical equation of an elliptic curve are described in [11]. We change variables as

$$\tilde{z} = \frac{z + 375t^2}{(50t + 1)^2}, \quad \tilde{w} = \frac{108w + 6250t^3 - 5625t^2 + 2250tz - 315z + 825t + 8}{(50t + 1)^3}$$

and $\tilde{t} = t/(50t + 1)$, so that we obtain the following equation of a cubic surface in \mathbb{P}^3 with a singular point $(\tilde{z}, \tilde{w}, \tilde{t}) = (52/375, 0, 12/625)$:

$$\frac{1}{216}\tilde{w}^2 = 100 \left(\tilde{z} - 10\tilde{t} + \frac{4}{75} \right)^2 \left(8\tilde{z} - 105\tilde{t} + \frac{68}{75} \right) + \frac{1}{24} \left(9\tilde{z} - 115\tilde{t} + \frac{24}{25} \right)^2.$$

One can easily parametrize this cubic surface by the two-dimensional family of lines in \mathbb{P}^3 which pass through the singular point, because such a line in general intersects the cubic surface in one non-singular point. For example, a birational parametrization is:

$$\tilde{z} = \frac{\eta(\xi - \eta + 1)(2\xi - 21)}{3000\xi} + \frac{52}{375}, \quad \tilde{t} = \frac{\eta(\xi - \eta + 1)(\xi - 8)}{15000\xi} + \frac{12}{625}$$

and $\tilde{w} = \eta(\xi - \eta + 1)(\xi - 2\eta + 1)/200\xi$. Further, one can express coefficients p_2, p_3, p_4, p_5 in ξ, η and parametrize almost all \mathbf{G} -equivalence classes of $\mathcal{S}_{3,5}(C)$. One should additionally regard those points on $\mathbf{S}_{3,5}$ which are blown-down by birational morphisms we used, have non-trivial stabilizers in \mathbf{G} , or correspond to infinite values of parameters. Some subvarieties of the parametric space correspond to points in $\mathbf{P}_{2,5}$ or outside \mathbf{F}_5 .

2.4 $\mathbf{S}_{n,d}$ with $n = 2$

It was mentioned that our varieties $\mathbf{S}_{n,d}$ with $n = 1$ were considered in [47]. The next easiest case is $n = 2$ which we consider here. The results are summarized in the following theorem. The first part (i) of it is covered by the main result of the last section. Nevertheless, its proof presented here is an integral part of the whole proof of all three statements, and presents an approach how to “compute” $\mathbf{S}_{n,d}$ for small n .

Theorem 2.4.1 (i) *The morphism $\pi_v : \mathbf{S}_{2,d} \rightarrow \mathbf{V}_2$ is finite of degree $d + 1$.*

(ii) *$\mathbf{S}_{2,d}$ is irreducible.*

(iii) *The quotient $\mathbf{S}_{2,d}/\mathbf{G}$ is isomorphic to $\mathbf{K}_d \setminus \mathbf{B}_d$, where \mathbf{K}_d is a complete smooth curve of genus $\lceil \frac{d(d-4)}{12} \rceil$, and \mathbf{B}_d — a set of $\lceil \frac{d+1}{2} \rceil$ points on \mathbf{K}_d . (As usual, $\lceil x \rceil$ for rational x denotes the smallest integer such that $x \leq \lceil x \rceil$.)*

Proof. Let $R \in \mathcal{R}_C$. For a polynomial $v = a_2x^2 + a_1x + a_0 \in \mathcal{V}_2(R)$ consider a linear operator $L_v : W_R^d \rightarrow W_R^d$ defined by

$$L_v(G) = G'' + 2(a_2x^2 + a_1x + a_0)G' - 2da_2xG. \quad (2.18)$$

We use the basis $(x^d, \dots, x, 1)$ of W_R^d in this proof. Note that if $\lambda \in R$ and $F \in \mathcal{F}_d(C)$ are such that $(v, F, v' + v^2 + 2da_2x + \lambda) \in \mathcal{S}_{2,d}(R)$, then $L_v(F) = \lambda F$. One may say that λ is an eigenvalue of L_v and F — a corresponding eigenvector, but these notions are not unambiguously generalized to the general ring-theoretical contest. We use the notion of the characteristic polynomial of an endomorphism of a free module over a ring defined in [38]. In our situation, an “eigenvalue” $\lambda \in R$ with a monic “eigenvector” F must be a root of the characteristic polynomial $\det(\lambda - L_v)$ of L_v , because monic F shows that the first column of the matrix of $\lambda - L_v$ in the chosen basis is an R -linear combination of the remaining columns. We claim that every root $\lambda \in R$ of the characteristic polynomial of L_v gives exactly one element of $\mathcal{S}_{2,d}(R)$ with $r = v' + v^2 + 2da_2x + \lambda$. Let M' be the matrix formed by deleting the first column from the matrix of $\lambda - L_v$. Note that for any $\lambda \in R$ the polynomials $\lambda x^k - L_v(x^k)$ for $k = 0, \dots, d-1$ have different degrees and invertible leading coefficients. Hence if a monic “eigenvector” for λ exists, it is unique. Also it shows that the submatrix of M' formed by the first d rows is lower-triangular with invertible entries on its diagonal, hence the maximal minors of M' generate the unit ideal in R . If $\det(\lambda - L_v) = 0$ then we apply the lemma 2.3.6 to conclude that the first column of $\lambda - L_v$ is a linear combination of columns of M' , or in other words, there exists a monic “eigenvector” F and the required element of $\mathcal{S}_{2,d}(R)$.

It follows that the functor $\mathcal{S}_{n,d}$ is equivalent to a functor, which assigns to R the set of pairs (v, λ) with $v \in \mathcal{V}_2(R)$ and $\lambda \in R$ is a root of the characteristic polynomial of L_v . This functor is represented by the ring $\tilde{R} = C[a_2, a_1, a_0, \lambda, a_2^{-1}]/(U_d)$, where $U_d = \det(\lambda - L_v)$ is the characteristic polynomial of L_v for the universal v of \mathcal{V}_2 . This ring is a finite $C[a_2, a_1, a_0, a_2^{-1}]$ module of rank $d + 1$, because U_d is of this degree in λ . The same holds for the isomorphic ring $\mathcal{O}(\mathbf{S}_{2,d})$. The first part is proved.

Consider the Zariski closure $\tilde{\mathbf{S}}_{2,d}$ of $\mathbf{S}_{2,d}$ in $\text{Spec } C[a_2, a_1, a_0, \lambda]$ and the geometric quotient $\tilde{\mathbf{S}}_{2,d}/\mathbf{G}$. The Zariski closure $\tilde{\mathbf{S}}_{2,d}$ is isomorphic to $\text{Spec } C[a_2, a_1, a_0, \lambda]/(U_d)$. We need some explicit information about U_d . Consider the matrix of $\lambda - L_v$ in the basis $(x^d, \dots, x, 1)$ of W_R^d . It has entries in $C[a_2, a_1, a_0, \lambda]$. The entries on the main diagonal

(from the top-left corner) are $\lambda - 2da_1, \lambda - 2(d-1)a_1, \dots, \lambda - 2a_1, \lambda$; the entries on the diagonal just above it are $2a_2, 4a_2, \dots, 2da_2$ and other entries above the main diagonal are zero. It follows that $U_d = \det(\lambda - L_v)$ has the form

$$U_d = \lambda(\lambda - 2a_1)(\lambda - 4a_1) \dots (\lambda - 2da_1) + \{\text{terms divisible by } a_2\}. \quad (2.19)$$

Let us denote $\tilde{U}_d = \lambda(\lambda - 2a_1)(\lambda - 4a_1) \dots (\lambda - 2da_1)$.

The expression (2.19) shows that $\bar{\mathbf{S}}_{2,d}$ is smooth at points with $a_2 = 0$, $a_1 \neq 0$, $\lambda \in \{0, 2a_1, \dots, 2da_1\}$. Since $\bar{\mathbf{S}}_{2,d}$ is smooth on the open $a_2 \neq 0$, singularities of $\bar{\mathbf{S}}_{2,d}$ can occur only on the line $a_2 = a_1 = \lambda = 0$. In other words $\bar{\mathbf{S}}_{2,d}$ is regular in codimension 1.

From the definition (2.18) of L_v we deduce that the non-reductive subgroup $\mathbb{G}_a \subset \mathbf{G}$ of transformations $x \mapsto x + \gamma$ acts on the coordinates of $\bar{\mathbf{S}}_{2,d}$ as follows:

$$a_2 \mapsto a_2, \quad a_1 \mapsto a_1 + 2a_2\gamma, \quad a_0 \mapsto a_0 + a_1\gamma + a_2\gamma^2, \quad \lambda \mapsto \lambda + 2da_2\gamma.$$

One can compute that the \mathbb{G}_a -invariant functions

$$z_2 = \lambda - da_1, \quad z_3 = a_2, \quad z_4 = a_1^2 - 4a_0a_2 \quad (2.20)$$

generate the coordinate ring $C[z_2, z_3, z_4]/(U_d)$ of the quotient $\bar{\mathbf{S}}_{2,d}^0 = \bar{\mathbf{S}}_{2,d}/\mathbb{G}_a$. Further, the group $\mathbb{G}_m \cong \mathbf{G}/\mathbb{G}_a$ of transformations $x \mapsto \beta x$ acts on $\bar{\mathbf{S}}_{2,d}^0$ so that $z_i \mapsto \beta^i z_i$ for $i = 2, 3, 4$. It follows that the quotient $\bar{\mathbf{S}}_{2,d}/\mathbf{G}$ exists and is isomorphic to $\bar{\mathbf{S}}_{2,d}^0/\mathbb{G}_m \cong \text{Proj } C[z_2, z_3, z_4]/(U_d)$, where we set $\deg z_i = i$. The polynomial U_d is homogeneous of degree $2d + 2$ as an element of $C[z_2, z_3, z_4]$.

Note that $\bar{\mathbf{S}}_{2,d}/\mathbf{G}$ is regular in codimension 1 because so is $\bar{\mathbf{S}}_{2,d}$. Moreover, $\bar{\mathbf{S}}_{2,d}/\mathbf{G}$ has dimension 1, hence it is smooth.

We constructed $\bar{\mathbf{S}}_{2,d}/\mathbf{G}$ together with an embedding into the weighted projective space $\mathbb{P}(2, 3, 4) = \text{Proj } C[z_2, z_3, z_4]$. As a matter of fact, $\mathbb{P}(2, 3, 4)$ has two singular points $z_2 = z_3 = 0$ and $z_2 = z_4 = 0$. If the smooth $\bar{\mathbf{S}}_{2,d}/\mathbf{G}$ contains one of these points, it must be defined at least by two equations on an open neighbourhood of it. For example on the open set $z_3 \neq 0$ the $\mathbb{P}(2, 3, 4)$ is isomorphic to $\text{Spec } C[y_1, y_2, y_3]/(y_2^3 - y_1y_3)$ by $y_1 = z_2^3/z_3^2$, $y_2 = z_2z_4/z_3^2$, $y_3 = z_4^3/z_3^4$. The ring of regular functions on the open $z_3 \neq 0$ of \mathbf{K}_d is isomorphic to $C[y_1, y_2, y_3]/(y_2^3 - y_1y_3, U_d/z_3^{2k})$ if $d = 3k - 1$, or to

$$C[y_1, y_2, y_3]/(y_2^3 - y_1y_3, z_2^{2-i}U_d/z_3^{2k+2}, z_4^{1+i}U_d/z_3^{2k+2}) \quad (2.21)$$

if $d = 3k + i$ with $i = 0$ or 1 .

Like in the proof of the proposition 2.3.8 we note that $\mathbb{P}(2, 3, 4)$ is a quotient of \mathbb{P}^2 by a finite group (namely by the 12th roots of unity in \mathbb{G}_m). If $\bar{\mathbf{S}}_{2,d}/\mathbf{G}$ is reducible, then its irreducible components are complete curves in $\mathbb{P}(2, 3, 4)$ and they must intersect, because their preimages by the finite covering $\mathbb{P}^2 \rightarrow \mathbb{P}(2, 3, 4)$ intersect in \mathbb{P}^2 . But the intersection of irreducible components contradicts the smoothness of $\bar{\mathbf{S}}_{2,d}/\mathbf{G}$. Therefore $\bar{\mathbf{S}}_{2,d}/\mathbf{G}$, and as a consequence $\bar{\mathbf{S}}_{2,d}$ and $\mathbf{S}_{2,d}$ are irreducible.

For the last statement of the proposition we take $\mathbf{K}_d = \bar{\mathbf{S}}_{2,d}/\mathbf{G}$. It is a complete and smooth curve. The open subset $z_3 \neq 0$ of \mathbf{K}_d is isomorphic to $\mathbf{S}_{2,d}/\mathbf{G}$ because the ring of regular functions on this open set of \mathbf{K}_d (like (2.21) for instance) is isomorphic to the ring of \mathbf{G} -invariant functions on $\mathbf{S}_{2,d}$. The complement of $\mathbf{S}_{2,d}/\mathbf{G}$ in \mathbf{K}_d is a set

of points with $z_3 = 0$. To find these points we have to rewrite (2.19) in the coordinates z_2, z_3, z_4 . First we replace $\lambda = z_2 + da_1$ and combine factors $z_2 + ka_1$ and $z_2 - ka_1$ ($k = d, d-2, \dots, 2$ or 1) in the part denoted by \tilde{U}_d to obtain the expression

$$U_d = (z_1^2 - d^2 a_1^2)(z_1^2 - (d-2)^2 a_1^2) \dots (z_1^2 - a_1^2 \text{ or } z_1) + \{\text{terms divisible by } a_2\}.$$

Since $a_1^2 = z_4 + 4a_0 a_2$, the polynomial U_d in z_2, z_3, z_4 has finally a form

$$\begin{aligned} (z_2^2 - z_4)(z_2^2 - 3^2 z_4) \dots (z_2^2 - d^2 z_4) + \{\text{terms divisible by } z_3\} & \quad \text{for odd } d, \\ z_2(z_2^2 - 2^2 z_4) \dots (z_2^2 - d^2 z_4) + \{\text{terms divisible by } z_3\} & \quad \text{for even } d. \end{aligned}$$

Each factor in the product similar to \tilde{U}_d gives a point on \mathbf{K}_d with $z_3 = 0$. Thus we have $\lceil \frac{d+1}{2} \rceil$ such points in total. It remains only to compute the genus of \mathbf{K}_d .

We consider the finite morphism $\bar{\pi}_v : \mathbf{K}_d \rightarrow \mathbb{P}^1$ defined by $(z_2 : z_4 : z_3) \mapsto (z_4^3 : z_3^2)$. On the open set $z_3 \neq 0$ it is the morphism between the quotients $\mathbf{S}_{2,d}/\mathbf{G} \rightarrow \mathbf{V}_2/\mathbf{G}$ induced by the finite morphism $\pi_v : \mathbf{S}_{2,d} \rightarrow \mathbf{V}_2$. The morphism $\bar{\pi}_v$ has also degree $d+1$, because the extension of function fields of curves $C(z_3^4/z_4^3, z_2 z_3^2/z_4^2)/(z_3^{d+1} U_d/z_4^{2d+2}) : C(z_3^4/z_4^3)$ has this degree. To find the genus of \mathbf{K}_d we compute the degree of the ramification divisor D of $\bar{\pi}_v$ on \mathbf{K}_d and then apply the Hurwitz formula.

The number of points on \mathbf{K}_d with $z_3 = 0$ is already computed and is equal to $\lceil \frac{d+1}{2} \rceil$. Therefore the points on the fiber of $\bar{\pi}_v$ over $(1 : 0) \in \mathbb{P}^1$ contribute $\lceil \frac{d}{2} \rceil$ to the degree of the ramification divisor D .

The ramification locus of π_v on $\mathbf{S}_{2,d}$ is given by $\partial U_d / \partial \lambda = 0$ (or the same $\partial U_d / \partial z_2 = 0$). Set-theoretically it is a union of two-dimensional \mathbf{G} -orbits along which π_v ramifies. Let J be the ideal $(U_d, \partial U_d / \partial z_2) \in C[z_2, z_3, z_4]$. Consider the \mathbf{G} -orbit in \mathbf{V}_2 defined by $z_4 = 0$ and the ramification of π_v above it. We can write the polynomial U_d in the form

$$U_d = z_2^{m_0} (z_2^3 - t_1 z_3^2)^{m_1} \dots (z_2^3 - t_k z_3^2)^{m_k} + z_4 \bar{H}_{2d-2}, \quad (2.22)$$

where $\{t_1, \dots, t_k\} \subset C^*$ are distinct, $m_0 + 3m_1 + \dots + 3m_k = d+1$, and $\bar{H}_{2d-2} \in C[z_2, z_3, z_4]$ is a homogeneous polynomial of degree $2d-2$. A factor $(z_2^3 - t_j z_3^2)^{m_j}$ in (2.22) gives a ramified \mathbf{G} -orbit Z_j if and only if $m_j \geq 2$. For a ramified orbit Z_j let \mathcal{O}_{Z_j} be the ring $\mathcal{O}(\mathbf{S}_{2,d})$ localized at the ideal of Z_j . It is a regular local ring of dimension 1, hence a discrete valuation ring. Let \mathfrak{m} be the maximal ideal of \mathcal{O}_{Z_j} . It is generated by $z_2^3 - t_j z_3^2$ because the local parameter z_4 is not a generator of \mathfrak{m} . From (2.22) we easily see that the function z_4 has order m_j at \mathfrak{m} (e.g. $z_4 \in \mathfrak{m}^{m_j} \setminus \mathfrak{m}^{m_j+1}$) and the function $\partial U_d / \partial z_2$ has order $m_j - 1$. Hence scheme-theoretically the orbit Z_j has multiplicity $m_j - 1$ as a component of $\text{Spec } C[z_2, z_3, z_4]/J$. Similarly π_v ramifies along the \mathbf{G} -orbit Z_0 defined by $z_2 = z_4 = 0$ precisely when $m_0 \geq 2$. Then Z_0 has multiplicity $m_0 - 1$ in $\text{Spec } C[z_2, z_3, z_4]/J$.

The discriminant Q of U_d with respect to z_2 (or λ) is the resultant of polynomials $U_d, \partial U_d / \partial z_2$ with respect to z_2 . It is also the norm of $\partial U_d / \partial z_2$ as an element of the finite $C[z_3, z_4]$ -module $C[z_2, z_3, z_4]/(U_d)$. The principal ideal $(Q) \in C[z_3, z_4]$ is the first (with respect to z_2) elimination ideal of J , that means $(Q) = J \cap C[z_3, z_4]$, see [14]. The discriminant Q is homogeneous in the grading of $C[z_3, z_4]$ defined by $\deg z_i = i$ and has degree $2d(d+1)$ because U_d is of degree $d+1$ in z_2 , and $\deg z_2 = 2$. Further, Q factors completely into factors like $z_4^3 - s z_3^4$ ($s \in C^*$) of degree 12 and factors z_4 of degree 4.

These factors correspond to \mathbf{G} -orbits in \mathbf{V}_2 above which π_v ramifies. We claim that the power r_0 of z_4 in Q is equal to $d - 3k + \{1 \text{ if } m_0 = 0\}$ when U_d has form (2.22). Indeed, the power to z_4 in Q is equal to the sum of multiplicities of the components Z_0, Z_1, \dots, Z_k in $\text{Spec } C[z_2, z_3, z_4]/J$, thus $r_0 = \max(0, m_0 - 1) + 3(m_1 - 1) + \dots + 3(m_k - 1) = d - 3k + \{1 \text{ if } m_0 = 0\}$. As a consequence, the number r_1 of factors of the form $z_4^3 - sz_3^4$ counted with multiplicities is equal to $(2d(d+1) - 4e_0)/12 = (2d(d-1) - \{4 \text{ if } m_0 = 0\})/12 + k$. Since r_1 is an integer, $m_0 = 0$ if $d = 2 \pmod 3$ and $m_0 > 0$ otherwise. With this information we can write $r_1 = \lfloor \frac{d(d-1)}{6} \rfloor + k$.

Consider now the ramification of $\bar{\pi}_v$ on the open $z_3z_4 \neq 0$. The coordinate ring of \mathbf{K}_d over this open set is isomorphic to $C[y_1, y_2, y_1^{-1}]/(\tilde{U}_d)$ where $y_1 = z_4^3/z_3^4, y_2 = z_2z_4/z_3^2$ and \tilde{U}_d is $z_4^{d+1}U_d/z_3^{2d+2}$ written in y_1, y_2 . The ramification divisor D on this open set is principal and is given by the function $\partial\tilde{U}_d/\partial y_2$. The push-forward of D (restricted to $z_3z_4 \neq 0$) by $\bar{\pi}_v$ is given by the discriminant of \tilde{U}_d with respect to y_2 . As an element of $C[z_3, z_4, z_3^{-1}, z_4^{-1}]$ it is equal up to powers of z_3 and z_4 to the previous discriminant Q . In particular, it has r_1 factors counted with multiplicities of the form $z_4^3 - sz_3^4$. Each such factor gives a ramification point of $\bar{\pi}_v$ over the corresponding point $(s : 1) \in \mathbb{P}^1$ and contributes 1 to the degree of D . Thus the degree of D restricted to the open $z_3z_4 \neq 0$ is r_1 .

It remains to take into account the ramified points with $z_4 = 0$. When U_d has the form (2.22) we have $(k + \{1 \text{ if } m_0 > 0\})$ distinct points on \mathbf{K}_d on the fiber of $\bar{\pi}_v$ over $(0 : 1) \in \mathbb{P}^1$. We noted that the condition $m_0 > 0$ can be replaced by $d \neq 2 \pmod 3$. Finally we can compute the degree of the ramification divisor:

$$\deg D = \left\lfloor \frac{d}{2} \right\rfloor + r_1 + (d + 1 - k - \{1, \text{ if } d \neq 2 \pmod 3\}) = \left\lfloor \frac{d(d+8)}{6} \right\rfloor$$

(this formula holds for $d = 0, 1, \dots, 5 \pmod 6$). Now it is straightforward to apply the Hurwitz formula and compute the genus of \mathbf{K}_d . The answer is $\lceil \frac{d(d-4)}{12} \rceil$. \square

Example 2.5 Let us have a look at some examples of \mathbf{K}_d and $\mathbf{S}_{2,d}$. They are defined by $U_d = 0$ in $\mathbb{P}(2, 3, 4)$. If one chooses the basis $(x + \frac{a_1}{2a_2})^d, \dots, x + \frac{a_1}{2a_2}, 1$ for W_R^d then the entries in the characteristic matrix of $\lambda - L_v$ for the general polynomial v would be functions in \mathbb{G}_a -invariant z_2, z_3, z_4 defined by (2.20). The characteristic matrix of $\lambda - L_v$ in this basis contains non-zero entries only on four diagonals:

- On the main diagonal: all the entries are $z_2 = \lambda - da_1$.
- On the diagonal right above the main diagonal: the entries from the left are $2z_3, 4z_3, \dots, 2dz_3$.
- On the diagonal right below the main diagonal: the entries from the left are $dz_4/(2z_3), (d-1)z_4/(2z_3), \dots, z_4/(2z_3)$.
- On the diagonal right below the previous diagonal: the entries from the left are $-d(d-1), -(d-1)(d-2), \dots, -6, -2$.

Here is the list of polynomials U_d for $d \leq 7$ in coordinates z_2, z_4 and $z_6 = -16z_3^2$.

$$\begin{aligned} U_1 &= z_2^2 - z_4, \\ U_2 &= z_2(z_2^2 - 4z_4) + z_6, \end{aligned}$$

$$\begin{aligned}
U_3 &= (z_2^2 - z_4)(z_2^2 - 9z_4) + 6z_2z_6, \\
U_4 &= z_2(z_2^2 - 4z_4)(z_2^2 - 16z_4) + 3(7z_2^2 - 16z_4)z_6, \\
U_5 &= (z_2^2 - z_4)(z_2^2 - 9z_4)(z_2^2 - 25z_4) + 8(7z_2^2 - 55z_4)z_2z_6 + 100z_6^2, \\
U_6 &= z_2(z_2^2 - 4z_4)(z_2^2 - 16z_4)(z_2^2 - 36z_4) + 18(z_2^2 - 16z_4)(7z_2^2 - 12z_4)z_6 + 1125z_2z_6^2, \\
U_7 &= (z_2^2 - z_4)(z_2^2 - 9z_4)(z_2^2 - 25z_4)(z_2^2 - 49z_4) + 36(7z_2^4 - 230z_2^2z_4 + 1183z_4^2)z_2z_6 \\
&\quad + 36(191z_2^2 - 686z_4)z_6^2.
\end{aligned}$$

Given a closed point $(z_2 : z_4 : z_6)$ with $z_6 \neq 0$ on one of the curves \mathbf{K}_d one can easily find an element $(v, F, r) \in \mathcal{S}_{2,d}(C)$ in a \mathbf{G} -equivalence class corresponding to this point. One can take for instance $v = (x^2 - ax + b)/c$ with $a = 2z_2/d$, $b = z_2^2/d^2 - z_4$, $c = z_6/2$, and $r - v' - v^2 = 2d(x - a)/c$. Then

$$F = x^d + \frac{d}{2}bx^{d-2} + \left(\frac{d}{3}ab + \frac{d(d-1)}{6}c\right)x^{d-3} + \dots, \quad (2.23)$$

where the coefficients p_i of F for $i > 2$ are defined recursively by

$$(k+1)p_{k+1} = akp_k + b(d-k+1)p_{k-1} + c\frac{(d-k+1)(d-k+2)}{2}p_{k-2}. \quad (2.24)$$

If one tries to compute F in (2.23) for a point $(z_2 : z_4 : z_6) = (md : d^2 : 0) \in \mathbf{K}_d$ (where $m = d, d-2, \dots, 1$ or 0), then one should get the polynomial

$$F = (x - d - m)^{\frac{d-m}{2}} (x + d - m)^{\frac{d+m}{2}}.$$

Indeed, one can check that the coefficients of this polynomial satisfy (2.24) using the fact that such F satisfies $(x^2 - ax + b)F' + d(x - a)F = 0$ for $a = 2m$, $b = m^2 - d^2$. This observations is compatible with the description of the Zariski closure of $\mathbf{P}_{n,d}$ in $\text{Spec } C[p_1, \dots, p_n]$ in the previous section, with one exception that the point with $m = d$ "should" give the polynomial (2.9) in $\mathcal{S}_{1,d}(C)$.

One obtains especially simple expressions for elements of $\mathcal{S}_{2,d}(C)$ which correspond to points on \mathbf{K}_d with $z_2 = z_4 = 0$. They occur if $d \not\equiv 2 \pmod{3}$ as we saw in the proof of (2.4.1). For example, such point on \mathbf{K}_7 gives the second order linear differential equation $y'' = (x^4 + 16x)y$ which has a Liouvillian solution $y = (x^7 + 7x^4 + 7x) \exp(x^3/3)$.

The curves \mathbf{K}_d for $d \leq 4$ are rational by the proposition 2.4.1. Thus we can parametrize them or the whole $\mathbf{S}_{2,d}$. For $d \leq 3$ the variety $\mathbf{S}_{2,d}$ can be parametrized using the isomorphism with $\mathbf{F}_d \times \mathbf{V}_{2-d}$ (by the proposition 2.3.2) or with an open set of \mathbf{F}_d . As an example, one can parametrize a set of all representatives of $\mathbf{S}_{2,4}/\mathbf{G}$ as follows:

$$\begin{aligned}
(v, F, r - v' - v^2) &= \left(\frac{t+1}{t(t-1)}(x^2 + x) + \frac{3}{4} \frac{t+1}{t}, \right. \\
&\quad \left. x^4 + \frac{3}{2}(t-1)x^2 + \frac{(t-1)^2}{t+1}x + \frac{3}{16} \frac{(3t-1)(t-1)^2}{t+1}, \frac{8(t+1)}{t(t-1)}(x+1) \right).
\end{aligned}$$

By the proposition (2.4.1) $\mathbf{S}_{2,4}/\mathbf{G}$ is isomorphic to $\mathbb{A}^1 \setminus \{0, 1\}$. But the above formula does not give the answer for parameter $t = -1$, which could be chosen $(v, F, r) =$

$(x^2, x^4 + 2x, x^4 + 10x)$. Probably a closed form expression for a set of representatives of all \mathbf{G} -equivalence classes of $\mathcal{S}_{2,4}(C)$ does not exist (the same hold for $\mathbf{S}_{2,3}$). This reminds the fact that there does not exist a universal family of elliptic curves over the j -line with less than 3 bad fibers.

The curves \mathbf{K}_5 and \mathbf{K}_6 have genus 1, thus $\mathbf{S}_{2,5}$ and $\mathbf{S}_{2,6}$ turn out to be the first non-unirational examples of the schemes classifying desired Riccati equations. These curves are isomorphic to the following smooth cubic curves in Weierstrass form (an isomorphism up to $\pm w$ could be constructed by the given t):

$$\begin{aligned} \mathbf{K}_5 : \quad w^2 &= t^3 + 10t^2 + 5t & \text{by } t &= -\frac{5}{4z_2^2} (z_2^2 - 5z_4), \\ \mathbf{K}_6 : \quad w^2 &= t^3 + 25t^2 - 25t + 275 & \text{by } t &= 20 \frac{z_2^2 - z_4}{z_2^2 - 16z_4}. \end{aligned}$$

Given a point (t, w) on \mathbf{K}_5 , one can easily find a representative of $\mathcal{S}_{5,2}(C)$ which corresponds to it:

$$\begin{aligned} (v, F, r - v' - v^2) &= \left(\frac{\frac{1}{2}x^2 - x - 2(t+1)}{11t + 3w + 5}, x^5 - 10(t+1)x^3 + 20(3t + w + 1)x^2 + \right. \\ &\quad \left. + 30(t^2 + 5t + w + 2)x - 4(45t^2 + 17tw + 20t + 5w - 1), \frac{5(x-2)}{11t + 3w + 5} \right). \end{aligned}$$

The quotient $\mathbf{S}_{2,5}/\mathbf{G}$ is isomorphic to $\mathbf{K}_5 \setminus \{(-1, 2), (5, -20), (-5/9, 10/27)\}$ — the three points lie on the line $11t + 3w + 5 = 0$. The point at infinity is discarded by the last formula. It corresponds to

$$(v, F, r) = \left(\frac{1}{6}(x^2 - 4), x^5 - 10x^3 + 20x^2 + 30x - 68, \frac{1}{36}(x^2 - 4)^2 + 2x \right).$$

Similarly, one can construct elements of $\mathcal{S}_{6,2}(C)$ from a point $(t, w) \in \mathbf{K}_6$ starting for example with v and $r - v' - v^2$ equal respectively to

$$\frac{2/27}{15t - 2w + 15} \left(\frac{x^2}{4t - 5} + x - \frac{5}{4}(t - 35) \right) \quad \text{and} \quad \frac{8/9}{15t - 2w + 15} \left(\frac{x}{4t - 5} + 1 \right).$$

The complement of $\mathbf{S}_{2,6}/\mathbf{G}$ in \mathbf{K}_6 consists of points on the line $15t - 2w + 15 = 0$ and the point at infinity. Again, one point $(t, w) = (5/4, -135/8)$ is “missing” by the obtained formula.

The curve \mathbf{K}_7 is hyperelliptic of genus 2, birationally isomorphic to

$$w^2 = t(t^5 + 40t^4 + 440t^3 + 1520t^2 + 1960t - 3024) \quad \text{by } t = \frac{24z_2^2}{z_2^2 - 49z_4}.$$

The curves \mathbf{K}_d with $d > 7$ are of greater genus.

As it is easy to see, the schemes $\mathbf{S}_{2,d}$ and curves \mathbf{K}_d are actually defined over \mathbb{Q} , even over \mathbb{Z} . An interesting question is to describe $\mathcal{S}_{2,d}(\mathbb{Q})$ — the set of triples (v, F, r) of polynomials in $\mathbb{Q}[x]$ which define solutions of Riccati equations of the same form as the

definition of $\mathcal{S}_{2,d}$ requires. Having a \mathbb{Q} -rational point on \mathbf{K}_d (with $z_3 \neq 0$) one can easily construct an element of $\mathcal{S}_{2,d}(\mathbb{Q})$ as in (2.23). Some \mathbf{G} -equivalent points in $\mathcal{S}_{2,d}(\mathbb{Q})$ are \mathbf{G} -equivalent only by an element of \mathbf{G} which is not defined over \mathbb{Q} . For example take $(x^2, x^3 + 1, x^4 + 8x)$ and $(x^2/2, x^3 + 2, x^4/4 + 4x)$ in $\mathcal{S}_{2,3}(\mathbb{Q})$. The \mathbb{Q} -rational points on \mathbf{K}_d for $d \leq 4$ are parametrized exactly in the same way as over C . The curves \mathbf{K}_5 and \mathbf{K}_6 are elliptic (if we take the points at infinity in a Weierstrass model as origin). The author used the `apecs` package for Maple to compute that the Mordell-Weil rank of both curves is 1 (assuming some standard conjectures in the case of \mathbf{K}_6), generated by points $(t, w) = (-1, 2)$ and $(35, 270)$ respectively. Additionally \mathbf{K}_5 has one non-trivial torsion point $(t, w) = (0, 0)$. The curves \mathbf{K}_d for $d \geq 7$ have finitely many rational points by the Faltings theorem (Mordell conjecture until 1983). For such d , elements in $\mathbf{S}_{2,d}(\mathbb{Q})$ are \mathbf{G} -equivalent to finitely many representatives. The points on \mathbf{K}_7 known to the author have $z_2 = 0$ or $z_4/z_2^2 \in \{1, 1/9, 1/25, 1/49, 9/49, 161/686\}$.

One can reduce the curves \mathbf{K}_d or the equations $U_d = 0$ modulo primes in \mathbb{Z} . Reduction of curves over \mathbb{Q} modulo primes is useful in studying their arithmetical properties, and in our situation, reduction of curves \mathbf{K}_d modulo primes $p > 2$ gives information about differential equations of form (2.1) with Liouvillian solutions with respect to $\mathbb{F}_p(x)$. Let p be a prime number, $p \neq 2$. We can obtain $U_d \bmod p$ first reducing the described matrix of $\lambda - L_v$ modulo p , and then performing substitutions (2.20) and $z_6 = -16z_3^2$ in its determinant. Let $M_{p,d}$ denote the reduced matrix of $\lambda - L_v$ and let $k = d \bmod p$. If $d \geq p$ then zeroes appear on the diagonal above and two diagonals below the main diagonal so that the matrix $M_{p,d}$ splits into a sequence of square blocks of size $k + 1$ and $p - k - 1$ alternatively on the main diagonal (with some non-zero entries outside these blocks, which do not affect the determinant however). A block of size $k + 1$ is easily identified with $M_{p,k}$, and of size $(p - k - 1)$ — with $M_{p,p-k-2}$, if we set $U_0 = z_2$, $U_{-1} = 1$ for convenience. It follows, that U_d factors modulo p :

$$U_d \equiv (U_k)^{\frac{d-k}{p}+1} (U_{p-k-2})^{\frac{d-k}{p}} \pmod{p}, \quad \text{where } k = d \bmod p.$$

This observation might be useful in studying differential equations (2.1) in $\mathbb{F}_p(x)$. Note that the given proof of proposition 2.3.3 can be adopted (with obvious reformulations of functors for \mathbb{F}_p -algebras instead of C -algebras) to prove that $\mathbf{S}_{2,d}$ is smooth if the base field has characteristic $p > d$. Also a part of the proof 2.4.1 is directly applicable to show that \mathbf{K}_d is smooth and irreducible in characteristic $p > d$. In this sense \mathbf{K}_d , as a curve over \mathbb{Q} , has good reduction at primes $p > d$.

2.5 Projection to the coefficients of v

In this section the part (iii) of the main results in the theorem 2.1.3 is proved. It is equivalent to the statement that the representing ring of $\mathcal{S}_{n,d}$ is a finite free module of degree $\binom{n+d-1}{d}$ over the ring $\mathcal{O}(\mathbf{V}_n) \cong C[a_n, \dots, a_0, a_n^{-1}]$. It implies in particular that for any polynomial $v \in \mathcal{V}_n(C)$ the set of elements $(v, F, r) \in \mathcal{S}_{n,d}(C)$ with fixed v is finite, of cardinality $\leq \binom{n+d-1}{d}$. Moreover, since the underlying scheme $\mathbf{S}_{n,d}$ is reduced, they are exactly this number of such triples for almost all v (non-empty, open set of \mathbf{V}_n).

Note that the functor $\mathcal{S}_{n,d}$ is equivalent to the functor, which associates to a ring $R \in \mathcal{R}_d$ the set of pairs $(v, F) \in \mathcal{V}_n(R) \times \mathcal{F}_d(R)$ of polynomials in $R[x]$ such that

the polynomial F divides $F'' + 2vF'$. Indeed, if $(v, F, r) \in \mathcal{S}_{n,d}(R)$ then F divides $F'' + 2vF'$ by the equation (2.4). On the other hand, if we have such a pair (v, F) then the discriminant of F is invertible (because otherwise there would be a specialization $R \rightarrow C$ so that the specialized $F \in C[x]$ would have multiple roots and would divide $F'' + 2vF'$ — a contradiction) and there exist the unique $r = v' + v^2 + (F'' + 2vF')/F$ so that the triple (v, F, r) is an element of $\mathcal{S}_{n,d}(R)$.

Therefore we are going to prove that for almost all $v \in C[x]$ of degree n there are exactly $\binom{n+d-1}{d}$ monic polynomials F of degree d such that F divides $F'' + 2vF'$. Actually a more general result is formulated and proved in this section. As a motivation consider two examples. Let $v \in C[x]$ be a polynomial of degree n without multiple roots. Then there are exactly $\binom{n+d-1}{d}$ monic polynomials $F \in C[x]$ of degree d such that F divides the polynomial vF' . Indeed, these are polynomials whose roots are roots of v with all possible combinations of multiplicities. The second example is even simpler: if $G \in C[x]$ is a polynomial of degree $m \geq d$ without multiple roots then there are $\binom{m}{d}$ monic polynomials F of degree d such that F divides G . These two examples and the question how many elements there are in $\mathcal{S}_{n,d}(C)$ with the prescribed $v \in \mathcal{V}_n(C)$ are special cases of a general situation. Namely, the main result of this section implies that for a broad class of linear maps $L : W_C^d \rightarrow W_C^m$ the number of monic polynomials F of degree d such that F divides $L(F)$ is exactly $\binom{m}{d}$. For instance, the second example above with “constant” polynomial G corresponds to a linear map $W_C^d \rightarrow W_C^m$ given by $f \mapsto p_0G$, where p_0 is the coefficient to x^d of $f \in W_C^d$.

To formulate the general problem we define two new functors. Let m, d be integers, $m < d$. Let $\mathcal{L}_{d,m}$ be a functor which associates to a ring $R \in \mathcal{R}_C$ the set of linear maps $L : W_R^d \rightarrow W_R^m$ with the following property. Let $c_0 \in R$ be a coefficient to x^m in $L(x^d)$. Then for any positive $k \leq d$ we require the polynomial $L(x^{d-k}) - c_0x^{m-k}$ to be of degree $m - k$ with invertible leading coefficient. It is a functor because for a homomorphism $R \rightarrow R'$ of C -algebras in \mathcal{R}_C the associated map $\mathcal{L}_{d,m}(R) \rightarrow \mathcal{L}_{d,m}(R')$ given by $L \mapsto L'$ (the action of L' on the basis $x^d, \dots, x, 1$ comes from L) preserves the mentioned property.

Consider also a functor $\mathcal{G}_{m,d}$, which associates to a ring $R \in \mathcal{R}_C$ a set of pairs (F, L) , where $F \in R[x]$ is monic of degree d and $L \in \mathcal{L}_{d,m}(R)$ such that the polynomial F divides $L(F)$. Note that the division algorithm by a monic polynomial is correctly defined over any ring, giving justified notions of quotient, remainder, and divisibility, which are preserved by homomorphisms of rings. Thus we have again a correctly defined covariant functor. The functor $\mathcal{S}_{n,d}$ is a “subfunctor” of $\mathcal{G}_{n+d-1,d}$ in a sense that for any $R \in \mathcal{R}_C$ we have an inclusion $\mathcal{S}_{n,d}(R) \hookrightarrow \mathcal{G}_{n+d-1,d}(R)$ given by $(v, F, r) \mapsto (F, f \mapsto f'' + 2vf')$. The set $\mathcal{G}_{m,d}(C)$ also includes solutions of the two examples above.

Both new functors are representable as follows. A linear map $L \in \mathcal{L}_{d,m}(R)$ for some $R \in \mathcal{R}_C$ is specified by c_0 — the coefficient of $L(x^d)$ to x^m , and by a linear map $\tilde{L} : W_R^d \rightarrow W_R^{m-1}$ given by $f \mapsto L(f) - c_0x^{m-d}f$ such that the defining restrictions for $L \in \mathcal{L}_{d,m}(R)$ are satisfied. In the bases $x^k, \dots, x, 1$ of involved W_R^k the matrix of the auxiliary \tilde{L} has the only restrictions that the most upper maximal minor is lower-triangular and elements on its main diagonal are invertible. According to these restrictions the functor $\mathcal{L}_{d,m}$ is representable by the ring

$$R_L = C[c_0, (c_{i,j})_{1 \leq j \leq i \leq d}, (c_{i,j})_{1 \leq j \leq d < i < m}, (c_{i,i}^{-1})_{1 \leq i \leq d}].$$

The universal L for $\mathcal{L}_{d,m}$ is given by

$$L(F) = c_0 x^{m-d} F + c_1 x^{m-1} + c_2 x^{m-2} + \dots + c_m, \quad (2.25)$$

$$c_k = c_{k,0} p_0 + \sum_{j=1}^{\min(k,d)} c_{k,j} p_j \quad (1 \leq k \leq m),$$

for $F = p_0 x^d + p_1 x^{d-1} + \dots + p_d$.

To represent the functor $\mathcal{G}_{m,d}$ we use the following characterization of divisibility of polynomials over a commutative ring R (with 1). The claim is that a polynomial $\bar{G} = \bar{c}_1 x^{m-1} + \dots + \bar{c}_m \in R[x]$ is divisible by a monic polynomial $\bar{F} = x^d + \bar{p}_1 x^{d-1} + \dots + \bar{p}_d \in R[x]$ if and only if all maximal minors of the matrix

$$M = \begin{pmatrix} \bar{c}_1 & \bar{c}_2 & \bar{c}_3 & \dots & \bar{c}_{m-1} & \bar{c}_m \\ 1 & \bar{p}_1 & \bar{p}_2 & \dots & \bar{p}_d & \\ & 1 & \bar{p}_1 & \bar{p}_2 & \dots & \bar{p}_d & \mathbf{0} \\ & \mathbf{0} & \ddots & \dots & \ddots & \\ & & & 1 & \bar{p}_1 & \bar{p}_2 & \dots & \bar{p}_d \end{pmatrix} \quad (2.26)$$

are zero. Indeed, M^T is the matrix (in the basis $x^k, \dots, x, 1$ of W_R^k again) of the linear map $\rho : Q_R^0 \times Q_R^{m-d-1} \rightarrow Q_R^{m-1}$ defined by $(c, f) \mapsto cE + fF$. If a monic \bar{F} divides \bar{G} , then ρ has non-trivial kernel and the first row of M is a linear combination of the other rows. Conversely, if all maximal minors of M are zero, then note that the left-lower submatrix of size $m - n - 1$ has determinant 1, hence we can apply the lemma 2.3.6 for M^T and conclude that the first row of M is the linear combination of the other rows, which means that F divides G . Alternatively, one can use the straightforward divisibility characterization that the remainder of division of \bar{G} by \bar{F} in a ring R is the zero polynomial. Actually the coefficients of the remainder are special maximal minors of M , namely the determinants of submatrices which contain the first $m - d$ columns of M . To see this note that we can imitate the usual division algorithm of polynomials by subtracting from the first row of M multiples of the second, third, \dots rows so that the first $m - d$ elements in the first row become zero. After these operations the last d elements in the first row are the coefficients of the remainder, because the mentioned left-lower submatrix has determinant 1, and the mentioned manipulations with rows do not change maximal minors of M . Such construction is basic in the subresultant theory, see [13].

Using the first criterion of divisibility the functor $\mathcal{G}_{m,d}$ is representable as follows. Let L be the universal linear map (2.25) in $\mathcal{L}_{d,m}(R_L)$. Take \bar{F} to be the universal monic polynomial $x^d + p_1 x^{d-1} + \dots + p_d$ of degree d , and $\bar{G} = L(\bar{F}) - c_0 x^{m-d} \bar{F} = c_1 x^{m-1} + c_2 x^{m-2} + \dots + c_m$, according to (2.25). Let M be the matrix over $R_L[p_1, \dots, p_d]$ like (2.26) for these \bar{F} and \bar{G} . Let J be the ideal in $R_L[p_1, \dots, p_d]$ generated by maximal minors of the matrix M . Then the ring $R_L[p_1, \dots, p_d]/J$ represents the functor $\mathcal{G}_{m,d}$.

Finally we define the schemes $\mathbf{G}_{m,d} = \text{Spec } R_L[p_1, \dots, p_d]/J$ and $\mathbf{L}_{d,m} = \text{Spec } R_L$. Let $\pi_L : \mathbf{G}_{m,d} \rightarrow \mathbf{L}_{d,m}$ be the morphism given by the natural transformation between functors $\mathcal{G}_{m,d}$ and $\mathcal{L}_{d,m}$ such that for $R \in \mathcal{R}_C$ the map $\mathcal{G}_{m,d}(R) \rightarrow \mathcal{L}_{d,m}(R)$ is defined by $(F, L) \mapsto L$. The main result of this chapter is the following.

Proposition 2.5.1 *The morphism $\pi_L : \mathbf{G}_{m,d} \rightarrow \mathbf{L}_{d,m}$ is finite of degree $\binom{m}{d}$.*

Proof. Set $n = m - d + 1$ for this proof. Let L and \bar{F} be the universal objects mentioned just above, let M be the described matrix like (2.26) for \bar{F} and $\bar{G} = L(F) - c_0 x^{m-d} F$, and let J be the ideal in $R_L[p_1, \dots, p_d]$ generated by maximal minors of M . For convenience we define sets (for a positive integer k):

$$\begin{aligned} \mathcal{Z}^k &= \{(s_1, \dots, s_k) \in \mathbb{Z}^k : 0 < s_1 < \dots < s_k \leq m\}, \\ \mathcal{I}^k &= \{(\alpha_1, \dots, \alpha_k) \in \mathbb{Z}^k : 1 \leq \alpha_1 \leq \dots \leq \alpha_k \leq d\}. \end{aligned}$$

For a vector $s \in \mathcal{Z}^k$ let M_s denote the submatrix of M , consisting of the s_1 th, \dots , s_k th columns (here and in the following, if s is a vector of integers, by s_i we denote the i th component of s). To make expressions shorter, for $s \in \mathcal{Z}^n$ we set $\tilde{c}_s = c_{s_1, s_1} \in R_L^*$ (note that $s_1 \leq d$ for s of length n).

For $\alpha \in \mathcal{I}^k$ let p_α denote a monomial $\prod_{i=1}^k p_{\alpha_i} \in R_L[p_1, \dots, p_d]$.

We shall use the graded reverse lexicographic monomial ordering on monomials on p_1, \dots, p_d over the quotient field of R_L . In our notations if $\alpha \in \mathcal{I}^k, \beta \in \mathcal{I}^l$ then

$$p_\alpha \prec p_\beta \iff k < l \text{ or } k = l, \alpha_j < \beta_j \text{ for } j = \min\{i : \alpha_i \neq \beta_i\}.$$

To prove the proposition it is enough to show that the ring $R_L[p_1, \dots, p_d]/J$ is a finite free R_L -module of rank $\binom{m}{d}$. We do this by showing that all maximal minors of M form a Gröbner basis (minimal, non-reduced, over the quotient field of R_L) for the ideal J with respect to the mentioned monomial ordering. In introduced notations these maximal minors are determinants of matrices M_s with $s \in \mathcal{Z}^n$.

First we show that for any $s \in \mathcal{Z}^n$ the leading term of the determinant of M_s with respect to the ordering is realized by a product of terms on the diagonal of M_s , and it is equal to $\tilde{c}_s p_{\gamma(s)}$, where the map $\gamma : \mathcal{Z}^n \rightarrow \mathcal{I}^n$ is defined by

$$\gamma(s)_j = s_j - j + 1, \quad \text{for } 1 \leq j \leq n.$$

Indeed, consider $\det M_s$ as an alternating sum of terms $q_\sigma = q_{1, \sigma(1)} \dots q_{n, \sigma(n)}$, where $q_{i,j}$ is an element on the i th row and j th column of M_s , and σ is a permutation of $\{1, \dots, n\}$. The leading term of the product of elements on the diagonal is the mentioned $\tilde{c}_s p_{\gamma(s)}$. Consider the leading term p_β of q_σ with $\sigma \neq \text{id}$. Let $k = \min\{i : \sigma(i) \neq i\}$ and $\mu = p_{(\beta_1, \dots, \beta_{k-1})}$. Then $q_{k, \sigma(k)}$ is below the diagonal, and if it is not zero, then it is equal either to 1 or some p_j with $j < \gamma(s)_k$. If the last case this p_j is \prec any indeterminate in $p_{\gamma(s)}/\mu$ and divides p_β/μ . Hence $p_\beta/\mu \prec p_{\gamma(s)}/\mu$. It follows that $p_\beta \prec p_{\gamma(s)}$ in every case.

It is easy to see that conversely, any monomial p_α of total degree n is a leading monomial of some M_s . More explicitly, $s = \gamma^{-1}(\alpha)$, where the inverse

$$\gamma^{-1}(\alpha)_j = \alpha_j + j - 1, \quad \text{for } 1 \leq j \leq n.$$

It follows that any monomial in $R_L[p_1, \dots, p_d]/J$ of total degree n (and greater) can be linearly expressed in \prec monomials, and as a consequence, in monomials in p_1, \dots, p_d of degree $< n$. In other words, $R_L[p_1, \dots, p_d]/J$ is a finite R_L -module generated by

monomials of degree less than n . We want to show that there are no elements in J whose leading monomial has degree $< n$. Then it would follow immediately that $R_L[p_1, \dots, p_d]/J$ is a finite free module over R_L , generated by monomials in p_1, \dots, p_d of degree $< n$, and its rank is equal to $\binom{m}{d}$ — the number of such monomials.

To show this we have to prove that all maximal minors of M form a Gröbner basis for J with respect to the graded reverse lexicographic ordering. Equivalently (see [14]) we have to show that for any $s, t \in \mathcal{Z}^n$ the S -polynomial of determinants of M_s and M_t can be expressed as follows:

$$\tilde{c}_t \frac{p_\beta}{\gcd(p_\alpha, p_\beta)} \det M_s - \tilde{c}_s \frac{p_\alpha}{\gcd(p_\alpha, p_\beta)} \det M_t = \sum_{q \in \mathcal{Z}^n} m_{s,t,q} \det M_q \quad (2.27)$$

(here $\alpha = \gamma(s)$ and $\beta = \gamma(t)$) with leading monomials of $m_{k,l,q} \det M_q$ being $\prec \text{lcm}(p_\alpha, p_\beta)$ — the lowest common multiple of p_α and p_β .

We prove the expression (2.27) for M_s and M_t by induction on the number of elements in $\{i : s_i \neq t_i\}$. First consider the case when maximal minors M_s and M_t differ by one column. Without loss of generality we may suppose that $s_k < t_k$ for some $k \leq n$ and $s_i = t_i$ for $i \neq k$. Then $\alpha = \gamma(s)$ and $\beta = \gamma(t)$ differ only by the k th place also. We construct a matrix \tilde{M} of size $(n+1) \times (n+1)$ as follows. The last n rows of it form a matrix M_z , where $z = (s_1, \dots, s_k, t_k, s_{k+1}, \dots, s_n) \in \mathcal{Z}^{n+1}$ (so the matrix M_z contains all columns of M_s and M_t). The first row of \tilde{M} is the first row of M_z if $k = 1$, or the k th row of M_z multiplied by \tilde{c}_s otherwise. Obviously the determinant of \tilde{M} is zero. If we expand it by $n \times n$ minors of \tilde{M} to the first row, we get

$$0 = \sum_{j=1}^{n+1} (-1)^{j+1} \hat{m}_j \det \tilde{M}_j \quad (2.28)$$

(here $\tilde{M}_j = M_{(z_1, \dots, z_{j-1}, z_{j+1}, \dots, z_n)}$ and \hat{m}_j is the j th element of the first row of \tilde{M}). This expression has properties:

- $\tilde{M}_k = M_t$ and $\tilde{M}_{k+1} = M_s$, and the leading monomials of \hat{m}_k and \hat{m}_{k+1} are p_{α_k} and p_{β_k} correspondingly. Up to constants in R_L^* these two terms give the left hand-side of (2.27); note that $\tilde{c}_s = \tilde{c}_t$ if $s_1 = t_1$. If $k = 1$, then the non-leading terms of \hat{m}_k and \hat{m}_{k+1} could be considered as two summands on the right-hand side of (2.27) with $q = s$ and $q = t$.
- If $j < k$, let $\mu = p_{(\alpha_1, \dots, \alpha_{j-1})}$; then the leading monomial of $\hat{m}_j \det \tilde{M}_j$ divided by μ is $\prec p_\alpha p_{\beta_k} / \mu$, because it is divisible by \hat{m}_j , and $\hat{m}_j \prec p_{\alpha_j}$. Hence the leading term of $\hat{m}_j \det \tilde{M}_j$ is $\prec p_\alpha p_{\beta_k}$.
- If $j > k$, let $\mu = p_{(\alpha_1, \dots, \alpha_k)}$. Then the smallest indeterminate in the leading term of $\hat{m}_j \det \tilde{M}_j$ divided by μ is $p_{\beta_{k+1}}$, which does not divide $p_\alpha p_{\beta_k} / \mu$. We can draw the same conclusion here also.

These properties imply that that (2.28) gives the required expression (2.27).

In general case, when M_s and M_t differ by more than one column, let k th be the first column from the left by which the matrices differ. Without loss of generality suppose $s_k > t_k$. Let $z \in \mathcal{Z}^n$ be defined by $z_i = s_i$ for $i \neq k$ and $z_k = t_k$. Then $z \in \mathcal{Z}^n$ indeed. By the induction hypothesis one can express S -polynomials $S(\det M_s, \det M_z)$ and

$S(\det M_z, \det M_t)$ as in (2.27). But the S -polynomial $S(\det M_s, \det M_t)$ is expressible as

$$\frac{\gcd(p_{\gamma(s)}, p_{\gamma(z)})}{\gcd(p_{\gamma(s)}, p_{\gamma(t)})} S(\det M_s, \det M_z) + \frac{\gcd(p_{\gamma(z)}, p_{\gamma(t)})}{\gcd(p_{\gamma(s)}, p_{\gamma(t)})} S(\det M_z, \det M_t).$$

Therefore we can express the S -polynomial of any M_s and M_t like in (2.27).

As a conclusion, maximal minors of M form a Gröbner basis for J with respect to the graded reverse lexicographic ordering. It was already noted that this fact implies that the ring $R_L[p_1, \dots, p_d]/J$ is a finite free R_L -module of the required rank. \square

This proposition implies, that for all linear maps $L \in \mathcal{L}_{d,m}(C)$ the number of monic polynomials of degree F such that F divides $L(F)$ is $\leq \binom{m}{d}$. Since we have examples of L that the number of such F is exactly $\binom{m}{d}$, in general a linear transformation $L \in \mathcal{L}_{d,m}(C)$ has this maximal number of such polynomials F .

The part (iii) of the original problem is a direct consequence of the proved proposition, because it remains to restrict us to a subvariety of $\mathbf{L}_{m,d}$ isomorphic to \mathbf{V}_n . In other words, we tensor $R_L[p_1, \dots, p_d]/J \rightarrow R_L$ with the surjective image of $R_L \rightarrow \mathcal{O}(\mathbf{V}_n)$ and conclude that $R_{n,d} \cong R_L[p_1, \dots, p_d]/J \otimes_C \mathcal{O}(\mathbf{V}_n)$ is a finite free module over $\mathcal{O}(\mathbf{V}_n) \cong C[a_n, \dots, a_0, a_n^{-1}]$ of rank $\binom{n+d-1}{d}$. This is the same as to say that $\pi_r : \mathbf{S}_{n,d} \rightarrow \mathbf{V}_n$ is finite of the same degree, as promised. Since $\mathbf{S}_{n,d}$ is smooth, for most $v \in C[x]$ the number of elements in $\mathcal{S}_{n,d}(C)$ “above” v is exactly $\binom{n+d-1}{d}$.

