Validity proof of Lazard's method for CAD construction

Scott McCallum

Department of Computing, Macquarie University, NSW 2109, Australia

Adam Parusiński

Univ. Nice Sophia Antipolis, CNRS, LJAD, UMR 7351, 06108 Nice, France

Laurentiu Paunescu

School of Mathematics and Statistics, University of Sydney, NSW 2006, Australia

Abstract

In 1994 Lazard proposed an improved method for cylindrical algebraic decomposition (CAD). The method comprised a simplified projection operation together with a generalized cell lifting (that is, stack construction) technique. For the proof of the method's validity Lazard introduced a new notion of valuation of a multivariate polynomial at a point. However a gap in one of the key supporting results for his proof was subsequently noticed. In the present paper we provide a complete validity proof of Lazard's method. Our proof is based on the classical parametrized version of Puiseux's theorem and basic properties of Lazard's valuation. This result is significant because Lazard's method can be applied to any finite family of polynomials, without any assumption on the system of coordinates. It therefore has wider applicability and may be more efficient than other projection and lifting schemes for CAD.

1 Introduction

Cylindrical algebraic decomposition (CAD) of Euclidean n-space $\mathbb{R}^n$, relative to a given set of n-variate integral polynomials A, is an important tool in computational algebra and geometry. It was introduced by Collins [10] as the key component of a method for quantifier elimination (QE) for real closed fields. Applications of CAD and QE include robot motion planning [31], stability analysis of differential equations [18], simulation and optimization [33], epidemic modelling [8], and programming with complex functions [14]. A key

operation for CAD construction is *projection*: the projection of a set of n-variate integral polynomials is a set of $(n-1)$-variate integral polynomials. In view of its central role, much effort has been devoted to improving this operation [24,25,17,7]. Cell lifting, or stack construction, is also an important component of CAD.

In 1994 Lazard [20] proposed an improved method for CAD computation. The method comprised a simplified projection operation together with a generalized cell lifting process. However a gap in one of the key supporting results of [20] was subsequently noticed [11,7]. This was disappointing because Lazard's proposed approach has some advantages over other methods. In particular, it is relatively simple and it requires no assumption on the system of coordinates.

Inherent in [20] is a certain notion of valuation of a multivariate polynomial and, more generally, multivariate Laurent-Puiseux (that is fractional meromorphic) series, at a point. The related notion of the valuation-invariance of such series in a subset of $\mathbb{R}^n$ is also implicit in [20]. Lazard's proposed approach is in contrast with the classical approach based on the concept of the order (of vanishing) of a multivariate polynomial or analytic function at a point, and the related concept of order-invariance, see McCallum [24,25].

A partial validity proof of Lazard's projection only was recently published by McCallum and Hong, [27]. It was shown there that Lazard's projection is valid for CAD construction for so-called well-oriented polynomial sets. The key underlying results related to order-invariance rather than valuation-invariance, and the validity proof was built upon established results concerning improved projection. While this was an important step forward it was only a partial validation of Lazard's approach since the method was not proved to work for non well-oriented polynomials and it did not involve valuation-invariance.

The present paper provides a complete validity proof of Lazard's method using his notion of valuation. There is no restriction of the method to well-oriented sets. This result is significant because Lazard's method has wider applicability and may be more efficient than other projection and lifting schemes for CAD.

This paper is organised as follows. We first recall Lazard's method and main claim (Section 2). We then study the concept of Lazard's valuation (Section 3). In this paper we only consider Lazard's valuation for a multivariate polynomial. Section 4 contains the statement of a key mathematical result (the Puiseux with parameter theorem) underlying our validation of Lazard's method. In Section 5 we present our proof of Lazard's main claim using Lazard's notion of valuation. The main idea of the proof is to use monomial test curves that allow us to change the valuation invariance along an analytic submanifold to the order invariance. In the appendix at the end of the paper we present, for the reader convenience, a proof of the Puiseux with parameter

theorem.

2 Lazard's proposed method and claims

Background material on CAD, and in particular its projection operation, can be found in [2,10–12,17,24,25]. We present a precise definition of the projection operator P_L for CAD introduced by Lazard [20]. Put $R_0 = \mathbb{Z}$ and, for $n \geq 1$, put $R_n = R_{n-1}[x_n] = \mathbb{Z}[x_1, \ldots, x_n]$. Elements of the ring R_n will usually be considered to be polynomials in x_n over R_{n-1}. We shall call a subset A of R_n whose elements are irreducible polynomials of positive degree and pairwise relatively prime an *irreducible basis*. (This concept is analogous to that of *squarefree basis* which is used in the CAD literature, for example [24].)

Definition 2.1 (Lazard projection)**.** Let A be a finite irreducible basis in R_n, with $n \geq 2$. The *Lazard projection* $P_L(A)$ of A is the subset of R_{n-1} comprising the following polynomials:

(1) all leading coefficients of the elements of A,
(2) all trailing coefficients (i.e. coefficients independent of x_n) of the elements of A,
(3) all discriminants of the elements of A, and
(4) all resultants of pairs of distinct elements of A.

Remark 2.2. Let A be an irreducible basis. Lazard's projection $P_L(A)$ is contained in and is usually strictly smaller than the McCallum projection $P_M(A)$ [24,25]. Indeed $P_M(A)$ includes the "middle coefficients" (i.e. those coefficients other than the leading and trailing ones) of the elements of A, which $P_L(A)$ omits. In other respects these two projection operators are the same.

However $P_L(A)$ contains and is usually strictly larger than the Brown-McCallum projection $P_{BM}(A)$ [7]. Indeed $P_{BM}(A)$ omits the trailing coefficients of the elements of A, which $P_L(A)$ includes, but in other respects is the same as $P_L(A)$. This remark notwithstanding, the Lazard projection is still of interest because of certain limitations of the Brown-McCallum projection. The two chief drawbacks of the projection $P_{BM}(A)$ are as follows. First, the method of [7] could fail in case A is not well-oriented [25,7]. Second, the method requires that any 0-dimensional nullifying cells [25,7] in each dimension be identified and added during CAD construction. These drawbacks are elaborated in [7].

Lazard [20] outlined a claimed CAD algorithm for $A \subset R_n$ and $\mathbb{R}^n$ which uses the projection set $P_L(A)$. The specification of his algorithm requires the following concept of his valuation:

Definition 2.3 (Lazard valuation)**.** Let K be a field. Let $n \geq 1$, $f \in K[x_1, \ldots, x_n]$ nonzero, and $\alpha = (\alpha_1, \ldots, \alpha_n) \in K^n$. The *Lazard valuation* (*valuation*, for short) $v_\alpha(f)$ of f at α is the element $\mathbf{v} = (v_1, \ldots, v_n)$ of $\mathbb{N}^n$ least (with respect to $\leq_{lex}$) such that f expanded about α has a term

$$c(x_1 - \alpha_1)^{v_1} \cdots (x_n - \alpha_n)^{v_n}$$

with $c \neq 0$. (Note that $\leq_{lex}$ denotes the *lexicographic order* on $\mathbb{N}^n$ – see next section.)

Example 2.4. Let $n = 1$. Then $v_\alpha(f)$ is the familiar order $\mathrm{ord}_\alpha(f)$ of $f \in K[x_1]$ at $\alpha \in K$. Thus, for instance, if $f(x_1) = x_1^2 - x_1^3$ then $v_0(f) = 2$ and $v_1(f) = 1$. As another example, let $n = 2$ and $f(x_1, x_2) = x_1 x_2^2 + x_1^2 x_2 = x_1 x_2 (x_2 + x_1)$. Then $v_{(0,0)}(f) = (1, 2)$, $v_{(1,0)}(f) = (0, 1)$, and $v_{(0,1)}(f) = (1, 0)$.

The above defines $v_\alpha(f)$ for $f \in K[x_1, \ldots, x_n]$ nonzero and $\alpha \in K^n$. Lazard [20] actually defined $v_\alpha(f)$ for nonzero elements f of the much larger domain of all Laurent-Puiseux (that is, fractional meromorphic) series in $x_1 - \alpha_1, \ldots, x_n - \alpha_n$ over K. In this sense the above is a more limited definition of valuation. With K, n and f as in the above definition, and $S \subset K^n$, we say f is *valuation-invariant* in S if the valuation of f is the same at every point of S. Some basic properties of this Lazard valuation, and the associated notion of valuation-invariance, are presented in Section 3 below. Lazard's proposed CAD algorithm also uses a technique for "evaluating" a polynomial $f \in R_n$ at a sample point in $\mathbb{R}^{n-1}$. This technique is described in slightly more general terms as follows:

Definition 2.5 (Lazard evaluation)**.** Let K be a field which supports explicit arithmetic computation. Let $n \geq 2$, take a nonzero element f in $K[x_1, \ldots, x_n]$, and let $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in K^{n-1}$. The *Lazard evaluation* $f_\alpha(x_n) \in K[x_n]$ of f at α is defined to be the result of the following process (which determines also nonnegative integers v_i, with $1 \leq i \leq n-1$):

$f_\alpha \leftarrow f$
For $i \leftarrow 1$ to $n-1$ do
    $v_i \leftarrow$ the greatest integer v such that $(x_i - \alpha_i)^v \mid f_\alpha$
    $f_\alpha \leftarrow f_\alpha / (x_i - \alpha_i)^{v_i}$
    $f_\alpha \leftarrow f_\alpha(\alpha_i, x_{i+1}, \ldots, x_n)$

Example 2.6. We illustrate the above evaluation method using two simple examples. For both examples we take $K = \mathbb{Q}$, $n = 3$ and $\alpha = (0, 0)$. We denote (x_1, x_2, x_3) by (x, y, z). First let $f(x, y, z) = z^2 + y^2 + x^2 - 1$. After the first pass through the method ($i = 1$) we have $v_1 = 0$ and $f_\alpha(y, z) = z^2 + y^2 - 1$. After the second pass ($i = 2$) we have $v_2 = 0$ and $f_\alpha(z) = z^2 - 1$. In this case $f_\alpha(z) = f(0, 0, z)$. For our second example let $f(x, y, z) = yz - x$. After the first pass ($i = 1$) we have $v_1 = 0$ and $f_\alpha(y, z) = yz$. After the second pass

$(i = 2)$ we have $v_2 = 1$ and $f_\alpha(z) = yz/y = z$. In this case $f_\alpha(z) \neq f(0, 0, z)$, because the latter polynomial is zero.

Remark 2.7. Notice that the assertion "$f_\alpha \neq 0$" is an invariant of the above process. With K, n, f, α and the v_i as in the above definition of Lazard evaluation, notice that $f(\alpha, x_n) = 0$ (identically) if and only if $v_i > 0$, for some i in the range $1 \leq i \leq n-1$. With $\alpha_n \in K$ arbitrary, notice also that the integers v_i, with $1 \leq i \leq n-1$, are the first $n-1$ coordinates of $v_{(\alpha,\alpha_n)}(f)$. It will on occasion be handy to refer to the $(n-1)$-tuple $(v_1, \ldots, v_{n-1})$ as the *Lazard valuation of f on α*.

Remark 2.8. Let $f \in K[x_1, \ldots, x_n]$ be nonzero, $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in K^{n-1}$, and let $\mathbf{v} = (v_1, \ldots, v_{n-1})$ be the Lazard valuation of f on α. If we expand f at α

$$f(x_1, \ldots, x_n) = \sum_u f^{\mathbf{u}}(x_n) \prod_{i=1}^{n-1} (x_i - \alpha_i)^{u_i} \tag{1}$$

where $\mathbf{u} = (u_1, \ldots, u_{n-1}) \in \mathbb{N}^{n-1}$, with coefficients $f^{\mathbf{u}}(x_n) \in K[x_n]$, then $f_\alpha = f^{\mathbf{v}}$. This follows from the fact that $\mathbf{v}$ is the minimum of $\{\mathbf{u} : f^{\mathbf{u}} \neq 0\}$ for the lexicographic order.

One more definition is needed before we can state Lazard's main claim and his algorithm based on it. This definition is not explicit in [20] – it was introduced in [27] to help clarify and highlight Lazard's main claim:

Definition 2.9. [Lazard delineability] Let $f \in R_n$ be nonzero and S a subset of $\mathbb{R}^{n-1}$. We say that f is *Lazard delineable* on S if

(1) the Lazard valuation of f on α is the same for each point $\alpha \in S$;
(2) the set of real roots of $f_\alpha(x_n), \alpha \in S$ is either empty or it consists of finitely many continuous functions $\theta_1 < \cdots < \theta_k$ from S to $\mathbb{R}$, with $k \geq 1$; and, in the latter case
(3) there exist positive integers $m_1, \ldots, m_k$ such that, for all $\alpha \in S$ and all i, m_i is the multiplicity of $\theta_i(\alpha)$ as a root of $f_\alpha(x_n)$.

When f is Lazard delineable on S we refer to the graphs of the θ_i as the *Lazard sections* of f over S; and the regions between successive Lazard sections, together with the region below the lowest Lazard section and that above the highest Lazard section, are called *Lazard sectors*. Notice that f Lazard-delineable on S implies f valuation-invariant in every Lazard section and sector over S.

We express Lazard's main claim, essentially the content of his Proposition 5 and subsequent remarks, as follows (as in [27]):

> Let A be a finite irreducible basis in R_n, where $n \geq 2$. Let S be a connected subset of $\mathbb{R}^{n-1}$. Suppose that each element of $P_L(A)$ is valuation-invariant in S. Then each element of A is Lazard delineable on S, the Lazard sections over S of the elements of A are pairwise disjoint, and each element of A is valuation-invariant in every Lazard section and sector over S so determined.

Our wording of this claim is different from Lazard's – we have tried to highlight and clarify the essence of his assertions. This claim concerns valuation-invariant lifting in relation to $P_L(A)$: it asserts that the condition, "each element of $P_L(A)$ is valuation-invariant in S", is sufficient for an A-valuation-invariant stack in $\mathbb{R}^n$ to exist over S. We prove Lazard's main claim in Section 5. We can now describe Lazard's proposed CAD algorithm (as in [27]):

Algorithm 1 (Valuation-invariant CAD using Lazard projection)**.**

$(\mathcal{I}, \mathcal{S}) \leftarrow \text{VCADL}(A)$

Input: A is a list of integral polynomials in $x_1, \ldots, x_n$.
Output: $\mathcal{I}$ and $\mathcal{S}$ are lists of indices and sample points, respectively, of the cells comprising an A-valuation-invariant CAD of $\mathbb{R}^n$.

(1) If $n > 1$ then go to (2).
Isolate the real roots of the irreducible factors of the nonzero elements of A.
Construct cell indices $\mathcal{I}$ and sample points $\mathcal{S}$ from the real roots. Exit.
(2) $B \leftarrow$ the finest squarefree basis for $\text{prim}(A)$.
$P \leftarrow \text{cont}(A) \cup P_L(B)$.
$(\mathcal{I}', \mathcal{S}') \leftarrow \text{VCADL}(P)$.
$\mathcal{I} \leftarrow$ the empty list. $\mathcal{S} \leftarrow$ the empty list.
For each $\alpha = (\alpha_1, \ldots, \alpha_{n-1})$ in $\mathcal{S}'$ do
  Let i be the index of the cell containing α.
  $f^* \leftarrow \prod_{f \in B} f_\alpha$. (Each f_α is constructed using exact arithmetic in $\mathbb{Q}(\alpha)$.)
  Isolate the real roots of f^*.
  Construct cell indices and sample points for Lazard sections and sectors of elements of B from i, α and the real roots.
  Add the cell indices to $\mathcal{I}$ and the sample points to $\mathcal{S}$.
Exit.

The correctness of the above algorithm – namely, the claim that, given $A \subset R_n$, it produces a CAD of $\mathbb{R}^n$ such that each cell of the CAD is valuation-invariant with respect to each element of A – follows from Lazard's main claim by

induction on n.

3 Basic properties of Lazard's valuation

In this section we study Lazard's valuation [20] in the relatively special setting, namely that of multivariate polynomials over a ring, in which it was defined in the previous section. We shall clarify the notion and basic properties of this special valuation, and identify some relationships between valuation-invariance and order-invariance. The content of this section is based on very similar material found in [26].

We recall the standard algebraic definition of the term valuation [13,3,39]. A mapping $v : R - \{0\} \rightarrow \Gamma$, R a ring, into a totally ordered abelian monoid (written additively) Γ is said to be a *valuation* of R if the following two conditions are satisfied:

(1) $v(fg) = v(f) + v(g)$ for all f and g;
(2) $v(f + g) \geq \min\{v(f), v(g)\}$, for all f and g (with $f + g \neq 0$).

Perhaps the simplest and most familiar example of a valuation in algebraic geometry is the order of an n-variate polynomial over a field K at a point $\alpha \in K^n$. That is, the mapping $\mathrm{ord}_\alpha : K[x_1, \ldots, x_n] - \{0\} \rightarrow \mathbb{N}$ defined by

$$\mathrm{ord}_\alpha(f) = \text{the order of } f \text{ at } \alpha$$

is a valuation of the ring $K[x_1, \ldots, x_n]$. The order of f at α is also called "the multiplicity of f at α".

Let $n \geq 1$. Recall that the *lexicographic order* $\leq_{lex}$ on $\mathbb{N}^n$ is defined by $v = (v_1, \ldots, v_n) \leq_{lex} (w_1, \ldots, w_n) = w$ if and only if either $v = w$ or there is some i, $1 \leq i \leq n$, with $v_j = w_j$, for all j in the range $1 \leq j < i$, and $v_i < w_i$. Then $\leq_{lex}$ is an *admissible* order on $\mathbb{N}^n$ in the sense of [5]. Indeed $\mathbb{N}^n$, together with componentwise addition and $\leq_{lex}$, forms a totally ordered abelian monoid. The lexicographic order $\leq_{lex}$ can be defined similarly on $\mathbb{Z}^n$, forming a totally ordered abelian group.

Recall the definition of $v_\alpha(f)$ for $f \in K[x_1, \ldots, x_n]$ nonzero and $\alpha \in K^n$ from Section 2: $v_\alpha(f)$ is the element $(v_1, \ldots, v_n)$ of $\mathbb{N}^n$ least (with respect to $\leq_{lex}$) such that f expanded about a has a term $c(x_1 - \alpha_1)^{v_1} \cdots (x_n - \alpha_n)^{v_n}$ with $c \neq 0$. Notice that $v_\alpha(f) = (0, \ldots, 0)$ if and only if $f(\alpha) \neq 0$. Where there is no ambiguity we shall usually omit the qualifier "Lazard" from "Lazard valuation". We state some basic properties of the valuation $v_\alpha(f)$, analogues

of properties of the familiar order $\mathrm{ord}_\alpha(f)$. The first property is the fulfilment of the axioms.

Proposition 3.1. *Let f and g be nonzero elements of $K[x_1, \ldots, x_n]$ and let $\alpha \in K^n$. Then $v_\alpha(fg) = v_\alpha(f) + v_\alpha(g)$ and $v_\alpha(f+g) \geq_{lex} \min\{v_\alpha(f), v_\alpha(g)\}$ (if $f + g \neq 0$).*

Proof. These claims follow since $\mathbb{N}^n$, together with componentwise addition and $\leq_{lex}$, forms a totally ordered abelian monoid. □

Proposition 3.2. *(Upper semicontinuity of valuation) Let f be a nonzero element of $K[x_1, \ldots, x_n]$ and let $v = (v_1, \ldots, v_n) \in \mathbb{N}^n$. Then the set $\{\gamma \in K^n; v_\gamma(f) \geq_{lex} v\}$ is an algebraic subset of K^n. In particular, the Lazard valuation is upper semi-continuous (in Zariski topology for any field K and in the classical topology for $K = \mathbb{R}$ or $\mathbb{C}$).*

Proof. Denote $w = (w_1, \ldots, w_n)$, $\alpha = (\alpha_1, \ldots, \alpha_n)$. The coefficient $c_{w,\alpha}$ in the expansion of f at α

$$f = \sum_w c_{w,\alpha}(x_1 - \alpha_1)^{w_1} \cdots (x_n - \alpha_n)^{w_n},$$

for w fixed, is a polynomial in α. (If K is of characteristic zero then this coefficient equals $\dfrac{1}{w_1! \cdots w_n!} \dfrac{\partial^{w_1+\cdots+w_n} f}{\partial x_1^{w_1} \cdots \partial x_n^{w_n}}$.) The set $\{\alpha \in K^n; v_\alpha(f) \geq_{lex} v\}$ is the intersection of the zero set of polynomials $c_{w,\alpha}$ for $w = (w_1, \ldots, w_n) <_{lex} v$. Therefore it is algebraic. The algebraic sets are closed in Zariski topology by definition and clearly also, if $K = \mathbb{R}$ or $\mathbb{C}$, in the classical topology. □

Remark 3.3. Let $f : U \to K$, $K = \mathbb{R}$ or $\mathbb{C}$, be analytic, where U is an open connected subset of K^n, and suppose that f does not vanish identically. Then the Lazard valuation $v_\alpha(f)$ for $\alpha \in U$ can be defined exactly as in Definition 2.4 and it satisfies the upper semicontinutiy property for the classical topology. But the Lazard valuation extended to rational or meromorphic functions does not satisfy the upper semicontinutiy, see [26] for a discussion.

We shall say that f is *valuation-invariant* in a subset $S \subset K^n$ if $v_\alpha(f)$ is constant as α varies in S.

For the remaining properties we state we shall assume that $K = \mathbb{R}$ or $\mathbb{C}$.

Proposition 3.4. *Let f and g be two polynomials and suppose neither f nor g vanishes identically. Let $S \subset K^n$ be connected. Then fg is valuation-invariant in S if and only if both f and g are valuation-invariant in S.*

Proof. It follows easily from Proposition 3.2. See for instance the proof of Lemma A.3 of [24]. □

The next lemma is in a sense another analogue of the familiar order, and is particular to the case $n = 2$.

Lemma 3.5. *Let $f(x, y) \in K[x, y]$ be primitive of positive degree in y and squarefree. Then for all but a finite number of points $(\alpha, \beta) \in K^2$ on the curve $f(x, y) = 0$ we have $v_{(\alpha,\beta)}(f) = (0, 1)$.*

Proof. Denote by $R(x)$ the resultant $\mathrm{res}_y(f, f_y)$ of f and f_y with respect to y. Then $R(x) \neq 0$ since f is assumed squarefree. Let $(\alpha, \beta) \in K^2$, suppose $f(\alpha, \beta) = 0$ and assume that $v_{(\alpha,\beta)}(f) \neq (0, 1)$. Then $f_y(\alpha, \beta) = 0$. Hence $R(\alpha) = 0$. So α belongs to the set of roots of $R(x)$, a finite set. Now $f(\alpha, \beta) = 0$ and $f(\alpha, y) \neq 0$, since f is assumed primitive. So β belongs to the set of roots of $f(\alpha, y)$, a finite set. □

Let us further consider the relationship between the concepts of order-invariance and valuation-invariance for a subset S of K^n. The concepts are the same in case $n = 1$ because order and valuation are the same for this case. For $n = 2$ order-invariance in S does not imply valuation-invariance in S. (For consider $S = \{= x^2 + y^2 - 1\}$ in K^2. The order of $f(x, y) = x^2 + y^2 - 1$ at every point of S is 1. The valuation of f at every point $(\alpha, \beta) \in S$ except $(\pm 1, 0)$ is $(0, 1)$. But $v_{(\pm 1,0)}(f) = (0, 2)$.) However for $n = 2$ we can prove the following.

Proposition 3.6. *Let $f \in K[x, y]$ be nonzero and $S \subset K^2$ be connected. If f is valuation-invariant in S then f is order-invariant in S.*

Proof. Assume that f is valuation-invariant in S. Write f as a product of irreducible elements f_i of $K[x, y]$. By Proposition 3.3 each f_i is valuation-invariant in S. We shall show that each f_i is order-invariant in S. Take an arbitrary factor f_i. If the valuation of f_i in S is $(0, 0)$ then the order of f_i throughout S is 0, hence f_i is order-invariant in S. So we may assume that the valuation of f_i is nonzero in S, that is, that S is contained in the curve $f_i(x, y) = 0$. Suppose first that f_i has positive degree in y. Now the conclusion is immediate in case S is a singleton, so assume that S is not a singleton. Since S is connected, S is an infinite set. By Lemma 3.5 and valuation-invariance of f_i in S, we must have $v_{(\alpha,\beta)}(f_i) = (0, 1)$ for all $(\alpha, \beta) \in S$. Hence f_i is order-invariant in S (since $\mathrm{ord} f_i = 1$ in S). Suppose instead that $f_i = f_i(x)$ has degree 0 in y. Since $f_i(x)$ is irreducible it has no multiple roots. Therefore $v_{(\alpha,\beta)}(f_i) = (1, 0)$ for all $(\alpha, \beta) \in S$. Hence f_i is order-invariant in S (since $\mathrm{ord} f_i = 1$ in S). The proof that f_i is order-invariant in S is finished and we conclude that f is order-invariant in S. □

However the following example indicates that Proposition 3.6 is not true for dimension greater than 2; that is, valuation-invariance does not imply order-invariance when $n > 2$. Let $f(x, y, z) = z^2 - xy$ and let S be the x-axis in $\mathbb{R}^3$. Now f is valuation-invariant in S, since the valuation of f at each point of S is $(0, 0, 2)$. But f is not order-invariant in S, since $\text{ord}_{(0,0,0)} f = 2$ and $\text{ord}_{(\alpha,0,0)} f = 1$ for $\alpha \neq 0$.

4 The Puiseux with parameter theorem

We recall the classical Puiseux with parameter theorem in the form given in [30]. This theorem is a special case of the Abhyankar-Jung theorem, see [1], [29], and hence can be traced back to [19]. Puiseux with parameter is closely related to certain algebraic results of Zariski concerning equisingularity in codimension 1 over an arbitrary algebraically closed field of charactersitic 0 (Thm 7 of [36] and Thms 4.4 and 4.5 of [37]). In the Appendix at the end of this paper we provide a short proof of this theorem for the reader's convenience.

We use the following notation: with $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_k)$, $U_{\varepsilon,r} = U_\varepsilon \times U_r$, where $U_\varepsilon = \{x = (x_1, \ldots, x_k) \in \mathbb{C}^k : |x_i| < \varepsilon_i, \forall i\}$, $U_r = \{y \in \mathbb{C} : |y| < r\}$. In this section "analytic" means "complex analytic".

Theorem 4.1. (Puiseux with parameter)
Let

$$f(x, y, z) = z^d + \sum_{i=0}^{d-1} a_i(x, y) z^i, \tag{2}$$

be a monic polynomial in z with coefficients $a_i(x, y)$ analytic in $U_{\varepsilon,r}$. Suppose that the discriminant of f is of the form $D_f(x, y) = y^m u(x, y)$ with analytic function u non vanishing on $U_{\varepsilon,r}$. Then, there are a positive integer N (we may take $N = d!$) and analytic functions $\xi_i(x, t) : U_{\varepsilon,r^{1/N}} \to \mathbb{C}$ such that

$$f(x, t^N, z) = \prod_{i=1}^{d} (z - \xi_i(x, t))$$

for all $(x, t) \in U_{\varepsilon,r^{1/N}}$.

The roots $\xi_i(x, t)$ satisfy, moreover, the following properties. Firstly, for every $i \neq j$, $\xi_i - \xi_j$ equals a power of t times a function nonvanishing on $U_{\varepsilon,r^{1/N}}$. Secondly, if the coefficients $a_i(x, y)$ of f are (complexifications of) real analytic functions then the set of functions $\xi_i(x, t)$ is complex conjugation invariant.

By analogy with [27] we now consider the more general case in which

$$f(x,y,z) = a_d(x,y)z^d + \sum_{i=0}^{d-1} a_i(x,y)z^i, \tag{3}$$

with coefficients $a_i(x,y)$ analytic in $U_{\varepsilon,r}$, under the assumption that both $a_d(x,y)$ and $D_f(x,y)$ are equal to a power of y times a unit. We may then apply Theorem 4.1 to $\tilde{f}(x,y,\tilde{z})$ defined by

$$\tilde{f}(x,y,\tilde{z}) = \tilde{z}^d + \sum_{i=0}^{d-1} a_i a_d^{d-1-i}\tilde{z}^i \tag{4}$$

because $D_{\tilde{f}} = a_d^{d^2-3d+2}D_f$ satisfies the assumptions of Theorem 4.1. Let $\eta_i(x,y)$ be the roots of $\tilde{f}$. Then

$$\prod_{i=1}^{d}(a_d z - \eta_i) = \tilde{f}(x,y,a_d z) = a_d^{d-1} f(x,y,z). \tag{5}$$

The above relation is key for proving the following result, a complex analytic version of Corollary 3.15 of [27].

Corollary 4.2. *Let $f(x,y,z)$ be as in (3) and suppose that $a_d(x,y)$, $a_0(x,y)$ and $D_f(x,y)$ are of the form a power of y times a nowhere vanishing analytic function. Then there are an integer $N > 0$, analytic functions $u_i(x,t) : U_{\varepsilon,r^{1/N}} \to \mathbb{C}$, $1 \le i \le d$ and non-negative integers $m_0, m_1, \ldots, m_d$, such that*

$$t^{dm_0} f(x,t^N,z) = a_d(x,t^N)\prod_{i=1}^{d}(t^{m_0}z - t^{m_i}u_i(x,t))$$

on $U_{\varepsilon,r^{1/N}}$, where the order of each u_i in t is 0.

The functions $u_i(x,t)$ satisfy, moreover, the following properties. For every $i \neq j$, $t^{m_i}u_i - t^{m_j}u_j$ equals a power of t times a function non vanishing on $U_{\varepsilon,r}$. If the coefficients of $a_i(x,y)$ of f are (complexifications of) real analytic functions then the set of functions $u_i(x,t)$ is complex conjugation invariant.

Proof. By the assumption $a_d(x,t^N) = t^{m_0}\tilde{a}_d(x,t^N)$ and $a_0(x,t^N) = t^m\tilde{a}_0(x,t^N)$, with $\tilde{a}_d$, $\tilde{a}_0$ nowhere vanishing. Since

$$\prod_i \eta_i(x,t^N) = a_d^{d-1}(x,t^N)a_0(x,t^N),$$

the same is true for each η_i (the roots of $\tilde{f}$), $\eta_i(x,t)) = t^{m_i}\tilde{\eta}_i(x,t))$, with $\tilde{\eta}_i(x,t))$ nowhere vanishing. By (5) we get $\tilde{a}_d^d\prod_{i=1}^d(t^{m_0}z - \tilde{a}_d^{-1}\eta_i) = \tilde{a}_d^d\prod_{i=1}^d(t^{m_0}z - t^{m_i}\tilde{a}_d^{-1}\tilde{\eta}_i) = a_d^{d-1}f(x,y,z)$. Hence, setting $u_i := \tilde{a}_d^{-1}(x,t^N)\tilde{\eta}_i(x,t))$ we obtain the required formula for $t^{dm_0}f(x,t^N,z)$. If the coefficients a_i are real then the

set of roots η_i is conjugation invariant and hence so is the set of functions $u_i(x,t)$ □

As follows from the next lemma the assumptions of Theorem 4.1 and Corollary 4.2 can be expressed equivalently as the order invariance of $a_d(x,y)$, $a_0(x,y)$ and $D_f(x,y)$ in the hyperplane $y=0$.

Lemma 4.3. *Denote $(x_1,\ldots,x_k)$ by x and let $g(x,y)$ be analytic in a neighbourhood of the origin in K^{k+1}, $K=\mathbb{R}$ or $\mathbb{C}$, and suppose that g does not vanish identically. The following are equivalent:*

(1) The order of $g(a,y)$ at $y=0$ equals m for all a sufficiently small.
(2) For some function u analytic near the origin with $u(0,0)\neq 0$ we have $g(x,y)=y^m u(x,y)$ for all (x,y) sufficiently small.
(3) g is order-invariant in the hyperplane $y=0$ near the origin and this order is equal to m.

Proof. First we show that (1) implies (2). Suppose that $g(\alpha,y)$ is of order m at $y=0$ for α within box B about the origin. Expand g about the origin as the following iterated series:

$$g(x,y)=g_0(x)+g_1(x)y+g_2(x)y^2+\cdots .$$

Take $(a,0)\in B$. By assumption $g_i(a)=0$ for all $i<m$ and $g_m(a)\neq 0$. Setting

$$u(x,t)=g_m(x)+g_{m+1}(x)y+g_{m+2}(x)y^2+\cdots ,$$

we have $g(x,y)=y^m u(x,y)$, and $u(0,0)\neq 0$, as required.

Our proof above that (1) implies (2) could be easily adapted to show that (3) implies (2). That (2) implies (1) and (3) is straightforward. □

Remark 4.4. One can adapt easily the above proof to show that the conditions (1)-(3) also are equivalent to

(4) g is valuation-invariant in the hyperplane $y=0$ near the origin, and this valuation is equal to (0,m) (where 0 denotes n-1 zeros).

We do not use this result in this paper.

5 Proof of Lazard's main claim

We first need to sharpen slightly the definition of Lazard delineability given in Section 2: we say that an n-variate real polynomial f is *Lazard analytic*

delineable on a submanifold S of $\mathbb{R}^{n-1}$ if conditions (1), (2) and (3) of Definition 2.9 are satisfied, where the continuous functions $\theta_1 < \ldots < \theta_k$ from S to $\mathbb{R}$ are moreover *analytic*. The major effort of this section is to prove the following result; the Lazard claim is then an easy consequence.

Theorem 5.1. *Let $f(x, x_n) \in \mathbb{R}[x, x_n]$ have positive degree d in x_n, where $x = (x_1, \ldots, x_{n-1})$. Let $D(x)$, $l(x)$ and $t(x)$ denote the discriminant, leading coefficient and trailing coefficient (that is, the coefficient independent of x_n) of f, respectively, and suppose that each of these polynomials is nonzero. Let S be a connected analytic submanifold of $\mathbb{R}^{n-1}$ in which D, l and t are all valuation-invariant. Then f is Lazard analytic delineable on S and is valuation invariant in every section and sector of f over S.*

A special form of Lazard's main claim, in which S is assumed to be a connected submanifold of $\mathbb{R}^{n-1}$, and each element of A, an irreducible basis, is concluded to be Lazard analytic delineable on S etc., follows from the above theorem by Proposition 3.3. This special form of Lazard's main claim is sufficient to validate Lazard's CAD method, as outlined in Section 2.

We first need to investigate transforming the valuation of f at a point p into the order of f along a curve passing through p.

5.1 Transforming the valuation

For a couple of vectors $\mathbf{c}, \mathbf{v}$ we denote by $\langle \mathbf{c}, \mathbf{v} \rangle$ their scalar product $\langle \mathbf{c}, \mathbf{v} \rangle = \sum_i c_i v_i$. Let $V \subset \mathbb{N}^n$ be a non-empty family. (Typically, V will be the set of valuations of some n-variate polynomial g. It is not difficult to see that such $\{v_\alpha(g) | \alpha \in \mathbb{K}^n\}$ is finite, in fact every i-th component $(v_\alpha(g))_i$ of $v_\alpha(g)$ is bounded by the maximal exponent of $x_i^{\beta_i}$ that appears in g.) We say that an n-tuple of positive integers $\mathbf{c} = (c_1, \ldots, c_n) \in (\mathbb{N}^*)^n$ is an *evaluator for V* if for every $i = 1, ..., n-1$ we have

$$c_i \geq 1 + \max_{\mathbf{v} \in V} \sum_{j>i} c_j v_j. \tag{6}$$

Such a $\mathbf{c}$ always exists for any given finite $V \subset \mathbb{N}^n$. Indeed, we may choose c_n arbitrarily and then use (6) to define $c_{n-1}, c_{n-2}, \ldots$ recursively.

Remark 5.2. If $\mathbf{c} = (c_1, \ldots, c_n)$ is an evaluator for V then $(c_1, \ldots c_{n-1})$ is an evaluator for $\{(v_1, \ldots, v_{n-1}) | \exists_{v_n} (v_1, \ldots, v_n) \in V\}$.

Lemma 5.3. *Let $V \subset \mathbb{N}^n$ be a non-empty family and let $\mathbf{c} = (c_1, ..., c_n) \in (\mathbb{N}^*)^n$ be an evaluator for V.*

If $\mathbf{v} \in V$, $\mathbf{u} \in \mathbb{N}^n$, and $\mathbf{v} <_{lex} \mathbf{u}$ for the lexicographic order, then $\langle \mathbf{c}, \mathbf{v} \rangle <$

$\langle \mathbf{c}, \mathbf{u} \rangle$. *In particular, if* $\mathbf{v}, \mathbf{u} \in V$ *then* $\langle \mathbf{c}, \mathbf{v} \rangle = \langle \mathbf{c}, \mathbf{u} \rangle$ *if and only if* $\mathbf{v} = \mathbf{u}$.

Proof. Suppose that $\mathbf{v} <_{lex} \mathbf{u}$, that is there is i such that $u_k = v_k$ for $k < i$ and $v_i < u_i$. Then

$$\begin{aligned} \langle \mathbf{c}, \mathbf{u} \rangle - \langle \mathbf{c}, \mathbf{v} \rangle &= c_i(u_i - v_i) + \sum_{j>i} c_j(u_j - v_j) \\ &\geq (u_i - v_i) + \sum_{j>i} c_j(u_j + (u_i - v_i - 1)v_j) > 0 \end{aligned}$$

□

The following result allows us to transform the Lazard valuation $v_p(g)$ into the order of g along a monomial curve of the form $\mathbb{R} \ni s \to p + (s^{c_1}, \ldots, s^{c_n})$.

Corollary 5.4. *Let* $g \in \mathbb{R}[x_1, ..., x_n]$, $g \neq 0$, $p \in \mathbb{R}^n$. *Suppose that* $v_p(g) \in V$ *and that* $\mathbf{c} = (c_1, ..., c_n) \in (\mathbb{N}^*)^n$ *is an evaluator for* V. *Then* $g(p + (s^{c_1}, \ldots, s^{c_n}))$ *is not identically equal to zero and its order at* $s = 0$ *equals* $\langle \mathbf{c}, v_p(g) \rangle$.

Proof. Write $g(x) = \sum_{\mathbf{v} \in \mathbb{N}^n} a_{\mathbf{v}}(x - p)^{\mathbf{v}}$ and denote $\Lambda = \{\mathbf{v}; a_{\mathbf{v}} \neq 0\}$. Then

$$g(p + (s^{c_1}, \ldots, s^{c_n})) = \sum_{\mathbf{v} \in \Lambda} a_v s^{\langle \mathbf{c}, \mathbf{v} \rangle} = a_{v_p(g)} s^{\langle \mathbf{c}, v_p(g) \rangle} + \sum_{\mathbf{u} >_{lex} v_p(g)} a_u s^{\langle \mathbf{c}, \mathbf{u} \rangle}$$

and the corollary follows from Lemma 5.3. □

5.2 Proof of Theorem 5.1

The proof is based on Corollary 5.4 and the Puiseux with parameter theorem that we recalled in the previous section.

Recall that, in the statement of the theorem to be proved, x denotes the $(n-1)$-tuple $(x_1, \ldots, x_{n-1})$. Write

$$f(x, x_n) = a_d(x)x_n^d + a_{d-1}(x)x_n^{d-1} + \cdots + a_0(x). \tag{7}$$

(Then $a_d(x) = l(x)$ and $a_0(x) = t(x)$.) We fix positive integers $c_1, ..., c_{n-1}$ that satisfy the following properties. Firstly we require that $\mathbf{c} = (c_1, ..., c_{n-1})$ should be an evaluator for $V_g = \{v_p(g) : p \in S\}$, where

$$g(x) := D(x)a_d(x)a_0(x).$$

Secondly, we want $(c_1, ..., c_{n-1}, c_n)$, with $c_n = 1$, to be an evaluator for $V_f = \{v_{(p,z)}(f) : (p, z) \in S \times \mathbb{R}\}$. Since V_g and V_f are finite such $c_1, ..., c_{n-1}$ exist.

Later in the course of the proof we may change $c_1, ..., c_{n-1}$ by multiplying them by a positive integer. Then clearly the new vector $(c_1, ..., c_{n-1})$ still is an evaluator for V_g, and the new $(c_1, ..., c_{n-1}, 1)$ for V_f. We shall use test monomial curves, as in Corollary 5.4, twice in the proof. First we translate the assumed Lazard invariance of D, a_d, and a_0 for $p \in S$ near a fixed point p_0 of S into order invariance of these polynomials along suitable monomial curve passing through p. Secondly, at the end of the proof, we use the order of f along such a monomial curve passing through $(p, z_0) \in S \times \mathbb{R}$ to obtain the Lazard valuation of f at (p, z_0).

Consider $\psi : S \times \mathbb{R} \to \mathbb{R}^{n-1}$ defined by

$$\psi(p, s) = p + (s^{c_1}, \ldots, s^{c_{n-1}}) \tag{8}$$

and $g_\psi(p, s) := g(\psi(p, s))$. By Corollary 5.4, for p fixed, $g_\psi(p, s)$, as a function of $s \in \mathbb{R}$, has order $m := \langle \mathbf{c}, \mathbf{v}_p g \rangle$ at $s = 0$, and by the assumption of Theorem 5.1 this order is independent of $p \in S$. Therefore, by Lemma 4.3 (applied with respect to suitable local coordinates on S near p_0), $g_\psi(p, s)$ as an analytic function is divisible by s^m with the quotient non-vanishing on $S \times \{0\}$ near $(p, 0)$. Consequently the same holds for its factors: each of $D \circ \psi$, $a_d \circ \psi$, $a_0 \circ \psi$ is equal to a power of s times an analytic function not vanishing on $S \times \{0\}$ near $(p_0, 0)$. Let

$$f_\psi(p, s, z) = f(\psi(p, s), z) = a_d(\psi(p, s))z^d + a_{d-1}(\psi(p, s))z^{d-1} + \cdots + a_0(\psi(p, s)).$$

Since $a_d(\psi(p, s))$ is not vanishing identically, the degree in z of f_ψ equals d and the discriminant $D_\psi(p, s)$ of f_ψ equals $D(\psi(p, s))$. Therefore we may apply to f_ψ, localised at $(p_0, 0) \in S \times \{0\}$, the Puiseux with parameter theorem in the form given by Corollary 4.2. Then we use the conclusion of Corollary 4.2 to show the Lazard delineability of f over a neighbourhood of p_0 in S. Now we present in detail this argument.

First, by replacing s by its appropriate power s^N, that amounts to multiplying $c_1, ..., c_{n-1}$ by N, by Corollary 4.2, we may write

$$f_\psi(p, s, z) = a_d(\psi(p, s)) \prod_i (z - s^{n_i} u_i(p, s)), \tag{9}$$

with $n_i \in \mathbb{Z}$ (maybe negative) and u_i nonvanishing.

To compute the Lazard valuation of f at $(p, z_0) \in S \times \mathbb{R}$ we use the test monomial curves and evaluate the order at $s = 0$ of $f_\psi(p, s^2, z_0 + s)$ that we denote by $\mathrm{ord}_0 f_\psi(p, s^2, z_0 + s)$. (Thus we again multiply $c_1, ..., c_{n-1}$ by a factor, equal to 2 this time, and leave $c_n = 1$ unchanged.) We write

$$f_\psi(p, s^2, z_0 + s) = a_d(\psi(p, s^2)) \prod_i (z_0 + s - s^{2n_i} u_i(p, s^2)) \tag{10}$$

and compute the order at $s = 0$ of each factor separately. If $n_i < 0$, then $\mathrm{ord}_0(z_0 + s - s^{2n_i}u_i(p, s^2)) = 2n_i$. If $n_i > 0$, then $2n_i \geq 2$ and hence $\mathrm{ord}_0(z_0 + s - s^{2n_i}u_i(p, s^2)) = 0$ for $z_0 \neq 0$. Otherwise, that is for $z_0 = 0$, this order is equal to 1. Suppose now that $n_i = 0$. Then $\mathrm{ord}_0(z_0 + s - s^{2n_i}u_i(p, s^2)) = 0$ for $z_0 \neq u_i(p, 0)$. For $z_0 = u_i(p, 0)$, this order is equal to 1.

Let us divide the set of indices $\{1, ..., d\} = I_- \cup I_0 \cup I_+$ by the sign of n_i and consider an auxiliary function

$$h(p, z) := z^c \prod_{i \in I_0} (z - u_i(p, 0)), \tag{11}$$

where $c = |I_+|$ is the number of u_i with $n_i > 0$. By the previous computation

$$\mathrm{ord}_0 f_\psi(p, s^2, z_0 + s) = \mathrm{ord}_0 a_d(p, s^2) + \sum_{i; n_i < 0} 2n_i + m_{z_0} h(p, z), \tag{12}$$

where $m_{z_0}h(p, z)$ is the multiplicity of z_0 as a root of $h(p, z)$ and therefore

$$\min_{z_0 \in \mathbb{R}} \mathrm{ord}_0 f_\psi(p, s^2, z_0 + s) = \mathrm{ord}_0 a_d(p, s^2) + \sum_{i; n_i < 0} 2n_i$$

is independent of p. Hence, by Corollary 5.4, the valuation of f on p does not depend on $p \in S$. Denote the value of this valuation $\mathbf{v} = (v_1, ..., v_{n-1})$. Then, by (12) and Corollary 5.4, $v_{(p,z_0)}(f) = (v_1, ..., v_{n-1}, m_{z_0}h(p, z))$ and $m_{z_0}h(p, z)$ is the multiplicity of z_0 as a root of Lazard evaluation $f_p(z)$.

Finally, by the last part of Corollary 4.2, any two $u_i(p, 0)$, $u_j(p, 0)$, $i, j \in I_0$, either coincide or differ at every p. Hence each $u_i(p, 0)$ is either real for all p, if $u_i(p, 0) \equiv \overline{u}_i(p, 0)$, or not real, if $u_i(p, 0) \neq \overline{u}_i(p, 0)$ for all p. Thus we may take as $\theta_j(p)$ of (2) of Definition 2.9, these $u_i(p, 0)$ that are real, and complete them by $\theta(p) \equiv 0$ if c of (11) is strictly positive.

This shows Lazard analytic delineability of f over a neighbourhood of p_0 in S. The delineability of f over S then follows from the connectedness of S. □

The following result explains the role in the above proof of the auxilary polynomial $h(p, z)$ of (11) and moreover provides an alternative argument for an important part of the proof.

Proposition 5.5. *The polynomial $h(p, z)$ defined in* (11) *equals, up to multiplication by a nonzero constant, the Lazard evaluation $f_p(z)$,*

Proof. We use formula (1) of Remark 2.8. Let $\mathbf{v} = (v_1, \ldots, v_{n-1})$ be the valuation of f on $p \in \mathbb{R}^{n-1}$. Then, by Remark 5.2,

$$f(p + (s^{c_1}, \ldots, s^{c_{n-1}}), z) = s^{\langle \mathbf{c}, \mathbf{v} \rangle}(f^{\mathbf{v}}(z) + sR(s, z), \tag{13}$$

with $R \in \mathbb{R}[s,z]$. Write (9) in the exact form given by Corollary 4.2 (we consider p fixed)

$$s^{dm_0} f(p + (s^{c_1}, \dots, s^{c_{n-1}}), z) = s^{m_0} \tilde{a}_d(s) \prod_{i=1}^{d} (s^{m_0} z - s^{m_i} u_i(s)), \qquad (14)$$

where $\tilde{a}_d(0) \neq 0$ and $u_i(0) \neq 0$ for all i. Let us divide the set of indices $\{1, ..., d\} = I_- \cup I_0 \cup I_+$ by the sign of $m_i - m_0$. Let c denote the cardinality of I_+ and put $m = m_0 + \sum_{i \in I_-} m_i + \sum_{i \in I_0 \cup I_+} m_0$. Then

$$\begin{aligned} f(p+(s^{c_1}, \dots, s^{c_{n-1}}), z) = \\ = s^{m-dm_0} \tilde{a}_d(s) \prod_{i \in I_-} (s^{m_0 - m_i} z - u_i(s)) \prod_{i \in I_0} (z - u_i(s)) \prod_{i \in I_+} (z - s^{m_i - m_0} u_i(s)) = \\ = s^{m-dm_0} \Big(Ch(p,z) + sR(s,z) \Big). \end{aligned}$$

for a nonzero costant C. We conclude by comparing the above formula to (13). □

Example 5.6. We illustrate the construction in the proof using two examples. Take $n = 4$, $f(x,y,z,w) = yw^2 + xw - yz^2$ and let $S \subset \mathbb{R}^3$ be the z-axis without the origin. The discriminant $D(x,y,z) = x^2 + 4y^2z^2$ vanishes identically on S. The valuations of D, the leading coefficient $a_2 = y$, and the trailing coefficient $a_0 = -yz^2$, at $(0,0,z)$, $z \neq 0$, are equal to $(0,2,0)$, $(0,1,0)$, and $(0,1,0)$ respectively. (At the origin they are $(0,2,2)$, $(0,1,0)$, and $(0,1,2)$ so we had to remove the origin from the z-axis)

In order to detect the decomposition of $S \times \mathbb{R}$ into the valuation (of f) invariant subsets we may take $c_1 = 18, c_2 = 9, c_3 = 3, c_4 = 1$, so that the condition (6) is satisfied for V_f as well as for every V_g, where g equals D, a_2, and a_0. The function f_ψ is given by

$$f_\psi(p,s,w) = s^9 w^2 + s^{18} w - s^9 (z + s^3)^2 = s^9 (w^2 + s^9 w - (z + s^3)^2),$$

where $p = (0,0,z)$. This case is particularly simple since by dividing by s^9 and then setting $s = 0$ we obtain a polynomial of the same degree as f. This polynomial $w^2 - z^2$ equals the Lazard evaluation polynomial $f_p(w)$, $p = (0,0,z)$, and its zeros give the decomposition of $S \times \mathbb{R}$ into the valuation invariant subsets: $v_{(p,w)}(f) = (0,1,0,1)$ if $w^2 = z^2 \neq 0$ and $v_{(p,w)}(f) = (0,1,0,0)$ if $w^2 \neq z^2$, $z \neq 0$. (If $w = z = 0$ then $v_{(p,w)}(f) = (0,1,0,2)$.)

A similar but more complicated example is $f(x,y,z,w) = xw^2 + yzw - x$ with the same S and similar discriminant $D(x,y,z) = y^2z^2 + 4x^2$. Then the Lazard evaluation polynomial $f_p(w) = zw$ for $p = (0,0,z)$, $z \neq 0$, (here z is treated as a constant), is of degree stricltly smaller than the degree of f. The function f_ψ is given by

$$f_\psi(p,s,w) = s^{18} w^2 + s^9 w(z + s^3) - s^{18} = s^9 (s^9 w^2 + w(z + s^3) - s^9).$$

The polynomial in parantheses has two roots for $s \neq 0$. One of them tends to 0 as s tends to 0 and the other one tends to infinity. In the formula (9) this latter root of has a strictly negative exponent n_i. The exponent associated to the first root is strictly positive.

5.3 Proof of the Lazard's original claim

Corollary 5.7. *Suppose $f(x, x_n) \in \mathbb{R}[x, x_n]$ satisfies the assumption of Theorem 5.1. Let S be a connected subset of $\mathbb{R}^{n-1}$ in which D, l and t are all valuation-invariant. Then f is Lazard delineable on S and is valuation invariant in every section and sector of f over S.*

Proof. This corollary follows from Theorem 5.1 by standard arguments of semialgebraic geometry: stratifications and the curve selection lemma.

First we note that there is a finite semialgebraic stratification $\sqcup_i T_i = \mathbb{R}^{n-1}$ such that D, l and t are all valuation-invariant on each stratum. Here, by definition of stratification, each T_i is a connected locally closed semialgebraic subset and an analytic submanifold of $\mathbb{R}^{n-1}$ and any two strata satisfy the frontier condition: if $T_i \cap \overline{T}_j \neq \emptyset$ then $T_i \subset \overline{T}_j$. The existence of such a stratification follows from general theory of semialgebraic sets, see e.g. Proposition 9.1.8 of [6] or Proposition 2.5.1 of [4]. Actually such a stratification is provided automatically by the valuation-invariant CAD using Lazard projection, whose validity follows from Theorem 5.1.

Now for $S \subset \mathbb{R}^{n-1}$ as in the assumption of corollary we consider $S_1 = \sqcup_{i \in \Lambda} T_i$, the union of all strata intersecting S. Clearly S_1 is connected, D, l and t are all valuation-invariant in S_1, and Lazard delineabily over S_1 implies Lazard delineability over S. Thus we may replace S by S_1.

In order to show Lazard delineability over a connected union of strata it suffices to show it over S of the form $S = T_i \cup T_j$ with $T_i \subset \overline{T}_j$. Thus suppose that $S = T_i \cup T_j$ and that D, l and t are valuation-invariant on S. We show that f is delineable over S. For this it is enough to show that the Lazard valuation on α is independent of $\alpha \in S$, that the number of sections of f_α over T_i and T_j coincide, that these sections are given by functions continuous on whole S, and finally that their multiplicities as roots of f_α are the same on T_i and T_j. By standard arguments based on the curve selection lemma, see e.g. Proposition 8.1.13 of [6], it suffices to show all these claims over $p([0, \varepsilon))$, where $p(y) : (-\varepsilon, \varepsilon) \to S$ is an arbitrary real analytic curve such that $p(0) \in T_i$ and $p(y) \in T_j$ for $y > 0$. By replacing y by y^2 we may assume that $p(y) \in T_j$ for $y \neq 0$. Then we follow the main steps of the proof of Theorem 5.1. Let

$\psi : (-\varepsilon, \varepsilon) \times \mathbb{R} \to \mathbb{R}^{n-1}$ be defined by

$$\psi(y, s) = p(y) + (s^{c_1}, \ldots, s^{c_{n-1}}),$$

where $(c_1, ..., c_{n-1})$ is an evaluator for $V_g = \{v_p(g) : p \in S\}$, with $g(x) := D(x)l(x)t(x)$, and $(c_1, ..., c_{n-1}, 1)$ is an evaluator for $V_f = \{v_{(p,z)}(f) : (p, z) \in S \times \mathbb{R}\}$. Since D, l and t are valuation-invariant on the image of $p(y)$, $f_\psi(y, s, z) = f(\psi(y, s), z)$ satisfies the assumptions of Puiseux with parameter theorem, Corollary 4.2. Then the proof of Theorem 5.1 shows that f is Lazard delineable over the image of $p(y)$, and hence, by the curve selection lemma, over S. □

6 Conclusion

We first summarise the work reported herein. We presented the results of our investigation of Lazard's proposed CAD method, including both his proposed projection and valuation. In [27] we already found that Lazard's projection is valid for CAD construction for well-oriented polynomial sets. In the present paper (Section 5) Lazard's main claim is proved using his valuation. A consequence of this result is that Lazard's CAD method is valid, with no well-orientedness restriction.

Further work could usefully be done in a number of directions. It will be interesting to compare experimentally the Brown-McCallum projection [7] with the Lazard projection. It would be worthwhile to try to extend the theory of equational constraints using the Lazard projection. Examination of the other ideas suggested in [20] could also be fruitful.

Another inportant direction will be to understand the topological and geometric structure of the output of the CAD algorithm. This concerns all the methods, not only the Lazard one presented in this paper, see [21]. To study it will be interesting to use the new ideas proposed in a recent paper on Zariski equisingularity and stratifications [28].

7 Appendix. Proof of Puiseux with parameter theorem

In this section, for the reader's convenience, we present a concise proof of Theorem 4.1. This proof is based on the classical theory of complex analytic functions and uses a parametrized version of the Riemann removable singularity theorem. The proof we present below is due to Łojasiewicz and Pawłucki,

see [30]. For a similar approach, with slightly different details, see [29] Proposition 2.1.

Let us first recall the basic notation: $U_{\varepsilon,r} = U_\varepsilon \times U_r$, where $U_\varepsilon = \{x = (x_1, \ldots, x_k) \in \mathbb{C}^k : |x_i| < \varepsilon_i, \forall i\}$, $U_r = \{y \in \mathbb{C} : |y| < r\}$. We also denote the punctured disc $U_r \setminus \{0\}$ by U_r^*.

Proof of Theorem 4.1. Consider the polynomial in z,

$$P(x, w, z) := f(x, e^{2\pi i w}, z),$$

whose coefficients $a_i(x, e^{2\pi i w})$ are analytic on $U_\varepsilon \times H$, where $H = \{w : 2\pi \mathrm{Im}(w) > -\ln r\}$. By assumption the discriminant $D_P(x, w) = D_f(x, e^{2\pi i w})$ does not vanish on $U_\varepsilon \times H$ and hence P admits global complex analytic roots

$$\tilde{\xi}_1(x, w), \cdots, \tilde{\xi}_d(x, w).$$

(If the $D_P(x, w)$ is nonzero then the equation $P = \partial P/\partial z = 0$ has no solution. Therefore the local solutions $\tilde{\xi}(x, w)$ of $P = 0$ are analytic by the implicit function theorem. They are well-defined global analytic functions because $U_\varepsilon \times H$ is contractible.)

The coefficients of P are periodic: $P(x, w + 1, z) = P(x, w, z)$. Hence for each root $\tilde{\xi}_i(x, w)$ there is another root $\tilde{\xi}_{\varphi(i)}(x, w)$ such that $\tilde{\xi}_i(x, w+1) = \tilde{\xi}_{\varphi(i)}(x, w)$. The map $\varphi : \{1, \ldots, d\} \to \{1, \ldots, d\}$ is a permutation and hence $\varphi^{d!} = id$. Therefore, for $N = d!$,

$$\tilde{\xi}_i(x, w + N) = \tilde{\xi}_i(x, w). \tag{15}$$

Thus there are analytic functions $\xi_i(x, t) : U_\varepsilon \times U^*_{r^{1/N}} \to \mathbb{C}$ such that $\tilde{\xi}_i(x, w) = \xi_i(x, e^{2\pi i w/N})$. Since $\xi_i(x, t)$ are roots of $f(x, t^N, z)$ they are bounded on $U_{\varepsilon_0} \times U^*_{r_0^{1/N}}$, for every $\varepsilon_0 < \varepsilon$, $r_0 < r$. Hence they extend to functions analytic on $U_\varepsilon \times U_{r^{1/N}}$ by Riemann's theorem on removable singularities, cf. [15] Theorem 3, p. 19. □

Acknowledgements

We acknowledge grants which supported visits to the University of Sydney by the second named author in 2015 and 2016 : Sydney University BSG, IRMA Project ID: 176623 and ANR project STAAVF (ANR-2011 BS01 009). We are grateful to Hoon Hong for kindly granting us permission to include some basic material from the technical report [26] in Section 3.

References

[1] Abhyankar, S. S. On the ramification of algebraic functions. *Amer. J. Math. 77*, (1955), 575–592.

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

[3] Atiyah, M. F., MacDonald, I. G. *Introduction to Commutative Algebra.* Addison-Wesley, Reading, 1969.

[4] Benedetti, R., Risler, J.-J. *Algebraic and Semi-Algebraic Sets.* Hermann, Paris, 1990.

[5] Becker, T., Weispfenning, V., and Kredel, H. *Groebner Bases: A Computational Approach to Commutative Algebra.* Corrected Second Printing. Springer, New York, 1998.

[6] Bochnak, J., Coste, M., Roy, M.-F., *Real Algebraic Geometry.* Springer-Verlag, Berlin Heidelberg, 1998.

[7] Brown, C. W. Improved projection for cylindrical algebraic decomposition. *Journal of Symbolic Computation 32*, (2001), 447–465.

[8] Brown, C., Kahoui, M., Novotni, D., Weber, A. Algorithmic methods for investigating equilibria in epidemic modelling. *J. Symbolic Computation 41*, (2006), 1157–1173.

[9] Caviness, B., and Johnson, J. R., Eds. *Quantifier Elimination and Cylindrical Algebraic Decomposition.* Texts and Monographs in Symbolic Computation. Springer-Verlag, 1998.

[10] Collins, G. E. Quantifier elimination for the elementary theory of real closed fields by cylindrical algebraic decomposition. In: *Lecture Notes In Computer Science*, Vol. 33, (1975), Springer-Verlag, Berlin, pp. 134–183. Reprinted in [9].

[11] Collins, G. E. Quantifier elimination by cylindrical algebraic decomposition - twenty years of progress. In: [9].

[12] Collins, G. E., and Hong, H. Partial cylindrical algebraic decomposition for quantifier elimination. *Journal of Symbolic Computation 12*, (1991), 299–328.

[13] Danilov, V. I. Valuation. Springer-Verlag Online Encyclopaedia of Math., 2010.

[14] Davenport, J.H., Bradford, R., England, M., Wilson, D. Program verification in the presence of complex numbers etc. In: *SYNASC'12* (2012), IEEE, pp. 83–88.

[15] Gunning, H.C., Rossi, C. Analytic Functions of Several Complex Variables. AMS Chelsea Publishing, Providence, Rhode Island, 2009.

[16] Hensel, K. Ueber eine neue Theorie der algebraischen Funktionen zweier Variablen. *Acta Math. 23*, (1900), 339–416.

[17] Hong, H. An improvement of the projection operator in cylindrical algebraic decomposition. In: *Proceedings of ISSAC'90*, Watanabe, S. and Nagata, M. (Eds.), (1990), ACM Press, New York, pp. 261–264. Reprinted in [9].

[18] Hong, H., Liska, R., Steinberg, S. Testing stability by quantifier elimination. *J. Symbolic Computation 24*, (1997), 161–187.

[19] Jung, H. W. E. Darstellung der Funktionen eines algebraischen Koerpers zweier unabhaengigen Veraenderlichen x,y in der Umgebung einer Stelle x=a, y=b. *J. reine u. angewadte Math. 133*, (1908), 289–314.

[20] Lazard, D. An improved projection for cylindrical algebraic decomposition. In *Algebraic Geometry and its Applications*, Bajaj, C.L. (ed.), Springer, New York, 1994.

[21] Lazard, D. CAD and Topology of Semi-Algebraic Sets *Math.Comput.Sci.*, (2010) 4:93–112.

[22] Lipman, J., Teissier, B., Eds. *Oscar Zariski: Collected Papers, Volume 4: Equisingularity on Algebraic Varieties.* MIT Press, Cambridge, 1979.

[23] McCallum, S. An improved projection operation for cylindrical algebraic decomposition. PhD thesis, University of Wisconsin-Madison, 1984.

[24] McCallum, S. An improved projection operation for cylindrical algebraic decomposition of three-dimensional space. *Journal of Symbolic Computation 5*, (1988), 141–161.

[25] McCallum, S. An improved projection operation for cylindrical algebraic decomposition. In [9].

[26] McCallum, S., and Hong, H. On Lazard's valuation and CAD construction. arXiv:1501.06563 [math.AG].

[27] McCallum, S., and Hong, H. On using Lazard's projection in CAD construction. *Journal of Symbolic Computation 72*, (2016), 65–81.

[28] Parusiński, A., and Paunescu, L. Arcwise Analytic Stratification, Whitney Fibering Conjecture and Zariski Equisingularity. arXiv:1503.00130 [math.AG].

[29] Parusiński, A., and Rond, G. The Abhyankar-Jung theorem. *J. Algebra 365*, (2012), 29–41.

[30] Pawłucki, W. Le théorème de Puiseux pour une application sous-analytique. *Bull. Polish Acad. Sci. Matha 32.*, (1984), 555–560.

[31] Schwartz, J., Sharir, M. On the "piano-movers" problem II: General techniques for computing topological properties of real algebraic manifolds. *Adv. Appl. Math. 4*, (1983), 298–351.

[32] Walker, R. J. *Algebraic Curves.* Springer-Verlag, New York, 1978.

[33] Weispfenning, V. Simulation and optimization by quantifier eleimination. *J. Symbolic Computation 24*, (1997), 189–208.

[34] Whitney, H. *Complex Analytic Varieties.* Addison-Wesley, Menlo Park, 1972.

[35] Zariski, O. *Algebraic Surfaces.* Springer-Verlag, New York-Heidelberg-Berlin, 1935.

[36] Zariski, O. Studies in equisingularity I. Equivalent singularities of plane algebroid curves. *Amer. J. Math. 87*, (1965), 507–536. Reprinted in [22].

[37] Zariski, O. Studies in equisingularity II. Equisingularity in codimension 1 (and characteristic zero). *Amer. J. Math. 87*, (1965), 972–1006. Reprinted in [22].

[38] Zariski, O. On equimultiple subvarieties of algebroid hypersurfaces. *Proc. Nat. Acad. Sci., USA 72*, 4 (1975), 1425–1426.

[39] Zariski, O., Samuel, P. *Commutative Algebra Volume II.* Springer-Verlag, New York, 1960.