SCHOOL OF OPERATIONS RESEARCH
AND INDUSTRIAL ENGINEERING
COLLEGE OF ENGINEERING
CORNELL UNIVERSITY
ITHACA, NEW YORK 14853

TECHNICAL REPORT NO. 748

May 1987

ON THE WORST CASE ARITHMETIC COMPLEXITY OF APPROXIMATING ZEROS OF SYSTEMS OF POLYNOMIALS

By

James Renegar

This work was supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship and was performed while the author was visiting the Department of Operations Research at Stanford University.

ON THE WORST CASE ARITHMETIC COMPLEXITY OF APPROXIMATING ZEROS OF SYSTEMS OF POLYNOMIALS

James Renegar
School of Operations Research
and Industrial Engineering
Cornell University
Ithaca, NY 14853

May, 1987

ABSTRACT

Let $d_1,\ldots,d_n$ be positive integers. Let $\mathcal{P}$ denote the set of systems of polynomials $f: \mathbb{C}^n \longrightarrow \mathbb{C}^n$ which have only finitely many zeros, including those "at infinity", and that satisfy $\text{degree}(f_i) = d_i$ for all i. Let $0 < \epsilon \leqslant R$. For fixed $d_1,\ldots,d_n$, we show that with respect to a certain model of computation, the worst case computational complexity of obtaining ϵ-approximations to at least those zeros ξ satisfying $|\xi| \leqslant R$, for arbitrary $f \in \mathcal{P}$, is $\Theta(\log\log(R/\epsilon))$, that is, we prove both upper and lower bounds. We introduce an algorithm for proving the upper bound. The number of operations required by this algorithm is

$$O\left[n\mathcal{D}^4(\log \mathcal{D})(\log\log(R/\epsilon)) + n^2\mathcal{D}^4\binom{1+\sum d_i}{n}^4\right], \text{ where } \mathcal{D} = \Pi_{i=1}^{n} d_i.$$

This work was supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship and was performed while the author was visiting the Department of Operations Research at Stanford University.

1. Introduction

Let $P_d(R)$ denote the set of degree d univariate complex polynomials with all zeros ξ satisfying $|\xi| \leqslant R$. For fixed $d \geqslant 2$, it was shown in Renegar (1987b) that with respect to a certain model of computation, the worst-case arithmetic complexity of obtaining ϵ-approximations to either one, or to each, zero of arbitrary $f \in P_d(R)$ is $\Theta(\log\log(R/\epsilon))$. More specifically, in terms of d as well, a lower bound of $\Omega(\log\log(R/\epsilon))-0(\log d)$ operations was proven, and a new algorithm, requiring $0(d^2(\log d)(\log\log(R/\epsilon)) + d^3 \log d)$ operations, was introduced for the problem of obtaining ϵ-approximations to all of the zeros. We refer the reader to Renegar (1987b) for the general model of "computation tree" used to prove the lower bound, but we remark that it encompasses algebraic RAMs whose operations are +, −, ×, ÷, complex conjugation and inequality comparison. (See Borodin and Munro (1975) as a reference.) Arithmetic operations are assumed to be performed with infinite precision over the complex numbers. The coefficients of the polynomials are not assumed to be rationals, so that simplifying properties like lower bounds on the distance between distinct zeros, in terms of the "length" of the coefficients, cannot be used. For fixed length rational coefficients a uniform $\log\log(R/\epsilon)$ upper bound is fairly straightforward to prove, but for arbitrary complex coefficients it is not.

The purpose of this paper is to present appropriate generalizations of the above results to the several variable setting.

Of course, systems of polynomials are not nearly as simple as univariate polynomials. For example, univariate polynomials have finitely many zeros but polynomial systems $f: \mathbb{C}^n \longrightarrow \mathbb{C}^n$ can have infinitely many zeros, so we cannot hope to approximate all of the zeros unless we restrict attention to "nice" systems. The nice systems that we restrict attention to in this paper are those systems having only finitely many zeros, including the zeros "at infinity". Formally, if $F: \mathbb{C}^{n+1} \longrightarrow \mathbb{C}^n$ is the homogenization of f (i.e., if degree $(f_i) = d_i$, then the terms of F_i are obtained by multiplying the terms of f_i by the appropriate powers of z_{n+1} so as all to become of degree d_i), then f is said to have finitely many zeros, including those at infinity, if the zero set of F is the union of finitely many complex lines through the origin in $\mathbb{C}^{n+1}$. We refer to these lines as the "zero lines" of F; in the literature they are often referred to as the "solution rays" of F. The zero lines of F that are in $\mathbb{C}^n \times \{0\}$ correspond to the zeros of f at infinity. There is an obvious correspondence between the other zero lines of F and the zeros of f in $\mathbb{C}^n$.

Let $d_1,\dots,d_n$ be positive integers. Let $\mathcal{P}$ denote the set of systems

$f = (f_1,\ldots,f_n)\colon \mathbb{C}^n \longrightarrow \mathbb{C}^n$ with only finitely many zeros, including those at infinity, and satisfying degree$(f_i) = d_i$ for all i. (Of course $\mathcal{P}$ depends on the specific values of $d_1,\ldots,d_n$).

We consider the following problem. Let $R \geqslant \epsilon > 0$ and assume $f\colon \mathbb{C}^n \longrightarrow \mathbb{C}^n$ is a polynomial system satisfying degree$(f_i) = d_i$ for all i. First, determine if $f \in \mathcal{P}$. If so, determine ϵ-approximations to a subset of the zeros of f containing at least all zeros ξ satisfying $|\xi| \leqslant R$. (An ϵ-approximation of a zero is a point within Euclidean distance ϵ of the zero.) More specifically, determine points $X^{(1)},\ldots,X^{(m)} \in \mathbb{C}^n$ for which there exist zeros $\xi^{(1)},,,,.\xi^{(m)}$ of f with $\|X^{(i)}-\xi^{(i)}\| \leqslant \epsilon$, where each zero ξ of f satisfying $|\xi| \leqslant R$ is listed among the $\xi^{(i)}$ a number of times exactly equal to its multiplicity, and where no zero of f is listed among the $\xi^{(i)}$ a greater number of times than its multiplicity. (Thus, if each zero ξ of f satisfies $|\xi| \leqslant R$, then each zero can be considered as being approximated by several points $X^{(i)}$, the number of such points being equal to its multiplicity.)

We refer to the above approximation problem as "the (ϵ,R)-approximation problem for f".

We present a test involving $O\left[n\mathcal{D}^2\binom{1+\sum d_i}{n}^4\right]$ operations, where

$$\mathcal{D} = \Pi_{i=1}^n d_i$$

for determining if $f \in \mathcal{P}$. The validity of this test follows straightforwardly from well-known facts regarding resultants. (Resultants are discussed in Section 2.) For those f that pass this test, that is, for $f \in \mathcal{P}$, we also present an algorithm for solving the (ϵ,R)-approximation problem for f. The operation count for this algorithm is

$$O\left[n\mathcal{D}^4(\log \mathcal{D})(\operatorname{loglog}(R/\epsilon)) + n^2\mathcal{D}^4\binom{1+\sum d_i}{n}^4\right].$$

Note that coefficient "sizes" do not enter into this bound in any way.

A significant fact about the bound is how it depends on ϵ and R, that is, the $\operatorname{loglog}(R/\epsilon)$ term. The lower bound in Renegar (1987b) showed that in the univariate setting this is the best possible dependence on R and ϵ that can be obtained. However, that lower bound implies the same lower bound for the several variable setting. For assume one of the $d_i \geqslant 2$, say $d_1 \geqslant 2$. If $g \in P_{d_1}(R)$ (i.e., a degree d_1 univariate polynomial with all zeros ξ satisfying $|\xi| \leqslant R$), then $f\colon \mathbb{C}^n \longrightarrow \mathbb{C}^n$ defined by $f_1(z) = g(z_1)$, $f_2(z) = z_2^{d_2}, \ldots, f_n(z) = z_n^{d_n}$ satisfies $f \in \wp$. Any ϵ-approximation to a zero of f easily gives an ϵ-approximation to a zero of g. Hence, the (ϵ,R)-approximation problem for arbitrary $f \in \wp$ is at least as hard as the ϵ-approximation problem for arbitrary $g \in P_{d_1}(R)$, and thus, in the worst case, equires $\Omega(\log\log(R/\epsilon)) - O(n + \log d_1)$ operations. (The "n" occurs to account for the cost of conversion to the several variable problem.)

Together, our upper and lower bounds give

Main Theorem: Fix $d_1,\ldots,d_n$ and assume $\mathcal{D} = \Pi^n_{i=1} d_i \geqslant 2$. Let $0 < \epsilon \leqslant R$. The arithmetic complexity of obtaining ϵ-approximations to at least those zeros ξ of arbitrary $f \in \wp$ satisfying $|\xi| \leqslant R$ is $\Theta(\log\log(R/\epsilon))$.

Another noteworthy fact about the upper bound is that it is not doubly exponential in n, in contrast to bounds for classical approaches using elimination theory (e.g., see the sections on elimination theory that appear in Van der Waerden (1950)--these sections to not appear in newer editions of the book).

The algorithm for obtaining approximations to the zeros of $f \in \wp$ is actually an algorithm for obtaining approximations to all of the zero lines of the homogenization $F\colon \mathbb{C}^{n+1} \longrightarrow \mathbb{C}^n$ of f, along with a few operations to transform the approximations for F to those for f. By "ϵ-approximations to all of the zero lines of F" we mean non-zero vectors $\mathbb{X}^{(i)} \in \mathbb{C}^{n+1}$, $i = 1,\ldots,\mathcal{D}$ for which there exists a one-to-one correspondence with non-zero vectors $\xi^{(i)} \in \mathbb{C}^{n+1}$, $i = 1,\ldots,\mathcal{D}$ (say, $\mathbb{X}^{(i)}$ corresponds to $\xi^{(i)}$) where the zero lines of F are precisely the lines $\{\lambda\xi^{(i)};\ \lambda \in \mathbb{C}\}$, $i = 1,\ldots,\mathcal{D}$, each occuring according to its multiplicity, and where

$$\left\|\frac{\mathbb{X}^{(i)}}{\|\mathbb{X}^{(i)}\|} - \frac{\xi^{(i)}}{\|\xi^{(i)}\|}\right\| \leqslant \epsilon,$$

$\|\ \|$ denoting the Euclidean norm on $\mathbb{C}^{n+1}$. (The fact that F has $\mathcal{D}$ zero lines, counting multiplicities, is immediate from Theorem 2.3.)

Assuming $\epsilon \leqslant R$, in the appendix we show that if $\mathbb{X}^{(i)}$, $i = 1,\ldots,\mathcal{D}$, are

$\epsilon/4(R+1)^2$-approximations to all of the zero lines of F, then the set of vectors

$$(1.1) \qquad \left\{\left[\left(\frac{\mathbb{X}_1^{(i)}}{\mathbb{X}_{n+1}^{(i)}},\dots,\frac{\mathbb{X}_n^{(i)}}{\mathbb{X}_{n+1}^{(i)}}\right)\right];\ \left|\mathbb{X}_{n+1}^{(i)}\right|/\left\|\mathbb{X}^{(i)}\right\| \geqslant 3/4(R+1)\right\}$$

is a solution for the (ϵ,R)-approximation problem for f.

Let $d_1,\dots,d_n$ be positive integers. Let $\mathcal{H}$ denote the set of systems of homogeneous polynomials $F\colon \mathbb{C}^{n+1} \longrightarrow \mathbb{C}^n$ that have only finitely many zero lines and that satisfy $\text{degree}(F_i) = d_i$ for all i.

Henceforth, we focus on the following problem. Given a system of homogeneous polynomials $F\colon \mathbb{C}^{n+1} \longrightarrow \mathbb{C}^n$, where $\text{degree}(F_i) = d_i$ for all i, is $F \in \mathcal{H}$? If so, determine ϵ-approximations to all of the zero lines of F.

We present a test involving $O\left[n\mathcal{D}^2\binom{1+\sum d_i}{n}\right]$ operations for determining if $F \in \mathcal{H}$, where $\mathcal{D} = \Pi_{i=1}^n d_i$. For $F \in \mathcal{H}$, we present an algorithm for obtaining ϵ-approximations to all of the zero lines of F. The operation count for this algorithm is

$$(1.2) \qquad O\left[n\mathcal{D}^4(\log\ \mathcal{D})(\log\log(1/\epsilon)) + n^2\mathcal{D}^4\binom{1+\sum d_i}{n}^4\right].$$

From these bounds and (1.1) follow the earlier stated upper bounds for determining if $f \in \mathcal{P}$ and for solving the (ϵ,R)-approximation problem for arbitrary $f \in \mathcal{P}$.

Using the lower bound of Renegar (1987b), one can prove that as regards ϵ, the term $\log\log(1/\epsilon)$ occuring in (1.2) is the best possible.

Our algorithm is similar in spirit with the algorithm of Lazard (1981); both algorithms work by factoring the "u-resultant". Lazard only sketches a complexity analysis, avoiding degenerate situations and implicitly assuming that the zeros of a single variable polynomial can be calculated exactly. It is not very difficult to determine "reasonable" complexity bounds for his algorithm if one is only concerned with rational coefficients and is satisfied with a bound on the number of arithmetic operations that grows with the coefficient "lengths". However, his algorithm and analysis are far from providing a uniform bound on arithmetic operations that is independent of the coefficients.

It should be mentioned that Lazard does not restrict attention to the field of complex numbers.

Chistov and Grigor'ev (1983), (1984), extended Lazard's analysis to the problem of approximating a point in each component of the zero set of an arbitrary system of polynomials f: $\mathbb{C}^n \longrightarrow \mathbb{C}^m$ with rational coefficients. Their bound on the required number of arithmetic operations has the maximal coefficient length as a factor. Similarly, this length appears as a factor in the arithmetic operation bound for the recent algorithm of Canny (1987). Canny's algorithm approximates zeros of systems f: $\mathbb{C}^n \longrightarrow \mathbb{C}^n$ also via the u-resultant.

Of related interest is Grigor'ev and Vorobjov (1988), where the problem of constructing approximate solutions to systems of real polynomial inequalities with rational coefficients is considered. Their arithmetic operation bound has the maximal coefficient length as a factor.

It is certainly not the case that our upper bound can be obtained by rounding coefficients to rationals (where the bounding is a function of R and ϵ) and then applying the above mentioned results. Because those results have arithmetic operation bounds (not just bit operation bounds) with the maximal coefficient bit length as a fundamental factor, to prove our $\log\log(R/\epsilon)$ result in this manner would require showing that every polynomial system can be perturbed to one with rational coefficients of length bounded by $\log(R/\epsilon)$, where each zero ξ, $\|\xi\| \leqslant R$, of the original system is approximated within distance ϵ by a zero of the perturbed system. For example, assuming $R = 1$ and $\epsilon = (1/2)^L$, in the univariate case of degree d one would at least need each point in the unit disk in $\mathbb{C}$ to be within distance $(1/2)^L$ of a root of one of the $[O(L)]^{2(d+1)}$ polynomials $\sum_{i=0}^{d} a_i z^i$ with a_i complex rationals of bit length O(L). Of course this is not possible for L large compared to d.

In Renegar (1987a), a probabilistic analysis of an algorithm for approximating all of the zeros of systems of polynomials is given. The bounds are polynomial in n, $\mathcal{D}$ and L, where L is the number of non-zero coefficients in the considered systems. Hence, by focusing on "sparse" systems, a probabilistic bound independent of $\binom{1+\sum d_i}{n}$ can be obtained. (Note that $\binom{1+\sum d_i}{n}$ grows like $\mathcal{D}^n$ when, for example, all polynomials except one are linear.)

Our algorithm relies on the univariate algorithm of Renegar (1987b). The reliance on that particular algorithm is not crucial. What is needed is an algorithm for approximating all zeros of arbitrary $f \in P_d(R)$ with worst-case operation count growing only like $\log\log(R/\epsilon)$ with respect to ϵ and R.

The author gratefully acknowledges the detailed comments provided by an annonymous referee.

2. A Few Facts About Resultants

Let $\mathcal{H}^n_{d_1,\dots,d_n}$ denote the set of all homogeneous polynomial systems $G\colon \mathbb{C}^n \longrightarrow \mathbb{C}^n$ satisfying degree $(G_i) = d_i$. The resultant R for systems in $\mathcal{H}^n_{d_1,\dots,d_n}$ is a homogeneous polynomial in the coefficients of these systems. It has the property that $R(G) = 0$ if and only if G has a non-trivial zero, i.e., $G(x) = 0$ for some $x \neq 0$. In this section we state a few facts regarding the resultant that are crucial for our algorithm.

Let $\bar{d} = 1 - n + \sum_i d_i$ and consider $\mathcal{H}^n_{\bar{d}}$, the vector space consisting of all homogeneous polynomials $g\colon \mathbb{C}^n \longrightarrow \mathbb{C}$ of degree $\bar{d}$, along with the zero map. A basis for this space is easily seen to be given by the set of terms

$$B = \{z_1^{i_1} z_2^{i_2} \dots z_n^{i_n};\ \sum_j i_j = \bar{d},\ \text{each } i_j \text{ a non-negative integer}\}.$$

It is easily shown by the definition of $\bar{d}$ that each of the terms in B satisfies $i_j \geqslant d_j$ for at least one j. Partition B into the disjoint union $\cup_{j=1}^n B_j$ where B_j contains all terms $z_1^{i_1}\dots z_n^{i_n}$ satisfying $i_1 < d_1,\dots,i_{j-1} < d_{j-1},\ i_j \geqslant d_j$.

To each system $G \in \mathcal{H}^n_{d_1,\dots,d_n}$ we can associate a linear map from $\mathcal{H}^n_{\bar{d}}$ to itself, defined for the basis terms in B_j by

$$z_1^{i_1}\dots z_n^{i_n} \longmapsto z_1^{i_1}\dots z_j^{i_j - d_j}\dots z_n^{i_n} \cdot G_j(z_1,\dots,z_n).$$

Let $a_j(i_1,\dots,i_n)$ denote the coefficient in G_j of the term $z_1^{i_1}\dots z_n^{i_n}$. In terms of the basis B, the matrix corresponding to the above linear map is simply the following: the entry in the intersection of the column and row corresponding to $z_1^{i_1}\dots z_n^{i_n} \in B_j$ and $z_1^{k_1}\dots z_n^{k_n}$, respectively, is $a_j(k_1-i_1,\dots,k_j-i_j+d_j,\dots,k_n-i_n)$ if $i_1 \leqslant k_1,\dots,i_j \leqslant k_j+d_j,\dots,i_n \leqslant k_n$, and equals zero otherwise. Let D(G) denote the determinant of this matrix. Then D(G) is a homogeneous polynomial in the coefficients of $G \in \mathcal{H}^n_{d_1,\dots,d_n}$. In fact, it is homogeneous in the coefficients of G_i and has degree, in those coefficients, equal to the number of terms in B_i. Its total degree equals the number of terms in B, that is, $\binom{\bar{d}+n-1}{n-1} = \binom{\Sigma d_i}{n-1}$.

Assume that the linear map associated with $G \in \mathcal{H}^n_{d_1,\ldots,d_n}$ is non-singular, so that for each i = 1,...,n, some polynomial in $\mathcal{H}^n_{\bar{d}}$ is mapped to the term $z_i^{\bar{d}}$. Hence, for each i,

$$z_i^{\bar{d}} = \sum_{j=1}^{n} p_j(z_1,\ldots,z_n)G_j(z_1,\ldots,z_n)$$

for some polynomials $p_1,\ldots,p_n$ (dependent on i). It easily follows that $G(x) \neq 0$ if $x \neq 0$. Thus $D(G) = 0$ is a necessary condition for there to exist a non-trivial zero for G. However, it is not a sufficient condition, but we do have the following remarkable theorem.

Theorem 2.1 (Macaulay, 1902, Theorem 6): Let M(G) denote the determinant of the submatrix (of the matrix corresponding to the linear map induced by G) consisting of entries for which both the row and column correspond to terms in B of the form $z_1^{i_1}\ldots z_n^{i_n}$ with at least two i_j and i_k satisfying $i_j \geqslant d_j$, $i_k \geqslant d_k$. Then M(G), a polynomial in the coefficients of $G \in \mathcal{H}^n_{d_1,\ldots,d_n}$, is a factor of the polynomial D(G). Moreover, letting R(G) be the polynomial satisfying D(G) = M(G)R(G), then R(G) = 0 is a necessary and sufficient condition for G to have a non-trivial zero. □

Remark: Macaulay's Theorem 6 actually does not state the last conclusion of Theorem 2.1. This was well-known to him, and is stated in the introduction to his paper. A proof of the last conclusion is given in Van der Waerden (1950), Section 82. (Beware that in some editions of Van der Waerden's book this section on elimination theory has been eliminated!)

The polynomial R(G) is the "resultant". Both it and M(G) are homogeneous in the coefficients of each G_i. The degree of R(G) in the coefficients of G_i is $\Pi_{j \neq i} d_j$. Also, M(G) is independent of the coefficients of G_n.

Now we turn attention to systems of homogeneous polynomials

$F\colon \mathbb{C}^{n+1} \longrightarrow \mathbb{C}^n$ satisfying degree $(F_i) = d_i$. Let $\mathcal{H}^{n+1}_{d_1,\ldots,d_n}$ denote the set of these systems. Here we are concerned with the question, "Does $F \in \mathcal{H}^{n+1}_{d_1,\ldots,d_n}$ have only finitely many zero lines?"

Let $u_1,\ldots,u_{n+1}$ denote variables. For specified values of these variables, consider the system $z \longmapsto (F(z), u\cdot z)$, where $u\cdot z = \sum_i u_i z_i$. This is a system in $\mathcal{H}^{n+1}_{d_1,\ldots,d_n,1}$. Let $R(F,u)$ denote the resultant of this system. For D and M as in Theorem 2.1, define $D(F,u)$ and $M(F,u)$ analogously. These are polynomials in the coefficients of $F \in \mathcal{H}^{n+1}_{d_1,\ldots,d_n}$ and the variables u. In the literature, $R(F,u)$ is sometimes refered to as "the u-resultant of F".

We remark, for future reference, that the determinant $M(F,u)$ is independent of the variables u. Also, $D(F,u)$ is the determinant of a $\left[\begin{matrix}1+\sum d_i\\ n\end{matrix}\right] \times \left[\begin{matrix}1+\sum d_i\\ n\end{matrix}\right]$ matrix, and $M(F,u)$ is the determinant of a smaller matrix.

Proposition 2.2: Fix $F \in \mathcal{H}^{n+1}_{d_1,\ldots,d_n}$. Then $R(F,u) = 0$ for all u if and only if F has infinitely many zero lines.

Proof: This is well-known, but I was unable to find a reference for it. Here is a short proof.

Assume that F has finitely many solution lines. For each of these lines, choose a non-zero vector on that line. Assume $\alpha^{(1)},\ldots,\alpha^{(m)}$ are the chosen vectors. There exists $x \in \mathbb{C}^{n+1}$ such that $x\cdot\alpha^{(i)} \neq 0$ for all i. Then the system $z \longmapsto (F(z), x\cdot z)$ has no non-trivial zero and hence $R(F,x) \neq 0$.

Now assume that F has infinitely many solution lines. Choose non-zero vectors $\alpha^{(1)},\alpha^{(2)},\ldots,$ on each line in an infinite, but countable, subset of the zero lines. Fix $x \in \mathbb{C}^{n+1}$ satisfying $x \notin \bigcup_i \{y;\ \alpha^{(i)}\cdot y = 0\}$. There exists a complex line L containing x that has infinitely many intersection points with $\bigcup_i \{y;\ \alpha^{(i)}\cdot y = 0\}$. However, for each of these intersection points y, the map $z \longmapsto (F(z), y\cdot z)$ has a nontrivial solution so that $R(F,y) = 0$. Hence, the univariate polynomial obtained by restricting $R(F,u)$ to $u \in L$ has infinitely many zeros, and thus must be the zero polynomial. Consequently, $R(F,x) = 0$. Finally, if

$x \in \bigcup_i \{y;\ \alpha^{(i)} \cdot y = 0\}$ then it is easy to prove that $R(F,x) = 0$. □

The following theorem is the cornerstone for our algorithm.

<u>**Theorem**</u> <u>**2.3**</u>: Assume that $F \in \mathcal{H}^{n+1}_{d_1,\ldots,d_n}$ has only finitely many zero lines. For $u \in \mathbb{C}^{n+1}$, let $R(u) \doteq R(F,u)$. Then $R(u)$ has factorization

$$R(u) = \Pi_{\ell=1}^{\mathcal{D}} (\xi^{(\ell)} \cdot u)$$

where $\xi^{(\ell)} \cdot u = \sum_i \xi_i^{(\ell)} u_i$, $\mathcal{D} = \Pi_{i=1}^n d_i$ and each $\xi^{(\ell)}$ is a non-trivial zero of F. Moreover, for each zero line of F, the number of the $\xi^{(\ell)}$ that are contained in that zero line equals the multiplicity of that zero line.

<u>**Proof**</u>: A proof can be found in Section 83 of Van der Waerden (1950). (Again, be careful to choose an edition of Van der Waerden's book containing the section on elimination theory.) □

3. Computing R(u)

Using the notation of the previous section, assume that $F \in \mathcal{H}^{n+1}_{d_1,\ldots,d_n}$ has only finitely many solution lines and let $R(u) \doteq R(F,u)$, where $R(F,u)$ is the u-resultant of F. Our algorithm depends on being able to compute $R(u)$ and some of its derivatives along certain complex lines. In this section we discuss procedures for doing this.

Let $\alpha, \beta \in \mathbb{C}^{n+1}$, where $\alpha \neq 0$. We first discuss a procedure for obtaining an expansion of the single variable polynomial $\lambda \longmapsto R(\lambda\alpha+\beta)$.

Refering again to the notation of the previous section, begin by computing the determinant $M(F,u)$--this determinant is independent of the variables u, depending only on the fixed coefficients of F. It can be computed with $O\left[\binom{\bar{d}+n}{n}^3\right]$ operations, where $\bar{d} = n - 1 + \sum_i d_i$.

If $M(F,u) \neq 0$, then by Theorem 2.1, $R(u) = D(F,u)/M(F,u)$. Noting that $D(\lambda\alpha+\beta) \doteq D(F,\lambda\alpha+\beta)$ is defined as the determinant of a certain $\binom{1+\sum d_i}{n} \times \binom{1+\sum d_i}{n}$ matrix, and is of degree $\mathcal{D}$ in the variable λ, compute the coefficients of the polynomial $D(\lambda\alpha+\beta)$ by evaluating this determinant at $\mathcal{D} + 1$ distinct values of λ, and then interpolating. Thus, assuming $M(F,u) \neq 0$, we can obtain the coefficients of a non-zero multiple of $R(\lambda\alpha+\beta)$ with $O\left[\mathcal{D}\binom{1+\sum d_i}{n}^3\right]$ operations (using $\mathcal{D} < \binom{1+\sum d_i}{n}$).

Now assume $M(F,u) = 0$. For $t \in \mathbb{R}$, let $F_i^t(z) = tz_i^{d_i} + (1-t)F_i(z)$ for $i = 1,\ldots,n$. Then $M(F^t,u)$ is a polynomial in t alone, and is of degree not exceeding $\binom{1+\sum d_i}{n}$. It is non-constant since $M(F^0,u) = 0$ and $M(F^1,u) = 1$. Determine the coefficients of $M(F^t,u)$ by evaluating the corresponding determinant for $\binom{1+\sum d_i}{n} + 1$ distinct values of t, and then interpolating.

Determine <u>the least</u> integer $0 \leqslant k \leqslant \binom{1+\sum d_i}{n}$ such that

$$\frac{d^k}{dt^k} M(F^t,u)\Big|_{t=0} \neq 0.$$

Then, using Theorem 2.1 and the product rule for differentiation,

$$\left.\frac{d^k D(F^t,u)}{dt^k}\right|_{t=0} = R(F,u)\cdot\left.\frac{d^k M(F^t,u)}{dt^k}\right|_{t=0}$$

as polynomials in u. Hence, $R(\lambda\alpha+\beta)$ equals

$$\left.\frac{d^k D(F^t,\lambda\alpha+\beta)}{dt^k}\right|_{t=0}$$

divided by the already computed non-zero constant

$$\left.\frac{d^k M(F^t,u)}{dt^k}\right|_{t=0}.$$

Finally, we examine the computation of

$$\left.\frac{d^k D(F^t,\lambda\alpha+\beta)}{dt^k}\right|_{t=0}.$$

Since $D(F^t,\lambda\alpha+\beta)$ is a polynomial in the variables λ and t, of degree not exceeding $\mathcal{D}$ in λ and of degree not exceeding $\begin{Bmatrix} 1+\sum d_i \\ n \end{Bmatrix}$ in t, $D(F^t,\lambda\alpha+\beta)$ can be expanded as follows:

$$D(F^t,\lambda\alpha+\beta) = \sum_{i=0}^{\begin{Bmatrix} 1+\sum d_i \\ n \end{Bmatrix}} \left\{\sum_{j=0}^{\mathcal{D}} a_{ij}\lambda^j\right\} t^i.$$

We wish to determine $\sum_{j=0}^{\mathcal{D}} a_{kj}\lambda^j$, for k as defined earlier.

Choose $\mathcal{D}+1$ distinct values $\lambda_\ell \in \mathbb{C}$ and $\begin{Bmatrix} 1+\sum d_i \\ n \end{Bmatrix}+1$ distinct values t_m. For fixed λ_ℓ, evaluate the determinant $D(F^{t_m},\lambda_\ell\alpha+\beta)$ for all pairs $\{(\lambda_\ell,t_m)\}_m$. Interpolate in t to determine the expansion of the single variable polynomial $D(F^t,\lambda_\ell\alpha+\beta)$, thereby obtaining the value $\sum_{j=0}^{\mathcal{D}} a_{kj}\lambda_\ell^j$. Do this for each λ_ℓ. Then interpolate in λ to obtain the expansion $\sum_{j=0}^{\mathcal{D}} a_{kj}\lambda^j$.

Thus, we have a method for computing the coefficients of $R(\lambda\alpha+\beta)$. The total operation count is dominated by the operation count required to compute the

$[\mathcal{D}+1]\left[\left[\binom{1+\sum d_i}{n}\right]+1\right]$ determinants $D(F^{t_m},\lambda_\ell\alpha+\beta)$. Hence, the total operation count is $O\left[\mathcal{D}\left[\binom{1+\sum d_i}{n}\right]^4\right]$.

Besides an expansion for $R(\lambda\alpha+\beta)$, we will also need expansions for the multi-variable polynomials $R(\lambda\alpha+\rho_1 e_i+\rho_2 e_j+\beta)$, where ρ_1 and ρ_2 are variables over $\mathbb{C}$ and where e_i and e_j are the i^{th} and j^{th} unit vectors. Defining F^t as before, and writing

$D(F^t,\lambda\alpha+\rho_1 e_i+\rho_2 e_j+\beta)$

$$= \sum_{m_1=1}^{\binom{1+\sum d_i}{n}} \left[\sum_{m_2=0}^{\mathcal{D}}\left[\sum_{m_3=0}^{\mathcal{D}}\left[\sum_{m_4=0}^{\mathcal{D}} a_{m_1m_2m_3m_4}\rho_2^{m_4}\right]\rho_1^{m_3}\right]\lambda^{m_2}\right]t^{m_1},$$

we wish to obtain the triple summation which is a multiple of t^k, where k is the smallest integer such that $\left.\frac{d^kM(F^t,u)}{dt^k}\right|_{t=0} \neq 0$. Dividing that triple summation by the constant $\left.\frac{d^kM(F^t,u)}{dt^k}\right|_{t=0}$ gives $R(\lambda\alpha+\rho_1 e_i+\rho_2 e_j+\beta)$. However, to obtain the triple summation we can use the generalization of the procedure we used for computing $\left.\frac{d^kD(F^t,\lambda\alpha+\beta)}{dt^k}\right|_{t=0}$. First, interpolate in t to obtain

$$\sum_{m_2=0}^{\mathcal{D}}\left[\sum_{m_3=0}^{\mathcal{D}}\left[\sum_{m_n=0}^{\mathcal{D}} a_{m_1m_2m_3k}\rho_2^{m_4}\right]\rho_1^{m_3}\right]\lambda^{m_2}$$

for <u>fixed</u> values of the parameters ρ_1,ρ_2 and λ. Then interpolate in λ to obtain

$$\sum_{m_3=0}^{\mathcal{D}}\left[\sum_{m_4=0}^{\mathcal{D}} a_{m_1m_2m_3k}\rho_2^{m_4}\right]\rho_1^{m_3}, \qquad m_2 = 1,\ldots,\mathcal{D}$$

for fixed values of the parameters ρ_1 and ρ_2. For each m_2, interpolate in ρ_1 to obtain

$$\sum_{m_4}^{\mathcal{D}} a_{m_1m_2m_3k}\rho_2^{m_4} \qquad m_2,m_3 = 1,\ldots,\mathcal{D}$$

for fixed values of the parameter ρ_2. Finally, for each pair (m_2,m_3), interpolate in

ρ_1 to obtain all of the coefficients $a_{m_1 m_2 m_3 k}$. Altogether, $O\left[\mathcal{D}^3 \binom{1+\sum d_i}{n}^4\right]$ operations suffice.

4. The Algorithm

In this section we present the algorithm which, given $F \in \mathcal{H}^{n+1}_{d_1,\ldots,d_n}$, determines if F has only finitely many solution lines and, if so, obtains ϵ-approximations to all of them.

The idea underlying the algorithm is rather simple, although the technicalities that must be dealt with are not. Here is the idea. Assume that F has only finitely many solution lines and, for simplicity, assume that each of these are of multiplicity one. By Theorem 2.1,

$$R(u) = \Pi_{\ell=1}^{\mathcal{D}}(\xi^{(\ell)}\cdot u), \tag{4.1}$$

where the $\xi^{(\ell)}$ are vectors on the solution lines. Let

$$H^{(\ell)} = \{x \in \mathbb{C}^{n+1};\ \xi^{(\ell)}\cdot x = 0\}. \tag{4.2}$$

Assume $\alpha', \beta' \in \mathbb{C}^{n+1}$, $\alpha' \neq 0$, and assume that the complex line $\{\lambda\alpha'+\beta';\ \lambda \in \mathbb{C}\}$ intersects each of the hyperplanes $H^{(\ell)}$, but does not intersect $H^{(\ell)} \cap H^{(m)}$ if $\ell \neq m$. Compute the zeros λ' of the degree $\mathcal{D}$ single variable polynomial $R(\lambda\alpha'+\beta')$--for the moment we assume that these can be calculated exactly. There is a one-to-one correspondence between the λ' and the ℓ defined by the relation $\lambda'\alpha'+\beta' \in H^{(\ell)}$. For λ' corresponding to ℓ, the vector

$$\left(\frac{\partial}{\partial u_1}R(u)\Big|_{u=\lambda'\alpha+\beta},\ldots,\frac{\partial}{\partial u_{n+1}}R(u)\Big|_{u=\lambda'\alpha+\beta}\right)$$

is a non-zero scalar multiple of $\xi^{(\ell)}$ and hence is on the zero line $\{\lambda\xi^{(\ell)};\ \lambda \in \mathbb{C}\}$. This is the main idea behind the algorithm.

Of course the algorithm must be able to work without relying on the above simplifying assumptions.

We present the steps of the algorithm and state propositions regarding the steps simultaneously in hopes that this will better motivate what the steps are designed to accomplish. Proofs are relegated to section 5. Some of the propositions rely on O( ) notation for upper bounds and Ω( ) notation for lower bounds. The constants are independent of $n, d_1, \ldots, d_n$ and hence independent of F. Specific constants can be obtained with more lengthy proofs.

For non-zero $\mathbb{X},Y \in \mathbb{C}^{n+1}$, define

$$\mathrm{dis}(X,Y) = \min\left\{\left|\left|\frac{w_1 X}{||w_1 X||} - \frac{w_2 Y}{||w_2 Y||}\right|\right|;\ w_1,w_2 \in \mathbb{C}\setminus\{0\}\right\}.$$

Using the homogeneity of F, it is easily shown that $\mathbb{X}^{(i)}$, $i = 1,\ldots,\mathcal{D}$ are ϵ-approximations to the zero lines of F if and only if $\mathrm{dis}(\mathbb{X}^{(i)},\xi^{(i)}) \leqslant \epsilon$ for all i, where the $\xi^{(i)}$ are as in (4.1).

For $x \in \mathbb{C}$, define

$$\mu(x) = (1,x,x^2,\ldots,x^n).$$

We use λ to denote a complex variable.

__Step 1__: Compute $R(\alpha)$ for all $\alpha \in \{\mu(j);\ j = 0,1,\ldots,n\mathcal{D}\}$.

From the results in Section 3, Step 1 can be accomplished with $O\left[n\mathcal{D}^2\left(\frac{1+\Sigma d_i}{n}\right)^4\right]$ operations.

__Proposition 4.1__: All numbers computed in Step 1 are zero if and only if F has infinitely many zero lines.

__Proof:__ Since for any distinct integers $j_1,\ldots,j_{n+1}$ the $(n+1) \times (n+1)$ matrix with i^{th} row $\mu(j_i)$ is invertible, there are at most $n\mathcal{D}$ integer values j such that $\mu(j) \in \bigcup_{\ell}\{u;\ \zeta^{(\ell)}\cdot u = 0\}$. □

Hereafter, we assume that F has only finitely many zero lines.

The purpose of the next two steps is to determine a vector α' for which the "angle of incidence" of α' with any of the complex hyperplanes $H^{(\ell)}$ can be bounded away from zero. This property of α' will be relied on in the analysis in two ways. First, it will provide a bound on the absolute value of the zeros of any univariate polynomial $\lambda \longmapsto R(\lambda\alpha' + \beta)$. We will need this bound when we call on the univariate algorithm of Renegar (1987b). Second, the property of α' will guarantee that for any β, if $\mathrm{dis}(\xi^{(\ell)},\xi^{(m)})$ is small, then so is $|\lambda^{(\ell)} - \lambda^{(m)}|$ where $\lambda^{(\ell)}\alpha' + \beta \in H^{(\ell)}$, $\lambda^{(m)}\alpha' + \beta \in H^{(m)}$. This will be important for proving the correctness of the procedure for determining the number of lines in a "clustered" set of zero lines.

More specifically, for α' as to be determined by Steps 2 and 3, we have the following.

Proposition 4.2: For any $\beta \in \mathbb{C}^{n+1}$, all zeros λ' of $R(\lambda\alpha' + \beta)$ satisfy

$$|\lambda'| = O(\|\beta\|[n\mathcal{D}]^{2n\mathcal{D}}).$$

Moreover, if $\lambda^{(\ell)}\alpha' + \beta \in H^{(\ell)}$, $\lambda^{(m)}\alpha' + \beta \in H^{(m)}$, then

$$|\lambda^{(\ell)} - \lambda^{(m)}| = O(\|\beta\|[n\mathcal{D}]^{5n\mathcal{D}}\mathrm{dis}(\xi^{(\ell)},\xi^{(m)})).$$

Proof: Proposition 5.4. □

If we are only concerned with polynomial systems with rational coefficients, an analogue of Proposition 4.2 with bounds depending on the bit lengths of the coefficients is easily proven. Bounds, such as ours, which hold for all polynomial systems require more detailed arguments.

Step 2: For each $j = 0,1,\ldots,n\mathcal{D}$ and each $i = 1,\ldots,n+1$, compute the coefficients $a_k(i,j)$ of $R(\lambda\alpha+e_i) = \sum_{k=1}^{\mathcal{D}} a_k(i,j)\lambda^k$, where $\alpha = \mu(j)$.

From the results in Section 3, Step 2 can be accomplished with $O\left[n^2\mathcal{D}^2\binom{1+\sum d_i}{n}^4\right]$ operations.

Note that $a_{\mathcal{D}}(i,j) = R(\mu(j))$.

Step 3: Let $J \subseteq \{0,1,\ldots,n\mathcal{D}\}$ denote the subset $J = \{j;\ R(\mu(j)) \neq 0\}$. By

Proposition 4.1, $J \neq \emptyset$. Determine $j' \in J$ satisfying

$$\max_{\substack{i\\ k<\mathcal{D}}} \left|\frac{a_k(i,j')}{R(\mu(j'))}\right|^2 = \min_{j\in J} \max_{\substack{i\\ k<\mathcal{D}}} \left|\frac{a_k(i,j)}{R(\mu(j))}\right|^2 .$$

Let $\alpha' = \mu(j)$.

The reduction to the univariate case occurs in the next step. However, rather than a reduction to a single univariate polynomial, we are forced to consider $n\mathcal{D}(\mathcal{D}-1)/2+1$ univariate polynomials, approximating the zeros for each of these. Here is why we are forced to do this. Recall the "idea" behind the algorithm as discussed at the beginning of this section. Assume β' is such that the complex line $\{\lambda\alpha' + \beta';\ \lambda \in \mathbb{C}\}$ intersects $H^{(\ell)}$ and $H^{(m)}$ at nearly the same point, yet $\text{dis}(\xi^{(\ell)},\xi^{(m)})$ is large. Then even if $\gamma^{(\ell)}$ is a close approximation to the point $\lambda^{(\ell)}$ for which $\lambda^{(\ell)}\alpha' + \beta' \in H^{(\ell)}$, it is not likely that $\text{dis}(X^{(\ell)},\xi^{(\ell)})$ is small where

$$X^{(\ell)} = \left\{\frac{\partial}{\partial u_1} R(u)\Big|_{u=\gamma^{(\ell)}\alpha'+\beta'},\ldots,\frac{\partial}{\partial u_{n+1}} R(u)\Big|_{u=\gamma^{(\ell)}\alpha'+\beta'}\right\}.$$

To guarantee good approximations, we need $\{\lambda\alpha' + \beta';\ \lambda \in \mathbb{C}\}$ to intersect $H^{(\ell)}$ and $H^{(m)}$ at nearly the same point only if $\text{dis}(\xi^{(\ell)},\xi^{(m)})$ is small. (Furthermore, in that case, we need to define $X^{(\ell)}$ by appropriate higher order derivatives.) As will be proven, at least one of the β's considered in Step 4 has this property. The large amount of computation required in Steps 4, 5 and 6 is to determine which one. (What these steps are designed to accomplish can be achieved easily if we restrict ourselves to rational coefficients and are only concerned with bounding the number of required arithmetic operations in the algorithm by a polynomial in the bit length of the coefficients.)

Step 4 involves a new parameter, $\epsilon' > 0$.

<u>Step</u> <u>4</u>: For each $k = 0,1,\ldots,n\mathcal{D}(\mathcal{D}-1)/2$ apply the algorithm in Renegar (1987b) (or any other algorithm with an $O(\log\log(R/\epsilon))$ bound) to obtain ϵ'-approximations $\gamma_1(k),\ldots,\gamma_{\mathcal{D}}(k)$ for all of the zeros $\lambda_1(k),\ldots,\lambda_{\mathcal{D}}(k)$ (counting multiplicities) of

$R(\lambda\alpha'+\beta)$, where $\beta = \mu(k)$.

We will show later that any value $\epsilon' = O(\epsilon^{n\mathcal{D}^4+1}/[n\mathcal{D}]^{10n^2\mathcal{D}^5+3n+3})$ suffices for our purposes.

The algorithm in Renegar (1987b) requires an apriori bound on the $|\lambda_i(k)|$. However, since $\|\mu(k)\| < [n\mathcal{D}]^{2n}$, such a bound can be obtained from Proposition 4.2. Using this and the $O(d^2(\log d)(\log\log(R/\epsilon)) + d^3\log d)$ bound for the algorithm in Renegar (1987b), we find that step 4 can be accomplished with $O(n\mathcal{D}^4(\log \mathcal{D})(\log\log(1/\epsilon')) + n\mathcal{D}^5\log \mathcal{D})$ operations.

In the next step we partition the approximations $\gamma_1(k),\ldots,\gamma_{\mathcal{D}}(k)$ into clusters, for each k. Roughly, a cluster of the approximations is a subset of the approximations that is contained in a disk and for which none of the other approximations is contained in a much larger concentric disk. The radius ϵ'' of the smaller disk and the magnitude δ of the quotient of the radius of the larger disk to that of the smaller disk will be crucial in our analysis.

In Step 6 we will single out a k for which Step 5 has produced the largest number of clusters. As we will prove, this k has the property that $\{\lambda\alpha' + \mu(k);\ \lambda \in \mathbb{C}\}$ intersects $H^{(\ell)}$ and $H^{(m)}$ at nearly the same point only if $\mathrm{dis}(\xi^{(\ell)},\xi^{(m)})$ is small.

Step 5 requires the cluster parameter δ mentioned above. As will be proven, all $\delta = \Omega([n\mathcal{D}]^{10n\mathcal{D}}/\epsilon)$ will suffice for our purposes.

__Step 5__: Initially, let $\epsilon'' = \epsilon'$, where ϵ' is as in Step 4.

5.1: Determine if there exists i,j,k such that

$$(\epsilon'')^2 < |\gamma_i(k) - \gamma_j(k)|^2 \leqslant (\delta\epsilon'')^2$$

If so, let $\delta\epsilon'' \longrightarrow \epsilon''$ and repeat 5.1.

5.2: For each k partition the approximations into disjoint subsets $P^{[h]}(k)$, $h = 1,\ldots,h(k)$, where $\gamma_i(k)$ and $\gamma_j(k)$ are in the same subset if and only if $|\gamma_i(k) - \gamma_j(k)| \leqslant \epsilon''$. (To establish the existence of this partition, we need the property that $|\gamma_i(k) - \gamma_j(k)| \leqslant \epsilon''$ and $|\gamma_j(k) - \gamma_m(k)| \leqslant \epsilon''$ together imply $|\gamma_i(k) - \gamma_m(k)| \leqslant \epsilon''$. But this is trivial, assuming $\delta \geqslant 2$, since 5.1 has been passed through.

It is easily seen that 5.1 will be passed through after at most $O(n\mathcal{D}^4)$ iterations and hence the final value of ϵ'' satisfies $\epsilon'' \leqslant \delta^{n\mathcal{D}^4}\epsilon'$. Since each iteration of 5.1 involves $O(n\mathcal{D}^4)$ operations, as does 5.2, the operation count for Step 5 is $O(n^2\mathcal{D}^8)$.

__Step 6__: Determine k' satisfying $h(k') = \max\limits_{k} h(k)$, i.e., a k with the largest number of clusters. Let $\beta' = \mu(k')$. For each h fix a $\gamma^{[h]} \in P^{[h]}(k')$. Let $x^{[h]} = \gamma^{[h]}\alpha' + \beta'$. (If $h(k') = 1$, we define $x[h] = 0$ to simplify the analysis later.)

To ease the exposition, we now alter our notation slightly. There is a one-to-one correspondence between the points $\lambda_i(k')$, k' as in step 6, and the complex hyperplanes $H^{(\ell)}$, where $\lambda_i(k')$ corresponds to $H^{(\ell)}$ only if $\lambda_i(k')\alpha'+\beta' \in H^{(\ell)}$. Reindexing the hyperplanes if necessary, we may write $\lambda^{(\ell)}$ for the $\lambda_i(k')$ corresponding to $H^{(\ell)}$, and $\gamma^{(\ell)}$ for the approximation $\gamma_i(k')$ of that $\lambda_i(k')$. Also, we replace $P^{[h]}(k')$ by $P^{[h]}$.

The goals of all preceeding steps are summarized in the following proposition.

__Proposition 4.3__: For any $\delta = \Omega([n\mathcal{D}]^{10n\mathcal{D}})$ and for ϵ'' as given at the end of Step 5.1,

(4.3) $$\gamma^{(\ell)} \in P^{[h]} \Rightarrow |\xi^{(\ell)}\cdot x^{[h]}| = O(\epsilon''[n\mathcal{D}]^{n+1}\|\xi^{(\ell)}\|),$$

(4.4) $$\gamma^{(\ell)} \notin P^{[h]} \Rightarrow |\xi^{(\ell)}\cdot x^{[h]}| = O(\delta\epsilon''\|\xi^{(\ell)}\|/[n\mathcal{D}]^{2n\mathcal{D}}),$$

(4.5) $$\gamma^{(\ell)},\gamma^{(m)} \in P^{[h]} \Rightarrow \mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) = O(\epsilon''[n\mathcal{D}]^{3n+2}).$$

__Proof__: Proposition 5.6. □

Combining Proposition 4.3 with the following two propositions will motivate the final step of the algorithm. The first of these two propositions covers a "trivial" case.

__Proposition 4.4:__ Assume that for all $\ell, m \in \{1,\dots,\mathcal{D}\}$ we have that $\mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) \leqslant \epsilon'''$. For all $\epsilon''' = O(1/\sqrt{n})$, the following is then true. Let i' be an index satisfying

$$\left|\left.\frac{\partial^{\mathcal{D}} R(u)}{\partial u_{i'}^{\mathcal{D}}}\right|_{u=0}\right| = \max_{i}\left|\left.\frac{\partial^{\mathcal{D}} R(u)}{\partial u_{i}^{\mathcal{D}}}\right|_{u=0}\right|$$

and let $\mathbb{X} \in \mathbb{C}^{n+1}$ be the vector

$$\mathbb{X}_i = \left.\frac{\partial^{\mathcal{D}} R(u)}{\partial u_{i'}^{\mathcal{D}-1}\partial u_i}\right|_{u=0} \qquad i = 1,\dots,n+1.$$

Then $\mathrm{dis}(\mathbb{X},\xi^{(\ell)}) = O(n\epsilon''')$ for all ℓ.

__Proof:__ Proposition 5.8. □

__Proposition 4.5:__ Let $S \subset \{1,\dots,\mathcal{D}\}$ contain N elements, where $0 < N < \mathcal{D}$. Assume that for all $\ell, m \in S$, we have $\mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) \leqslant \epsilon'''$. Let $x \in \mathbb{C}^{n+1}$, $x \neq 0$. Assume that if $\ell \notin S$, then $|\xi^{(\ell)} \cdot x| \leqslant \rho_1 \|\xi^{(\ell)}\|\,\|x\|$, and assume that if $\ell \notin S$, then $|\xi^{(\ell)} \cdot x| \geqslant \rho_2 \|\xi^{(\ell)}\|\,\|x\|$ where $\rho_2 > 0$. Then for all $\epsilon''' = O(1/\sqrt{n})$ and for all $\rho_1/\rho_2 = O(\epsilon'''/\mathcal{D}!n)$, the following is true. Let i' be an index satisfying

$$\left|\left.\frac{\partial^{N} R(u)}{\partial u_{i'}^{N}}\right|_{u=x}\right| = \max_{i}\left|\left.\frac{\partial^{N} R(u)}{\partial u_{i}^{N}}\right|_{u=x}\right|,$$

and let $\mathbb{X} \in \mathbb{C}^{n+1}$ be the vector

$$\mathbb{X}_i = \left.\frac{\partial^{N} R(u)}{\partial u_{i'}^{N-1}\partial u_i}\right|_{u=x} \qquad i = 1,\dots,n+1.$$

Then $\mathrm{dis}(\mathbb{X},\xi^{(\ell)}) = O(n\mathcal{D}\epsilon''')$ for all $\ell \in S$.

__Proof:__ Proposition 5.9. □

Now we combine the last three propositions to motivate and prove the correctness of the final step of the algorithm.

Assume that $0 < C \leqslant 1$ is sufficiently small so that for all $n,\mathcal{D}$ and $0 < \epsilon \leqslant 1$,

$$\epsilon''' \doteq \frac{C\epsilon}{n\mathcal{D}} \tag{4.6}$$

satisfies the conditions required for Propositions 4.4 and 4.5.

For $h = 1,\ldots,h(k')$, let

$$S^{[h]} = \{\ell;\ \gamma^{(\ell)} \in P^{[h]}\},$$

i.e., the "indices" of the approximations in $P^{[h]}$. We now show that for all

$$\delta = \Omega([n\mathcal{D}]^{10n\mathcal{D}}/\epsilon), \tag{4.7}$$

and for all

$$\epsilon' = O(\epsilon/\delta^{n\mathcal{D}^4}[n\mathcal{D}]^{3n+3}) \tag{4.8}$$

the conditions required for Proposition 4.4 (if $h(k') = 1$) or the conditions required for Proposition 4.5 (if $h(k') > 1$) are satisfied by $S = S^{[h]}$, $x = x^{[h]}$ for ϵ''' as defined by (4.6).

First note that combining the bound $\epsilon'' \leqslant \delta^{n\mathcal{D}^4}\epsilon'$ (as discussed after Step 5) with (4.5) gives

$$\ell,m \in S^{[h]} \Rightarrow \mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) \leqslant O(\delta^{n\mathcal{D}^4}[n\mathcal{D}]^{3n+2}\epsilon'). \tag{4.9}$$

Assume $h(k') = 1$. Then assuming δ is of the form (4.7) (to meet the requirement of Proposition 4.3), by choosing ϵ' of the form (4.8) we have from (4.9) that $\mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) \leqslant \epsilon'''$ for all ℓ,m, where ϵ''' is as in (4.6). Hence the conditions required for Proposition 4.4 are then satisfied.

Now assume $h(k') > 1$ and fix $h \in \{1,\ldots,h(k')\}$. Define

$$\rho_1 = \max\{|\xi^{(\ell)}\cdot x^{[h]}|/\|\xi^{(\ell)}\|\ \|x^{[h]}\|;\ \ell \in S^{[h]}\},$$

(4.10)

$$\rho_2 = \min\{|\xi^{(\ell)}\cdot x^{[h]}|/\|\xi^{(\ell)}\|\ \|x^{[h]}\|;\ \ell \notin S^{[h]}\}.$$

By (4.3) and (4.4),

$$\frac{\rho_1}{\rho_2} = O([n\mathscr{D}]^{2n\mathscr{D}+n+1}/\delta),$$

and hence, assuming (4.7), we find that ρ_1/ρ_2 is sufficiently small as required by Proposition 4.5 for ϵ''' as in (4.6). Also, assuming δ fixed and of the form (4.7), by choosing ϵ' of the form (4.8) we have from (4.9) that

$$\ell, m \in S^{[h]} \Rightarrow \mathrm{dis}(\xi^{(\ell)}, \xi^{(m)}) \leqslant \epsilon''',$$

for ϵ''' as in (4.6). Finally, we note that $x^{[h]} \neq 0$ since otherwise would contradict (4.4) for $\ell \notin S^{[h]}$. We have thus established the conditions required for Proposition 4.5 in the case that h(k') > 1 and for Proposition 4.4 in the case that h(k') = 1.

Step 7: If h(k') = 1, then determine the index i' satisfying

$$\left|\frac{\partial^{\mathscr{D}} R(u)}{\partial u_{i'}^{\mathscr{D}}}\right|_{u=0}\Bigg|^2 = \max_i \left|\frac{\partial^{\mathscr{D}} R(u)}{\partial u_i^{\mathscr{D}}}\right|_{u=0}\Bigg|^2,$$

and let $\mathbb{X}^{[1]} \in \mathbb{C}^{n+1}$ be the vector

$$\mathbb{X}_i^{[1]} = \frac{\partial^{\mathscr{D}} R(u)}{\partial u_{i'}^{\mathscr{D}-1}\partial u_i}\Bigg|_{u=0} \qquad i = 1,\ldots,n+1.$$

If h(k') > 1, then perform the following for each $h \in \{1,\ldots,h(k')\}$. Let $N = N_h$ where N_h is the number of indices in $S^{[h]}$. Determine the index i' satisfying

$$\left|\frac{\partial^{N} R(u)}{\partial u_{i'}^{N}}\right|_{u=x^{[h]}}\Bigg|^2 = \max_i \left|\frac{\partial^{N} R(u)}{\partial u_i^{N}}\right|_{u=x^{[h]}}\Bigg|^2,$$

and let $\mathbb{X}^{[h]}$ be the vector

$$\mathbb{X}_i^{[h]} = \left.\frac{\partial^N R(u)}{\partial u_{i'}^{N-1}\,\partial u_i}\right|_{u=x^{[h]}} \qquad i = 1,\ldots,n+1.$$

Letting $\mathbb{X}^{(i)}$, $i = 1,\ldots,\mathscr{D}$ be the vectors $\mathbb{X}^{[h]}$, $h = 1,\ldots,h(k')$, where $\mathbb{X}^{[h]}$ occurs N_h times, we find from the conclusions of Proposition 4.4 and 4.5 that if C in (4.6) is sufficiently small, then $\mathbb{X}^{(i)}$, $i = 1,\ldots,\mathscr{D}$ give ϵ-approximations to the zero lines of F, accounting for their multiplicities.

We assume the computations in Step 7 are carried out as follows. (If $h(k') = 1$, redefine $\alpha' = \beta' = x^{[1]} = 0$.) First compute the coefficients for the three variable polynomials $R(\lambda\alpha'+\rho_1 e_i+\rho_2 e_j+\beta')$, $i,j = 1,\ldots,n+1$, using the method of Section 3. This requires $O\left[n^2\mathscr{D}^3\left\{\frac{1+\sum d_i}{n}\right\}^4\right]$ operations. From these compute the required derivatives. In all, Step 7 requires $O\left[n^2\mathscr{D}^3\left\{\frac{1+\sum d_i}{n}\right\}^4\right]$ operations.

Relying on (4.7), (4.8) and the operation counts already given for each of the steps, the total operation count for the algorithm is

$$O\left\{n\mathscr{D}^4(\log\mathscr{D})(\log\log(1/\epsilon)) + n^2\mathscr{D}^8 + n^2\mathscr{D}^3\left\{\frac{1+\sum d_i}{n}\right\}^4\right\}.$$

5. Proofs

In this section we prove the propositions relied on in the previous section. In the course of doing this we will need to prove several lemmas.

In our calculations we sometimes implicitly use the assumption $\mathcal{D} \geqslant 2$. For example, under this assumption we may write $n\mathcal{D} + n + 1 \leqslant 2n\mathcal{D}$. The following lemma will also occasionally be used implicitly in the analysis.

We retain the notation $\xi^{(\ell)}$ and $H^{(\ell)}$ as in (4.1) and (4.2).

Lemma 5.1: Assume $R(u) \not\equiv 0$ (i.e., is not identically the zero polynomial). Let $\alpha \in \mathbb{C}^{n+1}$. Then $\alpha \in \bigcup_{\ell} H^{(\ell)}$ implies $R(\lambda\alpha+\beta)$ is of degree less than $\mathcal{D}$ for all $\beta \in \mathbb{C}^{n+1}$, and $\alpha \notin \bigcup_{\ell} H^{(\ell)}$ implies $R(\lambda\alpha+\beta)$ is of degree exactly $\mathcal{D}$ for all $\beta \in \mathbb{C}^{n+1}$.

Proof: Follows immediately from the identity $R(\lambda\alpha+\beta) = \prod_{\ell} \xi^{(\ell)} \cdot (\lambda\alpha+\beta)$. □

Recall that $\mu(x) = (1,x,x^2,\ldots,x^n)$.

Lemma 5.2: Let $\mathcal{M}$ be any set of complex hyperplanes M in $\mathbb{C}^{n+1}$. Let N denote the number of hyperplanes in $\mathcal{M}$. For at least one $j'' \in \{0,1,\ldots,nN\}$, $\mu(j'')$ satisfies

$$\|\mu(j'')-x\| \geqslant 1/(1+nN)^{n+1} \qquad \text{for all } x \in M \in \mathcal{M}.$$

Proof: For each $j \in \{0,1,\ldots,nN\}$, let $v(j)$ be a vector of smallest length such that $\mu(j) + v(j)$ lies in a hyperplane in $\mathcal{M}$. Note that for some distinct $j_1,\ldots,j_{n+1}$, each of the $\mu(j_i) + v(j_i)$ must lie in the same hyperplane. Thus, letting A, resp. B, be the matrix with ith row $\mu(j_i)$, resp. $v(j_i)$, we have that A + B is singular. Hence,

$$\min_{\|w\|=1} \|Aw\| \leqslant \max_{\|w\|=1} \|Bw\| \leqslant \sqrt{n+1} \max_{j_i} \|v(j_i)\|.$$

Letting $j'' \in \{j_1,\dots,j_{n+1}\}$ denote an index satisfying $\|v(j'')\| = \max_{j_i} \|v(j_i)\|$, we thus have

$$(5.1) \qquad \|\mu(j'')-x\| \geqslant \frac{1}{\sqrt{n+1}} \min_{\|w\|=1} \|Aw\|, \text{ for all } x \in M \in \mathcal{M}.$$

Note that for any $w \neq 0$, Aw has coordinates equal to the values taken on by the non-zero polynomial of degree at most n, $z \longmapsto \sum_{i=0}^{n} w_{i+1}z^i$, at the n+1 distinct integers j_i. Since this polynomial can have at most n zeros, $Aw \neq 0$ and hence A is invertible.

Finally we note that for each i, $A^{-1}e_i$ gives the coefficients of the degree n polynomial p satisfying $p(j_i) = 1$, $p(j_k) = 0$ if $k \neq i$, that is, the coefficients of $p(z) = \prod_{k\neq i} (z-j_k)/ \prod_{k\neq i} (j_i-j_k)$. Writing $p(z) = \sum a_i z^i$ and noting $\left|\prod_{k\neq i} j_i-j_k\right| \geqslant 1$, we thus have

$$\|A^{-1}e_i\| \leqslant \sum |a_i| \leqslant \sum_{j=0}^{n} \binom{n}{j}(nN)^j = (1+nN)^n.$$

Hence

$$\min_{\|w\|=1} \|Aw\| = \frac{1}{\max_{\|w\|=1}\|A^{-1}w\|} \geqslant \frac{1}{\sqrt{n+1}\ \max_i \|A^{-1}e_i\|} \geqslant \frac{1}{\sqrt{n+1}\ (1+nN)^n}.$$

Together with (5.1) this gives the lemma. □

<u>**Lemma 5.3**</u>: Assume $R(u) \not\equiv 0$. For at least one $j'' \in \{0,1,\dots,n\mathcal{D}\}$, $\alpha'' = \mu(j'')$ has the property that for all i, $R(\lambda\alpha''+e_i)$ is a degree $\mathcal{D}$ polynomial with all zeros λ'' satisfying $|\lambda''| \leqslant (1+n\mathcal{D})^{n+1}$.

<u>**Proof**</u>: Let $\mathcal{M} = \{H^{(\ell)};\ \ell = 1,\dots,\mathcal{D}\}$ and let $j'' \in \{0,1,\dots,n\mathcal{D}\}$ denote an integer such that $\alpha'' = \mu(j'')$ satisfies the conclusion of Lemma 5.2. Then $\alpha'' \notin \bigcup_{\ell} H^{(\ell)}$ and hence, by Lemma 5.1, $R(\lambda\alpha''+e_i)$ is of degree $\mathcal{D}$ for all i. Moreover, for all i and ℓ,

$$\frac{|\xi^{(\ell)}\cdot\alpha''|}{\|\xi^{(\ell)}\|} = \min\{\|x-\alpha''\|;\ x \in H^{(\ell)}\} \geq 1/(1+n\mathcal{D})^{n+1}$$

Hence, if $\lambda''\alpha''+e_i \in H^{(\ell)}$, so that $\xi^{(\ell)}\cdot(\lambda''\alpha''+e_i) = 0$, then

$$|\lambda''| = \frac{|\xi^{(\ell)}\cdot e_i|}{|\xi^{(\ell)}\cdot\alpha''|} \leq (1+n\mathcal{D})^{n+1}. \qquad \square$$

Proposition 5.4: Assume $R(u) \not\equiv 0$. Let α' be as chosen in Step 3 of the algorithm. Then for all ℓ,

$$(5.2) \qquad |\xi^{(\ell)}\cdot\alpha'| = \Omega(\|\xi^{(\ell)}\|/[n\mathcal{D}]^{2n\mathcal{D}}).$$

Moreover, for any $\beta \in \mathbb{C}^{n+1}$, letting $\lambda^{(\ell)},\lambda^{(m)} \in \mathbb{C}$ satisfy $\lambda^{(\ell)}\alpha'+\beta \in H^{(\ell)}$, $\lambda^{(m)}\alpha'+\beta \in H^{(m)}$, we have

$$(5.3) \qquad |\lambda^{(\ell)}| = O(\|\beta\|[n\mathcal{D}]^{2n\mathcal{D}}),$$

$$(5.4) \qquad |\lambda^{(\ell)}-\lambda^{(m)}| = O(\|\beta\|[n\mathcal{D}]^{5n\mathcal{D}}\mathrm{dis}(\xi^{(\ell)},\xi^{(m)})).$$

Proof: For any polynomial $\sum_{k=0}^{d} a_k\lambda^k$, $a_d \neq 0$, with zeros $\lambda_1,\dots,\lambda_d$ we of course have $|a_k/a_d| = |\Sigma\lambda_{i_1}\dots\lambda_{i_k}|$, where the summation is over all tuples $i_1 < i_2 < \dots < i_k$. Hence if $|\lambda_i| \leq R$ for all i, then $|a_k/a_d| \leq \binom{d}{k}R^k$. In particular, letting j" be as in Lemma 5.3, then for j' as in Step 3 of the algorithm

$$(5.5) \qquad \max_{i,k}\left|\frac{a_k(i,j')}{a_{\mathcal{D}}(i,j')}\right| \leq \max_{i,k}\left|\frac{a_k(i,j'')}{a_{\mathcal{D}}(i,j'')}\right| \leq (1+n\mathcal{D})^{(n+1)\mathcal{D}}.$$

For each zero λ' of a polynomial $\sum_{k=0}^{d} a_k\lambda^k$, $a_d \neq 0$, one has the property that $|\lambda'| \leq 1 + \max\{|a_k/a_d|;\ 0 \leq k < d\}$ (cf. Marden (1966), Theorem 27.2). In particular, using (5.5), we find that for each i, every zero λ' of $R(\lambda\alpha'+e_i)$ satisfies

$$(5.6) \qquad |\lambda'| = O([n\mathcal{D}]^{(n+1)\mathcal{D}}).$$

Fix ℓ and assume that $\left|\xi_i^{(\ell)}\right| \geqslant \|\xi^{(\ell)}\|/\sqrt{n+1}$ (this is certainly true for some i). Assume $\lambda^{(\ell)}\alpha'+e_i \in H^{(\ell)}$. Then $|\lambda^{(\ell)}|\ \ |\xi^{(\ell)}\cdot\alpha'| = |\xi^{\ell}\cdot e_i| \geqslant \|\xi^{(\ell)}\|/\sqrt{n+1}$. Thus, using (5.6),

$$|\xi^{(\ell)}\cdot\alpha'| = \Omega(\|\xi^{(\ell)}\|/\sqrt{n}\,[n\mathcal{D}]^{(n+1)\mathcal{D}})$$

from which (5.2) is immediate.

Since $R(\lambda\alpha'+e_i)$ is of degree exactly $\mathcal{D}$ (for any i) by choice of α', Lemma 5.1 implies $R(\lambda\alpha'+\beta)$ is of degree exactly $\mathcal{D}$ for any $\beta \in \mathbb{C}^{n+1}$. Fix β and assume $\lambda^{(\ell)}\alpha'+\beta \in H^{(\ell)}$. Then

$$|\lambda^{(\ell)}|\ \ |\xi^{(\ell)}\cdot\alpha'| = |\xi^{(\ell)}\cdot\beta| \leqslant \|\xi^{(\ell)}\|\ \|\beta\|.$$

Substituting (5.2) into this inequality gives (5.3).

Finally, let $\mathscr{Z}^{(\ell)} = w_1\xi^{(\ell)}$, $\mathscr{Z}^{(m)} = w_2\xi^{(m)}$ $(w_1,w_2 \in \mathbb{C})$ be such that $|\mathscr{Z}^{(\ell)}| = |\mathscr{Z}^{(m)}| = 1$ and $\|\mathscr{Z}^{(\ell)}-\mathscr{Z}^{(m)}\| = \text{dis}(\xi^{(\ell)},\xi^{(m)})$. Then

$$\begin{aligned} 0 &= \mathscr{Z}^{(\ell)}\cdot(\lambda^{(\ell)}\alpha'+\beta) \\ &= (\mathscr{Z}^{(m)}+[\mathscr{Z}^{(\ell)}-\mathscr{Z}^{(m)}])\cdot([\lambda^{(m)}\alpha'+\beta]+[\lambda^{(\ell)}-\lambda^{(m)}]\alpha') \\ &= [(\mathscr{Z}^{(\ell)}-\mathscr{Z}^{(m)})]\cdot[(\lambda^{(m)}\alpha'+\beta)]+[(\lambda^{(\ell)}-\lambda^{(m)})]\mathscr{Z}^{(\ell)}\cdot\alpha'. \end{aligned}$$

However, using (5.3) and $\|\alpha'\| < (n\mathcal{D})^{n+1}$, we have

$$|[(\mathscr{Z}^{(\ell)}-\mathscr{Z}^{(m)})]\cdot[(\lambda^{(m)}\alpha'+\beta)]| = O([n\mathcal{D}]^{3n\mathcal{D}}\|\beta\|\cdot\text{dis}(\xi^{(\ell)},\xi^{(m)})),$$

and by (5.2),

$$|\lambda^{(\ell)}-\lambda^{(m)}|\ \ |\mathscr{Z}^{(\ell)}\cdot\alpha'| = \Omega(|\lambda^{(\ell)}-\lambda^{(m)}|/[n\mathcal{D}]^{2n\mathcal{D}}).$$

Now (5.4) follows. □

The next lemma will be used in proving Proposition 4.3.

<u>Lemma</u> <u>5.5</u>: Assume $R(u) \not\equiv 0$. Let α' be as in Step 3 of the algorithm. For some

$k'' \in \{0,1,\ldots,n\mathscr{D}(\mathscr{D}-1)/2\}$, $\beta'' = \mu(k'')$ has the property that for all ℓ and m, if $\lambda^{(\ell)}\alpha'+\beta'' \in H^{(\ell)}$, $\lambda^{(m)}\alpha'+\beta'' \in H^{(m)}$, then

$$\mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) = O([n\mathscr{D}]^{3n+2}|\lambda^{(\ell)} - \lambda^{(m)}|).$$

<u>**Proof:**</u> For all pairs $\ell < m$, $\ell,m \in \{1,\ldots,\mathscr{D}\}$ such that $H^{(\ell)} \neq H^{(m)}$, let

$$M^{(\ell,m)} = \{\lambda\alpha'+y;\ \lambda \in \mathbb{C},\ y \in H^{(\ell)} \cap H^{(m)}\}.$$

Let $\mathfrak{M} = \{M^{(\ell,m)}\}$. Let $k'' \in \{0,1,\ldots,n\mathscr{D}(\mathscr{D}-1)/2\}$ denote an integer such that $\mu(k'')$ satisfies the conclusion of Lemma 5.2 with this choice of $\mathfrak{M}$. Let $\beta'' = \mu(k'')$.

If $H^{(\ell)} = H^{(m)}$, then the bound on $|\lambda^{(\ell)}-\lambda^{(m)}|$ provided by the lemma is trivial. So assume $H^{(\ell)} \neq H^{(m)}$. By a change of coordinates $x \longmapsto Qx$, where Q is a complex unitary matrix (to preserve distances), and by replacement of $\xi^{(\ell)}$ (resp. $\xi^{(m)},\alpha',\beta''$) with $Q^{-1}\xi^{(\ell)}$ (resp. $Q^{-1}\xi^{(m)},Q\alpha',Q\beta''$) we may assume without loss of generality that $\xi_3^{(\ell)} = 0,\ldots,\xi_{n+1}^{(\ell)} = 0$, $\xi_3^{(m)} = 0,\ldots,\xi_{n+1}^{(m)} = 0$ and

$$H^{(\ell)} \cap H^{(m)} = \{x \in \mathbb{C}^{n+1};\ x_1 = x_2 = 0\}.$$

Let $x = \lambda^{(\ell)}\alpha' + \beta'' \in H^{(\ell)}$. Then by the definition of $M^{(\ell,m)}$ and the choice of β'' (satisfying the conclusion of Lemma 5.2), we must have the distance from x to $H^{(\ell)} \cap H^{(m)}$ bounded below by $1/(1 + n\mathscr{D}^2)^{n+1}$, that is,

$$(|x_1|^2 + |x_2|^2)^{1/2} \geqslant 1/(1 + n\mathscr{D}^2)^{n+1}. \tag{5.7}$$

Let $\mathscr{X}^{(\ell)} = w_1\xi^{(\ell)}$, $\mathscr{X}^{(m)} = w_2\xi^{(m)}$ be such that $\|\mathscr{X}^{(\ell)}\| = \|\mathscr{X}^{(m)}\| = 1$ and $\mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) = \|\mathscr{X}^{(\ell)} - \mathscr{X}^{(m)}\|$. Since $\mathscr{X}^{(\ell)} \cdot x = 0$, $\mathscr{X}^{(m)} \cdot [x + (\lambda^{(m)} - \lambda^{(\ell)})\alpha'] = 0$ and the last $n - 1$ coordinates of both $\mathscr{X}^{(\ell)}$ and $\mathscr{X}^{(m)}$ are zero, we have

$$\begin{bmatrix} \mathscr{X}_1^{(\ell)} & \mathscr{X}_2^{(\ell)} \\ \mathscr{X}_1^{(m)} & \mathscr{X}_2^{(m)} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = (\lambda^{(\ell)} - \lambda^{(m)})(\mathscr{X}^{(m)} \cdot \alpha') \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Solving for x via Cramer's rule and then using (5.7) gives

(5.8)
$$\frac{|\lambda^{(\ell)} - \lambda^{(m)}|\ |\mathscr{Z}^{(m)} \cdot \alpha'|}{|\mathscr{Z}_1^{(\ell)}\mathscr{Z}_2^{(m)} - \mathscr{Z}_2^{(\ell)}\mathscr{Z}_1^{(m)}|} \geqslant \frac{1}{(1 + n\mathscr{D}^2)^{n+1}} .$$

Noting that $\{\omega(-\bar{\mathscr{Z}}_2^{(m)}, \bar{\mathscr{Z}}_1^{(m)});\ \omega \in \mathbb{C}\}$ is the orthogonal complement of $\{\omega(\mathscr{Z}_1^{(m)}, \mathscr{Z}_2^{(m)});\ \omega \in \mathbb{C}\}$ when considered as subspaces of $\mathbb{R}^4$, we have

$$(\mathscr{Z}_1^{(\ell)}, \mathscr{Z}_2^{(\ell)}) = v(\mathscr{Z}_1^{(m)}, \mathscr{Z}_2^{(m)}) + w(-\bar{\mathscr{Z}}_2^{(m)}, \bar{\mathscr{Z}}_1^{(m)})$$

where $v \geqslant 0$, $w \in \mathbb{C}$ and $v^2 + |w|^2 = 1$. (In stating $v \geqslant 0$ we are using the fact that $\|\mathscr{Z}^{(\ell)} - \mathscr{Z}^{(m)}\| = \mathrm{dis}(\mathscr{Z}^{(\ell)}, \mathscr{Z}^{(m)})$.) Substituting for $\mathscr{Z}^{(\ell)}$ in the denominator of (5.8) gives

(5.9)
$$\frac{|\lambda^{(\ell)} - \lambda^{(m)}|\ |\mathscr{Z}^{(m)} \cdot \alpha'|}{|w|} \geqslant \frac{1}{(1 + n\mathscr{D}^2)^{n+1}} .$$

Observe that

$$\mathrm{dis}^2(\xi^{(\ell)}, \xi^{(m)}) = \|\mathscr{Z}^{(\ell)} - \mathscr{Z}^{(m)}\|^2 = (1 - v)^2 + |w|^2 \leqslant 2|w|^2,$$

where the inequality follows from $v^2 + |w|^2 = 1$ and $v \geqslant 0$. Substituting for $|w|$ in (5.9) and using $|\mathscr{Z}^{(m)} \cdot \alpha'| \leqslant \|\alpha'\| \leqslant \sqrt{n+1}(n\mathscr{D})^n$ gives the proposition. □

We can now give the proof of Proposition 4.3, which relies on the notation introduced just prior to that proposition. For the reader's convenience, we restate the proposition as

Proposition 5.6: For all $\delta = \Omega([n\mathscr{D}]^{10n\mathscr{D}})$ and for ϵ'' as given at the end of Step 5,

(5.10)
$$\gamma^{(\ell)} \in P^{[h]} \Rightarrow |\xi^{(\ell)} \cdot x^{[h]}| = O(\epsilon''[n\mathscr{D}]^{n+1}\|\xi^{(\ell)}\|),$$

(5.11)
$$\gamma^{(\ell)} \notin P^{[h]} \Rightarrow |\xi^{(\ell)} \cdot x^{[h]}| = O(\delta\epsilon''\|\xi^{(\ell)}\|/[n\mathscr{D}]^{2n\mathscr{D}}),$$

(5.12)
$$\gamma^{(\ell)}, \gamma^{(m)} \in P^{[h]} \Rightarrow \mathrm{dis}(\xi^{(\ell)}, \xi^{(m)}) = O(\epsilon''[n\mathscr{D}]^{3n+2}).$$

<u>**Proof:**</u> We begin by recalling that for each $k = 0,1,\ldots,\mathcal{D}(\mathcal{D} - 1)/2$, Step 5 partitions the approximations $\gamma_i(k)$ into "clusters" $P^{[h]}(k)$, $h = 1,\ldots,h(k)$ where

$$(5.13) \qquad \gamma_i(k),\gamma_j(k) \in P^{[h]}(k) \Rightarrow |\gamma_i(k) - \gamma_j(k)| \leqslant \epsilon'',$$

$$(5.14) \qquad \gamma_i(k) \in P^{[h]}(k),\ \gamma_j(k) \notin P^{[h]}(k) \Rightarrow |\gamma_i(k) - \gamma_j(k)| > \delta\epsilon''.$$

To prove (5.10), note that since $x^{[h]} = \gamma^{(m)}\alpha'+\beta'$ for some $\gamma^{(m)} \in P^{[h]}$ where $\gamma^{(m)}$ approximates $\lambda^{(\ell)}$ within distance ϵ', we have

$$|\xi^{(\ell)}\cdot x^{[h]}| \leqslant |\xi^{(\ell)}\cdot(\gamma^{(m)}-\gamma^{(\ell)})\alpha'| + |\xi^{(\ell)}\cdot(\gamma^{(\ell)}-\lambda^{(\ell)})\alpha'| + |\xi^{(\ell)}\cdot(\lambda^{(\ell)}\alpha'+\beta')|$$

$$\leqslant (\epsilon''+\epsilon')\ \|\xi^{(\ell)}\|\ \|\alpha'\| + 0 \qquad \text{(using (5.13))}.$$

Since $\epsilon' \leqslant \epsilon''$ by the construction of Step 5 and $\|\alpha'\| < (n\mathcal{D})^{n+1}$, (5.10) follows.

Now we prove (5.11). Again assume $x^{[h]} = \gamma^{(m)}\alpha'+\beta'$, but now assume $\gamma^{(\ell)} \notin P^{[h]}$. Then $|\gamma^{(m)}-\gamma^{(\ell)}| > \delta\epsilon''$ by (5.14). Using this and (5.2) along with $|\gamma^{(\ell)}-\lambda^{(\ell)}| \leqslant \epsilon'$ and $\|\alpha'\| < (n\mathcal{D})^{n+1}$, we have

$$|\xi^{(\ell)}\cdot x^{[h]}| = |\xi^{(\ell)}\cdot x^{[h]}| + |\xi^{(\ell)}\cdot(\lambda^{(\ell)}\alpha' + \beta')| = |\xi^{(\ell)}\cdot(\gamma^{(m)}-\lambda^{(\ell)})\alpha'|$$
$$\geqslant |\xi^{(\ell)}\cdot(\gamma^{(m)}-\gamma^{(\ell)})\alpha'| - |\xi^{(\ell)}\cdot(\gamma^{(\ell)}-\lambda^{(\ell)})\alpha'|$$
$$= \Omega(\delta\epsilon''\|\xi^{(\ell)}\|/[n\mathcal{D}]^{2n\mathcal{D}}) - 0(\epsilon'\|\xi^{(\ell)}\|(n\mathcal{D})^{n+1}).$$

Assuming $\delta = \Omega([n\mathcal{D}]^{3n\mathcal{D}})$ and using $\epsilon'' \geqslant \epsilon'$, (5.11) follows.

Now we turn to proving (5.12). Let β'' be as in Lemma 5.5. Let $P^{[j]}(k'')$, $j = 1,\ldots,h(k'')$ be the sets determined for β'' at the end of Step 5. Assuming $\lambda^{(\ell)}(k'') \in \mathbb{C}$ satisfies $\lambda^{(\ell)}(k'')\alpha'+\beta'' \in H^{(\ell)}$, let $\gamma^{(\ell)}(k'')$ denote the ϵ'-approximation to $\lambda^{(\ell)}(k'')$ obtained in Step 4. We will show that if $\gamma^{(\ell)}(k''),\gamma^{(m)}(k'') \in P^{[j]}(k'')$ for some j, then $\gamma^{(\ell)},\gamma^{(m)} \in P^{[h]}$ for some h. However, since the union $\bigcup_j P^{[j]}(k'')$ contains the same number of elements as the disjoint union $\bigcup_h P^{[h]}$, and since $h(k') \geqslant h(k'')$ by choice of β'', it follows that the converse is also true, that is, if $\gamma^{(\ell)},\gamma^{(m)} \in P^{[h]}$ for some h, then $\gamma^{(\ell)}(k''),\gamma^{(m)}(k'') \in P^{[j]}(k'')$ for some j. Then $|\gamma^{(\ell)}(k'')-\gamma^{(m)}(k'')| \leqslant \epsilon''$

by (5.13) and hence $|\lambda^{(\ell)}(k'')-\lambda^{(m)}(k'')| \leqslant 2\epsilon'+\epsilon''$. Thus, since $\mathcal{B}''$ satisfies the conclusion of Lemma 5.5,

$$\mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) = O(\epsilon''[n\mathcal{D}]^{3n+2}),$$

establishing (5.12).

Finally, we prove that if $\gamma^{(\ell)}(k''),\gamma^{(m)}(k'') \in P^{[j]}(k'')$ for some j, then $\gamma^{(\ell)},\gamma^{(m)} \in P^{[h]}$ for some h. Assume otherwise. Then $|\gamma^{(\ell)}-\gamma^{(m)}| > \delta\epsilon''$ by (5.14) and hence $|\lambda^{(\ell)}-\lambda^{(m)}| > \delta\epsilon'' - 2\epsilon'$. Assuming $\delta \geqslant 3$ and thus $\delta\epsilon'' - 2\epsilon' \geqslant \delta\epsilon''/3$, and using $\|\mathcal{B}''\| < (n\mathcal{D}^2)^n$, we conclude from (5.4) that

$$\mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) = \Omega(\delta\epsilon''/[n\mathcal{D}]^{7n\mathcal{D}}). \tag{5.15}$$

However, since $\gamma^{(\ell)}(k''),\gamma^{(m)}(k'') \in P^{[j]}(k'')$, we have that $|\lambda^{(\ell)}(k'')-\lambda^{(m)}(k'')| \leqslant 2\epsilon' + \epsilon''$, and hence, since the conclusion of Lemma 5.5 holds for $\mathcal{B}''$,

$$\mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) = O(\epsilon''[n\mathcal{D}]^{3n+2}). \tag{5.16}$$

But for $\delta = \Omega([n\mathcal{D}]^{10n\mathcal{D}})$, (5.15) and (5.16) contradict one another, concluding the proof of the proposition. □

Finally, we turn to proving Propositions 4.4 and 4.5. We begin with a lemma.

<u>**Lemma 5.7**</u>: Fix $\xi^{(m)}$ and assume $\xi_i^{(m)} \neq 0$. If $\mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) \leqslant |\xi_i^{(m)}|/2\|\xi^{(m)}\|$, then

$$\frac{|\xi_i^{(\ell)}|}{\|\xi^{(\ell)}\|} \geqslant \frac{|\xi_i^{(m)}|}{2\|\xi^{(m)}\|}, \tag{5.17}$$

$$\left\|\frac{\xi^{(\ell)}}{\xi_i^{(\ell)}} - \frac{\xi^{(m)}}{\xi_i^{(m)}}\right\| \leqslant \frac{4\|\xi^{(m)}\|^2\cdot\mathrm{dis}(\xi^{(\ell)},\xi^{(m)})}{|\xi_i^{(m)}|^2}. \tag{5.18}$$

<u>**Proof**</u>: Assume $\mathcal{X}^{(\ell)} = w_1\xi^{(\ell)}$, $\mathcal{X}^{(m)} = w_2\xi^{(m)}$ satisfy $\|\mathcal{X}^{(\ell)}\| = \|\mathcal{X}^{(m)}\| = 1$ and

$\mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) = \|\mathcal{Z}^{(\ell)} - \mathcal{Z}^{(m)}\|$. Since $\mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) \leqslant |\mathcal{Z}_i^{(m)}|/2$, it is easily shown that $|\mathcal{Z}_i^{(\ell)}| \geqslant |\mathcal{Z}_i^{(m)}|/2$, and hence (5.17).

Note that

$$\begin{aligned}
\left\|\frac{\xi^{(\ell)}}{\xi_i^{(\ell)}} - \frac{\xi^{(m)}}{\xi_i^{(m)}}\right\| &= \left\|\frac{\mathcal{Z}^{(\ell)}}{\mathcal{Z}_i^{(\ell)}} - \frac{\mathcal{Z}^{(m)}}{\mathcal{Z}_i^{(m)}}\right\| \\
&= \left\|\frac{\mathcal{Z}^{(\ell)}}{\mathcal{Z}_i^{(\ell)}} - \frac{\mathcal{Z}^{(m)}}{\mathcal{Z}_i^{(\ell)}} + \left(\frac{\mathcal{Z}_i^{(m)} - \mathcal{Z}_i^{(\ell)}}{\mathcal{Z}_i^{(\ell)}\mathcal{Z}_i^{(m)}}\right)\mathcal{Z}^{(m)}\right\| \\
&\leqslant \frac{1}{|\mathcal{Z}_i^{(\ell)}|}\left[\mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) + \left(\frac{\mathrm{dis}(\xi^{(\ell)},\xi^{(m)})}{|\mathcal{Z}_i^{(m)}|}\right)\right].
\end{aligned}$$

However, $2|\mathcal{Z}_i^{(\ell)}| \geqslant |\mathcal{Z}_i^{(m)}| = |\xi_i^{(m)}|/\|\xi^{(m)}\|$. Now (5.18) follows. □

Here is Proposition 4.4 restated as

Proposition 5.8: Assume that for all $\ell, m \in \{1,\ldots,\mathcal{D}\}$ we have that $\mathrm{dis}(\xi^{(\ell)},\xi^{(m)}) \leqslant \epsilon'''$. For all $\epsilon''' = O(1/\sqrt{n})$, the following is then true. Let i' be an index satisfying

$$\left|\left.\frac{\partial^{\mathcal{D}}R(u)}{\partial u_{i'}^{\mathcal{D}}}\right|_{u=0}\right| = \max_i\left|\left.\frac{\partial^{\mathcal{D}}R(u)}{\partial u_i^{\mathcal{D}}}\right|_{u=0}\right|$$

and let $\mathbb{X} \in \mathbb{C}^{n+1}$ be the vector

$$\mathbb{X}_i = \left.\frac{\partial^{\mathcal{D}}R(u)}{\partial u_{i'}^{\mathcal{D}-1}\partial u_i}\right|_{u=0} \qquad i = 1,\ldots,n+1.$$

Then $\mathrm{dis}(\mathbb{X},\xi^{(\ell)}) = O(n\epsilon''')$ for all ℓ.

Proof: Fix $m \in \{1,\ldots,\mathcal{D}\}$ and let i" denote an index satisfying $|\xi_{i''}^{(m)}| \geqslant \|\xi^{(m)}\|/\sqrt{n+1}$. Then, by (5.17), assuming $\epsilon''' \leqslant 1/2\sqrt{n+1}$, we have that $|\xi_{i''}^{(\ell)}| \geqslant \|\xi^{(\ell)}\|/2\sqrt{n+1}$ for all $\ell \in \{1,\ldots,\mathcal{D}\}$.

Next, note that by definition of i' and using $R(u) = \prod_{\ell}(\xi^{(\ell)}\cdot u)$,

$$\mathcal{D}!\left|\prod_{\ell}\xi_{i'}^{(\ell)}\right| = \left|\left.\left|\frac{\partial^{\mathcal{D}}R(u)}{\partial u_{i'}^{\mathcal{D}}}\right|\right._{u=0}\right| \geqslant \left|\left.\left|\frac{\partial^{\mathcal{D}}R(u)}{\partial u_{i''}^{\mathcal{D}}}\right|\right._{u=0}\right| = \mathcal{D}!\left|\prod_{\ell}\xi_{i''}^{(\ell)}\right|.$$

Hence, for at least one $k \in \{1,\ldots,\mathcal{D}\}$, we have that $|\xi_{i'}^{(k)}| \geqslant |\xi_{i''}^{(k)}|$. Since $|\xi_{i''}^{(k)}| \geqslant \|\xi^{(k)}\|/2\sqrt{n+1}$, we thus have $|\xi_{i'}^{(k)}| \geqslant \|\xi^{(k)}\|/2\sqrt{n+1}$. It thus follows from (5.17) that if $\epsilon''' \leqslant 1/4\sqrt{n+1}$, then

$$|\xi_{i'}^{(\ell)}| \geqslant \|\xi^{(\ell)}\|/4\sqrt{n+1} \quad \text{for all } \ell. \tag{5.19}$$

Consider the identity

$$\left.\frac{\partial^{\mathcal{D}}R(u)}{\partial u_{i'}^{\mathcal{D}-1}\partial u_{i}}\right|_{u=0} = (\mathcal{D}-1)!\sum_{\ell}\left[\xi_{i}^{(\ell)}\prod_{m\neq\ell}\xi_{i'}^{(m)}\right].$$

Defining $\mathbb{X}$ as in the statement of the proposition, we thus have

$$\frac{\mathbb{X}}{\prod_{\ell}\xi_{i'}^{(\ell)}} = (\mathcal{D}-1)!\sum_{\ell}\frac{\xi^{(\ell)}}{\xi_{i'}^{(\ell)}}. \tag{5.20}$$

However, using (5.18) and (5.19), if $\epsilon''' \leqslant 1/8\sqrt{n+1}$ we have that for any m,

$$\left\|\mathcal{D}\frac{\xi^{(m)}}{\xi_{i'}^{(m)}} - \sum_{\ell}\frac{\xi^{(\ell)}}{\xi_{i'}^{(\ell)}}\right\| \leqslant 64(\mathcal{D}-1)(n+1)\epsilon'''.$$

Hence, for any m, (5.20) gives

$$\left\|\frac{\mathbb{X}}{\prod_{\ell}\xi_{i'}^{(\ell)}} - \mathcal{D}!\frac{\xi^{(m)}}{\xi_{i'}^{(m)}}\right\| \leqslant 64(\mathcal{D}!)(n+1)\epsilon'''.$$

Since $\|\xi^{(m)}\|/|\xi_{i'}^{(m)}| \geqslant 1$, it follows that $\mathrm{dis}(\mathbb{X},\xi^{(m)}) = O(n\epsilon''')$. □

Finally, we prove Proposition 4.5 restated as

<u>**Proposition 5.9:**</u> Let $S \subset \{1,\ldots,\mathcal{D}\}$ contain N elements, where $0 < N < \mathcal{D}$. Assume

that for all $\ell, m \in S$, we have $\mathrm{dis}(\xi^{(\ell)}, \xi^{(m)}) \leqslant \epsilon'''$. Let $x \in \mathbb{C}^{n+1}$, $x \neq 0$. Assume that if $\ell \in S$, then $|\xi^{(\ell)} \cdot x| \leqslant \rho_1 \|\xi^{(\ell)}\| \, \|x\|$, and assume that if $\ell \notin S$, then $|\xi^{(\ell)} \cdot x| \geqslant \rho_2 \|\xi^{(\ell)}\| \, \|x\|$ where $\rho_2 > 0$. Then for all $\epsilon''' = O(1/\sqrt{n})$ and for all $\rho_1/\rho_2 = O(\epsilon'''/\mathcal{D}!n)$, the following is true. Let i' be an index satisfying

$$\left| \left. \frac{\partial^N R(u)}{\partial u_{i'}^N} \right|_{u=x} \right| = \max_i \left| \left. \frac{\partial^N R(u)}{\partial u_i^N} \right|_{u=x} \right|,$$

and let $\mathbb{X} \in \mathbb{C}^{n+1}$ be the vector

$$\mathbb{X}_i = \left. \frac{\partial^N R(u)}{\partial u_{i'}^{N-1} \partial u_i} \right|_{u=x} \qquad i = 1,\ldots,n+1.$$

Then $\mathrm{dis}(\mathbb{X}, \xi^{(\ell)}) = O(n\mathcal{D}\epsilon''')$ for all $\ell \in S$.

__Proof__: The proof is analogous to, but much more complicated than, the proof of Proposition 5.8.

We begin by showing that if ϵ''' and ρ_1/ρ_2 are as small as certain prescribed quantities, then $|\xi_{i'}^{(\ell)}| \geqslant \|\xi^{(\ell)}\|/8\sqrt{n+1}$ for all $\ell \in S$.

Fix $m \in S$ and let i" denote an index satisfying $|\xi_{i''}^{(m)}| \geqslant \|\xi^{(m)}\|/\sqrt{n+1}$. Then, by (5.17), if $\epsilon''' \leqslant 1/2\sqrt{n+1}$ we have that

$$\left|\xi_{i''}^{(\ell)}\right| \geqslant \|\xi^{(\ell)}\|/2\sqrt{n+1} \qquad \text{for all } \ell \in S.$$

Consider the identity

$$\left. \frac{d^N R}{du_{i''}^N} \right|_{u=x} = \Sigma \left[\prod_{\ell \in L} \xi_{i''}^{(\ell)} \right] \left[\prod_{\ell \notin L} \xi^{(\ell)} \cdot x \right] \tag{5.21}$$

where the summation is over all ordered N-tuples $(\ell_1,\ldots,\ell_N)$ of distinct indices from $\{1,\ldots,\mathcal{D}\}$, and where $\ell \in L$ is used to denote $\ell \in \{\ell_1,\ldots,\ell_N\}$. Let Σ^* denote summation over the N! N-tuples with $\ell_1,\ldots,\ell_N \in S$, and let Σ^{**} denote summation over the remaining tuples. Then from (5.21)

$$\frac{1}{\left[\prod_{\ell\in S}\xi^{(\ell)}_{i''}\right]\left[\prod_{\ell\notin S}\xi^{(\ell)}\cdot x\right]}\cdot\frac{d^N R}{du^N_{i''}}\bigg|_{u=x} \tag{5.22}$$

$$= N! + \sum^{**}\left[\prod_{\ell\in S\setminus L}\frac{\xi^{(\ell)}\cdot x}{\xi^{(\ell)}_{i''}}\right]\left[\prod_{\ell\in L\setminus S}\frac{\xi^{(\ell)}_{i''}}{\xi^{(\ell)}\cdot x}\right].$$

Note that (i) $|\xi^{(\ell)}\cdot x/\xi^{(\ell)}_{i''}| \leqslant 2\rho_1\sqrt{n+1}\|x\|$ for all $\ell \in S$ since $|\xi^{(\ell)}_{i''}| \geqslant \|\xi^{(\ell)}\|/2\sqrt{n+1}$ for all $\ell \in S$; (ii) $|\xi^{(\ell)}_{i''}/\xi^{(\ell)}\cdot x| \leqslant 1/\rho_2\|x\|$ for all $\ell \notin S$; (iii) $L\setminus S$ and $S\setminus L$ have the same number of elements; (iv) at least one $\ell \in S$ satisfies $\ell \notin L$ for each of the tuples defining $\sum^{**}$; (v) $\sum^{**}$ is a summand over fewer than $\mathcal{D}!$ N-tuples; and (vi)

$$\left|\frac{d^N R}{du^N_{i'}}\bigg|_{u=x}\right| \geqslant \left|\frac{d^N R}{du^N_{i''}}\bigg|_{u=x}\right|$$

by choice of i'. Assuming $\rho_1 \leqslant \rho_2/8\sqrt{n+1}\mathcal{D}!$, it then follows from (5.22) that

$$\left|\frac{1}{\left[\prod_{\ell\in S}\xi^{(\ell)}_{i''}\right]\left[\prod_{\ell\notin S}\xi^{(\ell)}\cdot x\right]}\cdot\frac{d^N R}{du^N_{i'}}\bigg|_{u=x}\right| \geqslant N! - \frac{1}{4}.$$

Relying on the identity (5.21) with i' replacing i", this becomes

$$\left|\sum^{*}\left[\prod_{\ell\in S}\frac{\xi^{(\ell)}_{i'}}{\xi^{(\ell)}_{i''}}\right]\right. \tag{5.23}$$

$$\left. + \sum^{**}\left[\prod_{\ell\in S\cap L}\frac{\xi^{(\ell)}_{i'}}{\xi^{(\ell)}_{i''}}\right]\left[\prod_{\ell\in S\setminus L}\frac{\xi^{(\ell)}\cdot x}{\xi^{(\ell)}_{i''}}\right]\left[\prod_{\ell\in L\setminus S}\frac{\xi^{(\ell)}_{i'}}{\xi^{(\ell)}\cdot x}\right]\right| \geqslant N! - \frac{1}{4}.$$

Making use of the above observations (i)-(v) with i' replacing i" in (ii), as well as $|\xi^{(\ell)}_{i'}/\xi^{(\ell)}_{i''}| \leqslant 2\sqrt{n+1}$ for all $\ell \in S$ (since $|\xi^{(\ell)}_{i''}| \geqslant \|\xi^{(\ell)}\|/2\sqrt{n+1}$ for all $\ell \in S$), and assuming that $\rho_1 \leqslant \rho_2/4(2\sqrt{n+1})^N\mathcal{D}!$, it follows from (5.23) that

$$N! \left| \prod_{\ell \in S} \frac{\xi_{i'}^{(\ell)}}{\xi_{i''}^{(\ell)}} \right| \geqslant N! - \frac{1}{2}.$$

Hence, for at least one $m \in S$ we must have $\left|\xi_{i'}^{(m)}\right| \geqslant \left|\xi_{i''}^{(m)}\right|/2$. Since $\left|\xi_{i''}^{(m)}\right| \geqslant \|\xi^{(m)}\|/2\sqrt{n+1}$, it now follows from (5.17) that if $\epsilon''' < 1/8\sqrt{n+1}$, then

$$\left|\xi_{i'}^{(\ell)}\right| \geqslant \|\xi^{(\ell)}\|/8\sqrt{n+1} \qquad \text{for all } \ell \in S. \tag{5.24}$$

Consider the identity, for any i,

$$\begin{aligned} &\frac{1}{\left[\prod_{\ell \in S} \xi_{i'}^{(\ell)}\right]\left[\prod_{\ell \notin S} \xi^{(\ell)} \cdot x\right]} \left.\frac{d^N R}{du_{i'}^{N-1} du_i}\right|_{u=x} = (N-1)! \sum_{\ell \in S} \frac{\xi_i^{(\ell)}}{\xi_{i'}^{(\ell)}} \\ &\qquad + \sum\nolimits^{**} \left[\prod_{\ell \in S \setminus L} \frac{\xi^{(\ell)} \cdot x}{\xi_{i'}^{(\ell)}}\right]\left[\prod_{\ell \in L^{\square} \setminus S} \frac{\xi_{i'}^{(\ell)}}{\xi^{(\ell)} \cdot x}\right] \cdot g(x,\ell_N), \end{aligned} \tag{5.25}$$

where $L^{\square} = \{\ell_1,\ldots,\ell_{N-1}\}$ and

$$g(x,\ell_N) = \begin{cases} \xi_i^{(\ell_N)}/\xi_{i'}^{(\ell_N)} & \text{if } \ell_N \in S \\ \xi_i^{(\ell_N)}/\xi^{(\ell_N)} \cdot x & \text{if } \ell_N \notin S. \end{cases}$$

Making use of the above observations (iii)–(v) and (5.23), we find from (5.25) that if $\rho_1/\rho_2 \leqslant \epsilon'''/8\sqrt{n+1}$, then for $\mathbb{X}$ as defined in the statement of the proposition, we have

$$\left\| \frac{\mathbb{X}}{\left[\prod_{\ell \in S} \xi_{i'}^{(\ell)}\right]\left[\prod_{\ell \notin S} \xi^{(\ell)} \cdot x\right]} - (N-1)! \sum_{\ell \in S} \frac{\xi^{(\ell)}}{\xi_{i'}^{(\ell)}} \right\| \leqslant \epsilon'''. \tag{5.26}$$

However, using (5.18) and (5.24), if $\epsilon''' \leqslant 1/16\sqrt{n+1}$ we have that for any $m \in S$,

$$\left|\left|\frac{N}{\xi_{i'}^{(m)}}\xi^{(m)} - \sum_{\ell\in S}\frac{\xi^{(\ell)}}{\xi_{i'}^{(\ell)}}\right|\right| \leqslant 256(N-1)(n+1)\epsilon'''.$$

Hence, for any $m \in S$, (5.26) gives

$$\left|\left|\frac{\mathbb{X}}{\left[\prod_{\ell\in S}\xi_{i'}^{(\ell)}\right]\left[\prod_{\ell\notin S}\xi^{(\ell)}\cdot x\right]} - \frac{N!\,\xi^{(m)}}{\xi_{i'}^{(m)}}\right|\right| \leqslant \epsilon''' + 16(N-1)(n+1)\epsilon'''.$$

Since $\|\xi^{(m)}\|/|\xi_{i'}^{(m)}| \geqslant 1$, the proposition follows. □

6. Appendix

Here we prove the claim (1.1). Let $\epsilon' = \epsilon/4(R+1)^2$, $0 < \epsilon \leqslant R$, and assume that $\mathbb{X}^{(i)}$, $i = 1,\ldots,\mathscr{D}$ are ϵ'-approximations to all of the zero lines of F. In the notation of section 1, $\|\mathbb{X}^{(i)}/\|\mathbb{X}^{(i)}\| - \xi^{(i)}/\|\xi^{(i)}\|\| \leqslant \epsilon'$ where the zero lines of F are precisely the lines $\{\lambda\xi^{(i)};\ \lambda \in \mathbb{C}\}$.

For each $\xi^{(i)}$ such that $\xi^{(i)}_{n+1} \neq 0$, let

$$\tilde{\xi}^{(i)} = \left[\frac{\xi^{(i)}_1}{\xi^{(i)}_{n+1}},\ldots,\frac{\xi^{(i)}_n}{\xi^{(i)}_{n+1}}\right].$$

Then $\tilde{\xi}^{(i)}$ is the zero of f corresponding to the solution line $\{\lambda\xi^{(i)};\ \lambda \in \mathbb{C}\}$ of F. Define $\tilde{\mathbb{X}}^{(i)}$ analogously.

We show that

$$\|\tilde{\xi}^{(i)}\| \leqslant R \Rightarrow \frac{|\mathbb{X}^{(i)}_{n+1}|}{\|\mathbb{X}^{(i)}\|} \geqslant \frac{3}{4(R+1)}, \tag{6.1}$$

and

$$\frac{|\mathbb{X}^{(i)}_{n+1}|}{\|\mathbb{X}^{(i)}\|} \geqslant \frac{3}{4(R+1)} \Rightarrow \|\tilde{\mathbb{X}}^{(i)} - \tilde{\xi}^{(i)}\| \leqslant \epsilon. \tag{6.2}$$

Together, (6.1) and (6.2) imply that the points $\{\tilde{\mathbb{X}}^{(i)};\ |\mathbb{X}^{(i)}_{n+1}|/\|\mathbb{X}^{(i)}\| \geqslant 3/4(R+1)\}$ are a solution for the (ϵ,R)-approximation problem for f.

To prove (6.1), first note that $\|\tilde{\xi}^{(i)}\| \leqslant R$ if and only if $\|\xi^{(i)}\|^2 \leqslant (R^2+1)|\xi^{(i)}_{n+1}|^2$. Thus, if $\|\tilde{\xi}^{(i)}\| \leqslant R$, then

$$\frac{|\mathbb{X}^{(i)}_{n+1}|}{\|\mathbb{X}^{(i)}\|} \geqslant \frac{|\xi^{(i)}_{n+1}|}{\|\xi^{(i)}\|} - \epsilon' \geqslant \left[1 - \frac{\epsilon}{4(R+1)}\right]\frac{1}{R+1} \geqslant \frac{3}{4(R+1)}.$$

In proving (6.2), let $\hat{\mathbb{X}}^{(i)} = \mathbb{X}^{(i)}/\|\mathbb{X}^{(i)}\|$ and $\hat{\xi}^{(i)} = \xi^{(i)}/\|\xi^{(i)}\|$. Then, assuming that $\hat{\mathbb{X}}^{(i)}_{n+1} \geqslant 3/4(R+1)$, we have

$$\|\tilde{\mathbb{X}}^{(i)} - \tilde{\xi}^{(i)}\| = \left\| \frac{\hat{\mathbb{X}}^{(i)}}{\hat{\mathbb{X}}^{(i)}_{n+1}} - \frac{\hat{\xi}^{(i)}}{\hat{\xi}^{(i)}_{n+1}} \right\| = \frac{1}{|\hat{\mathbb{X}}^{(i)}_{n+1}|} \left\| \hat{\mathbb{X}}^{(i)} - \frac{\hat{\mathbb{X}}^{(i)}_{n+1}}{\hat{\xi}^{(i)}_{n+1}} \hat{\xi}^{(i)} \right\|$$

$$\leqslant \frac{1}{|\hat{\mathbb{X}}^{(i)}_{n+1}|} \left[\|\hat{\mathbb{X}}^{(i)} - \hat{\xi}^{(i)}\| + \frac{|\hat{\mathbb{X}}^{(i)}_{n+1} - \hat{\xi}^{(i)}_{n+1}|}{|\hat{\xi}^{(i)}_{n+1}|} \right]$$

$$\leqslant \frac{4}{3}(R+1) \left[\epsilon' + \frac{\epsilon'}{\frac{3}{4(R+1)} - \epsilon'} \right]$$

$$\leqslant \frac{4}{3}(R+1) \left[\epsilon' + 2(R+1)\epsilon' \right] \quad \text{(by substituting } \epsilon' = \epsilon/4(R+1)^2 < 1/4(R+1) \text{ in the denominator)}$$

$$< 4(R+1)^2 \epsilon' = \epsilon.$$

Hence, (6.2) is proven.

7. References

Borodin, A. and Munro, I., (1975), "The Computational Complexity of Algebraic and Numeric Problems," American Elsevier.

Canny, J., (1987), A new algebraic method for robot motion planning and real geometry, Proc. 28th IEEE Sump. FOCS, Los Angeles, 39-48.

Chistov, A.L. and Grigor'ev, D.Y., (1983), Subexponential time solving systems of algebraic equations, I and II, LOMI preprints E-9-83, E-10-83, Leningrad.

Chistov, A.L. and Grigor'ev, D.Y., (1984), Complexity of quantifier elimination in the theory of algebraically closed fields, *Lecture Notes in Computer Science*, 176, Springer Verlag.

Grigor'ev, D.Y. and Vorobjov, N.N., (1986), Solving systems of polynomial inequalities in subexponential time. To appear in a 1988 issue of the *Journal of Symbolic Computation*.

Lazard, D., (1981), Résolution des systèmes d'équations algébriques, *Theor. Comp. Sci.* (15) 1, 77-110.

Marden, M., (1966), "Geometry of Polynomials," Amer. Math. Soc., Providence.

Macaulay, F.S., (1902), Some Formulae in Elimination, *Proc. London Math. Soc.* (1) 35, 3-27.

Renegar, J., (1987a), On the Efficiency of Newton's Method in Approximating All Zeros of a System of Complex Polynomials, *Math. Op. Res.* (12) 1, 121-148.

Renegar, J., (1987b), On the Worst-Case Arithmetic Complexity of Approximating Zeros of Polynomials, *Jour. of Complexity* (3) 90-113.

Van der Waerden, B.L., (1950), "Modern Algebra", Volume 2, (English Translation), Frederick Ungar Publishing Co., New York.