Algoritmos de deformación para la resolución de sistemas polinomiales

Waissbein, Ariel

2013

UNIVERSIDAD DE BUENOS AIRES

Facultad de Ciencias Exactas y Naturales

Departamento de Matemática

Algoritmos de deformación para la resolución de sistemas polinomiales

Tesis presentada para optar al título de Doctor de la Universidad de Buenos Aires en el área Ciencias Matemáticas

Ariel Waissbein

Director de tesis: Dr. Guillermo Matera

Consejero de estudios: Dr. Guillermo Matera

Buenos Aires, 17 de Diciembre de 2013

Algoritmos de deformación para la resolución de sistemas polinomiales

Esta tesis está dedicada a ciertas tareas computacionales de geometría algebraica en característica cero. Apuntamos a analizar y descubrir la complejidad de problemas definidos por sistemas de ecuaciones polinomiales con una perspectiva de álgebra computacional. La intratabilidad computacional de los enfoques generalistas a los problemas de geometría computacional nos impele a estudiar familias particulares de sistemas de ecuaciones polinomiales en los que la complejidad del *peor caso* es tratable (y significativamente más baja que la del caso general). Cuando sea posible, proveeremos un método eficiente para encontrar su solución.

Como "brújula" para determinar estas familias usamos técnicas de deformación las que, según mostraremos, son sensibles a problemas con buenas propiedades semánticas. Entonces, este trabajo consiste en establecer algunos problemas de eliminación que son tratables y exhibir algoritmos eficientes que los resuelven.

Nuestras técnicas de deformación se basan en un procedimiento de levantamiento *à la* Newton–Hensel que se adapta bien para producir algoritmos que corren en menos pasos cuando las propiedades semánticas referenciadas anteriormente son buenas. Construiremos, entonces, un catálogo de resultados sobre la resolución de sistemas de ecuaciones polinomiales, usando algoritmos de álgebra altamente eficientes, que constituyen mejoras en relación con el estado del arte.

Palabras clave: algoritmos eficientes, ecuaciones polinomiales, eliminación geométrica, levantamiento de Newton-Hensel, algoritmos simbólicos, algoritmos probabilísticos, complejidad.

Deformation Algorithms for Polynomial System Solving

This thesis is devoted to computational tasks of basic algebraic geometry in characteristic zero. We aim to analyse and discover the complexity of problems defined by systems of polynomial equations from a computer algebra perspective. The computational intractability of a general approach to geometric elimination problems compels us to study the difficulty of elimination for particular families of polynomial equation systems where worst-case complexity is tractable (and significantly lower than the complexity of tackling the general case). When possible, we provide an efficient solution method.

As our "compass" for determining these families, we use deformation techniques which, we will show, are susceptible to problems with well-posed semantic properties. Hence, this work consists in establishing some elimination problems that are tractable, and for these, exhibiting efficient algorithms that tackle them.

Our deformation techniques rely on a Newton-Hensel lifting procedure which adapts well in order to obtain algorithms running in fewer steps when certain semantic parameters are "low". Using highly-efficient algorithms for constructing these geometric elimination procedures, we develop a catalogue of results on polynomial system solving that improve over the prior art.

Keywords: efficient algorithms, polynomial equations, geometric elimination, Newton-Hensel lifting, symbolic algorithms, probabilistic algorithms, complexity.

Agradecimientos

Quisiera agradecer de manera especial y sincera al profesor Dr. Guillermo Matera por aceptar ser mi director y acompañarme durante este doctorado con empeño y generosidad, contribuyendo con un aporte invaluable.

Quiero también expresar mi agradecimiento al profesor Dr. Joos Heintz por haber generado ese interés en mi por la eliminación geométrica, por las muchas charlas matemáticas y de tantas otras cosas.

Me gustaría agradecer a los varios profesores y alumnos, co-autores, conferencistas y aquellos otros científicos con los que me crucé durante esta carrera.

Debo agradecer a mi familia por su apoyo, por ayudarme a destinar las horas necesarias de trabajo a este doctorado, y por las palabras de aliento.

Contents

Introducción

Dado un sistema de ecuaciones polinomiales sobre los racionales queremos contestar preguntas sobre sus soluciones. Según la tradición en informática, los problemas se especifican por sus parámetros sintácticos. En el caso que nos compete, esto significa buscar un algoritmo (no necesariamente uniforme) que, dados enteros d, n y s, calcula las soluciones de un sistema de s polinomios n-variados de grado total acotado por d cuando éste define una variedad de dimensión cero. Es sabido que este problema es $P^{\#}$-duro y que el problema de decidir si un sistema definido sobre los enteros define o no la variedad vacía es NP- y $\mathrm{NP}_{\mathbb{C}}$-duro ([HM93], [SS93a]).

De hecho, tanto el acercamiento simbólico como el numérico a la resolución de sistemas de ecuaciones polinomiales se hace por demás intrincado. Los métodos numéricos no pueden ser aplicados directamente a sistemas paramétricos, sobre-determinados, sub-determinados o degenerados —que son de gran interés (ver, e.g., [Par95]). Más aún, cuando comparamos los acercamientos simbólicos con los numéricos de [SS93a], [SS93b], [SS93c], [SS96b], [SS94], [CS99] y [BCSS98], es posible mostrar que este acercamiento numérico es inferior en términos de complejidad bit (ver [CHMP01] y [CJPS02]).

Por otro lado, el famoso resultado de Mayr y Meyer ([MM82]) implica que el “Hauptproblem der Idealtheorie” (i.e., el problema de pertenencia a un ideal) es EXPSPACE-completo; y, por ende, esto es evidencia de que los métodos simbólicos basados en re-escritura, tales como aquellos basados en bases de Gröbner (ver, e.g., [Buc85]), necesitan de un espacio de memoria exponencial en el peor de los casos (ver también, e.g., [May89], [KM96] y [Küh98]). De otro resultado, éste de D. Lazard, T. Mora, W. Masser y P. Philippon (ver [Bro87]), podemos deducir que el número de operaciones aritméticas necesarias para resolver un sistema polinomial expresado por su codificación densa es inevitablemente exponencial. Sin embargo, los métodos simbólicos basados en re-escritura son los preferidos en la gran mayoría del software disponible.

Nosotros proponemos evitar este crecimiento de la complejidad para algoritmos simbólicos restringiéndonos a “preguntas geométricas” o a casos especiales de sistemas de ecuaciones polinomiales, e.g., aquellos con un número finito de soluciones. Sin embargo, incluso para sistemas con un conjunto finito de soluciones, la cantidad de operaciones aritméticas que necesitan algoritmos simbólicos optimales es del orden de $sd^{O(n^2)}$. Este hecho se debe a que los algoritmos simbólicos están limitados por las representaciones densas (o ralas) de los polinomios de entrada. Podemos evitar este dilema si la representación de los polinomios de entrada está dada por cajas negras o “(division-free) straight-line programs” que los evalúan. Aún en este caso, la cota para el peor caso se limita a $sd^{O(n)}$ para aquellos algoritmos que fueron implementados usando las reglas de ingeniería de software (ver [HKR11] y [HKR12]).

Un catálogo

Tomamos el problema de buscar clases de sistemas de ecuaciones que pueden resolverse con recursos computacionales “razonables” y disponibles para ingenieros y científicos en nuestros días.

Nuestro acercamiento se construye sobre los cimientos de [GHM$^+$98], [GHH$^+$97], [GHMP97] y [Par95]. En estos artículos los autores introducen algoritmos para resolución de sistemas polinomiales basándose en una deformación homotópica que es “seguida” mediante un levantamiento *à la* Newton-Hensel. Dichos algoritmos toman como entrada un straight-line program que calcula los polinomios que definen el sistema bajo estudio y devuelven una solución geométrica de este sistema en un tiempo polinomial en un parámetro que llaman el *grado del sistema*, y que está acotado por el número de Bézout del sistema.

Además, también nos basamos en las enseñanzas de [HKP$^+$00], [GLS01], [HMW01] y [Sch03]. En esta segunda familia de artículos, los autores aíslan un algoritmo de deformación basado en la técnica de levantamiento anterior, estiman el costo de este algoritmo en términos de parámetros más finos de carácter geométrico y producen procedimientos eficientes que calculan la solución de algunos sistemas polinomiales.

Antes de describir estas técnicas de deformación queremos dar un paso atrás y recordar un resultado de [CGH$^+$03] (cf. [HMPW98], [Par00], [GH01], [BP06]), que muestra que cualquier algoritmo universal y robusto que resuelve ciertos sistemas polinomiales sobre los complejos requiere de al menos $D^{\Omega(1)}$ operaciones aritméticas, donde D denota el número de Bézout del sistema de entrada. Ergo, para los sistemas polinomiales en nuestro catálogo apuntamos a: a) reemplazar a D por parámetros más finos que reflejen las propiedades geométricas del sistema, y b) reemplazar a $\Omega(1)$ en la reciente estimación por un número que sea lo más bajo posible. Nuestro esfuerzo no constituye un ataque al caso general, sino —como ya lo explicamos— para que esto quede reflejado en los casos particulares que forman parte de nuestro catálogo.

Supongamos dados polinomios $f_1, \ldots, f_n \in \mathbb{Q}[X_1, \ldots, X_n]$ que definen un sistema de dimensión cero $V \subset \mathbb{C}^n$. Supongamos que podemos definir una curva algebraica $\mathcal{V} \subset \mathbb{C}^{n+1}$ y un morfismo dominante y genéricamente no ramificado $\pi : \mathcal{V} \to \mathbb{C}$ tal que vale $\pi^{-1}(1) = \{1\} \times V$, donde $\mathcal{V}$ es el conjunto de ceros comunes en $\mathbb{C}^{n+1}$ de ciertos polinomios $F_1, \ldots, F_n \in \mathbb{Q}[T, X_1, \ldots, X_n]$ y el morfismo π está dado por la regla $\pi(t, x_1, \ldots, x_n) := t$. Entonces, tomando como entrada una descripción completa de una fibra no ramificada $\pi^{-1}(t_0)$ (ver la Sección 2.2.1 para una definición precisa), podemos calcular una descripción de cualquier fibra $\pi^{-1}(t)$, y por lo tanto una de V. Llamamos "algoritmo de levantamiento" a un procedimiento que resuelve este problema.

Típicamente produciremos a $F_1, \ldots, F_n$ como perturbaciones de $f_1, \ldots, f_n$ de manera que el sistema cero-dimensional $\{F_1(t_0, X) = 0, \ldots, F_n(t_0, X) = 0\}$ es "fácil" de resolver y vale $F_i(1, X) = f_i(X)$ para $1 \leq i \leq n$. Para este algoritmo de levantamiento, pedimos que los polinomios $F_1, \ldots, F_n$ de $\mathbb{Q}[T, X] := \mathbb{Q}[T, X_1, \ldots, X_n]$ formen una sucesión regular y generen un ideal radical en $\mathbb{Q}[T, X]$. También pedimos un punto $t_0 \in \mathbb{Q}$ tal que su fibra por π sea no ramificada, y una forma lineal $U \in \mathbb{Q}[X]$ tal que U separe los puntos de $\pi^{-1}(t_0)$.

El algoritmo de levantamiento calcula una descripción completa de $\mathcal{V}$ a partir de un straight-line program en $\mathbb{Q}[T, X]$ que evalúa a $F_1, \ldots, F_n$ y una descripción completa de la fibra $\pi^{-1}(t_0)$. La salida del algoritmo consiste en $n+1$ polinomios univariados que forman la codificación densa de una solución geométrica.

Con nuestras hipótesis, existen $\#\pi^{-1}(t_0)$ n-uplas de series formales $R := (R_1, \ldots, R_n) \in \mathbb{C}[\![T - t_0]\!]^n$ que son solución del sistema $F_1 = 0, \ldots, F_n = 0$, i.e., vale que $F_i(T, R) = 0$ en $\mathbb{C}[\![T - t_0]\!]$ para $1 \leq i \leq n$. El levantamiento de Newton-Hensel que mencionamos se usa para aproximar estas series formales de las cuales se calcula la descripción de $\mathcal{V}$.

Seguidamente ilustramos la técnica de levantamiento mostrando cómo es que el operador formal de Newton-Hensel aproxima a las series formales antes referidas. Esto no descubre, de ninguna manera, los pasos que seguimos en nuestros algoritmos y que detallaremos en las próximas secciones.

Sea $(t_0, \xi) \in \mathbb{C}^{n+1}$ un punto en la fibra $\pi^{-1}(t_0)$. Entonces, de nuestras hipótesis se sigue que existe una única n–upla de series formales $R^{(\xi)} := (R_1^{(\xi)}, \ldots, R_n^{(\xi)}) \in \mathbb{C}[\![T - t_0]\!]^n$ tal que $R^{(\xi)}(0) = \xi$ y $F_i(T, R^{(\xi)}(T)) = 0$ en $\mathbb{C}[\![T - t_0]\!]$ para cada $1 \leq i \leq n$.

Denotemos por $J_F(X) := (\partial F_i / \partial X_j)_{1 \leq i,j \leq n}$ a la matriz Jacobiana de $F_1, \ldots, F_n$ con respecto a $X_1, \ldots, X_n$ y sea

$$N_F(X) := \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} - (J_F(T, X))^{-1} \begin{pmatrix} F_1(T, X) \\ \vdots \\ F_n(T, X) \end{pmatrix}$$

el operador (formal) de Newton-Hensel asociado al sistema. Para cada $\kappa \in \mathbb{Z}_{\geq 0}$, sea

$$R^{(\xi,\kappa)} := (R_1^{(\xi,\kappa)}, \ldots, R_n^{(\xi,\kappa)}) := N_F^{\kappa}(T, \xi)$$

la κ–ésima iteración del operador de Newton-Hensel N_F comenzando desde ξ. Entonces, afirmamos que:

- $\det(J_F(T, R^{(\xi,\kappa)})) \notin (T - t_0)\mathbb{C}[T]_{(T-t_0)}$, y
- $F_i(T, R^{(\xi,\kappa)}) \in (T - t_0)^{2^\kappa}\mathbb{C}[T]_{(T-t_0)}$ para $1 \leq i \leq n$.

Más aún, también

- Los primeros 2^κ términos en $(T - t_0)$ de $R^{(\xi,\kappa+1)}$ y $R^{(\xi,\kappa)}$ son iguales, i.e., $R_i^{(\xi,\kappa+1)} - R_i^{(\xi,\kappa)} \in (T - t_0)^{2^\kappa}\mathbb{C}[T]_{(T-t_0)}$ para $1 \leq i \leq n$.

Es fácil ver que estas afirmaciones son verdaderas para $\kappa = 0$, porque por hipótesis el ideal $(F_1(t_0, X), \ldots, F_n(t_0, X))$ de $\mathbb{C}[X]$ es radical, ya que la fibra

$\pi^{-1}(t_0)$ se supone no ramificada. Esto implica que $\det(J_F(t_0,\xi)) \neq 0$ y luego $\det(J_F(T,R^{(\xi,0)})) \notin (T-t_0)\mathbb{C}[T]_{(T-t_0)}$. Por otro lado, vale que $F_i(T,R^{(\xi,0)}) = F_i(T,\xi) \in (T-t_0)\mathbb{C}[T]_{(T-t_0)}$ para $1 \leq i \leq n$. De la identidad

$$R^{(\xi,1)} = R^{(\xi,0)} + J_F(T,R^{(\xi,0)})^{-1}F(T,R^{(\xi,0)})$$

deducimos que $R_i^{(\xi,1)} - R_i^{(\xi,0)} \in (T-t_0)\mathbb{C}[T]_{(T-t_0)}$ para $1 \leq i \leq n$.

El paso inductivo se sigue de la definición del operador N_F y el desarrollo de Taylor de F_i y $\det(J_F)$ como series formales en $(T-t_0)$: si para cada $1 \leq i \leq n$, multiplicamos cada miembro de la igualdad

$$R^{(\xi,\kappa+1)} - R^{(\xi,\kappa)} = -J_F^{-1}(T,R^{(\xi,\kappa)}) \cdot \begin{pmatrix} F_1(T,R^{(\xi,\kappa)}) \\ \vdots \\ F_n(T,R^{(\xi,\kappa)}) \end{pmatrix}$$

por la i–ésima fila de $J_F(T,R^{(\xi,\kappa)})$, se sigue que

$$J_F(T,R^{(\xi,\kappa)})_i \cdot (R^{(\xi,\kappa+1)} - R^{(\xi,\kappa)}) = -F_i(T,R^{(\xi,\kappa)}). \tag{1}$$

Combinando (1) con la congruencia

$$F_i(T,R^{(\xi,\kappa+1)}) \equiv F_i(T,R^{(\xi,\kappa)}) + \sum_{j=1}^{n} \frac{\partial F_i}{\partial X_j}(T,R^{(\xi,\kappa)}) \cdot (R_j^{(\xi,\kappa+1)} - R_j^{(\xi,\kappa)})$$

mod $(R^{(\xi,\kappa+1)} - R^{(\xi,\kappa)})^2$ de $\mathbb{C}[\![T-t_0]\!]_{(T-t_0)}$, se deduce que $F_i(T,R^{(\xi,\kappa+1)}) \equiv 0$ mod $(R^{(\xi,\kappa+1)} - R^{(\xi,\kappa)})^2$ in $\mathbb{C}[\![T-t_0]\!]_{(T-t_0)}$. De la hipótesis inductiva se sigue que $(R^{(\xi,\kappa+1)} - R^{(\xi,\kappa)})^2 \subset ((T-t_0)^{2^\kappa})^2 \subset (T-t_0)^{2^{\kappa+1}}$ lo que prueba la segunda parte del paso inductivo.

La última parte del paso inductivo sale de la siguiente igualdad

$$R^{(\xi,\kappa+2)} - R^{(\xi,\kappa+1)} = -J_F^{-1}(T,R^{(\xi,\kappa+1)}) \cdot \begin{pmatrix} F_1(T,R^{(\xi,\kappa+1)}) \\ \vdots \\ F_n(T,R^{(\xi,\kappa+1)}) \end{pmatrix}$$

y lo que acabamos de probar. Por otro lado, del desarrollo del determinante Jacobiano $\det(J_F)$ se puede inferir que

$$\begin{aligned} \det(J_F(T,R^{(\xi,\kappa+1)}) \;&\equiv\; \det(J_F(T,R^{(\xi,\kappa)}) + \\ &\sum_{j=1}^{n} \frac{\partial \det(J_F)}{\partial X_j}(T,R^{(\xi,\kappa)}) \cdot (R_j^{(\xi,\kappa+1)} - R_j^{(\xi,\kappa)}) \end{aligned}$$

mod $(R^{(\xi,\kappa+1)} - R^{(\xi,\kappa)})^2$ en $\mathbb{C}[\![T-t_0]\!]_{(T-t_0)}$. Así, de la primera parte de la hipótesis inductiva deducimos su contraparte en el paso inductivo.

En el transcurso de esta tesis produciremos distintos algoritmos de levantamiento cuya algorítmica no puede inferirse directamente de los razonamientos anteriores, que se basan en contribuciones a la algorítmica de [GLS01] y [Sch03], y usan aproximadamente $O(\deg \mathcal{V} \deg \pi)$ operaciones aritméticas en $\mathbb{Q}$ (omitiendo algunos términos de orden poli-logarítmico en los parámetros de la expresión), donde $\deg \mathcal{V}$ es el grado de la variedad $\mathcal{V}$ y $\deg \pi$ el grado del morfismo π (ver la Sección 2.3 para las definiciones de medidas de complejidad y la Sección 2.4 para obtener más precisiones sobre este resultado). Vale aclarar que en nuestro caso $\deg \pi \leq \deg \mathcal{V} \leq D$, donde D es el número de Bézout del sistema que define a $\mathcal{V}$.

Teniendo a este algoritmo disponible, el punto crítico para la aplicación del algoritmo de homotopía/levantamiento es el de obtener morfismos π con "grado bajo" y una fibra no ramificada que sea "fácil de resolver".

Sistemas generalizados de Pham

Comenzamos nuestro catálogo con una clase importante de sistemas cuadrados, con coeficientes racionales, que definen una variedad cero-dimensional sobre los complejos, llamados sistemas generalizados de Pham (ver [PS04] y [DMW09]) o intersecciones completas estrictas (ver [CDS96]), que aparecen relacionados con distintos problemas en geometría algebraica computacional (ver, e.g., [MT00], [HM00]). Un sistema generalizado de Pham puede ser descripto someramente como el resultado de la deformación de una singularidad proyectiva de intersección completa; intuitivamente se corresponde a la noción de un sistema "sin puntos en el infinito" (ver [PS04, Remark 17] o [CDS96, Section 1]).

Un sistema n–dimensional generalizado de Pham está definido por n polinomios de la forma

$$\phi_1 + \varphi_1, \ldots, \phi_n + \varphi_n,$$

donde para cada $1 \leq i \leq n$ vale que $\phi_i \in \mathbb{Q}[X_1, \ldots, X_n]$ es homogéneo, φ_i es un polinomio (no necesariamente homogéneo) de grado total menor que $d_i := \deg \phi_i$, y tal que $\phi_1, \ldots, \phi_n$ definen la variedad proyectiva vacía de $\mathbb{P}^{n-1}(\mathbb{C})$.

Un ejemplo específico de sistema generalizado de Pham es el de un sistema (n–dimensional) de Pham, que queda definido por polinomios de la forma

$$X_1^{d_1} + \varphi_1, \ldots, X_n^{d_n} + \varphi_n,$$

donde $\varphi_i \in \mathbb{Q}[X_1, \ldots, X_n]$ es de grado menor que d_i para $1 \leq i \leq n$ (en la Sección 3.1 esgrimiremos otros ejemplos interesantes de sistemas generalizados de Pham).

Las soluciones de un sistema de Pham $f_1 = 0, \ldots, f_n = 0$ dado por polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ pueden calcularse con una adaptación de [Sch03] o incluso usando un resultado de [BMWW04, Section 5] —trabajo del que soy co-autor. En breve, podríamos aplicar el algoritmo de proyección de los artículos citados a la deformación definida por el morfismo $\pi_{\mathcal{W}} : \mathcal{W} \to \mathbb{A}^1$ dado por la regla $\pi_{\mathcal{W}}(t, x) := t$, donde la variedad $\mathcal{W} \subset \mathbb{A}^{n+1}$ viene dada por las soluciones del sistema

$$a_i X_i^{d_i} + T(f_i - a_i X_i^{d_i}) + b_i(1 - T) = 0 \quad (1 \leq i \leq n),$$

siendo a_i el coeficiente de X^{d_i} en f_i y b_i un racional arbitrario elegido aleatoriamente $1 \leq i \leq n$. En [BMWW04] exhibimos un sistema que resuelve sistemas de Pham con complejidad cuadrática y usa un algoritmo de homotopía directamente (para el caso $d_1 = \ldots = d_n$). Describiremos dicho procedimiento más adelante en el Capítulo 4 en un contexto distinto.

Desafortunadamente, el anillo de coordenadas de un sistema generalizado de Pham carece de la estructura monomial simple que aparece en los sistemas de Pham, y eso hace que este procedimiento (cf. [BMWW04]) —pero también los de [MP97], [GLGV98], [MP00], [MT00]— devengan en algoritmos con complejidad más que cuadrática en el número de Bézout del sistema de entrada. A saber, mirando el producto $\deg(\pi_{\mathcal{W}}) \deg \mathcal{W}$, que es el término dominante en la estimación de complejidad de nuestro algoritmo, para este caso particular vale que $\deg(\pi_{\mathcal{W}}) = D := d_1 \cdots d_n$ y $\deg W \leq E := (d_1 + 1) \cdots (d_n + 1)$ por la desigualdad de Bézout. Entonces, cuando $n \gg \text{máx}\{d_1, \ldots, d_n\}$ se sigue que $E \gg D$ y luego $DE \gg D^2$.

No obstante, veremos que podemos producir un algoritmo probabilístico que resuelve sistemas generalizados de Pham en complejidad *cuadrática* en el número de Bézout de la entrada. Dicho algoritmo hará uso de, no una, sino $n + 1$ homotopías sobre curvas producidas artificialmente, a fin de computar la solución del sistema original.

En el Capítulo 3 nos abocaremos al diseño de dicho algoritmo y la prueba de los resultados matemáticos necesarios. Este es uno de los dos resultados principales de [DMW09]; artículo del que soy co-autor. El segundo resultado de aquel artículo dice que la resolución de sistemas generalizados de Pham por algoritmos robustos y universales necesita de al menos $D^{\Omega(1)}$ operaciones aritméticas en $\mathbb{Q}$ (en el peor caso), donde D es el número de Bézout del sistema generalizado de Pham. Esta cota es independiente de la representación de entrada y salida del algoritmo, aunque el exponente en la Ω sí depende de dicha representación. Por ejemplo, mostramos que si usáramos la representación densa o rala (por rala entendemos la lista de todos los coeficientes no nulos), entonces el exponente de D en la cota de complejidad es del orden de $\Omega(D)$, mientras que si usamos un straight–line program para representarlos entonces el exponente es del orden de $\Omega(D^{1/2})$. Este segundo resultado implica que nuestra cota superior es casi optimal.

Levantamiento de fibras ramificadas

El segundo ítem del catálogo es una generalización del algoritmo de levantamiento que presentamos y usamos arriba. Sea $\mathcal{V} \subset \mathbb{C}^{n+1}$ una curva algebraica definida sobre $\mathbb{Q}$, y supongamos que el morfismo $\pi : \mathcal{V} \to \mathbb{C}$ inducido por la proyección canónica en la primera coordenada es dominante y genéricamente no ramificado. Supongamos dada la estructura infinitesimal de una fibra finita y ramificada $\pi^{-1}(t_r)$. Queremos calcular una descripción completa de una fibra arbitraria $\pi^{-1}(t)$. Mientras que en el caso de una fibra no ramificada podíamos usar un levantamiento *à la* Newton-Hensel para aproximar las soluciones y derivar una descripción completa de una fibra arbitraria $\pi^{-1}(t)$, esto se vuelve imposible en el caso de que la fibra sea ramificada. A saber, supongamos dada una fibra $\pi^{-1}(t_u)$ no ramificada para cierto $t_u \in \mathbb{Q}$. Recordemos que el cuerpo de fracciones $\mathbb{C}(\!(T - t_u)\!)$ del anillo de series formales $\mathbb{C}[\![T - t_u]\!]$ no es algebraicamente cerrado, y que el cuerpo de series de Puiseux $\overline{\mathbb{Q}}\langle T - t_u\rangle^*$ es una clausura algebraica de $\mathbb{Q}(\!(T - t_u)\!)$ (ver, e.g., [Wal50]). Por lo expuesto anteriormente (Sección “Un catálogo”) se sigue que todas las soluciones en $\mathbb{A}^n(\mathbb{C}\langle T - t_u\rangle^*)$ del sistema

$$F_1(T, X) = 0, \ldots, F_n(T, X) = 0 \tag{2}$$

están, de hecho, en $\mathbb{C}[\![T - t_u]\!]^n$. Sin embargo, cuando consideramos a (2) como un sistema en $\mathbb{A}^n(\mathbb{C}\langle T - t_r\rangle^*)$, no podemos aplicar el argumento de la

Sección "Un catálogo"; de hecho, sucede que no todas las soluciones están en $\mathbb{C}[\![T-t_r]\!]^n$. En particular, no podemos usar el algoritmo de levantamiento para este caso.

Una manera de salvar este problema es requiriendo una descripción completa del conjunto de partes singulares de los desarrollos en series de Puiseux de las ramas de $\mathcal{V}$ que están sobre t_r (ver la Sección 4.1 para más detalles). En el Capítulo 4 exhibiremos un algoritmo que calcula una descripción completa de una fibra arbitraria $\pi^{-1}(t)$, dada dicha descripción de una fibra ramificada, y que usa aproximadamente $O(\deg \mathcal{V}(\deg \pi)^{\alpha})$ operaciones aritméticas en $\mathbb{Q}$, siendo $\alpha = 1$ en varios ejemplos importantes. Este es el resultado principal de [BMWW04], del que soy co-autor, que extiende y mejora los resultados de [HKP$^+$00] y [Sch03] (cf. [DMW09]).

Asimismo repasaremos algunos ejemplos de familias a las que le subyace una fibra ramificada que es "fácil" de resolver. Para esos casos, nuestro nuevo algoritmo de levantamiento calculará una solución completa de cualquier miembro de la familia $\mathcal{V}$.

Por ejemplo, sean $n, d \in \mathbb{N}$ y consideremos el sistema de Pham

$$f_1 := X_1^d - \varphi_1(X), \ldots, f_n := X_n^d - \varphi_n(X),$$

la curva definida por el sistema

$$F_1 := X_1^d + T\varphi_1(X), \ldots, F_n := X_n^d + T\varphi_n(X),$$

y el morfismo π dado por $\pi(t,x) := t$. Entonces, la fibra $\pi^{-1}(0) = \{0\}$ tiene un solo punto y es ramificada. En este caso, las partes singulares de las ramas de la curva $\{F_1 = 0, \ldots, F_n = 0\}$ que están sobre $T = 0$ son

$$(\xi^{i_1}\alpha_1^{1/d}T^{1/d}, \ldots, \xi^{i_n}\alpha_n^{1/d}T^{1/d})$$

para $0 \leq i_1, \ldots, i_n \leq d-1$, donde $\alpha := (\alpha_1, \ldots, \alpha_n) := (\varphi_1(0), \ldots, \varphi_n(0))$. Veremos que es posible aplicar el nuevo algoritmo de levantamiento para resolver este sistema a partir de la fibra de $t = 0$ en aproximadamente $O(\mathsf{T} \deg \mathcal{V} \deg \pi) = O(\mathsf{T} d^{2n})$ operaciones aritméticas en $\mathbb{Q}$.

La familia de sistemas de ecuaciones del próximo ítem es también un ejemplo donde podemos aplicar este nuevo algoritmo.

Sistemas ralos y homotopías poliedrales

Cerramos nuestro catálogo con un procedimiento para calcular todas las soluciones de un sistema polinomial ralo (en el que el conjunto de coeficientes no nulos es pequeño) y que se vale de una homotopía poliedral.

El famoso resultado de D.N. Bernstein, A.G. Kushnirenko y A.G. Khovanski ([Ber75], [Kus76], [Kho78]) acota el número de soluciones de un sistema polinomial en términos de un invariante combinatorio asociado a los exponentes de los monomios con coeficientes no nulos de los polinomios del sistema. Explícitamente, el Teorema de Bernstein-Kushnirenko-Khovanski (que abreviamos por BKK) dice que el número de soluciones aisladas en el toro complejo $(\mathbb{C}^*)^n$ de un sistema polinomial dado por n ecuaciones en n variables está acotado por el *volumen mixto* de los polítopos de Newton de los polinomios que definen al sistema.

Los métodos numéricos (de continuación homotópica) para sistemas ralos se basan típicamente en una familia de deformaciones que se llaman homotopías poliedrales ([HS95], [VVC94], [VGC96], [Roj03]). Las homotopías poliedrales preservan el polítopo de Newton del sistema polinomial de entrada; asimismo, les subyace una versión efectiva del Teorema BKK (ver, e.g., [HS95], [HS97]).

Supongamos dado un sistema cero-dimensional $(\Delta_1, \ldots, \Delta_n)$-ralo dado por n polinomios $f_1, \ldots, f_n \in \mathbb{Q}[X_1, \ldots, X_n]$, con soportes $\Delta_1, \ldots, \Delta_n \subset \mathbb{Z}^n$ respectivamente. Sea $V \subset (\mathbb{C}^*)^n$ la variedad definida por los ceros comunes de $f_1, \ldots, f_n$ en $(\mathbb{C}^*)^n$. Entonces, una homotopía poliedral consiste en una curva algebraica $\mathcal{V} \subset (\mathbb{C}^*)^{n+1}$ tal que la proyección $\pi : \mathcal{V} \to \mathbb{C}^*, \pi(t,x) := t$ en la primera coordenada es dominante, con fibras genéricamente no ramificadas cuyo grado es igual al volumen mixto $MV(conv(\Delta_1), \ldots, conv(\Delta_n))$ de las cápsulas convexas de $\Delta_1, \ldots, \Delta_n$, tal que vale la identidad $\pi^{-1}(1) = \{1\} \times V$, y tal que es fácil calcular los primeros términos de los desarrollos de Puiseux de las ramas de $\mathcal{V}$ que están sobre 0. Los métodos de continuación numéricos calculan los primeros términos de los desarrollos de Puiseux y luego siguen las ramas de $\mathcal{V}$ por el intervalo $[0, 1]$ para obtener aproximaciones a todos los puntos de V.

Vamos a ver cómo combinar los procedimientos numéricos basados en homotopías poliedrales de [HS95] con nuestras técnicas de deformación —en particular, las técnicas de deformación del Capítulo 4 (y de [BMWW04])—

a fin de diseñar un algoritmo probabilístico simbólico para resolver sistemas polinomiales ralos de dimensión cero con un costo cúbico en el tamaño de la estructura combinatoria de la entrada. Para esto, en el Capítulo 5 reproduciremos los resultados de [JMSW09] —que también es de mi co-autoría.

Aproximadamente, el resultado principal de este capítulo es el siguiente resultado (ver el Teorema 5.23 para más precisiones).

Sean $f_1, \ldots, f_n$ polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ tal que el sistema $f_1 = 0, \ldots, f_n = 0$ define una variedad afín cero-dimensional V en $\mathbb{C}^n$. Sean $\Delta_1, \ldots, \Delta_n \subset \mathbb{Z}^n_{\geq 0}$ los soportes de $f_1, \ldots, f_n$ y supongamos que $0 \in \Delta_i$ para $1 \leq i \leq n$, y que el volumen mixto D de los polítopos de Newton $Q_1 := \mathrm{Conv}(\Delta_1), \ldots, Q_n := \mathrm{Conv}(\Delta_n)$ es distinto de cero.

Entonces, mediante un algoritmo probabilístico en $\mathbb{Q}$, podemos calcular la solución geométrica de V en

$$O(NDD')$$

operaciones aritméticas en $\mathbb{Q}$ (omitiendo términos poli-logarítmicos), donde $N := \sum_{1 \leq i \leq n} \#\Delta_i$ y $D' := \sum_{1 \leq i \leq n} \mathcal{M}(\Delta, Q_1, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n)$; Δ denota el símplice n-dimensional y $\mathcal{M}$ denota volumen mixto.

Este ítem será estudiado en detalle en el Capítulo 5.

Chapter 1

Introduction

Given a polynomial equation system over the rationals, we want to answer questions about its zero set. According to tradition in theoretical computer science, problems are specified by syntactic parameters. For polynomial systems, this amounts to producing a (not necessarily uniform) algorithm that, given integers d, n and s, for every system of n-variate polynomials over the rationals consisting of s equations of total degree bounded by d which define a zero-dimensional variety, computes its zero set. It can be shown that this problem is $P^{\#}$-hard and one sees easily that the problem to decide wether a given polynomial equation system over the integers is consistent is NP- and $\mathrm{NP}_{\mathbb{C}}$-hard ([HM93], [SS93a]).

In fact, both symbolic and numeric approaches to polynomial system solving suffer from grave disadvantages. The numeric approach cannot be applied directly to solve parametric, overdetermined, underdetermined, or degenerated systems —that are of great interest (see, e.g., [Par95]). Moreover, when comparing symbolic and numeric approaches, such as the numeric procedures of [SS93a], [SS93b], [SS93c], [SS96b], [SS94], [CS99], [BCSS98], one can show that the latter is worse in terms of bitwise computations (see [CHMP01] and [CJPS02]).

On the other hand, the infamous result of Mayr and Meyer ([MM82]) says that the "Hauptproblem der Idealtheorie" (i.e., the ideal membership problem) is EXPSPACE-complete; and, in turn this is evidence that symbolic approaches based on re-writing techniques, such as Gröbner basis computations (see [Buc85]), require exponential memory in worst case (see also, e.g., [May89], [KM96] and [Küh98]). Another result, due to D. Lazard, T. Mora, W. Masser and P. Philippon (see [Bro87]), shows that an exponential number of computations is unavoidable when using the dense representation of polynomials. The symbolic re-writing approach is nevertheless used by a considerable portion of the software that is currently available for this problem.

We propose to avoid this complexity blow up of symbolic algorithms by restricting our attention to "geometric questions" or special cases of polynomial equation systems, e.g., to those which have only finite zero sets. However, even for the case of systems having a finite zero set, the time complexity of optimal symbolic algorithms is of order $sd^{O(n^2)}$. This is due to the fact that symbolic algorithms are limited to the dense (or sparse) representations of polynomials. A way out of this dilemma is given by the representation of polynomials by (division-free) straight-line programs which evaluate them. But even in this case, the improvement of the worst-case complexity is limited to $sd^{O(n)}$ for algorithms which are implemented using the rules of software engineering ([HKR11], [HKR12]).

1.1. A catalogue

The problem we undertake then is to determine classes of systems that can be solved with "reasonable" computational resources available to scientists and engineers these days.

Our approach grows from the findings of [GHM$^+$98], [GHH$^+$97], [GHMP97], [Par95]. In these articles the authors introduce algorithms for solving polynomial systems that rely on a homotopic deformation which is "tracked" by means of a Newton-Hensel lifting. These procedures take as input a straight-line program computing the polynomials defining the system under consideration and output its (geometric) solution in time polynomial in a new parameter called the *degree of the system*, which is bounded by the Bézout number of this system.

We further take on the teachings of [HKP$^+$00], [GLS01], [HMW01] and [Sch03]. In this second instalment of works, the authors isolate a deformation algorithm based on the recently-mentioned lifting techniques, determine its cost in terms of certain geometric parameters and produce efficient procedures to compute the solution of certain polynomial systems.

Before we describe these deformation techniques, we want to take a step back to recall a result of [CGH$^+$03] (cf. [HMPW98], [Par00], [GH01], [BP06]), which shows that any robust universal algorithm solving certain polynomial systems over the complex numbers require at least $D^{\Omega(1)}$ arithmetic operations, where D denotes the Bézout number of the input system. For the classes of polynomial systems in our catalogue we aim to: a) replace the Bézout number D by parameters that reflect the geometric properties of the input system, and b) replace the $\Omega(1)$ in the above estimate for a constant that is as low as possible. This effort will be done not to make a dent in the general case, as we have already explained, but in particular examples that will constitute the items of our catalogue.

Suppose that we are given polynomials $f_1, \ldots, f_n \in \mathbb{Q}[X_1, \ldots, X_n]$ defining a zero-dimensional solution set $V \subset \mathbb{C}^n$. Assume that we can define an algebraic curve $\mathcal{V} \subset \mathbb{C}^{n+1}$ and a dominant and generically-unramified morphism $\pi : \mathcal{V} \to \mathbb{C}$ such that $\pi^{-1}(1) = \{1\} \times V$ holds, where $\mathcal{V}$ is the set of common zeros in $\mathbb{C}^{n+1}$ of polynomials $F_1, \ldots, F_n \in \mathbb{Q}[T, X_1, \ldots, X_n]$ and the morphism is defined by $\pi(t, x_1, \ldots, x_n) := t$. Then, from a complete description of an unramified fibre $\pi^{-1}(t_0)$ (see Section 2.2.1 for a precise definition) we can compute a complete description of an arbitrary fibre $\pi^{-1}(t)$, and thus of V. We call "lifting procedure" to an algorithm that solves this problem.

We will typically produce $F_1, \ldots, F_n$ as perturbations of $f_1, \ldots, f_n$ so that the polynomial system $\{F_1(t_0, X) = 0, \ldots, F_n(t_0, X) = 0\}$ is "easy" to solve and $F_i(1, X) = f_i(X)$ holds for $1 \leq i \leq n$. For this lifting procedure, the polynomials $F_1, \ldots, F_n$ in $\mathbb{Q}[T, X] := \mathbb{Q}[T, X_1, \ldots, X_n]$ are required to form a regular sequence and span a radical ideal in $\mathbb{Q}[T, X]$. The method requires a point $t_0 \in \mathbb{Q}$ such that its fibre under π is unramified and a linear form $U \in \mathbb{Q}[X]$ such that U separates the points of $\pi^{-1}(t_0)$.

The lifting procedure computes a complete description of $\mathcal{V}$ from: a straight-line program in $\mathbb{Q}[T, X]$ that computes $F_1, \ldots, F_n$ and a complete description of the fibre $\pi^{-1}(t_0)$. The output consists of $n + 1$ univariate polynomials which are given by its dense representation.

With these hypotheses, there exist $\#\pi^{-1}(t_0)$ different n-tuples of formal power series $R := (R_1, \ldots, R_n) \in \mathbb{C}[\![T - t_0]\!]^n$ that are solutions of the system $F_1 = 0, \ldots, F_n = 0$, i.e., it holds that $F_i(T, R) = 0$ in $\mathbb{C}[\![T - t_0]\!]$ for $1 \leq i \leq n$.

The Newton-Hensel lifting we refer to computes an approximation to these formal power series and computes a complete description of $\mathcal{V}$ from it.

We illustrate the Newton-Hensel lifting by depicting how the Newton-Hensel operator (formally) approximates the solutions of the system under consideration. This is by no means an algorithm that will be used later on to solve polynomial systems.

Let $\xi \in \mathbb{C}^n$ be any point in $\pi^{-1}(t_0)$. Then, with our hypotheses, we can show that there exists a unique n–tuple of formal power series $R^{(\xi)} := (R_1^{(\xi)}, \ldots, R_n^{(\xi)}) \in \mathbb{C}[\![T - t_0]\!]^n$ such that $R^{(\xi)}(0) = \xi$ and $F_i(T, R^{(\xi)}(T)) = 0$ for every $1 \leq i \leq n$ in $\mathbb{C}[\![T - t_0]\!]$.

Write $J_F(X) := (\partial F_i / \partial X_j)_{1 \leq i,j \leq n}$ for the Jacobian matrix of $F_1, \ldots, F_n$ with respect to $X_1, \ldots, X_n$ and let

$$N_F(X) := \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} - (J_F(T,X))^{-1} \begin{pmatrix} F_1(T,X) \\ \vdots \\ F_n(T,X) \end{pmatrix}$$

denote the (formal) Newton-Hensel operator. For $\kappa \in \mathbb{Z}_{\geq 0}$, let

$$R^{(\xi,\kappa)} := (R_1^{(\xi,\kappa)}, \ldots, R_n^{(\xi,\kappa)}) := N_F^{\kappa}(T, \xi)$$

denote the κ–the fold iteration of the Newton-Hensel operator N_F starting at ξ. We claim that for every $\kappa \in \mathbb{Z}_{\geq 0}$ it holds that

- $\det(J_F(T, R^{(\xi,\kappa)})) \notin (T - t_0)\mathbb{C}[T]_{(T-t_0)}$, and
- $F_i(T, R^{(\xi,\kappa)}) \in (T - t_0)^{2^\kappa}\mathbb{C}[T]_{(T-t_0)}$ for $1 \leq i \leq n$.

Moreover, it also holds that

- $R^{(\xi,\kappa+1)}$ agrees with $R^{(\xi,\kappa)}$ in its first 2^κ powers of $(T - t_0)$, i.e., $R_i^{(\xi,\kappa+1)} - R_i^{(\xi,\kappa)} \in (T - t_0)^{2^\kappa}\mathbb{C}[T]_{(T-t_0)}$ for $1 \leq i \leq n$.

It is straightforward to show that these assertions are true when $\kappa = 0$, because by hypotheses the ideal $(F_1(t_0, X), \ldots, F_n(t_0, X))$ of $\mathbb{C}[X]$ is radical, since the fibre $\pi^{-1}(t_0)$ is unramified. This implies that $\det(J_F(t_0, \xi)) \neq 0$

and therefore $\det(J_F(T, R^{(\xi,0)})) \notin (T-t_0)\mathbb{C}[T]_{(T-t_0)}$. Besides, it holds that $F_i(T, R^{(\xi,0)}) = F_i(T,\xi) \in (T-t_0)\mathbb{C}[T]_{(T-t_0)}$ for $1 \leq i \leq n$. From the identity

$$R^{(\xi,1)} = R^{(\xi,0)} + J_F(T, R^{(\xi,0)})^{-1} F(T, R^{(\xi,0)})$$

we deduce that $R_i^{(\xi,1)} - R_i^{(\xi,0)} \in (T-t_0)\mathbb{C}[T]_{(T-t_0)}$ for $1 \leq i \leq n$.

The inductive step follows from the definition of the operator N_F and the Taylor expansions of the F_i and $\det(J_F)$ as power series in $(T-t_0)$. For each $1 \leq i \leq n$, we multiply each member of the equality

$$R^{(\xi,\kappa+1)} - R^{(\xi,\kappa)} = -J_F^{-1}(T, R^{(\xi,\kappa)}) \cdot \begin{pmatrix} F_1(T, R^{(\xi,\kappa)}) \\ \vdots \\ F_n(T, R^{(\xi,\kappa)}) \end{pmatrix}$$

by the i–th row of $J_F(T, R^{(\xi,\kappa)})$ and deduce that

$$J_F(T, R^{(\xi,\kappa)})_i \cdot (R^{(\xi,\kappa+1)} - R^{(\xi,\kappa)}) = -F_i(T, R^{(\xi,\kappa)}). \tag{1.1}$$

Combining (1.1) with the congruence relation

$$F_i(T, R^{(\xi,\kappa+1)}) \equiv F_i(T, R^{(\xi,\kappa)}) + \sum_{j=1}^{n} \frac{\partial F_i}{\partial X_j}(T, R^{(\xi,\kappa)}) \cdot (R_j^{(\xi,\kappa+1)} - R_j^{(\xi,\kappa)})$$

mod $(R^{(\xi,\kappa+1)} - R^{(\xi,\kappa)})^2$ in $\mathbb{C}[\![T-t_0]\!]_{(T-t_0)}$, we deduce that $F_i(T, R^{(\xi,\kappa+1)}) \equiv 0$ mod $(R^{(\xi,\kappa+1)} - R^{(\xi,\kappa)})^2$ in $\mathbb{C}[\![T-t_0]\!]_{(T-t_0)}$. From the inductive hypotheses we obtain that $(R^{(\xi,\kappa+1)} - R^{(\xi,\kappa)})^2 \subset ((T-t_0)^{2^\kappa})^2 \subset (T-t_0)^{2^{\kappa+1}}$ which proves the second claim in the inductive step.

The last claim in the inductive step follows from the equality

$$R^{(\xi,\kappa+2)} - R^{(\xi,\kappa+1)} = -J_F^{-1}(T, R^{(\xi,\kappa+1)}) \cdot \begin{pmatrix} F_1(T, R^{(\xi,\kappa+1)}) \\ \vdots \\ F_n(T, R^{(\xi,\kappa+1)}) \end{pmatrix}$$

and what we just proved. On the other hand, from the Taylor expansion of the Jacobian determinant $\det(J_F)$ we infer that

$$\begin{aligned} \det(J_F(T, R^{(\xi,\kappa+1)}) &\equiv \det(J_F(T, R^{(\xi,\kappa)}) + \\ &\sum_{j=1}^{n} \frac{\partial \det(J_F)}{\partial X_j}(T, R^{(\xi,\kappa)}) \cdot (R_j^{(\xi,\kappa+1)} - R_j^{(\xi,\kappa)}) \end{aligned}$$

mod $(R^{(\xi,\kappa+1)} - R^{(\xi,\kappa)})^2$ in $\mathbb{C}[\![T-t_0]\!]_{(T-t_0)}$. From the first claim in the inductive hypotheses we deduce its counterpart in the inductive step.

We shall produce different variations of lifting procedures which follow steps that cannot be inferred in a straightforward fashion from the claims above. These rely mainly on the algorithmic contributions of [GLS01] and [Sch03] and use roughly $O(\deg \mathcal{V} \deg \pi)$ arithmetic operations in $\mathbb{Q}$, where $\deg \mathcal{V}$ and $\deg \pi$ denote the degree of the variety $\mathcal{V}$ and the degree of the morphism π respectively (see Section 2.3 for definitions of complexity measures and Section 2.4 for a precise statement). In our setting, $\deg \pi \leq \deg \mathcal{V} \leq D$ holds, where D is the Bézout number of the system defining $\mathcal{V}$.

With this algorithm available, a critical point for the application of this homotopy-lifting method is to obtain morphisms π as above of "low degree" with a fibre that is "easy to solve".

1.1.1. Generalized Pham Systems

Our catalogue starts with a significant class of zero–dimensional square polynomial systems with rational coefficients over the complex numbers, called generalized Pham systems (see [PS04] and [DMW09]) or strict complete intersections (see [CDS96]), which arise in connection with several problems in computational algebraic geometry (see, e.g., [MT00], [HM00]). A generalized Pham system may be roughly described as the result of a deformation of an isolated projective complete–intersection singularity and corresponds to the intuitive notion of a system with "no points at infinity" (see [PS04, Remark 17] or [CDS96, Section 1]).

An n–dimensional generalized Pham system is defined by n polynomials of the form

$$\phi_1 + \varphi_1, \ldots, \phi_n + \varphi_n,$$

where for each $1 \leq i \leq n$, it holds that $\phi_i \in \mathbb{Q}[X_1, \ldots, X_n]$ is homogeneous and φ_i is a polynomial (not necessarily homogenous) of degree less than $d_i := \deg \phi_i$, and such that $\phi_1, \ldots, \phi_n$ define the empty projective variety of $\mathbb{P}^{n-1}(\mathbb{C})$.

A particular example of a generalized Pham system is an (n–dimensional)

Pham system, defined by n polynomials of the form

$$X_1^{d_1} + \varphi_1, \ldots, X_n^{d_n} + \varphi_n,$$

where $\varphi_i \in \mathbb{Q}[X_1, \ldots, X_n]$ has degree less than d_i for $1 \leq i \leq n$ (in Section 3.1 we shall exhibit other useful examples of generalized Pham systems).

The solutions of a Pham system $f_1 = 0, \ldots, f_n = 0$ in $\mathbb{Q}[X_1, \ldots, X_n]$ can be computed with an adaptation of [Sch03] or even using a result in [BMWW04, Section 5], a paper that I co-authored. One would apply the "projection algorithm" (as in the cited articles) to the deformation $\pi_{\mathcal{W}} : \mathcal{W} \to \mathbb{A}^1$ determined by the morphism $\pi_{\mathcal{W}}(t, x) := t$, where the variety $\mathcal{W} \subset \mathbb{A}^{n+1}$ consists in the common zeros of the system

$$a_i X_i^{d_i} + T(f_i - a_i X_i^{d_i}) + b_i(1 - T) = 0 \quad (1 \leq i \leq n),$$

where a_i stands for the coefficient of X^{d_i} in f_i and b_i is a randomly chosen rational for $1 \leq i \leq n$. In [BMWW04] we exhibited a procedure solving families of Pham systems, of quadratic complexity, using the homotopy-lifting procedure in a straightforward fashion (in the case where $d_1 = \ldots = d_n$). This procedure is described later in Chapter 4 under a different context.

Unfortunately, the coordinate ring of a generalized Pham system lacks the simple monomial structure arising in a Pham system and therefore this procedure (cf. [BMWW04]) —but also the procedures of [MP97], [GLGV98], [MP00], [MT00]— leads to an algorithm with more than quadratic complexity in the Bézout number of the input system. Explicitly, considering the product $\deg(\pi_{\mathcal{W}}) \deg \mathcal{W}$, which is the dominant term of the complexity of this algorithm, in this case we have $\deg(\pi_{\mathcal{W}}) = D := d_1 \cdots d_n$ and $\deg W \leq E := (d_1 + 1) \cdots (d_n + 1)$ according to the Bézout inequality. In particular, for $n \gg \max\{d_1, \ldots, d_n\}$ we have $E \gg D$ and hence $DE \gg D^2$.

Notwithstanding, we shall show that it is still possible to produce a probabilistic algorithm which solves generalized Pham systems with *quadratic* complexity in the Bézout number of the input system. The algorithm will underly not one, but a sequence of $n + 1$ homotopies in artificially produced curves that will lead to the computation of the solution of the original system.

The design of this algorithm and the proof of the required mathematical facts are the subject of Chapter 3. This is one of the two main results covered in [DMW09], which I co-authored. The second result states that a robust universal algorithm solving generalized Pham systems has (worst–case) complexity of order $D^{\Omega(1)}$, where D is the Bézout number of the input system. This bound is independent of the representation of input and output, but the value of the exponent underlying the Ω–notation does depend on such a representation. For example, if the usual dense or sparse representation (the list of all or of all nonzero coefficients) is used, then the complexity of the corresponding algorithm is of order $\Omega(D)$, while for the straight–line program representation a lower bound of order $\Omega(D^{1/2})$ is achieved. This shows that our procedure is almost optimal (in its class).

1.1.2. Lifting from ramified fibres

The second item in our catalogue serves as a generalization for the algorithm we presented and used for the previous item. Let $\mathcal{V} \subset \mathbb{C}^{n+1}$ be a $\mathbb{Q}$–definable algebraic curve, and let us assume that the morphism $\pi : \mathcal{V} \to \mathbb{C}$ induced by the canonical projection in the first coordinate is dominant and generically unramified. Suppose that we are given the infinitesimal structure of a finite and ramified fibre $\pi^{-1}(t_r)$. We want to compute a complete description of an arbitrary fibre $\pi^{-1}(t)$.

While in the case of an unramified fibre, we could use a Newton-Hensel lifting to approximate the solutions and derive a complete description of an arbitrary fibre $\pi^{-1}(t)$, this is no longer possible when the fibre is ramified. Suppose that the fibre $\pi^{-1}(t_u)$ is unramified for a given $t_u \in \mathbb{Q}$. Recall that the quotient field $\mathbb{C}(\!(T - t_u)\!)$ of the ring of formal power series $\mathbb{C}[\![T - t_u]\!]$ is not algebraically closed, and that the field of Puiseux series $\overline{\mathbb{Q}}(T - t_u)^*$ is an algebraic closure of $\mathbb{Q}(\!(T - t_u)\!)$ (see, e.g., [Wal50]). Then, all the solutions in $\mathbb{A}^n(\mathbb{C}(T - t_u)^*)$ of the system

$$F_1(T, X) = 0, \ldots, F_n(T, X) = 0 \tag{1.2}$$

belong to $\mathbb{C}[\![T - t_u]\!]^n$ as we have already shown in Section 1.1. However, when (1.2) is considered as a system in $\mathbb{A}^n(\mathbb{C}(T - t_r)^*)$, the argument we used in Section 1.1 fails; in fact, not all its solutions necessarily belong to $\mathbb{C}[\![T - t_r]\!]^n$. This implies that we can not use our lifting algorithm in this context.

Our way out of this dilemma is by requiring a complete description of the set of singular parts of the Puiseux expansions of the branches of $\mathcal{V}$ lying above t_r (see Section 4.1 for further details). In Chapter 4 we will exhibit an algorithm which computes a complete description of an arbitrary fibre $\pi^{-1}(t)$ and which requires roughly $O(\deg \mathcal{V}(\deg \pi)^{\alpha})$ operations in $\mathbb{Q}$, where $\alpha = 1$ in several important cases. This is the main result of [BMWW04], which I co-authored. This result extends and improves the procedures in [HKP$^+$00] and [Sch03] (cf. [DMW09]).

We shall also provide examples where the families underly some "easy fibres" that are ramified. In such cases, this new lifting technique allows us to compute a complete description of any member of the family $\mathcal{V}$.

For example, for $n, d \in \mathbb{N}$, consider the Pham system

$$f_1 := X_1^d - \varphi_1(X), \ldots, f_n := X_n^d - \varphi_n(X),$$

the curve defined by the system

$$F_1 := X_1^d + T\varphi_1(X), \ldots, F_n := X_n^d + T\varphi_n(X),$$

and the morphism π induced by the projection on the T coordinate. Then, the fibre $\pi^{-1}(0) = \{0\}$ has only one point and is ramified. In this case, the singular parts of the branches of the curve $\{F_1 = 0, \ldots, F_n = 0\}$ lying above $T = 0$ are given by

$$(\xi^{i_1}\alpha_1^{1/d}T^{1/d}, \ldots, \xi^{i_n}\alpha_n^{1/d}T^{1/d})$$

for $0 \leq i_1, \ldots, i_n \leq d-1$, where $\alpha := (\alpha_1, \ldots, \alpha_n) := (\varphi_1(0), \ldots, \varphi_n(0))$. As we will show, one may apply our lifting techniques for ramified fibres in order to solve this example with roughly $O(\mathsf{T} \deg \mathcal{V} \deg \pi) = O(\mathsf{T} d^{2n})$ arithmetic operations in $\mathbb{Q}$.

The family of polynomial systems below shall serve as another example where this new algorithm can be applied.

1.1.3. Sparse systems and polyhedral homotopies

The catalogue concludes with a procedure for computing all solutions to zero-dimensional sparse polynomial systems (where the set of non-zero coefficients of the defining polynomials is "small") and which uses a polyhedral homotopy.

The infamous results by D.N. Bernstein, A.G. Kushnirenko and A.G. Khovanski ([Ber75], [Kus76], [Kho78]) bound the number of solutions of a polynomial system in terms of a combinatorial invariant associated to the set of exponents of the monomials arising with nonzero coefficients in the defining polynomials. More precisely, the Bernstein-Kushnirenko-Khovanski (BKK for short) theorem asserts that the number of isolated solutions in the n-dimensional complex torus $(\mathbb{C}^*)^n$ of a polynomial system of n equations in n unknowns is bounded by the *mixed volume* of the family of Newton polytopes of the corresponding polynomials.

Numeric (homotopy continuation) methods for sparse systems are typically based on a specific family of deformations called polyhedral homotopies ([HS95], [VVC94], [VGC96], [Roj03]). Polyhedral homotopies preserve the Newton polytope of the input polynomials and yield an effective version of the BKK theorem (see, e.g., [HS95], [HS97]).

Suppose that we are given a zero-dimensional $(\Delta_1, \ldots, \Delta_n)$-sparse system defined by n polynomials $f_1, \ldots, f_n \in \mathbb{Q}[X_1, \ldots, X_n]$, where $\Delta_1, \ldots, \Delta_n \subset \mathbb{Z}^n$ are the supports of $f_1, \ldots, f_n$. Let $V \subset (\mathbb{C}^*)^n$ be the variety defined by the common zeros of $f_1, \ldots, f_n$ in $(\mathbb{C}^*)^n$. Then a polyhedral homotopy consists in an algebraic curve $\mathcal{V} \subset (\mathbb{C}^*)^{n+1}$ such that the projection $\pi : \mathcal{V} \to \mathbb{C}^*, \pi(t, x) := t$ onto the first coordinate is dominant with generically finite fibres whose degree is the mixed volume $MV(conv(\Delta_1), \ldots, conv(\Delta_n))$ of the convex hulls of $\Delta_1, \ldots, \Delta_n$, the identity $\pi^{-1}(1) = \{1\} \times V$ holds and the first terms of the Puiseux expansions of the branches of $\mathcal{V}$ lying above 0 can be easily computed. Numerical continuation methods compute the first terms of these Puiseux expansions and then follow the branches of $\mathcal{V}$ along the interval $[0, 1]$ to obtain approximations to all the points of the input variety V.

We will show how to combine the homotopic procedures of [HS95] with our deformation techniques, particularly in the version of Chapter 4 (and [BMWW04]), in order to derive a symbolic probabilistic algorithm for solving sparse zero-dimensional polynomial systems with cubic cost in the size of the combinatorial structure of the input system. This chapter reproduces the results of [JMSW09] —an article that I co-authored.

Our main result may be stated as follows (see Theorem 5.23 for a precise statement):

Let $f_1, \ldots, f_n$ be polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ such that the system $f_1 = 0, \ldots, f_n = 0$ defines a zero-dimensional affine sub-variety V of $\mathbb{C}^n$. Denote by $\Delta_1, \ldots, \Delta_n \subset \mathbb{Z}^n_{\geq 0}$ the supports of $f_1, \ldots, f_n$. Assume that $0 \in \Delta_i$

for $1 \leq i \leq n$ and the mixed volume D of the Newton polytopes $Q_1 := \mathrm{Conv}(\Delta_1), \ldots, Q_n := \mathrm{Conv}(\Delta_n)$ is nonzero.

Then, we can probabilistically compute a geometric solution of the variety V using $O(NDD')$ arithmetic operations in $\mathbb{Q}$ (omitting poly-logarithmic terms), with $N := \sum_{1 \leq i \leq n} \#\Delta_i$ and $D' := \sum_{1 \leq i \leq n} \mathcal{M}(\Delta, Q_1, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n)$, where Δ denotes the standard n-dimensional simplex and $\mathcal{M}$ stands for mixed volume.

All this shall be covered in Chapter 5.

Chapter 2

Preliminaries

2.1. Notation

Let K be a zero-characteristic field and let $\overline{K}$ be an algebraically closed field containing K. We shall use the standard notation for the set of integers $\mathbb{Z}$, positive integers $\mathbb{N}$, and the fields of rationals $\mathbb{Q}$, algebraic numbers $\overline{\mathbb{Q}}$ and complex numbers $\mathbb{C}$.

For any positive real number a, by $\log a$ we denote its binary logarithm (in base 2).

Let $n \in \mathbb{N}$. Let $X_1, \ldots, X_n$ be indeterminates over K. Unless otherwise stated X shall stand for the vector $X := (X_1, \ldots, X_n)$. We denote by $K[X_1, \ldots, X_n]$ (or $K[X]$ for short) the ring of polynomials in $\boldsymbol{n}$ variables over K. We shall also consider the elements in $K[X]$ as functions from K^n to K.

2.2. Geometry

Let $\mathbb{A}^n := \mathbb{A}^n\left(\overline{K}\right)$ be the $\boldsymbol{n}$–dimensional affine space $\overline{K}^n$.

Let be given a set of polynomials $S \subseteq \overline{K}[X_1, \ldots, X_n]$. The set of common zeroes of the polynomials in S is denoted by

$$V(S) := \{x \in \mathbb{A}^n : f(x) = 0 \quad \forall f \in S\}.$$

We say that $V \subset \mathbb{A}^n$ is a K–definable algebraic variety if and only if there exists a set $S \subseteq K[X_1, \ldots, X_n]$ such that $V = V(S)$. Unless specifically noted, variety shall mean K–definable algebraic variety.

In the affine space $\mathbb{A}^n$ we define the Zariski topology over K, where the closed sets are all the K–definable algebraic varieties $V \subset \mathbb{A}^n\left(\overline{K}\right)$.

In particular we shall consider fields K such as the fields of rational numbers $\mathbb{Q}$, complex numbers $\mathbb{C}$, rational functions with rational coefficients $\mathbb{Q}(T)$ or its algebraic closure $\overline{\mathbb{Q}(T)} = \overline{\mathbb{Q}}(T)^*$, namely the field of Puiseux series, where T is a new indeterminate. Further, we shall consider the rings of n–variate polynomials over these fields.

An algebraic variety V is irreducible if it is not the union of two varieties which are proper subsets of V. Note that since $\mathbb{A}^n$ is Noetherian, every algebraic variety V is the union of a finite number of irreducible algebraic varieties. Moreover, the irreducible varieties in such a decomposition are unique up to reordering and are called the irreducible components of V.

The dimension of a variety V of $\mathbb{A}^n$, which we denote by $\dim_{\mathbb{A}^n} V$ or $\dim V$, is the supremum over the integers r such that

$$W_0 \subset \ldots \subset W_r$$

is a strictly ascending sequence of irreducible sub-varieties of V —and it is the same as the Krull dimension of the ring $K[X_1, \ldots, X_n]/\mathcal{I}(V)$. Here $\mathcal{I}(V) := \{f \in K[X] : f(x) = 0 \ \forall x \in V\}$ is the ideal defined by all the polynomials that vanish on V. A variety V of $\mathbb{A}^n$ is said equidimensional if all its irreducible components have the same dimension.

Let W and V be sub-varieties of $\mathbb{A}^n$ such that $W \subseteq V$ and V is irreducible. When W is irreducible, the co-dimension of W in V is the supremum over the integers r such that $W \subset W_1 \subset \ldots \subset W_r$ is a strictly increasing chain of irreducible varieties contained in V. For an arbitrary sub-variety W of V, its co-dimension is defined as the infimum of the co-dimensions of its irreducible components. An hypersurface of V is an equidimensional sub-variety of co-dimension 1. When $V = \mathbb{A}^n$, and in other important cases, a variety V is an hypersurface if and only if it is the set of zeros of one non-constant polynomial $f \in K[X_1, \ldots, X_n]$.

Let $V \subset \mathbb{A}^n$ be a nonempty irreducible variety of dimension $\dim V = r$.

The degree $\deg V$ of V is defined as

$$\deg V := \deg_{\mathbb{A}^n} V := \sup \Big\{ \#\left(H_1 \cap \ldots \cap H_r \cap V\right) : H_1, \ldots, H_r \text{ are}$$
$$\text{affine hyperplanes of } \mathbb{A}^n, \text{ and the intersection is finite} \Big\}.$$

This is always a finite number. If V is an arbitrary algebraic sub-variety of $\mathbb{A}^n$, following [Hei83] and [Ful84], we define its degree as the sum of the degrees of all its irreducible components. If V and W are subvarieties of $\mathbb{A}^n$, then the *Bézout inequality* ([Hei83]; see also [Ful84], [Vog84]) asserts that:

$$\deg(V \cap W) \leq \deg V \deg W. \tag{2.1}$$

Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be K–definable varieties. The restriction of a polynomial function $P \in K[X]$ to V is called a regular function of V. The set of regular functions of V is a ring that we denote by $K[V]$. A morphism of varieties is a map φ from V to W given by regular functions $\varphi_1, \ldots, \varphi_m \in K[V]$ such that for every $t \in V$ it holds that $\varphi(t) = (\varphi_1(t), \ldots, \varphi_m(t)) \in W$.

The total quotient ring of V, denoted by $K(V)$, is the ring resulting from the localisation $S^{-1} \cdot K[V]$, where S is the set of nonzero divisors of $K[V]$. The members of $K(V)$ are called rational functions. We note that if V is irreducible, then $K(V)$ is the field of fractions of $K[V]$; however, in the general case it is the product of the fields of fractions $\prod K(C_i)$, where C_i runs over the irreducible components of V.

A morphism (of varieties) $\varphi : V \to W$ is said dominant if its image $\varphi(V)$ is dense in W (in the Zariski topology).

A morphism of varieties $\varphi : V \to W$ induces a morphism of rings $\varphi^* : K[W] \to K[V]$ from $K[W] = K[Y_1, \ldots, Y_m]/\mathcal{I}(W)$ to $K[V] = K[X_1, \ldots, X_n]/\mathcal{I}(V)$, which is univocally determined by mapping the regular functions of $K[W]$ defined by the variables Y_i, for $1 \leq i \leq m$, to $\varphi^*(Y_i) = \varphi_i$ respectively.

A morphism $\varphi : V \to W$ is said a finite morphism if $K[V]$ is integral over $K[W]$; in particular, its fibres are nonempty and finite (i.e., $0 < \#\varphi^{-1}(y) < \infty$ for every $y \in \varphi(V)$).

Let V and W be equidimensional sub-varieties of $\mathbb{A}^n$ and $\mathbb{A}^m$ respectively, and of equal dimension $\dim V = \dim W$. Let $\varphi : V \to W$ be a dominant morphism. When V is irreducible, we define the degree of φ as

$$\deg \varphi := [K(V) : \varphi^*(K(W))],$$

where the brackets denote the degree of the field extension $\varphi^*(K(W)) \to K(V)$. More generally, if the decomposition of V into irreducible components is given by $V = \cup \mathcal{C}_i$ and each of the restrictions $\varphi|_{\mathcal{C}_i} : \mathcal{C}_i \to W$ is dominant, we define the degree of φ as the sum of the degrees of the restrictions $\varphi|_{\mathcal{C}_i}$, namely

$$\deg \varphi := \sum_i \deg(\varphi|_{\mathcal{C}_i}) = \sum_i [K(\mathcal{C}_i) : \varphi^*(K(W))].$$

In particular, when $V \subset \mathbb{A}^{n+1}$ is equidimensional of dimension 1, $V = C_1 \cup \cdots \cup C_N$ is a decomposition into irreducible components, and the morphism $\pi : V \to \mathbb{A}^1$ defined by $\pi(x_1, \ldots, x_{n+1}) := x_1$ is such that the restriction $\pi|_{C_i}$ is dominant for $1 \leq i \leq N$, then the degree of π is the integer $D = \sum_{i=1}^N [K(C_i) : K(X_1)]$, where $[K(C_i) : K(X_1)]$ denotes the degree of the (finite) field extension $K(X_1) \to K(C_i)$ for $1 \leq i \leq N$.

Polynomials $f_1, \ldots, f_s$ are said to form a regular sequence in $K[X_1, \ldots, X_n]$ if f_1 is not zero and f_i is not a zero divisor in $K[X_1, \ldots, X_n]/(f_1, \ldots, f_{i-1})$ for $i = 2, \ldots, s$. In such a case, the affine variety $V := V(f_1, \ldots, f_s) \subset \mathbb{A}^n$ that they define is equidimensional of dimension $n - s$, and is called a set-theoretic complete intersection variety. Further, if the ideal $(f_1, \ldots, f_s)$ generated by $f_1, \ldots, f_s$ is radical, then we say that V is ideal-theoretic complete intersection.

Let V be an equidimensional sub-variety of $\mathbb{A}^n$ of dimension $\dim V = r$ defined by polynomials $f_1, \ldots, f_{n-r}$, and such that the ideal $\mathcal{I} := (f_1, \ldots, f_{n-r})$ of $K[X_1, \ldots, X_n]$ is radical. Then Noether's normalization theorem states that there exist linear forms $Y_1, \ldots, Y_r \in K[X_1, \ldots, X_n]/\mathcal{I}$ algebraically independent over $K[X_1, \ldots, X_n]/\mathcal{I}$ such that the extension

$$K[Y_1, \ldots, Y_r] \to K[X_1, \ldots, X_n]/\mathcal{I}$$

is finite. In such a case, we say that $Y_1, \ldots, Y_r$ are in Noether position with respect to the variety $V(f_1, \ldots, f_{n-r})$.

Let $f \in K[X]$ be a regular function of $\mathbb{A}^n$. Then the differential of f at a point $x \in \mathbb{A}^n$ is the linear map

$$\begin{array}{rcl} d_x f : K^n & \to & K \\ \xi & \mapsto & \sum_{i=1}^n \frac{\partial f}{\partial X_i}(x) \xi_i \end{array} .$$

Let $V \subset \mathbb{A}^n$ be a variety and $x \in V$. We define the tangent space of V at x by

$$T_xV = \{\xi \in \mathbb{A}^n : d_xg(\xi) = 0 \; \forall g \in \mathcal{I}(V)\}.$$

Let $W \subset \mathbb{A}^m$ be an algebraic variety. Let us assume that $\varphi : V \to W$ is a finite morphism. Let $y = (y_1, \ldots, y_m) \in W$ and let $\mathcal{M}_y$ be the maximal ideal of $K[Y_1, \ldots, Y_m]$ generated by the polynomials $Y_1 - y_1, \ldots, Y_m - y_m$. We borrow two notions from the realm of schemes. We say that the $K[W]_{\mathcal{M}_y}/\mathcal{M}_yK[W]_{\mathcal{M}_y}$–algebra

$$K[V]_{\mathcal{M}_y}/\mathcal{M}_yK[V]_{\mathcal{M}_y}$$

represents the fibre of y under φ.

We say that φ is unramified at a point $x \in V$ if, and only, if the differential map $d_x\varphi : T_xV \to T_{\varphi(x)}W$ is injective. We say that the fibre of $y \in \varphi(V) \subset W$ is unramified if φ is unramified at every $x \in \varphi^{-1}(y)$.

Assume further that V and W are equidimensional and of equal dimension $r := \dim V = \dim W$. Then, unramifiedness for the fibre of $y = \varphi(x)$ under φ is equivalent to $K[V]_{\mathcal{M}_y}/\mathcal{M}_yK[V]_{\mathcal{M}_y}$ being a product of fields. In fact, it must hold that

$$K[V]_{\mathcal{M}_y}/\mathcal{M}_yK[V]_{\mathcal{M}_y} = \left(K[W]_{\mathcal{M}_y}/\mathcal{M}_yK[W]_{\mathcal{M}_y}\right)^{\deg \varphi}.$$

A particular case of this situation which will be important for us is the following: assume that $V := V(f_1, \ldots, f_{n-r})$ is an ideal-theoretic complete intersection defined by polynomials $f_1, \ldots, f_{n-r} \in K[X_1, \ldots, X_n]$, the variables $X_1, \ldots, X_r$ are in Noether position and let $\varphi : V \to \mathbb{A}^r$ be the linear mapping defined by $\varphi(x) := (x_1, \ldots, x_r)$. Then φ is unramified at a point $y \in \mathbb{A}^r$ if and only if

$$\det\left(\left(\frac{\partial f_i}{\partial X_{j+r}}\right)_{1 \le i,j \le n-r}\right)(x) \ne 0$$

at every $x \in \pi^{-1}(y)$.

With the assumptions above, we say that φ verifies a generic condition, e.g., flatness or unramifiedness, if this condition holds for the generic fibre $K(X_1, \ldots, X_r)[X_{r+1}, \ldots, X_n]/(f_1, \ldots, f_{n-r})$. In particular, φ is generically unramified if and only if the Jacobian determinant

$$\det\left(\left(\frac{\partial f_i}{\partial X_{r+j}}\right)_{1\leq i,j\leq n-r}\right)$$

is a unit in $K(X_1,\dots,X_r)[X_{r+1},\dots,X_n]/(f_1,\dots,f_{n-r})$.

2.2.1. Geometric Solutions

The notion of a geometric solution of an algebraic variety was first introduced in the works of Kronecker and König in the last years of the XIXth century. Nowadays, geometric solutions are widely used in computer algebra to represent algebraic varieties, especially in the zero-dimensional case.

We first introduce this notion in the case of zero-dimensional varieties and then extend it to curves. Let $V=\{\xi^{(1)},\dots,\xi^{(D)}\}$ be a zero-dimensional sub-variety of $\mathbb{A}^n(\overline{K})$ defined over K. Let Y be a new indeterminate. A geometric solution of V consists of

- a linear form $u=u_1X_1+\cdots+u_nX_n\in K[X]$ which separates the points of V, i.e., satisfying $u(\xi^{(i)})\neq u(\xi^{(k)})$ for $i\neq k$,
- the minimal polynomial $m_u:=\prod_{1\leq i\leq D}(Y-u(\xi^{(i)}))\in K[Y]$ of u in V,
- polynomials $w_1,\dots,w_n\in K[Y]$, with $\deg w_j<D$ for every $1\leq j\leq n$, satisfying

$$V=\{(w_1(\eta),\dots,w_n(\eta))\in\overline{K}^n:\eta\in\overline{K},\ m_u(\eta)=0\}.$$

The linear form u is also a primitive element of the ring extension $K\to K[V]$ (or of V).

In the sequel, we shall be given a polynomial system $f_1=0,\dots,f_n=0$ of n-variate polynomials of $\mathbb{Q}[X]$ defining a zero-dimensional affine variety $V\subset\mathbb{A}^n(\mathbb{C})$. We shall consider the system $f_1=0,\dots,f_n=0$ (symbolically) "solved" if we obtain a geometric solution of V as defined above.

Example. Let $f_1,f_2\in\mathbb{Q}[X_1,X_2]$ be the following polynomials:

$$\begin{aligned}f_1&:=X_1^3-3X_1^2X_2+3X_1X_2^2-X_2^3-11X_1+9X_2+7,\\ f_2&:=X_1^2-2X_1X_2+X_2^2-3X_1+2X_2+1,\end{aligned}$$

which define the zero-dimensional variety $V := \{(4,1),(0,-1),(9,11)\}$ in $\mathbb{C}^2$. Let $u := X_1 - X_2 \in \mathbb{Q}[X_1, X_2]$. Note that u is a separating linear form for V. The geometric solution of V associated with u consists of

- the minimal polynomial $m_u := (Y-3)(Y-1)(Y+2) = Y^3 - 2Y^2 - 5Y + 6$,
- the polynomials $w_1 := Y^2 - 2Y + 1$ and $w_2 := Y^2 - 3Y + 1$, which satisfy the identities $(w_1(3), w_2(3)) = (4{,}1)$, $(w_1(1), w_2(1)) = (0{,}-1)$ and $(w_1(-2), w_2(-2)) = (9,11)$. □

The notion of geometric solution can be extended to equidimensional varieties of positive dimension. For our purposes, it will suffice to consider the case of curves.

Suppose that we are given a curve $V \subset \mathbb{A}^{n+1}$ defined by polynomials $f_1, \ldots, f_n \in K[T, X] = K[T, X_1, \ldots, X_n]$. Assume that for each irreducible component C of V, the identity $\mathcal{I}(C) \cap K[T] = \{0\}$ holds. This implies that the morphism $\pi|_C : C \to \mathbb{A}^1$ defined by $\pi(t,x) := t$ is dominant for each irreducible component C of V. Let u be a nonzero linear form of $K[X]$ such that u separates the points of a generic fibre $\pi^{-1}(t)$ (such a linear form will be called a primitive element of the ring extension $K(T) \to K(V)$ or of V). Let $\pi_u : V \to \mathbb{A}^2$ be the morphism defined by $\pi_u(x,t) := (t, u(x))$. Our assumptions on V imply that the Zariski closure $\overline{\pi_u(V)}$ of the image of V under π_u is an hypersurface of $\mathbb{A}^2$ defined over K. Then there exists a unique (up to scaling by nonzero elements of K) polynomial $M_u \in K[T, Y]$ of minimal degree defining $\overline{\pi_u(V)}$. Let $m_u \in K(T)[Y]$ denote the (unique) monic multiple of M_u with $\deg_Y(m_u) = \deg_Y(M_u)$. We call m_u the minimal polynomial of u in V. In these terms, a geometric solution of the curve V consists of

- the linear form $u \in K[X]$,
- the minimal polynomial $m_u \in K(T)[Y]$,
- elements $v_1, \ldots, v_n$ of $K(T)[Y]$ such that $\frac{\partial m_u}{\partial Y} X_i = v_i$ in $K(T) \otimes K[V]$ and $\deg_Y(v_i) < \deg_Y(m_u)$ holds for $1 \le i \le n$.

2.3. Complexity

Algorithms in computational algebraic geometry are usually described using the standard dense (or sparse) complexity model, i.e., encoding multivariate polynomials by means of the vector of all (or of all nonzero) coefficients. Taking into account that a generic n–variate polynomial of degree d has $\binom{d+n}{n} = O(d^n)$ nonzero coefficients, we see that the dense representation of multivariate polynomials requires an exponential size, and their manipulation usually requires an exponential number of arithmetic operations with respect to the parameters d and n. In order to avoid this exponential behavior, we are going to use an alternative encoding of input and intermediate results of our computations by means of straight-line programs (cf. [BCS97]).

2.3.1. Complexity model

A straight-line program β in $\mathbb{Q}(X) := \mathbb{Q}(X_1, \ldots, X_n)$ is a finite sequence of rational functions $(f_1, \ldots, f_k) \in \mathbb{Q}(X)^k$ such that for $1 \leq i \leq k$, the function f_i is an element of the set $\{X_1, \ldots, X_n\}$, or an element of $\mathbb{Q}$ (a parameter), or there exist $1 \leq i_1, i_2 < i$ such that $f_i = f_{i_1} \circ_i f_{i_2}$ holds, where $\circ_i$ is one of the arithmetic operations $+, -, \times, \div$. The straight-line program β is called division–free if $\circ_i$ is different from $\div$ for $1 \leq i \leq k$. A natural measure of the complexity of β is its time or length (cf. [BCS97]), which is the total number of arithmetic operations performed during the evaluation process defined by β. We say that the straight-line program β computes or represents a subset S of $\mathbb{Q}(X)$ if $S \subset \{f_1, \ldots, f_k\}$ holds.

Our model of computation is based on the concept of straight-line programs. However, a model of computation consisting *only* of straight-line programs is not expressive enough for our purposes. Therefore we allow our model to include decisions and selections (subject to previous decisions). For this reason we shall also consider computation trees, which are straight-line programs with branchings. The evaluation time of a given computation tree is defined similarly to the case of straight-line programs as the maximum evaluation time over the different branches (see, e.g., [vzG86], [BCS97] for more details on the notion of computation trees).

In the future, when we refer to algorithms we shall mean computation trees, and when we refer to their complexity or evaluation time we shall mean the number of arithmetic operations in $\mathbb{Q}$ they perform.

Our algorithms are of *Monte Carlo* or *BPP* type (see, e.g., [BDG88], [Zip93], [vzGG99]), i.e., they return the correct output with probability at least a fixed value strictly greater than 1/2. This means that the error probability can be made arbitrarily small by iteration of the algorithms. On the other hand, our algorithms do not seem to be of *Las Vegas* or *ZPP* type, i.e., we have no means of checking the correctness of our output results. We observe that the probabilistic aspect of our algorithms is related to the random choice of points outside certain Zariski closed subsets of suitable affine spaces, whose probability of success is explicitly estimated.

2.3.2. Probabilistic identity testing

A difficult problem to handle efficiently in the manipulation of multivariate polynomials given by straight–line programs is the so-called identity testing problem: given a straight-line program over K representing two polynomials f and g of $K[X] := K[X_1, \dots, X_n]$, decide whether f and g represent the same polynomial function on $\overline{K}^n$. Indeed, all known deterministic algorithms solving this problem have complexity at least $(\max\{\deg f, \deg g\})^{\Omega(n)}$. We are going to use *probabilistic* algorithms to solve the identity testing problem, based on the following result, know as the Zippel-Schwartz Theorem.

Theorem 2.1 ([vzGG99, Lemma 6.44]). *Let f be a nonzero polynomial of $\mathbb{C}[X]$ of degree at most d and let $\mathcal{S}$ be a finite subset of $\mathbb{C}$. Then the number of zeros of f in $\mathcal{S}^n$ is at most $d(\#\mathcal{S})^{n-1}$.*

For the analysis of our algorithms, we shall interpret the statement of Theorem 2.1 in terms of probabilities. More precisely, given a nonzero polynomial f in $\mathbb{C}[X]$ of degree at most d, we conclude from Theorem 2.1 that the probability of picking a random point a in $\mathcal{S}^n$ such that $f(a) = 0$ holds is bounded from above by $d/\#\mathcal{S}$ (assuming a uniform distribution of probability on the elements of $\mathcal{S}^n$).

2.3.3. Basic complexity estimates

In order to estimate the complexity of our procedures we shall frequently use the notation $\mathsf{M}(m) := m \log^2 m \log\log m$. Recall that log denotes the binary logarithm. Let R be a commutative ring of characteristic zero with unity. We recall that the number of arithmetic operations in R necessary to compute the multiplication or division with remainder of two univariate polynomials in $R[T]$ of degree at most m is $O\big(\mathsf{M}(m)/\log(m)\big)$ (cf. [vzGG99], [BP94]). Multipoint evaluation and interpolation of univariate polynomials of $R[T]$ of degree m at *invertible* points $a_1, \ldots, a_m \in R$ can be performed with $O\big(\mathsf{M}(m)\big)$ arithmetic operations in R (see, e.g., [BLS03]).

If $R = K$ is a field, then we shall use algorithms based on the Extended Euclidean Algorithm (EEA for short) in order to compute the gcd or resultant of two univariate polynomials in $K[T]$ of degree at most m with $O\big(\mathsf{M}(m)\big)$ arithmetic operations in K (cf. [vzGG99], [BP94]). We use Padé approximation in order to compute the dense representation of the numerator and denominator of a rational function $f = p/q \in K(T)$ with $\max\{\deg p, \deg q\} \leq m$ from its Taylor series expansion up to order $2m$. This also requires $O(\mathsf{M}(m))$ arithmetic operations in K ([vzGG99], [BP94]).

For brevity, we will denote by Ω the exponent that appears in the complexity estimate $O(n^{\Omega})$ for the multiplication of two $(n \times n)$-matrices with coefficients in $\mathbb{Q}$. We remark that the (theoretical) bound $\Omega < 2.376$ is typically impractical and we prefer to take $\Omega := \log 7 \sim 2.81$ (cf. [BP94]).

Finally, sometimes we will refer to rough complexity estimates and omit poly-logarithmic terms from the estimate. For example, a rough estimate for $O(m \log^2 m \log\log m)$ may be $O(m)$.

2.4. Deformation algorithms based on lifting techniques

We discuss in depth the lifting technique mentioned earlier in Section 1.1. This technique relies on a formal version of the Newton-Hensel lifting algorithm that was introduced, in the context of polynomial equation solving, in [GHM$^+$98] and [GHH$^+$97]. Its essentials became described in [HKP$^+$00] and its study was continued in [BMWW04], [Sch03], and [JMSW09].

Deformation algorithms based on lifting techniques appear in flavours of the following statement:

Let n be a positive integer and let $F_1, \ldots, F_n \in \mathbb{Q}[T, X_1, \ldots, X_n]$ be polynomials defining an equidimensional algebraic variety $\mathcal{V} \subseteq \mathbb{A}^{n+1}$ of dimension 1. Let $\pi : \mathcal{V} \to \mathbb{A}^1$ be the morphism defined by $\pi(t, x) := t$ for $(t, x) := (t, x_1, \ldots, x_n) \in \mathcal{V}$. Assume π to be finite and generically unramified. Let $g \in \mathbb{Q}[\mathcal{V}]$ be the element in the coordinate ring of $\mathcal{V}$ that is defined by a polynomial $G \in \mathbb{Q}[T, X]$. Then, there exists a unique polynomial $P \in \mathbb{Q}[T, Y]$ which is the (minimal) integral dependence equation that is satisfied by g in the extension $\mathbb{Q}[T] \to \mathbb{Q}[\mathcal{V}]$.

Suppose furthermore that we are given a point $t_0 \in \mathbb{Q}$ such that its fibre under π is unramified and that G maps $\pi^{-1}(t_0)$ onto $\deg_Y P$ distinct points.

The projection problem is that of computing P given the polynomials $F_1, \ldots, F_n$, the polynomial G and a geometric solution of the affine zero-dimensional variety $\pi^{-1}(t_0)$. We call P the projection of g onto $\mathcal{V}$.

The main algorithm in [HKP$^+$00] solves the projection problem when $F_1, \ldots, F_n, G$ are given by a straight-line program in $\mathbb{Q}[T, X]$ such that $F_1, \ldots, F_n$ form a regular sequence and span a radical ideal in $\mathbb{Q}[T, X]$, and the geometric solution of the fibre $\pi^{-1}(t_0)$ is provided by the dense representation of the univariate polynomials in $\mathbb{Q}[Y]$ that define it. The output P is provided in its dense representation. The computation takes roughly

$$O((\mathcal{T} + n^4)(\deg \pi)^3 \deg_T P) = O(\mathcal{T} n^4 (\deg \pi)^3 \deg \mathcal{V} \deg_X G) \tag{2.2}$$

arithmetic operations in $\mathbb{Q}$ (omitting poly-logarithmic terms). Here, $\deg_T P$ denotes the partial degree of P in the variable T and $\deg_X G$ denotes the partial degree of G in the variables $X_1, \ldots, X_n$, $\deg V$ stands for the degree of the affine variety V and $\deg \pi$ stands for the degree of the morphism π.

Note that when G is a generic linear form (i.e., $\deg_X G = 1$), its projection is actually the minimal polynomial in a geometric solution (that has G as its separating linear form). In this case, $\deg_Y P = \deg \pi$ since G separates points on $\pi^{-1}(t_0)$, so $\#\pi^{-1}(t_0) = \deg \pi$, and therefore $P(t_0, Y)$ has $\deg \pi$ distinct roots.

It can also be shown (see, e.g., [DMW09]) that a complexity estimate of order $\deg \pi^{O(1)} \deg \mathcal{V}^{O(1)}$ is unavoidable; in fact, by tracing how these parameters are introduced one sees that $\deg \mathcal{V}$ is the accuracy we require for our approximations and $\deg \pi$ is the number of approximations we should compute (i.e., one per point in the zero-dimensional variety $\pi^{-1}(t_0)$). However, a reduction to roughly

$$O(n^5 \mathcal{T} \deg \pi (\deg \mathcal{V}) \deg_X G)$$

arithmetic operations in $\mathbb{Q}$ is possible (see Theorem 2.2 below; see also [GLS01] and [Sch03]).

2.4.1. The lifting process

Let the notions and notations from the preceding section hold. Let us see how to compute the minimal polynomial P of the projection of $\mathcal{V}$ defined by a linear form $U \in K[X]$ (i.e., the minimal integral dependence equation in $K[T] \to K[\mathcal{V}]$ of a representative of $U \in K[X]$ in $K[\mathcal{V}]$). Extending this procedure to an arbitrary polynomial $G(T, X)$ is straightforward but unnecessary for what follows (see [HKP$^+$00] for details).

We discuss the extension of [Sch03] to a method of [GLS01] for computing a geometric solution of the curve V.

Theorem 2.2. *Let $F_1, \dots, F_n \in K[T, X]$, t_0 be a point in K, U be a linear form in $K[X_1, \dots, X_n]$ and $q, w_1, \dots, w_n \in K[Y]$. Let $\mathcal{V} \subset \mathbb{A}^{n+1}$ be the variety defined by $F_1, \dots, F_n$, and let $\pi : \mathcal{V} \to \mathbb{A}^1$ be the morphism defined by the projection $\pi(t, x) := t$. Assume that:*

- *The polynomials $F_1, \dots, F_n$ form a regular sequence and span a radical ideal in $K[T, X]$; also, they are computed by a straight-line program β in T operations over K.*
- *The morphism π is dominant and generically unramified.*
- *It holds that $\#\pi^{-1}(t_0) = \deg \pi$.*
- *The coordinate functions defined by the linear form U are primitive elements in both the extension $K \to K[\mathcal{V}_{t_0}]$ and $K[T] \to K[\mathcal{V}]$, where $\mathcal{V}_{t_0}$ is the sub-variety of $\mathbb{A}^n$ for which $\pi^{-1}(t_0) = \{t_0\} \times \mathcal{V}_{t_0}$ holds.*
- *The polynomials $q, w_1, \dots, w_n$ define a geometric solution of the zero dimensional variety $\mathcal{V}_{t_0}$ with respect to the linear form U.*

Assume we are given the straight–line program β computing $F_1, \ldots, F_n$, the coordinates defining U, the point t_0 and the vectors that stand for the dense representation of $q, v_1, \ldots, v_n$. Then, we can compute a geometric solution of $\mathcal{V}$ with $O((n\mathsf{T} + n^3)\mathsf{M}(\deg \pi)\mathsf{M}(\deg_T m_u))$ operations in K.

Proof. We want to compute polynomials $\hat{q}, \hat{v}_1, \ldots, \hat{v}_n \in K(T)[Y]$ defining a geometric solution of $\mathcal{V}$ with respect to the linear form U. Let $E := \deg_T m_u$. In order to do this, we claim that we can compute polynomials $Q, W_1, \ldots, W_n \in K[T, Y]$ such that

$$\begin{aligned} Q(T, U(X)) &\equiv \hat{q}(T, U(X)) \quad \bmod (T - t_0)^E \quad \text{and} \\ W_i(T, U(X)) &\equiv \left(\tfrac{\partial \hat{q}}{\partial Y}(T, U(X))\right)^{-1} \cdot \hat{v}_i(T, U(X)) \quad \bmod (T - t_0)^E \end{aligned} \tag{2.3}$$

in $K[\![T - t_0]\!][X]/(F_1, \ldots, F_n)$ for $1 \leq i \leq n$. Indeed, the existence of $\hat{q}, \hat{v}_1, \ldots, \hat{v}_n$ follows from our hypotheses. Since U separates the points of $\pi^{-1}(t_0)$ we conclude that $\hat{q}(t_0, Y)$ is a separable element of $K[Y]$. This shows that $\hat{q}(t_0, Y)$ and $\partial\hat{q}(t_0, Y)/\partial Y$ are relatively prime in $K[Y]$. Hence, $\partial\hat{q}/\partial Y$ is invertible mod $\hat{q}(T, Y)$ in $K[\![T - t_0]\!][Y]$ and thus, $\partial\hat{q}/\partial Y(T, U(X))$ is invertible in $K[\![T - t_0]\!][X_1, \ldots, X_n]/(F_1, \ldots, F_n)$.

As shown in the next claim, we compute the polynomials $W_1, \ldots, W_n, Q \in K[T, Y]$ through a recursive procedure which at step $\kappa \in \{0, 1, \ldots, \lceil \log E + 1 \rceil\}$ produces polynomials $R_1^{[\kappa]}, \ldots, R_{n+1}^{[\kappa]}$ that agree with $(\partial\hat{q}/\partial Y)^{-1}\hat{v}_1, \ldots, (\partial\hat{q}/\partial Y)^{-1}\hat{v}_n, \hat{q}$ in $\overline{K}[\![T - t_0]\!][Y]$ mod $(T - t_0)^{2^\kappa}$, e.g., with precision 2^κ, as depicted in (2.3). Once we computed the approximations with precision $2E$, we can use Padé approximation to recover the sought geometric solution.

Let $\mathcal{A} := \overline{K}[\![T - t_0]\!]$ and $\mathfrak{o} := (T - t_0)$. Write $X_{n+1} := Y$ and for the remainder of this section let $X := (X_1, \ldots, X_{n+1})$. Let

$$\varphi(X) := (X_1 - W_1(X_{n+1}), \ldots, X_n - W_n(X_{n+1}), Q(X_{n+1}))$$

in $(\mathcal{A}[X])^{n+1}$ denote the vector whose coordinates are the images of

$$X_1 - (\partial\hat{q}/\partial Y)^{-1}\hat{v}_1, \ldots, X_n - (\partial\hat{q}/\partial Y)^{-1}\hat{v}_n, \hat{q}$$

in $\mathcal{A}[X]$. Write $\varphi(X) = (\varphi_1, \ldots, \varphi_{n+1})(X)$. Note that, for every $1 \leq j \leq n + 1$, the polynomial φ_j of $\mathcal{A}[X]$:

- is monic in X_j,
- is reduced modulo $(\varphi_{j+1}, \dots, \varphi_{n+1})$ in the lexicographical order with $X_{n+1} > X_n > \cdots > X_1$.
- depends only on the variables $X_j, \dots, X_{n+1}$.

Moreover, let
$$F := (F_1(X), \dots, F_n(X), X_{n+1} - U(X))$$
denote the above tuple of polynomials considered as elements of $\mathcal{A}[X]$.

Claim: We claim that for each $\kappa \in \mathbb{Z}_{\geq 0}$, we can compute polynomials $R_1^{[\kappa]}, \dots R_{n+1}^{[\kappa]}$ in $K[T, X]$ such that their images in $(\mathcal{A}/\mathfrak{o}^{2^{\kappa+1}})[X]$ satisfy the following conditions:

a) $R_j^{[\kappa]}$ is monic in X_j,

b) $R_j^{[\kappa]} \equiv \varphi_j \bmod \mathfrak{o}^{2^\kappa}$ in $(\mathcal{A}/\mathfrak{o}^{2^{\kappa+1}})[X]$, and

c) $R_j^{[\kappa]}$ has the same support as φ_j

for $1 \leq j \leq n+1$. (The tuple $R^{[\kappa]}$ is to be understood as an approximation to φ of precision 2^κ in the modular ring $\mathcal{A}/\mathfrak{o}^{2^{\kappa+1}}[X]$.)

Proof of the Claim. Consider the ideals

$$(F_1(t_0, X), \dots, F_n(t_0, X), X_{n+1} - U(X)), \tag{2.4}$$
$$(X_1 - W_1(t_0, X_{n+1}), \dots, X_n - W_n(t_0, X_{n+1}), Q(t_0, X_{n+1})) \tag{2.5}$$

of $K[X]$. Since the ideal spanned by the $(F_1(t_0, X), \dots, F_n(t_0, X))$ in $K[X]$ is radical, the ideal in (2.4) is also radical. By definition of geometric solution, the varieties generated by the ideals (2.4) and (2.5) agree. Hence, it follows that these ideals are equal. Considering the univariate polynomials $q, w_1, \dots, w_n \in K[X_{n+1}]$ in the given geometric solution of $\pi^{-1}(t_0)$ as polynomials in $\mathcal{A}[X]$, it follows that $Q(t_0, X_{n+1}) = q(X_{n+1})$ and $W_i(t_0, X_{n+1}) = w_i(X_{n+1})$ for $1 \leq i \leq n$ in $\mathcal{A}[X]$. Then, each entry of

$$R^{[0]} := (X_1 - w_1(X_{n+1}), \dots, X_n - w_n(X_{n+1}), q(X_{n+1}))$$

is congruent to the corresponding entry of φ modulo $(T - t_0) = \mathfrak{o}^{2^0}$ in $\mathcal{A}[X]$ which implies b) for $\kappa = 0$. Conditions a) and c) are also fulfilled for $\kappa = 0$ by definition.

Let $\kappa \geq 0$ and assume that $R^{[\kappa]}$ fulfilling the hypotheses has been computed.

Let $\mathcal{H}_\kappa$ denote the ring $\mathcal{H}_\kappa := (\mathcal{A}/\mathfrak{o}^{2^{\kappa+1}})[X]/(R^{[\kappa]})$. By construction, $\mathcal{H}_\kappa$ is a free $(\mathcal{A}/\mathfrak{o}^{2^{\kappa+1}})$–module, and the monomials $\{X_1^{\alpha_1} \cdots X_{n+1}^{\alpha_{n+1}} : 0 \leq \alpha_i < \deg_{X_j} R_j^{[\kappa]}$ for $1 \leq j \leq n+1\}$ form a basis of this module. For any element $a \in \mathcal{A}[X]$, write a_κ for its projection in $\mathcal{H}_\kappa$.

Let $J(F) := (\partial F_i/\partial X_j)_{1 \leq i,j \leq n+1}$ denote the Jacobian matrix of $F_1, \ldots, F_{n+1}$ with respect to $X_1, \ldots, X_{n+1}$ in $\mathcal{A}[X]$. We make the following sub-claim:

Sub-claim 1. It holds that

$$J(R^{[\kappa]})_\kappa J(F)_\kappa^{-1} F_\kappa = \varphi_\kappa$$

in $\mathcal{H}_\kappa$.

Proof of sub-claim 1. Note that the Jacobian determinant $\det(J(F))$ is invertible in $\mathcal{A}[X]/(\varphi)$, since it is invertible in $K(T)[X]/(\varphi)$ and π is unramified at t_0.

Note that the ideals

$$(F_1(T, X), \ldots, F_n(T, X), X_{n+1} - U(X))$$

and

$$(X_1 - W_1(T, X_{n+1}), \ldots, X_n - W_n(T, X_{n+1}), Q(T, X_{n+1}))$$

of $K(T)[X]$ are equal. This implies that we may write every coordinate in F as a combination of the coordinates of φ. Moreover, we can assume that none of the denominators in T appearing in these equalities vanishes at $T = t_0$. This implies that there exists a matrix $A \in \mathcal{A}[X]^{(n+1)\times(n+1)}$ such that $F = A\varphi$.

Since $F = A\varphi$ in $\mathcal{A}[X]$ holds, the equality

$$J(F) = AJ(\varphi) + B$$

follows, where $B \in \mathcal{A}[X]^{(n+1)\times(n+1)}$ is a matrix whose entries belong to the ideal $(\varphi_1, \ldots, \varphi_{n+1}) \subset \mathcal{A}[X]$. On the other hand, by hypotheses we have that $\varphi_j \equiv R_j^{[\kappa]} \bmod \mathfrak{o}^{2^\kappa}$ holds in $(\mathcal{A}/\mathfrak{o}^{2^{\kappa+1}})[X]$ and hence

$$\varphi_j \equiv 0 \bmod \mathfrak{o}^{2^\kappa}$$

in $(\mathcal{A}/\mathfrak{o}^{2^{\kappa+1}})[X]/(R^{[\kappa]}) = \mathcal{H}_\kappa$. Combining these two facts, we deduce that in the equality

$$J(F)_\kappa = A_\kappa J(\varphi)_\kappa + B_\kappa \tag{2.6}$$

of $\mathcal{H}_\kappa$, all the entries in B_κ belong to the ideal $\mathfrak{o}^{2^\kappa}\mathcal{H}_\kappa$, or equivalently, that

$$J(F)_\kappa = A_\kappa J(\varphi)_\kappa \qquad \bmod \mathfrak{o}^{2^\kappa}$$

in $\mathcal{H}_\kappa$.

Since $J(F)_\kappa$ is invertible in $\mathcal{H}_\kappa/\mathfrak{o}^{2^\kappa}\mathcal{H}_\kappa$, this implies that A_κ and $J(\varphi)_\kappa$ are also invertible in $\mathcal{H}_\kappa/\mathfrak{o}^{2^\kappa}\mathcal{H}_\kappa$. Moreover, by Hensel's Lemma we deduce that $J(F)_\kappa, A_\kappa$ and $J(\varphi)_\kappa$ are also invertible in $\mathcal{H}_\kappa$.

By multiplying both sides of (2.6) to the right by $J(\varphi)_\kappa^{-1}$ and to the left by $J(\varphi)_\kappa J(F)_\kappa^{-1}$ in $\mathcal{H}_\kappa$ we have

$$I = J(\varphi)_\kappa J(F)_\kappa^{-1} A_\kappa + J(\varphi)_\kappa J(F)_\kappa^{-1} B_\kappa J(\varphi)_\kappa^{-1},$$

which in turn, implies

$$J(\varphi)_\kappa J(F)_\kappa^{-1} A_\kappa = I + C_\kappa \tag{2.7}$$

where the entries of C_κ belong to the ideal $\mathfrak{o}^{2^\kappa}$ of $\mathcal{H}_\kappa$. Finally, multiplying both sides of (2.7) to the right by φ_κ and replacing $A_\kappa\varphi_\kappa$ by F_κ (they are equal!), we obtain

$$J(\varphi)_\kappa J(F)_\kappa^{-1} A_\kappa \varphi_\kappa = J(\varphi)_\kappa J(F)_\kappa^{-1} F_\kappa = \varphi_\kappa + C_\kappa\varphi_\kappa = \varphi_\kappa$$

in $\mathcal{H}_\kappa$, where $C_\kappa\varphi_\kappa = 0$ since they are both elements of $\mathfrak{o}^{2^\kappa}$ and therefore their product belongs to $\mathfrak{o}^{2^{\kappa+1}}$.

In fact, since $R^{[\kappa]} - \varphi_\kappa$ is in the ideal $\mathfrak{o}^{2^\kappa}\mathcal{H}_\kappa$ of $\mathcal{H}_\kappa$, it follows that each entry of $J(R^{[\kappa]}) - J(\varphi_\kappa)$ is also in $\mathfrak{o}^{2^\kappa}\mathcal{H}_\kappa$. On the other hand, every entry of $F_\kappa = A_\kappa\varphi_\kappa$ is also in this ideal, since every entry in φ_κ belongs to $\mathfrak{o}^{2^\kappa}\mathcal{H}_\kappa$. Hence, combining these two facts we deduce that $(J(R^{[\kappa]}) - J(\varphi_\kappa))J(F)_\kappa^{-1}F_\kappa = 0$ in

$\mathcal{H}_\kappa$ and therefore we may replace $J(\varphi_\kappa)$ by $J(R^{[\kappa]})$ in the above equality and obtain:

$$J(R^{[\kappa]})_\kappa J(F)_\kappa^{-1} F_\kappa = \varphi_\kappa \tag{2.8}$$

in $\mathcal{H}_\kappa$ which proves sub-claim 1. **QED.**

Assume $J(R^{[\kappa]})_\kappa J(F)_\kappa^{-1} F_\kappa$ is computed in $\mathcal{H}_\kappa$ and let $\delta_\kappa = (\delta_{\kappa,1}, \ldots, \delta_{\kappa,n})$ denote a representative of $J(R^{[\kappa]})_\kappa J(F)_\kappa^{-1} F_\kappa$ in $\mathcal{A}/\mathfrak{o}^{2^{\kappa+1}}[X]$ that it is chosen so that[1]

$$\deg_{X_i}(\delta_{\kappa,j}) < \deg_{X_i} R_i^{[\kappa]} \quad \text{for } 1 \leq i, j \leq n+1. \tag{2.9}$$

From (2.8) we deduce that each entry in the tuple $\delta_\kappa - \varphi_\kappa$ is in the ideal $(R^{[\kappa]})$ of $\mathcal{A}/\mathfrak{o}^{2^{\kappa+1}}[X]$. Evidently the same happens with the entries of $\delta_\kappa - \varphi_\kappa + R^{[\kappa]}$; moreover, the next sub-claim proves that $R_j^{[\kappa]} + \delta_{\kappa,j} = \varphi_{j,\kappa}$ in $\mathcal{A}/\mathfrak{o}^{2^{\kappa+1}}[X]$.

Sub-claim 2. It holds that $\delta_{\kappa,j} = \varphi_{j,\kappa} - R_j^{[\kappa]}$ in $\mathcal{A}/\mathfrak{o}^{2^{\kappa+1}}[X]$.

Proof of sub-claim 2. Let $g_j := \delta_{\kappa,j} - \varphi_{j,\kappa} + R_j^{[\kappa]}$ in $\mathcal{A}/\mathfrak{o}^{2^{\kappa+1}}[X]$ for every $1 \leq j \leq n+1$.

When $j = n+1$ we have (by the inductive hypotheses) that both $R_{n+1}^{[\kappa]}$ and $\varphi_{n+1,\kappa}$ depend only on X_{n+1}, they are monic and of the same degree, so that $\deg_{X_{n+1}}(R_{n+1}^{[\kappa]} - \varphi_{n+1}) < \deg_{X_{n+1}}(R_{n+1}^{[\kappa]})$. Moreover, from (2.9) we deduce that $\deg_{X_i}(g_{n+1}) < \deg_{X_i}(R_i^{[\kappa]})$ for every $1 \leq i \leq n+1$. Since $\deg_{X_i}(R_i^{[\kappa]}) = 1$ for $1 \leq i \leq n$, we see that $g_{n+1} \in \mathcal{A}/\mathfrak{o}^{2^{\kappa+1}}[X_{n+1}]$. Furthermore, $\deg_{X_{n+1}} g_{n+1} < \deg_{X_{n+1}} R_{n+1}^{[\kappa]}$ and g_{n+1} is in the ideal $(R_{n+1}^{[\kappa]})$ of $\mathcal{A}/\mathfrak{o}^{2^{\kappa+1}}[X_{n+1}]$. This proves that $g_{n+1} = 0$.

For $j \leq n$, as before, we have that both $R_j^{[\kappa]}$ and $\varphi_{j,\kappa}$ are monic in X_j and of the same degree $\deg_{X_j}(R_j^{[\kappa]})$, so that $\deg_{X_j}(R_j^{[\kappa]} - \varphi_{j,\kappa}) < \deg_{X_j}(R_j^{[\kappa]})$. Moreover, from (2.9) we deduce that $\deg_{X_j}(g_j) < \deg_{X_j}(R_j^{[\kappa]})$.

Since φ_j is reduced modulo $\varphi_{j+1}, \ldots, \varphi_{n+1}$, this implies that

$$\deg_{X_i}(\varphi_j) < \deg_{X_i}(R_i^{[\kappa]}) \quad \text{for } j < i \leq n+1.$$

Hence, this also holds for $\varphi_{j,\kappa}$ and for $R_j^{[\kappa]}$; in the latter case this is because, by hypotheses, $R_j^{[\kappa]}$ has the same support as φ_j. Again, by equality (2.9) we

[1] We take the convention that the degree of the polynomial zero $\deg 0 = -\infty$ is smaller than every integer; so that when $\delta_{\kappa,j} = 0$ the inequality holds.

deduce that $\deg_{X_i}(g_j) < \deg_{X_i}(R_i^{[\kappa]})$ for $i = j+1, \ldots, n+1$. Finally, since $R_j^{[\kappa]}$ and $\varphi_{j,\kappa}$ have the same support and only depend on $X_j, \ldots, X_{n+1}$ we deduce as before that $g_j = 0$ in $\mathcal{A}/\mathfrak{o}^{2^{\kappa+1}}[X]$ thus proving sub-claim 2. **QED.**

Thence, we can set $R^{[\kappa+1]}$ as a representative of $R^{[\kappa]} + \delta_\kappa$ in $\mathcal{A}/\mathfrak{o}^{2^{\kappa+2}}[X]$. One verifies that $R^{[\kappa+1]}$ fulfils all the conditions in the inductive argument proving our claim. **QED.**

To estimate the complexity of each step, we first make some auxiliary estimations. The cost of operations in $\mathcal{H}_\kappa$ requires computations modulo $R^{[\kappa]}$ and next reduction modulo $\mathfrak{o}^{2^{\kappa+1}} = (T - t_0)^{2^{\kappa+1}}$. Since the polynomials $R_1^{[\kappa]}, \ldots, R_n^{[\kappa]}$ have their total degree bounded by $\deg \pi$ in $X_1, \ldots, X_{n+1}$, any arithmetic operation in $\mathcal{H}_\kappa$ has a cost of roughly $O(n(\deg \pi)2^{\kappa+1})$ arithmetic operations in K. Since $R^{[\kappa]}$ is constituted of $n+1$ vectors in $\mathcal{H}_\kappa$, evaluating the vector has a cost of $O(n(\deg \pi)2^\kappa)$ arithmetic operations in K. The evaluation of the matrix $J(F)$ is done using Baur-Strassen's algorithm ([BS83]) and then the evaluation of F and $J(F)$ can be estimated by $O(n\mathsf{T})$. Finally, linear algebra can be done using Samuelson's algorithm in $O(n^4)$ complexity. Combining these facts we deduce that roughly $O((n\mathsf{T}+n^4)(\deg \pi)2^{\kappa+1})$ arithmetic operations in K are required for each recursive step. Therefore, the computation of the approximation up to precision $2E = 2\deg_T m_u$ requires roughly $O((n\mathsf{T} + n^4)(\deg \pi)\deg_T m_u)$ arithmetic operations in K.

The reconstruction of the sought geometric solution is done using Padé approximation and uses at most $O(n \deg_T m_u)$ additional operations in K (cf. [BP94], [vzGG99]), thus the estimate for the whole procedure remains in $O((n\mathsf{T} + n^4)(\deg \pi)\deg_T m_u)$ arithmetic operations in K. □

Let $t_1 \in K$ be a new point in $\mathbb{A}^1$. Then, we can compute the geometric solution of $\pi^{-1}(t_1)$ by first applying the above procedure, specialising in t_1 and eventually cleaning multiplicities.

Lemma 2.3 (see [GLS01, §6.5]). *Let notations and assumptions be as in Theorem 2.2. Let be given $t_1 \in K$ such that U separates the points of the fibre $\pi^{-1}(t_1)$ and a geometric solution of $\mathcal{V}$ with underlying linear form U. Then we can compute a geometric solution of $\pi^{-1}(t_1)$ with $O(n\mathsf{M}(\deg \pi))$ arithmetic operations in K.*

2.4.2. From minimal equations to geometric solutions

We have exhibited a lifting technique which, given polynomials defining a curve, a lifting point, the coefficients of a linear separating form and the geometric solution of the corresponding fibre, computes the geometric solution of such a curve. However, in some cases it is possible to compute the minimal equation of the image of a projection through a different procedure and what is needed is to complete this to a geometric solution (e.g., see Section 5.2.4). We describe an algorithm that, given a procedure for computing a minimal equation for a primitive element in a zero-dimensional or a one-dimensional equidimensional variety, produces the geometric solution of this variety.

This procedure is extracted from [JMSW09] and [DMW09], both of which I co-authored, and is inspired in an idea of [GLS01].

Let notions and notations be as above and let $\Lambda_1, \ldots, \Lambda_n$ be new indeterminates over K. We return to the notation $X := (X_1, \ldots, X_n)$ and set $\Lambda := (\Lambda_1, \ldots, \Lambda_n)$. Denote by $I_{K(\Lambda)} \subset K(\Lambda)[X]$ the extension ideal of $I(V) \subset K[X]$. Note that the linear form $U := \Lambda_1 X_1 + \ldots + \Lambda_n X_n$ separates the points of $V(I_{K(\Lambda)})$. Suppose that we are given an algorithm Ψ in $K(\Lambda)$ which computes the minimal polynomial $m_U \in K[\Lambda, Y]$ of U in $K(\Lambda) \to K(\Lambda)/I_{K(\Lambda)}$ with T arithmetic operations in $K(\Lambda)$ and a separating linear form $u := \lambda_1 X_1 + \ldots + \lambda_n X_n \in K[X]$ such that the vector $(\lambda_1, \ldots, \lambda_n)$ annihilates none of the denominators in $K[\Lambda]$ of any intermediate result of the algorithm Ψ.

Note that $m_U(\Lambda, U)$ is in $I(\mathbb{A}^n \times V)$. Since $I(\mathbb{A}^n \times V)$ is generated by polynomials in $K[X]$, it follows that the derivative of $m_U(\Lambda, U)$ with respect to Λ_i,

$$\frac{\partial m_U}{\Lambda_i}(\Lambda, U) = \frac{\partial m_U}{\partial Y}(\Lambda, U) X_i + \frac{\partial m_U}{\partial \Lambda_i}(\Lambda, U),$$

also belongs to $I(\mathbb{A}^n \times V)$ for $1 \leq i \leq n$. Observe that the equality $\deg m_u = D := \#V$ and the estimate $\deg((\partial m_U/\partial \Lambda_i)(\lambda, Y)) \leq D-1$ hold. Substituting λ for Λ in $m_U(\Lambda, Y)$ we obtain $m_u(Y)$. Making the same substitution in $(\partial m_U/\partial Y)(\Lambda, Y)X_i + (\partial m_U/\partial \Lambda_i)(\Lambda, Y)$ for $1 \leq i \leq n$ and reducing modulo $m_u(Y)$ we obtain polynomials

$$\frac{\partial m_u}{\partial Y}(Y) X_i - v_i(Y)$$

that belong to the ideal $I(V)$ of $K[X]$.

Since $m_u(Y)$ is square-free, it follows that $m_u(Y)$ and $(\partial m_u/\partial Y)(Y)$ are relatively prime in $K[Y]$. Thus, we can compute a polynomial $(\partial m_u/\partial Y)^{-1}(Y)$ of degree at most $D-1$ representing the inverse of $(\partial m_u/\partial Y)(Y)$ modulo $m_u(Y)$. Hence, multiplying this polynomial by v_k modulo $m_u(Y)$ we obtain a polynomial $w_k(Y) := (\partial m_u/\partial Y)^{-1}v_k$ such that $\deg w_k < D$ and $w_k(u) - X_k \in I(V)$ for $1 \leq k \leq n$. Since u is a separating linear form, it follows that $w_1, \dots, w_n$ together with m_u form a geometric solution of V.

In order to compute the polynomials $w_1, \dots, w_n$, we observe that the Taylor expansion of $m_U(\Lambda, Y)$ in powers of $\Lambda - \lambda$ has the following expression

$$m_U(\Lambda, Y) = m_u(Y) + \sum_{k=1}^{n}\left(\frac{\partial m_u}{\partial Y}(Y)X_k - v_k(Y)\right)(\Lambda_k - \lambda_k) \mod (\Lambda-\lambda)^2. \tag{2.10}$$

We compute this first order expansion by computing the first-order Taylor expansion of each intermediate result in the algorithm Ψ. In this way, each arithmetic operation in $K(\Lambda)$ arising in the algorithm Ψ becomes an arithmetic operation between two polynomials of $K[\Lambda]$ of degree at most 1, and is truncated up to order $(\Lambda - \lambda)^2$. Since the first-order Taylor expansion of an addition, multiplication or division of two polynomials of $K[\Lambda]$ of degree at most 1 requires $O(n)$ arithmetic operations in K, we have that the whole step requires $O(n\mathsf{T})$ arithmetic operations in K, where T is the number of arithmetic operations in $K(\Lambda)$ performed by the algorithm Ψ.

The computation of the polynomials $w_1, \dots, w_n$ requires the inversion of $\partial m_u/\partial Y$ modulo $m_u(Y)$ and the modular multiplication

$$w_k(Y) := (\partial m_u/\partial Y)^{-1}v_k(Y)$$

for $1 \leq k \leq n$. These steps can be executed with additional $O\big(n\mathsf{M}(D)\big)$ arithmetic operations in K.

Hence, this solution can be computed with $O(n(\mathsf{T} + \mathsf{M}(D)))$ arithmetic operations in K. We can thus state this in the form of the following lemma.

Lemma 2.4. *Suppose that we are given:*

1. *an algorithm Ψ in $K(\Lambda)$ which computes the minimal polynomial $m_U \in K[\Lambda, Y]$ of $U := \Lambda X_1 + \cdots + \Lambda_n X_n$ with T arithmetic operations in $K(\Lambda)$,*

2. *a separating linear form* $u := \lambda_1 X_1 + \cdots + \lambda_n X_n \in K[X]$ *such that the vector* $(\lambda_1, \ldots, \lambda_n)$ *annihilates none of the denominators that are part of the intermediate results of the algorithm* Ψ *in* $K[\Lambda]$.

Then a geometric solution of the variety V *can be (deterministically) computed with* $O\big(n(\mathsf{T} + \mathsf{M}(D))\big)$ *arithmetic operations in* K.

In the situations of interest T is a polynomial of degree at least quadratic in D. Then the term $O(n\mathsf{T})$ dominates the complexity of the whole procedure for computing the geometric solutions under consideration, which includes the cost of the computation of projections and the subsequent use of this procedure in order to obtain such a geometric solution. Hence, we shall concentrate in computing projections efficiently.

Chapter 3

Robust algorithms for generalized Pham systems

We announced earlier that this chapter was going to be devoted to a family called *generalized Pham systems* or *strict complete intersections*, which were introduced in [PS04] and [CDS96]. Recall that an n–dimensional generalized Pham system is defined by n polynomials of the form $\phi_i - \varphi_i$ $(1 \leq i \leq n)$, where $\phi_i \in \mathbb{Q}[X_1, \ldots, X_n]$ is homogeneous of degree d_i, φ_i has degree less than d_i and $\phi_1, \ldots, \phi_n$ define the empty projective variety of $\mathbb{P}^{n-1}(\mathbb{C})$.

This chapter is based on an article of the same title that I co-authored with Ezequiel Dratman and Guillermo Matera ([DMW09]) and has two main results, one on lower bounds for generalised Pham systems and one on upper-bounds. We shall cover only the upper bound and not include the lower bound which is certainly not the topic of this thesis.

In Section 3.2 we prove Theorem 3.15. Namely, we exhibit a probabilistic algorithm which solves generalized Pham systems with quadratic complexity in the Bézout number $D = d_1 \cdots d_n$. As we discussed, the straightforward application of the deformation technique of Theorem 2.2 does not yield an efficient algorithm. A clever procedure that uses multiple deformations will endow us with a better result.

For this purpose, for $1 \leq r \leq n+1$, we define a sequence of homotopies $\pi_r : \mathcal{V}_r \to \mathbb{A}^1$ such that:

1. The fibre $\pi_1^{-1}(0)$ is unramified and "easy to solve",

2. For $1 \leq r \leq n$, the fibre $\pi_r^{-1}(1)$ is unramified and the equality $\pi_r^{-1}(1) = \pi_{r+1}^{-1}(0)$ holds, and $\pi_{n+1}^{-1}(1) = \{1\} \times V$ holds, where $V = V(\phi_1 - \varphi_1, \dots, \phi_n - \varphi_n)$.
3. For $1 \leq r \leq n+1$, our projection algorithm lifts $\pi_r^{-1}(0)$ to $\mathcal{V}_r$ with complexity that is quadratic in the Bézout number of the original input system.

These homotopies are reminiscent of certain "piecewise–linear homotopies" of numerical continuation methods acting coordinate by coordinate (see, e.g., [Sai83], [Duv90]). Basing our algorithm in these deformations, we shall take roughly $O\big((n\mathsf{T}+n^3)\mathsf{M}(D)\sum_{r=1}^{n+1}\mathsf{M}(D/d_r)\big)$ arithmetic operations in $\mathbb{Q}$ to compute the geometric solution of a generalized Pham system where T is the number of arithmetic operations required by the straight-line program that computes $\phi_1 - \varphi_1, \dots, \phi_n - \varphi_n$.

Comparison with related work

Let $f_1, \dots, f_n \in \mathbb{Q}[X_1, \dots, X_n]$ be the input polynomials. Since the input system $f_1 = \cdots = f_n = 0$ has no points at infinity, deterministic algorithms for solving zero–dimensional homogeneous systems can be applied to the homogenizations of $f_1, \dots, f_n$. Such ideas were applied in [Laz83] to deterministically solve zero–dimensional systems $f_1 = \cdots = f_n = 0$ having at most a finite number of points at infinity with complexity of order $D^{O(1)}$ (see also [Giu89], [Giu91] for similar results and [Bar04] for the complexity of deterministic algorithms for systems defined by a regular sequence).

In connection with the complexity of probabilistic algorithms solving generalized Pham systems, we observe that our algorithm solves any generalized Pham system with quadratic complexity in the Bézout number $D = d_1 \cdots d_n$, extending thus the results of [MP00], [MT00] and [BMWW04, Section 5] to generalized Pham systems.

Another probabilistic algorithm solving generalized Pham systems with quadratic complexity in the Bézout number D is obtained by a clever application of the algorithm of [GLS01]. Indeed, since a generalized Pham system is not necessarily defined by a reduced regular sequence, this inhibits the straightsforward application of the algorithm of [GLS01]. Nevertheless, if $g_1, \dots, g_n \in \mathbb{Q}[X_1, \dots, X_n]$ are n generic linear combinations of $f_1, \dots, f_n$, then with high probability the polynomials $g_1, \ldots, g_{n-1}$ form a reduced regular sequence and $g_1, \ldots, g_n$ define the same variety as $f_1, \ldots, f_n$ (see, e.g., [KP96, Section 6]). In such a case, the application of the algorithm of [GLS01] to the polynomials $g_1, \ldots, g_n$ has quadratic complexity in the Bézout number $D = d_1 \cdots d_n$, rather than in $\max\{d_1, \ldots, d_n\}^n$, as a simple minded analysis might suggest.

We observe that any generalized Pham system can be (partially) solved applying the *non–universal* symbolic homotopy algorithm of [PS04]. This algorithm has a cost which is roughly of order $D_*^{2.38}$, where D_* denotes the degree of certain irreducible component of the curve introduced by the linear homotopy considered by the authors. As a consequence, the resulting algorithm will improve over our estimates for certain particular systems for which the irreducible component of the underlying curve under consideration has "low" degree. Nevertheless, for a generic generalized Pham system such a curve is irreducible of degree D, which implies that the cost of the algorithm of [PS04] is roughly of order $O(D^{2.38})$.

When considering the particular families of generalized Pham systems defined below in Section 3.1.2 one is often interested only in the real positive solutions ([Can84, §20.3], [Pao92a, §1.1]). It has been shown that the set of stationary solutions of the heat equation with monomial reaction terms and boundary conditions has only one positive solution in the cases of "small" or "large" absorption ([CFQ91a]). Furthermore, in [DM09], [Dra10] it has been shown that there are no spurious positive stationary solutions of the corresponding semidiscretization, namely positive solutions not corresponding to anyone of the heat equation. This implies that there is only one positive solution of the systems arising from the semidiscretization in the cases mentioned above, provided that the number of nodes involved in the semidiscretization is large enough. Hence, the specially-crafted algorithms of [DM09, Dra10] compute ε–approximations of these solutions in time that is linear in n, and thus are more efficient than ours, which compute all the complex solutions and perform $O(d^{2n})$ arithmetic operations. In connection with this matter, it may also be worthwhile to mention that a generalization of this result has been obtained in [Dra13a], [Dra13b].

3.1. A catalogue of generalized Pham systems

In this section we discuss some sources of interest for the notion of a generalized Pham system. For this purpose we introduce three particular classes of zero–dimensional generalized Pham systems: Pham systems, systems arising in the analysis of the stationary solutions of certain parabolic differential equations and generalized Reimer systems.

3.1.1. Pham Systems

Fix $n, d_1, \ldots, d_n \in \mathbb{N}$. Let $g_1, \ldots, g_n \in \mathbb{Q}[X_1, \ldots, X_n]$ be polynomials with $\deg(g_i) < d_i$ for $1 \leq i \leq n$, and consider the polynomials

$$f_1 := X_1^{d_1} - g_1, \ldots, f_n := X_n^{d_n} - g_n.$$

The map $f := (f_1, \ldots, f_n) : \mathbb{C}^n \to \mathbb{C}^n$ is called a *Pham map* in [VA85, Chapter 1, Section 5.2] and is considered in connection with the study of the local multiplicity of a holomorphic map. Consistently, the system $f_1 = 0, \ldots, f_n = 0$ is called a *Pham system* (see, e.g., [GLGV98], [MP00], [BMWW04]).

3.1.2. Systems Coming from a Semidiscretization of certain Parabolic Differential Equations

Let Z be an indeterminate and let $f, g, h \in \mathbb{Q}[Z]$ be given polynomials. Several problems concerning unidimensional nonlinear heat transfer are described by a partial differential equation of the form $u_t = f(u)_{xx} + g(u)$ in a bounded domain, say $(0,1) \times [0, t_0)$, with (Newmann) boundary conditions $f(u)_x(1,t) = h\big(u(1,t)\big)$ and $f(u)_x(0,t) = 0$ in $[0, t_0)$ and $u(x,0) \geq 0$ in $[0,1]$ (see, e.g., [Pao92b]). In particular, the asymptotic behavior of the solutions of such boundary value problems has been intensively analyzed (cf. [SGKM95]). This behavior is mainly described by the corresponding *stationary solutions*, namely, the positive solutions of the ordinary differential equation $0 = f(u)'' + g(u)$ with boundary conditions $f(u)'(1) = h\big(u(1)\big)$ and $f(u)'(0) = 0$.

The usual numeric treatment of this latter problem consists in finding a numerical approximation provided by a standard second order finite difference scheme (see, e.g., [BR01], [FGR02]). The solutions of such numerical approximation are represented by the system defined by the following polynomials:

$$\begin{aligned} f_1 &:= 2(n-1)^2\big(f(X_2)-f(X_1)\big)-g(X_1),\\ f_i &:= (n-1)^2\big(f(X_{i+1})-2f(X_i)+f(X_{i-1})\big)-g(X_i), \quad (2\le i\le n-1)\\ f_n &:= 2(n-1)^2\big(f(X_{n-1})-f(X_n)\big)+2(n-1)h(X_n)-g(X_n). \end{aligned} \tag{3.1}$$

Two important cases of study are the porous medium equation with nonlinear source terms and boundary condition (see, e.g., [Hen81], [Pao92b]), which leads to instances of (3.1) with $f = h := Z^d$ and $g := Z$ (see, e.g., [FGR02]), and the heat equation with polynomial reaction terms and boundary conditions, which leads to instances of (3.1) with $f := Z$, $h := Z^{d_1}$ and $g := Z^{d_2}$ (see, e.g., [BR01], [MD04], [MD05]).

3.1.3. Reimer Systems

We now consider another family of examples called *(generalized) Reimer systems* (see [BM96], [BMWW04]). A generalized Reimer system is defined by polynomials $f_1, \dots, f_n \in \mathbb{Q}[X_1, \dots, X_n]$ of the following form:

$$f_i := \alpha_i + \sum_{j=1}^{n} a_{i,j} X_j^{i+1}, \tag{3.2}$$

where $a_{i,j}, \alpha_i$ $(1 \le i, j \le n)$ are suitable elements of $\mathbb{Q}$ with $\alpha_i \ne 0$ for $1 \le i \le n$. More precisely, in [BMWW04, Lemma 17] it is shown that there exists a nonempty Zariski open set $\mathcal{U} \subset \mathbb{C}^{n^2}$ with the following property: for every $a := (a_{i,j})_{1\le i,j\le n} \in \mathcal{U}$, the corresponding polynomials $f_1, \dots, f_n$ in (3.2) define a zero–dimensional system with $(n+1)!$ distinct complex solutions. A system $f_1 = \cdots = f_n = 0$ is called a generalized Reimer system if $f_1, \dots, f_n$ are defined as in (3.2) with $\alpha_i \ne 0$ for $1 \le i \le n$ and $a := (a_{i,j})_{1\le i,j\le n} \in \mathcal{U}$.

3.1.4. Generalized Pham Systems

Let $f_1, \dots, f_n \in \mathbb{Q}[X_1, \dots, X_n]$ be given polynomials of (total) positive degrees $d_1, \dots, d_n$ respectively. Following [PS04] we say that $f_1, \dots, f_n$ define a *generalized Pham system* if the projective variety $\{\bar{x} \in \mathbb{P}^{n-1}(\mathbb{C})$:

$\phi_1(\bar{x}) = 0, \ldots, \phi_n(\bar{x}) = 0\}$ is empty, where $\phi_i \in \mathbb{Q}[X_1, \ldots, X_n]$ denotes the homogeneous component of f_i of degree d_i for $1 \leq i \leq n$.

It is easy to see that the systems introduced in Sections 3.1.1, 3.1.2 and 3.1.3 are generalized Pham systems. We remark that the solution set of a generalized Pham system is a zero–dimensional affine variety of $\mathbb{C}^n$ (see, e.g., [PS04, Proposition 18]).

3.2. The Solution of a Generalized Pham System

Let $f_1, \ldots, f_n$ be polynomials in $\mathbb{Q}[X]$ which can be computed by a division–free straight–line program of length T, and let $V := V(f_1, \ldots, f_n)$ denote the affine subvariety of $\mathbb{A}^n$ defined by $f_1, \ldots, f_n$. For $1 \leq i \leq n$, set $d_i := \deg f_i$ and write $f_i = \phi_i + \varphi_i$, where $\phi_i \in \mathbb{Q}[X]$ is the (nonzero) homogeneous component of f_i of degree d_i. Let $\delta := \deg V$ denote the degree of V. Finally, set $D := d_1 \cdots d_n$ and note that $\delta \leq D$ by the Bézout inequality.

Assume that $f_1, \ldots, f_n$ define a generalized Pham system, that is, the projective variety $\{\phi_1(\bar{x}) = 0, , \ldots, \phi_n(\bar{x}) = 0\} \subset \mathbb{P}^{n-1}$ is the empty set. The following result will be important in the sequel.

Lemma 3.1 ([PS04, Proposition 18]). *The set of solutions of an n–variate generalized Pham system is a zero–dimensional affine subvariety of $\mathbb{A}^n$.*

Let $f_1^h, \ldots, f_n^h$ denote the homogenizations of $f_1, \ldots, f_n$ with homogenizing variable X_0. Observe that the polynomials $f_1^h, \ldots, f_n^h$ are of the form

$$f_1^h = \phi_1(X) + X_0\widetilde{\varphi}_1(X_0, X), \ldots, f_n^h = \phi_n(X) + X_0\widetilde{\varphi}_n(X_0, X),$$

for some polynomials $\widetilde{\varphi}_1, \ldots, \widetilde{\varphi}_n \in \mathbb{Q}[X_0, X]$. From this representation we deduce that the projective variety $V^h := \{f_1^h(\bar{x}) = 0, \ldots, f_n^h(\bar{x}) = 0\} \subset \mathbb{P}^n$ is contained in the Zariski–open set $\{\overline{x}_0 \neq 0\}$, or equivalently the ideal generated by X_0 is not contained in the ideal generated by $f_1^h, \ldots, f_n^h$. By the Bézout theorem in the form of [EH99, Theorem III.71] it follows that the projective variety V^h has precisely D points in $\mathbb{P}^n$, counting multiplicities. Since V^h has no points at infinity, from [CGH91, Proposition 1.11] we conclude that V has D points, counting multiplicities.

3.2.1. The architecture of our solution method

We introduce a sequence of deformations which play the role of certain piecewise–linear homotopies of numerical continuation methods acting coordinate by coordinate (cf. [Sai83], [Duv90]). More precisely, for $1 \leq r \leq n+1$ we introduce a deformation $\pi_r : \mathcal{V}_r \to \mathbb{A}^1$ such that the following conditions are satisfied:

(i) $\mathcal{V}_r \subset \mathbb{A}^{n+1}$ is equidimensional of dimension 1 for $1 \leq r \leq n+1$,

(ii) π_r is dominant and generically unramified for $1 \leq r \leq n+1$,

(iii) $\deg \pi_r = D = \#\pi_r^{-1}(0)$ and $\deg \mathcal{V}_r \leq 2D$ holds for $1 \leq r \leq n+1$,

(iv) $\pi_r^{-1}(1) = \pi_{r+1}^{-1}(0)$ for $1 \leq r < n+1$,

(v) $\pi_1^{-1}(0)$ is "easy to solve" and $\pi_{n+1}^{-1}(1) = \{1\} \times V$ holds.

In order to compute a geometric solution of the fibre $\pi_{n+1}^{-1}(1) = \{1\} \times V$, and thus of V, we shall apply repeatedly the "projection algorithm" of Theorem 2.2. This algorithm takes as input a geometric solution of the unramified fibre $\pi_{r+1}^{-1}(0) = \pi_r^{-1}(1)$ of the morphism π_{r+1} and outputs a geometric solution of $\mathcal{V}_{r+1}$ for any $1 \leq r \leq n$. Making the substitution $T = 1$ in the polynomials that form the computed geometric solution of $\mathcal{V}_{r+1}$ we obtain polynomials that form a geometric solution of $\pi_{r+1}^{-1}(1) = \pi_{r+2}^{-1}(0)$. Since the fibre $\pi_1^{-1}(0)$ is easy to solve, after n applications of such a projection algorithm we obtain a geometric solution $\pi_{n+1}^{-1}(1)$.

Assume that we are given deformations $\pi_r : \mathcal{V}_r \to \mathbb{A}^1$ $(1 \leq r \leq n+1)$ satisfying conditions (i)–(v) above. The following is a sketch of our algorithm for computing a geometric solution of the input system $f_1 = 0, \ldots, f_n = 0$.

Algorithm 3.2 (Sketch of the algorithm for solving $f_1 = 0, \ldots, f_n = 0$)**.**

1. *Find a geometric solution of the "easy–to–solve" fibre* $\pi_1^{-1}(0)$.

2. *For* $r = 1$ *to* n *do:*

   a*) Apply a "projection algorithm" in order to compute a geometric solution of* $\mathcal{V}_r$ *from the geometric solution of* $\pi_r^{-1}(0)$ *computed in the previous step.*

b*) Make the substitution $T = 1$ in the polynomials that form the geometric solution of $\mathcal{V}_r$ computed in the previous step. These polynomials form a geometric solution of $\pi_{r+1}^{-1}(0) = \pi_r^{-1}(1)$ for $1 \leq r \leq n-1$ and may include multiplicities for $r = n$.*

3. *Clean multiplicities from the polynomials computed in the previous step for $r = n$ to obtain a geometric solution of $\mathcal{V}_{n+1} = \{1\} \times V$, and thus of V.*

3.2.2. Designing suitable deformations

In the description of our deformations $\pi_r : \mathcal{V}_r \to \mathbb{A}^1$ we shall make use of certain $\mathbb{Q}$–linearly independent linear forms $Y_1, \dots, Y_n \in \mathbb{Q}[X]$ and nonzero rational numbers $b_1, \dots, b_n \in \mathbb{Q} \setminus \{0\}$ to be fixed during the setup stage of our algorithm (Section 3.2.3 below).

Fix r with $1 \leq r \leq n$ and consider the following polynomials of $\mathbb{Q}[T, X]$:

$$\begin{cases} F_j^{(r)}(T,X) := \phi_j(X) + b_j \quad (1 \leq j \leq r-1), \\ F_r^{(r)}(T,X) := Y_r^{d_r} + T(\phi_r(X) - Y_r^{d_r}) + b_r, \\ F_j^{(r)}(T,X) := Y_j^{d_j} + b_j \quad (r+1 \leq j \leq n). \end{cases} \tag{3.3}$$

In particular, for $r = 1$ we have

$$\begin{array}{lll} F_1^{(1)}(T,X) := & Y_1^{d_1} + T(\phi_1(X) - Y_1^{d_1}) + b_1 & , \\ F_j^{(1)}(T,X) := & Y_j^{d_j} + b_j & \text{for } 2 \leq j \leq n \end{array}$$

and for $r = n$ we have

$$\begin{array}{lll} F_j^{(n)}(T,X) := & \phi_j(X) + b_j & \text{for } 1 \leq j \leq n-1, \\ F_n^{(n)}(T,X) := & Y_n^{d_n} + T(\phi_n(X) - Y_n^{d_n}) + b_n. & \end{array}$$

Finally, consider the following polynomials of $\mathbb{Q}[T, X]$:

$$F_i^{(n+1)}(T,X) := \phi_i(X) + T(\varphi_i(X) - b_i) + b_i \quad \text{for } 1 \leq i \leq n. \tag{3.4}$$

For any $1 \leq r \leq n+1$, let $\mathcal{I}_r := (F_1^{(r)}, \dots, F_n^{(r)}) \subset \mathbb{Q}[T, X]$, let $J_r := \det(\partial F_i^{(r)} / \partial X_j)_{1 \leq i,j \leq n}$ be Jacobian determinant of $F_1^{(r)}, \dots, F_n^{(r)}$ with respect to the variables X and let $\mathcal{V}_r := V(\mathcal{I}_r : J_r^{\infty}) \subset \mathbb{A}^{n+1}$ be the variety defined by the saturation $(\mathcal{I}_r : J_r^\infty)$. The rth deformation $\pi_r : \mathcal{V}_r \to \mathbb{A}^1$ is determined by the projection $\pi_r(t,x) := t$ and the affine variety $\mathcal{V}_r \subset \mathbb{A}^{n+1}$.

Having defined the deformations $\pi_r : \mathcal{V}_r \to \mathbb{A}^1$ $(1 \le r \le n+1)$, we discuss the validity of conditions (i)–(v) of the previous section. The fulfillment of these conditions relies on a suitable choice of the coefficients of the linear forms $Y_1, \dots, Y_n$ and the rational numbers $b_1, \dots, b_n$. In the next section we prove that for certain random choice of these coefficients, the following assertions hold with high probability:

($\mathcal{A}$) The polynomials $F_i^{(r)}(t,X)$ $(1 \le i \le n)$ define a generalized Pham system for a generic choice $t \in \mathbb{A}^1$ and every $1 \le r \le n+1$ (see Corollary 3.8 bellow).

($\mathcal{B}$) The affine variety $V\big(F_1^{(r)}(0,X), \dots, F_n^{(r)}(0,X)\big)$ consists of D nonsingular points for $1 \le r \le n+1$ (see Proposition 3.9 below).

Assuming that assertions ($\mathcal{A}$)–($\mathcal{B}$) hold, from ($\mathcal{A}$) and Lemma 3.1 we conclude that $\{F_1^{(r)}(t,X) = 0, \dots, F_n^{(r)}(t,X) = 0\}$ is a zero–dimensional subvariety of $\mathbb{A}^n$ for a generic choice $t \in \mathbb{A}^1$. This shows that the generic fibre of the projection mapping $\pi_r : V(\mathcal{I}^{(r)}) \to \mathbb{A}^1$ is nonempty for $1 \le r \le n+1$ (and consists of at most D points by the Bézout inequality (2.1)). Furthermore, ($\mathcal{B}$) asserts that the fibre $\pi_r^{-1}(0)$ consists of D nonsingular points for $1 \le r \le n+1$. Summarizing, under the assumption of assertions ($\mathcal{A}$)–($\mathcal{B}$) it follows that the deformations $\pi_r : \mathcal{V}_r \to \mathbb{A}^1$ satisfy the following conditions for $1 \le r \le n+1$:

($\mathcal{C}$) $0 < \#\pi_r^{-1}(t) \le D$ holds for a generic value $t \in \mathbb{A}^1$,

($\mathcal{D}$) $\#\pi_r^{-1}(0) = D$ and $J_r(0,x) \ne 0$ holds for every $(0,x) \in \pi_r^{-1}(0)$.

Proposition 3.3. *Let be given polynomials $F_1, \dots, F_n \in \mathbb{Q}[T,X]$, a positive integer D and $t_0 \in \mathbb{Q}$. Let $\mathcal{I} \subset \mathbb{Q}[T,X]$ be the ideal generated by $F_1, \dots, F_n$ and set $\mathcal{W} := V(\mathcal{I}) = V(F_1, \dots, F_n)$. Let $J := \det(\partial F_i/\partial X_j)_{1 \le i,j \le n}$ be the Jacobian determinant of $F_1, \dots, F_n$ with respect to the variables X and let $\mathcal{V} := V(\mathcal{I} : J^\infty) \subset \mathbb{A}^{n+1}$ be the variety defined by the saturation $(\mathcal{I} : J^\infty)$.*

Let $\pi : \mathcal{W} \to \mathbb{A}^1$ denote the projection $\pi(t,x) := t$. Assume that

- *$0 < \#\pi^{-1}(t) \le D$ holds for a generic value $t \in \mathbb{A}^1$,*

- *$\#\pi^{-1}(t_0) = D$ and $J(t_0, x) \neq 0$ holds for every $(t_0, x) \in \pi^{-1}(t_0)$.*

Then the following assertions hold:

- *$\mathcal{V}$ is an equidimensional variety of dimension 1.*
- *$\mathcal{V}$ is the union of all the irreducible components of $\mathcal{W}$ having a nonempty intersection with $\pi^{-1}(t_0)$.*
- *$\mathcal{V}$ is the union of all the irreducible components of $\mathcal{W}$ projecting dominantly on $\mathbb{A}^1$.*
- *$\pi : \mathcal{V} \to \mathbb{A}^1$ is a dominant map of degree D.*

Proof. First we observe that $\dim(C) \geq 1$ holds for each irreducible component C of $\mathcal{W}$, since $\mathcal{W}$ is defined by n polynomials in an $(n+1)$–dimensional space. By definition, $\mathcal{V}$ consists of all irreducible components of $\mathcal{W}$ on which the Jacobian determinant J does not vanish identically.

Let C be an irreducible component of $\mathcal{W}$ for which $\pi^{-1}(t_0) \cap C \neq \emptyset$ holds. Consider the restriction $\pi|_C : C \to \mathbb{A}^1$ of π. Then we have that $\pi|_C^{-1}(t_0)$ is a nonempty variety of dimension zero, which implies that the generic fibre of $\pi|_C$ is either zero-dimensional or empty. Since $\dim(C) \geq 1$, the theorem on the dimension of fibres implies that $\dim(C) = 1$ holds and that $\pi|_C : C \to \mathbb{A}^1$ is a dominant map with generically finite fibres. Finally, [Sha94, §II.6, Theorem 4] shows the inclusion $C \subset \mathcal{V}$ and, in particular, that $\mathcal{V}$ is nonempty.

Conversely, we have that $\pi^{-1}(t_0) \cap C \neq \emptyset$ holds for any irreducible component C of $\mathcal{V}$. Indeed, assume on the contrary the existence of a component C_0 not satisfying this condition. Let $t_1 \in \mathbb{A}^1$ be a point having a finite fibre $\pi^{-1}(t_1)$ such that $\pi|_{C_0}^{-1}(t_1)$ and $\pi|_C^{-1}(t_1)$ have maximal cardinality for every C with $C \cap \pi^{-1}(t_0) \neq \emptyset$. This implies that $\#\pi^{-1}(t_1) > \#\pi^{-1}(t_0) = D$, leading to a contradiction.

We conclude that $\mathcal{V}$ is the equidimensional variety of dimension 1 which consists of all the irreducible components C of $\mathcal{W}$ with $\pi^{-1}(t_0) \cap C \neq \emptyset$. Furthermore, this shows that the restriction $\pi|_{\mathcal{V}} : \mathcal{V} \to \mathbb{A}^1$ is a dominant map of degree D.

Finally we show that $\mathcal{V}$ consists of all irreducible components of $\mathcal{W}$ projecting dominantly on $\mathbb{A}^1$. Let C be one such irreducible component of $\mathcal{W}$.

Then by [Sha94, §II.6, Theorem 4] it follows that there exists an unramified fibre of $\pi|_C$. On such a fibre the Jacobian J does not vanish, which in turn proves that J does not vanish identically on C. Therefore, $C \subset \mathcal{V}$ holds. On the other hand, if C is an irreducible component of $\mathcal{W}$ for which the projection $\pi|_C : C \to \mathbb{A}^1$ is not dominant, then C is the set of common zeros of the polynomials $F_1, \dots, F_n, T - t_C$ for some value t_C. Since $\dim(C) \geq 1$, we have that the Jacobian matrix $\partial(F_1, \dots, F_n, T - t_C)/\partial(X_1, \dots, X_n, T)$ is singular at every point (x, t_C) of C. Hence, its determinant, which equals J, vanishes over C. □

We claim that the validity of $(\mathcal{A})$–$(\mathcal{B})$ implies that conditions (i)–(v) of Section 3.2.1 hold. Indeed, combining $(\mathcal{A})$–$(\mathcal{B})$ with the first conclusion of Proposition 3.3 immediately implies that $\mathcal{V}_r$ is an equidimensional variety of dimension 1 for $1 \leq r \leq n+1$, that is, condition (i) holds.

By $(\mathcal{B})$ and the third and fourth conclusions of Proposition 3.3 we have that the morphism $\pi_r : \mathcal{V}_r \to \mathbb{A}^1$ is dominant and generically unramified for $1 \leq r \leq n+1$, proving thus that condition (ii) holds.

In the proof of $(\mathcal{C})$–$(\mathcal{D})$ we have already shown that $(\mathcal{A})$–$(\mathcal{B})$ imply that the identity $\deg \pi_r = \pi_r^{-1}(0) = D$ holds for $1 \leq r \leq n+1$, which is the first part of condition (iii). Furthermore, by the Bézout inequality (2.1) we have:

$$\deg V(\mathcal{I}_r) \leq d_1 \cdots d_{r-1}(d_r + 1)d_{r+1} \cdots d_n \leq 2D$$

for $1 \leq r \leq n$ and

$$\deg V(\mathcal{I}_{n+1}) \leq D.$$

From these estimates and the definition of the varieties $\mathcal{V}_r$ we conclude that the following estimates, and thus the second part of condition (iii), hold:

$$\deg \mathcal{V}_r \leq d_1 d_2 \cdots d_{r-1}(d_r + 1)d_{r+1} \cdots d_n \leq 2D$$

for $1 \leq r \leq n$ and

$$\deg V_{n+1} \leq D.$$

From the second conclusion of Proposition 3.3 we deduce the following identities, which imply (iv):

$$\begin{aligned} &\#\big(V(\mathcal{I}_r) \cap \{T = 0\}\big) = \#\big(\mathcal{V}_r \cap \{T = 0\}\big) = D \quad (1 \leq r \leq n+1), \\ &\#\big(V(\mathcal{I}_r) \cap \{T = 1\}\big) = \#\big(\mathcal{V}_r \cap \{T = 1\}\big) \quad (1 \leq r \leq n). \end{aligned}$$

Concerning the second assertion of condition (v), we observe that the identity $V(\mathcal{I}_{n+1}) \cap \{T = 1\} = V_{n+1} \cap \{T = 1\}$ holds, because $\mathcal{I}_{n+1} = (\mathcal{I}_{n+1} : J_{n+1}^{\infty})$ holds since the finiteness of the projection $\pi_{n+1} : V(\mathcal{I}_{n+1}) \to \mathbb{A}^1$ implies that $V(\mathcal{I}_{n+1})$ contains no vertical component.

Finally, for the first assertion of (v) we observe that $V(\mathcal{I}_1) \cap \{T = 0\}$ is defined by a "diagonal" square system and therefore can be easily solved (see the algorithm underlying Lemma 3.11 below). This finishes the proof of our claim.

3.2.3. Preparation: random choices

This section is devoted to showing that we can choose the linear forms $Y_1, \dots, Y_n$ and the vector $b := (b_1, \dots, b_n) \in \mathbb{Q}^n$ such that conditions $(\mathcal{A})$–$(\mathcal{B})$ above are satisfied.

We prove the technical results that we shall use for establishing conditions on the coefficients of $Y_1, \dots, Y_n$ which assure that the polynomials in (3.3) and (3.4) define generalized Pham systems. In the sequel we shall use the following simple criterion, which is a well–known consequence of the Macaulay un-mixedness theorem (see, e.g., [Mat80, Exercise 16.3]).

Remark 3.4. *Let $Q_1, \dots, Q_n \in \mathbb{Q}[X] := \mathbb{Q}[X_1, \dots, X_n]$ be nonzero homogeneous polynomials defining the empty projective variety $\{Q_1(\bar{x}) = 0, \dots, Q_n(\bar{x}) = 0\}$ of $\mathbb{P}^{n-1}$. Then $Q_1, \dots, Q_n$ form a regular sequence in $\mathbb{Q}[X]$.*

As a first consequence of this remark we observe that, since $f_1, \dots, f_n$ determine a generalized Pham system, the polynomials $\phi_1, \dots, \phi_n$ define the empty projective variety of $\mathbb{P}^{n-1}$. Hence, applying Remark 3.4 we deduce the following result.

Corollary 3.5. *The polynomials $\phi_1, \dots, \phi_n$ form a regular sequence in $\mathbb{Q}[X]$.*

Next we provide a consistent condition which assures that the polynomials $\phi_1, \dots, \phi_r, Y_{r+1}^{d_{r+1}}, \dots, Y_n^{d_n}$ form a regular sequence in $\mathbb{Q}[X]$ for $1 \leq r \leq n$.

Proposition 3.6. *Fix a positive integer ρ and suppose that the coefficients of the linear forms $Y_1, \dots, Y_n$ are randomly chosen in the set $\{1, \dots, 2n\rho D\}$.*

Then with error probability at most $1/\rho$*, the polynomials* $\phi_1, \ldots, \phi_r, Y_{r+1}^{d_{r+1}}, \ldots, Y_n^{d_n}$ *form a regular sequence in* $\mathbb{Q}[X]$ *for* $0 \leq r \leq n$*.*

Proof. For $1 \leq r \leq n$, we deduce from Corollary 3.5 that the affine variety

$$W_{r,0} := \{x \in \mathbb{A}^n; \phi_1(x) = 0, \ldots, \phi_r(x) = 0\}$$

is equidimensional of dimension $n-r$ for $1 \leq r < n$. This in particular shows the condition of the statement of the proposition for $r = n$ is automatically satisfied.

Let $A_{i,j}$ $(1 \leq i, j \leq n)$ be new indeterminates over $\mathbb{Q}[X]$, and denote $A^{(r)} := (A_{r,1}, \ldots, A_{r,n})$ for $1 \leq r \leq n$ and $A := (A_{i,j})_{1 \leq i,j \leq n}$.

We construct the linear forms $Y_1, \ldots, Y_n$ iteratively so that at step r:

- the coefficients of the linear forms $Y_1, \ldots, Y_r$ are randomly chosen in the set $\{1, \ldots, 2n\rho D\}$, and
- for any pair (i, j) with $0 \leq i < j \leq r$, the variety
$$W_{i,j} := \{x \in \mathbb{A}^n; \phi_1(x) = 0, \ldots, \phi_i(x) = 0, Y_{i+1}(x) = 0, \ldots, Y_j(x) = 0\} \tag{3.5}$$
is equidimensional of dimension $n - j$ with error probability at most $\sum_{j=1}^{r}(1 + \sum_{i=1}^{j-1} d_1 \cdots d_i)/2n\rho D$.

Fix arbitrarily a nonzero linear form $Y_1 \in \mathbb{Q}[X]$ with coefficients in $\{1, \ldots, 2n\rho D\}$ and an index r with $1 < r \leq n$. If $r = 1$, then the conditions are satisfied, since for any nonzero linear form Y_1 the affine variety $W_{0,1}$ is equidimensional of dimension 1.

Assume $r > 1$ and that $Y_1, \ldots, Y_{r-1}$ have been chosen fulfilling the conditions above. We can now discuss the choice of the linear form Y_r. For any i with $0 \leq i \leq r-1$, let $\mathcal{S}_{i,r-1} \subset W_{i,r-1}$ be a finite set consisting of one arbitrary nonzero point in each irreducible component of $W_{i,r-1}$. By the Bézout inequality (2.1) we have $\#\mathcal{S}_{i,r-1} \leq \deg W_{i,r-1} \leq d_1 \ldots d_i$ for $i = 1, \ldots, r-1$ and $\#\mathcal{S}_{0,r-1} = \deg W_{0,r-1} = 1$. Let $Q_r \in \mathbb{Q}[A^{(r)}]$ be the nonzero polynomial defined in the following way:

$$Q_r(A^{(r)}) := \prod_{i=0}^{r-1} \prod_{\xi \in \mathcal{S}_{i,r-1}} \sum_{j=1}^{n} \xi_j \, A_{r,j}.$$

Let $a^{(r)}$ be an arbitrary point of $\mathbb{Q}^n$ not annihilating Q_r and define $Y_r := a^{(r)}X$. By construction, we have that $Y_r(\xi) \neq 0$ holds for every $\xi \in \mathcal{S}_{i,r-1}$ and every $0 \leq i \leq r-1$. This shows that the hyperplane $\{Y_r = 0\}$ cuts properly all the irreducible components of $W_{i,r-1}$ for $0 \leq i \leq r-1$. We conclude that the variety

$$W_{i,r} := \{x \in \mathbb{A}^n; \phi_1(x) = 0, \ldots, \phi_i(x) = 0, Y_{i+1}(x) = 0, \ldots, Y_r(x) = 0\} \tag{3.6}$$

is equidimensional of dimension $n-r$ and degree at most $d_1 \cdots d_i$ for $0 \leq i \leq r$. Combining (3.5), (3.6) we see that the varieties $W_{i,j}$ are equidimensional of dimension $n-j$ for $0 \leq i < j \leq r$, completing thus the rth step of our inductive argument.

Observe that $\deg Q_r \leq 1 + \sum_{i=1}^{r-1} d_1 \cdots d_i$ holds. Hence, applying Theorem 2.1 we conclude that for a random choice of the coefficient vector $a^{(r)}$ of Y_r in the set $\{1, \ldots, 2n\rho D\}^n$, the inequality $Q_r(a^{(r)}) \neq 0$, and thus (3.6), holds, with error probability at most $(1 + \sum_{i=0}^{r-1} d_1 \cdots d_i)/2n\rho D$.

After n steps as described, we obtain linear forms $Y_1, \ldots, Y_n$ such that, with error probability at most $\sum_{j=1}^{n}(1 + \sum_{i=1}^{j-1} d_1 \cdots d_i)/2n\rho D$, the variety $W_{i,j}$ is equidimensional of dimension $n-j$ for $i < j \leq n$ and $0 \leq i \leq n$. In particular, this implies that the polynomials $\phi_1, \ldots, \phi_r, Y_{r+1}, \ldots, Y_n$ form a regular sequence of $\mathbb{Q}[X]$ for $0 \leq r \leq n$. Therefore, by [Mat86, Theorem 16.1] we conclude that $\phi_1, \ldots, \phi_r, Y_{r+1}^{d_{r+1}}, \ldots, Y_n^{d_n}$ form a regular sequence in $\mathbb{Q}[X]$ for $0 \leq r \leq n$. Since

$$\begin{aligned} \frac{1}{2n\rho D} \sum_{j=1}^{n} \Big(1 + \sum_{i=1}^{j-1} d_1 \cdots d_i\Big) &= \frac{1}{2n\rho D} \Big(n + \sum_{j=1}^{n} (n-j) d_1 \cdots d_j\Big) \\ &= \frac{1}{2\rho D} \left(1 + \sum_{j=1}^{n} d_1 \cdots d_j\right) \leq \frac{1}{\rho}, \end{aligned}$$

we deduce the statement of the proposition. □

As a first consequence on the choice of the linear forms $Y_1, \ldots, Y_n$ we deduce that for a generic value $t \in \mathbb{A}^1$ the polynomials in (3.3) define a generalized Pham system. More precisely, we have the following result.

Corollary 3.7. *Let $Y_1, \ldots, Y_n \in \mathbb{Q}[X]$ be linear forms satisfying the statement of Proposition 3.6. Then, for $1 \leq r \leq n$, the polynomials*

$$\phi_1(X), \ldots, \phi_{r-1}(X), Y_{r+1}^{d_{r+1}}, \ldots, Y_n^{d_n}, Y_r^{d_r} + T(\phi_r(X) - Y_r^{d_r}) \tag{3.7}$$

form a regular sequence in $\mathbb{Q}[T, X]$. Furthermore, for a generic value $t \in \mathbb{A}^1$

$$\phi_1(X), \ldots, \phi_{r-1}(X), Y_{r+1}^{d_{r+1}}, \ldots, Y_n^{d_n}, Y_r^{d_r} + t(\phi_r(X) - Y_r^{d_r})$$

form a regular sequence in $\mathbb{C}[X]$.

Proof. Fix r with $1 \leq r \leq n$. From Proposition 3.6 it follows that the polynomials $\phi_1, \ldots, \phi_r, Y_{r+1}^{d_{r+1}}, \ldots, Y_n^{d_n}$ form a regular sequence in $\mathbb{Q}[X]$. Since these are homogeneous polynomials, from [Mat86, Corollary of Theorem 16.3] we see that $\phi_1, \ldots, \phi_{r-1}, Y_{r+1}^{d_{r+1}}, \ldots, Y_n^{d_n}$ form a regular sequence of $\mathbb{Q}[X]$. Therefore, in order to prove the lemma it suffices to show that $H_r(T, X) := Y_r^{d_r} + T(\phi_r - a_r Y_r^{d_r})$ is not a zero divisor modulo the ideal $\mathcal{I}_r^* := (\phi_1, \ldots, \phi_r, Y_{r+1}^{d_{r+1}}, \ldots, Y_n^{d_n}) \subset \mathbb{Q}[T, X]$.

Let $V(\mathcal{I}_r^c) := \cup_{j \in \mathcal{J}} C_j$ be the decomposition of the projective subvariety of $\mathbb{P}^{n-1}$ defined by the ideal $\mathcal{I}_r^c := (\phi_1, \ldots, \phi_r, Y_{r+1}^{d_{r+1}}, \ldots, Y_n^{d_n}) \subset \mathbb{Q}[X]$. Fix a point $\bar{p}^{(j)}$ in each irreducible component C_j of $V(\mathcal{I}_r^c)$. Since $Y_r^{d_r}$ and ϕ_r are not zero divisors modulo $\mathcal{I}_r^c$, it follows that $\alpha_j := Y_r(\bar{p}^{(j)})^{d_r}$ and $\beta_j := \phi_r(\bar{p}^{(j)})$ are nonzero complex numbers and hence $\alpha_j + T(\beta_j - \alpha_j)$ is a nonzero polynomial of $\mathbb{C}[T]$ for every $j \in \mathcal{J}$. Finally, let $t \in \mathbb{A}^1$ be any value with $\prod_{j \in \mathcal{J}}(\alpha_j + t(\beta_j - \alpha_j)) \neq 0$. Then $Y_r^{d_r} + t(\phi_r(X) - Y_r^{d_r})$ is not a zero divisor modulo $\mathcal{I}_r^c$. Furthermore, taking into account that $V(\mathcal{I}_r^*) = \cup_{j \in \mathcal{J}}(\mathbb{A}^1 \times C_j)$ is the decomposition of $V(\mathcal{I}_r^*) \subset \mathbb{P}^n$ into irreducible components, from the condition $\prod_{j \in \mathcal{J}}(\alpha_j + t(\beta_j - \alpha_j)) \neq 0$ we conclude that $Y_r^{d_r} + T(\phi_r - Y_r^{d_r})$ is not a zero divisor modulo $\mathcal{I}_r^*$. This finishes the proof. □

A consequence of Corollary 3.7 is that $\phi_1, \ldots, \phi_{r-1}, Y_r^{d_r} + t(\phi_r - Y_r^{d_r}), Y_{r+1}^{d_{r+1}}, \ldots, Y_n^{d_n}$ define the empty projective variety of $\mathbb{P}^{n-1}$ for all but a finite number of $t \in \mathbb{A}^1$. Likewise, from Corollary 3.5 we conclude that (3.4) is a generalized Pham system for every substitution $T = t$. Therefore, we have the following result.

Corollary 3.8. *Let $Y_1, \ldots, Y_n$ be linear forms satisfying the statement of Proposition 3.6. Then for all but a finite number of values $t \in \mathbb{A}^1$, making the substitution $T = t$ in (3.3) and (3.4) yields a generalized Pham system for $1 \leq r \leq n + 1$.*

This proves that our choice of $Y_1, \ldots, Y_n$ implies that condition $(\mathcal{A})$ in Section 3.2.2 holds.

Next we consider condition $(\mathcal{B})$. Fix r with $1 \leq r \leq n+1$ and let $b_1, \ldots, b_n$ be nonzero rational numbers to be fixed. Condition $(\mathcal{B})$ asserts that the affine subvariety $V(F_1^{(r)}(0,X), \ldots, F_n^{(r)}(0,X))$ of $\mathbb{A}^n$ consists of D distinct points, none of which is annihilated by the Jacobian determinant $J_r(0,X) := \det(\partial F_i^{(r)}(0,X)/\partial X_j)_{1 \leq i,j \leq n}$.

We observe that the smoothness of the variety $V(F_1^{(r)}(0,X), \ldots, F_n^{(r)}(0,X))$ for a generic value of b is a direct consequence of the Sard's theorem (see, e.g., [GP74, §1.7]). The next lemma is an effective version of this result in our context.

Proposition 3.9. *Let $B_1, \ldots, B_n$ be new indeterminates over $\mathbb{Q}[X]$ and set $B := (B_1, \ldots, B_n)$. Let $Y_1, \ldots, Y_n \in \mathbb{Q}[X]$ be linear forms satisfying the statement of Proposition 3.6. Then there exists a nonzero polynomial $P^{(2)} \in \mathbb{Q}[B]$ of degree at most $2nD^2$ such that for every $b \in \mathbb{Q}^n$ with $P^{(2)}(b) \neq 0$, the affine variety defined by the polynomials $F_1^{(r)}(0,X), \ldots, F_n^{(r)}(0,X)$ for this value of b consists of D nonsingular points for $1 \leq r \leq n+1$.*

Proof. First we observe that choosing arbitrarily $b_1 \neq 0, \ldots, b_n \neq 0$, the affine variety $\{Y_1(x)^{d_1} + b_1 = 0, \ldots, Y_n(x)^{d_n} + b_n = 0\}$ consists of D distinct points which are not annihilated by the Jacobian $J_1(0,X) := \det(\partial Y_i(x)^{d_i}/\partial X_k)_{1 \leq i,j \leq n}$, since no point of this variety has a zero coordinate. This proves the result for $r = 1$.

Now fix r with $2 \leq r \leq n$ and consider the following polynomials of $\mathbb{Q}[B,X]$:

$$\phi_1(X) + B_1, \ldots, \phi_{r-1}(X) + B_{r-1}, Y_r^{d_r} + B_r, \ldots, Y_n^{d_n} + B_n. \tag{3.8}$$

Denote by W_r the affine subvariety of $\mathbb{A}^{2n}$ defined by these polynomials. Since the polynomials in (3.8) define a generalized Pham system for any substitution $B = b$, from Lemma 3.1 it follows that the morphism

$$\theta_r : W_r \to \mathbb{A}^n, \quad \theta_r(b,x) := b$$

is surjective. Furthermore, we claim that θ_r is finite. Indeed, let $N_r \in \mathbb{N}$ with $N_r > d$ and $h_{i,j}^{(r)} \in \mathbb{Q}[X]$ $(1 \leq i,j \leq n)$ be polynomials of degree $N_r - d_r$ such that

$$X_i^{N_r} = \sum_{j=1}^{r-1} h_{i,j}^{(r)} \phi_j + \sum_{j=r}^{n} h_{i,j}^{(r)} Y_j^{d_j}.$$

Then for every $1 \leq i \leq n$ we have

$$\sum_{j=1}^{r-1} h_{i,j}^{(r)} (\phi_j + B_j) + \sum_{j=r}^{n} h_{i,j}^{(r)} (Y_j^{d_j} + B_j) = X_i^{N_r} + \sum_{j=1}^{n} h_{i,j}^{(r)} B_j,$$

with $\deg h_{i,j}^{(r)} B_j < N_r$ for $1 \leq i, j \leq n$. This proves that $\mathbb{Q}[B] \hookrightarrow \mathbb{Q}[W_r]$ is an integral ring extension. Taking into account that W_r is irreducible, from the previous assertions and [Sha94, II.6.3, Theorem 4] we conclude that θ_r is generically unramified.

Let $\eta \in \mathbb{C}[X]$ be a linear form that induces a primitive element of the ring extension $\mathbb{C}[B] \hookrightarrow \mathbb{C}[W_r]$. Consider its minimal polynomial $M_\eta^{(r)} \in \mathbb{Q}[B, Y]$, and let $\Delta_r \in \mathbb{C}[B]$ denote its discriminant with respect to the variable Y. For every $b \in \mathbb{Q}^n$ such that $\Delta_r(b) \neq 0$ it follows that the $M_\eta(b, Y)$ is square–free, and therefore the morphism θ_r is unramified at $B = b$.

Furthermore, for every $b \in \mathbb{Q}^n$ with $\Delta_r(b) \neq 0$, the corresponding polynomials $\phi_1(X)+b_1, \ldots, \phi_{r-1}(X)+b_{r-1}, Y_r^{d_r}+b_r, \ldots, Y_n^{d_n}+b_n$ define a generalized Pham system and generate a radical ideal in $\mathbb{Q}[X]$. Let $f_{r,1}^h, \ldots, f_{r,n}^h$ denote the homogenizations of $\phi_1(X) + b_1, \ldots, \phi_{r-1}(X) + b_{r-1}, Y_r^{d_r} + b_r, \ldots, Y_n^{d_n} + b_n$ with homogenizing variable X_0. Then $f_{r,1}^h, \ldots, f_{r,n}^h$ is a radical zero–dimensional ideal. We conclude that $f_{r,1}^h, \ldots, f_{r,n}^h$ form a regular sequence of $\mathbb{Q}[X]$. Applying the Bézout theorem in the form of [EH99, Theorem III.71] we see that the projective variety defined by $f_{r,1}^h, \ldots, f_{n,r}^h$ has precisely $\deg V^h = D$ distinct points in $\mathbb{P}^n$. Finally, since there are no points at infinity, from [CGH91, Proposition 1.11] we conclude that $\theta_r^{-1}(b)$ consists of exactly D distinct points.

A similar argument shows that there exists a polynomial $\Delta_{n+1} \in \mathbb{Q}[B]$ such that, for every $b \in \mathbb{Q}^n$ with $\Delta_{n+1}(b) \neq 0$, the polynomials $F_1^{(n+1)}(0, X)$, $\ldots, F_n^{(n+1)}(0, X)$ corresponding to this value of b have D nonsingular common zeros.

Let $P^{(2)} := (B_1 \cdots B_n) \cdot \Delta_2 \cdots \Delta_{n+1}$. From the Bézout inequality (2.1) we deduce that $\deg W_r \leq D$ holds, which in turns implies that the minimal polynomial of η has degree bounded by D. It follows that the degree of its discriminant Δ_r is bounded by $2D^2$ for $2 \leq r \leq n+1$ and hence $\deg P^{(2)} \leq n + 2(n-1)D^2 \leq 2nD^2$ holds. In conclusion, the polynomial $P^{(2)}$ satisfies all the requirement of the proposition. □

Fix a positive integer ρ. From Theorem 2.1 it follows that for a random choice of $b_1, \ldots, b_n$ in the set $\{1, \ldots, 2n\rho D^2\}$, the inequality $P^{(2)}(b_1, \ldots, b_n) \neq 0$ holds with error probability at most $1/\rho$. Then we have the following result.

Corollary 3.10. *If $b_1, \ldots, b_n$ are randomly chosen in the set $\{1, \ldots, 2n\rho D^2\}$, then the variety defined by $F_1^{(r)}(0, X), \ldots, F_n^{(r)}(0, X)$ for such values $b_1, \ldots, b_n$ consists of D nonsingular points for $1 \leq r \leq n+1$ with error probability at most $1/\rho$.*

3.2.4. The main algorithm

By means of Propositions 3.6 and 3.9 we obtain deformations $\pi_r : \mathcal{V}_r \to \mathbb{A}^1$ satisfying conditions (i)–(v) of Section 3.2.1. In this section we present a more detailed outline of Algorithm 3.2 and estimate its complexity and error probability.

Algorithmic tools

In order to present a more detailed outline of Algorithm 3.2, we need to make explicit the procedures that arise during the execution of this algorithm:

- the procedure for computing a geometric solution of a zero–dimensional diagonal square system used in the first step,
- the "projection algorithm" used in the second step,
- the procedure used to clean multiplicities used in the third step.

For the last two procedures, we shall use the algorithms underlying Theorem 2.2 and Lemma 2.3. A procedure for solving a given zero–dimensional diagonal square system follows.

Lemma 3.11. *Let be given $\mathbb{Q}$–linearly independent linear forms $Y_1, \ldots, Y_n \in \mathbb{Q}[X]$ and nonzero rational numbers $b_1, \ldots, b_n$. Set $g_i(X) := Y_i(X)^{d_i} + b_i$ $(1 \leq i \leq n)$ and let $V_0 \subset \mathbb{A}^n$ be the affine variety defined by $g_1, \ldots, g_n$.*

Then, given a generic linear form $u \in \mathbb{Q}[X]$ we can compute a geometric solution of V_0 with $O(n\mathsf{M}(D^2))$ arithmetic operations in $\mathbb{Q}$.

Proof. Suppose that we are given a linear form $u := \lambda_1 X_1 + \cdots + \lambda_n X_n \in \mathbb{Q}[X]$ that induces a primitive element of the $\mathbb{Q}$–algebra extension $\mathbb{Q} \to \mathbb{Q}[V_0]$. We can compute the minimal polynomial of u as follows: let Y, Z be new variables and set

$$\begin{aligned} m_1(Y) &:= \lambda_1^{-d_1} Y^{d_1} - b_1, \\ m_r(Y) &:= \mathit{Res}_Z\big(\lambda_r^{-d_r}(Y - Z)^{d_r} - b_r, m_{r-1}(Z)\big) \ (2 \leq r \leq n). \end{aligned} \tag{3.9}$$

We claim that the polynomial m_n equals (up to scaling by a nonzero element of $\mathbb{Q}$) the minimal polynomial $m_u \in \mathbb{Q}[Y]$ of u in $\mathbb{Q} \to \mathbb{Q}[V_0]$. Indeed, for every $2 \leq r \leq n$, the polynomial $m_r(Y)$ is a linear combination of $\lambda_r^{-d_r}(Y - Z)^{d_r} - b_r$ and $m_{r-1}(Z)$ over $\mathbb{Q}[Y, Z]$ by properties of the resultant. Let $u^{(r)} := \lambda_1 X_1 + \cdots + \lambda_r X_r$ for $1 \leq r \leq n$. Then, the identity

$$\lambda_r^{-d_r}(u^{(r)} - u^{(r-1)})^{d_r} - b_r = 0$$

holds in $\mathbb{Q}[V_0]$. Thus, assuming inductively that $m_{r-1}(u^{(r-1)}) = 0$ holds in $\mathbb{Q}[V_0]$, it follows that $m_r(u^{(r)}) = 0$ holds in $\mathbb{Q}[V_0]$ as well. Since $m_1(u^{(1)}) = X_1^{d_1} - b_1 = 0$ in $\mathbb{Q}[V_0]$ it holds that $m_n(u^{(n)}) = 0$ in $\mathbb{Q}[V_0]$. Taking into account the estimate $\deg m_n \leq D$ and the fact that m_u is a nonzero polynomial of degree $D = \#(V_0)$, we conclude that our claim holds.

In order to compute the polynomial m_u, we compute the resultants in (3.9). Since the resultant $\mathit{Res}_Z\big(\lambda_r^{-d_r}(Y - Z)^{d_r} - b_r, m_{i-1}(Z)\big)$ is a polynomial of $\mathbb{Q}[Y]$ of degree $d_1 \cdots d_r$, by univariate interpolation in the variable Y we reduce its computation to the computation of $d_1 \cdots d_r + 1$ resultants of univariate polynomials in $\mathbb{Q}[Z]$. This interpolation step requires $O\big(\mathsf{M}(d_1^2 \cdots d_r^2)\big)$ arithmetic operations in $\mathbb{Q}$ and does not require any division by a nonconstant polynomial in the coefficients $\lambda_1, \ldots, \lambda_n$ (see, e.g., [BLS03], [BS05]). Each univariate resultant can be computed with $\mathsf{M}(d_1 \cdots d_r)$ arithmetic operations in $\mathbb{Q}$ (see Section 2.3.3). Altogether, we obtain an algorithm for computing m_u which performs $O\big(\mathsf{M}(D^2)\big)$ arithmetic operations in $\mathbb{Q}$.

Finally, by the genericity of the linear form u we see that we can extend this algorithm to an algorithm computing a geometric solution of V_0 as explained in Section 2.4.2. From Lemma 2.4 we deduce the statement of the lemma. □

We remark that the genericity condition underlying the choice of the linear form u shall be discussed below.

Outline of the main algorithm and complexity and error probability estimate

Now we can give a more detailed outline of the algorithm computing a geometric solution of the input variety V.

Algorithm 3.12 (Algorithm for solving $f_1 = 0, \ldots, f_n = 0$)**.**

1. *Choose linear forms* $Y_1, \ldots, Y_n \in \mathbb{Q}[X]$ *and* $b_1, \ldots, b_n \in \mathbb{Q} \setminus \{0\}$ *according to Propositions 3.6 and 3.9. (These choices determine the deformations* $\pi_1, \ldots, \pi_{n+1}$*.)*

2. *Choose randomly a linear form* $u \in \mathbb{Q}[X]$ *which induces a primitive element of* V *and* $\pi_r^{-1}(0)$ *for* $1 \leq r \leq n+1$ *and such that we can apply Lemma 3.11.*

3. *Since* $\pi_1^{-1}(0) = \{Y_i(x)^{d_i} + b_i = 0;\ 1 \leq i \leq n\}$ *holds, then the fibre* $\pi_1^{-1}(0)$ *is defined by a diagonal system. Apply the algorithm underlying Lemma 3.11 in order to compute a geometric solution of* $\pi_1^{-1}(0)$ *with* u *as primitive element.*

4. *For* $r = 1$ *to* $n+1$ *do:*

   a) *Use the "projection algorithm" underlying Lemma 2.2 in order to compute a geometric solution of* V_r *with* u *as primitive element, from the geometric solution of* $\pi_r^{-1}(0)$ *computed in the previous step.*

   b) *The equalities* $\pi_r^{-1}(1) = \pi_{r+1}^{-1}(0)$ $(1 \leq r \leq n)$ *and* $\pi_{n+1}^{-1}(1) = \{1\} \times V$ *hold. Make the substitution* $T = 1$ *in the polynomials that form the geometric solution of* V_r *computed in the previous step. The univariate polynomials obtained form a geometric solution* *of $\pi_r^{-1}(1)$ for $1 \leq r \leq n$ and a complete description (eventually including multiplicities) of $\pi_{n+1}^{-1}(1) = \{1\} \times V$ for $r = n+1$.*

5. *Apply the algorithm underlying Lemma 2.3 to the polynomials that form a complete description of $\pi_{n+1}^{-1}(1) = \{1\} \times V$ computed in the previous step. The output is a geometric solution of V.*

In order to estimate the cost of this algorithm we need to estimate the cost of computing the geometric solution of the variety $\mathcal{V}_r$ of the step 4(a) for each r with $2 \leq r \leq n+1$. According to Lemma 2.2 such a cost depends on the height E_r of the projection $\pi_r : \mathcal{V}_r \to \mathbb{A}^1$, namely, the degree $\deg_T M_u^{(r)}$ in T of the minimal polynomial $M_u^{(r)} \in \mathbb{Q}[T, Y]$ of a generic linear form $u \in \mathbb{Q}[X_1, \ldots, X_n]$ in $\mathcal{V}_r$. While the obvious estimate $E_{n+1} \leq D$ is an immediate consequence of the Bézout inequality (2.1), in order to estimate E_r for $1 \leq r \leq n$, we have the following result (cf. Lemma 5.3).

Lemma 3.13. *The inequality $E_r \leq D/d_r$ holds for $2 \leq r \leq n$.*

Proof. Observe that substituting a generic value $y \in \mathbb{Q}$ for Y in $M_u^{(r)}(T, Y)$ we have $\deg_T M_u^{(r)}(T, Y) = \deg_T M_u^{(r)}(T, y) = \#\{t \in \mathbb{C}; M_u^{(r)}(t, y) = 0\}$. Moreover, it follows that $M_u^{(r)}(t, y) = 0$ if and only if there exists $x \in \mathbb{A}^n$ with $y = u(x)$ and $(t, x) \in \mathcal{V}_r$. Thus, it suffices to estimate the number of points $(t, x) \in \mathbb{A}^{n+1}$ with $u(x) - y = 0, F_1^{(r)}(t, x) = 0, \ldots, F_n^{(r)}(t, x) = 0$. Being u generic, the system

$$u(X) - y = 0, F_1^{(r)}(T, X) = 0, \ldots, F_n^{(r)}(T, X) = 0 \tag{3.10}$$

has finitely many solutions in $\mathbb{A}^{n+1}$. Furthermore, $u(X) - y, F_1^{(r)}, \ldots, F_{r-1}^{(r)}, F_{r+1}^{(r)}$ $, \ldots, F_n^{(r)} \in \mathbb{Q}[X]$ define a zero–dimensional variety W_r of $\mathbb{A}^n$ of degree at most D/d_r. Let $\ell \in \mathbb{Q}[X]$ be a separating linear form of W_r, and let $m_\ell, w_1, \ldots, w_n \in \mathbb{Q}[Y]$ be a geometric solution of W_r. Then an eliminating polynomial for T modulo $(u - y, F_1^{(r)}, \ldots, F_n^{(r)})$ is the resultant $q_T(Y) := Res_Y\big(m_\ell(Y), F_r^{(r)}(T, w(Y))\big)$. It is easy to see that $\deg_T q_T \leq D/d_r$, which implies the statement of the lemma. □

The following result is a critical step for our error probability estimate.

Proposition 3.14. *Suppose that the coefficients of the linear form u are randomly chosen in the set $\{1, \ldots, 4n\rho D^3\}$, where ρ is a fixed positive integer. Then the following assertions hold with error probability at most $1/\rho$:*

- *u separates the points of V and the fibres $\pi_r^{-1}(0)$ for $1 \leq r \leq n+1$,*
- *the algorithm underlying Lemma 3.11 outputs the right result.*

Proof. Let $\Lambda_1, \dots, \Lambda_n$ be new indeterminates and set $U_\Lambda := \Lambda_1 X_1 + \cdots + \Lambda_n X_n$. Fix r with $1 \leq r \leq n+1$. From Proposition 3.9 we see that $\pi_r^{-1}(0)$ is a zero–dimensional variety of degree D. Let $\pi_r^{-1}(0) := \{\xi^{(1)}, \dots, \xi^{(D)}\}$. Then the nonzero polynomial

$$P^{(r)} := \prod_{1 \leq i < j \leq D} \big(U_\Lambda(\xi^{(i)}) - U_\Lambda(\xi^{(j)})\big)$$

has degree $D(D-1)/2$ and satisfies the following condition: for any $\lambda \in \mathbb{Q}^n$ with $P^{(r)}(\lambda) \neq 0$, the linear form $u := \lambda_1 X_1 + \cdots + \lambda_n X_n$ separates the points of $\pi_r^{-1}(0)$. Similarly, let $V := \{\zeta^{(1)}, \dots, \zeta^{(\delta)}\}$ and set

$$Q := \prod_{1 \leq i < j \leq \delta} \big(U_\Lambda(\zeta^{(i)}) - U_\Lambda(\zeta^{(j)})\big).$$

Finally, define $P := P^{(1)} \cdots P^{(n+1)} Q$ and observe that $\deg P = (n+1)D(D-1)/2 + \delta(\delta-1)/2 \leq nD^2$. For any $\lambda \in \mathbb{Q}^n$ with $P(\lambda) \neq 0$, the linear form $u := \lambda_1 X_1 + \cdots + \lambda_n X_n$ separates the points of V and the fibres $\pi_r^{-1}(0)$ for $1 \leq r \leq n+1$.

From Theorem 2.1 it follows that for a random choice of the coefficients of u in the set $\{1, \dots, 4n\rho D^3\}$, the linear form u separates the points of $\pi_r^{-1}(0)$ for $1 \leq r \leq n+1$ and V with error probability at most $1/4\rho D \leq 1/2\rho$.

Next we consider the second requirement of the proposition, namely, the computation of the univariate resultants of the generic versions of the polynomials in (3.9). This is required in order to extend the algorithm for computing the minimal polynomial of u in $\pi_1^{-1}(0)$ to an algorithm for computing a geometric solution of $\pi_1^{-1}(0)$. We use a fast algorithm for computing resultants over $\mathbb{Q}(\Lambda)$ based on the EEA (Extended Euclidean Algorithm; see Section 2.3.3). We perform the EEA over the ring of power series $\mathbb{Q}[\![\Lambda - \lambda]\!]$, truncating all the intermediate results up to order 2. Therefore, the choice of the coefficients of u must guarantee that all the elements of $\mathbb{Q}[\Lambda]$ which have to be inverted during the execution of the EEA are invertible elements of $\mathbb{Q}[\![\Lambda - \lambda]\!]$.

For this purpose, we observe that, similarly to the proof of [vzGG99, Theorem 6.52], one deduces that all the denominators of the elements of

$\mathbb{Q}(\Lambda)$ arising during the application of the EEA to the generic version of the polynomials $\lambda_r^{-d_r}(\alpha - u^{(r-1)})^{d_r} - b_r$ and $m_{r-1}(u^{(r-1)})$ are divisors of at most $d_1 \cdots d_{r-1}$ polynomials of $\mathbb{Q}[\Lambda]$ of degree $2d_1 \cdots d_r$ for any $\alpha \in \mathbb{Q}$. This EEA step must be executed for $1 + d_1 \cdots d_r$ distinct values of $\alpha \in \mathbb{Q}$, in order to perform the interpolation step. Hence the product of the denominators arising during all the applications of the EEA has degree at most $2nD^3$. Therefore, from Theorem 2.1 we conclude that for a random choice of its coefficients in the set $\{1, \ldots, 4n\rho D^3\}$, the linear form u satisfies our second requirement with error probability at most $1/2\rho$.

Adding both probability estimates finishes the proof of the proposition. □

Now we can estimate the complexity and error probability of Algorithm 3.12.

Theorem 3.15. *Suppose that we are given a division–free straight–line program of length* T *evaluating polynomials* $\phi_1, \ldots, \phi_n, \varphi_1, \ldots, \varphi_n \in \mathbb{Q}[X]$ *such that* ϕ_i *is homogeneous of degree* $d_i > 0$ *and* $\deg \varphi_i < d_i$ *holds for* $1 \leq i \leq n$. *Assume that* $f_1 := \phi_1 + \varphi_1, \ldots, f_n := \phi_n + \varphi_n$ *define a generalized Pham system. Furthermore, fix a positive integer* ρ *and suppose that, for* $D := d_1 \cdots d_n$,

- *the coefficients of the linear forms* $Y_1, \ldots, Y_n$ *of step (1) of Algorithm 3.12 are randomly chosen in the set* $\{1, \ldots, 6n\rho D\}$,
- *the rational numbers* $b_1, \ldots, b_n$ *of step (1) of Algorithm 3.12 are randomly chosen in the set* $\{1, \ldots, 6n\rho D^2\}$,
- *the coefficients of the linear form* u *of step (2) of Algorithm 3.12 are randomly chosen in the set* $\{1, \ldots, 12n\rho D^3\}$.

Then Algorithm 3.12 computes a geometric solution of V *with*

$$O\big((n\mathsf{T} + n^3)\mathsf{M}(D){\textstyle\sum_{r=1}^{n+1}}\mathsf{M}(D/d_r)\big) \tag{3.11}$$

arithmetic operations in $\mathbb{Q}$ *and error probability at most* $1/\rho$, *where* $d_{n+1} := 1$.

Proof. According to Proposition 3.6, Corollary 3.10 and Proposition 3.14, for a random choice of the coefficients of $Y_1, \ldots, Y_n, u$ and $b_1, \ldots, b_n$ as in the statement of the theorem, with probability at least $1/\rho$ the following assertions hold:

(a) the linear forms $Y_1, \ldots, Y_n$ satisfy the statement of Proposition 3.6,

(b) the rational numbers $b_1, \ldots, b_n$ satisfy the statement of Corollary 3.10,

(c) the linear form u satisfy the statement of Proposition 3.14.

From (c) we conclude that the algorithm underlying Lemma 3.11 computes a geometric solution of $\pi_1^{-1}(0)$ with $O\big(n\mathsf{M}(D)^2\big)$ arithmetic operations in $\mathbb{Q}$.

From (b) and (c) we see that the deformations $\pi_r : \mathcal{V}_r \to \mathbb{A}^1$ satisfy all the requirements of Lemma 2.2 for $1 \le r \le n+1$. Furthermore, from the input straight–line program evaluating $\phi_1, \ldots, \phi_n, \varphi_1, \ldots, \varphi_n$ we may easily obtain a straight–line program evaluating the polynomials $F_i^{(r)}$ $(1 \le i \le n)$ of (3.3) or (3.4) with $\mathsf{T} + O(n)$ arithmetic operations in $\mathbb{Q}$. Hence, applying the algorithm underlying Lemma 2.2 successively to the fibre $\pi_r^{-1}(0)$ and the variety $\mathcal{V}_r$ for $r = 1, \ldots, n+1$, we finally obtain polynomials $m_u, v_1, \ldots, v_n \in \mathbb{Q}[T, Y]$ which form a geometric solution of V_{n+1}. These steps require $O\big((n\mathsf{T} + n^3)\mathsf{M}(D)\sum_{r=1}^{n+1}\mathsf{M}(D/d_r)\big)$ arithmetic operations in $\mathbb{Q}$.

Finally, we apply the algorithm underlying Lemma 2.3 to the polynomials $m_u, v_1, \ldots, v_n \in \mathbb{Q}[T, Y]$ and obtain a geometric solution of V with $O(n\mathsf{M}(D))$ additional arithmetic operations in $\mathbb{Q}$. This finishes the proof of the theorem. □

Chapter 4

Polynomial equation solving by lifting procedures for ramified fibres

Let V be a $\mathbb{Q}$–definable equidimensional affine variety of dimension 1, a curve, and let be given a generically unramified, finite morphism $\pi : V \to \mathbb{C}$. Earlier in this thesis, we have exhibited an algorithm which computes a geometric solution of V given a geometric solution of a particular unramified fibre $\pi^{-1}(\varepsilon_0)$ by using a global version of the Newton–Hensel lifting. Now we introduce an algorithm which, given a generically unramified family of zero–dimensional affine varieties, represented by a dominant (not necessarily finite) morphism $\pi : V \to \mathbb{C}$, and the infinitesimal structure of a particular (eventually *ramified*) fibre $\pi^{-1}(\varepsilon_0)$, computes a complete geometric solution of V.

This chapter is based on an article with the same title which I co-authored with A. Bompadre, G. Matera and R. Wachenchauzer ([BMWW04]). More explicitly, let $V \subset \mathbb{C}^{n+1}$ be a $\mathbb{Q}$–definable algebraic curve, and let us assume that the morphism $\pi : V \to \mathbb{C}$ induced by the canonical projection in the first coordinate is dominant and generically unramified. Let $\pi^{-1}(\varepsilon_0)$ be a finite and ramified fibre. Suppose further that we are given the infinitesimal structure of $\pi^{-1}(\varepsilon_0)$, i.e. the set of singular parts of the Puiseux expansions of the branches of V lying above ε_0 (see Section 4.1 for further details). Then we exhibit an algorithm which computes a complete description of an arbitrary fibre $\pi^{-1}(\varepsilon)$ (see Section 4.3).

Our algorithmic method is essentially based on a new variant of the global Newton–Hensel procedure. It is described in Section 4.2. Its time–space complexity is roughly $O(\deg V(\deg \pi)^{\alpha})$, where $\alpha = 1$ in several important cases. Then our algorithm extends and improves the procedures in [HKP$^+$00] and [Sch03]. Furthermore, our algorithm treats all the branches of V lying above ε_0 separately, improving thus the refinements of [HKP$^+$00, Section 3].

4.1. Puiseux expansions of space curves

In this section we introduce terminology about space curves, extending the usual terminology of Puiseux expansions of plane curves (see e.g. [Wal50]) and rational Puiseux expansions (see e.g. [Duv89], [Wal99]).

Let $T, \mathcal{E}, X_1, \ldots, X_n$ be indeterminates over $\mathbb{Q}$. Let n be a fixed positive integer, and $\mathbb{A}^n$ and $\mathbb{A}^{n+1}$ denote the affine spaces $\mathbb{A}^n(\mathbb{C})$ and $\mathbb{A}^{n+1}(\mathbb{C})$. We denote their coordinates by $x \in \mathbb{C}^n$ and $(\varepsilon, x) \in \mathbb{C}^{n+1}$ with $\varepsilon \in \mathbb{C}$.

Let $F_1, \ldots, F_n$ be polynomials in $\mathbb{Q}[\mathcal{E}, X] = \mathbb{Q}[\mathcal{E}, X_1, \ldots, X_n]$ which form a regular sequence and generate a radical ideal in $\mathbb{Q}[\mathcal{E}, X]$. Let $V := \{(\varepsilon, x) \in \mathbb{A}^{n+1} : F_1(\varepsilon, x) = 0, \ldots, F_n(\varepsilon, x) = 0\}$, and note that this is a curve.

Let $\pi : V \to \mathbb{A}^1$ be the morphism induced by the restriction to V of the canonical projection in the first coordinate $\pi(\varepsilon, x) := \varepsilon$. Assume that π is generically unramified; this implies that the Jacobian determinant $J_F := \det(\partial F_i / \partial X_j)_{1 \le i,j \le n}$ is not a zero divisor in $\mathbb{Q}[V]$.

A parameterization of the curve V is a non–constant vector $(\widetilde{\mathcal{E}}, \widetilde{X})$ of elements of the field of Laurent series $\overline{\mathbb{Q}}(\!(T)\!)$, with $\widetilde{X} := (\widetilde{X}_1, \ldots, \widetilde{X}_n) \in \overline{\mathbb{Q}}(\!(T)\!)^n$, such that $F_1(\widetilde{\mathcal{E}}, \widetilde{X}) = 0, \ldots, F_n(\widetilde{\mathcal{E}}, \widetilde{X}) = 0$ holds in $\overline{\mathbb{Q}}(\!(T)\!)$. A parameterization $(\widetilde{\mathcal{E}}, \widetilde{X})$ is called irreducible if there does not exist an integer $k > 1$ for which $(\widetilde{\mathcal{E}}, \widetilde{X}) \in \overline{\mathbb{Q}}(\!(T^k)\!)^{n+1}$ holds. The coefficient field of a parameterization $(\widetilde{\mathcal{E}}, \widetilde{X})$ of V is the field extension of $\mathbb{Q}$ generated by the coefficients of the series $\widetilde{\mathcal{E}}, \widetilde{X}_1, \ldots, \widetilde{X}_n$.

Given an element $\varphi \in \overline{\mathbb{Q}}(\!(T)\!)$, we define its order $o_T(\varphi)$ in T as the least power of T appearing with a nonzero coefficient in φ. Two parameterizations $(\widetilde{\mathcal{E}}, \widetilde{X})$ and $(\widetilde{\mathcal{E}}', \widetilde{X}')$ are called equivalent if there exists a power series $\varphi \in \mathbb{C}[\![T]\!]$

of order 1 such that $\widetilde{\mathcal{E}}(T) = \widetilde{\mathcal{E}}'(\varphi(T))$, $\widetilde{X}_1(T) = \widetilde{X}_1'(\varphi(T)), \ldots, \widetilde{X}_n(T) = \widetilde{X}_n'(\varphi(T))$ holds in $\overline{\mathbb{Q}}(\!(T)\!)$. A branch $\mathcal{C}$ of the curve V is defined as the equivalence class of an irreducible parameterization of V. We say that a branch $\mathcal{C}$ lies above a point $\varepsilon \in \mathbb{A}^1$ if there exists a parameterization $(\widetilde{\mathcal{E}}, \widetilde{X})$ in the equivalence class that defines the branch $\mathcal{C}$ with $\widetilde{\mathcal{E}} \in \overline{\mathbb{Q}}[\![T]\!]$ and $\widetilde{\mathcal{E}}(0) = \varepsilon$.

In what follows we shall consider the branches of V lying above 0. It is well–known that if 0 is an unramified value of the morphism $\pi : V \to \mathbb{A}^1$ defined by the rule $\pi(\varepsilon, x) := \varepsilon$, then all the branches of V lying above 0 have a parameterization of the form $(T, \widetilde{X})$ with $\widetilde{X} \in \mathbb{Q}[\![T]\!]^n$ (see Section 1.1).

Now we explain how the parameterizations of the branches of V lying above 0 can be represented by means of Puiseux series in $\mathcal{E}$. Let $\overline{\mathbb{Q}}(\mathcal{E})^* := \cup_{q \geq 0} \overline{\mathbb{Q}}(\mathcal{E}^{1/q})$ denote the field of Puiseux series in the variable $\mathcal{E}$ over $\overline{\mathbb{Q}}$, where $\overline{\mathbb{Q}}$ is the field of algebraic numbers. It is well–known that $\overline{\mathbb{Q}}(\mathcal{E})^*$ is an algebraically closed field. In fact, it is an algebraic closure of $\mathbb{Q}(\mathcal{E})$ (see e.g. [Wal50]).

Let us consider $F_1, \ldots, F_n$ as elements of the polynomial ring $\overline{\mathbb{Q}}(\mathcal{E})^*[X]$. Since the $\mathbb{Q}$–algebra extension $\mathbb{Q}(\mathcal{E}) \hookrightarrow \mathbb{Q}(V)$ is finitely generated, it follows that the affine variety $\{\bar{x} \in \mathbb{A}^n(\overline{\mathbb{Q}}(\mathcal{E})^*) : F_1(\bar{x}) = 0, \ldots, F_n(\bar{x}) = 0\}$ has dimension zero. Therefore, under our hypotheses there exist $D := \deg \pi$ distinct n–tuples $x^{(\ell)} := (x_1^{(\ell)}, \ldots, x_n^{(\ell)}) \in (\overline{\mathbb{Q}}(\mathcal{E})^*)^n$ of Puiseux series which are solutions of the system defined by $F_1, \ldots, F_n$ over $\overline{\mathbb{Q}}(\mathcal{E})^*$, i.e. such that the following equalities hold in $\overline{\mathbb{Q}}(\mathcal{E})^*$ for $1 \leq \ell \leq D$:

$$F_1(\mathcal{E}, x^{(\ell)}) = 0 \,, \ \ldots \ , \ F_n(\mathcal{E}, x^{(\ell)}) = 0. \tag{4.1}$$

For $1 \leq \ell \leq D$, let us write $x^{(\ell)} := (x_1^{(\ell)}, \ldots, x_n^{(\ell)})$ and $x_i^{(\ell)} := \sum_{m \geq m_\ell} a_{i,m}^{(\ell)} \cdot \mathcal{E}^{\frac{m}{e_\ell}}$ $(1 \leq i \leq n)$, with $e_\ell \in \mathbb{N}$, $m_\ell \in \mathbb{Z}$ and $a_{i,m}^{(\ell)} \in \overline{\mathbb{Q}}$. Without loss of generality we may assume for $1 \leq \ell \leq D$ that e_ℓ has no common factors with the greatest common divisor of the set of m's for which $a_{i,m}^{(\ell)} \neq 0$ holds. The number e_ℓ is called the ramification index of the series $x^{(\ell)}$. Let us remark that for $1 \leq \ell \leq D$ the coefficient field generated by all the coordinates of $x^{(\ell)}$ is a finite extension of $\mathbb{Q}$ (see e.g. [Duv89]). Its degree f_ℓ is called the residual degree of $x^{(\ell)}$.

Following [Duv89] (see also [Wal99]), a set of non–equivalent parameterizations

$$\{(\widetilde{\mathcal{E}}^{(1)}, \widetilde{X}^{(1)}), \ldots, (\widetilde{\mathcal{E}}^{(\widehat{g})}, \widetilde{X}^{(\widehat{g})})\} \subset \overline{\mathbb{Q}}(\!(T)\!)^{n+1} \tag{4.2}$$

containing a complete set of representatives of the branches of V lying above 0 is called a system of rational Puiseux expansions (of the branches of V lying above 0) if it is invariant under the action of the Galois group of the field extension $\overline{\mathbb{Q}}/\mathbb{Q}$ and $\widetilde{\mathcal{E}}^{(\ell)} = \lambda_\ell T^{e_\ell}$, with $e_\ell \in \mathbb{N}$ and $\lambda_\ell \in \overline{\mathbb{Q}} \setminus \{0\}$ for $1 \leq \ell \leq \widehat{g}$. Let g be the number of orbits defined on the set (4.2) under the action of the Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$ and suppose that we have chosen the numbering in (4.2) such that the first g elements represent different orbits.

Let us observe that from a given system of rational Puiseux expansions we may easily obtain the system of classical Puiseux expansions of the branches of V lying above 0, i.e. the complete set of solutions of (4.1). Indeed, let

$$\Big\{(\widetilde{\mathcal{E}}^{(\ell)}, \widetilde{X}^{(\ell)}) := \big(\lambda_\ell T^{e_\ell}, \sum_{m \geq m_\ell} a_{1,m}^{(\ell)} T^m, \ldots, \sum_{m \geq m_\ell} a_{n,m}^{(\ell)} T^m\big) : 1 \leq \ell \leq g\Big\} \quad (4.3)$$

be a system of rational Puiseux expansions of V, and let $\xi_\ell, \lambda_\ell^{-1/e_\ell} \in \overline{\mathbb{Q}}$ denote a primitive e_ℓ–th root of 1 and an e_ℓ–th root of λ_ℓ^{-1} for $1 \leq \ell \leq g$. Then the classical Puiseux expansions of the branches of V lying above 0 are given by

$$\Big\{\widetilde{X}^{(\ell)}(\xi_\ell^j \lambda_\ell^{-1/e_\ell} \mathcal{E}^{1/e_\ell}) : 1 \leq \ell \leq g,\, 1 \leq j \leq e_\ell\Big\}.$$

Observe that the ramification index of the expansion $\widetilde{X}^{(\ell)}(\xi_\ell^j \lambda_\ell^{-1/e_\ell} \mathcal{E}^{1/e_\ell})$ is e_ℓ. Let R denote the least integer such that the partial expansion vectors $\sum_{m=m_\ell}^R a_m^{(\ell)} T^m := \sum_{m=m_\ell}^R (a_{1,m}^{(\ell)}, \ldots, a_{n,m}^{(\ell)}) T^m$ are pairwise distinct for $1 \leq \ell \leq D$.

Let us remark that a combination of [Sch03, Proposition 1] and [Duv89, Lemma 2] yields the estimate $R - m_\ell \leq 2(e_\ell f_\ell)^2$. The integer R is called the regularity index of the system (4.3). For $1 \leq \ell \leq g$, the partial expansion $\sum_{m=m_\ell}^R a_m^{(\ell)} T^m$ is called the singular part of $\widetilde{X}^{(\ell)}$.

4.2. Lifting procedures for ramified fibres

With notations and assumptions as in Section 4.1, let $\{(\widetilde{\mathcal{E}}^{(\ell)}, \widetilde{X}^{(\ell)}) : 1 \leq \ell \leq g\}$ be a set of parameterizations which induces a system of rational Puiseux expansions of the branches of V lying above 0 by the action of the Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$. For $1 \leq \ell \leq g$, let $e_\ell, f_\ell \in \mathbb{N}$ denote the ramification index and the residual degree of the Puiseux expansions associated to the parameterization

$$(\widetilde{\mathcal{E}}^{(\ell)}, \widetilde{X}^{(\ell)}) := \Big(\lambda_\ell T^{e_\ell}, \sum_{m \geq m_\ell} a_m^{(\ell)} T^m\Big), \tag{4.4}$$

with $a_m^{(\ell)} \in \overline{\mathbb{Q}}^n$ for $1 \leq \ell \leq g$, $m \geq m_\ell$. We have $\sum_{\ell=1}^{g} e_\ell f_\ell = D$ (see, e.g., [Duv89]). Let $R \in \mathbb{Z}$ be the regularity index of the system of rational Puiseux expansions (4.4). Let us recall the estimate $R - m_\ell \leq 2(e_\ell f_\ell)^2$ on the size of the singular parts of the parameterizations in (4.4) from Section 4.1.

Let $T, Y_1, \ldots, Y_n$ be indeterminates over $\overline{\mathbb{Q}}$ and write $Y := (Y_1, \ldots, Y_n)$. Let $K^{(\ell)} := \mathbb{Q}(\{\lambda_\ell, a_{m,1}^{(\ell)}, \ldots, a_{m,n}^{(\ell)} : m \geq m_\ell\})$ be the coefficient field of the parameterization $(\widetilde{\mathcal{E}}^{(\ell)}, \widetilde{X}^{(\ell)})$. Denote by $\sigma_1^{(\ell)}, \ldots, \sigma_{f_\ell}^{(\ell)}$ the morphisms of the Galois group of the field extension $\mathbb{Q} \hookrightarrow K^{(\ell)}$. For any $(\ell, j, k) \in \mathbb{N}^3$ with $1 \leq \ell \leq g$, $1 \leq j \leq n$ and $1 \leq k \leq f_\ell$, let us define $G_j^{(\ell,k)} \in \overline{\mathbb{Q}}[T, Y]$ by:

$$G_j^{(\ell,k)} := T^{\alpha_{j,\ell}} F_j\Big(\sigma_k^{(\ell)}(\lambda_\ell) T^{e_\ell}, \sum_{m=m_\ell}^{R-1} \sigma_k^{(\ell)}(a_m^{(\ell)}) T^m + Y T^R\Big), \tag{4.5}$$

where $\alpha_{j,\ell} \in \mathbb{Z}$ is chosen such that the order of $G_j^{(\ell,k)}$ in T equals zero.

Our algorithmic methods are based on a deformation technique which allows us to compute an arbitrary fibre of the morphism $\pi : V \to \mathbb{A}^1$ by "lifting" the fibre $\pi^{-1}(0)$. In order to perform this process of lifting, we would like to use a global Newton–Hensel procedure as in Chapter 1 (see also [GHM+98], [GHH+97], [HKP+00], [Sch03]). Unfortunately, this is no longer possible because the essential hypothesis on the unramifiedness of the fibre $\pi^{-1}(0)$ is missed.

In order to circumvent this difficulty, one might try to proceed as in the plane curve case and consider the ideal $\mathcal{I}^{(\ell,k)}$ of $\overline{\mathbb{Q}}[T, Y]$ generated by the polynomials $G_1^{(\ell,k)}, \ldots, G_n^{(\ell,k)}$ for $1 \leq \ell \leq g$ and $1 \leq k \leq f_\ell$. Let $V^{(\ell,k)}$ be the affine sub-variety of $\mathbb{A}^{n+1}$ defined by $\mathcal{I}^{(\ell,k)}$, and let $\pi^{(\ell,k)} : V^{(\ell,k)} \to \mathbb{A}^1$ be the morphism defined by $\pi^{(\ell,k)}(t, x) := t$. Unlike the plane curve case, $G_1^{(\ell,k)}, \ldots, G_n^{(\ell,k)}$ are not necessarily smooth at $T = 0$, unless a suitable flatness condition is satisfied (compare [BM93], [ANMR91] and [ANMR92]). In Section 4.2.2 we exhibit a flatness condition which assures that the points of the fibre $(\pi^{(\ell,k)})^{-1}(0)$ are $(G_1^{(\ell,k)}, \ldots, G_n^{(\ell,k)})$–smooth. Then in Section 4.2.3

we describe a variant of the global Newton–Hensel procedure of Section 2.4.1 specifically adapted to our situation. Finally, in Section 4.2.4 we show that this flatness condition is also necessary to assure smoothness.

Let us observe that the main results of this section, namely Theorems 4.5 and 4.7 below, depend on the infinitesimal structure of the fibre $\pi^{-1}(0)$, and hence can be (slightly) generalized to the case where $F_1, \ldots, F_n$ form a regular sequence of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$ and generate a radical ideal of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$. Nevertheless, for the sake of clarity we are not going to prove this generalization.

4.2.1. Properties of the ideal $\mathcal{I}^{(\ell,k)}$

Let us fix integers ℓ, k with $1 \leq \ell \leq g$ and $1 \leq k \leq f_\ell$. In order to exhibit our flatness condition we first need to establish some properties of the ideal $\mathcal{I}^{(\ell,k)}$.

Let $\mathcal{I}^{(\ell,k)}\overline{\mathbb{Q}}(T)^*[Y]$ denote the (extended) ideal generated by $\mathcal{I}^{(\ell,k)}$ in $\overline{\mathbb{Q}}(T)^*[Y]$. In order to describe the zero set of $\mathcal{I}^{(\ell,k)}\overline{\mathbb{Q}}(T)^*[Y]$ in $\mathbb{A}^n(\overline{\mathbb{Q}}(T)^*)$, for any pair (ℓ, k), let $\mathcal{L}_{\ell,k}$ be the set of pairs (ℓ', k') for which there exists a vector of Puiseux series associated to the (ℓ', k')–th parameterization which agrees up to order R with one associated to the (ℓ, k)–th parameterization, i.e.

$$\mathcal{L}_{\ell,k} := \Big\{(\ell', k');\ e_\ell = e_{\ell'},\ m_\ell = m_{\ell'},\ \big(\exists\, \lambda_\ell^{-1/e_\ell}\big)\big(\exists\, \lambda_{\ell'}^{-1/e_{\ell'}}\big) \\ \sum_{m=m_\ell}^{R-1} \sigma_k^{(\ell)}(a_m^{(\ell)})\sigma_k^{(\ell)}(\lambda_\ell^{-\frac{1}{e_\ell}})^m T^m = \sum_{m=m_\ell}^{R-1} \sigma_{k'}^{(\ell')}(a_m^{(\ell')})\sigma_{k'}^{(\ell')}(\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^m T^m\Big\}. \tag{4.6}$$

The sets $\mathcal{L}_{\ell,k}$ form a partition of the set of pairs $\cup_{1\leq \ell \leq g}\{\ell\} \times \{1, \ldots, f_\ell\}$. For any (ℓ, k) let

$$\widetilde{V}^{(\ell,k)} := V\left(\mathcal{I}^{(\ell,k)}\overline{\mathbb{Q}}(T)^*[Y]\right)$$

be the affine subvariety of $\mathbb{A}^n(\overline{\mathbb{Q}}(T)^*)$ induced by $\mathcal{I}^{(\ell,k)}\overline{\mathbb{Q}}(T)^*[Y]$.

Lemma 4.1. *The extended ideal $\mathcal{I}^{(\ell,k)}\overline{\mathbb{Q}}(T)^*[Y]$ defines a zero–dimensional subvariety $\widetilde{V}^{(\ell,k)}$ of $\mathbb{A}^n(\overline{\mathbb{Q}}(T)^*)$. Furthermore, we have*

$$\widetilde{V}^{(\ell,k)} \cap \overline{\mathbb{Q}}[\![T]\!]^n = \left\{\sum_{m\geq R} \sigma_{k'}^{(\ell')}(a_m^{(\ell')})\sigma_{k'}^{(\ell')}(\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^m \sigma_k^{(\ell)}(\lambda_\ell^{\frac{1}{e_\ell}})^m T^{m-R};\ (\ell', k') \in \mathcal{L}_{\ell,k}\right\}. \tag{4.7}$$

Proof. From the definition of $G_1^{(\ell,k)},\dots,G_n^{(\ell,k)}$ and the parameterization $(\widetilde{\mathcal{E}}^{(\ell)},\widetilde{X}^{(\ell)})$, it follows that the vector of power series $\sum_{m\ge R}\sigma_k^{(\ell)}(a_m^{(\ell)})T^{m-R}$ is a point of $\widetilde{V}^{(\ell,k)}\subset\mathbb{A}^n(\overline{\mathbb{Q}}(T)^*)$.

On the other hand, we observe that any point of $\widetilde{V}^{(\ell,k)}$ induces univocally a finite set of points $\overline{x}\in\mathbb{A}^n(\overline{\mathbb{Q}}(\mathcal{E})^*)$ such that $F_j(\mathcal{E},\overline{x})=0$ holds in $\overline{\mathbb{Q}}(\mathcal{E})^*$ for $1\le j\le n$. Since $\{x\in\mathbb{A}^n(\overline{\mathbb{Q}}(\mathcal{E})^*):F_1(\overline{x})=0,\dots,F_n(\overline{x})=0\}$ has dimension zero (see Subsection 4.1), it follows that $\widetilde{V}^{(\ell,k)}$ must also have dimension zero.

Now we show identity (4.7). Let $\widehat{V}^{(\ell,k)}$ be the right–hand side of identity (4.7):

$$\widehat{V}^{(\ell,k)}:=\Big\{\sum_{m\ge R}\sigma_{k'}^{(\ell')}(a_m^{(\ell')})\sigma_{k'}^{(\ell')}(\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^m\sigma_k^{(\ell)}(\lambda_\ell^{\frac{1}{e_\ell}})^mT^{m-R};\ (\ell',k')\in\mathcal{L}_{\ell,k}\Big\}.$$

It is easy to see that $\widehat{V}^{(\ell,k)}\subset\widetilde{V}^{(k,\ell)}$ holds. On the other hand, we observe that any point $\sum_{m\ge0}b_mT^m\in\widetilde{V}^{(\ell,k)}\cap\overline{\mathbb{Q}}[\![T]\!]^n$ induces a unique parameterization

$$\varphi:=\big(\sigma_k^{(\ell)}(\lambda_\ell)T^{e_\ell},\sum_{m=m_\ell}^{R-1}\sigma_k^{(\ell)}(a_m^{(\ell)})T^m+\sum_{m\ge R}b_{m-R}T^m\big)$$

of a branch of V lying above 0, and hence a vector of Puiseux series

$$\overline{x}:=\sum_{m=m_\ell}^{R-1}\sigma_k^{(\ell)}(a_m^{(\ell)})\sigma_k^{(\ell)}(\lambda_\ell^{-\frac{1}{e_\ell}})^m\mathcal{E}^{\frac{m}{e_\ell}}+\sum_{m\ge R}b_{m-R}\sigma_k^{(\ell)}(\lambda_\ell^{-\frac{1}{e_\ell}})^m\mathcal{E}^{\frac{m}{e_\ell}}$$

satisfying $F_j(\mathcal{E},\overline{x})=0$ for $j=1,\dots,n$. Then there exists (ℓ_0,k_0) such that $\overline{x}=\sum_{m\ge m_{\ell_0}}\sigma_{k_0}^{(\ell_0)}(a_m^{(\ell_0)})\sigma_{k_0}^{(\ell_0)}(\lambda_{\ell_0}^{-1})^{m/e_{\ell_0}}\mathcal{E}^{m/e_{\ell_0}}$. This shows that (ℓ_0,k_0) belongs to $\mathcal{L}_{\ell,k}$ and

$$\varphi=\big(\sigma_k^{(\ell)}(\lambda_\ell)T^{e_\ell},\sum_{m\ge m_\ell}\sigma_{k_0}^{(\ell_0)}(a_m^{(\ell_0)})\sigma_{k_0}^{(\ell_0)}(\lambda_{\ell_0}^{-1/e_{\ell_0}})^m\sigma_k^{(\ell)}(\lambda_\ell^{1/e_\ell})^mT^m\big)$$

holds. Then

$$\sum_{m\ge R}b_mT^{m-R}=\sum_{m\ge R}\sigma_{k_0}^{(\ell_0)}(a_m^{(\ell_0)})\sigma_{k_0}^{(\ell_0)}(\lambda_{\ell_0}^{-1/e_{\ell_0}})^m\sigma_k^{(\ell)}(\lambda_\ell^{1/e_\ell})^mT^{m-R},$$

which shows identity (4.7). □

Let us observe that $G_1^{(\ell,k)},\dots,G_n^{(\ell,k)}$ are obtained from $F_1,\dots,F_n$ by applying the mapping $\Psi_R^{(\ell,k)}:\overline{\mathbb{Q}}[\mathcal{E},X]\to\overline{\mathbb{Q}}[T,Y]$ defined by

$$\Psi_R^{(\ell,k)}\big(F(\mathcal{E},X)\big):=T^{\alpha_F}F\Big(\sigma_k^{(\ell)}(\lambda_\ell)T^{e_\ell},\sum_{m=m_\ell}^{R-1}\sigma_k^{(\ell)}(a_m^{(\ell)})T^m+YT^R\Big),$$

where $\alpha_F\in\mathbb{Z}$ is chosen such that the order in T of $\Psi_R^{(\ell,k)}(F)$ is zero. In order to "invert" the mapping $\Psi_R^{(\ell,k)}$, up to a power of $\mathcal{E}$, we introduce the following morphism $\Phi_R^{(\ell,k)}:\overline{\mathbb{Q}}(T)[Y]\to\overline{\mathbb{Q}}(\mathcal{E})[X]$ of $\overline{\mathbb{Q}}$–algebras:

$$\Phi_R^{(\ell,k)}\big(F(T,Y)\big):=F\Big(\mathcal{E},\mathcal{E}^{-R}\big(X-\sum_{m=m_\ell}^{R-1}\sigma_k^{(\ell)}(a_m^{(\ell)})\mathcal{E}^m\big)\Big).$$

We have $\mathcal{E}^{-\alpha_F}\Phi_R^{(\ell,k)}\big(\Psi_R^{(\ell,k)}(F)\big)=F(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell},X)$ for any $F\in\overline{\mathbb{Q}}[\mathcal{E},X]$.

Lemma 4.2. *$G_1^{(\ell,k)},\dots,G_n^{(\ell,k)}$ form a regular sequence of $\overline{\mathbb{Q}}[T,Y]$.*

Proof. Arguing by contradiction, assume that $G_1^{(\ell,k)},\dots,G_n^{(\ell,k)}$ do not form a regular sequence. Then there exists $j\geq 2$ such that $G_j^{(\ell,k)}$ is a zero divisor of $\overline{\mathbb{Q}}[T,Y]/(G_1^{(\ell,k)},\dots,G_{j-1}^{(\ell,k)})$, i.e. there exist $\widetilde{H},\widetilde{P}_1,\dots,\widetilde{P}_{j-1}\in\overline{\mathbb{Q}}[T,Y]$ such that

$$\widetilde{H}\Psi_R^{(\ell,k)}(F_j)=\widetilde{H}G_j^{(\ell,k)}=\sum_{i=1}^{j-1}\widetilde{P}_iG_i^{(\ell,k)}=\sum_{i=1}^{j-1}\widetilde{P}_i\Psi_R^{(\ell,k)}(F_i)\qquad(4.8)$$

holds in $\overline{\mathbb{Q}}[T,Y]$ with $\widetilde{H}\notin(G_1^{(\ell,k)},\dots,G_{j-1}^{(\ell,k)})$. Applying the morphism $\Phi_R^{(\ell,k)}$ to the left and right–hand side members of identity (4.8) and multiplying by a suitable power of $\mathcal{E}$, we deduce that there exist $H,P_1,\dots,P_{j-1}\in\overline{\mathbb{Q}}[\mathcal{E},X]$ such that

$$HF_j\big(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell},X\big)=\sum_{i=1}^{j-1}P_iF_i\big(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell},X\big)\qquad(4.9)$$

holds in $\overline{\mathbb{Q}}[\mathcal{E},X]$. Identity (4.9) may be rewritten in the following way:

$$\sum_{h=0}^{e_\ell-1}\mathcal{E}^hH_hF_j\big(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell},X\big)=\sum_{h=0}^{e_\ell-1}\mathcal{E}^h\sum_{i=1}^{j-1}P_{i,h}F_i\big(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell},X\big),\qquad(4.10)$$

with $H_h, P_{1,h}, \dots, P_{j-1,h} \in \overline{\mathbb{Q}}[\mathcal{E}^{e_\ell}, X]$ for $0 \le h \le e_\ell - 1$. Then identity (4.10) holds if and only if the following identity

$$H_h F_j\big(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X\big) = \sum_{i=1}^{j-1} P_{i,h} F_i\big(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X\big)$$

holds in $\overline{\mathbb{Q}}[\mathcal{E}, X]$ for $0 \le h \le e_\ell - 1$, with at least one polynomial $H_h \notin (F_1(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X), \dots, F_n(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X))$. This implies that F_j is a zero divisor of the $\overline{\mathbb{Q}}$–algebra $\overline{\mathbb{Q}}[\mathcal{E}, X]/(F_1, \dots, F_{j-1})$, which contradicts our hypotheses. □

Let us remark that Lemma 4.2 shows in particular that the ring $\overline{\mathbb{Q}}[T, Y]/\mathcal{I}^{(\ell,k)}$ is Cohen–Macaulay.

Let $1 \le \ell \le g, 1 \le k \le f_\ell$. From now on we fix the notations: $J_F := \det\big(\frac{\partial F_i}{\partial X_j}\big)_{1 \le i,j \le n}$, $J_{G^{(\ell,k)}} := \det\big(\frac{\partial G_i^{(\ell,k)}}{\partial Y_j}\big)_{1 \le i,j \le n}$.

Lemma 4.3. *The ideal $\mathcal{I}^{(\ell,k)}$ is a radical ideal of $\overline{\mathbb{Q}}[T, Y]$.*

Proof. Since by hypothesis the morphism π is generically unramified, the Jacobian determinant J_F is not a zero divisor of $\overline{\mathbb{Q}}[\mathcal{E}, X]/(F_1, \dots, F_n)$. We claim that the Jacobian determinant $J_{G^{(\ell,k)}}$ is not a zero divisor of $\overline{\mathbb{Q}}[T, Y]/\mathcal{I}^{(\ell,k)}$.

Suppose that there exist polynomials $\widetilde{H}, \widetilde{P}_1, \dots, \widetilde{P}_n \in \overline{\mathbb{Q}}[T, Y]$ such that

$$\widetilde{H} J_{G^{(\ell,k)}} = \sum_{i=1}^{n} \widetilde{P}_i G_i^{(\ell,k)} \tag{4.11}$$

holds in $\overline{\mathbb{Q}}[T, Y]$. Observe that $J_F\big(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X\big) = \mathcal{E}^\alpha \Phi_R^{(\ell,k)}(J_{G^{(\ell,k)}})$ holds for a suitable $\alpha \in \mathbb{Z}$. Arguing as in the proof of Lemma 4.2 we conclude that there exist polynomials $H_h, P_{i,h} \in \overline{\mathbb{Q}}[\mathcal{E}^{e_\ell}, X]$ for every $0 \le h \le e_\ell - 1$ and $1 \le i \le n$ such that identity (4.11) holds if and only if the identity

$$H_h J_F\big(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X\big) = \sum_{i=1}^{n} P_i F_i\big(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X\big)$$

holds in $\overline{\mathbb{Q}}[\mathcal{E}^{e_\ell}, X]$ for every $0 \le h \le e_\ell - 1$ where at least one polynomial H_h does not belong to $(F_1, \dots, F_n)$. We conclude that J_F is a zero divisor of $\overline{\mathbb{Q}}[\mathcal{E}, X]/(F_1, \ldots, F_n)$, contradicting thus the hypothesis on the generic unramifiedness of π. We conclude that $J_{G^{(\ell,k)}}$ is not a zero divisor of $\overline{\mathbb{Q}}[T, Y]/\mathcal{I}^{(\ell,k)}$. This implies that the ideal generated by the $n \times n$ minors of the Jacobian matrix of $G_1^{(\ell,k)}, \ldots, G_n^{(\ell,k)}$ with respect to $T, Y_1, \ldots, Y_n$ has codimension at least 1 in $\overline{\mathbb{Q}}[T, Y]/\mathcal{I}^{(\ell,k)}$. Since $\overline{\mathbb{Q}}[T, Y]/\mathcal{I}^{(\ell,k)}$ is a Cohen–Macaulay ring, from [Eis95, Theorem 18.15] we conclude that $\mathcal{I}^{(\ell,k)}$ is radical. □

4.2.2. The unramifiedness of the morphism $\pi^{(\ell,k)}$ at $T = 0$

In what follows, we shall use the following terminology: For a given polynomial $G \in \overline{\mathbb{Q}}[T, Y] := \overline{\mathbb{Q}}[T, Y_1, \ldots, Y_n]$, let us write $G(T, Y) = T^\alpha g(Y) + \widehat{G}$, where g is a nonzero polynomial of $\overline{\mathbb{Q}}[Y]$ and $\widehat{G} \in \mathbb{Q}[T, Y]$ has at least order $\alpha+1$ in T. The polynomial $g(Y)$ is called the *initial form* of G and is denoted $in(G)$.

Let us fix $\ell, k \in \mathbb{N}$ with $1 \leq \ell \leq g$ and $1 \leq k \leq e_\ell$. We are going to show that the morphism $\pi^{(\ell,k)} : V^{(\ell,k)} \to \mathbb{A}^1$ defined by $\pi^{(\ell,k)}(t, y) := t$ is unramified at every point of the fibre $(\pi^{(\ell,k)})^{-1}(0)$. For this purpose, we are going to prove that for any point $b \in (\pi^{(\ell,k)})^{-1}(0)$ there exists a unique holomorphic branch of the curve $V^{(\ell,k)}$ passing through b, and $b \in (\pi^{(\ell,k)})^{-1}(0)$ has multiplicity 1 in this branch. This is equivalent to showing that the zero–dimensional affine variety defined by the (initial) ideal $in(\mathcal{I}^{(\ell,k)}) \subset \overline{\mathbb{Q}}[Y]$ generated by the set $\{in(F) : F \in \mathcal{I}^{(\ell,k)}\}$ has as many points as the number of holomorphic branches of $V^{(\ell,k)}$ passing through points of $(\pi^{(\ell,k)})^{-1}(0)$, namely $\#(\widetilde{V}^{(\ell,k)} \cap \overline{\mathbb{Q}}[\![T]\!]^n)$ with the notations of Lemma 4.1. This is the content of our next result.

Proposition 4.4. *Let $W^{(\ell,k)}$ denote the affine subvariety of $\mathbb{A}^n$ defined by the ideal $in(\mathcal{I}^{(\ell,k)})$. Then the following identity holds in $\mathbb{A}^n$:*

$$W^{(\ell,k)} = \{\sigma_{k'}^{(\ell')}(a_R^{(\ell')})\sigma_{k'}^{(\ell')}(\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^R \sigma_k^{(\ell)}(\lambda_\ell^{\frac{1}{e_\ell}})^R : (\ell', k') \in \mathcal{L}_{\ell,k}\}.$$

Proof. Let $\widehat{W}^{(\ell,k)} := \{\sigma_{k'}^{(\ell')}(a_R^{(\ell')})\sigma_{k'}^{(\ell')}(\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^R \sigma_k^{(\ell)}(\lambda_\ell^{\frac{1}{e_\ell}})^R : (\ell', k') \in \mathcal{L}_{\ell,k}\}$. We want to show that $W^{(\ell,k)} = \widehat{W}^{(\ell,k)}$ holds.

We first prove the inclusion $W^{(\ell,k)} \supset \widehat{W}^{(\ell,k)}$. Let $b \in \widehat{W}^{(\ell,k)}$ and let $F \in \mathcal{I}^{(\ell,k)}$. Then there exists $(\ell', k') \in \mathcal{L}_{\ell,k}$ such that

$$b = \sigma_{k'}^{(\ell')}(a_R^{(\ell')})\sigma_{k'}^{(\ell')}(\lambda_{\ell'}^{-1/e_{\ell'}})^R\sigma_k^{(\ell)}(\lambda_\ell^{1/e_\ell})^R$$

holds. Let us write $F = T^\alpha\, in(F) + \widehat{F}$, with $in(F) \in \overline{\mathbb{Q}}[Y] \setminus \{0\}$ and $\widehat{F} \in \overline{\mathbb{Q}}[T, Y]$ of order at least $\alpha + 1$ in T. From Lemma 4.1 we have

$$\begin{array}{rcl} 0 & = & F\big(T, \sum_{m \geq R} \sigma_{k'}^{(\ell')}(a_m^{(\ell')})\sigma_{k'}^{(\ell')}(\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^m \sigma_k^{(\ell)}(\lambda_\ell^{\frac{1}{e_\ell}})^m T^{m-R}\big) \\ & = & T^\alpha in(F)\big(\sigma_{k'}^{(\ell')}(a_R^{(\ell')})\sigma_{k'}^{(\ell')}(\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^R \sigma_k^{(\ell)}(\lambda_\ell^{\frac{1}{e_\ell}})^R\big) + T^{\alpha+1}\widehat{f}(T) \\ & = & T^\alpha in(F)(b) + T^{\alpha+1}\widehat{f}(T), \end{array}$$

with $\widehat{f} \in \overline{\mathbb{Q}}[\![T]\!]$. Then $in(F)(b) = 0$, which shows the inclusion $W^{(\ell,k)} \supset \widehat{W}^{(\ell,k)}$.

In order to prove the converse inclusion, let $U \in \mathbb{Q}[X]$ be a linear form for $V = V(F_1, \ldots, F_n) \subset \mathbb{A}^n$ such that the minimal polynomial $m_u \in \mathbb{Q}(\mathcal{E})[Z]$ of the element induced by U in the extension $\mathbb{Q}[\mathcal{E}] \to \mathbb{Q}[V]$ has degree $D = \deg \pi$ (for $\pi : V \to A^1(\mathbb{C})$ defined by $\pi(\varepsilon, x) := \varepsilon$; see Section 2.4).

For $1 \leq i \leq D$, let $U^{(i)}$ be the element of $\overline{\mathbb{Q}}(\mathcal{E})^*$ defined by $U^{(i)} := U(x^{(i)})$, where $\{x^{(1)}, \ldots, x^{(D)}\}$ denote the classical Puiseux expansions of the branches of V lying above 0. Let u be the rational function induced by U in $\mathbb{Q}(V)$. Observe that $\prod_{i=1}^D (Z - U^{(i)})$ annihilates u in the zero–dimensional $\overline{\mathbb{Q}}(\mathcal{E})^*$–algebra $\overline{\mathbb{Q}}(\mathcal{E})^* \otimes \mathbb{Q}(V)$. Taking into account that $\prod_{i=1}^D (Z - U^{(i)})$ belongs to $\mathbb{Q}(\mathcal{E})[Z]$ (see [Duv89]) and has degree D in Z, we conclude that $m_u = \prod_{i=1}^D (Z - U^{(i)})$ holds. This shows that $U^{(j)} \neq U^{(k)}$ for $1 \leq j < k \leq D$ and we have the following expression for $m_u(Z)$ in $\overline{\mathbb{Q}}(\mathcal{E})^*[Z]$ (compare [Duv89]):

$$m_u(\mathcal{E}, Z) = \prod_{\ell=1}^{g} \prod_{k=1}^{f_\ell} \prod_{j=1}^{e_\ell} \big(Z - \sum_{m \geq m_\ell} U\big(\sigma_k^{(\ell)}(a_m^{(\ell)})\big)\sigma_k^{(\ell)}(\lambda_\ell^{-\frac{1}{e_\ell}})^m \xi_\ell^{jm} \mathcal{E}^{\frac{m}{e_\ell}}\Big),$$

where $\sigma_1^{(\ell)}, \ldots, \sigma_{f_\ell}^{(\ell)}$ range over all the morphisms of the Galois group of the field extension $\mathbb{Q} \hookrightarrow K^{(\ell)}$ and $\lambda_\ell^{-1/e_\ell}, \xi_\ell$ denote an e_ℓ–th root of λ_ℓ^{-1} and a primitive e_ℓ–th root of 1. From [Duv89, Theorem 2], we deduce that, for $1 \leq \ell \leq g$,

$$m_u^{(\ell)} := \prod_{k=1}^{f_\ell} m_u^{(\ell,k)} := \prod_{k=1}^{f_\ell} \Bigg(\prod_{j=1}^{e_\ell} \Big(Z - \sum_{m \geq m_\ell} U\big(\sigma_k^{(\ell)}(a_m^{(\ell)})\big)\sigma_k^{(\ell)}(\lambda_\ell^{-\frac{1}{e_\ell}})^m \xi_\ell^{jm} \mathcal{E}^{\frac{m}{e_\ell}}\Big)\Bigg) \tag{4.12}$$

is an irreducible polynomial of $\mathbb{Q}(\!(\mathcal{E})\!)[Z]$, and, for $1 \leq k \leq f_\ell$, $m_u^{(\ell,k)}$ is an irreducible element of $\overline{\mathbb{Q}}(\!(\mathcal{E})\!)[Z]$ satisfying

$$m_u^{(\ell,k)}\left(\sigma_k^{(\ell)}(\lambda_\ell)T^{e_\ell}, Z\right) = \prod_{j=1}^{e_\ell}\Big(Z - \sum_{m \geq m_\ell} U\big(\sigma_k^{(\ell)}(a_m^{(\ell)})\big)(\xi_\ell^j T)^m\Big). \tag{4.13}$$

For $1 \leq \ell \leq g$ and $1 \leq k \leq f_\ell$, let us consider the morphism of $\overline{\mathbb{Q}}$-algebras

$$\begin{aligned} \widetilde{\Psi}_R^{(\ell,k)} : \overline{\mathbb{Q}}(\!(\mathcal{E})\!)[X] &\longrightarrow \overline{\mathbb{Q}}(\!(T)\!)[Y] \\ F(\mathcal{E}, X) &\longmapsto F\big(\sigma_k^{(\ell)}(\lambda_\ell)T^{e_\ell} \,,\, \sum_{m=m_\ell}^{R-1} \sigma_k^{(\ell)}(a_m^{(\ell)})T^m + YT^R\big). \end{aligned}$$

Let us fix ℓ', k' with $1 \leq \ell' \leq g$ and $1 \leq k' \leq e_\ell$. Applying the morphism $\widetilde{\Psi}_R^{(\ell,k)}$ to the polynomial $m_u^{(\ell',k')}(\mathcal{E}, U(X))$, from identity (4.12) we obtain:

$$\begin{aligned} \widetilde{\Psi}_R^{(\ell,k)}\Big(m_u^{(\ell',k')}\big(\mathcal{E}, U(X)\big)\Big) = \prod_{j=1}^{e_{\ell'}}\Big(&\sum_{m=m_\ell}^{R-1} U\big(\sigma_k^{(\ell)}(a_m^{(\ell)})\big)T^m + U(Y)T^R - \\ &- \sum_{m \geq m_\ell} U\big(\sigma_{k'}^{(\ell')}(a_m^{(\ell')})\big)\sigma_{k'}^{(\ell')}(\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^m \sigma_k^{(\ell)}(\lambda_\ell^{\frac{1}{e_\ell}})^m \xi_\ell^{jm} T^{\frac{me_\ell}{e_{\ell'}}}\Big). \end{aligned}$$

This identity shows that all the factors of $\widetilde{\Psi}_R^{(\ell,k)}\big(m_u^{(\ell',k')}\big(\mathcal{E}, U(X)\big)\big)$ have order at most R and the coefficient of the least nonzero power of T arising in the Laurent series $\widetilde{\Psi}_R^{(\ell,k)}\big(m_u^{(\ell',k')}\big(\mathcal{E}, U(X)\big)\big) \in \overline{\mathbb{Q}}[Y](\!(T)\!)$ is

– either of the form

$$\alpha U\left(Y - \sigma_{k'}^{(\ell')}(a_R^{(\ell')})\sigma_{k'}^{(\ell')}(\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^R \sigma_k^{(\ell)}(\lambda_\ell^{-\frac{1}{e_\ell}})^R\right)$$

with $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$, in case that $(\ell', k') \in \mathcal{L}_{\ell,k}$ holds,

– or a nonzero constant $\alpha \in \overline{\mathbb{Q}}$.

We deduce that the coefficients of the least nonzero power of T arising in the following elements of $\overline{\mathbb{Q}}[Y](\!(T)\!)$:

$$\widetilde{\Psi}_R^{(\ell,k)}\Big(\prod_{(\ell',k') \in \mathcal{L}_{\ell,k}} m_u^{(\ell',k')}\big(\mathcal{E}, U(X)\big)\Big), \quad \widetilde{\Psi}_R^{(\ell,k)}\Big(\prod_{(\ell',k') \notin \mathcal{L}_{\ell,k}} m_u^{(\ell',k')}\big(\mathcal{E}, U(X)\big)\Big),$$

are of the form $\alpha\prod_{b\in\widehat{W}^{(\ell,k)}}U(Y-b)\in\overline{\mathbb{Q}}[Y]$ with $\alpha\in\overline{\mathbb{Q}}\setminus\{0\}$, and a constant $\widetilde{\alpha}\in\overline{\mathbb{Q}}\setminus\{0\}$ respectively. We conclude that the following identity holds:

$$in\big(\Psi_R^{(\ell,k)}\big(m_u(\mathcal{E},U(X))\big)\big)=\alpha\prod_{b\in\widehat{W}^{(\ell,k)}}U(Y-b). \tag{4.14}$$

Since $m_u(\mathcal{E},U(X))\in\mathcal{I}(V)$, we conclude that there exists $\alpha\in\mathbb{Z}$ such that $T^\alpha\Psi_R^{(\ell,k)}\big(m_u(\mathcal{E},U(X))\big)\in\mathcal{I}^{(\ell,k)}$. Then $in\big(\Psi_R^{(\ell,k)}\big(m_u(\mathcal{E},U(X))\big)\big)\in in(\mathcal{I}^{(\ell,k)})$.

Now, let $U_1,\ldots,U_n$ be $\mathbb{Q}$–linearly independent generic linear forms. Repeating the previous arguments with $U_1,\ldots,U_n$, from identity (4.14) we conclude that $W^{(\ell,k)}$ is a zero–dimensional subvariety of $\mathbb{A}^n$. Furthermore, we have

$$\deg\widehat{W}^{(\ell,k)}\le\deg W^{(\ell,k)}\le\deg\big(\prod_{b\in\widehat{W}^{(\ell,k)}}U(Y-b)\big)=\#(\widehat{W}^{(\ell,k)}).$$

This shows that $\#(\widehat{W}^{(\ell,k)})=\#(W^{(\ell,k)})$. Therefore, taking into account the inclusion $\widehat{W}^{(\ell,k)}\subset W^{(\ell,k)}$, we have that $W^{(\ell,k)}=\widehat{W}^{(\ell,k)}$ holds. □

Now we exhibit a flatness condition which assures that any point of the fibre $(\pi^{(\ell,k)})^{-1}(0)$ is $(G_1^{(\ell,k)},\ldots,G_n^{(\ell,k)})$–smooth. For this purpose, we introduce the notion of standard basis (see [CLO98]). In our setting, a set $\{G_1,\ldots,G_s\}\subset\overline{\mathbb{Q}}[T,Y]:=\overline{\mathbb{Q}}[T,Y_1,\ldots,Y_n]$ is called a standard basis (of the ideal I they generate) if the ideal $(in(G_1),\ldots,in(G_s))$ generated by the initial forms of $G_1,\ldots,G_s$ in $\overline{\mathbb{Q}}[Y]$ agrees with the ideal $in(I):=(in(G):G\in I)$ generated by the initial forms of all the polynomials $G\in I$.

Theorem 4.5. *Let notations and assumptions be as above. Suppose further that $G_1^{(\ell,k)}(T,Y),\ldots,G_n^{(\ell,k)}(T,Y)$ form a standard basis of the ideal $\mathcal{I}^{(\ell,k)}$. Then the Jacobian determinant $J_{G^{(\ell,k)}}$ does not vanish at any point of $(\pi^{(\ell,k)})^{-1}(0)$.*

Proof. Since $G_1^{(\ell,k)},\ldots,G_n^{(\ell,k)}$ form a standard basis of $\mathcal{I}^{(\ell,k)}$ we see that

$$\begin{aligned}(\pi^{(\ell,k)})^{-1}(0)&=\{0\}\times V\big(G_1^{(\ell,k)}(0,Y),\ldots,G_n^{(\ell,k)}(0,Y)\big)=\\&=\{0\}\times V\big(in(G_1^{(\ell,k)}),\ldots,in(G_n^{(\ell,k)})\big)=\{0\}\times W^{(\ell,k)}\end{aligned}$$

holds. From Proposition 4.4 we see that for any $b\in W^{(\ell,k)}$ there exists a unique vector of power series $\varphi\in\overline{\mathbb{Q}}[\![T]\!]$ such that $\varphi(0)=b$ and $G_i^{(\ell,k)}(T,\varphi)=$

0 hold for $1 \leq i \leq n$. Then [ANMR91, Lemma 3] shows that $Y = b$ has multiplicity 1 as a zero of the ideal generated by $G_1^{(\ell,k)}(0,Y), \ldots, G_n^{(\ell,k)}(0,Y)$. Therefore, $J_{G^{(\ell,k)}}$ does not vanish at any point $(0,y) \in (\pi^{(\ell,k)})^{-1}(0)$. □

4.2.3. A global Newton–Hensel lifting

In the context of this chapter, the projection problem (see Section 2.4) can be stated as follows:

Lifting of a projection: given a set $\{(\widetilde{\mathcal{E}}^{(1)}, \widetilde{X}^{(1)}), \ldots, (\widetilde{\mathcal{E}}^{(g)}, \widetilde{X}^{(g)})\}$ *of parameterizations of* V *(i.e., by their singular parts), whose orbits under the action of the Galois group of* $\overline{\mathbb{Q}}/\mathbb{Q}$ *form a system of rational Puiseux expansions of the branches of the curve* V *lying above* 0*, and a generic linear form* $U \in \mathbb{Q}[X]$*, compute the projection polynomial* $m_u \in \mathbb{Q}(\mathcal{E})[Z]$*.*

Let us fix ℓ with $1 \leq \ell \leq g$ and let S_1, S_2 be indeterminates over $\mathbb{Q}$. Let $q^{(\ell)}$ be a monic irreducible polynomial of $\mathbb{Q}[S_1]$ of degree $f_\ell = [K^{(\ell)} : \mathbb{Q}]$ such that there exists a $\mathbb{Q}$–isomorphism of fields $\Upsilon_\ell : \mathbb{Q}[S_1]/(q^{(\ell)}(S_1)) \to K^{(\ell)}$. For any $m \geq m_\ell$ and $1 \leq j \leq n$, let $f^{(\ell)}, f_{m,j}^{(\ell)}$ be the (unique) polynomials of $\mathbb{Q}[S_1]$ of degree at most $f_\ell - 1$, such that $\Upsilon_\ell(f^{(\ell)}) := \lambda_\ell^{-1}$ and $\Upsilon_\ell(f_m^{(\ell)}) := a_{m,j}^{(\ell)}$. Finally, let $p^{(\ell)} \in \mathbb{Q}[S_1, S_2]$ be the polynomial $p^{(\ell)} := S_2^{e_\ell} - f^{(\ell)}(S_1)$, and let

$$W^{(\ell)} := \{(s_1, s_2) \in \mathbb{A}^2 : p^{(\ell)}(s_1, s_2) = 0, q^{(\ell)}(s_1) = 0\}. \tag{4.15}$$

It is easy to see that $W^{(\ell)}$ is a zero–dimensional variety of degree $\deg W^{(\ell)} = e_\ell f_\ell$. [Duv89] shows that the field $K^{(\ell)}$ is the field extension of $\mathbb{Q}$ generated by the coefficients $a_{j,m}^{(\ell)}$ for $1 \leq j \leq n$ and $m_\ell \leq m < R$. In particular, $K^{(\ell)}$ is the minimal field extension of $\mathbb{Q}$ containing the coefficients of the singular parts of the given set of rational Puiseux expansions.

For $\kappa \geq R$, let $u^{(\kappa,\ell)} := \sum_{m=m_\ell}^{\kappa} U(f_m^{(\ell)}(S_1))(S_2 T)^m \in \mathbb{Q}(S_1, S_2, T)$ and let $\chi_{u^{(\kappa,\ell)}} \in \mathbb{Q}(T)[Z]$ denote the characteristic polynomial of the projection $\pi_{u^{(\kappa,\ell)}}^{(\ell)} : \mathbb{A}^1 \times W^{(\ell)} \to \mathbb{A}^2$ defined by $\pi_{u^{(\kappa,\ell)}}^{(\ell)}(t, s_1, s_2) := (t, u^{(\kappa,\ell)}(t, s_1, s_2))$. We have

$$\chi_{u^{(\kappa,\ell)}} = \prod_{k=1}^{f_\ell} \prod_{j=1}^{e_\ell} \Big(Z - \sum_{m=m_\ell}^{\kappa} U\big(\sigma_k^{(\ell)}(a_m^{(\ell)})\big)\big(\xi_\ell^j \sigma_k^{(\ell)}(\lambda_\ell^{-\frac{1}{e_\ell}})T\big)^m \Big). \tag{4.16}$$

Observe that if the norm in the field extension $\mathbb{Q}(T^{e_\ell}) \to K^{(\ell)}(\sigma_k^{(\ell)}(\lambda_\ell^{-1/e_\ell})T)$

is extended to polynomials, then $\chi_{u^{(\kappa,\ell)}}$ is the norm of $Z-\sum_{m=m_\ell}^{\kappa} U(a_m^{(\ell)})\lambda_\ell^{-1/e_\ell}T^m$. This shows that $\chi_{u^{(\kappa,\ell)}}$ is an element of $\mathbb{Q}(T^{e_\ell})[Z]$.

Before continuing, we introduce the following terminology: for $G, \widetilde{G} \in \overline{\mathbb{Q}}(\!(\mathcal{E})\!)$ and any $s \in \mathbb{Z}$, we say that $\widetilde{G}$ *approximates* G *with precision* s in $\overline{\mathbb{Q}}(\!(\mathcal{E})\!)$ if the Laurent series $G-\widetilde{G}$ has order at least $s+1$ in $\mathcal{E}$. We shall use the notation $G \equiv \widetilde{G} \mod (\mathcal{E}^{s+1})$. Furthermore, if $G, \widetilde{G}$ are two elements of a polynomial ring $\overline{\mathbb{Q}}(\!(\mathcal{E})\!)[Z]$, we say that $\widetilde{G}$ approximates G with precision s if every coefficient $\widetilde{a} \in \overline{\mathbb{Q}}(\!(\mathcal{E})\!)$ of $\widetilde{G}$ approximates the corresponding coefficient $a \in \overline{\mathbb{Q}}(\!(\mathcal{E})\!)$ of G with precision s (in the sense of the previous definition).

From identities (4.12) and (4.16) we easily deduce that the congruence relation

$$m_u^{(\ell)}(T^{e_\ell}, Z) \equiv \chi_{u^{(\kappa,\ell)}}(T,Z) \mod (T^{\kappa-\delta_0 m_\ell e_\ell f_\ell+1}) \tag{4.17}$$

holds in $\mathbb{Q}(\!(T)\!)[Z]$, with $\delta_0 := -1$ for $m_\ell < 0$ and $\delta_0 := 0$ otherwise. Taking into account that $\chi_{u^{(\kappa,\ell)}}(T,Z)$ is an element of $\mathbb{Q}(T^{e_\ell})[Z]$, replacing T^{e_ℓ} by $\mathcal{E}$ in (4.17) we obtain the following result.

Lemma 4.6. *For any $\kappa \geq R$, $\chi_{u^{(\kappa,\ell)}}(\mathcal{E}^{1/e_\ell}, Z) \in \mathbb{Q}(\mathcal{E})[Z]$ approximates the polynomial $m_u^{(\ell)}(\mathcal{E}, Z) \in \mathbb{Q}(\!(\mathcal{E})\!)[Z]$ with precision $\lfloor \frac{\kappa-\delta_0 m_\ell e_\ell f_\ell}{e_\ell} \rfloor$ in $\mathbb{Q}(\!(\mathcal{E})\!)[Z]$.*

Now we state our version of the global Newton–Hensel lifting.

Theorem 4.7. *Let the assumptions of Theorem 4.5 hold. Let be given $\kappa \geq 0$. For $1 \leq j \leq n$, let $G_j^{(\ell)}$ be the following element of $\mathbb{Q}[S_1, S_2, S_2^{-1}, T, Y]$:*

$$G_j^{(\ell)}(S_1,S_2,T,Y) := T^{\alpha_{j\ell}} F_j\Big(T^{e_\ell}, \sum_{m=m_\ell}^{R-1} f_m^{(\ell)}(S_1)(S_2T)^m + YT^R\Big).$$

Let $N_{G^{(\ell)}}$ be the Newton–Hensel operator associated to $G_1^{(\ell)}, \ldots, G_n^{(\ell)}$, namely

$$N_{G^{(\ell)}}(Y) := \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} - \Big(\frac{\partial G_i^{(\ell)}}{\partial Y_j}\Big)_{1\leq i,j\leq n}^{-1} \cdot \begin{pmatrix} G_1^{(\ell)} \\ \vdots \\ G_n^{(\ell)} \end{pmatrix} \tag{4.18}$$

and let $N_{G^{(\ell)}}^{\kappa}$ denote the κ–th fold iteration of $N_{G^{(\ell)}}$. Finally, let

$$\widetilde{u}^{(\kappa,\ell)} := U\Big(\sum_{m=m_\ell}^{R-1} f_m^{(\ell)}(S_1)(S_2T)^m + N_{G^{(\ell)}}^{\kappa}\big(S_1, S_2, T, f_R^{(\ell)}(S_1)S_2^R\big)T^R\Big)$$

and let $\chi_{\widetilde{u}^{(\ell,k)}} \in \overline{\mathbb{Q}}(T)[Z]$ be its characteristic polynomial. Then $\chi_{\widetilde{u}^{(\ell,k)}}(\mathcal{E}^{\frac{1}{e_\ell}},Z)$ approximates the polynomial $m_u^{(\ell)}$ with precision $\lfloor \frac{R-1-\delta_0 m_\ell e_\ell f_\ell+2^\kappa}{e_\ell} \rfloor$ in $\mathbb{Q}(\!(\mathcal{E})\!)[Z]$.

Proof. Let (s_1, s_2) be a point of the variety $W^{(\ell)}$. Then there exists a (unique) pair (k, j) with $1 \leq k \leq f_\ell$ and $1 \leq j \leq e_\ell$, such that $f^{(\ell)}(s_1) = \sigma_k^{(\ell)}(\lambda_\ell^{-1})$, $s_2 = \xi_\ell^j \sigma_k^{(\ell)}(\lambda_\ell^{-1/e_\ell})$ and $f_m^{(\ell)}(s_1) = \sigma_k^{(\ell)}(a_m^{(\ell)})$ hold for $m_\ell \leq m \leq R$. This implies that the following identity holds in $\overline{\mathbb{Q}}[T, Y]$ for $1 \leq i \leq n$:

$$G_i^{(\ell)}(s_1, s_2, T, Y) = s_2^{\alpha_{j\ell}} G_i^{(\ell,k)}(s_2 T, s_2^{-R} Y). \tag{4.19}$$

Let us observe that $s_2^R \sigma_k^{(\ell)}(a_R^{(\ell)}) \in \mathbb{A}^n$ belongs to the affine variety defined by $G_1^{(\ell)}(s_1, s_2, 0, Y), \ldots, G_n^{(\ell)}(s_1, s_2, 0, Y)$. Furthermore, from Theorem 4.5 and identity (4.19) we conclude that $J_{G^{(\ell)}}(T, Y) := \det(\partial G_i^{(\ell)}/\partial Y_j)_{1 \leq i,j \leq n}(s_1, s_2, T, Y)$ does not vanish at $(0, s_2^R \sigma_k^{(\ell)}(a_R^{(\ell)})) \in \mathbb{A}^{n+1}$, and hence $J_{G^{(\ell)}}(T, s_2^R \sigma_k^{(\ell)}(a_R^{(\ell)}))$ is a unit in the local ring $(\overline{\mathbb{Q}}[\![T]\!], (T))$.

From Hensel's Lemma (see e.g. [Eis95]) in the version of [HKP$^+$00] we deduce that the following congruence relation holds in $\overline{\mathbb{Q}}[\![T]\!]^n$:

$$N_{G^{(\ell)}}^\kappa\big(s_1, s_2, T, \sigma_k^{(\ell)}(a_R^{(\ell)}) s_2^R\big) \;\equiv\; \sum_{m \geq R} \sigma_k^{(\ell)}(a_m^{(\ell)}) s_2^m T^{m-R} \bmod (T^{2^\kappa}).$$

Therefore, we obtain

$$\begin{aligned} U\Big(\sum_{m=m_\ell}^{R-1} f_m^{(\ell)}(s_1)(s_2 T)^m + N_{G^{(\ell)}}\big(s_1, s_2, T, \sigma_k^{(\ell)}(a_R^{(\ell)}) s_2^R\big) T^R\Big) &\equiv \\ \equiv\; U\Big(\sum_{m \geq m_\ell} \sigma_k^{(\ell)}(a_m^{(\ell)})(s_2 T)^m\Big) &\bmod (T^{R+2^\kappa}), \end{aligned}$$

which implies $\widetilde{u}^{(\kappa,\ell)}(s_1, s_2, T) \;\equiv\; u^{(R-1+2^\kappa,\,\ell)}(s_1, s_2, T) \bmod (T^{R+2^\kappa})$.

Lemma 4.6 shows that $\chi_{u^{(R-1+2^\kappa,\,\ell)}}(\mathcal{E}^{1/e_\ell}, Z)$ approximates $m_u^{(\ell)}$ in $\mathbb{Q}(\!(\mathcal{E})\!)[Z]$ with precision $\lfloor \frac{R-1-\delta_0 m_\ell e_\ell f_\ell+2^\kappa}{e_\ell} \rfloor$. Therefore, $\chi_{\widetilde{u}^{(\kappa,\,\ell)}}(\mathcal{E}^{1/e_\ell}, Z)$ also approximates $m_u^{(\ell)}$ in $\mathbb{Q}(\!(\mathcal{E})\!)[Z]$ with precision $\lfloor \frac{R-1-\delta_0 m_\ell e_\ell f_\ell+2^\kappa}{e_\ell} \rfloor$. This proves the theorem. □

4.2.4. Unramifiedness and flatness conditions

All the hypotheses of Theorems 4.5 and 4.7 are fairly "geometric" in nature, and hence reasonable assumptions from our point of view (compare

[HKP$^+$00]), except perhaps for the standard basis requirement. Nevertheless, this is not an arbitrary "algebraic" requirement, as shown by the following result.

Lemma 4.8. *Let notations and assumptions be as in Lemmas 4.1, 4.2 and 4.3. Suppose that the morphism $\pi^{(\ell,k)}$ is unramified at $T=0$. Then $G_1^{(\ell,k)},\dots,$ $G_n^{(\ell,k)}$ form a standard basis of the ideal $\mathcal{I}^{(\ell,k)}$.*

Proof. Let $x\in\mathbb{A}^{n+1}$ be a point of the fibre $(\pi^{(\ell,k)})^{-1}(0)$. Let $(\mathcal{O}_{V^{(\ell,k)},x},\mathfrak{m}_x)$ denote the local ring of the point x on the variety $V^{(\ell,k)}$ and let $(\mathcal{O}_{\mathbb{A}^1,0},\mathfrak{m}_0)$ denote the local ring of 0 on $\mathbb{A}^1$. Since $\pi^{(\ell,k)}$ is unramified at $T=0$, we have

$$\mathfrak{m}_x=(\pi^{(\ell,k)})^*(\mathfrak{m}_0) \tag{4.20}$$

for any $x\in(\pi^{(\ell,k)})^{-1}(0)$, where $(\pi^{(\ell,k)})^*$ denotes the local homomorphism $(\pi^{(\ell,k)})^*:\mathcal{O}_{\mathbb{A}^1,0}\to\mathcal{O}_{V^{(\ell,k)},x}$ induced by the morphism $\pi^{(\ell,k)}$.

Identity (4.20) implies that the morphism $d_x\pi^{(\ell,k)}:T_{V^{(\ell,k)},x}\to T_{\mathbb{A}^1,0}$ of tangent spaces is injective [Dan94]. We deduce that the dimension $\dim(T_{V^{(\ell,k)},x})$ of the tangent space $T_{V^{(\ell,k)},x}$ of $V^{(\ell,k)}$ at x is at most 1. Taking into account that $V^{(\ell,k)}$ is an equidimensional variety of dimension 1 (Lemma 4.2), we conclude that $\dim(T_{V^{(\ell,k)},x})=1$. Therefore, x is a smooth point of $V^{(\ell,k)}$.

Identity (4.20) shows that the quotient ring $\mathcal{O}_{V^{(\ell,k)},x}/(\pi^{(\ell,k)})^*(\mathfrak{m}_0)$ is a zero–dimensional $\overline{\mathbb{Q}}$–algebra. Let us observe that $\mathcal{O}_{V^{(\ell,k)},x}$ is a Cohen–Macaulay ring (because it is a localization of a Cohen–Macaulay ring), the local ring $\mathcal{O}_{\mathbb{A}^1,0}$ is a regular ring and the identity

$$\dim\mathcal{O}_{V^{(\ell,k)},x}=\dim\mathcal{O}_{\mathbb{A}^1,0}+\dim\mathcal{O}_{V^{(\ell,k)},x}/(\pi^{(\ell,k)})^*(\mathfrak{m}_0)$$

holds. Then applying [Mat86, Theorem 23.1] we conclude that the local homomorphism

$$(\pi^{(\ell,k)})^*:\mathcal{O}_{\mathbb{A}^1,0}\to\mathcal{O}_{V^{(\ell,k)},x} \tag{4.21}$$

induced by $\pi^{(\ell,k)}$ is flat.

We observe that the localization $\overline{\mathbb{Q}}[V^{(\ell,k)}]_{\mathfrak{m}_0}$ is a semilocal ring, whose maximal ideals correspond to the maximal ideals $\mathfrak{m}_x$ induced by the points x of $(\pi^{(\ell,k)})^{-1}(0)$. Therefore, since the morphism of (4.21) is flat for any point $x\in$ of $(\pi^{(\ell,k)})^{-1}(0)$, applying [Mat86, Theorem 7.1] we conclude that

$$(\pi^{(\ell,k)})^*:\overline{\mathbb{Q}}[\mathbb{A}^1]_{\mathfrak{m}_0}\to\overline{\mathbb{Q}}[V^{(\ell,k)}]_{\mathfrak{m}_0}$$

induced by $\pi^{(\ell,k)}$ is flat, i.e. $\pi^{(\ell,k)}$ is flat at $T=0$. Therefore, from [Art76, Part I, Proposition 3.1] (see also [BM93]) it follows that any syzygy $(h_1,\ldots,h_n)\in\overline{\mathbb{Q}}[Y]^n$ of the polynomials $G_1^{(\ell,k)}(0,Y),\ldots,G_n^{(\ell,k)}(0,Y)$ "lifts" to a syzygy $(H_1,\ldots,H_n)\in\overline{\mathbb{Q}}[T,Y]^n$ of $G_1^{(\ell,k)},\ldots,G_n^{(\ell,k)}$, i.e. for $1\le i\le n$ the identity $H_i(0,Y)=h_i(Y)$ holds.

Now we adapt the contents of e.g. [MPT92] to our setting. For $F\in\overline{\mathbb{Q}}[T,Y]$, let $o_T(F)$ denote the highest power of T dividing F. We claim that any polynomial $G\in\mathcal{I}^{(\ell,k)}$ has a representation

$$G=\sum_{i=1}^n H_iG_i^{(\ell,k)} \tag{4.22}$$

with order $o_T(H_i)\ge o_T(G)$ for $1\le i\le n$. Let $G\in\mathcal{I}^{(\ell,k)}$ be a polynomial with a representation $G=\sum_{i=1}^n H_iG_i^{(\ell,k)}$. Let $\alpha:=\min\{o_T(H_i):1\le i\le n\}$, and suppose that $\alpha<o_T(G)$ holds. Let $\mathcal{J}$ be the set of indices i for which $\alpha=o_T(H_i)$ holds. Then the identity

$$\sum_{i\in\mathcal{J}}(T^{-\alpha}H_i)(0,Y)G_i^{(\ell,k)}(0,Y)=0$$

shows that $(h_1,\ldots,h_n)\in\overline{\mathbb{Q}}[Y]^n$, with $h_i:=(T^{-\alpha}H_i)(0,Y)$ if $i\in\mathcal{J}$ and $h_i:=0$ otherwise, is a syzygy of $G_1^{(\ell,k)}(0,Y),\ldots,G_n^{(\ell,k)}(0,Y)$. Then there exists a lifting $(\widetilde{H}_1,\ldots,\widetilde{H}_n)\in\overline{\mathbb{Q}}[T,Y]^n$ of the syzygy $(h_1,\ldots,h_n)$, and we have:

$$G=\sum_{i=1}^n(H_i-T^\alpha\widetilde{H}_i)G_i^{(\ell,k)},$$

with $o_T(H_i-T^\alpha\widetilde{H}_i)>\alpha$ for $1\le i\le n$. Repeating this argument at most $o_T(G)$ times, we conclude the validity of our claim.

Finally, let $G\in\mathcal{I}^{(\ell,k)}$. Then we have a representation of G as in (4.22), with order $o_T(H_i)\ge o_T(G)$ for $1\le i\le n$. Let $\mathcal{J}$ be the (nonempty) set of indices i for which $o_T(G)=o_T(H_i)$ holds. Then we have

$$\begin{aligned} in(G)=\big(T^{-o_T(G)}G\big)(0,Y) &= \sum_{i\in\mathcal{J}}\big(T^{-o_T(G)}H_i\big)(0,Y)\cdot G_i^{(\ell,k)}(0,Y)\\ &= \sum_{i\in\mathcal{J}}\big(T^{-o_T(G)}H_i\big)(0,Y)\cdot in(G_i^{(\ell,k)}). \end{aligned}$$

This shows that $G_1^{(\ell,k)},\ldots,G_n^{(\ell,k)}$ form a standard basis of the ideal $\mathcal{I}^{(\ell,k)}$. □

4.3. Algorithms and complexity estimates

Let notations and assumptions be as in Section 4.1. Let $\delta := \deg V$ denote the degree of the variety V, and let $D := \deg \pi$ denote the degree of the morphism $\pi : V \to \mathbb{A}^1$. Suppose that we are given a straight–line program β computing $F_1, \ldots, F_n$ with $\mathcal{T}$ arithmetic operations in $\mathbb{Q}$.

Let S_1, S_2 be indeterminates over $\mathbb{Q}$. With the notations of Section 4.2.3, for $1 \leq \ell \leq g$ and $m_\ell \leq m \leq R$, let $q^{(\ell)}, f^{(\ell)}, f^{(\ell)}_{m,1}, \ldots, f^{(\ell)}_{m,n} \in \mathbb{Q}[S_1]$ and $p^{(\ell)} \in \mathbb{Q}[S_1, S_2]$ be polynomials defining the system of rational Puiseux expansions of the branches of V lying above 0 of Section 4.2.3. In particular, we have the estimates $\deg(q^{(\ell)}) = f_\ell$, $\deg(f^{(\ell)}) < f_\ell$ and $\deg(f^{(\ell)}_{m,i}) < f_\ell$ for $1 \leq i \leq n$, and the singular parts of the (classical) Puiseux expansions of the branches of V lying over 0 are given by

$$\bigcup_{\ell=1}^{g} \Big\{ \big(T^{e_\ell}, \sum_{m=m_\ell}^{R} f^{(\ell)}_m(s_1) s_2^m T^m\big); p^{(\ell)}(s_1, s_2) = q^{(\ell)}(s_1) = 0 \Big\}, \tag{4.23}$$

where $f^{(\ell)}_m := (f^{(\ell)}_{m,1}, \ldots, f^{(\ell)}_{m,n}) \in \mathbb{Q}[S_1]^n$. Let $U \in \mathbb{Q}[X]$ a generic linear form, i.e. a linear form whose projection polynomial $m_u \in \mathbb{Q}(\mathcal{E})[Z]$ satisfies $\deg_Z m_u = D$. Then identity (4.12) of Section 4.2 shows that m_u has the following factorization into irreducible factors in $\mathbb{Q}((\mathcal{E}))[Z]$:

$$m_u = \prod_{\ell=1}^{g} m_u^{(\ell)} := \prod_{\ell=1}^{g} \Big(\prod_{k=1}^{f_\ell} \prod_{j=1}^{e_\ell} \Big(Z - \sum_{m \geq m_\ell} U\big(\sigma_k^{(\ell)}(a_m^{(\ell)})\big) \sigma_k^{(\ell)}(\lambda_\ell^{-\frac{1}{e_\ell}})^m \xi_\ell^{jm} \mathcal{E}^{\frac{m}{e_\ell}} \Big)\Big). \tag{4.24}$$

In this section we exhibit an algorithm which has as input the straight–line program β and the dense representation of $p^{(\ell)}, q^{(\ell)}, f^{(\ell)}, f^{(\ell)}_{m,1}, \ldots, f^{(\ell)}_{m,n}$ for $1 \leq \ell \leq g$ and $m_\ell \leq m \leq R$ and computes a geometric solution of V.

Let us fix ℓ with $1 \leq \ell \leq g$. The critical part of our algorithm is a procedure which computes a suitable approximation $\hat{m}_u^{(\ell)} \in \mathbb{Q}(\mathcal{E})[Z]$ of the polynomial $m_u^{(\ell)} \in \mathbb{Q}((\mathcal{E}))[Z]$. This procedure applies our variant of the global Newton–Hensel lifting based on Theorem 4.7. For this purpose, we shall deal with the variety $W^{(\ell)}$ of (4.15), namely

$$W^{(\ell)} := \{(s_1, s_2) \in \mathbb{A}^2 : q^{(\ell)}(s_1) = 0, p^{(\ell)}(s_1, s_2) = 0\}.$$

From the fact that $\deg W^{(\ell)} = e_\ell f_\ell$ holds, we easily conclude that S_2 is a primitive element of the $\mathbb{Q}$–algebra extension $\mathbb{Q} \hookrightarrow \mathbb{Q}[W^{(\ell)}]$. Therefore, we have a geometric solution of $W^{(\ell)}$ of the form

$$W^{(\ell)} = \{(s_1, s_2) \in \mathbb{A}^2 : m_{S_2}^{(\ell)}(s_2) = 0, s_1 \frac{\partial m_{S_2}^{(\ell)}}{\partial Z}(s_2) - v^{(\ell)}(s_2) = 0\}, \qquad (4.25)$$

where $m_{S_2}^{(\ell)} \in \mathbb{Q}[Z]$ is the minimal polynomial of S_2 in the extension $\mathbb{Q} \hookrightarrow \mathbb{Q}[W^{(\ell)}]$ and $v^{(\ell)} \in \mathbb{Q}[Z]$ satisfies $\deg v^{(\ell)} < \deg W^{(\ell)}$.

Lemma 4.9. *There exists an algorithm that computes the geometric solution (4.25) of $W^{(\ell)}$ in $O(\max\{e_\ell, f_\ell\}\mathsf{M}(e_\ell f_\ell))$ arithmetic operations in $\mathbb{Q}$.*

Proof. Let us suppose first $f_\ell = 1$. Then we may assume without loss of generality $q^{(\ell)} = S_1$. Furthermore, we have $f^{(\ell)} \in \mathbb{Q}\setminus\{0\}$ and $p^{(\ell)} = S_2^{e_\ell} - f^{(\ell)}$. Therefore, $m_{S_2}^{(\ell)} = p^{(\ell)} = Z^{e_\ell} - f^{(\ell)}$ and $v^{(\ell)} = 0$ yield in fact the geometric solution of $W^{(\ell)}$ we are looking for (and we have nothing to compute).

Now suppose that $f_\ell > 1$ holds. Let us introduce a new indeterminate Λ, and let us consider the linear form $\mathcal{L} := \Lambda S_1 + S_2 \in \mathbb{Q}[\Lambda][S_1, S_2]$. It is easy to see that $\mathcal{L}$ is a primitive element of the integral ring extension $\mathbb{Q}[\Lambda] \hookrightarrow \mathbb{Q}[\Lambda] \otimes \mathbb{Q}[W^{(\ell)}]$, with minimal equation

$$m_{\mathcal{L}}^{(\ell)}(Z) \;=\; Res_{S_1}\big(q^{(\ell)}(S_1), p^{(\ell)}(S_1, Z - \Lambda S_1)\big), \qquad (4.26)$$

where $Res_{S_1}(f, g)$ denotes the resultant of f and g with respect to S_1. Arguing as in (2.10), we have a congruence relation:

$$m_{\mathcal{L}}^{(\ell)}(Z) = m_{S_2}^{(\ell)}(Z) + \Lambda \left(S_1 \frac{\partial m_{S_2}^{(\ell)}}{\partial Z}(Z) + \widetilde{v}^{(\ell)}(Z) \right) \mod (\Lambda^2),$$

with $\widetilde{v}^{(\ell)} \in \mathbb{Q}[Z]$, $\deg \widetilde{v}^{(\ell)} < e_\ell f_\ell$ and $S_1(\partial m_{S_2}^{(\ell)}/\partial Z)(S_2) + \widetilde{v}^{(\ell)}(S_2) \in I(W^{(\ell)})$. Then $m_{S_2}^{(\ell)}$ and $v^{(\ell)} := -\widetilde{v}^{(\ell)}$ can be obtained from the resultant of the right–hand side of identity (4.26) modulo Λ^2. Using interpolation in the variable Z, this computation can be performed with $O(\max\{e_\ell, f_\ell\}\mathsf{M}(e_\ell f_\ell))$ arithmetic operations in $\mathbb{Q}$. □

Our variant of the global Newton–Hensel lifting requires the R–th "initial approximation" of $m_u^{(\ell)}$ given by the following expression (compare with

(4.24)):

$$\widetilde{m}_u^{(\ell)}(T^{e_\ell}, Z) := \prod_{k=1}^{f_\ell}\prod_{j=1}^{e_\ell}\Big(Z - \sum_{m=m_\ell}^{R} U\big(\sigma_k^{(\ell)}(a_m^{(\ell)})\big)\sigma_k^{(\ell)}(\lambda_\ell^{-\frac{1}{e_\ell}})^m \xi_\ell^{jm} T^m\Big). \quad (4.27)$$

Lemma 4.10. *There exists a computation tree which takes as input the polynomials $p^{(\ell)}, q^{(\ell)}, f^{(\ell)}, f_{m,i}^{(\ell)}$ $(1 \le i \le n, m_\ell \le m \le R), m_{S_2}^{(\ell)}, v^{(\ell)}$, which define the ℓ–th expansion of the given system of rational Puiseux expansions of V and form the geometric solution (4.25) of $W^{(\ell)}$, and computes the dense representation of $\widetilde{m}_u^{(\ell)}$ in $O(R_\ell e_\ell f_\ell \mathsf{M}(e_\ell f_\ell))$ arithmetic operations in $\mathbb{Q}$, where $R_\ell := (R - m_\ell)e_\ell f_\ell + 1$.*

Proof. From the definition of $\widetilde{m}_u^{(\ell)}$ and the variety $W^{(\ell)}$ we easily see that $T^{-m_\ell e_\ell f_\ell}\widetilde{m}_u^{(\ell)}(T^{e_\ell}, T^{m_\ell}Z)$ equals the characteristic polynomial $\chi_{\widetilde{u}}$ of the polynomial $\widetilde{u}(T, S_1, S_2) := \sum_{m=m_\ell}^{R} U(\, f_m^{(\ell)}(S_1)\,)\, S_2^m\, T^{m-m_\ell}$ in the $\mathbb{Q}$–algebra $\mathbb{Q}[T] \otimes \mathbb{Q}[W^{(\ell)}] \cong \mathbb{Q}[\mathbb{A}^1 \times W^{(\ell)}]$. Let us observe that S_2 is a primitive element of the extension $\mathbb{Q}[T] \hookrightarrow \mathbb{Q}[\mathbb{A}^1 \times W^{(\ell)}]$ and the input polynomials $m_{S_2}^{(\ell)}, v^{(\ell)}$ also yield a geometric solution of the variety $\mathbb{A}^1 \times W^{(\ell)}$.

In order to compute the dense representation of $\chi_{\widetilde{u}}$ we use a straightforward adaptation of the algorithm of [HMW01, Lemma 3]. Let $M \in \mathbb{Q}^{(e_\ell f_\ell)\times(e_\ell f_\ell)}$ be the companion matrix of the polynomial $m_{S_2}^{(\ell)}$. Then the characteristic polynomial of the matrix $N := \widetilde{u}(T, v^{(\ell)}(M), M)$ equals the characteristic polynomial $\chi_{\widetilde{u}}$.

Let us suppose first that $R = m_\ell$ holds. Then $\chi_{\widetilde{u}}$ is a pseudo–homogeneous polynomial whose coefficients can be computed using [HMW01, Lemma 3] with $O(e_\ell f_\ell \mathsf{M}(e_\ell f_\ell))$ arithmetic operations in $\mathbb{Q}$. On the other hand, if $R \ne m_\ell$, taking into account that the algorithm manipulates polynomials in T of degree at most $(R - m_\ell)e_\ell f_\ell$, and the fact that the polynomial $m_{S_2}^{(\ell)}(Z)$ does not depend on the variable T, we conclude that the procedure underlying [HMW01, Lemma 3] can be executed with $O((R - m_\ell)e_\ell^2 f_\ell^2 \mathsf{M}(e_\ell f_\ell))$ arithmetic operations in $\mathbb{Q}$. In conclusion, we see that the procedure takes in both cases $O(((R - m_\ell)e_\ell f_\ell + 1)\mathsf{M}(e_\ell f_\ell))$ arithmetic operations in $\mathbb{Q}$. Finally, taking into account that the dense representation of $\widetilde{m}_u^{(\ell)}$ can be immediately obtained from that of $\chi_{\widetilde{u}}$ finishes the proof of the lemma. □

Now we can describe the algorithm computing an arbitrary approximation in $\mathbb{Q}(\mathcal{E})[Z]$ of the polynomial $m_u^{(\ell)} \in \mathbb{Q}(\!(\mathcal{E})\!)[Z]$. This algorithm applies our variant of the global Newton–Hensel lifting (Theorem 4.7), combined with an adaptation of the procedure of [GLS01, Proposition 7]. For this purpose, following Theorem 4.7, let $Y_1, \ldots, Y_n$ be indeterminates over $\mathbb{Q}$, let $Y := (Y_1, \ldots, Y_n)$, and let us define $G_1^{(\ell)}, \ldots, G_n^{(\ell)} \in \mathbb{Q}[S_1, S_2^{-1}, S_2, T, Y]$ by:

$$G_j^{(\ell)} := T^{\alpha_{j\ell}} F_j \left(T^{e_\ell}, \sum_{m=m_\ell}^{R-1} f_m^{(\ell)}(S_1)(S_2T)^m + YT^R \right). \tag{4.28}$$

Proposition 4.11. *Let us fix $\kappa > 0$. Then there exists a computation tree which takes as input the polynomials $p^{(\ell)}, q^{(\ell)}, f^{(\ell)}, f_{m,i}^{(\ell)}$ $(1 \le i \le n, m_\ell \le m \le R), m_{S_2}^{(\ell)}, v^{(\ell)}$, which define the ℓ–th parameterization of the given system of rational Puiseux expansions of V and form the geometric solution (4.25) of $W^{(\ell)}$, and computes an approximation $\hat{m}_u^{(\ell)} \in \mathbb{Q}(\mathcal{E})[Z]$ of $m_u^{(\ell)}$ in $\mathbb{Q}(\!(\mathcal{E})\!)[Z]$ with precision $\lceil \frac{R+\kappa}{e_\ell} \rceil + 1$ and parameterizations of $Y_1, \ldots, Y_n$ in terms of the linear form U up to order $\lceil \frac{R+\kappa}{e_\ell} \rceil + 1$, in*

$$O\big(n(\mathcal{T}_\ell + n^4)\mathsf{M}(\kappa + \delta_0 m_\ell e_\ell f_\ell + (R_\ell - 1)e_\ell f_\ell)\mathsf{M}(e_\ell f_\ell)\big)$$

arithmetic operations in $\mathbb{Q}$, where $R_\ell := (R - m_\ell)e_\ell f_\ell + 1$, $\delta_0 := -1$ for $m_\ell < 0$ and $\delta_0 := 0$ otherwise, and $\mathcal{T}_\ell$ denotes arithmetic operations in $\mathbb{Q}$ required for the evaluation of the polynomials $G_1^{(\ell)}, \ldots, G_n^{(\ell)}$.

Proof. Theorem 4.5 shows that the Newton operator $N_{G^{(\ell)}}$ of (4.18) is well defined at $f_R^{(\ell)}(s_1)s_2^R$ for any $(s_1, s_2) \in W^{(\ell)}$. Then Theorem 4.7 shows that from the $\tau := \lceil \log_2(\kappa + \delta_0 m_\ell e_\ell f_\ell + 1) \rceil$–fold iteration of the Newton operator $N_{G^{(\ell)}}$ we obtain a rational function $\hat{m}_u \in \mathbb{Q}(\mathcal{E})[Z]$ which approximates $m_u^{(\ell)}$ in $\mathbb{Q}(\!(\mathcal{E})\!)$ with precision $\lfloor \frac{R+\kappa}{e_\ell} \rfloor$.

In order to compute $\hat{m}_u(T^{e_\ell}, Z)$ we use an adaptation of the procedure of [GLS01, Proposition 7]: we start with the initial approximation provided by the polynomial $\widetilde{m}_u^{(\ell)}$ of (4.27) and parameterizations of $X_1, \ldots, X_n$ in terms of the linear form U up to order $R+1$, i.e. elements $\widetilde{v}_1^{(\ell)}, \ldots, \widetilde{v}_n^{(\ell)}$ of $\mathbb{Q}(\mathcal{E})[Z]$ such that $\frac{\partial \widetilde{m}_u^{(\ell)}}{\partial Z}(T^{e_\ell}, U)X_i \equiv \widetilde{v}_i^{(\ell)}(T^{e_\ell}, U) \bmod (T^{R+1}, m_u^{(\ell)}(T^{e_\ell}, U))$. Then we perform τ steps of the global Newton–Hensel lifting of [GLS01, Proposition 7] applied to the polynomials $G_1^{(\ell)}, \ldots, G_n^{(\ell)}$.

Applying Lemma 4.10 we can compute the polynomial $\widetilde{m}_u^{(\ell)}$ of (4.27) in $O(R_\ell e_\ell f_\ell \mathsf{M}(e_\ell f_\ell))$ arithmetic operations in $\mathbb{Q}$. Combining Lemma 4.10

and the formulae of e.g. [ABRW96], [Rou97] or [GLS01] as in the proof of Lemma 4.9 we obtain the parameterizations of $X_1, \ldots, X_n$ in terms of U up to order $R+1$ using $O(nR_\ell e_\ell f_\ell \mathsf{M}(e_\ell f_\ell))$ arithmetic operations in $\mathbb{Q}$.

Now, applying [GLS01, Lemma 2] we obtain an approximation of $m_u^{(\ell)}$ with precision $R+\kappa+1$ in $\mathbb{Q}((T))[Z]$ and parameterizations of $X_1, \ldots, X_n$ in terms of U up to order $R+\kappa+1$ with time

$$O\big(n(\mathcal{T}_\ell + n^4)\mathsf{M}(\kappa + \delta_0 m_\ell e_\ell f_\ell + (R_\ell - 1)e_\ell f_\ell)\mathsf{M}(e_\ell f_\ell)\big).$$

Since $m_u^{(\ell)}(T^{e_\ell}, Z)$ and the parameterizations of $X_1, \ldots, X_n$ in terms of U are elements of $\mathbb{Q}((T^{e_\ell}))[Z]$, replacing T^{e_ℓ} by $\mathcal{E}$ we obtain $\hat{m}_u^{(\ell)}$ and the parameterizations of $X_1, \ldots, X_n$ in terms of U up to order $\lfloor \frac{R+\kappa}{e_\ell} \rfloor + 1$. Adding the complexity of each step of our procedure the proposition follows. □

Now we state the main result of this section.

Theorem 4.12. *There exists an algorithm in $\mathbb{Q}[\mathcal{E}, X]$ which takes as input the straight–line program β defining the polynomials $F_1, \ldots, F_n$ and the given system of rational Puiseux expansions and computes a geometric solution of V in*

$$O\left(\sum_{\ell=1}^{g} n e_\ell (\mathcal{T}_\ell + n^4)(\delta + \delta_0 m_\ell f_\ell + R_\ell)\mathsf{M}(e_\ell f_\ell)\right)$$

arithmetic operations in $\mathbb{Q}$, where $R_\ell := (R - m_\ell)e_\ell f_\ell + 1$, $\delta_0 := -1$ for $m_\ell < 0$ and $\delta_0 := 0$ otherwise, and $\mathcal{T}_\ell$ denotes the number of arithmetic operations in $\mathbb{Q}$ required for the evaluation of the polynomials $G_1^{(\ell)}, \ldots, G_n^{(\ell)}$ of (4.28). Furthermore, for any $\rho \geq 2$, such a computation tree can be randomly constructed with a probability of success of at least $1 - \frac{1}{2\rho} \geq \frac{3}{4}$.

Proof. Let $U \in \mathbb{Q}[X]$ be a generic linear form. Let us fix $\rho \geq 2$. Using the Zippel–Schwartz Theorem (Theorem 2.1), we conclude that the coefficients of U can be randomly chosen in the set $\{1, \ldots, 4\rho n D^2\}$ with a probability of success of at least $1 - \frac{1}{2\rho} \geq \frac{3}{4}$, where $D := \deg \pi$.

Let $\delta := \deg V$. Applying Proposition 4.11 for $1 \leq \ell \leq g$ with $\kappa := 3e_\ell\delta - R$, we obtain elements $\hat{m}_u^{(\ell)}, \hat{v}_1^{(\ell)}, \ldots, \hat{v}_n^{(\ell)}$ $(1 \leq \ell \leq g)$ of $\mathbb{Q}(\mathcal{E})[Z]$ such that:

1. $\hat{m}_u^{(\ell)}(\mathcal{E}, Z) \equiv m_u^{(\ell)}(\mathcal{E}, Z)$ modulo $(\mathcal{E}^{3\delta+1})$,

2. $\frac{\partial \hat{m}_u^{(\ell)}}{\partial Z}(\mathcal{E},U)X_i \equiv \hat{v}_i^{(\ell)}(\mathcal{E},U)$ modulo $\big(\mathcal{E}^{3\delta+1}, m_u^{(\ell)}(\mathcal{E},U)\big)$,

3. $\deg_Z \hat{m}_u^{(\ell)} \leq e_\ell f_\ell$ and $\deg_Z v_i^{(\ell)} \leq e_\ell f_\ell - 1$ for $1 \leq i \leq n$.

These polynomials can be computed with

$$O\left(\sum_{\ell=1}^{g} n(\mathcal{T}_\ell + n^4)\mathsf{M}(e_\ell\delta + \delta_0 m_\ell e_\ell f_\ell + (R_\ell - 1)e_\ell f_\ell)\mathsf{M}(e_\ell f_\ell)\right)$$

arithmetic operations in $\mathbb{Q}$. Let $v_1, \ldots, v_n$ be the elements of $\mathbb{Q}(\mathcal{E})[Z]$ parameterizing $X_1, \ldots, X_n$ in terms of the linear form U in V, i.e. satisfying $\frac{\partial m_u}{\partial Z}(\mathcal{E},U)X_i \equiv v_i(\mathcal{E},U)$ mod $I(V)$ for $1 \leq i \leq n$. From [Sch03, Proposition 1] we see that the orders $o_{\mathcal{E}}(m_u), o_{\mathcal{E}}(v_1), \ldots, o_{\mathcal{E}}(v_n)$ are bounded from below by $-\delta$. Combining this observation with properties (1), (2), (3) we conclude that the following congruence relations hold in $\mathbb{Q}(\!(\mathcal{E})\!)[Z]$:

$$\begin{array}{rcll} \breve{m}_u := \prod_{\ell=1}^{g} \hat{m}_u^{(\ell)} & \equiv & m_u & \text{mod } (\mathcal{E}^{2\delta+1}), \\ \breve{v}_i := \sum_{1\leq \ell \leq g} \left(\prod_{\ell' \neq \ell} \hat{m}_u^{(\ell')}\right) \hat{v}_i^{(\ell)} & \equiv & v_i & \text{mod } (\mathcal{E}^{2\delta+1}). \end{array}$$

Using fast procedures for multiplication and Chinese Remainder Theorem (see e.g. [BP94]), we compute the polynomials $\breve{m}_u, \breve{v}_1, \ldots, \breve{v}_n$ using $O(n\mathsf{M}(\delta D))$ arithmetic operations in $\mathbb{Q}$.

Taking into account the estimates

$$\begin{array}{rclrcl} \deg_Z m_u & = & D, & \deg_Z v_i & \leq & D-1, \ (1 \leq i \leq n), \\ \deg_{\mathcal{E}} m_u & \leq & \delta, & \deg_{\mathcal{E}} v_i & \leq & \delta \ (1 \leq i \leq n), \end{array}$$

(see [Sch03]), we conclude that $m_u, v_1, \ldots, v_n$ can be computed from the truncated Laurent series $\breve{m}_u, \breve{v}_1, \ldots, \breve{v}_n$ using Padé approximants. More precisely, by interpolation in the variable Z we reduce the computation of the polynomials $m_u, v_1, \ldots, v_n$ to at most $(n+1)D$ problems of Padé approximation of degree at most δ. Thus, using a fast algorithm for computing Padé approximations (see e.g. [BP94]), we conclude that the polynomials $m_u, v_1, \ldots, v_n$ can be computed in $O(n\mathsf{M}(\delta D))$ arithmetic operations in $\mathbb{Q}$. Adding the number of arithmetic operations used in each step of our procedure we deduce the complexity estimate of the statement of Theorem 4.12. □

Let us make here a few remarks concerning the hypotheses and complexity estimates of Theorem 4.12. First we observe that the parameter T_ℓ can be roughly estimated by $O(\mathcal{T}+nR_\ell)$, where $\mathcal{T}$ is the number of arithmetic operations in $\mathbb{Q}$ that the straight–line program requires for computing $F_1,\ldots,F_n$. Then we have the rough worst–case estimate of $O(n^4\mathcal{T}\delta D^4)$ arithmetic operations in $\mathbb{Q}$ for the procedure underlying Theorem 4.12. Nevertheless, these estimates can be improved in several important cases, such as that where $R = m_\ell$ and $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})} \hookrightarrow \mathbb{Q}[V]_{(\mathcal{E})}$ is an integral extension: In this case we have the rough estimate $O((\mathcal{T}+n^4)n\delta De)$ arithmetic operations in $\mathbb{Q}$, with $e := \max\{e_\ell : 1 \leq \ell \leq g\}$ (see Subsections 4.4.3 and 4.4.4).

Theorem 4.12 generalizes the results of [HKP$^+$00] and [Sch03] in the unidimensional case. More precisely, in case that the "known" π–fibre is unramified, the corresponding (rough) estimate is of $O((n^4+\mathcal{T})D\delta)$ arithmetic operations in $\mathbb{Q}$, which improve the estimates of [HKP$^+$00] and have the same asymptotic behaviour as those of [Sch03].

The algorithm underlying Theorem 4.12 proceeds by computing a suitable approximation of the factors $m_u^{(\ell)}$ of the minimal polynomial $m_u = \prod_{1\leq\ell\leq g} m_u^{(\ell)}$ of the linear form U. Observe that for $1 \leq \ell \leq g$ the polynomial $m_u^{(\ell)}$ is an irreducible polynomial of $\mathbb{Q}((\mathcal{E}))[Z]$ (see Section 4.2). In this sense, this algorithm constitutes an improvement of the refinements described in Section 3 of [HKP$^+$00] (based on the factorization of the polynomial m_u in $\mathbb{Q}[\mathcal{E}, Z]$).

The singular parts (4.23) can be efficiently computed from the input polynomials $F_1,\ldots,F_n$ and a geometric solution of an *unramified* fibre of the morphism π, by a suitable combination of the following algorithmic tools.

- A Newton polygon algorithm for computing the singular parts of a system of rational Puiseux expansions as in [Duv89] or [Wal00].
- A projection procedure for unramified fibres as in [Sch03].

The asymptotic time complexity of such a procedure is roughly $O(During+\varrho^2)$ arithmetic operations in $\mathbb{Q}$, where ϱ denotes the geometric degree of the system $F_1,\ldots,F_n$ (in the sense of [GHH$^+$97]). Observe that the estimates $D \leq \delta \leq \varrho$ hold.

In [PR11] and [PR12] the authors describe an algorithm to compute the singular parts of rational Puiseux expansions of an equation given by a bivariate polynomial $F(X,Y) = 0$. The approach is based on a modification of an algorithm due to D. Duval ([Duv89]). The randomized algorithm presented in [PR12] chooses a suitable finite field L to perform computations and uses the finite fields procedure of [PR11], which roughly takes an expected number of $O(d_Y^3 d_X^2 + d_Y^2 d_X t_0 \log p)$ arithmetic operations in L to compute the singular parts of all the rational Puiseux expansions above 0. Here $t_0 := [L : \mathbb{F}_p]$ denotes the degree of the field extension $L/\mathbb{F}_p$ and d_X and d_Y are the degree of F in the variable X and Y respectively.

Nevertheless, as we are only interested in particular cases where the singular parts can be immediately generated (see Subsections 4.4.3 and 4.4.4), we are not going to use this procedure.

4.4. Examples

In this section we apply our algorithmic method in order to compute a geometric solution of certain zero–dimensional polynomial equation systems. In Section 4.4.1 we treat the case of Pham–Brieskorn systems. In Section 4.4.2 we treat a family of systems which arise from a semidiscretization of certain parabolic differential equations with nonlinear source terms and nonlinear boundary conditions. Finally, in Section 4.4.4 we treat a generalization of Reimer systems, which we called generalized Reimer systems.

In all the above cases, we "deform" the polynomial equation system under consideration to a one–dimensional polynomial equation system satisfying the hypotheses of Theorem 4.7. Then the algorithm underlying the proof of Theorem 4.12 yields an efficient procedure to compute a geometric solution of the original zero–dimensional polynomial equation system.

We observe that all these examples are particular instances of a generalized Pham system. Nevertheless, the deformations we shall introduce have a ramified fibre with a very simple infinitesimal structure. This will allow us to slightly improve the cost that we obtain when applying the main algorithm of Chapter 3 to the polynomial systems which arise in these examples.

4.4.1. Pham–Brieskorn systems

Let us fix $n, d \in \mathbb{N}$. Let $g_1, \ldots, g_n \in \mathbb{Q}[X] := \mathbb{Q}[X_1, \ldots, X_n]$ satisfy $\deg(g_i) < d$ and $g_i(0, \ldots, 0) \neq 0$ for $1 \leq i \leq n$. Let us define $f_1, \ldots, f_n \in \mathbb{Q}[X]$ by:

$$f_1 := X_1^d - g_1, \ldots, f_1 := X_n^d - g_n. \tag{4.29}$$

A system of this form is called a *Pham–Brieskorn system* (see e.g. [LV98], [GV98], [Bom00], [PS04]). It is easy to see that $f_1, \ldots, f_n$ form a regular sequence of $\mathbb{Q}[X]$.Therefore, $f_1, \ldots, f_n$ define a zero–dimensional affine subvariety $\widetilde{V}$ of $\mathbb{A}^n$. Our aim is to compute a geometric solution of this variety $\widetilde{V}$.

Let $\mathcal{E}$ be an indeterminate over $\mathbb{Q}$ and define $F_1, \ldots, F_n \in \mathbb{Q}[\mathcal{E}, X]$ by:

$$F_1 := X_1^d - \mathcal{E} g_1 \ , \ \ldots \ , \ F_n := X_n^d - \mathcal{E} g_n. \tag{4.30}$$

Let V be the affine subvariety of $\mathbb{A}^{n+1}$ defined by the polynomials $F_1, \ldots, F_n$, and let $\pi : V \to \mathbb{A}^1$ be the morphism defined by $\pi(\varepsilon, x) := \varepsilon$. We observe that $\pi^{-1}(1) = \{1\} \times \widetilde{V}$ and $\pi^{-1}(0) = \{0\} \subset \mathbb{A}^{n+1}$ hold.

In Section 4.4.3 we exhibit an algorithm which computes a geometric solution of the variety V. Furthermore, specializing the polynomials of $\mathbb{Q}[\mathcal{E}, X]$ which constitute this geometric solution into the value $\mathcal{E} = 1$ we shall obtain a geometric solution of $\widetilde{V}$.

4.4.2. Systems coming from a semidiscretization of certain parabolic differential equations

In this section we consider a family of polynomial equation systems which arises in the analysis of the stationary solutions of a numerical approximation, obtained by a semidiscretization in space, of certain parabolic differential equations with nonlinear source terms and nonlinear boundary conditions (see e.g. [BR01], [FGR02]).

Let us fix $n, d \in \mathbb{N}$ with $d \geq 2$. Let T be an indeterminate over $\mathbb{Q}$, and let $g, h \in \mathbb{Q}[T] \setminus \{0\}$ satisfy $\deg(g) < d$ and $\deg(h) = d$. Let us write $h = aT^d + h_1(T)$ with $a \neq 0$ and $\deg(h_1) < d$. Let $f_1, \ldots, f_n$ be the polynomials of $\mathbb{Q}[X] := \mathbb{Q}[X_1, \dots, X_n]$ defined in the following way:

$$\begin{array}{rcl} f_1 & := & 2(n-1)^2(X_2^d - X_1^d) - g(X_1), \\ f_i & := & (n-1)^2(X_{i+1}^d - 2X_i^d + X_{i-1}^d) - g(X_i), \quad (2 \leq i \leq n-1) \\ f_n & := & 2(n-1)^2(X_{n-1}^d - X_n^d) + 2(n-1)h(X_n) - g(X_n). \end{array} \tag{4.31}$$

An important case of study is that of the stationary solutions of the porous medium equation with nonlinear source terms and nonlinear boundary condition (see e.g. [Hen81], [CFQ91b]). Typical discretizations of this problem lead for example to instances of system (4.31) with $h := T^d$ and $g := T$ (see e.g. [FGR02]).

Let $\widetilde{V}$ be the affine subvariety of $\mathbb{A}^n$ defined by the polynomials $f_1, \dots, f_n$. Our aim is to exhibit an efficient algorithm which computes a geometric solution of the variety $\widetilde{V}$. For this purpose, let $f := (f_1, \dots, f_n)$, $e_n := (0, \dots, 0, 1) \in \mathbb{Q}^n$, $G := (g(X_1), \dots, g(X_n))$, and $X^d := (X_1^d, \dots, X_n^d)$. Let $A \in \mathbb{Q}^{n \times n}$ be the following nonsingular tridiagonal matrix:

$$A := (n-1)^2 \begin{pmatrix} -2 & 2 & & & & \\ 1 & -2 & 1 & & & \\ & & \ddots & \ddots & \ddots & \\ & & & 1 & -2 & 1 \\ & & & & 2 & -2 + \frac{2a}{n-1} \end{pmatrix}.$$

Then the polynomials $f_1, \dots, f_n$ can be expressed as:

$$f^t = A \cdot (X^d)^t + 2(n-1)h_1(X_n)e_n^t - G^t, \tag{4.32}$$

where ^{t} denotes transposition.

In order to solve the system defined by the polynomials in (4.32), we introduce a new indeterminate $\mathcal{E}$ and consider the following polynomials of $\mathbb{Q}[\mathcal{E}, X]$:

$$(\widetilde{F}_1, \dots, \widetilde{F}_n)^t := A \cdot (X^d)^t + \mathcal{E}\big(2(n-1)h_1(X_n)e_n^t - G^t\big) - 2(n-1)\mathcal{E}(1-\mathcal{E})e_n^t. \tag{4.33}$$

Let V be the affine subvariety of $\mathbb{A}^{n+1}$ defined by the polynomials $\widetilde{F}_1, \dots, \widetilde{F}_n$ and let $\pi : V \to \mathbb{A}^1$ be the morphism defined by $\pi(\varepsilon, x) = \varepsilon$. We observe that $\pi^{-1}(1) = \{1\} \times \widetilde{V}$ and $\pi^{-1}(0) = \{0\} \subset \mathbb{A}^{n+1}$. Since the matrix A is nonsingular, multiplying both sides of (4.33) by A^{-1} we obtain the following polynomials, whose zero set also defines the variety V:

$$(F_1, \dots, F_n)^t := (X^d)^t + \mathcal{E}A^{-1}\big(2(n-1)h_1(X_n)e_n^t - G^t\big) - \mathcal{E}(\mathcal{E}-1)v^t, \tag{4.34}$$

where $v := \frac{n-1}{2a}(1, \dots, 1)$. In Section 4.4.3 we exhibit an algorithm computing a geometric solution of the variety V. By specializing the polynomials of $\mathbb{Q}[\mathcal{E}, X]$ which constitute this geometric solution into the value $\mathcal{E} = 1$ we shall obtain a geometric solution of our input variety $\widetilde{V}$.

4.4.3. A common approach to both examples

In this section we describe an algorithm which finds a geometric solution of the variety defined by any system of the form (4.30) and (4.34). Then, we shall specialize the polynomials of $\mathbb{Q}[\mathcal{E}, X]$ which form such geometric solution into the value $\mathcal{E} = 1$ in order to obtain a geometric solution of the variety defined by the corresponding system of the form (4.29) and (4.31).

Let us fix $n, d \in \mathbb{N}$. For $1 \le i \le n$, let $H_i \in \mathbb{Q}[\mathcal{E}, X]$ satisfy $\deg H_i \le d-1$ and $\alpha_i := H_i(0,0) \neq 0$. Suppose further that we are given a straight–line program computing the polynomials $H_1, \dots, H_n$ using $\mathcal{T}$ arithmetic operations in $\mathbb{Q}$.

For $1 \le i \le n$, let us define $F_i \in \mathbb{Q}[\mathcal{E}, X]$ by the following expression:

$$F_i := X_i^d - \mathcal{E}H_i(\mathcal{E}, X). \tag{4.35}$$

Let $\mathcal{I}$ be the ideal of $\mathbb{Q}[\mathcal{E}, X]$ generated by $F_1, \dots, F_n$ and let V be the affine subvariety of $\mathbb{A}^{n+1}$ defined by $\mathcal{I}$. Let $\pi : V \to \mathbb{A}^1$ denote the restriction to V of the canonical projection onto the first coordinate. Our purpose is to compute a geometric solution of $\{1\} \times \widetilde{V} := \pi^{-1}(1)$.

It is easy to see that any system of the form (4.30) and (4.34) is a particular instance of a system of the form (4.35). In order to apply our algorithmic method, we first show in Lemmas 4.13 and 4.14 below that the polynomials $F_1, \dots, F_n$ of (4.35) form a regular sequence of $\mathbb{Q}[\mathcal{E}, X]$, the ideal $\mathcal{I} \subset \mathbb{Q}[\mathcal{E}, X]$ they generate is radical, and the morphism π is finite and generically unramified.

Lemma 4.13. *The polynomials $F_1, \dots, F_n$ form a regular sequence of $\mathbb{Q}[\mathcal{E}, X]$ and the morphism π is finite.*

Proof. From Buchberger's first criterion (see e.g. [BW93]), we conclude that for $1 \leq i \leq n$ the polynomials $F_1, \dots, F_i$ form a Gröbner basis of the ideal they generate with respect to the graded lexicographical order induced by the ordering $X_1 > \cdots > X_n > \mathcal{E}$. This implies that the affine variety of $\mathbb{A}^{n+1}$ defined by $F_1, \dots, F_i$ has codimension i for $1 \leq i \leq n$. Then $F_1, \dots, F_n$ form a regular sequence of $\mathbb{Q}[\mathcal{E}, X]$.

Furthermore, we observe that the leading monomial of F_i under this order is X_i^d for $1 \leq i \leq n$. Therefore, the set $\{X_1^{i_1} \cdots X_n^{i_n} : 0 \leq i_1, \dots, i_n < d\}$ is a basis as $\mathbb{Q}[\mathcal{E}]$–module of $\mathbb{Q}[\mathcal{E}, X]/\mathcal{I}$. This proves that π is a finite morphism. □

For $1 \leq i \leq n$, let $G_i \in \mathbb{Q}[\mathcal{E}, X]$ be the following polynomial:

$$G_i(\mathcal{E}, X) := \mathcal{E}^{-d} F_i(\mathcal{E}^d, \mathcal{E}X).$$

Let $\widetilde{W} \subset \mathbb{A}^{n+1}$ be the affine variety defined by $G_1, \dots, G_n$, and let $\widetilde{\pi} : \widetilde{W} \to \mathbb{A}^1$ be the morphism induced by the canonical projection onto the first coordinate. We claim the morphism $\widetilde{\pi}$ is generically unramified.

Let us observe that for $\varepsilon \neq 0$ we have $\#(\widetilde{\pi}^{-1}(\varepsilon)) = \#(\pi^{-1}(\varepsilon^d))$. Therefore, from the fact that the morphism π is finite we easily conclude that $\widetilde{\pi}$ is dominant and $\dim \widetilde{W} \geq 1$ holds. Furthermore, from the fact that $\mathbb{Q}(V)$ is a zero–dimensional $\mathbb{Q}(\mathcal{E})$–algebra, we deduce that $\mathbb{Q}(\widetilde{W})$ is also a zero–dimensional $\mathbb{Q}(\mathcal{E})$–algebra. This shows that $\widetilde{W}$ is a one–dimensional variety.

Let us fix $\varepsilon \in \mathbb{A}^1$. Taking into account that $\deg_X G_i(\varepsilon, X) = d$ for $1 \leq i \leq n$, from the Bézout inequality (2.1) we deduce that $\deg \widetilde{\pi}^{-1}(\varepsilon) \leq d^n$ holds. On the other hand, for $1 \leq i \leq n$ we have $G_i(0, X) = X_i^d - \alpha_i$, where $\alpha_i = H_i(0,0) \neq 0$. This implies that $\widetilde{\pi}^{-1}(0)$ has cardinality d^n. We conclude that any generic fibre $\widetilde{\pi}^{-1}(\varepsilon)$ has cardinality d^n.

Lemma 4.14. *$\mathcal{I}$ is a radical ideal and the morphism π is generically unramified.*

Proof. For a generic choice $\varepsilon \in \mathbb{A}^1$, we have $\#(\widetilde{\pi}^{-1}(\varepsilon)) = \#(\pi^{-1}(\varepsilon^d)) = d^n$. This implies that there exists a fibre $\pi^{-1}(\varepsilon)$ of cardinality d^n. On the other hand, applying the Bézout inequality (2.1) we see that $\#(\pi^{-1}(\varepsilon)) \leq d^n$ holds for any $\varepsilon \in \mathbb{A}^1$. We conclude that $\#(\pi^{-1}(\varepsilon)) = d^n$ holds for any generic choice of the value $\varepsilon \in \mathbb{A}^1$.

Let ε be a generic element of $\mathbb{A}^1$. Then

$$\dim_{\mathbb{C}} \mathbb{C}[X]/\big(F_1(\varepsilon, X), \ldots, F_n(\varepsilon, X)\big) = d^n = \deg \pi^{-1}(\varepsilon).$$

This implies (see e.g. [CLO98, Corollary 2.6]) that $\pi^{-1}(\varepsilon)$ is a smooth variety and the polynomials $F_1(\varepsilon, X), \ldots, F_n(\varepsilon, X)$ generate a radical ideal of $\mathbb{C}[X]$. In particular, we have that the Jacobian determinant $J_F(\varepsilon, X) := \det(\partial F_i/\partial X_j)_{1\leq i,j\leq n}(\varepsilon, X)$ does not vanish on any point $x \in \mathbb{A}^n$ with $(\varepsilon, x) \in \pi^{-1}(\varepsilon)$. Thus, $J_F(\mathcal{E}, X)$ is not a zero divisor of $\mathbb{Q}[\mathcal{E}, X]/\mathcal{I}$ and π is generically unramified. Finally, since $F_1, \ldots, F_n$ form a regular sequence of $\mathbb{Q}[\mathcal{E}, X]$, from [Eis95, Theorem 18.15] we deduce that the ideal $\mathcal{I}$ is radical. □

Let us observe that the origin $0 \in \mathbb{A}^{n+1}$ is the only point of $\pi^{-1}(0)$. Therefore, there are $\deg(\pi) = d^n$ branches of the curve V passing through $0 \in \mathbb{A}^{n+1}$.

For $F \in \mathbb{Q}[\mathcal{E}, X]$, let us write $F(\mathcal{E}^d, \mathcal{E}X) = \mathcal{E}^\alpha f(X) + O(\mathcal{E}^{\alpha+1})$, with $f \neq 0$. We define the initial term of F with respect to the weight $(d, 1, \ldots, 1)$ as the polynomial $in_d(F) := f$. Let $in_d(\mathcal{I}) \subset \mathbb{Q}[X]$ be the ideal generated by the set $\{in_d(F) : F \in \mathcal{I}\}$ and let $W \subset \mathbb{A}^n$ be the affine variety defined by $in_d(\mathcal{I})$.

Lemma 4.15. *$W = V(X_1^d - \alpha_1, \ldots, X_n^d - \alpha_n)$ and $G_1, \ldots, G_n$ form a standard basis.*

Proof. Let us observe that the set $\{in_d(F) : F \in \mathcal{I}\}$ is contained in the set of initial terms (in the sense of Section 4.2) of the polynomials of the ideal $(G_1, \ldots, G_n)$. Let $F \in (G_1, \ldots, G_n)$, and let us write $F = \mathcal{E}^\alpha \widetilde{F}(\mathcal{E}, X)$, with $\alpha \geq 0$ and $\widetilde{F}(0, X) \neq 0$. Since $\mathcal{E}$ is not a zero divisor of the $\mathbb{Q}$–algebra $\mathbb{Q}[\mathcal{E}, X]/(G_1, \ldots, G_n)$, we conclude that $\widetilde{F} \in (G_1, \ldots, G_n)$ holds. Then

$$in(\widetilde{F}) = \widetilde{F}(0, X) \in \big(G_1(0, X), \ldots, G_n(0, X)\big) = (X_1^d - \alpha_1, \ldots, X_n^d - \alpha_n),$$

which implies that $in_d(\mathcal{I}) \subset (X_1^d - \alpha_1, \ldots, X_n^d - \alpha_n)$ holds and $G_1, \ldots, G_n$ form a standard basis. On the other hand,

$$(X_1^d - \alpha_1, \ldots, X_n^d - \alpha_n) = \big(in_d(F_1), \ldots, in_d(F_n)\big) \subset in_d(\mathcal{I}),$$

from which the statement of Lemma 4.15 follows. □

Since there are d^n branches of V lying above 0 and $\deg W = d^n$, we conclude that the system of (classical) Puiseux expansions of the branches of the curve V lying above 0 has regularity index 1, and the singular parts of its expansions are represented by the points of W.

Lemmas 4.14 and 4.15 show that the polynomials of (4.35) satisfy the hypotheses of Theorems 4.7 and 4.12. In order to apply the algorithm underlying Theorem 4.12 to our input system, we first need an explicit description of the set of singular parts of a system of rational Puiseux expansions of the branches of V lying above 0. For this purpose, we observe that the set of singular parts is given by

$$\big\{(T^d, \xi^{j_1}\alpha_1^{1/d}T, \dots, \xi^{j_n}\alpha_n^{1/d}T); 0 \leq j_1, \dots, j_n < d\big\} \subset \overline{\mathbb{Q}}[T]^{n+1},$$

where $\xi \in \overline{\mathbb{Q}}$ is a primitive d–th root of 1 and $\alpha_1^{1/d}, \dots, \alpha_n^{1/d} \in \overline{\mathbb{Q}}$ are d–th roots of $\alpha_1, \dots, \alpha_n$ respectively. Replacing T by $\alpha_1^{-1/d}T$ we obtain the following system of rational Puiseux expansions of the branches of V lying above 0:

$$\big\{(\alpha_1^{-1}T^d, T, \xi^{j_2}\beta_2^{1/d}T, \dots, \xi^{j_n}\beta_n^{1/d}T); 0 \leq j_2, \dots, j_n < d\big\} \subset \overline{\mathbb{Q}}[T]^{n+1},$$

where $\beta_2^{1/d}, \dots, \beta_n^{1/d} \in \overline{\mathbb{Q}}$ are d–th roots of $\beta_2 := \alpha_1^{-1}\alpha_2, \dots, \beta_n := \alpha_1^{-1}\alpha_n$ respectively. With the notations of Section 4.1, we have $g = 1$, $e_1 = d$, $f_1 = d^{n-1}$.

Let $Y_2, \dots, Y_n$ be new indeterminates over $\mathbb{Q}$. Let

$$W_0 := \big\{(\xi^{j_2}\beta_2^{1/d}, \dots, \xi^{j_n}\beta_n^{1/d}); 0 \leq j_2, \dots, j_n < d\big\} = V(Y_2^d - \beta_2, \dots, Y_n^d - \beta_n).$$

Then we see that a geometric solution of the variety W_0 yields the polynomials $q^{(1)}, f_2^{(1)}, \dots, f_n^{(1)}$ required for the application of the algorithm of Theorem 4.12.

Let $U := \gamma_2 Y_2 + \cdots + \gamma_n Y_n$ be a linear form of $\mathbb{Q}[Y_2, \dots, Y_n]$ inducing a primitive element of the $\mathbb{Q}$–algebra extension $\mathbb{Q} \hookrightarrow \mathbb{Q}[W_0]$. In order to compute a geometric solution of W_0 we apply the algorithm underlying the proof of Lemma 3.11. Fix $\rho \geq 2$ and suppose that the coefficients of $\gamma_2, \dots, \gamma_n$ are randomly chosen in the set $\{1, \dots, 4n\rho d^{3n-3}\}$. By Lemma 3.11 and Proposition 3.14 we conclude that such a geometric solution can be computed with $O(\mathsf{M}(d^{2n-2})$ arithmetic operations in $\mathbb{Q}$. Finally, applying Theorem 4.12 we obtain the following result.

Theorem 4.16. *There exists a computation tree computing a geometric solution of the variety V with $O(\mathcal{T}\mathsf{M}(d^n)^2)$ arithmetic operations in $\mathbb{Q}$.*

The geometric solution provided by Theorem 4.16 consists of a randomly chosen linear form $U \in \mathbb{Q}[X]$ and polynomials $m_u, v_1, \dots, v_n \in \mathbb{Q}[\mathcal{E}, Z]$. Suppose that U is also a primitive element of the original variety $\{1\} \times \widetilde{V} = V \cap (\{1\} \times \mathbb{A}^n)$. Specializing $m_u, v_1, \dots, v_n$ into the value $\mathcal{E} = 1$, we obtain polynomials $m_u(1, Z), v_1(1, Z), \dots, v_n(1, Z)$ of $\mathbb{Q}[X]$ defining a (eventually non–reduced) Shape–Lemma–like representation of $\widetilde{V}$. Therefore, computing a square–free representation of $m_u(1, Z)$, and cleaning the multiple factors of the polynomial $m_u(1, Z)$ out of $v_1(1, Z), \dots, v_n(1, Z)$ we obtain a geometric solution of $\widetilde{V}$ with the same complexity estimate (see [GLS01] for details).

This result improves the rough $O(3^n d^{2n})$ complexity estimate of [MP97]. Let us also mention the results of [MP00], where the authors announce a rough $O(d^{2n})$ complexity estimate for approximating one root of a Pham system. Comparing our result with the rough $O(\mathcal{T} d^{2n-1})$ complexity estimate provided by the application of the algorithm of [GLS01] to this case, we see that the performance of [GLS01] is better. Nevertheless, let us observe that the leading term d^{2n} of our complexity estimate can be expressed as $\delta \deg_{\mathcal{E}} m_u$ and we are dealing in this case with an “ill-conditioned” system, for which the worst case estimates $\delta = d^n$ and $\deg_{\mathcal{E}} m_u = d^n$ hold. If the input system satisfies $\deg_{\mathcal{E}} m_u \ll d^n$, then the performance of [GLS01] does not change, whereas in our complexity estimate the d^{2n} factor reduces accordingly. Furthermore, if $\deg_{\mathcal{E}} m_u = 1$, we achieve the lower bound d^n of this factor (see [CGH+03]).

4.4.4. Reimer Systems

In this section we consider another family of examples called (generalized) Reimer systems (compare [BM96]). Let us fix $n \in \mathbb{N}$, and let us define $f_1, \dots, f_n \in \mathbb{Q}[X] := \mathbb{Q}[X_1, \dots, X_n]$ in the following way:

$$f_i := \alpha_i + \sum_{j=1}^{n} a_{i,j} X_j^{i+1}, \tag{4.36}$$

where $a_{i,j}, \alpha_i$ $(1 \leq i, j \leq n)$ are *generic* elements of $\mathbb{Q}$ (see Lemma 4.17 below) with $\alpha_i, a_{i,i} \neq 0$ for $1 \leq i \leq n$. Let $\widetilde{V}$ be the affine subvariety of $\mathbb{A}^n$

defined by $f_1, \dots, f_n$. Our purpose is to compute a geometric solution of $\widetilde{V}$.

Our next result shows that $\widetilde{V}$ has dimension zero and degree $(n+1)!$.

Lemma 4.17. *Let $U := (U_{i,j})_{1 \le i,j \le n}$ be a matrix of indeterminates and let $H_1, \dots, H_n$ be the elements of $\mathbb{Q}[U, X]$ defined in the following way:*

$$H_i := \alpha_i + \sum_{j=1}^{n} U_{i,j} X_j^{i+1}.$$

Then there exists a non–empty Zariski open set $\mathcal{U} \subset \mathbb{A}^{n^2}$ with the following property: for any $u \in \mathcal{U}$, the affine subvariety of $\mathbb{A}^n$ defined by the polynomials $H_1(u, X), \dots, H_n(u, X)$ has dimension 0 and degree $(n+1)!$.

Proof. Let Z be the affine variety of $\mathbb{A}^{n^2+n}$ defined by $H_1, \dots, H_n$ and let $\pi_U : Z \to \mathbb{A}^{n^2}$ be the morphism defined by $\pi(u, x) = u$. Let $\wp$ be the prime ideal of $\mathbb{Q}[U]$ generated by the set $\{U_{i,j}; 1 \le i,j \le n, i \ne j\}$. We claim that $H_1, \dots, H_n$ form a regular sequence of $\mathbb{Q}[U]_\wp[X]$.

In order to prove this claim, following [HJS$^+$02], we define a "triangular" sequence $(R_j^{(i)})_{1 \le i \le n, i+1 \le j \le n} \subset \mathbb{Q}[U, X]$ in the following way:

- $R_j^{(1)} := Res_{X_1}(H_1, H_j)$ for $j = 2, \dots, n$.
- $R_j^{(i)} := Res_{X_i}(R_i^{(i-1)}, R_j^{(i-1)})$ for $2 \le i \le n-1$ and $i+1 \le j \le n$.

From elementary properties of the resultant we see that $R_i^{(i-1)}$ is a nonzero element of $\mathbb{Q}[U, X_i, \dots, X_n] \cap (H_1, \dots, H_i)$, with $\deg_X R_i^{(i-1)} = \deg_{X_i} R_i^{(i-1)}$. Furthermore, a recursive argument shows that the coefficient of the highest power of X_i occurring in $R_i^{(i-1)}$ does not belong to the prime ideal $\wp$. We conclude that $H_1, \dots, H_i$ define an ideal of $\mathbb{Q}[U]_\wp[X]$ of Krull dimension $n-i$. This implies that $H_1, \dots, H_n$ form a regular sequence of $\mathbb{Q}[U]_\wp[X]$.

Furthermore, the polynomial $R_n^{(n-1)}$ gives an integral dependence equation for the coordinate class of X_n in the ring $\mathbb{Q}[U]_\wp[X_1, \dots, X_n]/(H_1, \dots, H_n)$ over the ring $\mathbb{Q}[U]_\wp$. Then a recursive argument with the polynomials $R_i^{(i-1)}$ for $1 \le i \le n$ shows that

$$\mathbb{Q}[U]_\wp \hookrightarrow \mathbb{Q}[U]_\wp[X_1, \dots, X_n]/(H_1, \dots, H_n) \tag{4.37}$$

is an integral $\mathbb{Q}$–algebra extension.

We conclude that there exists a Zariski neighborhood $\widetilde{\mathcal{U}} \subset \mathbb{A}^{n^2}$ of $V(\wp)$ such that $\pi_U|_{Z\cap(\widetilde{\mathcal{U}}\times\mathbb{A}^n)} : Z\cap(\widetilde{\mathcal{U}}\times\mathbb{A}^n) \to \widetilde{\mathcal{U}}$ is a finite morphism and $Z\cap(\widetilde{\mathcal{U}}\times\mathbb{A}^n)$ is an equidimensional variety of dimension n^2. This shows that for any choice of $u \in \widetilde{\mathcal{U}}$ the variety $Z \cap \{U = u\} = \pi_U^{-1}(u)$ has dimension 0.

Now we show that the existence of the Zariski open set $\mathcal{U} \subset \widetilde{\mathcal{U}}$ of the statement of the lemma. First, we observe that the Bézout inequality (2.1) implies $\deg(\pi_U^{-1}(u)) \leq (n+1)!$ for any $u \in \widetilde{\mathcal{U}}$. On the other hand, for any nonsingular diagonal matrix $u^{(0)} \in \widetilde{\mathcal{U}}$ we have $\deg(\pi_U^{-1}(u^{(0)})) = (n+1)!$. We conclude that there exists a non–empty Zariski open set $\mathcal{U} \subset \widetilde{\mathcal{U}}$ such that $\deg(\pi_U^{-1})(u) = (n+1)!$ holds for any $u \in \mathcal{U}$. □

Let us observe that for any $u \in \mathcal{U}$ we have that $\mathbb{C}[X]/(H_1(u,X), \ldots, H_n(u,X))$ is a finite–dimensional $\mathbb{C}$–vector space of dimension at most $(n+1)!$. On the other hand, we have $\#(\pi_U^{-1}(u)) = (n+1)!$. We conclude that the polynomials $H_1(u,X), \ldots, H_n(u,X)$ generate a radical zero–dimensional ideal of $\mathbb{C}[X]$, and hence the Jacobian determinant $J_H(u,X) := \det(\partial H_i/\partial X_j)_{1\leq i,j\leq n}(u,X)$ does not vanish on any point x with $(u,x) \in \pi_U^{-1}(u)$. This implies that J_H does not vanish on any point of $Z \cap (\mathcal{U} \times \mathbb{A}^n)$.

In order to solve a system of the form (4.36) with $a := (a_{i,j})_{1\leq i,j\leq n} \in \mathcal{U}$, let us introduce an indeterminate $\mathcal{E}$ over $\mathbb{Q}$ and the following elements of $\mathbb{Q}[\mathcal{E}, X]$:

$$F_i := \alpha_i \mathcal{E}^{i+1} + a_{i,i}X_i^{i+1} + \sum_{\substack{1\leq j\leq n\\ j\neq i}} a_{i,j}\mathcal{E}X_j^{i+1} \quad (1 \leq i \leq n). \tag{4.38}$$

Let V be the affine subvariety of $\mathbb{A}^{n+1}$ defined by $F_1, \ldots, F_n$ and let $\pi : V \to \mathbb{A}^1$ be the morphism defined by $\pi(\varepsilon, x) := \varepsilon$. We have $\pi^{-1}(1) = \{1\} \times \widetilde{V}$ and $\pi^{-1}(0) = \{0\} \subset \mathbb{A}^{n+1}$. We are going to show that $F_1, \ldots, F_n$ form a regular sequence of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$ and generate a radical ideal of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$, and the morphism π is dominant and generically unramified.

For this purpose, let us define $G_1, \ldots, G_n \in \mathbb{Q}[\mathcal{E}, X]$ in the following way:

$$G_i := \mathcal{E}^{-(i+1)}F_i(\mathcal{E}, \mathcal{E}X) = \alpha_i + \sum_{j=1}^{n} g_{i,j}X_j^{i+1},$$

where $g_{i,j} := a_{i,j}\,\mathcal{E}$ for $i \neq j$ and $g_{i,i} := a_{i,i}$. Let $\widetilde{W}$ be the affine subvariety of $\mathbb{A}^{n+1}$ defined by $G_1, \ldots, G_n$, and let $\widetilde{\pi} : \widetilde{W} \to \mathbb{A}^1$ be the morphism defined by $\widetilde{\pi}(\varepsilon, x) = \varepsilon$. Observe that $g(1) \in \mathcal{U}$ holds, where $\mathcal{U} \subset \mathbb{A}^{n^2}$ is the Zariski open set of the statement of Lemma 4.17. Therefore, for a generic choice $\varepsilon \in \mathbb{A}^1$, we have $g(\varepsilon) \in \mathcal{U}$. Taking into account the remarks after the proof of Lemma 4.17, we conclude that $\widetilde{\pi}$ is dominant and generically unramified.

Finally, since $\#(\widetilde{\pi}^{-1}(\varepsilon)) = \#(\pi^{-1}(\varepsilon))$ holds for any $\varepsilon \neq 0$, we deduce the following result.

Lemma 4.18. *The morphism π is dominant and generically unramified.*

On the other hand, we have the following result.

Lemma 4.19. *$F_1, \ldots, F_n$ form a regular sequence in $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$ and generate a radical ideal of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$.*

Proof. For $1 \leq i \leq n$, let $\widehat{F}_i \in [\mathcal{E}, X_0, \ldots, X_n]$ denote the homogenization of the polynomial F_i with respect to the variables X. We have $\widehat{F}_i \equiv a_{i,i}X_i^{i+1}$ mod $(\mathcal{E})$. Following [HJS+02], we define the following "triangular" sequence $(\widehat{R}_j^{(i)})_{1\leq i\leq n, i+1\leq j\leq n}$ of $\mathbb{Q}[\mathcal{E}, X]$:

- $\widehat{R}_j^{(1)} := Res_{X_1}(\widehat{F}_1, \widehat{F}_j)$ for $j = 2, \ldots, n$.
- $\widehat{R}_j^{(i)} := Res_{X_i}(\widehat{R}_i^{(i-1)}, \widehat{R}_j^{(i-1)})$ for $2 \leq i \leq n-1$ and $i+1 \leq j \leq n$.

From the elementary properties of the resultant we deduce that $\widehat{R}_j^{(i)}$ is an homogeneous polynomial of $(\widehat{F}_1, \ldots, \widehat{F}_j) \cap \mathbb{Q}[\mathcal{E}, X_0, X_{i+1}, \ldots, X_n]$. Furthermore, taking into account the congruence relation $\widehat{F}_i \equiv a_{i,i}X_i^{i+1}$ mod $(\mathcal{E})$, a simple recursive argument shows that $\widehat{R}_i^{(i-1)} \equiv c_i X_i^{m_i}$ mod $(\mathcal{E})$ holds for suitable $c_i \in \mathbb{Q} \setminus \{0\}$ and $m_i \in \mathbb{N}$. This shows that the coefficient of $X_i^{m_i}$ in $R_i^{(i-1)}$ does not belong to the prime ideal $(\mathcal{E}) \subset \mathbb{Q}[\mathcal{E}]$. Specializing the variable X_0 into the value $X_0 = 1$, with a similar argument as in the proof of Lemma 4.17 we conclude that $F_1, \ldots, F_n$ form a regular sequence of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$ and

$$\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})} \hookrightarrow \mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]/(F_1, \ldots, F_n)$$

is an integral $\mathbb{Q}$–algebra extension.

Finally, since $F_1, \dots, F_n$ form a regular sequence of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$, and the morphism π is generically unramified, applying [Eis95, Theorem 18.15] as in Lemma 4.14 we conclude that the ideal generated by $F_1, \dots, F_n$ in $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$ is radical. □

Let us observe that the origin $0 \in \mathbb{A}^{n+1}$ is the only point of $\pi^{-1}(0)$. Therefore, there are $\deg(\pi) = (n+1)!$ branches of V passing through $0 \in \mathbb{C}^{n+1}$.

For any $F \in \mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$, let us write $F(\mathcal{E}, \mathcal{E}X) = \mathcal{E}^{\alpha}\widetilde{F}(\mathcal{E}, X)$ with $\widetilde{F} \in \mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X] \setminus (\mathcal{E})\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$. We define the initial term of F with respect to the weight $(1, \dots, 1)$ as $in_1(F) := \widetilde{F}(0, X)$. Let $\mathcal{I}$ be the ideal of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$ generated by $F_1, \dots, F_n$, and let $in_1(\mathcal{I}) \subset \mathbb{Q}[X]$ be the ideal generated by the set $\{in_1(F) : F \in \mathcal{I}\}$. Let $W := V(in_1(\mathcal{I})) \subset \mathbb{A}^n$.

Lemma 4.20. *$W = V(a_{1,1}X_1^2 - \alpha_1, \dots, a_{n,n}X_n^{n+1} - \alpha_n)$ and $G_1, \dots, G_n$ form a standard basis in $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$.*

Proof. Let us observe that the set $\{in_1(F) : F \in \mathcal{I}\}$ is contained in the set of initial terms (in the sense of Section 4.2) of the polynomials of the ideal $(G_1, \dots, G_n) \subset \mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$. Let $F \in (G_1, \dots, G_n)$ and write $F = \mathcal{E}^{\alpha}\widetilde{F}(\mathcal{E}, X)$, with $\alpha \geq 0$ and $\widetilde{F}(0, X) \neq 0$. Since $\mathcal{E}$ is not a zero divisor of the $\mathbb{Q}$–algebra $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]/(G_1, \dots, G_n)$, we conclude that $\widetilde{F} \in (G_1, \dots, G_n)$ holds. Then

$$in_1(\widetilde{F}) = \widetilde{F}(0,X) \in \big(G_1(0,X), \dots, G_n(0,X)\big) = (a_{1,1}X_1^2 - \alpha_1, \dots, a_{n,n}X_n^{n+1} - \alpha_n),$$

which implies that $in_1(\mathcal{I}) \subset (a_{1,1}X_1^2 - \alpha_1, \dots, a_{n,n}X_n^{n+1} - \alpha_n)$ holds and $G_1, \dots, G_n$ form a standard basis. On the other hand, we have the inclusion

$$(a_{1,1}X_1^2 - \alpha_1, \dots, a_{n,n}X_n^{n+1} - \alpha_n) = \big(in_1(F_1), \dots, in_1(F_n)\big) \subset in_1(\mathcal{I}),$$

from which the lemma follows. □

Since there are $(n+1)!$ branches of V lying above 0 and $\deg W = (n+1)!$, we conclude that the system of (classical) Puiseux expansions of the branches of the curve V lying above 0 has regularity index 1, and the singular parts of its expansions are represented by the points of W.

Lemmas 4.18, 4.19 and 4.20 show that the polynomials $F_1, \dots, F_n$ of (4.38) satisfy all the hypotheses of Theorems 4.7 and 4.12 (see the remark right before Section 4.2.1). In order to apply the algorithm underlying Theorem 4.12 we need a description of the singular parts of the branches of V lying above 0. A similar argument as in Section 4.4.3 shows that, with the notations of Section 4.1, $g = 1$, $e_1 = 1$ and $f_1 = (n+1)!$ in this case. Hence, we have that a geometric solution of the variety W yields the polynomials $q^{(1)}, f_1^{(1)}, \dots, f_n^{(1)}$ required for the application of Theorem 4.12. Such a geometric solution can be obtained in $O(n\mathsf{M}((n+1)!)^2)$ arithmetic operations in $\mathbb{Q}$, using a similar algorithm to that of Section 4.4.3. Finally, applying Theorem 4.12 we obtain the following result.

Theorem 4.21. *There exists a straight–line program computing a geometric solution of the variety V in $O(n\mathsf{M}((n+1)!)^2)$ arithmetic operations in $\mathbb{Q}$.*

In order to obtain a geometric solution of the variety $\{1\} \times \widetilde{V} = \pi^{-1}(1)$ from the geometric solution of V provided by Theorem 4.21, we proceed in a similar way as in Section 4.4.3 (see the remarks after Theorem 4.16).

Chapter 5

Deformation techniques for sparse systems

This chapter deals with the symbolic computation of all the solutions to zero-dimensional sparse multivariate polynomial equation systems, i.e., systems with a finite number of common complex zeros defined by a sparse square system of polynomials. It is based on an article of the same title that I co-authored with Gabriela Jerónimo, Guillermo Matera, and Pablo Solernó ([JMSW09]).

The origins of sparse elimination theory can be traced back to the results by D.N. Bernstein, A.G. Kushnirenko and A.G. Khovanski ([Ber75], [Kus76], [Kho78]) that bound the number of solutions of a polynomial system in terms of a combinatorial invariant associated to the set of exponents of the monomials arising with nonzero coefficients in the defining polynomials. More precisely, the Bernstein-Kushnirenko-Khovanski (BKK for short) theorem asserts that the number of isolated solutions in the n-dimensional complex torus $(\mathbb{C}^*)^n$ of a polynomial system of n equations in n unknowns is bounded by the *mixed volume* of the family of Newton polytopes of the corresponding polynomials. Hence sparse elimination looks for techniques that profit from a low mixed volume of the underlying system or other sparsity parameters.

Numeric (homotopy continuation) methods for sparse systems are typically based on a specific family of deformations called polyhedral homotopies ([HS95], [VVC94], [VGC96], [Roj03]). Polyhedral homotopies preserve the

Newton polytope of the input polynomials and yield an effective version of the BKK theorem (see, e.g., [HS95], [HS97]).

In this chapter we combine the homotopic procedures of [HS95] with the symbolic deformation techniques developed in the previous chapters in order to derive a symbolic probabilistic algorithm for solving sparse zero-dimensional polynomial systems with cubic cost in the size of the combinatorial structure of the input system. Our main result may be stated as follows (see Theorem 5.23 below for a precise statement).

Theorem 5.1. *Let $f_1, \dots, f_n$ be polynomials in $\mathbb{Q}[X_1, \dots, X_n]$ such that the system $f_1 = 0, \dots, f_n = 0$ defines a zero-dimensional affine subvariety V of $\mathbb{C}^n$. Denote by $\Delta_1, \dots, \Delta_n \subset \mathbb{Z}^n_{\geq 0}$ the supports of $f_1, \dots, f_n$, and assume that $0 \in \Delta_i$ for $1 \leq i \leq n$ and the mixed volume D of the Newton polytopes $Q_1 := \mathrm{Conv}(\Delta_1), \dots, Q_n := \mathrm{Conv}(\Delta_n)$ is nonzero.*

Then, we can probabilistically compute a geometric solution of the variety V using roughly $O(NDD')$ arithmetic operations in $\mathbb{Q}$, with $N := \sum_{1 \leq i \leq n} \#\Delta_i$, $D := \sum_{1 \leq i \leq n} \mathcal{M}(\Delta, Q_1, \dots, Q_n)$ and $D' := \sum_{1 \leq i \leq n} \mathcal{M}(\Delta, Q_1, \dots, Q_{i-1}, Q_{i+1}, \dots, Q_n)$, where Δ denotes the standard n-dimensional simplex and $\mathcal{M}$ stands for mixed volume.

As input we are given polynomials $f_1, \dots, f_n \in \mathbb{Q}[X_1, \dots, X_n]$ which define a zero-dimensional variety of $\mathbb{A}^n(\mathbb{C})$. We assume that the combinatorics of the polyhedral deformation mentioned above are known. More precisely, we assume that we are given a certain collection of subsets of the input supports $\Delta_1, \dots, \Delta_n$, which defines a *fine-mixed subdivision* of $\Delta_1, \dots, \Delta_n$, together with the *lifting function* which yields such a subdivision (for precise definitions see [HS95, Section 2] or Section 5.1 below). For an efficient algorithm computing these objects see, for instance, [LL01].

The input of our algorithm is the standard sparse representation of the polynomials $f_1, \dots, f_n \in \mathbb{Q}[X_1, \dots, X_n]$, that is, the list of exponents of all nonzero monomials arising in $f_1, \dots, f_n$ together with the corresponding coefficients. We observe that in our setting there are no significant differences between the sparse and the straight–line program representation. Indeed, any polynomial $f \in \mathbb{Q}[X_1, \dots, X_n]$ of degree at most $d > 0$ having support $\Delta \subset \mathbb{Z}^n_{\geq 0}$ can be evaluated with $O(n\#\Delta \log d)$ arithmetic operations in $\mathbb{Q}$. In this sense, we see that f has a straight–line program representation whose size is of the same order as its standard sparse representation, and can be efficiently obtained from the latter. On the other hand, from a straight–line program which evaluates a polynomial $f \in \mathbb{Q}[X_1, \dots, X_n]$ of (known) support Δ with $\mathcal{L}$ arithmetic operations, the corresponding sparse representation can be easily obtained by a process of multipoint evaluation and interpolation with cost $O(\mathcal{L}\#\Delta)$, up to logarithmic terms. Since the routines of our procedure are of black-box type (cf. [CGH$^+$03]), that is, they only call the input polynomials and their first derivatives for substitutions of the variables $X_1, \dots, X_n$ into values belonging to suitable commutative zero-dimensional algebras, we conclude that the straight–line program representation of intermediate results is better suited than the sparse one. In particular, we note that computing the first derivatives of a multivariate polynomial can be done more efficiently for polynomials given by straight–line programs than by their sparse encoding (cf. [BS83]).

The complexity of our algorithm is mainly expressed in terms of three quantities which measure the size of the combinatorial structure of the input system: the number of nonzero coefficients $N := \sum_{1 \le i \le n} \#\Delta_i$ and the mixed volumes $D := \mathcal{M}(Q_1, \dots, Q_n)$ and $D' = \sum_{1 \le i \le n} \mathcal{M}(\Delta, Q_1, \dots, Q_{i-1}, Q_{i+1}, \dots, Q_n)$. While D represents the (optimal) number of paths which are followed during our homotopy, the quantity D' is an arithmetic analogue of D (see [PS03], [PS05]) which measures the "precision" at which the paths of our homotopy must be followed. We observe that the invariant D' is also optimal for a generic choice of the coefficients of the polynomials $f_1, \dots, f_n$ (see Lemma 5.3 below; compare also with [PS08, Theorem 1.1]). Therefore, we may paraphrase our complexity estimate as saying that it is *cubic* in the combinatorial structure of the input system, with a geometric component, an arithmetic component and a component related to the size of the input data. In this sense, we see that the cost of our algorithm strongly resembles the cost $O(ND\mu^2)$ of numerical continuation algorithms, where μ is the highest sparse condition number arising from the application of the Implicit Function Theorem to the points of the paths which are followed (cf. [Ded97]; see also [MR04] for a probability analysis of the condition numbers of sparse systems).

Our result improves and refines the estimate of Chapter 4 in the case of a sparse system, which is expressed as a fourth power of D and the maximum of the degrees of two varieties associated with the input (we observe that this maximum is an upper bound for the parameter D'). On the other hand, it also improves [Roj99], [Roj00], which solve a sparse system with a complexity which is roughly quartic in the size of the combinatorial structure of the input system. We shall also provide explicit estimates of the error probability of all the steps of our algorithm. This might be seen as a further contribution to the symbolic stage of the probabilistic semi-numeric method of [HS95], which lacks such an analysis of error probability.

The interest in tropical algebraic geometry has spawned results that generalise ours. Herrero et al. ([HJS13]) extend our results to the case where the square system $f_1 = 0, \dots, f_n = 0$ has a positive-dimensional solution set. In fact, the article (op. cit) describes an algorithm for computing one representative point in each irreducible component. More precisely, it outputs a list of geometric solutions —one per equidimensional component— where each geometric solution describes one point per irreducible component. The algorithm uses $\widetilde{O(}n^4dND^2)$ arithmetic operations in $\mathbb{Q}$, where $d := \max_{1\leq j\leq n}\{deg(f_j)\}$, $N = \sum_{j=1}^{n} \#(\mathcal{A}_j \cup \Delta)$ and $D = MV_n(\mathcal{A}_1 \cup \Delta, \dots, \mathcal{A}_n \cup \Delta)$.

Likewise, [Ver09] presents a different method for representing all the solutions of a possibly positive-dimensional polynomial system having at least as many equations as unknowns. It may also be worthwhile to mention that other authors of polyhedral homotopy methods aim to solve the problem by solving the face enumeration problem of finding all the lower facets of a mixed subdivision (see, e.g., [MTK07], [Miz08] and the bibliography therein).

The main algorithm of this chapter proceeds in two main steps: in the first step, the polyhedral deformation introduced in [HS95] is applied to solve an auxiliary generic sparse system with the same combinatorial structure as the input polynomials (Section 5.2; see also Section 5.2.1 for a discussion on the genericity conditions underlying the choice of the coefficients of the corresponding polynomials). In the second step the solutions of this generic system enable us to recover the solutions of the given system by means of a standard homotopic deformation (see Section 5.3).

In the first step, we partake to solve a system $h_1 = 0, \dots, h_n = 0$ with the same supports $\Delta_1, \dots, \Delta_n$ as $f_1, \dots, f_n$ but with generic coefficients, which are chosen randomly. In order to do this, the polyhedral homotopy of [HS95] introduces a new variable T and deforms each polynomial h_i by multiplying each nonzero monomial of h_i by a power of T (which is determined by the given lifting function). The roots of the resulting parametric system are algebraic functions of the parameter T whose expansions as Puiseux series can be obtained by "lifting" the solutions from certain associated zero-dimensional polynomial systems, which in turn can be easily solved due to their specific structure (see Section 5.2.4 for details). This enables us to compute a geometric solution of the zero set of this parametric system (Section 5.2.5). Substituting 1 for T in the computed polynomials we obtain a geometric solution of the set of common zeros of $h_1, \dots, h_n$ (Section 5.2.6).

For the sake of comprehensiveness, throughout Section 5.2 the whole first step of the algorithm will be illustrated with a bivariate polynomial example borrowed from [HS95, Example 2.7].

After solving the system $h_1 = 0, \dots, h_n = 0$, in the second step the solutions to the input system $f_1 = 0, \dots, f_n = 0$ are recovered by considering a second homotopy of type $Tf_1 + (1-T)h_1, \dots, Tf_n + (1-T)h_n$ (see Section 5.3). As in the first step, the algorithm first solves this parametric system (Section 5.3.1) and then, substituting 1 for T, a complete representation of the solution set of the input system is obtained. This representation eventually includes multiplicities, which are removed in a further computation (Section 5.3.2).

5.1. Sparse Elimination

Here we introduce some notions and notations of convex geometry and sparse elimination theory (see, e.g., [GKZ94], [HS95], [Roj03]) that will be used in the sequel.

Let $X_1, \dots, X_n$ be indeterminates over $\mathbb{Q}$ and write $X := (X_1, \dots, X_n)$. For $q := (q_1, \dots, q_n) \in \mathbb{Z}^n$, we use the notation $X^q := X_1^{q_1} \cdots X_n^{q_n}$. Let $f := \sum_q c_q X^q$ be a Laurent polynomial in $\mathbb{Q}[X,X^{-1}] := \mathbb{Q}[X_1,X_1^{-1},\dots,X_n,X_n^{-1}]$. By the support of f we understand the subset of $\mathbb{Z}^n$ defined by the elements $q \in \mathbb{Z}^n$ for which $c_q \neq 0$ holds. The Newton polytope of f is the convex hull of the support of f in $\mathbb{R}^n$.

A sparse polynomial system with supports $\Delta_1, \dots, \Delta_n \subset (\mathbb{Z}_{\geq 0})^n$ is defined by polynomials

$$f_i(X) := \sum_{q \in \Delta_i} a_{i,q} X^q \quad (1 \leq i \leq n),$$

with $a_{i,q} \in \mathbb{C} \setminus \{0\}$ for each $q \in \Delta_i$ and $1 \leq i \leq n$.

For a finite subset Δ of $\mathbb{Z}^n$, we denote by $Q := \mathrm{Conv}(\Delta)$ its convex hull in $\mathbb{R}^n$. The usual Euclidean volume of a polytope Q in $\mathbb{R}^n$ will be denoted by $\mathrm{Vol}_{\mathbb{R}^n}(Q)$.

Let $Q_1, \dots, Q_n$ be polytopes in $\mathbb{R}^n$. For $\lambda_1, \dots, \lambda_n \in \mathbb{R}_{\geq 0}$, we use the notation $\lambda_1 Q_1 + \cdots + \lambda_n Q_n$ to refer to the Minkowski sum $\lambda_1 Q_1 + \cdots + \lambda_n Q_n := \{x \in \mathbb{R}^n : x = \lambda_1 x_1 + \cdots + \lambda_n x_n \text{ with } x_1 \in Q_1, \dots, x_n \in Q_n\}$. Consider the real-valued function $(\lambda_1, \dots, \lambda_n) \mapsto \mathrm{Vol}_{\mathbb{R}^n}(\lambda_1 Q_1 + \cdots + \lambda_n Q_n)$. This is a homogeneous polynomial function of degree n in the λ_i (see, e.g., [CLO98, Chapter 7, Proposition §4.4.9]). The **mixed volume** $\mathcal{M}(Q_1, \dots, Q_n)$ of $Q_1, \dots, Q_n$ is defined as the coefficient of the monomial $\lambda_1 \cdots \lambda_n$ in $\mathrm{Vol}_{\mathbb{R}^n}(\lambda_1 Q_1 + \cdots + \lambda_n Q_n)$.

For $i = 1, \dots, n$, let Δ_i be a finite subset of $\mathbb{Z}^n_{\geq 0}$ and let $Q_i := \mathrm{Conv}(\Delta_i)$ denote the corresponding polytope. Let $f_1, \dots, f_n$ be a sparse polynomial system with respect to $\Delta_1, \dots, \Delta_n$. The BKK Theorem ([Ber75], [Kus76], [Kho78]) asserts that the system $f_1 = 0, \dots, f_n = 0$ has at most $\mathcal{M}(Q_1, \dots, Q_n)$ isolated common solutions in the n-dimensional torus $(\mathbb{C}^*)^n$, with equality for generic choices of the coefficients of $f_1, \dots, f_n$. Furthermore, if the condition $0 \in Q_i$ holds for $1 \leq i \leq n$, then $\mathcal{M}(Q_1, \dots, Q_n)$ bounds the number of solutions in $\mathbb{C}^n$ (see [LW96]).

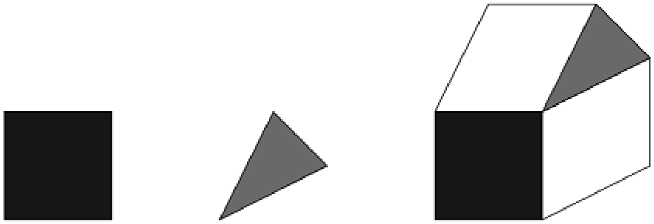
Example. Let $\Delta_1 := \{(0,0), (2,0), (0,2), (2,2)\}$ and $\Delta_2 := \{(0,0), (1,2), (2,1)\}$ in $\mathbb{Z}^2$. A sparse polynomial system with supports Δ_1, Δ_2 is a system defined by polynomials of the following type:

$$\begin{cases} f_1 = a_{(0,0)} + a_{(2,0)} X_1^2 + a_{(0,2)} X_2^2 + a_{(2,2)} X_1^2 X_2^2, \\ f_2 = b_{(0,0)} + b_{(1,2)} X_1 X_2^2 + b_{(2,1)} X_1^2 X_2, \end{cases} \tag{5.1}$$

with a_q, $b_q \in \mathbb{C} \setminus \{0\}$.

Let $Q_1 := \mathrm{Conv}(\Delta_1)$ and $Q_2 := \mathrm{Conv}(\Delta_2)$. Then $\mathcal{M}(Q_1, Q_2) = \mathrm{Vol}_{\mathbb{R}^2}(Q_1 + Q_2) - \mathrm{Vol}_{\mathbb{R}^2}(Q_1) - \mathrm{Vol}_{\mathbb{R}^2}(Q_2) = 8$.

The pictures of Q_1, Q_2 and $Q_1 + Q_2$ are respectively:



5.1.1. Mixed subdivisions

Assume that the union of the sets $\Delta_1, \ldots, \Delta_n$ affinely generates $\mathbb{Z}^n$, and consider the partition of $\Delta_1, \ldots, \Delta_n$ defined by the relation $\Delta_i \sim \Delta_j$ if and only if $\Delta_i = \Delta_j$. Let $s \in \mathbb{N}$ denote the number of classes in this partition, and let $\mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(s)} \subset \mathbb{Z}^n$ denote a member in each class. Write $\mathcal{A} := (\mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(s)})$. For $\ell = 1, \ldots, s$, let $k_\ell := \#\{i : \Delta_i = \mathcal{A}^{(\ell)}\}$. Without loss of generality, we will assume that $\Delta_1 = \cdots = \Delta_{k_1} = \mathcal{A}^{(1)}$, $\Delta_{k_1+1} = \cdots = \Delta_{k_1+k_2} = \mathcal{A}^{(2)}$ and so on.

A cell of $\mathcal{A}$ is a tuple $C = (C^{(1)}, \ldots, C^{(s)})$ with $C^{(\ell)} \neq \emptyset$ and $C^{(\ell)} \subset \mathcal{A}^{(\ell)}$ for $1 \leq \ell \leq s$. We define

$$\begin{aligned} \mathit{type}(C) &:= (\dim(\mathrm{Conv}(C^{(1)})), \ldots, \dim(\mathrm{Conv}(C^{(s)}))), \\ \mathrm{Conv}(C) &:= \mathrm{Conv}(C^{(1)} + \cdots + C^{(s)}), \\ \#(C) &:= \#(C^{(1)}) + \cdots + \#(C^{(s)}), \\ \mathrm{Vol}_{\mathbb{R}^n}(C) &:= \mathrm{Vol}_{\mathbb{R}^n}(\mathrm{Conv}(C)). \end{aligned}$$

A face of a cell C is a cell $\mathcal{C} = (\mathcal{C}^{(1)}, \ldots, \mathcal{C}^{(s)})$ of C with $\mathcal{C}^{(\ell)} \subset C^{(\ell)}$ for $1 \leq \ell \leq s$ such that there exists a linear functional $\gamma : \mathbb{R}^n \to \mathbb{R}$ that takes its minimum over $C^{(\ell)}$ at $\mathcal{C}^{(\ell)}$ for $1 \leq \ell \leq s$. One such functional γ is called an inner normal of C.

A mixed subdivision of $\mathcal{A}$ is a collection of cells $\mathfrak{C} = \{C_1, \ldots, C_m\}$ of $\mathcal{A}$ satisfying conditions (1)–(4) below.

1. $\dim(\mathrm{Conv}(C_j)) = n$ for $1 \leq j \leq m$,
2. the intersection $\mathrm{Conv}(C_i) \cap \mathrm{Conv}(C_j) \subset \mathbb{R}^n$ is either the empty set or a face of both $\mathrm{Conv}(C_i)$ and $\mathrm{Conv}(C_j)$ for $1 \leq i < j \leq m$,
3. $\bigcup_{j=1}^m \mathrm{Conv}(C_j) = \mathrm{Conv}(\mathcal{A})$,
4. $\sum_{\ell=1}^s \dim(\mathrm{Conv}(C_j^{(\ell)})) = n$ for $1 \leq j \leq m$.

If $\mathfrak{C}$ also satisfies the condition

5. $\#(C_j) = n + s$ for $1 \leq j \leq m$,

we say that $\mathfrak{C}$ is a fine-mixed subdivision of $\mathcal{A}$. Observe that, as a consequence of conditions (4) and (5), for each cell $C_j = (C_j^{(1)}, \ldots, C_j^{(s)})$ in a fine-mixed subdivision the identity $\dim(\mathrm{Conv}(C_j^{(\ell)})) = \#C_j^{(\ell)} - 1$ holds for $1 \leq \ell \leq s$. In the sequel, we are going to consider only cells of type $(k_1, \ldots, k_s)$ in a fine-mixed subdivision.

We point out that a mixed subdivision $\mathfrak{C}$ of $\mathcal{A}$ enables us to compute the mixed volume of the family $Q_1 = \mathrm{Conv}(\Delta_1), \ldots, Q_n = \mathrm{Conv}(\Delta_n)$ by means of the following identity (see [HS95, Theorem 2.4.]):

$$\mathcal{M}(Q_1, \ldots, Q_n) = \sum_{\substack{C_i \in \mathfrak{C} \\ \mathrm{type}(C_i) = (k_1, \ldots, k_s)}} k_1! \ldots k_s! \cdot \mathrm{Vol}_{\mathbb{R}^n}(C_i). \tag{5.2}$$

A fine-mixed subdivision of $\mathcal{A}$ can be obtained by means of a lifting process as explained in what follows. For $1 \leq \ell \leq s$, let $\omega_\ell : \mathcal{A}^{(\ell)} \to \mathbb{R}$ be an arbitrary function. The tuple $\omega := (\omega_1, \ldots, \omega_s)$ is called a lifting function for $\mathcal{A}$. Once a lifting function ω is fixed, the graph of any subset $C^{(\ell)}$ of $\mathcal{A}^{(\ell)}$ will be denoted by $\widehat{C}^{(\ell)} := \{(q, \omega_\ell(q)) \in \mathbb{R}^{n+1} : q \in C^{(\ell)}\}$. Then, for a sufficiently generic lifting function ω, the set of cells C of $\mathcal{A}$ satisfying the following conditions.

i. $\dim(\mathrm{Conv}(\widehat{C}^{(1)} + \cdots + \widehat{C}^{(s)})) = n$,

ii. $(\widehat{C}^{(1)}, \ldots, \widehat{C}^{(s)})$ is a face of $(\widehat{\mathcal{A}}^{(1)}, \ldots, \widehat{\mathcal{A}}^{(s)})$ whose inner normal has positive last coordinate,

is a fine-mixed subdivision of $\mathcal{A}$ (see [HS95, Section 2]).

Example. We continue with the example introduced at the end of the previous subsection. Here $\mathcal{A} := (\mathcal{A}^{(1)}, \mathcal{A}^{(2)})$, where $\mathcal{A}^{(1)} := \Delta_1$ and $\mathcal{A}^{(2)} := \Delta_2$.

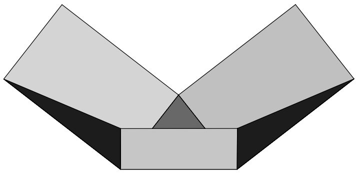
Following [HS95, Example 2.7], the lifting function $\omega = (\omega_1, \omega_2)$ defined by

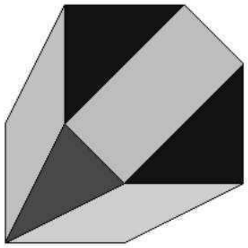
$$\omega_1(q) := \begin{cases} 0 & \text{for } q = (0,0) \\ 1 & \text{for } q \in \mathcal{A}^{(1)} \setminus \{(0,0)\} \end{cases} \quad \text{and} \quad \omega_2(q) := 0 \text{ for every } q \in \mathcal{A}^{(2)}, \tag{5.3}$$

induces a fine-mixed subdivision of $\mathcal{A}$. More precisely, such a fine–mixed subdivision consists of the set of cells satisfying conditions (i) and (ii) above, which are listed below together with the inner normals of the faces they come from:

- $C_1 := \{\{(0,0),(0,2)\},\{(0,0),(1,2)\}\}$, $\gamma^{(1)} := (2,-1,2)$.
- $C_2 := \{\{(0,0),(2,0)\},\{(0,0),(2,1)\}\}$, $\gamma^{(2)} := (-1,2,2)$.
- $C_3 := \{\{(0,0),(2,2)\},\{(1,2),(2,1)\}\}$, $\gamma^{(3)} := (-1,-1,4)$.
- $C_4 := \{\{(0,0)\},\{(0,0),(1,2),(2,1)\}\}$, $\gamma^{(4)} := (0,0,1)$.
- $C_5 := \{\{(0,0),(0,2),(2,2)\},\{(1,2)\}\}$, $\gamma^{(5)} := (0,-1,2)$.
- $C_6 := \{\{(0,0),(2,0),(2,2)\},\{(2,1)\}\}$, $\gamma^{(6)} := (-1,0,2)$.

The pictures below show the lower envelope of $\widehat{\mathcal{A}}^{(1)} + \widehat{\mathcal{A}}^{(2)} \subset \mathbb{R}^3$ and its projection to $\mathbb{R}^2$ respectively.





Note that the cells of type $(k_1,k_2) = (1,1)$ are C_1, C_2 and C_3.

The following result (cf. [HS95, Section 2]) states a generic condition for a lifting function to induce a fine-mixed subdivision:

Lemma 5.2. *The lifting process associated to a lifting function ω yields a fine-mixed subdivision of $\mathcal{A}$ if the following condition holds: for every $r_1,\ldots,r_s \in \mathbb{Z}_{\geq 0}$ with $\sum_{\ell=1}^{s} r_\ell > n$ and every cell $(C^{(1)},\ldots,C^{(s)})$ with $C^{(\ell)} :=$*

$\{q_{\ell,0},\dots,q_{\ell,r_\ell}\}\subset\mathcal{A}^{(\ell)}$ $(1\leq\ell\leq s)$, *if*

$$V(C):=\begin{pmatrix} q_{1,1}-q_{1,0}\\ \vdots\\ q_{1,r_1}-q_{1,0}\\ \cdots\\ \cdots\\ q_{s,1}-q_{s,0}\\ \vdots\\ q_{s,r_s}-q_{s,0}\end{pmatrix}\quad \textit{and}\, V(\widehat{C}):=\begin{pmatrix} q_{1,1}-q_{1,0} & \omega_1(q_{1,1})-\omega_1(q_{1,0})\\ \vdots & \vdots\\ q_{1,r_1}-q_{1,0} & \omega_1(q_{1,r_1})-\omega_1(q_{1,0})\\ \cdots & \cdots\\ \cdots & \cdots\\ q_{s,1}-q_{s,0} & \omega_s(q_{s,1})-\omega_s(q_{s,0})\\ \vdots & \vdots\\ q_{s,r_s}-q_{s,0} & \omega_s(q_{s,r_s})-\omega_s(q_{s,0})\end{pmatrix},$$

then $\operatorname{rank}(V(C))=n$ *implies* $\operatorname{rank}(V(\widehat{C}))=n+1$.

Note that the condition $\operatorname{rank}(V(\widehat{C}))=n+1$ can be restated as the non-vanishing of the maximal minors of the matrix $V(\widehat{C})$. Since $\operatorname{rank}(V(C))=n$, these maximal minors are nonzero linear forms in the unknown values $\omega_\ell(q_{\ell,j})$ of the lifting function. Thus, if $\mathcal{N}_\ell=\#\mathcal{A}^{(\ell)}$ for every $1\leq\ell\leq s$, a sufficiently generic lifting function can be obtained by randomly choosing the values $\omega_\ell(q_{\ell,j})$ of ω at the points of $\mathcal{A}^{(\ell)}$ from the set $\{1,2,\dots,\rho 2^{\mathcal{N}_1+\cdots+\mathcal{N}_s}\}$, with probability of success at least $1-1/\rho$ for $\rho\in\mathbb{N}$.

In this chapter, we shall assume given a sufficiently generic lifting function and the induced fine-mixed subdivision of $\mathcal{A}$.

5.1.2. Degree estimates in the sparse setting

Suppose that we are given a curve $V\subset\mathbb{A}^{n+1}(\mathbb{C})$ defined by polynomials $f_1,\dots,f_n\in\mathbb{Q}[X,T]$. Assume that for each irreducible component C of V, the identity $I(C)\cap\mathbb{Q}[T]=\{0\}$ holds. Let u be a nonzero linear form of $\mathbb{Q}[X]$ and $\pi_u: V\to\mathbb{A}^2$ the morphism defined by $\pi_u(x,t):=(t,u(x))$.

Our assumptions on V imply that the Zariski closure $\overline{\pi_u(V)}$ of the image of V under π_u is an hypersurface of $\mathbb{A}^2$ defined over $\mathbb{Q}$, and hence, there exists a unique (up to scaling by nonzero elements of $\mathbb{Q}$) polynomial $M_u\in\mathbb{Q}[T,Y]$ of minimal degree defining $\overline{\pi_u(V)}$. Let $m_u\in\mathbb{Q}(T)[Y]$ denote the (unique) monic multiple of M_u with $\deg_Y(m_u)=\deg_Y(M_u)$; so m_u is the minimal polynomial of u in V.

As in the previous chapters, the complexity of the algorithms for solving a system $f_1 = 0, \ldots, f_n = 0$ defining such a curve can be expressed mainly by means of the *degree* and *height* of the projection $\pi_u : V \to \mathbb{A}^1$. The degree of π_u is equal to the degree $\deg m_u = \deg_Y M_u$ of the minimal polynomial of a generic linear form $u \in \mathbb{Q}[X_1, \ldots, X_n]$ and the height of π_u is equal to the partial degree $\deg_T M_u$ (see Section 2.4).

In the sparse setting, we can estimate $\deg_Y M_u$ and $\deg_T M_u$ in terms of combinatorial quantities (namely, mixed volumes) associated to the polynomial system under consideration (see also [PS08]).

Lemma 5.3. *Let assumptions and notations be as above. For $1 \leq i \leq n$, let $Q_i \subset \mathbb{R}^n$ be the Newton polytope of f_i, considering f_i as an element of $\mathbb{Q}(T)[X]$. Let $\widehat{Q}_1, \ldots, \widehat{Q}_n \subset \mathbb{R}^{n+1}$ be the Newton polytopes of $f_1, \ldots, f_n$, considering $f_1, \ldots, f_n$ as elements of $\mathbb{Q}[X, T]$, and let $\Delta \subset \mathbb{R}^{n+1}$ be the standard n-dimensional simplex in the hyperplane $\{T = 0\}$, i.e., the Newton polytope of a generic linear form $u \in \mathbb{Q}[X]$. Assume that $0 \in \widehat{Q}_i$ for every $1 \leq i \leq n$. Then the following estimates hold:*

$$\deg_Y M_u \leq \mathcal{M}(Q_1, \ldots, Q_n), \quad \deg_T M_u \leq \mathcal{M}(\Delta, \widehat{Q}_1, \ldots, \widehat{Q}_n). \tag{5.4}$$

Furthermore, if there exist $c_1, \ldots, c_n \in \mathbb{R}_{\geq 0}$ such that $\widehat{Q}_i \subset Q_i \times [0, c_i]$ for $1 \leq i \leq n$, then the following inequality holds:

$$\deg_T M_u \leq \sum_{i=1}^{n} c_i \, \mathcal{M}(\Delta, Q_1, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n). \tag{5.5}$$

Proof. The upper bound $\deg_Y M_u \leq \mathcal{M}(Q_1, \ldots, Q_n)$ follows straightforwardly from the BKK bound and the affine root count in [LW96].

In order to obtain an upper bound for $\deg_T M_u$, we observe that substituting a generic value $y \in \mathbb{Q}$ for Y we have $\deg_T M_u(T,Y) = \deg_T M_u(T, y) = \#\{t \in \mathbb{C}; M_u(t, y) = 0\}$. Moreover, it follows that $M_u(t, y) = 0$ if and only if there exists a point $x \in \mathbb{A}^n$ with $y = u(x)$ and $(x, t) \in V$. Therefore, it suffices to estimate the number of points $(x, t) \in \mathbb{A}^{n+1}$ satisfying $u(x) - y = 0, f_1(x, t) = 0, \ldots, f_n(x, t) = 0$. Being u a generic linear form, the system

$$u(X) - y = 0, f_1(X, T) = 0, \ldots, f_n(X, T) = 0 \tag{5.6}$$

has finitely many common zeros in $\mathbb{A}^{n+1}$. Combining the BKK bound with the affine root count of [LW96] we see that there are at most $\mathcal{M}(\Delta, \widehat{Q}_1, \ldots, \widehat{Q}_n)$

solutions of (5.6). We conclude that $\deg_T M_u \leq \mathcal{M}(\Delta, \widehat{Q}_1, \ldots, \widehat{Q}_n)$ holds, showing thus (5.4).

In order to prove (5.5), we make use of basic properties of the mixed volume (see, for instance, [Ewa96, Ch. IV]). Since $\widehat{Q}_i \subset Q_i \times [0, c_i]$ holds for $1 \leq i \leq n$, by the monotonicity of the mixed volume we have

$$\mathcal{M}(\Delta, \widehat{Q}_1, \ldots, \widehat{Q}_n) \leq \mathcal{M}(\Delta, Q_1 \times [0, c_1], \ldots, Q_n \times [0, c_n]).$$

Note that $Q_i \times [0, c_i] = S_{i,0} + S_{i,1}$, where $S_{i,0} = Q_i \times \{0\}$ and $S_{i,1} = \{0\} \times [0, c_i]$ for $i = 1, \ldots, n$. Hence, by multilinearity,

$$\mathcal{M}(\Delta, Q_1 \times [0, c_1], \ldots, Q_n \times [0, c_n]) = \sum_{(j_1, \ldots, j_n) \in \{0,1\}^n} \mathcal{M}(\Delta, S_{1,j_1}, \ldots, S_{n,j_n}). \quad (5.7)$$

If the vector $(j_1, \ldots, j_n)$ has at least two nonzero coordinates, then two of the sets $S_{1,j_1}, \ldots, S_{n,j_n}$ are parallel line segments; therefore, $\mathcal{M}(\Delta, S_{1,j_1}, \ldots, S_{n,j_n}) = 0$. On the other hand, if j_i is the only nonzero coordinate, the corresponding term in the sum of the right-hand side of (5.7) is

$$\begin{aligned}\mathcal{M}(\Delta, Q_1 \times \{0\}, \ldots, Q_{i-1} \times \{0\}, \{0\} \times [0, c_i], Q_{i+1} \times \{0\}, \ldots, Q_n \times \{0\}) \\ = c_i\, \mathcal{M}(\Delta, Q_1, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n).\end{aligned}$$

Finally, for $(j_1 \ldots, j_n) = (0, \ldots, 0)$ we have $\mathcal{M}(\Delta, Q_1 \times \{0\}, \ldots, Q_n \times \{0\}) = 0$ since all the polytopes are included in an n-dimensional subspace.

We conclude that the right-hand side of (5.7) equals the right-hand side of (5.5). This finishes the proof of the lemma. □

Example. For the system

$$\begin{cases} a_{(0,0)} + a_{(2,0)} X_1^2 T + a_{(0,2)} X_2^2 T + a_{(2,2)} X_1^2 X_2^2 T = 0, \\ b_{(0,0)} + b_{(1,2)} X_1 X_2^2 + b_{(2,1)} X_1^2 X_2 = 0, \end{cases} \quad (5.8)$$

we have:

- $Q_1 = \mathrm{Conv}(\{(0,0), (0,2), (2,0), (2,2)\})$,
- $Q_2 = \mathrm{Conv}(\{(0,0), (1,2), (2,1)\})$,

- $\widehat{Q}_1 = \mathrm{Conv}(\{(0,0,0),(0,2,1),(2,0,1),(2,2,1)\})$,
- $\widehat{Q}_2 = \mathrm{Conv}(\{(0,0,0),(1,2,0),(2,1,0)\})$.

Therefore, the following upper bounds for the degree of the polynomial M_u hold for any separating linear form u:

$$\deg_Y M_u \leq \mathcal{M}(Q_1, Q_2) = 8 =: D, \tag{5.9}$$

$$\deg_T M_u \leq \mathcal{M}(\Delta, \widehat{Q}_1, \widehat{Q}_2) = 3 =: E, \tag{5.10}$$

where $\Delta := \mathrm{Conv}(\{(0,0,1),(1,0,0),(0,1,0)\})$.

5.2. Solution of a generic sparse system

Let $\Delta_1, \ldots, \Delta_n$ be fixed finite subsets of $\mathbb{Z}^n_{\geq 0}$ with $0 \in \Delta_i$ for $1 \leq i \leq n$ and let $D := \mathcal{M}(Q_1, \ldots, Q_n)$ denote the mixed volume of the polytopes $Q_1 := \mathrm{Conv}(\Delta_1), \ldots, Q_n := \mathrm{Conv}(\Delta_n)$. Assume that $D > 0$ holds or, equivalently, that $\dim\left(\sum_{i\in I} Q_i\right) \geq |I|$ for every non-empty subset $I \subset \{1, \ldots, n\}$ (see, for instance, [Oka97, Chapter IV, Proposition 2.3]).

Let $f_1, \ldots, f_n \in \mathbb{Q}[X]$ be polynomials defining a sparse system with respect to $\Delta_1, \ldots, \Delta_n$ and let $d_1, \ldots, d_n$ be their total degrees. Let $d := \max\{d_1, \ldots, d_n\}$. Suppose that $f_1, \ldots, f_n$ define a zero-dimensional variety V in $\mathbb{A}^n$. Group equal supports into $s \leq n$ distinct supports and define representatives as $\mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(s)}$ as we did in the previous section. Write $\mathcal{A} := (\mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(s)})$ and denote by k_ℓ the number of polynomials f_i with support $\mathcal{A}^{(\ell)}$ for $1 \leq \ell \leq s$.

From now on we assume that we are given a sufficiently generic lifting function $\omega := (\omega_1, \ldots, \omega_s)$ and the fine-mixed subdivision of $\mathcal{A}$ induced by ω. We assume further that, for every $1 \leq \ell \leq s$, the function $\omega_\ell : \mathcal{A}^{(\ell)} \to \mathbb{Z}$ takes only nonnegative values and $\omega_\ell(0, \ldots, 0) = 0$.

We introduce auxiliary *generic* polynomials $g_1, \ldots, g_n$ with the same supports $\Delta_1, \ldots, \Delta_n$ (satisfying a geometric condition to be made explicit in Section 5.2.1) and consider the perturbed polynomial system defined by $h_1 := f_1 + g_1, \ldots, h_n := f_n + g_n$. We observe that if the coefficients of the polynomials $f_1, \ldots, f_n$ satisfy this condition then our symbolic adaptation of Huber-Sturmfels method can be applied directly to $f_1, \ldots, f_n$. Otherwise, we first solve the system $h_1 = 0, \ldots, h_n = 0$ using the method to be discussed below and then recover the solutions to the input system $f_1 = 0, \ldots, f_n = 0$ by considering the standard homotopy $f_1+(1-T)g_1 = 0, \ldots, f_n+(1-T)g_n = 0$.

5.2.1. The polyhedral deformation

This section is devoted to introducing the polyhedral deformation of Huber and Sturmfels.

Let us maintain notions and notations from the previous section. Let $h_i := \sum_{q\in\Delta_i} c_{i,q}X^q$ for $1 \leq i \leq n$ be polynomials in $\mathbb{Q}[X]$, where $\Delta_1, \ldots, \Delta_n$ are the supports introduced in Section 5.2 and let V_1 denote the set of their common zeros in $\mathbb{A}^n$. For $i = 1, \ldots, n$, let ℓ_i be the (unique) integer with $\Delta_i = \mathcal{A}^{(\ell_i)}$, and let $\widetilde{\omega}_i := \omega_{\ell_i}$ be the lifting function associated to the support Δ_i. In order to simplify notations, the n-tuple $\widetilde{\omega} := (\widetilde{\omega}_1, \ldots, \widetilde{\omega}_n)$ will be denoted simply by $\omega = (\omega_1, \ldots, \omega_n)$.

As done before, we denote by $\widehat{C}^{(\ell)} := \{(q, \omega_\ell(q)) \in \mathbb{R}^{n+1} : q \in C^{(\ell)}\}$ the graph of any subset $C^{(\ell)}$ of $\mathcal{A}^{(\ell)}$ for $1 \leq \ell \leq s$, and extend this notation correspondingly. Let T be a new indeterminate. We consider a "deformation" of the polynomials $h_1, \ldots, h_n$ into polynomials $\widehat{h}_1, \ldots, \widehat{h}_n \in \mathbb{Q}[X, T]$ defined in the following way:

$$\widehat{h}_i(X,T) := \sum_{q\in\Delta_i} c_{i,q}X^qT^{\omega_i(q)} \quad \text{for } 1 \leq i \leq n. \tag{5.11}$$

Let I denote the ideal of $\mathbb{Q}[X, T]$ generated by $\widehat{h}_1, \ldots, \widehat{h}_n$ and let J denote the Jacobian determinant of $\widehat{h}_1, \ldots, \widehat{h}_n$ with respect to the variables $X_1, \ldots, X_n$. We set

$$\widehat{V} := V(I : J^\infty) \subset \mathbb{A}^{n+1}. \tag{5.12}$$

We shall show that, under a generic choice of the coefficients of $h_1, \ldots, h_n$, the system defined by the polynomials in (5.11) constitutes a deformation of the input system $h_1 = 0, \ldots, h_n = 0$, in the sense that the morphism $\pi : \widehat{V} \to \mathbb{A}^1$ defined by $\pi(x,t) := t$ is a dominant map with $\pi^{-1}(1) = V_1 \times \{1\}$.

We shall further exhibit degree estimates on the genericity condition underlying such choice of coefficients. These estimates will allow us to obtain suitable polynomials $h_1, \ldots, h_n$ by randomly choosing their coefficients in an appropriate finite subset of $\mathbb{Z}$.

According to [HS95, Section 3], the solutions over an algebraic closure $\overline{\mathbb{Q}(T)}$ of $\mathbb{Q}(T)$ to the system defined by the polynomials (5.11) are algebraic functions of the parameter T which can be represented as Puiseux series of the form

$$x(T) := (x_{1,0}T^{\frac{\gamma_1}{\gamma_{n+1}}} + \text{higher-order terms}, \dots, x_{n,0}T^{\frac{\gamma_n}{\gamma_{n+1}}} + \text{higher-order terms}), \tag{5.13}$$

where $\gamma := (\gamma_1, \dots, \gamma_n, \gamma_{n+1}) \in \mathbb{Z}^{n+1}$ is an inner normal with positive last coordinate $\gamma_{n+1} > 0$ of a (lower) facet $\widehat{C} = (\widehat{C}^{(1)}, \dots, \widehat{C}^{(s)})$ of $\widehat{\mathcal{A}}$ of type $(k_1, \dots, k_s)$, and $x_0 := (x_{1,0}, \dots, x_{n,0}) \in (\mathbb{C}^*)^n$ is a solution to the polynomial system defined by

$$h_{i,\gamma}^{(0)} := \sum_{q \in C^{(\ell_i)}} c_{i,q} X^q \qquad (1 \leq i \leq n), \tag{5.14}$$

where, as defined before, ℓ_i is the integer with $1 \leq \ell_i \leq s$ such that $\Delta_i = \mathcal{A}^{(\ell_i)}$. For a generic choice of the coefficients of the polynomials $h_1, \dots, h_n$ there are $k_1! \cdots k_s! \cdot \mathrm{Vol}(C)$ distinct solutions $x_0 \in (\mathbb{C}^*)^n$ to the system defined by the polynomials (5.14) and hence, there are $k_1! \cdots k_s! \cdot \mathrm{Vol}(C)$ distinct Puiseux series $x(T)$ as in (5.13).

We shall "lift" each of these solutions x_0 to a solution of the form (5.13) to the system defined by (5.11). Explicitly, on input x_0, we shall compute the Puiseux series expansion of the corresponding solution (5.13) truncated up to a suitable order.

Let

$$V_{0,\gamma} := \{x \in (\mathbb{C}^*)^n : h_{1,\gamma}^{(0)}(x) = 0, \dots, h_{n,\gamma}^{(0)}(x) = 0\}. \tag{5.15}$$

A particular feature of the polynomials (5.14) which makes the associated equation system "easy to solve" is that the vector of their supports is $(C^{(1)})^{k_1} \times \cdots \times (C^{(s)})^{k_s}$, where $(C^{(1)}, \dots, C^{(s)})$ is a cell of type $(k_1, \dots, k_s)$ in a fine-mixed subdivision of $\mathcal{A}$. Therefore, for every $1 \leq \ell \leq s$, the set $C^{(\ell)}$ consists of $k_\ell + 1$ points and hence, the (Laurent) polynomials in (5.14) are linear combinations of $n+1$ distinct monomials in n variables (up to monomial multiplication so that each polynomial has a nonzero constant term).

Denote $\Gamma \subset \mathbb{Z}^{n+1}$ the set of all primitive integer vectors of the form $\gamma := (\gamma_1, \dots, \gamma_n, \gamma_{n+1}) \in \mathbb{Z}^{n+1}$ with $\gamma_{n+1} > 0$ for which there is a cell $C = (C^{(1)}, \dots, C^{(s)})$ of type $(k_1, \dots, k_s)$ of the subdivision of $\mathcal{A}$ induced by ω such that $\widehat{C}$ has inner normal γ.

Fix a cell $C = (C^{(1)}, \dots, C^{(s)})$ of type $(k_1, \dots, k_s)$ of the subdivision of $\mathcal{A}$ induced by ω associated with a primitive inner normal $\gamma \in \Gamma$ with positive last coordinate. In order to lift the points of the variety $V_{0,\gamma}$ of (5.15) to a solution of the system defined by the polynomials in (5.11), we will work with a family of auxiliary polynomials $h_{1,\gamma}, \dots, h_{n,\gamma} \in \mathbb{Q}[X, T]$ which we define as follows:

$$h_{i,\gamma}(X, T) := T^{-m_i} \widehat{h}_i(T^{\gamma_1} X_1, \dots, T^{\gamma_n} X_n, T^{\gamma_{n+1}}) \quad (1 \le i \le n) \tag{5.16}$$

where $m_i \in \mathbb{Z}$ is the lowest power of T appearing in $\widehat{h}_i(T^{\gamma_1} X_1, \dots, T^{\gamma_n} X_n, T^{\gamma_{n+1}})$ for every $1 \le i \le n$. Note that the polynomials obtained by substituting $T = 0$ into $h_{1,\gamma}, \dots, h_{n,\gamma}$ are precisely those introduced in (5.14). Now we illustrate the objects introduced in this subsection with a particular sparse polynomial system with the same structure as the generic system (5.1).

Example. Consider the polynomials $h_1, h_2 \in \mathbb{Q}[X_1, X_2]$ defined as:

$$\begin{cases} h_1 := 1 - X_1^2 - X_2^2 - X_1^2 X_2^2, \\ h_2 := 1 + X_1^2 X_2 + X_1 X_2^2. \end{cases} \tag{5.17}$$

Observe that the polynomials above are a specialization of the generic polynomials introduced in (5.1).

We deform the polynomials h_1, h_2 using the lifting function ω defined in (5.3), obtaining thus the following polynomials:

$$\begin{cases} \widehat{h}_1 := 1 - X_1^2 T - X_2^2 T - X_1^2 X_2^2 T, \\ \widehat{h}_2 := 1 + X_1^2 X_2 + X_1 X_2^2. \end{cases} \tag{5.18}$$

These polynomials $\widehat{h}_1$, $\widehat{h}_2$ define the curve

$$\widehat{V} := V((\widehat{h}_1, \widehat{h}_2) : J^\infty) = V(\widehat{h}_1, \widehat{h}_2), \tag{5.19}$$

where J is the Jacobian determinant of $\widehat{h}_1$ and $\widehat{h}_2$ with respect to the variables X_1, X_2.

According to the remark at the end of the example of Subsection 5.1.1, the cells of type $(1, 1)$ in the fine-mixed subdivision of the support sets induced by ω, and the corresponding inner normals are:

- $C_1 := \{\{(0,0),(0,2)\},\{(0,0),(1,2)\}\}$, $\gamma^{(1)} := (2,-1,2)$.
- $C_2 := \{\{(0,0),(2,0)\},\{(0,0),(2,1)\}\}$, $\gamma^{(2)} := (-1,2,2)$.
- $C_3 := \{\{(0,0),(2,2)\},\{(1,2),(2,1)\}\}$, $\gamma^{(3)} := (-1,-1,4)$.

Therefore, the polynomial systems defined by the polynomials $h_{i,\gamma}^{(0)}$ of (5.14) and their solution sets $V_{0,\gamma}$ are:

$$\begin{cases} h_{1,\gamma^{(1)}}^{(0)} = 1 - X_2^2, \\ h_{2,\gamma^{(1)}}^{(0)} = 1 + X_1X_2^2, \end{cases} \qquad V_{0,\gamma^{(1)}} = \{(-1,1),(-1,-1)\}, \tag{5.20}$$

$$\begin{cases} h_{1,\gamma^{(2)}}^{(0)} = 1 - X_1^2, \\ h_{2,\gamma^{(2)}}^{(0)} = 1 + X_1^2X_2, \end{cases} \qquad V_{0,\gamma^{(2)}} = \{(1,-1),(-1,-1)\}, \tag{5.21}$$

$$\begin{cases} h_{1,\gamma^{(3)}}^{(0)} = 1 - X_1^2X_2^2, \\ h_{2,\gamma^{(3)}}^{(0)} = X_1^2X_2 + X_1X_2^2, \end{cases} \qquad V_{0,\gamma^{(3)}} = \{(1,-1),(-1,1),(i,-i),(-i,i)\}. \tag{5.22}$$

Finally, the polynomials $h_{i,\gamma}$ defined in (5.16) are:

$$\begin{cases} h_{1,\gamma^{(1)}} = 1 - X_1^2T^6 - X_2^2 - X_1^2X_2^2T^4, \\ h_{2,\gamma^{(1)}} = 1 + X_1^2X_2T^3 + X_1X_2^2, \end{cases} \tag{5.23}$$

$$\begin{cases} h_{1,\gamma^{(2)}} = 1 - X_1^2 - X_2^2T^6 - X_1^2X_2^2T^4, \\ h_{2,\gamma^{(2)}} = 1 + X_1^2X_2 + X_1X_2^2T^3, \end{cases} \tag{5.24}$$

$$\begin{cases} h_{1,\gamma^{(3)}} = 1 - X_1^2T^2 - X_2^2T^2 - X_1^2X_2^2, \\ h_{2,\gamma^{(3)}} = T^3 + X_1^2X_2 + X_1X_2^2. \end{cases} \tag{5.25}$$

5.2.2. On the genericity of the initial system

Here we discuss the genericity conditions underlying the choice of the polynomials $g_1, \dots, g_n$ that enable us to apply the polyhedral deformation defined by the lifting form ω to the system $h_1 := f_1 + g_1 = 0, \dots, h_n := f_n + g_n = 0$.

The first condition we require is that the set of common zeros of the perturbed polynomials $h_1, \dots, h_n$ is a zero-dimensional variety with the maximum number of points for a sparse system with the given structure. More precisely, we require that the following condition holds.

(H1) The set $V_1 := \{x \in \mathbb{A}^n : h_1(x) = 0, \dots, h_n(x) = 0\}$ is a zero-dimensional variety with $D := \mathcal{M}(Q_1, \dots, Q_n)$ distinct points.

In addition, we need that the system (5.14) giving the initial points to our first deformation for every $\gamma \in \Gamma$ has as many roots as possible, namely the mixed volume of their support vectors.

For each cell $C = (C^{(1)}, \dots, C^{(s)})$ of type $(k_1, \dots, k_s)$ of the induced fine-mixed subdivision, set an order on the $n+1$ points appearing in any of the sets $C^{(\ell)}$, after a suitable translation so that $0 \in C^{(\ell)}$ for every $1 \leq \ell \leq s$. Assume that $0 \in \mathbb{Z}^n$ is the last point according to this order. Denote $\gamma \in \mathbb{Z}^{n+1}$ the primitive inner normal of C with positive last coordinate. Consider the $n \times (n+1)$ matrix whose ith row is the coefficient vector of $h^{(0)}_{i,\gamma}$ in the prescribed monomial order and set $\mathcal{M}_\gamma \in \mathbb{Q}^{n\times n}$ and $\mathcal{B}_\gamma \in \mathbb{Q}^{n\times 1}$ for the submatrices consisting of the first n columns (coefficients of non-constant monomials) and the last column (constant coefficients) respectively. Then, the coefficients of $g_1, \dots, g_n$ are to be chosen so that the following condition holds.

(H2) For every $\gamma \in \Gamma$, the $(n \times n)$-matrix $\mathcal{M}_\gamma$ is nonsingular and all the entries of $(\mathcal{M}_\gamma)^{-1}\mathcal{B}_\gamma$ are nonzero.

Our next results assert that the above conditions can be met with good probability by randomly choosing the coefficients of $g_1, \dots, g_n$ in a certain set $\mathcal{S} \subset \mathbb{Z}$. We observe that our estimate on the size of $\mathcal{S}$ is not intended to be accurate, but to show that the growth of the size of the integers involved in the subsequent computations is not likely to create complexity problems.

Let $\{\Omega_{i,q} : 1 \leq i \leq n,\ q \in \Delta_i\}$ be a set of new indeterminates over $\mathbb{Q}$. For $1 \leq i \leq n$, write $\Omega_i := (\Omega_{i,q} : q \in \Delta_i)$ and let $H_i \in \mathbb{Q}[\Omega_i, X]$ be the generic polynomial

$$H_i(\Omega_i, X) := \sum_{q\in\Delta_i} \Omega_{i,q} X^q \tag{5.26}$$

with support Δ_i and $N_i := \#\Delta_i$ coefficients. Let $\Omega := (\Omega_1, \dots, \Omega_n)$ and let $N := N_1 + \cdots + N_n$ be the total number of indeterminate coefficients.

We start the analysis of the required generic conditions with the following quantitative version of Bernstein's result on the genericity of zero-dimensional sparse systems (see [Ber75, Theorem B], [HS95, Theorem 6.1]).

Lemma 5.4. *There exists a nonzero polynomial $P^{(0)} \in \mathbb{Q}[\Omega]$ with $\deg P^{(0)} \leq 3n^{2n+1}d^{2n-1}$ such that for any $c \in \mathbb{Q}^N$ with $P^{(0)}(c) \neq 0$, the system $H_1(c_1, X) = 0, \dots, H_n(c_n, X) = 0$ has D solutions in $\mathbb{A}^n$, counting multiplicities.*

Proof. Due to [HS95, Theorem 6.1] combined with [LW96], the system $H_1(c_1, X) = 0, \dots, H_n(c_n, X) = 0$ has D solutions in $\mathbb{A}^n$ counting multiplicities if and only if for every facet inner normal $\mu \in \mathbb{Z}^n$ of $Q_1 + \cdots + Q_n$, the sparse resultant $\mathrm{Res}_{\Delta_1^\mu, \dots, \Delta_n^\mu}$ does not vanish at $c := (c_1, \dots, c_n)$. Here Δ_i^μ denotes the set of points of Δ_i where the linear functional induced by μ attains its minimum for $1 \leq i \leq n$.

Therefore, the polynomial $P^{(0)} := \prod_\mu \mathrm{Res}_{\Delta_1^\mu, \dots, \Delta_n^\mu} \in \mathbb{Q}[\Omega]$, where the product ranges over all primitive inner normals $\mu \in \mathbb{Z}^n$ to facets of $Q_1 + \cdots + Q_n$, satisfies the required condition.

In order to estimate the degree of $P^{(0)}$, we observe that for every facet inner normal $\mu \in \mathbb{Z}^n$ the following upper bound holds:

$$\deg(\mathrm{Res}_{\Delta_1^\mu, \dots, \Delta_n^\mu}) \leq \sum_{i=1}^n \mathcal{M}_{n-1}(\Delta_1^\mu, \dots, \Delta_{i-1}^\mu, \Delta_{i+1}^\mu, \dots, \Delta_n^\mu) \leq nd^{n-1},$$

where $d := \max\{d_1, \dots, d_n\}$. On the other hand, it is not difficult to see that the number of facets of an n-dimensional integer convex polytope $P \subset \mathbb{R}^n$ which has an integer point in its interior is bounded by $n!\,\mathrm{Vol}_{\mathbb{R}^n}(P)$. Now, taking $P := (n+1)Q$, we obtain an integer polytope with the same number of facets as Q having an integer interior point. Then, the number of facets of Q is bounded by

$$\begin{aligned} n!\mathrm{Vol}_{\mathbb{R}^n}(P) = {} & n!\,\mathrm{Vol}_{\mathbb{R}^n}((n+1)Q) \\ = {} & (n+1)^n\, n!\,\mathrm{Vol}_{\mathbb{R}^n}(Q) \\ \leq {} & (n+1)^n (nd)^n, \end{aligned}$$

since Q is included in the n-dimensional simplex of size nd. This proves the upper bound for the degree $P^{(0)}$ of the statement of the lemma. □

The next lemma is concerned with the genericity of a smooth sparse system.

Lemma 5.5. *With the same notations as in Lemma 5.4 and before, there exists a nonzero polynomial $P^{(1)} \in \mathbb{Q}[\Omega]$ of degree at most $4n^{2n+1}d^{2n-1}$ such that for any $c \in \mathbb{Q}^N$ with $P^{(1)}(c) \neq 0$, the system $H_1(c_1, X) = 0, \ldots, H_n(c_n, X) = 0$ has exactly D distinct solutions in $\mathbb{A}^n$.*

Proof. Consider the incidence variety associated to $(\Delta_1, \ldots, \Delta_n)$-sparse systems, namely

$$W := \{(x, c) \in (\mathbb{C}^*)^n \times (\mathbb{A}^{N_1} \times \cdots \times \mathbb{A}^{N_n}) : \sum_{q \in \Delta_i} c_{i,q} x^q = 0 \text{ for } 1 \leq i \leq n\}.$$

As in [PS93, Proposition 2.3], it follows that W is a $\mathbb{Q}$-irreducible variety. Let $\pi_\Omega : W \to \mathbb{A}^{N_1} \times \cdots \times \mathbb{A}^{N_n}$ be the canonical projection, which is a dominant map.

By [Oka97, Chapter V, Corollary (3.2.1)], there is a nonempty Zariski open set $\mathcal{U}(\Delta_1, \ldots, \Delta_n) \subset \mathbb{A}^{N_1} \times \cdots \times \mathbb{A}^{N_n}$ of coefficients $c = (c_1, \ldots, c_n)$ for which the polynomials $H_1(c_1, X), \ldots, H_n(c_n, X)$ have supports $\Delta_1, \ldots, \Delta_n$ respectively and the set of their common zeros in $(\mathbb{C}^*)^n$ is a non-degenerate complete intersection variety. Then, the Jacobian $J_H := \det(\partial H_i / \partial X_j)_{1 \leq i,j \leq n}$ does not vanish at any point of $\pi_\Omega^{-1}(c)$ for every $c \in \mathcal{U}(\Delta_1, \ldots, \Delta_n)$.

Let $\mathbb{Q}(\Omega) \hookrightarrow \mathbb{Q}(W)$ be the finite field extension induced by the dominant map π_Ω. By the preceding paragraph we have that the rational function defined by J_H in $\mathbb{Q}(W)$ is nonzero. Therefore, its primitive minimal polynomial $M_J \in \mathbb{Q}[\Omega, Y]$ is well defined and satisfies the degree estimates

$$\deg_\Omega M_J \leq \deg W \cdot \deg J_H \leq \prod_{i=1}^{n} (d_i + 1) \cdot \sum_{i=1}^{n} d_i \leq 2^n d^{n+1} n$$

(see [SS96a], [Sch03]).

Let $P^{(1)} := P^{(0)} M_J^{(0)}$, where $P^{(0)}$ is the polynomial given by Lemma 5.4 and $M_J^{(0)}$ denotes the constant term of the expansion of M_J in powers of

Y. We claim that $P^{(1)}$ satisfies the requirements of the statement of the lemma. Indeed, let $c \in \mathbb{Q}^N$ satisfy $P^{(1)}(c) \neq 0$. Then $P^{(0)}(c) \neq 0$ holds and hence, Lemma 5.4 implies that $H_1(c, X) = 0, \dots, H_n(c, X) = 0$ is a zero-dimensional system. Furthermore, $M_J^{(0)}(c)$ is a nonzero multiple of the product $\prod_{x \in \pi_\Omega^{-1}(c)} J_H(c, x)$. Thus, the non-vanishing of $M_J^{(0)}(c)$ shows that all the points of $\pi_\Omega^{-1}(c)$ are smooth and therefore, from e.g. [Oka97, IV, Theorem 2.2], it follows that $\pi_\Omega^{-1}(c)$ consists of exactly D simple points in $(\mathbb{C}^*)^n$. Moreover, combining the assumption that $0 \in \Delta_i$ for $1 \leq i \leq n$ with [LW96, Theorem 2.4], we deduce that $\pi_\Omega^{-1}(c)$ consists of D simple points in $\mathbb{A}^n$. The estimate $\deg M_J^{(0)} \leq \deg_\Omega M_J \leq 2^n d^{n+1} n \leq n^{2(n+1)} d^{2n-1}$ implies the statement of the lemma. □

Finally, we exhibit a generic condition on the coefficients $h_1, \dots, h_n$ which implies that assumption (H2) holds.

Lemma 5.6. *With the previous assumptions and notations, there exists a nonzero polynomial* $P^{(2)} \in \mathbb{Q}[\Omega]$ *with* $\deg P^{(2)} \leq n(n+1)\#\Gamma$ *such that for every* $c := (c_1, \dots, c_n) \in \mathbb{Q}^N$ *with* $P^{(2)}(c) \neq 0$*, the polynomials* $h_i := H_i(c_i, X)$ $(1 \leq i \leq n)$ *satisfy condition* (H2).

Proof. Fix a primitive integer inner normal $\gamma \in \Gamma$ to a lower facet of $\widehat{\mathcal{A}}$. Let $\mathcal{M}_\gamma \in \mathbb{Q}[\Omega]^{n \times n}$ and $\mathcal{B}_\gamma \in \mathbb{Q}[\Omega]^{n \times 1}$ be the matrices constructed from the generic polynomials $H_1, \dots, H_n \in \mathbb{Q}[\Omega][X]$ as explained in the paragraph preceding condition (H2). Let $D_{0,\gamma} \in \mathbb{Q}[\Omega]$ be the (nonzero) determinant of $\mathcal{M}_\gamma$, and for every $1 \leq j \leq n$, let $D_{j,\gamma}$ be the determinant of the matrix obtained from $\mathcal{M}_\gamma$ by replacing its jth column with $\mathcal{B}_\gamma$. Set $P_\gamma := \prod_{j=0}^n D_{j,\gamma}$. Finally, take $P^{(2)} := \prod_{\gamma \in \Gamma} P_\gamma$. By Cramer's rule, whenever $P^{(2)}(c) \neq 0$, we have that the system $h_1, \dots, h_n$ with coefficient vector $c = (c_1, \dots, c_n)$ meets condition (H2).

The degree estimate for $P^{(2)}$ follows from the fact that $\deg P_\gamma \leq n(n+1)$ holds for every $\gamma \in \Gamma$, since each of the entries of the matrices whose determinants are involved has degree 1 in the variables Ω. □

Now, we are ready to state a generic condition on the coefficients of $h_1, \dots, h_n$ which implies that (H1) and (H2) hold.

Proposition 5.7. *Under the previous assumptions and notations, there exists a nonzero polynomial* $P \in \mathbb{Q}[\Omega]$ *with* $\deg P \leq 4n^{2n+1} d^{2n-1} + n(n+1)D$

such that for every $c \in \mathbb{Q}^N$ *with* $P(c) \neq 0$*, the polynomials* $h_i := H_i(c_i, X)$ $(1 \leq i \leq n)$ *satisfy conditions* (H1) *and* (H2)*.*

Proof. Set $P := P^{(1)}P^{(2)}$, where $P^{(1)}$ is the polynomial of the statement of Lemma 5.5 and $P^{(2)}$ is the one defined in the statement of Lemma 5.6. The result follows from Lemmas 5.5 and 5.6, and the upper bound $\#\Gamma \leq D$ for the cardinality of the set of the distinct inner normal vectors considered (one for each cell of type $(k_1, \ldots, k_s)$ in the given fine-mixed subdivision). □

5.2.3. Outline of the algorithm

Now we have all the tools necessary to give an outline of our algorithm for the computation of a geometric solution of the (sufficiently generic) sparse system $h_1 = 0, \ldots, h_n = 0$.

With notations as in the previous subsections, we assume that a fine-mixed subdivision of $\mathcal{A}$ induced by a lifting function ω is given. This means that we are given the set Γ of inner normals of the lower facets of the convex hull of $\widehat{\mathcal{A}}$, together with the corresponding cells of the convex hull of $\mathcal{A}$. In addition, we suppose that our input polynomials $h_1, \ldots, h_n \in \mathbb{Q}[X]$ satisfy conditions (H1) and (H2) and denote by $V_1 \subset \mathbb{A}^n$ the affine variety defined by $h_1, \ldots, h_n$.

First, we choose a *generic* linear form $u \in \mathbb{Q}[X]$ such that:

- u separates the points of the zero-dimensional varieties V_1 and $V_{0,\gamma}$ for every $\gamma \in \Gamma$. This condition is represented by the nonvanishing of a certain nonconstant polynomial of degree at most $4D^2$.

- An algorithm for the computation of the minimal polynomial of u in $V_{0,\gamma}$ described below can be extended to a computation of a geometric solution of $V_{0,\gamma}$ in the sense of Lemma 2.4 for every $\gamma \in \Gamma$. This condition is represented by the nonvanishing of a nonconstant polynomial of degree at most $4D_\gamma^3$ for each $\gamma \in \Gamma$.

- An algorithm for the computation of the minimal polynomial of u in $\widehat{V}$ described below can be extended to a computation of a geometric solution of $\widehat{V}$ in the sense of Lemma 2.4. This application of Lemma 2.4

requires that the coefficient vector of the linear form u does not annihilate a non-constant polynomial of degree at most $4D^4$.

As a first step, we fix $\rho \geq 2$. From Theorem 2.1 it follows that a linear form u satisfying these conditions can be obtained by randomly choosing its coefficients from the set $\{1, \ldots, 6\rho D^4\}$ with error probability at most $1/\rho$.

Second, we compute the monic minimal polynomial $\widehat{m}_u \in \mathbb{Q}(T)[Y]$ of the linear form u in the curve $\widehat{V}$ introduced in (5.12). For this purpose, we approximate the Puiseux series expansions of the branches of $\widehat{V}$ lying above 0 by means of a global Newton-Hensel lifting of the common zeros of the zero-dimensional varieties $V_{0,\gamma} \subset \mathbb{A}^n$ defined by the polynomials (5.14) for all $\gamma \in \Gamma$ (see Section 5.2.4).

This in turn requires the computation of a geometric solution of $V_{0,\gamma}$ for every $\gamma \in \Gamma$. By means of a change of variables we take the system $h_{1,\gamma}^{(0)} = 0, \ldots, h_{n,\gamma}^{(0)} = 0$ defining the variety $V_{0,\gamma}$ into a "diagonal" form (see Subsection 5.2.4 below), which allows us to compute the minimal polynomial $m_{u,\gamma}^{(0)}$ of u in $V_{0,\gamma}$. Since the linear form u satisfies condition (2) of the statement of Lemma 2.4, from this procedure we derive an algorithm computing a geometric solution of $V_{0,\gamma}$ according to Lemma 2.4.

Then we "lift" this geometric solution to a suitable (non-archimedean) approximation $\widetilde{m}_\gamma$ of a factor m_γ (over $\overline{\mathbb{Q}(T)}$) of the desired minimal polynomial $\widehat{m}_u$ of u.

In the third step we obtain the minimal polynomial $\widehat{m}_u = \prod_{\gamma \in \Gamma} m_\gamma$ from the approximate factors $\widetilde{m}_\gamma$, namely, we compute the dense representation of the coefficients (in $\mathbb{Q}(T)$) of $\widehat{m}_u$, using Padé approximation (see Subsection 5.2.5 below). To conclude this step, we apply the proof of Lemma 2.4 to derive an algorithm for computing a geometric solution of the variety $\widehat{V}$.

In the last step we compute a geometric solution of the variety V_1 by substituting 1 for T in the polynomials that form the geometric solution of $\widehat{V}$.

This algorithm which solves the system $h_1 = 0, \ldots, h_n = 0$ may be briefly sketched as follows:

Algorithm 5.8.

Step I *Choose the coefficients of a linear form $u \in \mathbb{Q}[X]$ at random from the* *set* $\{1,\ldots,6\rho D^4\}$.

Step II *For each* $\gamma \in \Gamma$:

Step II.1 *Find a geometric solution of the variety* $V_{0,\gamma}$ *defined in* (5.15).

Step II.2 *Obtain a straight-line program for the polynomials* $h_{1,\gamma},\ldots,h_{n,\gamma}$ *defined in* (5.16) *from the coefficients of* $h_1,\ldots,h_n$ *and the entries of* $\gamma \in \mathbb{Z}^{n+1}$.

Step II.3 *"Lift" the computed geometric solution of* $V_{0,\gamma}$ *to an approximation* $\widetilde{m}_\gamma$ *of the factor* m_γ *of* $\widehat{m}_u$ *by means of a symbolic Newton-Hensel procedure.*

Step III *Obtain a geometric solution of the curve* $\widehat{V}$:

Step III.1 *Compute the approximation* $\widetilde{m}_u := \prod_{\gamma\in\Gamma} \widetilde{m}_\gamma$ *of* $\widehat{m}_u$.

Step III.2 *Compute the dense representation of* $\widehat{m}_u$ *from* $\widetilde{m}_u$ *using Padé approximation.*

Step III.3 *Find a geometric solution of* $\widehat{V}$ *applying the proof of Lemma 2.4.*

Step IV *Substitute 1 for* T *in the polynomials which form the geometric solution of* $\widehat{V}$ *computed in the previous step to obtain a geometric solution of the variety* V_1.

Step I has been considered above. Next we discuss the following steps.

5.2.4. Geometric solutions of the starting varieties

In this subsection we exhibit an algorithm which covers Step II.1 of Algorithm 5.8 and computes, for a given inner normal $\gamma \in \Gamma$, a geometric solution of the variety $V_{0,\gamma} \subset (\mathbb{C}^*)^n$ defined by the polynomials $h_{i,\gamma}^{(0)}$ $(1 \le i \le n)$ for polynomials $h_1,\ldots,h_n$ satisfying assumptions (H1) and (H2). This algorithm is based on the procedure presented in [HS95].

Fix a cell $C = (C^{(1)},\ldots,C^{(s)})$ of type $(k_1,\ldots,k_s)$ of the given fine-mixed subdivision of $\mathcal{A}$ and let $\gamma \in \Gamma$ be its associated inner normal. For $1 \le \ell \le s$, we denote by $h_1^{(\ell)},\ldots,h_{k_\ell}^{(\ell)}$ the polynomials in the set $\{h_{1,\gamma}^{(0)},\ldots,h_{n,\gamma}^{(0)}\}$ that are supported in $C^{(\ell)}$. In the sequel, whenever there is no risk of confusion we will not write the subscript γ indicating which cell we are considering.

Our hypotheses imply that $h_1^{(\ell)}, \dots, h_{k_\ell}^{(\ell)}$ are $\mathbb{Q}$-linear combinations of precisely $k_\ell + 1$ monomials in $\mathbb{Q}[X]$ and, up to a multiplication by a monomial, we may assume one of them to be the constant term. Denote these monomials by $X^{\alpha_{\ell,0}}, \dots, X^{\alpha_{\ell,k_\ell}}$, with $\alpha_{\ell,0} := 0 \in \mathbb{Z}^n$. Let $\widetilde{\mathcal{M}}^{(\ell)}$ be the matrix of $\mathbb{Q}^{k_\ell \times (k_\ell+1)}$ for which the following equality holds in $\mathbb{Q}[X, X^{-1}]^{k_\ell}$:

$$\widetilde{\mathcal{M}}^{(\ell)} \begin{pmatrix} X^{\alpha_{\ell,k_\ell}} \\ \vdots \\ X^{\alpha_{\ell,0}} \end{pmatrix} = \begin{pmatrix} h_1^{(\ell)} \\ \vdots \\ h_{k_\ell}^{(\ell)} \end{pmatrix}, \tag{5.27}$$

and let $\mathcal{M}^{(\ell)}$ denote the square $(k_\ell \times k_\ell)$-matrix obtained by deleting the last column from $\widetilde{\mathcal{M}}^{(\ell)}$. Set

$$\mathcal{M} := \begin{pmatrix} \mathcal{M}^{(1)} & 0 & \cdots & 0 \\ 0 & \mathcal{M}^{(2)} & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & \mathcal{M}^{(s)} \end{pmatrix},$$

where 0 here represents different block matrices with all its entries equal to $0 \in \mathbb{Q}$. Then $\mathcal{M}$ is the matrix defined by the coefficients of the nonconstant terms of the (Laurent) polynomials $h_{1,\gamma}^{(0)}, \dots, h_{n,\gamma}^{(0)}$, up to a translation.

Due to condition (H2) we have that the matrix $\mathcal{M}$ is invertible, which in turn implies that the square matrices $\mathcal{M}^{(\ell)}$ are invertible for $1 \leq \ell \leq s$. Following [HS95], we apply Gaussian elimination to the matrix $\widetilde{\mathcal{M}}^{(\ell)}$ for $1 \leq \ell \leq s$ and obtain a set of $k_\ell + 1$ binomials

$$\begin{pmatrix} 1 & 0 & 0 & \dots & -c_{\alpha_{\ell,k_\ell}} \\ 0 & 1 & 0 & \dots & -c_{\alpha_{\ell,k_\ell-1}} \\ \vdots & & \ddots & & \\ 0 & 0 & \dots & 1 & -c_{\alpha_{\ell,0}} \end{pmatrix} \begin{pmatrix} X^{\alpha_{\ell,k_\ell}} \\ X^{\alpha_{\ell,k_\ell-1}} \\ \vdots \\ X^{\alpha_{\ell,0}} \end{pmatrix} = \begin{pmatrix} X^{\alpha_{\ell,k_\ell}} - c_{\alpha_{\ell,k_\ell}} \\ X^{\alpha_{\ell,k_\ell-1}} - c_{\alpha_{\ell,k_\ell-1}} \\ \vdots \\ X^{\alpha_{\ell,0}} - c_{\alpha_{\ell,0}} \end{pmatrix}$$

that generate the same linear subspace of $\mathbb{Q}[X, X^{-1}]$ as the polynomials in (5.27). Therefore, for $1 \leq \ell \leq s$ the set of common zeros in $(\mathbb{C}^*)^n$ of the polynomials $h_1^{(\ell)}, \dots, h_{k_\ell}^{(\ell)}$ is given by the system $X^{\alpha_{\ell,k_\ell}} = c_{\alpha_{\ell,k_\ell}}, \dots, X^{\alpha_{\ell,1}} = c_{\alpha_{\ell,1}}$. Putting these s systems together, we obtain a binomial system defining $V_{0,\gamma}$ of the form

$$X^{\alpha_1} = p_1, \dots, X^{\alpha_n} = p_n, \tag{5.28}$$

with $\alpha_i \in \mathbb{Z}^n$ and $p_i \in \mathbb{Q} \setminus \{0\}$ $(1 \leq i \leq n)$. Note that the second part of condition (H2) ensures the non-vanishing of the constants p_i for $1 \leq i \leq n$.

Now, let $\mathcal{E}$ denote the $(n \times n)$-matrix whose columns are the exponent vectors $\alpha_1, \dots, \alpha_n$. Using [Sto00, Proposition 8.10], we obtain unimodular matrices $K = (k_{i,j})_{1 \leq i,j \leq n}$, $L = (l_{i,j})_{1 \leq i,j \leq n}$ of $\mathbb{Z}^{n \times n}$, and a diagonal matrix $\operatorname{diag}(r_1, \dots, r_n) \in \mathbb{Z}^{n \times n}$ which give the Smith Normal Form for $\mathcal{E}$, i.e., matrices such that the identity

$$K \cdot \mathcal{E} \cdot L = \operatorname{diag}(r_1, \dots, r_n) \tag{5.29}$$

holds in $\mathbb{Z}^{n \times n}$. We observe that the upper bound

$$\log \|K\| \leq (4n + 5)(\log n + \log \|\mathcal{E}\|) \tag{5.30}$$

holds, where $\|A\|$ denotes the maximum of the absolute value of the entries of a given matrix A [Sto00, Proposition 8.10].

Let $Z_1, \dots, Z_n$ be new indeterminates, and write $Z := (Z_1, \dots, Z_n)$. We introduce the change of coordinates given by $X_i := Z_1^{k_{1,i}} \cdots Z_n^{k_{n,i}}$ for $1 \leq i \leq n$. Making this change of coordinates in (5.28) we obtain the system

$$Z^{K\alpha_1} = p_1, \dots, Z^{K\alpha_n} = p_n,$$

which is equivalent to the "diagonal" system

$$Z_j^{r_j} = \prod_{i=1}^{n} (Z^{K\alpha_i})^{l_{i,j}} = \prod_{i=1}^{n} p_i^{l_{i,j}} =: q_j \quad (1 \leq j \leq n).$$

Inverting some of the coefficients q_j if necessary we may assume without loss of generality that the integers $r_1, \dots, r_n$ are positive. We have thus a very convenient description of the variety $V_{0,\gamma}$ by a diagonal polynomial system in the coordinate system of $\mathbb{A}^n$ defined by $Z_1, \dots, Z_n$. We shall compute a geometric solution of $V_{0\gamma}$ in such a coordinate system, which will be then used to compute a geometric solution of $V_{0,\gamma}$ in the "standard" coordinate system defined by $X_1, \dots, X_n$.

Example. We illustrate the above procedure for the variety $V_{0,\gamma^{(3)}}$ of (5.22), namely,

$$\begin{cases} h_{1,\gamma^{(3)}}^{(0)} = 1 - X_1^2 X_2^2, \\ h_{2,\gamma^{(3)}}^{(0)} = X_1^2 X_2 + X_1 X_2^2, \end{cases} \qquad V_{0,\gamma^{(3)}} = \{(1,-1), (-1,1), (i,-i), (-i,i)\}. \tag{5.31}$$

Here the binomial system in (5.28) and the corresponding exponent vector matrix $\mathcal{E}$ are

$$\begin{cases} X_1^2X_2^2 = 1, \\ X_1X_2^{-1} = -1, \end{cases} \qquad \text{and} \qquad \mathcal{E} = \begin{pmatrix} 2 & 1 \\ 2 & -1 \end{pmatrix}.$$

Taking $K := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $L := \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$, we get $K \cdot \mathcal{E} \cdot L = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$, and hence, making the change of coordinates $X_1 = Z_1Z_2$, $X_2 = Z_2$ we obtain the equivalent diagonal system

$$\begin{cases} Z_1 = -1, \\ Z_2^4 = 1. \end{cases} \tag{5.32}$$

The algorithm for computing a geometric solution of the variety $V_{0,\gamma}$ in the coordinate system defined by $Z_1, \dots, Z_n$ takes as input the set of polynomials $Z_1^{r_1} - q_1, \dots, Z_n^{r_n} - q_n \in \mathbb{Q}[Z_1, \dots, Z_n]$ and outputs a linear form $\widetilde{u} \in \mathbb{Q}[Z_1, \dots, Z_n]$ which separates the points of $V_{0,\gamma}$, the minimal polynomial $m_{\widetilde{u}} \in \mathbb{Q}[Y]$ of $\widetilde{u}$ in $V_{0,\gamma}$ and the parametrizations $\widetilde{w}_1, \dots, \widetilde{w}_n$ of $Z_1, \dots, Z_n$ by the zeros of $m_{\widetilde{u}}$. Observe that $D_\gamma = r_1 \cdots r_n = \#(V_{0,\gamma})$

For this purpose we apply the algorithm for solving a "diagonal" system underlying Lemma 3.11. Combining Lemma 3.11 and Proposition 3.14 we obtain the following result.

Proposition 5.9. *Suppose that the coefficients of the linear form $\widetilde{u}$ are randomly chosen in the set $\{1, \dots, 4n\rho D_\gamma^3\}$, where ρ is a fixed positive integer. Then the algorithm described above computes a geometric solution of the variety $V_{0,\gamma}$ (in the coordinate system $Z_1, \dots, Z_n$) with error probability at most $1/\rho$ using $O\big(n\mathsf{M}(D_\gamma^2)\big)$ arithmetic operations in $\mathbb{Q}$.*

Example. For the system (5.32) defining the variety $V_{0,\gamma^{(3)}}$ in the coordinate system Z_1, Z_2, taking the separating linear form $\widetilde{u} = Z_1 + Z_2$ we obtain:

- $m_1 := Y + 1$,
- $m_2 := Res_{\widetilde{Y}}((Y - \widetilde{Y})^4 - 1, \widetilde{Y} + 1) = Y^4 + 4Y^3 + 6Y^2 + 4Y$.

Then, the minimal polynomial of $\widetilde{u}$ is $m_{\widetilde{u}} = Y^4 + 4Y^3 + 6Y^2 + 4Y$.

Next we compute a geometric solution of the variety $V_{0,\gamma}$ in the original coordinate system defined by $X_1, \dots, X_n$. As before, we consider $\gamma \in \Gamma$ fixed.

For this purpose, we compute the minimal polynomial $m_u \in \mathbb{Q}[Y]$ of a linear form $u = u_1X_1 + \cdots + u_nX_n \in \mathbb{Q}[X_1, \dots, X_n]$ in $V_{0,\gamma}$. Let $V_{0,\gamma} := \{\mathrm{x}_0^{(1,\gamma)}, \dots, \mathrm{x}_0^{(D_\gamma,\gamma)}\}$. Then we have $m_u(Y) = \prod_{j=1}^{D_\gamma}(Y - u(\mathrm{x}_0^{(j,\gamma)}))$. In order to compute m_u, we use the polynomials $m_{\widetilde{u}}, \widetilde{w}_1, \dots, \widetilde{w}_n$ which form the previously computed geometric solution of $V_{0,\gamma}$ in the variables $Z_1, \dots, Z_n$: from the identities $X_i := Z_1^{k_{1,i}} \cdots Z_n^{k_{n,i}}$ $(1 \le i \le n)$ we deduce that m_u equals the minimal polynomial of the image of the projection $\eta_u : V_{0,\gamma} \to \mathbb{A}^1$ defined by $\eta_u^{(\gamma)}(z_1, \dots, z_n) := \sum_{i=1}^n u_i z_1^{k_{1,i}} \cdots z_n^{k_{n,i}}$. Now, the identities $Z_i = \widetilde{w}_i(\widetilde{u})$, which hold in $\mathbb{Q}[V_{0,\gamma}]$ for $1 \le i \le n$, imply that

$$u = \sum_{i=1}^{n} u_i \big(\widetilde{w}_1(\widetilde{u})\big)^{k_{1,i}} \cdots \big(\widetilde{w}_n(\widetilde{u})\big)^{k_{n,i}} \tag{5.33}$$

holds in $\mathbb{Q}[V_{0,\gamma}]$, from which we easily conclude that m_u satisfies the following identity:

$$m_u(Y) = Res_{\widetilde{Y}}\left(Y - \sum_{i=1}^{n} u_i \big(\widetilde{w}_1(\widetilde{Y})\big)^{k_{1,i}} \cdots \big(\widetilde{w}_n(\widetilde{Y})\big)^{k_{n,i}}, m_{\widetilde{u}}(\widetilde{Y})\right). \tag{5.34}$$

Example. We compute now a geometric solution of $V_{0,\gamma^{(3)}}$ in the coordinate system X_1, X_2 for the linear form $u = X_1 - X_2$ from its geometric solution in the coordinates Z_1, Z_2 (see Subsection 5.2.4):

- $m_{\widetilde{u}} = Y^4 + 4Y^3 + 6Y^2 + 4Y$,
- $\widetilde{w}_1 = -1$,
- $\widetilde{w}_2 = Y + 1$.

From the change of coordinates $X_1 = Z_1Z_2, X_2 = Z_2$ leading to system (5.32), we have $u = Z_1Z_2 - Z_2$ and hence $u = -2(\widetilde{u} + 1)$. Therefore,

$$m_u = Res_{\widetilde{Y}}(Y+2(\widetilde{Y}+1)), \widetilde{Y}^4+4\widetilde{Y}^3+6\widetilde{Y}^2+4\widetilde{Y}) = Y^4-16.$$

Now, we estimate the complexity of this step. We compute the monomials $\big(\widetilde{w}_1(\widetilde{u})\big)^{k_{1,i}} \cdots \big(\widetilde{w}_n(\widetilde{u})\big)^{k_{n,i}}$ $(1 \le i \le n)$ in the right-hand side of (5.33) modulo $m_{\widetilde{u}}(Y)$, with $O\big(n^2 \log(\max_{i,j} |k_{i,j}|) \mathsf{M}(D_\gamma)\big)$ arithmetic operations in $\mathbb{Q}$. From (5.30) it follows that

$$O\big(n^2 \log(\max_{i,j} |k_{i,j}|) \mathsf{M}(D_\gamma)\big) = O\big(n^3 \log(n\|\mathcal{E}_\gamma\|) \mathsf{M}(D_\gamma)\big),$$

where $\mathcal{E}_\gamma$ is the matrix of the exponents of the cell corresponding to the inner normal γ. Observe that all these steps are independent of the coefficients of the linear form u we are considering and therefore do not introduce any division by a nonconstant polynomial in the coefficients $u_1, \ldots, u_n$.

In the next step we compute the right-hand side of (5.33) modulo $m_{\widetilde{u}}(Y)$, with $O\big(nD_\gamma\big)$ arithmetic operations in $\mathbb{Q}$. Then we compute the resultant (5.34) by a process which interpolates (5.34) in the variable Y to reduce the question to the computation of $D_\gamma + 1$ univariate resultants. This requires $O\big(\mathsf{M}(D_\gamma)^2\big)$ arithmetic operations in $\mathbb{Q}$.

If the linear form u separates the points of $V_{0,\gamma}$, then we can extend the algorithm for computing $m_u(Y)$ to an algorithm for computing a geometric solution of $V_{0,\gamma}$ with the algorithm underlying the proof of Lemma 2.4. This extension requires that the coefficients $u_1, \ldots, u_n$ of the linear form u do not annihilate the denominators in $\mathbb{Q}[\Lambda]$ which arise from the application of the algorithm described above to the generic version $\Lambda_1 X_1 + \cdots + \Lambda_n X_n$ of the linear form u. Such denominators arise only during the computation of the generic version of the resultant (5.34). Hence, with a similar analysis as in the proof of Proposition 5.9, we conclude that, if the coefficients of u are chosen randomly in the set $\{1, \ldots, 4n\rho D_\gamma^3\}$, then the error probability of our algorithm is bounded by $1/\rho$. In conclusion, we have the following result.

Proposition 5.10. *Suppose that we are given a geometric solution of $V_{0,\gamma}$ in the coordinate system $Z_1, \ldots, Z_n$, as provided by the algorithm underlying Proposition 5.9, and the coefficients of the linear form u are randomly chosen in the set $\{1, \ldots, 4n\rho D_\gamma^3\}$, where ρ is a fixed positive integer. Then the algorithm described above computes a geometric solution of the variety $V_{0,\gamma}$ with error probability at most $1/\rho$ using $O\big(n^3 \log(n\|\mathcal{E}_\gamma\|) \mathsf{M}(D_\gamma)^2\big)$ arithmetic operations in $\mathbb{Q}$.*

Finally, from Propositions 5.9 and 5.10 and the fact that $\|\mathcal{E}_\gamma\| \le 2\mathcal{Q}$ holds for $\mathcal{Q} := \max_{1\le i\le n}\{\|q\|; q \in \Delta_i\}$, we immediately deduce the following result.

Theorem 5.11. *Suppose that the coefficients of the linear forms $\widetilde{u}$ and u of the statement of Propositions 5.9 and 5.10 are chosen at random in the set $\{1, \ldots, 4n\rho D^3\}$, where ρ is a fixed positive integer. Then the algorithm underlying Propositions 5.9 and 5.10 computes a geometric solution of the varieties $V_{0,\gamma}$ for all $\gamma \in \Gamma$ with error probability at most $2/\rho$ using $O\big(n^3 \log(n\mathcal{Q})\mathsf{M}(D)^2\big)$ arithmetic operations in $\mathbb{Q}$.*

Example. For the polynomial system (5.17) we are considering and the linear form $u = X_1 - X_2$, the first step of Algorithm 5.8 computes the following geometric solutions of the varieties of (5.20), (5.21) and (5.22) respectively, as explained above:

$$\begin{array}{rcl} V_{0,\gamma^{(1)}} & = & \{(-1, -y-1) \in \mathbb{C}^2 : y^2 + 2y = 0\}, \\ V_{0,\gamma^{(2)}} & = & \{((y-1, -1) \in \mathbb{C}^2 : y^2 - 2y = 0\}, \\ V_{0,\gamma^{(3)}} & = & \{(\frac{1}{2}y, -\frac{1}{2}y) \in \mathbb{C}^2 : y^4 - 16 = 0\}. \end{array} \tag{5.35}$$

5.2.5. A geometric solution of the curve $\widehat{V}$

We recall the definition of the variety $\widehat{V}$. Let I denote the ideal of $\mathbb{Q}[X, T]$ generated by the polynomials

$$\widehat{h}_i(X, T) = \sum_{q \in \Delta_i} c_{i,q} X^q T^{\omega_i(q)} \quad (1 \leq i \leq n)$$

of (5.11), which form the polyhedral deformation of the generic polynomials $h_1, \ldots, h_n$, and let J denote the Jacobian determinant of $\widehat{h}_1, \ldots, \widehat{h}_n$ with respect to the variables $X_1, \ldots, X_n$. Let $V(I)$ be the set of common zeros in $\mathbb{A}^{n+1}$ of $\widehat{h}_1, \ldots, \widehat{h}_n$. Then $\widehat{V} := V(I : J^\infty)$.

Alternatively, let $\pi : V(I) \to \mathbb{A}^1$ be the linear projection defined by $\pi(x, t) := t$. Consider the decomposition of $V(I)$ into its irreducible components $V(I) = \bigcup_{i=1}^{r+s} \mathcal{C}_i$. Suppose that the restriction $\pi|_{\mathcal{C}_i} : \mathcal{C}_i \to \mathbb{A}^1$ of the projection π is dominant for $1 \leq i \leq r$ and is not dominant for $r+1 \leq i \leq s$. We shall show that $\widehat{V} := \bigcup_{i=1}^{r} \mathcal{C}_i$ holds, i.e., $\widehat{V}$ is the union of all the irreducible components of $V(I)$ which project dominantly over $\mathbb{A}^1$. Furthermore, we shall show that $\widehat{V} \subset \mathbb{A}^{n+1}$ is a curve which constitutes a suitable deformation of the variety defined by the system $h_1 = 0, \ldots, h_n = 0$. For this purpose, adapting Proposition 3.3 we deduce the following technical lemma.

Lemma 5.12. *Let $F_1, \dots, F_n \in \mathbb{Q}[X,T]$ be polynomials which generate an ideal $I := (F_1, \dots, F_n) \subset \mathbb{Q}[X,T]$ and let J denote the Jacobian determinant of $F_1, \dots, F_n$ with respect to the variables X. Set $\mathcal{V} := \{(x,t) \in \mathbb{A}^{n+1} : F_1(x,t) = 0, \dots, F_n(x,t) = 0\}$ and consider the linear projection $\pi : \mathcal{V} \to \mathbb{A}^1$ defined by $\pi(x,t) := t$. Assume that $\#\pi^{-1}(t) \leq D$ holds for generic values of $t \in \mathbb{A}^1$ and that there exists a point $t_0 \in \mathbb{A}^1$ such that the fiber $\pi^{-1}(t_0)$ is a zero-dimensional variety of degree D with $J(x,t_0) \neq 0$ for every $(x,t_0) \in \pi^{-1}(t_0)$.*

Let $\mathcal{V}_{\mathrm{dom}}$ be the union of all the irreducible components $\mathcal{C}$ of $\mathcal{V}$ with $\overline{\pi(\mathcal{C})} = \mathbb{A}^1$. Then:

- *$\mathcal{V}_{\mathrm{dom}}$ is a nonempty equidimensional variety of dimension 1.*
- *$\mathcal{V}_{\mathrm{dom}}$ is the union of all the irreducible components of $\mathcal{V}$ having a nonempty intersection with $\pi^{-1}(t_0)$.*
- *$\mathcal{V}_{\mathrm{dom}} = V(I : J^\infty)$.*
- *The restriction $\pi|_{\mathcal{V}_{\mathrm{dom}}} : \mathcal{V}_{\mathrm{dom}} \to \mathbb{A}^1$ is a dominant map of degree D.*

Now we return to the study of the variety $\widehat{V}$ and show that the assumptions of Lemma 5.12 hold. Observe that $\pi^{-1}(t) = V_t \times \{t\}$ holds for every $t \in \mathbb{A}^1$, where $V_t := \{x \in \mathbb{A}^n : \widehat{h}_1(x,t) = 0, \dots, \widehat{h}_n(x,t) = 0\}$. Furthermore, the polynomials $\widehat{h}_1(X,t), \dots, \widehat{h}_n(X,t)$ are obtained by a suitable substitution of the variables Ω of the generic polynomials $H_1, \dots, H_n \in \mathbb{Q}[\Omega, X]$ with supports $\Delta_1, \dots, \Delta_n$ introduced in (5.26). Indeed, if $c = (c_1, \dots, c_n)$ is the vector of coefficients of $h_1, \dots, h_n$, the coefficient vector of $\widehat{h}_i(X,t)$ $(1 \leq i \leq n)$ is $(c_{i,q}t^{\omega_i(q)})_{q \in \Delta_i}$ for every $t \in \mathbb{A}^1$. By Lemma 5.4, there exists a nonzero polynomial $P^{(0)} \in \mathbb{Q}[\Omega]$ such that, for any $c' = (c'_1, \dots, c'_n)$ with $P^{(0)}(c') \neq 0$, the associated sparse system defines a zero-dimensional variety. In particular, the coefficients $c = (c_1, \dots, c_n)$ of our input polynomials $h_1 := H_1(c_1, X), \dots, h_n = H_n(c_n, X)$ satisfy $P^{(0)}(c) \neq 0$. This shows that the polynomial $P_T^{(0)} \in \mathbb{Q}[T]$ obtained by substituting $\Omega_{i,q} \mapsto c_{i,q}T^{\omega_i(q)}$ $(1 \leq i \leq n,\ q \in \Delta_i)$ in the polynomial $P^{(0)}$ is nonzero, since it does not vanish at $T = 1$. We conclude that V_t is a zero-dimensional variety for all but a finite number of $t \in \mathbb{A}^1$. Thus, $\pi^{-1}(t)$ is finite for generic values of $t \in \mathbb{A}^1$.

Finally, by condition (H1), the fiber $\pi^{-1}(1) = V(h_1, \ldots, h_n) \times \{1\}$ is a zero-dimensional variety of degree $D = \deg(\pi)$ and the Jacobian determinant $J := \det(\partial \widehat{h}_i / \partial X_j)_{1 \leq i,j \leq n}$ does not vanish at any of its points. On the other hand, the fact that $\# \pi^{-1}(t) \leq D$ holds for generic values $t \in \mathbb{A}^1$ follows from the BKK theorem.

This shows that the variety $V(I)$ and its defining polynomials $\widehat{h}_1, \ldots, \widehat{h}_n$ satisfy all the assumptions of Lemma 5.12. Thus, we have the following result.

Lemma 5.13. *The variety $\widehat{V} \subset \mathbb{A}^{n+1}$ is a curve. Furthermore, every irreducible component of $\widehat{V}$ has a nonempty intersection with the fiber $\pi^{-1}(1)$ of the projection map $\pi : \widehat{V} \to \mathbb{A}^1$.*

Generic linear projections of $\widehat{V}$.

In order to compute a geometric solution of the space curve $\widehat{V}$, we shall first exhibit a procedure for computing the minimal polynomial of a generic linear projection of $\widehat{V}$. Let $u \in \mathbb{Q}[X_1, \ldots, X_n]$ be a linear form which separates the points of the "initial varieties" $V_{0,\gamma}$ for all the inner normals $\gamma := (\gamma_1, \ldots, \gamma_{n+1})$ of the lower facets of the polyhedral deformation under consideration. Let $\pi_u : \widehat{V} \to \mathbb{A}^2$ be the morphism defined by $\pi_u(x, t) := (t, u(x))$. Since the projection map $\pi : \widehat{V} \to \mathbb{A}^1$ defined by $\pi(x, t) := t$ is dominant, it follows that the Zariski closure of the image of π_u is a $\mathbb{Q}$-definable hypersurface of $\mathbb{A}^2$. Denote by $M_u \in \mathbb{Q}[T, Y]$ a minimal defining polynomial for this hypersurface. For the sake of the argument, we shall assume further that the identity $\deg(\pi) = D$, and thus $\deg_Y M_u = D$, holds.

We can apply estimate (5.4) of Lemma 5.3 in order to estimate $\deg_T M_u$ in combinatorial terms (compare with [PS08, Theorem 1.1]). Indeed, let $\widehat{Q}_1, \ldots, \widehat{Q}_n \subset \mathbb{R}^{n+1}$ be the Newton polytopes of the polynomials $\widehat{h}_1, \ldots, \widehat{h}_n$ of (5.11), and let $\Delta \subset \mathbb{R}^{n+1}$ be the standard n–dimensional simplex in the hyperplane $\{T = 0\}$. Then the following estimate holds:

$$\deg_T M_u \leq E := \mathcal{M}(\Delta, \widehat{Q}_1, \ldots, \widehat{Q}_n). \tag{5.36}$$

Furthermore, equality holds in (5.36) for a generic choice of the coefficients of the polynomials $\widehat{h}_i$ and the linear form u.

Our purpose is to exhibit a procedure for computing the unique monic multiple $\widehat{m}_u$ in $\mathbb{Q}(T)[Y]$ of M_u of degree D. This polynomial can be alternatively defined in terms of the Puiseux series solutions to the polynomials $\widehat{h}_1, \dots, \widehat{h}_n$ as we explain in what follows.

Since the projection map $\pi : \widehat{V} \to \mathbb{A}^1$ is dominant, it induces an extension $\mathbb{Q}[T] \hookrightarrow \mathbb{Q}[\widehat{V}]$, where $\mathbb{Q}[\widehat{V}]$ denotes the coordinate ring of $\widehat{V}$. This variety being a curve, $\mathbb{Q}[\widehat{V}]$ turns out to be a finitely generated $\mathbb{Q}[T]$-module. Thus, tensoring with $\mathbb{Q}(T)$, we deduce that $\mathbb{Q}[\widehat{V}] \otimes \mathbb{Q}(T)$ is a $\mathbb{Q}(T)$-vector space of finite dimension. We claim that $\mathbb{Q}[\widehat{V}] \otimes \mathbb{Q}(T) = \mathbb{Q}[V(I)] \otimes \mathbb{Q}(T)$ holds. Indeed, since $\widehat{V}$ consists of the irreducible components of $V(I)$ which are mapped dominantly onto $\mathbb{A}^1$ by the projection π, for each of the remaining irreducible components $\mathcal{C}$ of $V(I)$, the set $\pi(\mathcal{C}) \subset \mathbb{C}$ is a zero-dimensional $\mathbb{Q}$-definable variety. This implies that $I(\mathcal{C}) \cap \mathbb{Q}[T] \neq \{0\}$ holds.

Let $\widehat{m}_u$ be the minimal polynomial of u in the extension $\mathbb{Q}(T) \hookrightarrow \mathbb{Q}[\widehat{V}] \otimes \mathbb{Q}(T)$. The fact that $\mathbb{Q}[\widehat{V}] \otimes \mathbb{Q}(T)$ is finite-dimensional $\mathbb{Q}(T)$-vector space shows that the affine variety $\mathbb{V} := \{\bar{x} \in \mathbb{A}^n(\overline{\mathbb{Q}}(T)^*) : \widehat{h}_1(\bar{x}) = 0, \dots, \widehat{h}_n(\bar{x}) = 0\}$ has dimension zero. Here $\overline{\mathbb{Q}}(T)^* := \bigcup_{q \in \mathbb{N}} \overline{\mathbb{Q}}((T^{1/q}))$ denotes the field of Puiseux series in the variable T over $\overline{\mathbb{Q}}$ and $\widehat{h}_1, \dots, \widehat{h}_n$ are considered as elements of $\mathbb{Q}(T)[X]$. Our hypotheses imply that there exist D distinct n-tuples $x^{(\ell)} := (x_1^{(\ell)}, \dots, x_n^{(\ell)}) \in (\overline{\mathbb{Q}}(T)^*)^n$ of Puiseux series such that the following equalities hold in $\overline{\mathbb{Q}}(T)^*$ for $1 \le \ell \le D$:

$$\widehat{h}_1(x^{(\ell)}, T) = 0 \, , \; \dots \; , \; \widehat{h}_n(x^{(\ell)}, T) = 0 \tag{5.37}$$

(see [HS95]). Since $\mathbb{Q}[\widehat{V}] \otimes \mathbb{Q}(T)$ is the coordinate ring of the $\mathbb{Q}(T)$-variety $\mathbb{V}$, from (5.37) we deduce that the dimension of $\mathbb{Q}[\widehat{V}] \otimes \mathbb{Q}(T)$ over $\mathbb{Q}(T)$ equals D. Moreover, since $\deg_Y \widehat{m}_u = D$ holds as a consequence of our assumptions, we conclude that

$$\widehat{m}_u = \prod_{\ell=1}^{D} \big(Y - u(x^{(\ell)})\big). \tag{5.38}$$

Since $M_u(T, u(X)) \in I(\widehat{V})$, it follows that $M_u(T, u(X)) = 0$ holds in $\mathbb{Q}[\widehat{V}] \otimes \mathbb{Q}(T)$, from which we conclude that M_u is a multiple of $\widehat{m}_u$ by a factor in $\mathbb{Q}(T)[Y]$. Taking into account that both are polynomials of degree D in the variable Y and that $\widehat{m}_u$ is monic in this variable, we deduce that $\widehat{m}_u$ is the quotient of M_u by its leading coefficient. We summarize our arguments in the following statement.

Lemma 5.14. *Let $\pi_u : \widehat{V} \to \mathbb{A}^2$ be the projection defined by $\pi_u(x,t) := \big(t, u(x)\big)$. Assume that the identity* $\deg(\pi) = D$ *holds and let $M_u \in \mathbb{Q}[T,Y]$ be the minimal defining polynomial of the hypersurface $\overline{\pi_u(\mathbb{A}^2)}$. Denote by $\widehat{m}_u$ the only monic multiple of M_u in $\mathbb{Q}(T)[Y]$. Then $\widehat{m}_u(Y) = \prod_{\ell=1}^{D}(Y - u(x^{(\ell)}))$, where $x^{(1)}, \dots, x^{(D)} \in \mathbb{A}^n(\overline{\mathbb{Q}}(T)^*)$ are the solutions of* (5.37).

Next, we group the roots $u(x^{(\ell)})$ of the polynomial $\widehat{m}_u$ according to the facet from where they arise. With notations as in Section 5.2.1, let $\Gamma \subset \mathbb{Z}^{n+1}$ be the set of primitive integer vectors of the form $\gamma := (\gamma_1, \dots, \gamma_n, \gamma_{n+1}) \in \mathbb{Z}^{n+1}$ with $\gamma_{n+1} > 0$ for which there is a cell $C = (C^{(1)}, \dots, C^{(s)})$ of type $(k_1, \dots, k_s)$ of the subdivision of $\mathcal{A}$ induced by ω such that $\widehat{C}$ has inner normal γ. As asserted in Section 5.2.1, if $\gamma \in \Gamma$ is the inner normal of the lifting $\widehat{C}$ of a cell C of type $(k_1, \dots, k_s)$, there exist $D_\gamma := k_1! \cdots k_s! \cdot \mathrm{Vol}(C)$ vectors of Puiseux series $x^{(j,\gamma)} := (x_1^{(j,\gamma)}, \dots, x_n^{(j,\gamma)}) \in \mathbb{A}^n(\mathbb{Q}(T)^*)$ $(1 \le j \le D_\gamma)$ of the form

$$x_i^{(j,\gamma)} := \sum_{m \ge 0} x_{i,m}^{(j,\gamma)} T^{\frac{\gamma_i + m}{\gamma_{n+1}}}$$

satisfying (5.37). Considering the projection of the branches of $\widehat{V}$ parametrized by the D_γ vectors of Puiseux series $x^{(j,\gamma)}$ for each $\gamma \in \Gamma$, we obtain the following element m_γ of $\mathbb{Q}(\!(T^{1/\gamma_{n+1}})\!)[Y]$:

$$m_\gamma := \prod_{j=1}^{D_\gamma} \big(Y - u(x^{(j,\gamma)})\big). \tag{5.39}$$

From (5.2) we conclude that (5.38) may be expressed in the following way:

$$\widehat{m}_u = \prod_{\gamma \in \Gamma} m_\gamma. \tag{5.40}$$

Since $\widehat{m}_u$ belongs to $\mathbb{Q}(T)[Y]$ and its primitive multiple $M_u \in \mathbb{Q}[T,Y]$ satisfies the degree estimate $\deg_T M_u \le E$, in order to compute the dense representation of $\widehat{m}_u$ we shall compute the Puiseux expansions of the coefficients of the factors $m_\gamma \in \mathbb{Q}(\!(T^{1/\gamma_{n+1}})\!)[Y]$ of $\widehat{m}_u$ truncated up to order $2E$. Using Padé approximation it is possible to recover the dense representation of $\widehat{m}_u$ from this data.

Fix $\gamma \in \Gamma$ and set $\mathbf{x}_m^{(j,\gamma)} := (x_{1,m}^{(j,\gamma)}, \dots, x_{n,m}^{(j,\gamma)})$ for every $m \geq 0$ and $1 \leq j \leq D_\gamma$. Since

$$\widehat{h}_i\Big(\sum_{m\geq 0} x_{1,m}^{(j,\gamma)} T^{\frac{\gamma_1+m}{\gamma_{n+1}}}, \dots, \sum_{m\geq 0} x_{n,m}^{(j,\gamma)} T^{\frac{\gamma_n+m}{\gamma_{n+1}}}, T\Big) = 0$$

holds for $1 \leq j \leq D_\gamma$ and $1 \leq i \leq n$, we have

$$\begin{aligned} 0 &= T^{-m_i}\widehat{h}_i\big(\textstyle\sum_{m\geq 0} x_{1,m}^{(j,\gamma)} T^{\gamma_1+m}, \dots, \sum_{m\geq 0} x_{n,m}^{(j,\gamma)} T^{\gamma_n+m}, T^{\gamma_{n+1}}\big) \\ &= T^{-m_i}\widehat{h}_i\big(T^{\gamma_1}\textstyle\sum_{m\geq 0} x_{1,m}^{(j,\gamma)} T^{m}, \dots, T^{\gamma_n}\sum_{m\geq 0} x_{n,m}^{(j,\gamma)} T^{m}, T^{\gamma_{n+1}}\big) \\ &= h_{i,\gamma}\big(\textstyle\sum_{m\geq 0} \mathbf{x}_m^{(j,\gamma)} T^m, T\big), \end{aligned}$$

according to (5.16). Therefore the polynomial $m_\gamma(T^{\gamma_{n+1}}, Y) \in \mathbb{Q}(\!(T)\!)[Y]$ can be expressed in terms of the power series solutions

$$\sigma^{(j,\gamma)} := (\sigma_1^{(j,\gamma)}, \dots, \sigma_n^{(j,\gamma)}) := \sum_{m\geq 0} \mathbf{x}_m^{(j,\gamma)} T^m \quad (1 \leq j \leq D_\gamma) \tag{5.41}$$

of $h_{1,\gamma}, \dots, h_{n,\gamma}$. Indeed, from (5.39) it follows that

$$\begin{aligned} m_\gamma(T^{\gamma_{n+1}}, Y) &= \textstyle\prod_{j=1}^{D_\gamma}\big(Y - \sum_{i=1}^n u_i \sum_{m\geq 0} x_{i,m}^{(j,\gamma)} T^{\gamma_i+m}\big) \\ &= \textstyle\prod_{j=1}^{D_\gamma}\big(Y - \sum_{m\geq 0}\sum_{i=1}^n u_i x_{i,m}^{(j,\gamma)} T^{\gamma_i} T^m\big) \\ &= \textstyle\prod_{j=1}^{D_\gamma}\big(Y - \sum_{m\geq 0} u_\gamma(\mathbf{x}_m^{(j,\gamma)}) T^m\big) \\ &= \textstyle\prod_{j=1}^{D_\gamma}\big(Y - u_\gamma(\sum_{m\geq 0} \mathbf{x}_m^{(j,\gamma)} T^m)\big) \ =: \ m_{u_\gamma}(T, Y), \end{aligned}$$

where $u_\gamma := \sum_{i=1}^n u_i T^{\gamma_i} X_i$. In conclusion, we have the following result.

Lemma 5.15. *Fix $\gamma := (\gamma, \dots, \gamma_{n+1}) \in \Gamma$ and let m_γ be as in* (5.39)*. Then the Laurent polynomial $m_\gamma(T^{\gamma_{n+1}}, Y) \in \mathbb{Q}(\!(T)\!)[Y]$ equals the minimal polynomial $m_{u_\gamma}(T,Y)$ of the projection induced by $u_\gamma := \sum_{i=1}^n u_i T^{\gamma_i} X_i$ on the subvariety of $\mathbb{A}^n(\overline{\mathbb{Q}}(T)^*)$ consisting of the set of power series $\{\sigma^{(1,\gamma)}, \dots, \sigma^{(D_\gamma,\gamma)}\}$ of* (5.41)*.*

This lemma will be critical in order to obtain suitable approximations to the Laurent polynomials $m_\gamma(T^{\gamma_{n+1}}, Y)$ in $\mathbb{Q}(\!(T)\!)[Y]$.

A procedure for computing $\widehat{m}_u$.

Now we exhibit a procedure for computing the minimal polynomial $\widehat{m}_u$, which is based on the computation of the Laurent polynomials m_γ arising in the factorization of $\widehat{m}_u = \prod_{\gamma\in\Gamma} m_\gamma$ in terms of Puiseux expansions according to Lemmas 5.14 and 5.15. Then we will apply Lemma 2.4 to this procedure in order to obtain an algorithm for computing a geometric solution of the curve $\widehat{V}$.

In order to describe this approximation, we recall the following terminology: for $G, \widetilde{G} \in \overline{\mathbb{Q}}((T))$ and $s \in \mathbb{Z}$, we say that $\widetilde{G}$ approximates G with precision s in $\overline{\mathbb{Q}}((T))$ if the Laurent series $G - \widetilde{G}$ has order at least $s+1$ in T. We shall use the notation $G \equiv \widetilde{G} \bmod (T^{s+1})$. Furthermore, if $G, \widetilde{G}$ are two elements of a polynomial ring $\overline{\mathbb{Q}}((T))[Y]$, we say that $\widetilde{G}$ approximates G with precision s if every coefficient $\widetilde{a} \in \overline{\mathbb{Q}}((T))$ of $\widetilde{G}$ approximates the corresponding coefficient $a \in \overline{\mathbb{Q}}((T))$ of G with precision s (in the sense of the previous definition).

Fix $\gamma := (\gamma_1, \dots, \gamma_n) \in \Gamma$. Let $V_\gamma := \{\sigma^{(j,\gamma)} : 1 \le j \le D_\gamma\}$ denote the subset of $\mathbb{V}$ underlying γ. In order to compute the required approximation of the polynomial m_{u_γ} of the statement of Lemma 5.15, we first compute a corresponding approximation of the polynomials that form a geometric solution of the variety V_γ. Observe that

$$\begin{aligned}\{\sigma^{(j,\gamma)}(0) : 1 \le j \le D_\gamma\} &= \{\mathrm{x}_0^{(j,\gamma)} : 1 \le j \le D_\gamma\} \\ &= V(h_{1,\gamma}^{(0)}, \dots, h_{n,\gamma}^{(0)}) \cap (\mathbb{C}^*)^n \\ &= V(h_{1,\gamma}(X,0), \dots, h_{n,\gamma}(X,0)) \cap (\mathbb{C}^*)^n = V_{0,\gamma}\end{aligned}$$

holds. Since $\det(\partial h_{i,\gamma}(X,0)/\partial X_k)_{1\le i,k\le n}(\mathrm{x}_0^{(j,\gamma)}) \ne 0$ holds for $1 \le j \le D_\gamma$, we may apply of the global Newton iterator of [GLS01] in order to “lift” the given geometric solution of $V_{0,\gamma}$ to the geometric solution of the variety V_γ associated to the linear form $u \in \mathbb{Q}[X]$ with any prescribed precision.

Suppose that we are given polynomials $m_{u,\gamma}^{(0)}, w_{u,1,\gamma}^{(0)}, \dots, w_{u,n,\gamma}^{(0)} \in \mathbb{Q}[Y]$ which form a geometric solution of $V_{0,\gamma}$, as provided by the algorithm underlying Theorem 5.11. Recall that $m_{u,\gamma}^{(0)}\big(u(\mathrm{x}_0^{(j)})\big) = 0$ and $(\mathrm{x}_0^{(j,\gamma)})_i = w_{u,i,\gamma}^{(0)}\big(u(\mathrm{x}_0^{(j)})\big)$ hold for $1 \le i \le n$ and $1 \le j \le D_\gamma$. The global Newton iterator is a recursive procedure whose kth step computes approximations $m_{u,\gamma}^{(k)}, w_{u,1,\gamma}^{(k)}, \dots, w_{u,n,\gamma}^{(k)} \in$

$\mathbb{Q}[T,Y]$ of the polynomials $m_{u,\gamma}, w_{u,1,\gamma}, \dots, w_{u,n,\gamma}$ which form the geometric solution of V_γ associated with the linear form u with precision 2^k for any $k \geq 0$.

We may assume without loss of generality that $\gamma_i \geq 0$ and $0 = \min\{\gamma_1, \dots, \gamma_n\}$ hold for $1 \leq i \leq n$. Indeed, if there exists $\gamma_i < 0$, setting $\gamma_{i_0} := \min\{\gamma_1, \dots, \gamma_n\}$ we have

$$\begin{aligned} T^{-\gamma_{i_0}D_\gamma} m_\gamma(T^{\gamma_{n+1}}, T^{\gamma_{i_0}}Y) &= \prod_{j=1}^{D_\gamma} T^{-\gamma_{i_0}} \Big(T^{\gamma_{i_0}} Y - \sum_{i=1}^{n} u_i \sum_{m \geq 0} x_{i,m}^{(j,\gamma)} T^{\gamma_i + m} \Big) \\ &= \prod_{j=1}^{D_\gamma} \Big(Y - T^{-\gamma_{i_0}} \sum_{i=1}^{n} u_i \sum_{m \geq 0} x_{i,m}^{(j,\gamma)} T^{\gamma_i + m} \Big) \\ &= \prod_{j=1}^{D_\gamma} \Big(Y - \sum_{i=1}^{n} u_i \sum_{m \geq 0} x_{i,m}^{(j,\gamma)} T^{\gamma_i - \gamma_{i_0} + m} \Big). \end{aligned} \tag{5.42}$$

Since $\gamma_i - \gamma_{i_0} \geq 0$ holds for $1 \leq i \leq n$, this shows that the computation of an approximation of $m_{u_\gamma} = m_\gamma(T^{\gamma_{n+1}}, Y)$ can be easily reduced to a situation in which $\gamma_i \geq 0$ holds for $1 \leq i \leq n$.

Note that the global Newton iterator cannot be directly applied in order to compute the geometric solution of $\{\sigma^{(j,\gamma)}; 1 \leq j \leq D_\gamma\}$ associated with the linear form $u_\gamma \in \mathbb{Q}[T][X]$, because the coefficients of u_γ are nonconstant polynomials of $\mathbb{Q}[T]$. Indeed, two critical problems arise:

1. Although by hypothesis u_γ separates the points of V_γ, it might not separate the points of $V_{0,\gamma}$ and it is not clear from which precision on, the corresponding approximations of the points of V_γ are separated by u_γ. Requiring u_γ to be a separating form for all the approximations of the points of V_γ is an essential hypothesis for the iterator of [GLS01] which cannot be suppressed without causing a significant growth of the complexity of the procedure (see [Lec02], [Lec03]).

2. The iterator of [GLS01] makes critical use of the fact that the coefficients of the linear form under consideration are elements of $\mathbb{Q}$ in order to determine how a given precision can be achieved.

Nevertheless, we shall exhibit a modification of the procedure which computes an approximation of $m_{u_\gamma}(T,Y)$ with precision $2\gamma_{n+1}E$ without changing the asymptotic number of arithmetic operations performed.

In order to circumvent (1) we require an additional generic condition on the coefficients $u_1,\ldots,u_n$ defining $u_\gamma := \sum_{i=1}^n u_i T^{\gamma_i} X_i$, namely, the u_γ separates the first M_γ terms of the series $\sigma^{(j,\gamma)}$. Our next result asserts that for a random choice of the coefficients u_γ, this condition is likely to be satisfied.

Lemma 5.16. *For a random choice of values $u_1,\ldots,u_n$ in the set $\{1,\ldots,\rho D_\gamma^2\}$, the linear form $u_\gamma := \sum_{i=1}^n u_i T^{\gamma_i} X_i$ separates the initial terms $\sum_{m=0}^{M_\gamma} \mathrm{x}_m^{(j,\gamma)} T^m$ of the power series $\sigma^{(j,\gamma)}$ $(1 \le j \le D_\gamma)$ with probability at least $1-1/\rho$, where $M_\gamma := \max\{\gamma_1,\ldots,\gamma_n\}$.*

Proof. For a given linear form $u_\gamma := \sum_{i=1}^n u_i T^{\gamma_i} X_i$ as in the statement of the lemma, we have $u_\gamma(\sigma^{(j,\gamma)}) = \sum_{m\ge 0} \big(\sum_{i=1}^n u_i x_{i,m-\gamma_i}^{(j,\gamma)}\big) T^m$ for every $1 \le j \le D_\gamma$, where $x_{i,m-\gamma_i}^{(j,\gamma)} := 0$ for $m < \gamma_i$. We make the following claim.

Claim 5.17. *Let $\Lambda_1,\ldots,\Lambda_n$ be indeterminates over $\mathbb{C}[T,X]$. Then the following inequality holds for every $1 \le j,h \le D_\gamma$ with $j \ne h$:*

$$\sum_{m=0}^{M_\gamma} \Big(\sum_{i=1}^n \Lambda_i\, x_{i,m-\gamma_i}^{(j,\gamma)}\Big) T^m \ne \sum_{m=0}^{M_\gamma} \Big(\sum_{i=1}^n \Lambda_i\, x_{i,m-\gamma_i}^{(h,\gamma)}\Big) T^m.$$

Proof of Claim. Suppose on the contrary that there exist $j \ne h$ such that $\sum_{m=0}^{M_\gamma} \big(\sum_{i=1}^n \Lambda_i\, x_{i,m-\gamma_i}^{(j,\gamma)}\big) T^m = \sum_{m=0}^{M_\gamma} \big(\sum_{i=1}^n \Lambda_i\, x_{i,m-\gamma_i}^{(h,\gamma)}\big) T^m$. Substituting $T^{-\gamma_i}\Lambda_i$ for Λ_i in this identity for $i = 1,\ldots,n$, we have $\sum_{m=0}^{M_\gamma} \sum_{i=1}^n \Lambda_i\, x_{i,m-\gamma_i}^{(j,\gamma)} T^{m-\gamma_i} = \sum_{m=0}^{M_\gamma} \sum_{i=1}^n \Lambda_i\, x_{i,m-\gamma_i}^{(h,\gamma)} T^{m-\gamma_i}$, that is

$$\sum_{i=1}^n \sum_{m=0}^{M_\gamma-\gamma_i} \Lambda_i\, x_{i,m}^{(j,\gamma)} T^m = \sum_{i=1}^n \sum_{m=0}^{M_\gamma-\gamma_i} \Lambda_i\, x_{i,m}^{(h,\gamma)} T^m.$$

Substituting 0 for T in this identity, we deduce that

$$\sum_{i=1}^n \Lambda_i x_{i,0}^{(j,\gamma)} = \sum_{i=1}^n \Lambda_i x_{i,0}^{(h,\gamma)},$$

which contradicts the fact that the vectors $\mathbf{x}_0^{(j,\gamma)} = (x_{1,0}^{(j,\gamma)},\ldots,x_{n,0}^{(j,\gamma)})$ $(1 \le j \le D_\gamma)$ are all distinct. This finishes the proof of the claim.

By the claim we see that the polynomial $\sum_{m=0}^{M_\gamma}\big(\sum_{i=1}^{n}\Lambda_i\,(x_{i,m-\gamma_i}^{(j,\gamma)}-x_{i,m-\gamma_i}^{(h,\gamma)})\big)T^m$ of $\mathbb{Q}[\Lambda][T]$ is nonzero, and therefore has a nonzero coefficient $a_{j,h}\in\mathbb{C}[\Lambda]$ for every $1\le j<h\le D_\gamma$. Consider the polynomial $A_\gamma(\Lambda):=\prod_{1\le j<h\le D_\gamma}a_{j,h}\in\mathbb{C}[\Lambda]$. Since $a_{j,h}$ has degree 1 for every $1\le j<h\le D_\gamma$, it follows that A has degree $\binom{D_\gamma}{2}$. Furthermore, for every $(u_1,\ldots,u_n)\in\mathbb{C}^n$ with $A_\gamma(u_1,\ldots,u_n)\neq 0$, the corresponding polynomial $u_\gamma:=\sum_{i=1}^{n}u_iT^{\gamma_i}X_i$ separates the initial terms $\sum_{m=0}^{M_\gamma}\mathrm{x}_m^{(j,\gamma)}T^m$ of the power series $\sigma^{(j,\gamma)}$ $(1\le j\le D_\gamma)$. Therefore, by Theorem 2.1 we see that, for a random choice of the coefficients $u_1,\ldots,u_n$ in the set $\{1,\ldots,\rho D_\gamma^2\}$, the linear form u_γ separates the first M_γ terms of the points of V_γ with probability at least $1-1/\rho$. □

Assume that the coefficients $u_1,\ldots,u_n$ satisfy the statement of the lemma. A straight-line program for computing the polynomials $h_{1,\gamma},\ldots,h_{n,\gamma}$ can be easily derived from one computing $h_1,\ldots,h_n$ and the coordinates of γ. We assume this given, Step II.2 completed, and defer its complexity analysis. The algorithm for computing an approximation of m_{u_γ} (Step II.3) consists of the following three steps:

(Step II.3.a) We compute a suitable approximation to the geometric solution of V_γ associated to the linear form $u:=\sum_{i=1}^{n}u_iX_i$ by means of $\kappa_0:=\lceil\log(M_\gamma+1)\rceil$ steps of the global Newton iterator of [GLS01].

(Step II.3.b) We use the approximation of the previous step in order to obtain a corresponding approximation $m_{u_\gamma}^{(\kappa_0)},w_{u_\gamma,1}^{(\kappa_0)},\ldots,w_{u_\gamma,n}^{(\kappa_0)}$ of the polynomials that form the geometric solution of V_γ associated with u_γ.

(Step II.3.c) We apply an adaptation of the global Newton iterator which takes as input the polynomials of the previous step $m_{u_\gamma}^{(\kappa_0)},w_{u_\gamma,1}^{(\kappa_0)},\ldots,w_{u_\gamma,n}^{(\kappa_0)}$ and outputs the required approximation to the polynomials $m_{u_\gamma},w_{u_\gamma,1},\ldots,w_{u_\gamma,n}$ that form the geometric solution of V_γ associated with u_γ.

Proposition 5.18. *Fix $\gamma:=(\gamma_1,\ldots,\gamma_n)\in\Gamma$ and assume that a geometric solution of the variety $V_{0,\gamma}$ is given, as provided by Theorem 5.11. Assume further that the coefficients of the linear form u of the given geometric solution of $V_{0,\gamma}$ are randomly chosen in the set $\{1,\ldots,4\rho D_\gamma^3\}$ for a given $\rho\in\mathbb{N}$. Then the algorithm above computes an approximation to the polynomial $m_{u_\gamma}\in\mathbb{Q}((T))[Y]$ with precision $2E\gamma_{n+1}$. The procedure requires*

$O\big((nL_\gamma + n^3)\mathsf{M}(D_\gamma)\big(\mathsf{M}(M_\gamma)\mathsf{M}(D_\gamma)/\log(M_\gamma) + \mathsf{M}(E\gamma_{n+1})\big)\big)$ *arithmetic operations in* $\mathbb{Q}$ *, where* $M_\gamma := \max\{\gamma_1, \ldots, \gamma_n\}$ *and* L_γ *is the number of arithmetic operations required to evaluate the polynomials* $h_{i,\gamma}$ *of* (5.16)*, and has error probability at most* $2/\rho$*.*

Proof. We consider Steps II.3.a, II.3.b, II.3.c in detail. Step II.3.a takes as input the given geometric solution $m_{u,\gamma}^{(0)}, w_{u,1,\gamma}^{(0)}, \ldots, w_{u,n,\gamma}^{(0)}$ of $V_{0,\gamma}$, and performs $\kappa_0 := \lceil \log(M_\gamma + 1)\rceil$ times the global Newton iterator of Theorem 2.2 to obtain polynomials $m_{u,\gamma}^{(\kappa_0)}, w_{u,1,\gamma}^{(\kappa_0)}, \ldots, w_{u,n,\gamma}^{(\kappa_0)} \in \mathbb{Q}[T, Y]$ such that the following conditions hold:

$(i)_{u,\kappa_0}$ $\deg_Y m_{u,\gamma}^{(\kappa_0)} = D_\gamma$ and $\deg_T m_{u,\gamma}^{(\kappa_0)} \le M_\gamma$,

$(ii)_{u,\kappa_0}$ $\deg_Y w_{u,i,\gamma}^{(\kappa_0)} < D_\gamma$ and $\deg_T w_{u,i,\gamma}^{(\kappa_0)} \le M_\gamma$ for $1 \le i \le n$,

$(iii)_{u,\kappa_0}$ $m_{u,\gamma}^{(\kappa_0)} \equiv \prod_{j=1}^{D_\gamma} \big(Y - \varphi_{\kappa_0}^{(j,\gamma)}\big) \bmod (T^{M_\gamma+1})$,

$(iv)_{u,\kappa_0}$ $\sigma_i^{(j,\gamma)} \equiv w_{u,i,\gamma}^{(\kappa_0)}\big(T, \varphi_{\kappa_0}^{(j,\gamma)}\big) \bmod (T^{M_\gamma+1})$ for $1 \le i \le n$.

Here $\varphi_{\kappa_0}^{(j,\gamma)}$ is the Taylor expansion of order 2^{κ_0} of the power series $u(\sigma^{(j,\gamma)})$, that is, $\varphi_{\kappa_0}^{(j,\gamma)} := \sum_{m=0}^{2^{\kappa_0}} u(\mathrm{x}_m^{(j,\gamma)})T^m$ for $1 \le j \le D_\gamma$.

According to Theorem 2.2, it follows that this step requires performing roughly $O\big((nL_\gamma + n^3)\mathsf{M}(D_\gamma)\mathsf{M}(M_\gamma)/\log(M_\gamma)\big)$ arithmetic operations in $\mathbb{Q}$, where L_γ denotes the number of arithmetic operations in $\mathbb{Q}$ required to evaluate the polynomials $h_{i,\gamma}$ of (5.16). Furthermore, in view of the application of Lemma 2.4 it is important to remark that this step does not involve any division by a nonconstant polynomial in the coefficients $u_1, \ldots, u_n$.

Next we discuss Step II.3.b. Here we obtain approximations $m_{u_\gamma}^{(\kappa_0)}, w_{u_\gamma,1}^{(\kappa_0)}, \ldots, w_{u_\gamma,n}^{(\kappa_0)}$ of the polynomials that form the geometric solution of V_γ associated with $u_\gamma = u(T^{\gamma_1}X_1, \ldots, T^{\gamma_n}X_n)$ with precision $2^{\kappa_0} \ge M_\gamma$, namely

- $\deg_Y m_{u_\gamma}^{(\kappa_0)} = D_\gamma$ and $\deg_T m_{u_\gamma}^{(\kappa_0)} \le 2^{\kappa_0}$,
- $\deg_Y w_{u_\gamma,i}^{(\kappa_0)} < D_\gamma$ and $\deg_T w_{u_\gamma,i}^{(\kappa_0)} \le 2^{\kappa_0}$ for $1 \le i \le n$,
- $m_{u_\gamma}^{(\kappa_0)} \equiv \prod_{j=1}^{D_\gamma} \big(Y - \phi_{\kappa_0}^{(j,\gamma)}\big) \bmod (T^{2^{\kappa_0}+1})$,
- $\sigma_i^{(j,\gamma)} \equiv w_{u_\gamma,i}^{(\kappa_0)}\big(T, \phi_{\kappa_0}^{(j,\gamma)}\big) \bmod (T^{2^{\kappa_0}+1})$ for $1 \le i \le n$.

Here $\phi_{\kappa_0}^{(j,\gamma)}$ is the Taylor expansion of $\phi^{(j,\gamma)} := u_\gamma(\sigma^{(j,\gamma)})$ of order 2^{κ_0} for $1 \leq j \leq D_\gamma$.

From conditions $(i)_{u,\kappa_0}$– $(iv)_{u,\kappa_0}$ and elementary properties of the resultant it is easy to see that $m_{u_\gamma}^{(\kappa_0)}$ satisfies the following identity:

$$m_{u_\gamma}^{(\kappa_0)}(Y) = Res_{\widetilde{Y}}\Big(Y - \sum_{i=1}^{n} u_i T^{\gamma_i} w_{u,i,\gamma}^{(\kappa_0)}(\widetilde{Y}),\ m_{u,\gamma}^{(\kappa_0)}(\widetilde{Y})\Big). \tag{5.43}$$

The resultant of the right-hand side is computed mod $(T^{M_\gamma+1})$ by interpolation in the variable Y to reduce the problem to the computation of D_γ resultants, as explained in the computation of the resultant in (5.34). These D_γ resultants involve two polynomials of $\mathbb{Q}[T, \widetilde{Y}]$ of degree in $\widetilde{Y}$ bounded by D_γ and are computed mod $(T^{M_\gamma+1})$. Hence we deduce that this step requires roughly $O\big(\mathsf{M}(D_\gamma)D_\gamma\mathsf{M}(M_\gamma)/\log(M_\gamma)\big)$ arithmetic operations in $\mathbb{Q}$.

We apply Lemma 2.4 in order to extend this procedure to an algorithm computing $m_{u_\gamma}^{(\kappa_0)}, w_{u_\gamma,1}^{(\kappa_0)}, \ldots, w_{u_\gamma,n}^{(\kappa_0)}$. For this purpose, we observe that a similar argument as in the proof of Proposition 5.9 proves that the denominators in $\mathbb{Q}[\Lambda]$ which arise during the computation of the D_γ resultants required to compute the minimal polynomial of the generic version $\sum_{i=1}^{n} \Lambda_i T^{\gamma_i} X_i$ of the linear form u_γ are divisors of a polynomial of $\mathbb{Q}[\Lambda]$ of degree at most $4D_\gamma^3$. Applying Theorem 2.1 we see that for a random choice of the coefficients $u_1, \ldots, u_n$ in the set $\{1, \ldots, 4\rho D_\gamma^3\}$ none of these denominators are annihilated with probability at least $1 - 1/\rho$.

Next, we consider Step II.3.c. For $\kappa_1 := \lceil \log(2\gamma_{n+1}E + 1) \rceil$, we apply $\kappa_1 - \kappa_0$ times an adaptation of the global Newton iterator of [GLS01] to the polynomials $m_{u_\gamma}^{(\kappa_0)}, w_{u_\gamma,1}^{(\kappa_0)}, \ldots, w_{u_\gamma,n}^{(\kappa_0)}$ computed in the previous step. In the kth iteration step, we compute polynomials $m_{u_\gamma}^{(k)}, w_{u_\gamma,1}^{(k)}, \ldots, w_{u_\gamma,n}^{(k)}$ satisfying:

- $\deg_Y m_{u_\gamma}^{(k)} = D$ and $\deg_T m_{u_\gamma}^{(k)} \leq 2^k$,
- $m_{u_\gamma}^{(k)} = \prod_{j=1}^{D_\gamma}(Y - \phi_k^{(j,\gamma)})$,
- $\deg_Y w_{u_\gamma,i}^{(k)} < D$ and $\deg_T w_{u_\gamma,1}^{(k)} \leq 2^k$ for $1 \leq i \leq n$,
- $\sigma_i^{(j,\gamma)} \equiv w_{u_\gamma,i}^{(k)}(T, \phi_k^{(j,\gamma)})$ mod (T^{2^k+1}) for $1 \leq i \leq n$.

Here $\phi_k^{(j,\gamma)}$ is the Taylor expansion of $\phi^{(j,\gamma)} := u_\gamma(\sigma^{(j,\gamma)})$ of order 2^k for $1 \leq j \leq D_\gamma$. In particular, it follows that $m_{u_\gamma}^{(\kappa_1)}$ is the required approximation to m_{u_γ} with precision $2\gamma_{n+1}E$.

Fix $\kappa_0 < k \leq \kappa_1$. We briefly describe how we can obtain an approximation with precision 2^k of the polynomials that form the geometric solution of V_γ associated to the linear form u_γ from an approximation with precision 2^{k-1}. Similarly to [GLS01], set $\Delta_k(T,Y) := u_\gamma(\widetilde{w}_{u_\gamma}^{(k)}) - u_\gamma(w_{u_\gamma}^{(k-1)}) = u_\gamma(\widetilde{w}_{u_\gamma}^{(k)}) - Y$, where $\widetilde{w}_{u_\gamma}^{(k)}$ is the result of applying a "classical Newton step" to $w_{u_\gamma}^{(k-1)}$, as described in [GLS01]. Furthermore, write $\Delta_m(T,Y) := T^{-1-2^{k-1}}(m_{u_\gamma}^{(k)} - m_{u_\gamma}^{(k-1)})$. Since $m_{u_\gamma}^{(k)}(Y+\Delta_k) \equiv 0 \mod (T^{2^k+1}, m_{u_\gamma}^{(k-1)})$ holds (see [DL08, §4.2]), it follows that

$$\begin{aligned}0 \equiv m_{u_\gamma}^{(k)}(Y+\Delta_k) &\equiv m_{u_\gamma}^{(k-1)}(Y+\Delta_k) + T^{2^{k-1}+1}\Delta_m(Y+\Delta_k) \mod (T^{2^k+1}, m_{u_\gamma}^{(k-1)})\\ &\equiv \Delta_k \frac{\partial m_{u_\gamma}^{(k-1)}}{\partial Y}(Y) + T^{2^{k-1}+1}\Delta_m(Y) \mod (T^{2^k+1}, m_{u_\gamma}^{(k-1)}).\end{aligned}$$

We conclude that the following congruence relation holds:

$$m_{u_\gamma}^{(k)} \equiv m_{u_\gamma}^{(k-1)} - \Big(\Delta_k \frac{\partial m_{u_\gamma}^{(k-1)}}{\partial Y} \mod m_{u_\gamma}^{(k-1)}\Big) \mod (T^{2^k+1}). \tag{5.44}$$

A similar argument proves the following congruence relation:

$$w_{u_\gamma,i}^{(k)} \equiv \widetilde{w}_{u_\gamma,i}^{(k-1)} - \Big(\Delta_k \frac{\partial \widetilde{w}_{u_\gamma,i}^{(k-1)}}{\partial Y} \mod m_{u_\gamma}^{(k-1)}\Big) \mod (T^{2^k+1}) \text{ for } 1 \leq i \leq n. \tag{5.45}$$

Each iteration of our adaptation of the global Newton iteration is based on (5.44) and (5.45), which are extensions of the corresponding congruence relations of [GLS01]. We first compute $\widetilde{w}_{u_\gamma}^{(k)}$ by a standard Newton-Hensel lifting, and then evaluate the expressions (5.44) and (5.45). With a similar analysis as in [GLS01, Proposition 7] we conclude that the whole procedure requires roughly $O\big((nL_\gamma + n^3)\mathsf{M}(D_\gamma)\mathsf{M}(E\gamma_{n+1})\big)$ arithmetic operations in $\mathbb{Q}$.

Finally, combining the complexity estimates of Steps II.3.a, II.3.b, II.3.c and the probability of achievement of the two generic conditions imposed to the coefficients $u_1, \ldots, u_n$ (the condition underlying Lemma 5.16 and the application of Lemma 2.4 in Step II.3.b), we deduce the statement of the proposition. □

Example. Consider the sparse polynomial system defined in (5.17) and their associated inner normals $\gamma^{(1)} = (2,-1,2)$, $\gamma^{(2)} = (-1,2,2)$ and $\gamma^{(3)} = (-1,-1,4)$. In (5.35) we have computed the geometric solutions for the varieties $V_{0,\gamma^{(i)}}$ $(i = 1,2,3)$ associated to the linear form $u := X_1 - X_2$.

From these geometric solutions, in the Step II of Algorithm 5.8 we obtain approximations to the polynomials $m_{u_{\gamma^{(i)}}}$ $(i = 1,2,3)$. For the next step, to compute a complete geometric solution of the variety associated to the linear form $u := X_1 - X_2$, we will deal with the first-order Taylor approximations of the minimal polynomials of the generic linear form $U := \Lambda_1 X_1 + \Lambda_2 X_2$ centered at $(\Lambda_1, \Lambda_2) = (1,-1)$. Recall that, in this case, $E = 3$ (see (5.10)):

- For $i = 1$, we have $\gamma^{(1)} = (2,-1,2)$, $D_{\gamma^{(1)}} = 2$. Following (5.42), we compute an approximation of $T^2 m_{\gamma^{(1)}}(T^2, T^{-1}Y)$ with precision 12 by applying our modified Newton-Hensel lifting to the geometric solution of $V_{0,\gamma^{(1)}}$ previously computed, thus obtaining:

$$\begin{aligned} m_1 = {} & Y^2 + \big(-4T^{11} + 4T^9 + 2T^3 + \big(4T^{11} + 6T^9 + 2T^7 + 2T^3\big)(\Lambda_1 - 1) + (8T^{11} + 2T^9 + 2T^7)(\Lambda_2 + 1)\big)Y \\ & -6T^{12} + T^8 + T^4 - 1 + (-10T^{12} - 6T^{10})(\Lambda_1 - 1) + (2T^{12} - 6T^{10} - 2T^8 - 2T^4 + 2)(\Lambda_2 + 1). \end{aligned}$$

- For $i = 2$, we have $\gamma^{(2)} = (-1,2,2)$, $D_{\gamma^{(2)}} = 2$. Following (5.42), we compute an approximation of $T^2 m_{\gamma^{(2)}}(T^2, T^{-1}Y)$ with precision 12 by applying our modified Newton-Hensel lifting to the geometric solution of $V_{0,\gamma^{(2)}}$, thus obtaining:

$$\begin{aligned} m_2 = {} & Y^2 + (4T^{11} - 4T^9 - 2T^3 + (8T^{11} + 2T^9 + 2T^7)(\Lambda_1 - 1) + (4T^{11} + 6T^9 + 2T^7 + 2T^3)(\Lambda_2 + 1))Y \\ & -6T^{12} + T^8 + T^4 - 1 + (-2T^{12} + 6T^{10} + 2T^8 + 2T^4 - 2)(\Lambda_1 - 1) + (10T^{12} + 6T^{10})(\Lambda_2 + 1). \end{aligned}$$

- For $i = 3$, we have $\gamma^{(3)} = (-1,-1,4)$, $D_{\gamma^{(3)}} = 4$. Following (5.42), we first compute an approximation of $T^4 m_{\gamma^{(3)}}(T^4, T^{-1}Y)$ with precision 24 by applying our modified Newton-Hensel lifting to the geometric solution of $V_{0,\gamma^{(3)}}$, thus obtaining:

$m_3 := Y^4 + ((-12T^{21} - 8T^{17} - 4T^{13} - 2T^5)(\Lambda_1 - 1) + (-12T^{21} - 8T^{17} - 4T^{13} - 2T^5)(\Lambda_2 + 1))Y^3 + (28T^{22} - 2T^{14} + 4T^{10} - 2T^6 + 8T^2 + (-28T^{22} + 2T^{14} - 4T^{10} + 2T^6 - 8T^2)(\Lambda_2 + 1) + +(+28T^{22} - 2T^{14} + 4T^{10} - 2T^6 + 8T^2)(\Lambda_1 - 1))Y^2 + ((-192T^{23} - 70T^{19} - 48T^{15} - 2T^{11} - 16T^7 - 8T^3)(\Lambda_1 - 1) + (-192T^{23} - 70T^{19} - 48T^{15} - 2T^{11} -$

$16T^7-8T^3)(\Lambda_2+1))Y+152T^{24}+66T^{20}-32T^{16}+33T^{12}-16-8T^8+(-304T^{24}-132T^{20}+64T^{16}-66T^{12}+16T^8+32)(\Lambda_2+1)+(304T^{24}+132T^{20}-64T^{16}+66T^{12}-16T^8-32)(\Lambda_1-1)$.

Using the algorithm of the statement of Proposition 5.18 for all $\gamma \in \Gamma$ we obtain approximations of the factors m_{u_γ} which allow us to compute the minimal polynomial $\widehat{m}_u$ and hence a geometric solution of $\widehat{V}$. Our next result outlines this procedure, comprising Step III of Algorithm 5.8, and estimates its complexity and error probability.

Proposition 5.19. *Suppose that we are given a geometric solution of the variety $V_{0,\gamma}$ for all $\gamma \in \Gamma$, as provided by Theorem 5.11, with a linear form $u \in \mathbb{Q}[X_1, \dots, X_n]$ whose coefficients are randomly chosen in the set $\{1, \dots, 4\rho D^4\}$, where ρ is a fixed positive integer. Then we can compute a geometric solution of the curve $\widehat{V}$ with*

$$O\big((n^3 N \log \mathcal{Q} + n^4)\mathsf{M}(\mathcal{M}_\Gamma)\mathsf{M}(D)\big(\mathsf{M}(D) + \mathsf{M}(E)\big)\big)$$

arithmetic operations in $\mathbb{Q}$ and error probability bounded by $1/\rho$. Here $N := \sum_{i=1}^n \#\Delta_i$, $\mathcal{Q} := \max_{1\le i\le n}\{\|q\|; q \in \Delta_i\}$, and $\mathcal{M}_\Gamma := \max_{\gamma\in\Gamma} \max\{\gamma_1, \dots, \gamma_{n+1}\}$.

Proof. For each $\gamma \in \Gamma$, we apply the algorithm underlying the proof of Proposition 5.18 in order to obtain an approximation of m_{u_γ} with precision $2\gamma_{n+1}E$. Due to Lemma 5.15, this polynomial immediately yields an approximation with precision $2E$ of $m_\gamma(T, Y)$ in $\mathbb{Q}(\!(T^{1/\gamma_{n+1}})\!)[Y]$.

Multiplying all these approximations, we obtain an approximation with precision $2E$ of the polynomial $\widehat{m}_u = \prod_{\gamma\in\Gamma} m_\gamma$ of (5.40). Since every coefficient $a_j(T)$ of $\widehat{m}_u \in \mathbb{Q}(T)[Y]$ is a rational function of $\mathbb{Q}(T)$ having a reduced representation with numerator and denominator of degree at most E, such a representation of $a_j(T)$ can be computed from its approximation with precision $2E$ using Padé approximation with $O(\mathsf{M}(E))$ arithmetic operations in $\mathbb{Q}$.

In order to estimate the complexity of the whole procedure, we estimate the complexity of its three main steps:

(*i*) the computation of the polynomials m_γ with precision $2E$ for all $\gamma \in \Gamma$, which requires $O\big(\sum_{\gamma\in\Gamma}(nL_\gamma + n^3)\mathsf{M}(D_\gamma)\big(\mathsf{M}(M_\gamma)\mathsf{M}(D_\gamma)/\log(M_\gamma) + \mathsf{M}(E\gamma_{n+1})\big)\big)$ arithmetic operations in $\mathbb{Q}$,

- (ii) the computation of the product $\prod_{\gamma\in\Gamma} m_\gamma$ with precision $2E$, which requires $O\big(\mathsf{M}(D)\mathsf{M}(E)\big)$ arithmetic operations in $\mathbb{Q}$,
- (iii) the computation of a reduced representation of all the coefficients of $\widehat{m}_u \in \mathbb{Q}(T)[Y]$, which requires $O\big(\mathsf{M}(E)D\big)$ arithmetic operations in $\mathbb{Q}$.

Observe that, from the sparse representation of the polynomials $h_1, \ldots, h_n$, we easily obtain a straight–line program computing the polynomials $h_{i,\gamma}$ of (5.16) with $O(nN\log(\mathcal{Q}M_\gamma))$ arithmetic operations in $\mathbb{Q}$ for every $\gamma \in \Gamma$, where $N := \sum_{i=1}^n \#\Delta_i$ and $\mathcal{Q} := \max_{1\le i\le n}\{\|q\|; q \in \Delta_i\}$. Therefore, the algorithm performs $O\big((n^2N\log\mathcal{Q} + n^3)\mathsf{M}(\mathcal{M}_\Gamma)\mathsf{M}(D)\big(\mathsf{M}(D) + \mathsf{M}(E)\big)\big)$ arithmetic operations in $\mathbb{Q}$, where $\mathcal{M}_\Gamma := \max_{\gamma\in\Gamma}\{M_\gamma, \gamma_{n+1}\}$.

Next we discuss how this procedure can be extended to the computation of a geometric solution of $\widehat{V}$. Two computations of the above procedure involve divisions by the coefficients u_i of the linear form u: the computation of the resultant of (5.43) for all $\gamma \in \Gamma$ and the Padé approximations of (iii). Both computations are reduced to D applications of the EEA, which is performed in a ring $\mathbb{Q}(\Lambda)$. A similar analysis as in Proposition 5.9 shows that all the denominators in $\mathbb{Q}[\Lambda]$ arising during such application of the EEA are divisors of a polynomial of degree $4D^4$. Therefore, according to Lemma 2.4, we conclude that a geometric solution of $\widehat{V}$ can be computed with $O\big((n^3N\log\mathcal{Q}+n^4)\mathsf{M}(\mathcal{M}_\Gamma)\mathsf{M}(D)\big(\mathsf{M}(D)+\mathsf{M}(E)\big)\big)$ arithmetic operations in $\mathbb{Q}$, with an algorithm with error probability at most $1/\rho$, provided that the coefficients of u are randomly chosen in the set $\{1, \ldots, 4\rho D^4\}$. □

Example. We continue with our previous example.

• For $i = 1$, the algorithm obtains an approximation $\widetilde{m}_{\gamma^{(1)}}$ of $m_{\gamma^{(1)}}$ by substituting $Y = TY$ in the polynomial m_1 previously computed, multiplying it by T^{-2} and replacing T^2 with T, which yields:

$$\widetilde{m}_{\gamma^{(1)}}{=}Y^2{+}(-4T^5{+}4T^4{+}2T{+}(8T^5{+}2T^4{+}2T^3)(\Lambda_2{+}1){+}(4T^5{+}6T^4{+}2T^3{+}2T)(\Lambda_1{-}1))Y$$
$$-6T^5 + T^3 + T - \frac{1}{T} + (2T^5 - 6T^4 - 2T^3 - 2T + \frac{2}{T})(\Lambda_2 + 1) + (-10T^5 - 6T^4)(\Lambda_1 - 1).$$

• For $i = 2$, the algorithm obtains an approximation $\widetilde{m}_{\gamma^{(2)}}$ of $m_{\gamma^{(2)}}$ by substituting $Y = TY$ in the polynomial m_2, multiplying it by T^{-2} and replacing T^2 with T, which yields:

$$\begin{aligned}\widetilde{m}_{\gamma^{(2)}} =& Y^2+(4T^5-4T^4-2T+(8T^5+2T^4+2T^3)(\Lambda_1-1)+(4T^5+6T^4+2T^3+2T)(\Lambda_2+1))Y\\ &-6T^5+T^3+T-\frac{1}{T}+(-2T^5+6T^4+2T^3+2T-\frac{2}{T})(\Lambda_1-1)+(10T^5+6T^4)(\Lambda_2+1).\end{aligned}$$

- For $i=3$, the algorithm obtains an approximation $\widetilde{m}_{\gamma^{(3)}}$ of $m_{\gamma^{(3)}}$ by substituting $Y=TY$ in the polynomial m_3, multiplying it by T^{-4} and replacing T^4 with T, which yields:

$$\begin{aligned}\widetilde{m}_{\gamma^{(3)}} =& Y^4+((-12T^5-8T^4-4T^3-2T)(\Lambda_1-1)+(-12T^5-8T^4-4T^3-2T)(\Lambda_2+1))Y^3+\\ &(28T^5-2T^3+4T^2-2T+8+(28T^5-2T^3+4T^2-2T+8)(\Lambda_1-1)+(-28T^5-2T^3-4T^2+2T-8)(\Lambda_2+1))Y^2\\ &+((-192T^5-70T^4-48T^3-2T^2-16T-8)(\Lambda_1-1)+(-192T^5-70T^4-48T^3-2T^2-16T-8)(\Lambda_2+1))Y\\ &+152T^5+66T^4-32T^3+33T^2-8T-\frac{16}{T}+(304T^5+132T^4-64T^3+66T^2-16T-\frac{32}{T})(\Lambda_1-1)\\ &+(-304T^5-132T^4+64T^3-66T^2+16T+\frac{32}{T})(\Lambda_2+1).\end{aligned}$$

Computing the first-order Taylor approximation centered at $(\Lambda_1,\Lambda_2)=(1,-1)$ of the product $\widetilde{m}_{\gamma^{(1)}}\widetilde{m}_{\gamma^{(2)}}\widetilde{m}_{\gamma^{(3)}}$ with precision $2E=6$ in the variable T, and applying a Padé approximation algorithm, we obtain the polynomial

$$\begin{aligned}M :=& Y^8+\frac{8T-2}{T}Y^6+\frac{2T^2-32T+1}{T^2}Y^4+\frac{-28T^2-2T+40}{T^2}Y^2+\frac{33T^3+24T^2-16}{T^3}+\\ &\Big(\frac{8T-2}{T}Y^6-10Y^5+\frac{4T^2-64T+2}{T^2}Y^4+\frac{-48T+14}{T}Y^3+\frac{-84T^2-6T+120}{T^2}Y^2+\frac{14T^2+80T-8}{T^2}Y+\\ &\frac{132T^3+96T^2-64}{T^3}\Big)(\Lambda_1-1)+(\frac{-8T+2}{T}Y^6-10Y^5+\frac{-4T^2+64T-2}{T^2}Y^4+\frac{-48T+14}{T}Y^3+\\ &\frac{84T^2+6T-120}{T^2}Y^2+\frac{14T^2+80T-8}{T^2}Y+\frac{-132T^3-96T^2+64}{T^3})(\Lambda_2+1).\end{aligned}$$

This polynomial is the first-order Taylor approximation centered at $(\Lambda_1,\Lambda_2)=(1,-1)$ of the minimal polynomial of the generic linear form $U:=\Lambda_1X_1+\Lambda_2X_2$.

Therefore, a geometric solution of the curve $\widehat{V}$ defined in (5.19) is given by the polynomials

$$\widehat{m}_u(Y),\quad \frac{\partial\widehat{m}_u}{\partial Y}X_1+\widehat{v}_1(Y),\quad \frac{\partial\widehat{m}_u}{\partial Y}X_2+\widehat{v}_2(Y),$$

where

- $\widehat{m}_u = Y^8 + \frac{8T-2}{T}Y^6 + \frac{2T^2-32T+1}{T^2}Y^4 + \frac{-28T^2-2T+40}{T^2}Y^2 + \frac{24T^2+33T^3-16}{T^3}$ is the polynomial obtained substituting $\Lambda_1 = 1, \Lambda_2 = -1$ in M,

- $\widehat{v}_1 = \frac{8T-2}{T}Y^6 - 10Y^5 + \frac{4T^2-64T+2}{T^2}Y^4 + \frac{-48T+14}{T}Y^3 + \frac{-84T^2-6T+120}{T^2}Y^2 + \frac{14T^2+80T-8}{T^2}Y + \frac{132T^3+96T^2-64}{T^3}$ is the partial derivative $\partial M/\partial\Lambda_1$,

- $\widehat{v}_2 = \frac{-8T+2}{T}Y^6 - 10Y^5 + \frac{-4T^2+64T-2}{T^2}Y^4 + \frac{-48T+14}{T}Y^3 + \frac{84T^2+6T-120}{T^2}Y^2 + \frac{14T^2+80T-8}{T^2}Y + \frac{-132T^3-96T^2+64}{T^3}$ is the partial derivative $\partial M/\partial\Lambda_2$.

Putting together Theorem 5.11 and Proposition 5.19 we obtain the main result of this section.

Theorem 5.20. *Let ρ be a fixed positive integer. Suppose that the coefficients of the linear form $\widetilde{u}$ of the statement of Theorem 5.11 and of the linear form u are randomly chosen in the set $\{1, \dots, 4n\rho D^4\}$. Then the algorithm underlying Theorem 5.11 and Proposition 5.19 computes a geometric solution of the curve $\widehat{V}$ with error probability $3/\rho$ performing $O\big((n^3 N \log \mathcal{Q} + n^4)\mathsf{M}(\mathcal{M}_\Gamma)\mathsf{M}(D)\big(\mathsf{M}(D) + \mathsf{M}(E)\big)\big)$ arithmetic operations in $\mathbb{Q}$. Here $N := \sum_{i=1}^n \#\Delta_i$, $\mathcal{Q} := \max_{1 \le i \le n}\{\|q\|; q \in \Delta_i\}$, and $\mathcal{M}_\Gamma := \max_{\gamma\in\Gamma}\|\gamma\|$.*

5.2.6. Solving the generic sparse system

Now we obtain a geometric solution of the zero-dimensional variety $V_1 := \{x \in \mathbb{C}^n : h_1(x) = 0, \dots, h_n(x) = 0\}$ from a geometric solution of the curve $\widehat{V}$.

With notations as in the previous section, we have that $V_1 = \pi^{-1}(1)$, where $\pi : \widehat{V} \to \mathbb{A}^1$ is the linear projection defined by $\pi(x,t) := t$. Moreover, due to Lemma 5.13, the equality $V_1 = \pi^{-1}(1) \cap V(\mathcal{I})$ holds.

This enables us to easily obtain a geometric solution of V_1 from a geometric solution of the curve $\widehat{V}$. Indeed, let $\widehat{m}_u(T,Y), \widehat{v}_1(T,Y), \dots, \widehat{v}_n(T,Y)$ be the polynomials which form a geometric solution of $\widehat{V}$ associated to a linear form $u \in \mathbb{Q}[X]$. Suppose further that the linear form u separates the points of V_1. Making the substitution $T = 1$, we obtain new polynomials $\widehat{m}_u(1,Y), \widehat{v}_1(1,Y), \dots, \widehat{v}_n(1,Y) \in \mathbb{Q}[Y]$ such that $\widehat{m}_u(1, u(X))$ and

$\frac{\partial \widehat{m}_u}{\partial Y}(1, u(X))X_i - \widehat{v}_i(1, u(X))$ $(1 \leq i \leq n)$ vanish over V_1. Taking into account that $\deg_Y(\widehat{m}_u) = D = \# V_1$ and that u separates the points of V_1, it follows that the polynomials $\widehat{m}_u(1, Y), \widehat{v}_1(1, Y), \ldots, \widehat{v}_n(1, Y) \in \mathbb{Q}[Y]$ form a geometric solution of V_1.

Proposition 5.21. *Let ρ be a fixed positive integer. With assumptions and notations as in Theorem 5.20, the algorithm described above computes a geometric solution of the zero-dimensional variety V_1 with error probability $4/\rho$ using $O\big((n^3 N \log \mathcal{Q} + n^4)\mathsf{M}(\mathcal{M}_\Gamma)\mathsf{M}(D)\big(\mathsf{M}(D) + \mathsf{M}(E)\big)\big)$ arithmetic operations in $\mathbb{Q}$.*

Example. By substituting 1 for T in the geometric solution of the curve $\widehat{V}$ defined in (5.19) computed in the previous section, we obtain a geometric solution of the zero-dimensional variety $V_1 = \{(x_1, x_2) \in \mathbb{C}^2 : 1 - x_1^2 - x_2^2 - x_1^2 x_2^2 = 0,\ 1 + x_1^2 x_2 + x_1 x_2^2 = 0\}$ defined by the system (5.17), namely,

$$m_u(Y), \quad \frac{\partial m_u}{\partial Y}(Y)X_1 + v_1(Y), \quad \frac{\partial m_u}{\partial Y}(Y)X_2 + v_2(Y),$$

where

- $m_u(Y) := \widehat{m}_u(1, Y) = Y^8 + 6Y^6 - 29Y^4 + 10Y^2 + 41,$
- $v_1(Y) := \widehat{v}_1(1, Y) = 6Y^6 - 10Y^5 - 58Y^4 - 34Y^3 + 30Y^2 + 86Y + 164,$
- $v_2(Y) := \widehat{v}_2(1, Y) = -6Y^6 - 10Y^5 + 58Y^4 - 34Y^3 - 30Y^2 + 86Y - 164.$

5.3. The solution of the input system

Let notations and assumptions be as in the previous sections. Assume that we are given a geometric solution $m_u(Y), v_1(Y), \ldots, v_n(Y)$ of the zero-dimensional variety V_1 defined by the polynomials $h_1 = f_1 + g_1, \ldots, h_n = f_n + g_n$. Assume further that the linear form u of such a geometric solution separates the points of the zero-dimensional variety $f_1 = 0, \ldots, f_n = 0$. In this section we describe a procedure for computing a geometric solution of the input system $f_1 = 0, \ldots, f_n = 0$.

For this purpose, we introduce an indeterminate T over $\mathbb{Q}[X]$ and consider the "deformation" $F_1, \ldots, F_n \in \mathbb{Q}[X, T]$ of the polynomials $f_1, \ldots, f_n$ defined in the following way:

$$F_i(X,T) := f_i(X) + (1-T)g_i(X) \quad (1 \leq i \leq n). \tag{5.46}$$

Set $\mathcal{V} := \{(x,t) \in \mathbb{A}^{n+1} : F_1(x,t) = 0, \ldots, F_n(x,t) = 0\}$ and denote by $\pi : \mathcal{V} \to \mathbb{A}^1$ the projection map defined by $\pi(x,t) := t$. As in Subsection 5.2.5, we introduce the variety $\mathcal{V}_{\mathrm{dom}} \subset \mathbb{A}^{n+1}$ defined as the union of all the irreducible components of $\mathcal{V}$ whose projection over $\mathbb{A}^1$ is dominant.

5.3.1. Solution of the second deformation

In this section we describe an efficient procedure for computing a geometric solution of $\mathcal{V}_{\mathrm{dom}}$ from the geometric solution of $\pi^{-1}(0)$ provided by Proposition 5.21.

Since $\pi^{-1}(0)$ is the variety defined by the "sufficiently generic" sparse system $h_1(X) = F_1(X,0) = 0, \ldots, h_n(X) = F_n(X,0) = 0$, with similar arguments to those leading to the proof of Lemma 5.13, it is not difficult to see that the polynomials $F_1, \ldots, F_n$, the variety $\mathcal{V}$, the projection $\pi : \mathcal{V} \to \mathbb{A}^1$, and the fiber $\pi^{-1}(0)$ satisfy all the assumptions of Lemma 5.12. We conclude that $\mathcal{V}_{\mathrm{dom}}$ is a curve and that the identity $\mathcal{V} \cap \pi^{-1}(0) = \mathcal{V}_{\mathrm{dom}} \cap \pi^{-1}(0)$ holds. Furthermore, Lemma 5.12 implies that all the hypotheses of [Sch03, Theorem 2] are satisfied.

Therefore, applying the "formal Newton lifting process" underlying Theorem 2.2, we compute polynomials $\widetilde{m}_u(T,Y), \widetilde{v}_1(T,Y), \ldots, \widetilde{v}_n(T,Y) \in \mathbb{Q}[T,Y]$ which form a geometric solution of $\mathcal{V}_{\mathrm{dom}}$. The formal Newton lifting process requires $O\big((nL' + n^4)\mathsf{M}(D)\mathsf{M}(E')\big)$ arithmetic operations in $\mathbb{Q}$, where L' denotes the number of arithmetic operations required to evaluate $F_1, \ldots, F_n$ and E' is any upper bound of the degree of $\widetilde{m}_u$ in the variable T.

In order to estimate the quantity L', we observe that from the sparse representation of the polynomials $f_1, \ldots, f_n, h_1, \ldots, h_n$ we easily obtain a straight–line program of length at most $O(nN \log \mathcal{Q})$ which evaluates $f_1, \ldots, f_n, h_1, \ldots, h_n$. Therefore, the polynomials $F_1, \ldots, F_n$ can also be represented by a straight–line program of length at most $O(nN \log \mathcal{Q})$.

Furthermore, we can apply Lemma 5.3 in order to estimate $\deg_T \widetilde{m}_u$ in combinatorial terms. Indeed, let $\widetilde{Q}_1, \ldots, \widetilde{Q}_n \subset \mathbb{R}^{n+1}$ be the Newton polytopes of $F_1, \ldots, F_n$ and let $\Delta \subset \mathbb{R}^{n+1}$ be the standard n–dimensional simplex in the hyperplane $\{T = 0\}$. Since $\widetilde{Q}_i \subset Q_i \times [0,1]$ holds for $1 \leq i \leq n$, where $Q_i \subset \mathbb{R}^n$ is the Newton polytope of h_i, by (5.5) of Lemma 5.3 we deduce the following estimate:

$$\deg_T \widetilde{m}_u \leq E' := \sum_{i=1}^{n} \mathcal{M}(\Delta, Q_1, \dots, Q_{i-1}, Q_{i+1}, \dots, Q_n). \qquad (5.47)$$

With this estimate for L' and this definition of E', we have the following result.

Proposition 5.22. *Suppose that we are given a geometric solution of the variety V_1, as provided by Proposition 5.21. A geometric solution of $\mathcal{V}_{\mathrm{dom}}$ can be deterministically computed with $O\big((n^2 N \log \mathcal{Q} + n^4)\mathsf{M}(D)\mathsf{M}(E')\big)$ arithmetic operations in $\mathbb{Q}$.*

5.3.2. Solving the input system

Making the substitution $T = 1$ in the polynomials $\widetilde{m}_u(T,Y), \widetilde{v}_i(T,Y)$ $(1 \leq i \leq n)$ which form the geometric solution of $\mathcal{V}_{\mathrm{dom}}$ computed by the algorithm of Proposition 5.22 we obtain polynomials $\widetilde{m}_u(1,Y), \widetilde{v}_1(1,Y), \dots, \widetilde{v}_n(1,Y) \in \mathbb{Q}[Y]$ which represent a complete description of our input system $f_1(X) = 0, \dots, f_n(X) = 0$, eventually including multiplicities. Such multiplicities are represented by multiple factors of $\widetilde{m}_u(1,Y)$, which are also factors of $\widetilde{v}_1(1,Y), \dots, \widetilde{v}_n(1,Y)$ (see, e.g., [GLS01, §6.5]). In order to remove them, we compute $a(Y) := \gcd\big(\widetilde{m}_u(1,Y), (\partial \widetilde{m}_u/\partial Y)(1,Y)\big)$, and the polynomials $m(Y) := \widetilde{m}_u(1,Y)/a(Y)$, $b(Y) := \big((\partial \widetilde{m}_u/\partial Y)(1,Y)/a(Y)\big)^{-1} \bmod m(Y)$, and $w_i(Y) := b(Y)\big(\widetilde{v}_i(1,Y)/a(Y)\big) \bmod m(Y)$ $(1 \leq i \leq n)$. Then $m, w_1, \dots, w_n$ form a geometric solution of our input system and can be computed with $O\big(n\mathsf{M}(D)E'\big)$ additional arithmetic operations in $\mathbb{Q}$.

Summarizing, we sketch the whole procedure computing a geometric solution of the input system $f_1 = 0, \dots, f_n = 0$. Fix $\rho \geq 4$. We randomly choose the coefficients of the polynomials $g_1, \dots, g_n$ in the set $\{1, \dots, 4\rho(nd)^{2n+1} + 2\rho n^2 2^{\mathcal{N}_1 + \cdots + \mathcal{N}_s}\}$ and coefficients of linear forms $u, \widetilde{u}$ in the set $\{1, \dots, 16n\rho D^4\}$. By Theorem 2.1 it follows that the polynomials $g_1, \dots, g_n$ and the linear forms $u, \widetilde{u}$ satisfy all the conditions required with probability at least $1 - 1/\rho$. Then we apply the algorithms underlying Propositions 5.21 and 5.22 in order to obtain a geometric solution of the variety $\mathcal{V}_{\mathrm{dom}}$. Finally, we use the procedure above to compute a geometric solution of the input system $f_1 = 0, \ldots, f_n = 0$. This yields the following result.

Theorem 5.23. *The algorithm sketched above computes a geometric solution of the input system $f_1 = 0, \ldots, f_n = 0$ with error probability at most $1/\rho$ using*

$$O\Big(\big(n^3 N \log \mathcal{Q} + n^4\big)\, \mathsf{M}(D)\, \big(\mathsf{M}(\mathcal{M}_\Gamma)\big(\mathsf{M}(D) + \mathsf{M}(E)\big) + \mathsf{M}(E')\big)\Big)$$

arithmetic operations in $\mathbb{Q}$. Here $N := \sum_{i=1}^{n} \#\Delta_i$, $\mathcal{M}_\Gamma := \max_{\gamma \in \Gamma} \|\gamma\|$, $\mathcal{Q} := \max_{1 \leq i \leq n}\{\|q\|; q \in \Delta_i\}$ and E, E' are defined in (5.36) *and* (5.47) *respectively.*

We remark that our algorithm can be applied *mutatis mutandis* in order to compute the isolated points of an input system having a solution set with positive-dimensional components. Indeed, since the first deformation is not determined by the input system but by its monomial structure, it computes a geometric solution of a generic sparse system as described in Section 5.2. Then we execute our second deformation on the polynomials $F_1, \ldots, F_n$ of (5.46), considering the saturation $(I : J^\infty)$, where $I := (F_1, \ldots, F_n) \subset \mathbb{Q}[X, T]$ and J denotes the Jacobian determinant of $F_1, \ldots, F_n$ with respect to the variables X. From Lemma 5.12 it follows that positive–dimensional components of $f_1 = 0, , \ldots, f_n = 0$ are “cleaned” by the saturation $(I : J^\infty)$. Hence, our algorithm properly outputs the isolated points of $f_1 = 0, , \ldots, f_n = 0$, as stated.

Bibliography

[ABRW96] M.E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeroes, multiplicities and idempotents for zerodimensional systems. In *Algorithms in Algebraic Geometry and Applications, Proceedings of MEGA'94*, volume 143 of *Progr. Math.*, pages 1–15, Boston, 1996. Birkhäuser.

[ANMR91] M.E. Alonso, G. Niesi, T. Mora, and M. Raimondo. Local parametrizations of space curves at singular points. In *Computer Graphics and Mathematics*, Eurographic Seminar Series, pages 61–90, Berlin Heidelberg New York, 1991. Springer.

[ANMR92] M.E. Alonso, G. Niesi, T. Mora, and M. Raimondo. An algorithm for computing analytic branches of space curves at singular points. In *Proceedings 1992 International Workshop on Mathematics Mechanization, Beijing, China, July 16-18, 1992*, pages 135–166. International Academic Publishers, 1992.

[Art76] M. Artin. *Lectures on deformation of singularities*, volume 54 of *Tata Inst. Fundam. Res. Lect. Math.* Tata Inst. Fund. Res., Bombay, 1976.

[Bar04] M. Bardet. *Etude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie.* PhD thesis, Université Paris 6, 2004.

[BCS97] P. Bürgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren Math. Wiss.* Springer, Berlin, 1997.

[BCSS98] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation.* Springer, New York Berlin Heidelberg, 1998.

[BDG88] J.L. Balcázar, J. Díaz, and J. Gabarró. *Structural complexity I*, volume 11 of *Monogr. Theoret. Comput. Sci. EATCS Ser.* Springer, Berlin, 1988.

[Ber75] D.N. Bernstein. The number of roots of a system of equations. *Funct. Anal. Appl.*, 9:183–185, 1975.

[BLS03] A. Bostan, G. Lecerf, and E. Schost. Tellegen's principle into practice. In J.R. Sendra, editor, *Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC'03) (Philadelphia, USA, August 3–6, 2003)*, pages 37–44, New York, 2003. ACM Press.

[BM93] D. Bayer and D. Mumford. What can be computed in algebraic geometry? In D. Eisenbud and L. Robbiano, editors, *Computational Algebraic Geometry and Commutative Algebra*, volume XXXIV of *Sympos. Math.*, pages 1–49, Cambridge, 1993. Cambridge Univ. Press.

[BM96] D. Bini and B. Mourrain. Polynomial test suite. `http://www-sop.inria.fr/saga/POL`, 1996.

[BMWW04] A. Bompadre, Guillermo Matera, Rosita Wachenchauzer, and Ariel Waissbein. Polynomial equation solving by lifting procedures for ramified fibers. *Theor. Comput. Sci.*, 315(2-3):335–369, 2004.

[Bom00] A. Bompadre. Un problema de eliminación geométrica en sistemas de Pham–Brieskorn. Master's thesis, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, 2000.

[BP94] D. Bini and V. Pan. *Polynomial and matrix computations.* Progress in Theoretical Computer Science. Birkhäuser, Boston, 1994.

[BP06] C. Beltrán and L.M. Pardo. Non universal polynomial equation solving. In L.M. Pardo *et al.*, editor, *Foundations of Computational Mathematics, Santander 2005*, volume 331 of *London*

Math. Soc. Lecture Note Ser., pages 1–35, Cambridge, 2006. Cambridge Univ. Press.

[BR01] J. Fernandez Bonder and J. Rossi. Blow-up vs. spurious steady solutions. *Proc. Amer. Math. Soc.*, 129(1):139—144, 2001.

[Bro87] D.W. Brownawell. Bounds for the degree in the Nullstellensatz. *Ann. of Math.*, 126:577–591, 1987.

[BS83] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoret. Comput. Sci.*, 22:317–330, 1983.

[BS05] A. Bostan and E. Schost. Polynomial evaluation and interpolation on special sets of points. *J. Complexity*, 21(4):420–446, 2005.

[Buc85] B. Buchberger. Gröbner bases: An algoritmic method in polynomial ideal theory. In N. K. Bose et al, editor, *Multidimensional System Theory*, pages 374–383. Reidel, Dordrecht, 1985.

[BW93] T. Becker and V. Weispfenning. *Gröbner bases. A computational approach to commutative algebra*, volume 141 of *Grad. Texts in Math.* Springer, New York, 1993.

[Can84] J. Cannon. *The one-dimensional heat equation.* Cambridge University Press, Cambridge, 1984.

[CDS96] E. Cattani, A. Dickenstein, and B. Sturmfels. Computing multidimensional residues. In T. Recio and L. González-Vega, editors, *Algorithms in Algebraic Geometry and Applications, Proceedings of the MEGA-94 conference, Santander, Spain, April 5-9, 1994*, volume 143 of *Progr. Math.*, Basel, 1996. Birkhäuser.

[CFQ91a] M Chipot, M Fila, and P Quittner. Stationary solutions. blow up and convergence to stationary solutions for semilinear parabolic equations with nonlinear boundary conditions. *Acta Math Univ Comenian*, 60(1):35–103, 1991.

[CFQ91b] M. Chipot, M. Fila, and P. Quittner. Stationary solutions, blow up and convergence to stationary solutions for semilinear parabolic equations with nonlinear boundary conditions. *Acta Mathematica Universitatis Comenianae*, 60(1):35–103, 1991.

[CGH91] L. Caniglia, A. Galligo, and J. Heintz. Equations for the projective closure and effective Nullstellensatz. *Discrete Appl. Math.*, 33:11–23, 1991.

[CGH$^+$03] D. Castro, M. Giusti, J. Heintz, G. Matera, and L.M. Pardo. The hardness of polynomial equation solving. *Found. Comput. Math.*, 3(4):347–420, 2003.

[CHMP01] D. Castro, K. Hägele, J.E. Morais, and L.M. Pardo. Kronecker's and Newton's approaches to solving: a first comparison. *J. Complexity*, 17(1):212–303, 2001.

[CJPS02] D. Castro, J.L. Montaña, L.M. Pardo, and J. San Martín. The distribution of condition numbers of rational data of bounded bit length. *Foundations of Computational Mathematics*, 2(1):1—52, 2002.

[CLO98] D. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*, volume 185 of *Grad. Texts in Math.* Springer, New York, 1998.

[CS99] F. Cucker and S. Smale. Complexity estimates depending on condition and round–off error. *J. ACM*, 46(1):113–184, 1999.

[Dan94] V. Danilov. Algebraic varieties and schemes. In I.R. Shafarevich, editor, *Algebraic Geometry I*, volume 23 of *Encyclopaedia of Mathematical Sciences*, pages 167–307. Springer, Berlin Heidelberg New York, 1994.

[Ded97] J.-P. Dedieu. Condition number analysis for sparse polynomial systems. In F. Cucker and M. Shub, editors, *Foundations of computational mathematics (Rio de Janeiro, 1997)*, pages 267–276, Berlin Heidelberg New York, 1997. Springer.

[DL08] C. Durvye and G. Lecerf. A concise proof of the Kronecker polynomial system solver from scratch. *Expo. Math.*, 26(2):101–139, 2008.

[DM09] Ezequiel Dratman and Guillermo Matera. On the solution of the polynomial systems arising in the discretization of certain odes. *Computing*, 85(4):301–337, July 2009.

[DMW09] E. Dratman, G. Matera, and A. Waissbein. Robust algorithms for generalized Pham systems. *Comput. Complexity*, 18(1):105–154, 2009.

[Dra10] Ezequiel Dratman. Approximation of the solution of certain nonlinear {ODEs} with linear complexity. *Journal of Computational and Applied Mathematics*, 233(9):2339 – 2350, 2010.

[Dra13a] Ezequiel Dratman. Efficient approximation of the solution of certain nonlinear reaction–diffusion equations with small absorption. *Journal of Complexity*, 29(3–4):263 – 282, 2013.

[Dra13b] Ezequiel Dratman. Efficient approximation of the solution of certain nonlinear reaction-diffusion equations with large absorption. *J. Comput. Appl. Math.*, 238:180–202, January 2013.

[Duv89] D. Duval. Rational Puiseux expansions. *Compos. Math.*, 70:119–154, 1989.

[Duv90] J. Duvallet. Computation of solutions of two–point boundary value problems by a simplicial homotopy algorithm. In K. Georg E. Allgower, editor, *Computational Solution of Nonlinear Systems of Equations*, volume 26 of *Lectures Appl. Math.*, pages 135–150, Providence, RI., 1990. Amer. Math. Soc.

[EH99] D. Eisenbud and J. Harris. *The Geometry of Schemes*, volume 197 of *Grad. Texts in Math.* Springer, New York, 1999.

[Eis95] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Grad. Texts in Math.* Springer, New York, 1995.

[Ewa96] G. Ewald. *Combinatorial convexity and algebraic geometry*, volume 168 of *Grad. Texts in Math.* Springer, New York, 1996.

[FGR02] R. Ferreira, P. Groisman, and J.D. Rossi. Numerical blow–up for a nonlinear problem with a nonlinear boundary condition. *Mathematical models and methods in applied sciences*, 12(4):461–484, 2002.

[Ful84] W. Fulton. *Intersection Theory.* Springer, Berlin Heidelberg New York, 1984.

[GH01] M. Giusti and J. Heintz. Kronecker's smart, little black–boxes. In A. Iserles R. Devore and E. Süli, editors, *Proceedings of Foundations of Computational Mathematics, FoCM'99, Oxford 1999*, volume 284 of *London Math. Soc. Lecture Note Ser.*, pages 69–104, Cambridge, 2001. Cambridge Univ. Press.

[GHH$^+$97] M. Giusti, K. Hägele, J. Heintz, J.E. Morais, J.L. Montaña, and L.M. Pardo. Lower bounds for Diophantine approximation. *J. Pure Appl. Algebra*, 117,118:277–317, 1997.

[GHM$^+$98] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, and L.M. Pardo. Straight–line programs in geometric elimination theory. *J. Pure Appl. Algebra*, 124:101–146, 1998.

[GHMP97] M. Giusti, J. Heintz, J.E. Morais, and L.M. Pardo. Le rôle des structures de données dans les problèmes d'élimination. *C. R. Math. Acad. Sci. Paris*, 325:1223–1228, 1997.

[Giu89] M. Giusti. Complexity of standard bases in projective dimension zero. In J.H. Davenport, editor, *Proceedings of the European Conference on Computer Algebra*, volume 378 of *Lecture Notes in Comput. Sci.*, pages 333–335, Berlin, 1989. Springer.

[Giu91] M. Giusti. Complexity of standard bases in projective dimension zero II. In S. Sakata, editor, *Proceedings of Applied Algebra, Algebraic Algorithms and Error–Correcting Codes, AAECC–8, Aug 20–24, 1990, Tokyo, Japan*, volume 508 of *Lecture Notes in Comput. Sci.*, pages 322–328, Berlin, 1991. Springer.

[GKZ94] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants.* Birkhäuser, Boston, 1994.

[GLGV98] M.-J. Gonzalez-Lopez and L. Gonzalez-Vega. Newton identities in the multivariate case: Pham Systems. In B. Buchberger et al., editor, *Gröbner Bases and Applications*, volume 251 of *London Math. Soc. Lecture Note Ser.*, pages 351–366. Cambridge Univ. Press, Cambridge, 1998.

[GLS01] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *J. Complexity*, 17(1):154–211, 2001.

[GP74] V. Guillemin and A. Pollack. *Differential Topology*. Prentice–Hall, Englewood Cliffs, NJ, 1974.

[GV98] L. Gonzalez-Vega. A special quantifier elimination algorithm for Pham systems. In C. Detzell et al., editor, *Real algebraic geometry and ordered structures, AMS special session, Baton Rouge, LA, USA, April 17-21*, volume 253 of *Contemp. Math.*, pages 115–366, Providence, RI, 1998. Amer. Math. Soc.

[Hei83] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoret. Comput. Sci.*, 24(3):239–277, 1983.

[Hen81] D. Henry. *Geometric theory of semilinear parabolic equations*, volume 840 of *Lecture Notes in Mathematics*. Springer, Berlin Heideilberg, 1981.

[HJS$^+$02] J. Heintz, G. Jerónimo, J. Sabia, J. San Martín, and P. Solernó. Intersection theory and deformation algorithms. the multihomogeneous case. Manuscript Universidad de Buenos Aires, 2002.

[HJS13] MaríA Isabel Herrero, Gabriela Jeronimo, and Juan Sabia. Affine solution sets of sparse polynomial systems. *J. Symb. Comput.*, 51:34–54, April 2013.

[HKP$^+$00] J. Heintz, T. Krick, S. Puddu, J. Sabia, and A. Waissbein. Deformation techniques for efficient polynomial equation solving. *J. Complexity*, 16(1):70–109, 2000.

[HKR11] J. Heintz, B. Kuijpers, and A. Rojas Paredes. Software engineering and complexity in effective algebraic geometry. Computer Research Repository abs/1110.3030, 2011.

[HKR12] J. Heintz, B. Kuijpers, and A. Rojas Paredes. On the intrinsic complexity of elimination problems in effective algebraic geometry. Computer Research Repository abs/1201.4344, 2012.

[HM93] J. Heintz and J. Morgenstern. On the intrinsic complexity of elimination theory. *J. Complexity*, 9:471–498, 1993.

[HM00] T. Sauer H.M. Möller. H-bases for polynomial interpolation and system solving. *Adv. Comput. Math.*, 12(4):335–362, 2000.

[HMPW98] J. Heintz, G. Matera, L.M. Pardo, and R. Wachenchauzer. The intrinsic complexity of parametric elimination methods. *Electron. J. SADIO*, 1(1):37–51, 1998.

[HMW01] J. Heintz, G. Matera, and A. Waissbein. On the time–space complexity of geometric elimination procedures. *Appl. Algebra Engrg. Comm. Comput.*, 11(4):239–296, 2001.

[HS95] B. Huber and B. Sturmfels. A polyhedral method for solving sparse polynomial systems. *Math. Comp.*, 64(112):1541–1555, 1995.

[HS97] B. Huber and B. Sturmfels. Bernstein's Theorem in affine space. *Discrete Comput. Geom.*, 17:137–141, 1997.

[JMSW09] G. Jeronimo, G. Matera, P. Solernó, and A. Waissbein. Deformation techniques for sparse systems. *Found. Comput. Math*, 9:1–50, 2009.

[Kho78] A.G. Khovanski. Newton polyhedra and the genus of complete intersections. *Funct. Anal. Appl.*, 12:38–46, 1978.

[KM96] K. Kühnle and E. Mayr. Exponential space computation of Gröbner bases. In *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation, ISSAC'96 (Zürich, 24–26 July 1996)*, volume 358 of *ACM Press*, pages 63–71, New York, 1996. ACM Press.

[KP96] T. Krick and L.M. Pardo. A computational method for Diophantine approximation. In L. González-Vega and T. Recio, editors, *Algorithms in Algebraic Geometry and Applications, Proceedings of MEGA'94*, volume 143 of *Progr. Math.*, pages 193–254, Boston, 1996. Birkhäuser Boston.

[Küh98] K. Kühnle. *Space optimal computation of normal forms of polynomials*. PhD thesis, Technischen Universität München, München, Germany, 1998.

[Kus76] A.G. Kushnirenko. Newton polytopes and the Bézout Theorem. *Funct. Anal. Appl.*, 10:233–235, 1976.

[Laz83] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Computer algebra (London, 1983)*, number 162 in Lecture Notes in Comput. Sci., pages 146–156, Berlin, 1983. Springer.

[Lec02] G. Lecerf. Quadratic Newton iteration for systems with multiplicity. *Found. Comput. Math.*, 2(3):247–293, 2002.

[Lec03] G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *J. Complexity*, 19(4):564–596, 2003.

[LL01] T.-Y. Li and X. Li. Finding mixed cells in the mixed volume computation. *Found. Comput. Math.*, 1(2):161–181, 2001.

[LV98] M. J. Gonzalez Lopez and L. Gonzalez Vega. Newton identities in the multivariate case: Pham systems. *London Mathematical Society Lecture Notes Series*, 251:351–366, 1998.

[LW96] T.Y. Li and X. Wang. The BKK root count in $\mathbb{C}^n$. *Math. Comp.*, 65(216), 1996.

[Mat80] H. Matsumura. *Commutative Algebra*. Benjamin, 1980.

[Mat86] H. Matsumura. *Commutative Ring Theory*. Cambridge Univ. Press, Cambridge, 1986.

[May89] E. Mayr. Membership in polynomial ideals over Q is Exponential Space Complete. In B. Monien et al., editor, *Proceedings of the 6th Annual Symposium on Theoretical Aspects of Computer Science (STACS'89), Paderborn (FRG) 1989*, number 349 in Lecture Notes in Comput. Sci., pages 400–406, Berlin, 1989. Springer.

[MD04] G. Matera M. De Leo, E. Dratman. On the numerical solution of certain nonlinear systems arising in semilinear parabolic PDEs. In *Anales JAIIO (Jornadas Argentinas de Informática e Investigación Operativa*, 2004.

[MD05] G. Matera M. De Leo, E. Dratman. Numeric vs. symbolic homotopy algorithms in polynomial system solving: A case study. *J. Complexity*, 21(4):502–531, 2005.

[Miz08] Tomohiki Mizutani. *Finding All Mixed Cells for Polyhedral Homotopies*. PhD thesis, Tokyo Institute of Technology, 2008.

[MM82] E. Mayr and A. Meyer. The complexity of the word problem for commutative semigroups. *Adv. Math.*, 46:305–329, 1982.

[MP97] B. Mourrain and V. Pan. Solving special polynomial systems by using structural matrices and algebraic residues. In F. Cucker and M. Shub, editors, *Proceedings Foundations of Computational Mathematics (FOCM'97)*, pages 287–304, Berlin Heidelberg New York, 1997. Springer.

[MP00] B. Mourrain and V. Pan. Multivariate polynomials, duality and structured matrices. *J. Complexity*, 16(1):110–180, 2000.

[MPT92] T. Mora, G. Pfister, and C. Traverso. An introduction to the tangent cone algorithm. In C. Hoffmann, editor, *Issues in robotics and non-linear geometry*, volume 6 of *Advances in Computing Research*, pages 199–270. JAI Press, Greenwich Conn., 1992.

[MR04] G. Malajovich and J.M. Rojas. High probability analysis of the condition number of sparse polynomial systems. *Theor. Comput. Sci.*, 315(2–3):525–555, 2004.

[MT00] B. Mourrain and P. Trebuchet. Solving projective complete intersection faster. In *Proceedings 2000 ACM-SIGSAM International Symposium on Symbolic and Algebraic Computation ISSAC'2000 (August 6 - 10, 2000, St. Andrews, United Kingdom)*, pages 234–241, New York, 2000. ACM Press.

[MTK07] Tomohiko Mizutani, Akiko Takeda, and Masakazu Kojima. Dynamic enumeration of all mixed cells. *Discrete & Computational Geometry*, 37(3):351–367, 2007.

[Oka97] M. Oka. *Non-degenerate complete intersection singularity*. Hermann, Paris, 1997.

[Pao92a] C. Pao. *Nonlinear parabolic and elliptic equations*. Plenum Press, New York, 1992.

[Pao92b] C.V. Pao. *Nonlinear parabolic and elliptic equations*. Plenum Press, 1992.

[Par95] L.M. Pardo. How lower and upper complexity bounds meet in elimination theory. In G. Cohen, M. Giusti, and T. Mora, editors, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAECC–11*, volume 948 of *Lecture Notes in Comput. Sci.*, pages 33–69, Berlin, 1995. Springer.

[Par00] L.M. Pardo. Universal elimination requires exponential running time. In A. Montes, editor, *Computer Algebra and Applications, Proceedings of EACA–2000, Barcelona, Spain, September 2000*, pages 25–51, 2000.

[PR11] Adrien Poteaux and Marc Rybowicz. Complexity bounds for the rational newton-puiseux algorithm over finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 22(3):187–217, 2011.

[PR12] Adrien Poteaux and Marc Rybowicz. Good reduction of puiseux series and applications. *J. Symb. Comput.*, 47(1):32–63, 2012.

[PS93] P. Pedersen and B. Sturmfels. Product formulas for resultants and Chow forms. *Math. Z.*, 214(3), 1993.

[PS03] P. Philippon and M. Sombra. Hauteur normalisée des variétés toriques projectives. eprint math.NT/0406476, 38pp., 2003.

[PS04] L.M. Pardo and J. San Martín. Deformation techniques to solve generalized Pham systems. *Theoret. Comput. Sci.*, 315(2–3):593–625, 2004.

[PS05] P. Philippon and M. Sombra. Géométrie diophantienne et variétés toriques. *C. R. Math. Acad. Sci. Paris*, 340:507–512, 2005.

[PS08] P. Philippon and M. Sombra. Hauteur normalisée des variétés toriques projectives. *J. Inst. Math. Jussieu*, 7(2):327–373, 2008.

[Roj99] J.M. Rojas. Solving degenerate sparse polynomial systems faster. *J. Symbolic Comput.*, 28(1/2):155–186, 1999.

[Roj00] J.M. Rojas. Algebraic geometry over four rings and the frontier of tractability. In J. Denef et al., editor, *Proceedings of a Conference on Hilbert's Tenth Problem and Related Subjects (University of Gent, November 1–5, 1999)*, volume 270 of *Contemp. Math.*, pages 275–321, Providence, RI, 2000. Amer. Math. Soc.

[Roj03] J.M. Rojas. Why polyhedra matter in non–linear equation solving. In *Proceedings conference on Algebraic Geometry and Geometric Modelling (Vilnius, Lithuania, July 29–August 2, 2002)*, volume 334 of *Contemp. Math.*, pages 293–320, Providence, RI, 2003. Amer. Math. Soc.

[Rou97] F. Rouillier. Solving zero–dimensional systems through rational univariate representation. *Appl. Algebra Engrg. Comm. Comput.*, 9(5):433–461, 1997.

[Sai83] R. Saigal. A homotopy for solving large, sparse and structured fixed–point problems. *Math. Oper. Res.*, 8:557–578, 1983.

[Sch03] E. Schost. Computing parametric geometric resolutions. *Appl. Algebra Engrg. Comm. Comput.*, 13:349–393, 2003.

[SGKM95] A.A. Samarskii, V.A. Galaktionov, S.P. Kurdyumov, and A.P. Mikhailov. *Blow–up in quasilinear parabolic equations*, volume 19 of *de Gruyter Expositions in Mathematics.* Walter de Gruyter, Berlin, 1995.

[Sha94] I.R. Shafarevich. *Basic Algebraic Geometry: Varieties in Projective Space.* Springer, Berlin Heidelberg New York, 1994.

[SS93a] M. Shub and S. Smale. Complexity of Bézout's theorem I: Geometric aspects. *J. Amer. Math. Soc.*, 6(2):459–501, 1993.

[SS93b] M. Shub and S. Smale. Complexity of Bézout's theorem II: Volumes and probabilities. In F. Eyssette and A. Galligo, editors, *Computational Algebraic Geometry*, volume 109 of *Progr. Math.*, pages 267–285, Boston, 1993. Birkhäuser Boston.

[SS93c] M. Shub and S. Smale. Complexity of Bézout's theorem III: Condition number and packing. *J. Complexity*, 9:4–14, 1993.

[SS94] M. Shub and S. Smale. Complexity of Bézout's theorem V: Polynomial time. *Theoret. Comput. Sci.*, 133:141–164, 1994.

[SS96a] J. Sabia and P. Solernó. Bounds for traces in complete intersections and degrees in the Nullstellensatz. *Appl. Algebra Engrg. Comm. Comput.*, 6(6):353–376, 1996.

[SS96b] M. Shub and S. Smale. Complexity of Bézout's theorem IV: Probability of success. *SIAM J. Numer. Anal.*, 33:141–164, 1996.

[Sto00] A. Storjohann. *Algorithms for matrix canonical forms.* PhD thesis, ETH, Zürich, Switzerland, 2000.

[VA85] A. Varchenko V. Arnold, S. Gusein-Zade. *Singularities of Differentiable Maps*, volume I. Birkhäuser, Boston, 1985.

[Ver09] Jan Verschelde. Polyhedral methods in numerical algebraic geometry. In D.J. Bates, G. Besana, and S. Di Rocco, editors, *Interactions of Classical and Numerical Algebraic Geometry*, volume 496 of *nteractions of Classical and Numerical Algebraic Contemporary Mathematics*, pages 243–263. AMS, 2009.

[VGC96] J. Verschelde, K. Gatermann, and R. Cools. Mixed volume computation by dynamic lifting applied to polynomial system solving. *Discrete Comput. Geom.*, 16(1):69–112, 1996.

[Vog84] W. Vogel. *Results on Bézout's theorem*, volume 74 of *Tata Inst. Fundam. Res. Lect. Math.* Tata Inst. Fund. Res., Bombay, 1984.

[VVC94] J. Verschelde, P. Verlinden, and R. Cools. Homotopies exploiting Newton polytopes for solving sparse polynomial systems. *SIAM J. Numer. Anal.*, 31(3):915–930, 1994.

[vzG86] J. von zur Gathen. Parallel arithmetic computations: a survey. In J. Gruska, B. Rovan, and J. Wiedermann, editors, *Proceedings of the 12th International Symposium on Mathematical Foundations of Computer Science, Bratislava, Czechoslovakia, August 25–29, 1996*, volume 233 of *Lecture Notes in Comput. Sci.*, pages 93–112, Berlin, August 1986. Springer.

[vzGG99] J. von zur Gathen and J. Gerhard. *Modern computer algebra.* Cambridge Univ. Press, Cambridge, 1999.

[Wal50] R.J. Walker. *Algebraic Curves.* Dover Publications Inc., New York, 1950.

[Wal99] P.G. Walsh. On the complexity of rational Puiseux expansions. *Pacific J. Math.*, 188(2):369–387, 1999.

[Wal00] P.G. Walsh. A polynomial–time complexity bound for the computation of the singular part of a Puiseux expansion of an algebraic function. *Math. Comp.*, 69(231):1167–1182, 2000.

[Zip93] R. Zippel. *Effective Polynomial Computation*, volume 241 of *Kluwer Internat. Ser. Engrg. Comput. Sci.* Kluwer Acad. Publ., Dordrecht, 1993.

Firma de la Tesis

Director de Tesis

____

Firma

____

Fecha

Tesista

____

Firma

____

Fecha