POLAR VARIETIES AND EFFICIENT REAL ELIMINATION

B. BANK, M. GIUSTI, J. HEINTZ, AND G. M. MBAKOP

Dedicated to Steve Smale

Abstract. Let S_0 be a smooth and compact real variety given by a reduced regular sequence of polynomials $f_1, \dots, f_p$. This paper is devoted to the algorithmic problem of finding *efficiently* a representative point for each connected component of S_0 . For this purpose we exhibit explicit polynomial equations that describe the generic polar varieties of S_0. This leads to a procedure which solves our algorithmic problem in time that is polynomial in the (extrinsic) description length of the input equations $f_1, \dots, f_p$ and in a suitably introduced, intrinsic geometric parameter, called the *degree* of the real interpretation of the given equation system $f_1, \dots, f_p$.

Keywords: Real polynomial equation solving, polar variety, geometric degree, arithmetic circuit, arithmetic network, complexity.

1. Introduction

The core of this paper consists in the exhibition of a system of canonical equations which describe locally the generic polar varieties of a given semialgebraic complete intersection manifold S_0 contained in the real n–dimensional affine space $\mathbb{R}^n$. This purely mathematical description of the polar varieties allows the design of a new type of efficient algorithm (with intrinsic complexity bounds), which computes, in case that S_0 is smooth and compact, at least one representative point for each connected component of S_0 (the algorithm returns each such point in a suitable symbolic codification). This new algorithm (and, in particular, its complexity) is the main practical outcome of the present paper. Let us now briefly describe our results.

Suppose that the real variety S_0 is compact and given by polynomial equations of the following form:

$$f_1(X_1, \dots, X_n) = \cdots = f_p(X_1, \dots, X_n) = 0,$$

where $p, n \in \mathbb{N}$, $p \leq n$ and $f_1, \dots, f_p$ belong to the polynomial ring $\mathbb{Q}[X_1, \dots, X_n]$ in the indeterminates $X_1, \dots, X_n$ over the rational numbers $\mathbb{Q}$. Let d be a given natural number and assume that for $1 \leq k \leq p$ the total degree $\deg f_k$ of the polynomial f_k is bounded by d. Moreover, we suppose that the polynomials $f_1, \dots, f_p$ form a regular sequence in $\mathbb{Q}[X_1, \dots, X_n]$ and that they are given by a division-free

Research partially supported by the following German, French, Spanish and Argentinian grants: BA 1257/4-1 (DFG), ARG 018/98 INF (BMBF), UMS 658, ECOS A99E06, DGICYT PB96-0671-C02-02, ANPCyT 03-00000-01593, UBACYT TW 80 and PIP CONICET 4571/96. The first two authors wish to thank the MSRI at Berkeley for its hospitality during their stay, fall 1998.

arithmetic circuit of size L that evaluates them in any given point of the real (or complex) n–dimensional affine space $\mathbb{R}^n$ (or $\mathbb{C}^n$). Further, we assume that the Jacobian $J(f_1,\ldots,f_p)$ of the equation system $f_1=\cdots=f_p=0$ has maximal rank in any point of S_0 (thus, implicitly, we assume that S_0 is smooth). Let $W_0:=V(f_1,\ldots,f_p)$ denote the (complex) algebraic variety defined by the polynomials $f_1,\ldots,f_p$ in the affine space $\mathbb{C}^n$. We denote the singular locus of W_0 by $SingW_0$.

Moreover, let us suppose that the variables $X_1,\ldots,X_n$ are in generic position with respect to the equation system $f_1,\ldots,f_p$. For $1\le i\le n-p$ let W_i be the i–th *formal (complex) polar variety* associated with W_0 (and the variables $X_{p+i},\ldots,X_n$).

Further, let us denote the real counterpart of W_i by $S_i:=W_i\cap\mathbb{R}^n$. We call S_i the i–th formal *real* polar variety associated with the real semialgebraic variety S_0 (and the variables $X_{p+i},\ldots,X_n$). It turns out that the (locally) closed sets $W_i\setminus SingW_0$ and S_i are either empty or complex, or real manifolds of dimension $n-(p+i)$. Moreover, for $1\le i\le n-p$, one sees easily that

$$\widetilde{W}_i:=\overline{W_i\setminus SingW_0}$$

is the i–th polar variety (in the usual sense) associated with W_0 and the variables $X_{p+i},\ldots,X_n$ (here, $\overline{W_i\setminus SingW_0}$ denotes the $\mathbb{Q}$-Zariski closure in $\mathbb{C}^n$ of the quasi–affine variety $W_i\setminus SingW_0$). For a precise definition of the notion of formal polar varieties and of polar varieties in the usual sense we refer to Section 2.

Suppose that the real variety S_0 is non–empty and satisfies our assumptions. In Theorem 10 of this paper we show that every real polar variety $S_i=W_i\cap\mathbb{R}^n$, $1\le i\le n-p$, is a non–empty, smooth manifold of dimension $n-p-i$ containing at least one point of each connected component of the real variety S_0. In particular, the real variety S_{n-p} is a finite set containing at least one representative point of each connected component of S_0.

Under the same assumptions we show in Theorem 8 that for $1\le i\le n-p$ the quasi–affine variety $W_i\setminus SingW_0$ is a locally complete intersection that satisfies the Jacobian criterion. More precisely, the quasi–affine variety $W_i\setminus SingW_0$ is a smooth manifold of codimension $p+i$ that can be described locally by certain regular sequences consisting of the polynomials $f_1,\ldots,f_p$ and i many well–determined p–minors of the Jacobian $J(f_1,\ldots,f_p)$ of the $f_1,\ldots,f_p$. In particular, the quasi–affine variety $W_{n-p}\setminus SingW_0$ is zero-dimensional, whence $\widetilde{W}_{n-p}=W_{n-p}\setminus SingW_0$. Thus $\widetilde{W}_{n-p}$ is a zero-dimensional complex variety that contains a representative point of each connected component of the real variety S_0.

The practical outcome of Theorem 8 and Theorem 10 consists in the design of an efficient algorithm (with intrinsic complexity bounds), which adapts the elimination procedure for complex algebraic varieties developed in [30] and [31] to the real case. Under the additional assumption that, for $1\le k\le p$, the intermediate ideal $(f_1,\ldots,f_k)$ generated by $f_1,\ldots,f_k$ in $\mathbb{Q}[X_1,\ldots,X_n]$ is radical, we shall apply this procedure to the $p\binom{n}{p-1}$ well–determined equation systems of Theorem 8, which describe the zero-dimensional algebraic variety $\widetilde{W}_{n-p}=W_{n-p}\setminus SingW_0$ locally. In

[65] M. Shub, S. Smale: Complexity of Bezout's theorem III: Condition number and packing, J. of Complexity , 9, 4-14, (1993)
[66] M. Shub, S. Smale: Complexity of Bezout's theorem IV: Probability of Success, Extensions, SIAM J. Numer. Anal., 33, No.1, 128-148 (1996)
[67] M. Shub, S. Smale: Complexity of Bezout's theorem V: Polynomial time, Theoretical Comp. Sci., 133 (1994)
[68] P. Solernó: Complejidad de conjuntos semialgebraicos. Thesis Univ. de Buenos Aires (1989)

B. Bank, Institut für Mathematik, Humboldt-Universität zu Berlin, Germany
E-mail address: bank@mathematik.hu-berlin.de

M. Giusti, UMS MEDICIS, Laboratoire GAGE, École Polytechnique, Palaiseau, France
E-mail address: giusti@gage.polytechnique.fr

J. Heintz Departamento de Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, Santander, Spain
E-mail address: heintz@matesco.unican.es

Departamento de Matemática, Universidad de Buenos Aires, Argentina
E-mail address: joos@mate.dm.uba.ar

G. M. Mbakop, Institut für Mathematik, Humboldt-Universität zu Berlin, Germany
E-mail address: mbakop@mathematik.hu-berlin.de

order to find at least one representative point for every connected component of the real variety S_0, we have just to run the procedure of [30] and [31] on all these equation systems. Counting arithmetic operations in $\mathbb{Q}$ at unit costs, this can be done in sequential time

$$\binom{n}{p-1} L(nd\delta)^{O(1)},$$

where δ is the following geometric (and therefore, intrinsic) invariant:

$$\delta := \max\{\max\{\deg \overline{V(f_1,\dots,f_k)\setminus SingW_0}|1\leq k\leq p\},$$

$$\max\{\deg \widetilde{W}_i|1\leq i\leq n-p\}\}$$

(here, $\deg \overline{V(f_1,\dots,f_k)\setminus W_0}$ and $\deg \widetilde{W}_i$ denote the geometric degree in the sense of [37] of the corresponding algebraic varieties).
This is the content of Theorem 11 below. For any $1\leq k\leq p$ and any $1\leq i\leq n-p$ the quantity δ bounds the degree of the algebraic variety $\overline{V(f_1,\dots,f_k)\setminus SingW_0}$ and of the i–th polar variety $\widetilde{W}_i=\overline{W_i\setminus SingW_0}$.
In [30] and [31] the quantity $\max\{\deg V(f_1,\dots,f_i)|1\leq i\leq p\}$ is called the geometric degree (of the *complex* interpretation) of the equation system $f_1,\dots,f_p$. In analogy to this terminology, we shall call δ the *geometric degree* of the *real* interpretation of the equation system $f_1,\dots,f_p$. In view of the complexity result above we shall understand the parameter δ as an intrinsic measure for the size of the real interpretation of the given polynomial equation system. In order to make our complexity result more transparent we are going now to exhibit, in terms of extrinsic parameters, some estimations for the intrinsic system degree δ.
Let us write $d_1:=\deg f_1,\dots,d_p:=\deg f_p$ and let $D:=d_1\cdots d_p$ denote the classical Bézout number of the polynomial system $f_1,\dots,f_p$. Then we have the following degree estimations for the complex algebraic variety $W_0=V(f_1,\dots,f_p)$

$$\deg \overline{S_0}\leq \deg W_0\leq D\leq d^p,$$

$\overline{S_0}$ denotes again the $\mathbb{Q}$-Zariski closure in $\mathbb{C}^n$ of the real variety S_0.
On the other hand, we conclude from Theorem 8 that, for every i, $1\leq i\leq n-p$, the polar variety $\widetilde{W}_i$ is defined by the initial system $f_1,\dots,f_p$ and certain p–minors of the Jacobian $J(f_1,\dots,f_p)$. Let us denote the maximum degree of these p–minors by c_i. It turns out that for, any $1\leq i\leq n-p$, the polar variety $\widetilde{W}_i$ is a codimension one subvariety of $\widetilde{W}_{i-1}$. Now one sees easily that the quantity $D_i:=D\ c_1\cdots c_i$ represents a reasonable "Bézout number" of the variety $\widetilde{W}_i$ and that this Bézout number satisfies the estimate $\deg \widetilde{W}_i\leq D_i$. Putting all this together, we deduce the following estimate for the intrinsic system degree δ:

$$\delta\leq D_{n-p}=Dc_1\cdots c_{n-p}.$$

Observing that for any i, $1\leq i\leq n-p$, the inequality $c_i\leq d_1+\cdots+d_p-p$ holds, we find the estimations:

$$\delta\leq D(d_1+\cdots+d_p-p)^{n-p}\leq d^p(pd-p)^{n-p}<p^{n-p}d^n.$$

In conclusion, our new real algorithm has a time complexity that is, in worst case, polynomial in the "Bézout number" $Dc_1 \cdots c_{n-p}$ of the zero–dimensional polar variety $\widetilde{W}_{n-p}$.

Our complexity bound $\binom{n}{p-1} L(nd\delta)^{O(1)}$ depends on the intrinsic (geometric, semantic) parameter δ and on the extrinsic (algebraic) parameters d and n in a *polynomial* manner, and it depends on the syntactic parameter L only *linearly*. In this sense one may consider our complexity bound as *intrinsic*. Our real algorithm promises therefore to be practically applicable to special equation systems with low value for the intrinsic parameter δ.

On the other hand, *even in worst case* our algorithm *improves* upon the known $d^{O(n)}$–time procedures for the algorithmic problem under consideration, also in their most efficient versions [4], [5] (see also [3], [12], [19], [39], [40], [41], [59], [60], [14], [13]). However, this distinction does not become apparent when we measure complexities simply in terms of d and n (all mentioned algorithms have worst–case complexities of type $d^{O(n)}$), but it becomes clearly visible when we use the "Bézout number" just introduced as complexity parameter. Only our new algorithm is polynomial in this quantity. On the other hand, we are only able to reach our goal of algorithmic efficiency by means of a strict limitation to a purely geometric point of view. For the moment there is no hope that any of the standard questions of real algebra (e.g. finding generators for the real radical of a polynomial ideal or the formulation of an effective real Nullstellensatz) can be solved within the complexity framework of this paper (compare [52], [7] and [8]).

Our (algorithmic and mathematical) methods and results represent a non–obvious generalization of the main outcome of [1], where an intrinsic type algorithm was designed for the problem of finding at least one representative point in each connected component of a real, compact *hypersurface* given by an n–variate, smooth polynomial equation f of degree $d \geq 2$ with rational coefficients (such that f represents a regular equation of that hypersurface). This is the particular case of codimension $p = 1$ of the present paper, and our setting leads to the complexity bound $L(nd\delta)^{O(1)}$ proved in [1].

2. Polar Varieties

2.1. **Notations, Notions and General Assumptions.** Let $X_1, \ldots, X_n$ be indeterminates (or variables) over the rational numbers $\mathbb{Q}$ and let polynomials $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ with $1 \leq p \leq n$ be given. Let $\mathbb{C}^n$ and $\mathbb{R}^n$ denote the n–dimensional affine space over the complex and the real numbers, respectively. We think $\mathbb{C}^n$ to be equipped with the $\mathbb{Q}$-Zariski topology, whereas, on $\mathbb{R}^n$, we consider the strong topology. For any subset $U \subset \mathbb{C}^n$ we denote its $\mathbb{Q}$-Zariski–closure by $\overline{U}$. By $X := (X_1, \ldots, X_n)$ we denote the vector of variables $X_1, \ldots, X_n$ and by $x := (x_1, \ldots, x_n)$ any point of the affine space $\mathbb{C}^n$ or $\mathbb{R}^n$. We suppose that the polynomials $f_1, \ldots, f_p$ form a reduced regular sequence in $\mathbb{Q}[X_1, \ldots, X_n]$. The

[42] J. Heintz, C.P. Schnorr: Testing polynomials which are easy to compute, Proc. 12th Ann. ACM Symp. on Computing (1980) 262–268; also in Logic and Algorithmic. An International Symposium held in Honour of Ernst Specker , Monographie No.30,de l'Enseignement de Mathématiques, Genève, 237–254 (1982)

[43] J. Heintz, R. Wüthrich : An efficient quantifier elimination algorithm for algebraically closed fields of any characteristic, SIGSAM Bull. , vol.,9, No. 4 (1975)

[44] G. Hermann: Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, Math. Ann. 95, 736–788 (1926)

[45] T. Krick, L.M. Pardo: A Computational Method for Diophantine Approximation, in: Algorithms in Algebraic Geometry and Applications, MEGA'94 (L. Gonzales-Vega and T. Recio, eds.) Progress in Mathematics, 143, 193-254, Birkhäuser, Basel, (1996)

[46] T. Krick, L.M. Pardo: Une approche informatique pour l'approximation diophantienne, C. R. Acad. Sci. Paris, t. 318, Série I, no. 5, 407–412 (1994)

[47] S. Lang: Diophantine Geometry , Interscience Publishers John Wiley & Sons, New York, London (1962)

[48] D. Lazard: Algèbre linéaire sur $K[X_1, \ldots, X_n]$ et élimination, Bull. Soc. Math. France, 105, 165–190 (1977)

[49] D. Lazard : Résolution des systèmes d'équations algébriques, Theor. Comp. Sci.,15, 77–110 (1981)

[50] D. T. Lê, B. Teissier: Variétés polaires locales et classes de Chern des variétés singulières, Annals of Mathematics, 114, 457-491 (1981)

[51] A. K. Lenstra, H. W. Lenstra Jr., L. Lovász: Factoring polynomials with rational coefficients, Math. Ann., 261, 534-543 (1982)

[52] H. Lombardi: Une borne sur les degrés pour les Théorèmes des zéros réel effectif. in M. Coste, L. Mahé and M.–F. Roy (eds) Real Algebraic Geometry, Rennes 1991, Lecture Notes in Mathematics, Vol. 1524, pp 323–345, Springer Berlin, (1992)

[53] G. Matera: Probabilistic algorithms for geometric elimination. Appl. Algebra Eng. Commun. Comput. 9, No.6, 463-520 (1999)

[54] G. M. Mbakop: Effiziente Lösung reller polynomialer Gleichungssysteme. Dissertaion, Math.–Nat. Fak.II, Humboldt–Universität zu Berlin (1999)

[55] M. Milnor: On the Betti numbers of real algebraic varieties, Proc. Amer. Math. Soc.,15, 275-280 (1964)

[56] J. Morgenstern: How to compute fast a function and all its derivatives, Prépublication No. 49, Université de Nice (1984)

[57] L.M. Pardo: How lower and upper complexity bounds meet in elimination theory, in Proc. 11th International Symposium Applied Algebra, Algebraic Algorithms and Error–Correcting Codes, AAECC–11, Paris 1995, G. Cohen, M.Giusti and T. Mora, eds., Springer LNCS, 948, 33–69 (1995)

[58] R. Piene: Polar classes of singular varieties, Ann. scient. Éc. Norm. Sup. 4. série, t. 11, 247-276 (1978)

[59] J. Renegar: A faster PSPACE algorithm for the existential theory of the reals, Proc. 29th Annual IEEE Symposium on the Foundation of Computer Science (FOCS), 291-295, (1988)

[60] J. Renegar: On the Computational Complexity and Geometry of the first Order theory of the Reals. J. of Symbolic Comput., 13(3), 255-352 (1992)

[61] M.-F. Roy, A. Szpirglas: Complexity of computation with real algebraic numbers, J. Symbolic Computat. 10, 39-51 (1990)

[62] A. Seidenberg: Constructions in Algebra, Transactions Amer. Math. Soc., 197, 273–313 (1974)

[63] M. Shub, S. Smale: Complexity of Bezout's theorem I: Geometric aspects, J. Amer. Math. Soc., 6, 459-501 (1993)

[64] M. Shub, S. Smale: Complexity of Bezout's theorem II: Volumes and probabilities, in Proceedings Effective Methods in Algebraic Geometry, MEGA'92 Nice, 1992, F. Eyssette and A. Galligo, eds. Progress in Mathematics, Vol. 109, Birkhäuser, Basel, (1993) 267-285

[19] F. Cucker, S. Smale: Complexity estimates depending on condition and round-of error, Bilardi, Gianfranco (ed.) et al., Algorithms - ESA '98. 6th annual European symposium, Venice, Italy, August 24–26, 1998. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 1461, 115-126 (1998).
[20] J.-P. Dedieu, Estimations for the Separation Number of a Polynomial System, J. Symbolic Comp. 24, 683-693 (1997)
[21] J.-P. Dedieu, Approximate Solutions of Numerical Problems, Condition Number Analysis and Condition Number Theorems, Lectures in Applied Mathematics, Vol. 32, 263-283 (1996)
[22] M. Demazure, Catastrophes et bifurcations, Ellipses, Paris (1989)
[23] A. Dickenstein, N. Fitchas, M. Giusti, C. Sessa : The membership problem of unmixed ideals is solvable in single exponential time, Discrete Applied Mathematics, 33, 73–94 (1991) .
[24] I. Z. Emiris: On the Complexity of Sparse Elimination, Report No. UCB/CSD-94/840, Univ. of California (1994)
[25] J. von zur Gathen: Parallel arithmetic computations: A survey. Mathematical foundations of computer science, Proc. 12th Symp., Bratislava/Czech. 1986, Lect. Notes Comput. Sci. 233, 93-112 (1986). MSC 1991
[26] J. von zur Gathen: Parallel linear algebra. In J. Reif, editor Synthesis of parallel algorithmns. Morgan Kaufmann (1993)
[27] J. von zur Gathen, G. Seroussi: Boolean circuits versus arithmetic circuits, Information and Computation, 91, (1), 142-154 (1991)
[28] M. Giusti, J. Heintz: La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial, In Computational Algebraic Geometry and Commutative Algebra , Proceedings of the Cortona Conference on Computational Algebraic Geometry and Commutative Algebra, D. Eisenbud and L. Robbiano, eds., Symposia Matematica, vol. XXXIV, Istituto Nazionale di Alta Matematica, Cambridge University Press (1993).
[29] M. Giusti, J. Heintz, J.E. Morais, L.M. Pardo: When polynomial equation systems can be "solved" fast? in Proc. 11th International Symposium Applied Algebra, Algebraic Algorithms and Error–Correcting Codes, AAECC–11 , Paris 1995, G. Cohen, M.Giusti and T. Mora, eds., Springer LNCS, 948, 205–231 (1995)
[30] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, L.M. Pardo: Straight–line programs in Geometric Elimination Theory, J. Pure Appl. Algebra, 124, No.1-3, 101-146 (1998)
[31] M. Giusti, J. Heintz, K. Hägele, J. E. Morais, J. L. Montaña, L. M. Pardo: Lower Bounds for Diophantine Approximations, J. Pure and Applied Alg.,117 & 118, 277–317 (1997)
[32] M. Giusti, J.P. Henry: Minorations de nombres de Milnor, Bull. Soc. Math. Fr.,108, 17-45 (1980)
[33] M. Giusti, G. Lecerf, B. Salvy: A Gröbner Free Alternative for Polynomial System Solving, submitted to J. of Complexity (1999)
[34] M. Golubitsky, V. Guillemin: Stable Mappings and their Singularities, Springer-Verlag, New York (1986)
[35] D. Grigor'ev: Complexity of deciding Tarski Algebra, J. Symbolic Comput.,3, 65-108 (1987)
[36] D. Grigor'ev, N. Vorobjov: Solving Systems of Polynomial Inequalities in Subexponential Time, J. Symbolic Comput. J. Symb. Comput. 5, No.1/2, 37-64 (1988)
[37] J. Heintz: Fast quantifier elimination over algebraically closed fields, Theoret. Comp. Sci., 24, 239-277 (1983).
[38] J. Heintz, G. Matera, A. Waissbein: On the time–space complexity of geometric elimination procedures, submitted to AAECC (1999)
[39] J. Heintz, M.–F. Roy, P. Solernó: On the complexity of semialgebraic sets, Proc. Information Processing 89 (IFIP 89) San Francisco 1989, G.X.Ritter, ed., North-Holland (1989) 293–298.
[40] J. Heintz, M.–F. Roy, P. Solernó: Complexité du principe de Tarski–Seidenberg, C. R. Acad. Sci. Paris , t. 309, Série I, 825–830 (1989)
[41] J. Heintz, M–F. Roy and P. Solernó: Sur la complexité du principe de Tarski–Seidenberg, Bull. Soc. math. France, 18, 101–126 (1990)

Jacobian of these polynomials is denoted by

$$J(f_1,\dots,f_p) := \left[\frac{\partial f_k}{\partial X_j}\right]_{\substack{1\le k\le p\\ 1\le j\le n}}.$$

For any point $x\in\mathbb{C}^n$ we write

$$J(f_1,\dots,f_p)(x) := \left[\frac{\partial f_k}{\partial X_j}(x)\right]_{\substack{1\le k\le p\\ 1\le j\le n}}$$

for the Jacobian of the polynomials $f_1,\dots,f_p$ at x.

The common complex zeros of the polynomials $f_1,\dots,f_p$ form an affine, $\mathbb{Q}$-definable subvariety of $\mathbb{C}^n$, which we denote by

$$W_0 := V(f_1,\dots,f_p) := \{x\in\mathbb{C}^n \mid f_1(x)=\ldots=f_p(x)=0\}.$$

A point $x\in W_0=V(f_1,\dots,f_p)$ is said to be *smooth* (in W_0) if the rank of the Jacobian of $f_1,\dots,f_p$ in x satisfies the condition $rk\ J(f_1,\dots,f_p)(x)=p$. Otherwise x is called a *singular* point of W_0. By $SingW_0$ we denote the set of all singular points of W_0.

Remark 1. *If $x\in W_0$ is smooth, then the hypersurfaces defined by the polynomials $f_1,\dots,f_p$ intersect transversally at the point x.*

Definition 2. *For every i, $1\le i\le n-p$, let Δ_i denote the set of all common complex zeros of all p-minors of the Jacobian $J(f_1,\dots,f_p)$ corresponding to the columns $\{1,\dots,p+i-1\}$. In other words, Δ_i is the determinantal variety defined by all p-minors of the submatrix $J_1^{p+i-1}(f_1,\dots,f_p)$ determined by the columns $\{1,\dots,p+i-1\}$ of the Jacobian $J(f_1,\dots,f_p)$.*
We introduce the affine variety

$$W_i := W_0\cap\Delta_i$$

associated with the linear subspace of $\mathbb{C}^n$, namely

$$X^{p+i-1} := \{x\in\mathbb{C}^n \mid X_{p+i}(x)=\ldots=X_n(x)=0\}$$

*and call W_i the i–*th formal polar variety *of W_0. By*

$$\widetilde{W_i} := \overline{W_i\setminus SingW_0}$$

we denote the i–th polar variety *(in the usual sense) of the variety W_0.*

Remark 3.
- *The index i reflects the expected codimension of the formal polar variety W_i in W_0. With respect to the ambient space $\mathbb{C}^n$, one has always codim $W_i\ge p+i$.*
- *According to our notation, the common zeros of all p–minors of the Jacobian $J(f_1,\dots,f_p)$ form the determinantal variety Δ_{n-p+1}. Obviously, we have $Sing\ W_0 = W_0\cap\Delta_{n-p+1} = W_{n-p+1}$.*
- *The formal polar varieties W_i, $1\le i\le n-p$, form a decreasing sequence. In particular, we have*
  $W_0\supset W_1\supset\cdots\supset W_i\supset\cdots\supset W_{n-p}\supset W_{n-p+1}=Sing\ W_0$.

The concept of polar variety goes back to J.–V. Poncelet. Its development has a long history: Let us mention among others the contributions of F. Severi, J. A. Todd, S. Kleiman, R. Piene, D. T. Lê, B. Teissier, J.–P. Henry, M. Merle ... (see e.g. [58] and the references quoted there).

2.2. **Local Description of the Determinantal Varieties.** In this subsection we develop a succinct local description of the determinantal varieties Δ_i, $1 \le i \le n-p$. The following general Exchange Lemma will be our main tool for this description (this lemma is used in a similar form in [32]). It describes an exchange relation between certain minors of a given matrix .

Let A be a given $(p \times n)$-matrix with entries a_{ij} from an arbitrary commutative ring. Let l and k be any natural numbers with $l \le n$ and $k \le \min\{p, l\}$. Furthermore, let $I_k := (i_1, \ldots, i_k)$ be an ordered sequence of k different elements from the finite set of natural numbers $\{1, \ldots, l\}$ and let $M_A(I_k) := M_A(i_1, \ldots, i_k)$ denote the k-minor of the matrix A built up by the first k rows and the columns $i_1, \ldots, i_k$. If it is clear by the context what is the matrix A, we shall just write $M(i_1, \ldots, i_k) := M(I_k) := M_A(I_k)$.

Lemma 4 (Exchange Lemma)**.** *As before let a matrix A and natural numbers l and k be given, as well as two intersecting index sets $I_k = (i_1, \ldots, i_k)$ and $I_{k-1} = (j_1, \ldots, j_{k-1})$. Then, for suitable numbers $\varepsilon_j \in \{1, -1\}$ with $j \in I_k \setminus I_{k-1}$ we have the following identity:*

$$(*) \qquad M(I_{k-1})\, M(I_k) = \sum_{j \in I_k \setminus I_{k-1}} \varepsilon_j \; M(I_k \setminus \{j\})\, M(I_{k-1} \cup \{j\}) .$$

Proof

Consider the following $((2k-1) \times (2k-1))$-matrix L with entries from the given matrix A:

$$L := \left[\begin{array}{c|c} & L_1(I_k) \\ O & \vdots \\ & L_{k-1}(I_k) \\ \hline L_1(I_{k-1}) & L_1(I_k) \\ \vdots & \vdots \\ L_k(I_{k-1}) & L_k(I_k) \end{array} \right] .$$

Here, for any $1 \le j \le k$, $L_j(I_k)$ denotes the row vector of length k that we obtain selecting, from the j–th row of the matrix A, the k elements placed in the columns $I_k = (i_1, \ldots, i_k)$. Similarly, $L_j(I_{k-1})$ is obtained from the j–th row of A selecting the $k-1$ elements placed in the columns $I_{k-1} = (j_1, \ldots, j_{k-1})$.
Now it is not difficult to verify the identity $(*)$ by calculating the determinant $\det L$

represented by the network $\mathcal{N}^*$ returns all these points in a codification "à la Thom". Moreover, the non–empty set $W^*_{n-p} \cap \mathbb{R}^n$ contains at least one representative point for each connected component of the real variety S_0.

The proof of this remark is a straight–forward adaptation of the arguments of the proof of [1], Theorem 12 (which treats only the hypersurface case with $p := 1$) to the arguments of Theorem 11 above. Therefore, we omit this proof.

References

[1] Bank, B.; Giusti, M.; Heintz, J.; Mbakop, G.M. Polar varieties, real equation solving and data structures: The hypersurface case. J. Complexity 13, No.1, 5-27, (1997), Best Paper Award J. Complexity 1997
[2] Bank, B.; Giusti, M.; Heintz, J.; Mandel, R.; Mbakop, G. M.: Polar Varieties and Efficient Real Equation Solving: The Hypersurface Case. Proceedings of the 3rd Conference Approximation and Optimization in the Caribbean, in: Aportaciones Matemáticas, Mexican Society of Mathematics, J. Bustamante, M. A. Jimenez et al.(eds.) (1998)
[3] A. I. Barvinok: Feasibility testing for systems of real quadratic equations, Manuscript, Royal Institute of Technology, Stockholm (1991)
[4] S. Basu, R. Pollack, M.-F. Roy: On the Combinatorial and Algebraic Complexity of Quantifier Elimination. J.ACM 43, No. 6, 1002-1045,(1996)
[5] S. Basu, R. Pollack, M.-F. Roy: Complexity of computing semi-algebraic descriptions of the connected components of a semialgebraic set. Proceedings of ISSAC '98, Gloor, Oliver (ed.), Rostock, Germany, August 13–15, 1998. New York, NY: ACM Press. 25-29 (1998).
[6] W. Baur, V. Strassen: The complexity of partial derivatives, Theoret. Comput. Sci. 22, 317-330 (1982)
[7] E. Becker, R. Neuhaus: Computation of real radicals of polynomial ideals. Computanial algebraic geometry (Nice 1992), 1–20, Progr. Math. 109, Birkhäuser Boston, Boston MA, (1993)
[8] E. Becker, J. Schmidt: On the real Nullstellensatz. Algorithmic algebra and number theory (Heidelberg, 1997), 173–185, Springer Berlin (1999)
[9] M. Ben-Or, D. Kozen, J. Reif: The complexity of elementary algebra and geometry, J. Comput. Syst. Sci. 32, 251-264 (1986)
[10] B. Buchberger, Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems, Aequationes math. 4, 371–383 (1970)
[11] P. Bürgisser, M. Clausen, M. A. Shokrollahi Algebraic complexity theory. With the collaboration of Thomas Lickteig. Grundlehren der Mathematischen Wissenschaften. 315. Berlin: Springer. XXIII, 618 (1997)
[12] L. Blum, F. Cucker, M. Shub, S. Smale, Complexity and real computation. Foreword by Richard M. Karp. New York, NY: Springer. XVI, 453 p. (1997)
[13] J. F. Canny: Some Algebraic and Geometric Computations in PSPACE, Proc. 20th ACM Symp. on Theory of Computing (1988) 460-467
[14] J. F. Canny, I. Z. Emiris: Efficient Incremental Algorithms for the Sparse Resultant and the Mixed Volume, J. Symb. Comput. 20, No.2, 117-149 (1995)
[15] L. Caniglia, A. Galligo, J. Heintz: Some new effectivity bounds in computational geometry, Proc. AAECC–6, T. Mora, ed. , Springer LNCS, 357, 131–152 (1989)
[16] A. L. Chistov: Polynomial-time computation of the dimension of components of algebraic varieties in zero-characteristic, Preprint Université Paris XII (1995)
[17] A. L. Chistov, D. J. Grigor'ev: Subexponential time solving systems of algebraic equations , LOMI Preprints E-9-83, E-10-83, Leningrad (1983)
[18] M. Coste, M.-F. Roy: Thom's Lemma, the coding of real algebraic numbers and the computation of the topology of semialgebraic sets, J. Symbolic Comput., 5, 121-130 (1988)

Now, we are going to restate the main outcome of Theorem 11 in terms of the new complexity parameter δ^*. For this purpose we have to include the following two subroutines in our algorithmic model:

- the first subroutine we need is a factorization algorithm for univariate polynomials over $\mathbb{Q}$. In the bit complexity model the problem of factorizing univariate polynomials over $\mathbb{Q}$ is known to be of polynomial time complexity [51], whereas in the arithmetic model we are considering here this question is more intricate [27]. In the extended complexity model we are going to consider here, the cost of factorizing a univariate polynomial of degree D over $\mathbb{Q}$ (given by its coefficients) is accounted as $D^{O(1)}$.
- the second subroutine allows us to discard non-real irreducible components of the occurring complex polar varieties. This second subroutine starts from a straight-line program for a single polynomial in $\mathbb{Q}[X_1,\ldots,X_n]$ as input and decides whether this polynomial has a real zero (however, without actually exhibiting it if there is one). Again this subroutine is taken into account at polynomial cost.

We call an arithmetic network over $\mathbb{Q}$ *extended* if it contains extra nodes corresponding to the first and second subroutine.

Modifying our algorithmic model in this way, we are able to formulate the following complexity result, which generalizes [1], Theorem 12 and improves the complexity outcome of our previous Theorem 11.

Remark 13. *Let n,p,d,δ^*,L and ℓ be natural numbers with $d\geq 2$ and $p\leq n$. There exists an extended arithmetic network $\mathcal{N}^*$ over $\mathbb{Q}$ of size $\binom{n}{p-1}L(nd\delta^*)^{O(1)}$ with the following property: Let $f_1,\ldots,f_p$ be a family of n-variate polynomials of a degree at most d and assume that $f_1,\ldots,f_p$ are given by a division–free arithmetic circuit β in $\mathbb{Q}[X_1,\ldots,X_n]$ of size L. Suppose that the polynomials $f_1,\ldots,f_p$ satisfy the conditions (i), (ii), (iii), and (iv) contained in the formulation of Theorem 11. Let us now freely use the notations introduced in the present section. Assume that the real variety $S_0=\{x\in\mathbb{R}^n|f_1(x)=\cdots=f_p(x)=0\}$ is not empty and that the real degree of the polynomial system $f_1,\ldots,f_p$ is bounded by δ^*. The algorithm represented by the arithmetic network $\mathcal{N}^*$ starts from the circuit β as input and decides first whether the complex variety W^*_{n-p} is empty. If this is not the case, then W^*_{n-p} is a zero–dimensional complex variety and the network $\mathcal{N}^*$ produces an arithmetic circuit in $\mathbb{Q}$ of asymptotically the same size as $\mathcal{N}^*$, which represents the coefficients of $n+1$ univariate polynomials $q^*,p^*_1,\ldots,p^*_n\in\mathbb{Q}[X_n]$ satisfying the conditions*

$$\deg q^* = \#\, W^*_{n-p},$$

$$\max\{\deg p^*_k|1\leq k\leq n\}<\deg q^*,$$

$$W^*_{n-p}=\{(p^*_1(u),\ldots,p^*_n(u))|u\in\mathbb{C},q^*(u)=0\}.$$

Each over $\mathbb{Q}$ irreducible component of the complex variety W^*_{n-p} contains at least one real point characterized by an irreducible factor of the polynomial q^*. The algorithm

of the quadratic matrix L via Laplace expansion in two different ways. First, by expansion of $\det L$ according to the first $k-1$ columns of L, we obtain the left–hand side of $(*)$, disregarding the sign. Expansion of $\det L$ according to the first $k-1$ rows of L leads to the right–hand side of $(*)$. This implies the identity $(*)$ for an appropriate choice of the signs ε_j, with $j\in I_k\setminus I_{k-1}$. □

Let $m\in\mathbb{Q}[X_1,\ldots,X_n]$ denote the $(p-1)$–minor of the Jacobian $J(f_1,\ldots,f_p)$ given by the first $(p-1)$ rows and columns, i.e., let

$$m:=\det\left[\frac{\partial f_k}{\partial X_j}\right]_{\substack{1\leq k\leq p-1\\ 1\leq j\leq p-1}}.$$

We consider the determinantal variety Δ_i outside of the hypersurface

$$V(m):=\{x\in\mathbb{C}^n\mid m(x)=0\}$$

and denote this localization by $(\Delta_i)_m$, i.e., we set

$$(\Delta_i)_m:=\Delta_i\setminus V(m).$$

¿From now on, for $1\leq i_1\leq\cdots\leq i_p\leq n$, let us denote by

$$M(i_1,\ldots,i_p)$$

the polynomial in $\mathbb{Q}[X_1,\ldots,X_n]$ defined as the p–minor of the Jacobian $J(f_1,\ldots,f_p)$ built up by its p rows and the columns $i_1,\ldots,i_p$. As before, we denote by

$$M(i_1,\ldots,i_p)(x)$$

the specialization of $M(i_1,\ldots,i_p)$ in a given point $x\in\mathbb{C}^n$.

Proposition 5. *Let $1\leq i\leq n-p$ be arbitrarily fixed, and let m be the $(p-1)$–minor defined above. Then the determinantal variety Δ_i is locally (i.e., outside of the hypersurface $V(m)$) described by the i polynomials*

$$M(1,\ldots,p-1,p),M(1,\ldots,p-1,p+1),\ldots,M(1,\ldots,p-1,p+i-1).$$

In other words, we have

$$(\Delta_i)_m:=\{x\in\mathbb{C}^n|\ m(x)\neq 0,M(1,\ldots,p-1,s)(x)=0,s\in\{p,\ldots,p+i-1\}\},$$

where $M(1,\ldots,p-1,s)$ denotes, as above, the p–minor of the Jacobian $J(f_1,\ldots,f_p)$ built up by the first $p-1$ columns and the s–th column.

Proof

It suffices to show that

$$(\Delta_i)_m\supset\{x\in\mathbb{C}^n|\ m(x)\neq 0,M(1,\ldots,p-1,s)=0,s\in\{p,\ldots,p+i-1\}\}$$

holds.

Let $x^*\in\mathbb{C}^n$ be any point satisfying the conditions $m(x^*)\neq 0$ and $M(1,\ldots,p-1,s)(x^*)=0$ for every $s\in\{p,\ldots,p+i-1\}$. We have to verify that

$$M(i_1,\ldots,i_p)(x^*)=0$$

holds for all ordered p–tuples $(i_1, \ldots, i_p)$ of elements of $\{1, \ldots, p+i-1\}$.

Applying the Exchange Lemma to $m = M(1, \ldots, p-1)$ and $M(i_1, \ldots, i_p)$, we deduce the identity

$$m(x^*)M(i_1, \ldots, i_p)(x^*) =$$

$$\sum_{j \in \{i_1, \ldots, i_p\} \setminus \{1, \ldots, p-1\}} \varepsilon_j \ M(\{i_1, \ldots, i_p\} \setminus \{j\})(x^*)M(1, \ldots, p-1, j)(x^*)$$

for suitable numbers $\varepsilon_j \in \{1, -1\}$ with $j \in \{i_1, \ldots, i_p\} \setminus \{1, \ldots, p-1\}$. By assumption we have $m(x^*) \neq 0$ and $M(1, \ldots, p-1, j)(x^*) = 0$ for all $j \in \{p, \ldots, p+i-1\}$. This implies that x^* belongs to the set $(\Delta_i)_m$.

□

Notation 6. *In the sequel we shall simply write M_j for the p- minor $M(1, \ldots, p-1, j)$ given by the first $p-1$ columns of $J(f_1, \ldots, f_p)$ and the column $j \in \{p, \ldots, n\}$*.

Remark 7.
- *Proposition 5 implies that the codimension of Δ_i outside of the hypersurface $V(m)$ is at most i.*
- *Proposition 5 holds also for the determinantal variety Δ_{n-p+1} that defines the singular locus $Sing\ W_0 = W_{n-p+1}$ of the variety W_0. Hence, for any point $x^* \in \mathbb{C}^n$ satisfying the condition $m(x^*) \neq 0$ and the $n-p+1$ equations*

$$M_j(x^*) = 0, \ j \in \{p, \ldots, n\},$$

the Jacobian $J(f_1, \ldots, f_p)(x^*)$ becomes singular.
- *Replacing the previously chosen $(p-1)$-minor m by any other $(p-1)$-minor of the Jacobian $J(f_1, \ldots, f_p)$, the statement of Proposition 5 remains true mutatis mutandis.*

2.3. Local Description of the Formal Polar Varieties.

The aim of this subsection is to show the following fact:

Let the variables $X_1, \ldots, X_n$ be in generic position with respect to the polynomials $f_1, \ldots, f_p$, and let $\tilde{m}$ be any $(p-1)$–minor of the Jacobian $J(f_1, \ldots, f_p)$. In this subsection we are going to show that any formal polar variety W_i, $1 \leq i \leq n-p$, is a smooth complete intersection variety outside of the closed set $SingW_0 \cup V(\tilde{m})$. Moreover, we shall exhibit a reduced regular sequence describing this variety outside of $SingW_0 \cup V(\tilde{m})$.

As in the previous subsection, let $m \in \mathbb{Q}[X_1, \ldots, X_n]$ denote the $(p-1)$–minor of the Jacobian $J(f_1, \ldots, f_p)$ built up by the first $(p-1)$ rows and columns.

Let $Y_1, \ldots, Y_n$ be new variables and let $Y := (Y_1, \ldots, Y_n)$. For any linear coordinate transformation $X = AY$, with A being a regular $(n \times n)$–matrix, we define the polynomials

$$G_1(Y) := f_1(AY), \ldots, G_p(Y) := f_p(AY).$$

by means of an arithmetic network $\mathcal{N}_1$, which extends $\mathcal{N}_0$ and has asympotically the same size and nonscalar depth. The final arithmetic network $\mathcal{N}$ is now obtained from $\mathcal{N}_1$ in the same way as in the proof [1], Theorem 8. □

Remark 12. (i) *Using the refined algorithmic techniques of* [38] *or* [33] *it is not too difficult to see that for inputs $f_1, \ldots, f_p$ represented by straight–line programs of length T and space S the arithmetic network $\mathcal{N}$ can be converted into an algebraic computation tree which solves the algorithmic problem of Theorem 11 in time $O((Tdn^2 + n^5)\delta^3 \log^3 \delta \log^2 \log \delta)$ and space $O(Sdn\delta^2)$.*

(ii) *The smooth, compact hypersurface case (with $p := 1$) of Theorem 11 corresponds exactly to* [1], *Theorem 8.*

(iii) *Let $J(f_1, \ldots, f_p)^T$ denote the transposed matrix of the Jacobian $J(f_1, \ldots, f_p)$ of the polynomials $f_1, \ldots, f_p$ in the statement of Theorem 11 and let*

$$\mathcal{D} := \det J(f_1, \ldots, f_p)J(f_1, \ldots, f_p)^T.$$

¿From the well–known Cauchy–Binet formula one deduces easily that, with the notations of Section 2, the identity

$$\mathcal{D} = \sum_{1 \leq i_1 < \cdots < i_p \leq n} \det{}^2\ M(i_1, \ldots, i_p)$$

holds. Replacing now, in the statement and the proof of Theorem 11 for $1 \leq i \leq n-p$, the polar variety $\widetilde{W}_i$ by $\widehat{W}_i := \overline{W_i \setminus V(\mathcal{D})}$ and the parameter δ by

$$\widehat{\delta} := \max\{\max\{\deg \widetilde{V}_k | 1 \leq k \leq p\}, \max\{\deg \widehat{W}_i | 1 \leq i \leq n-p\}\}$$

one obtains a somewhat improved complexity result, since $\widehat{\delta} \leq \delta$ holds.

Let us now suppose that the polynomials $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ satisfy the conditions (i), (ii), (iii), (iv) above. Unfortunately, the complexity parameter δ of Theorem 11 is strongly related to the *complex* degrees of the polar varieties $\widetilde{W}_1, \ldots, \widetilde{W}_{n-p}$ of $W_0 = \{x \in \mathbb{C}^n | f_1(x) = \cdots = f_p(x) = 0\}$ and not to their *real* degrees. Under some additional algorithmic assumptions, which we are going to explain below, we may replace the complexity parameter δ by a smaller one that measures only the real degrees of the polar varieties $\widetilde{W}_1, \ldots, \widetilde{W}_{n-p}$. We shall call this new complexity parameter the *real degree* of the equation system $f_1, \ldots, f_p$ and denote it by δ^*.

Let $1 \leq k \leq p$ and let us consider the decomposition of the intermediate variety $\widetilde{V}_k$ into irreducible components with respect to the $\mathbb{Q}$-Zariski topology of $\mathbb{C}^n$ say $\widetilde{V}_k = C_1 \cup \cdots \cup C_s$. We call an irreducible component C_r, $1 \leq r \leq s$, *real* if $C_r \cap \mathbb{R}^n$ contains a smooth point of C_r. The union of all real irreducible components of $\widetilde{V}_k$ is called the *real part* of $\widetilde{V}_k$ and denoted by V_k^*. We call $\deg V_k^*$ the *real degree* of the intermediate variety $\widetilde{V}_k$. Similarly, we introduce for every $1 \leq i \leq n-p$ the real part W_i^* of the polar variety $\widetilde{W}_i$ and its real degree $\deg W_i^*$. Finally, we define the *real degree of the equation system* $f_1, \ldots, f_p$ as

$$\delta^* := \max\{\max\{\deg V_k^* | 1 \leq k \leq p\}, \max\{\deg W_i^* | 1 \leq i \leq n-p\}\}.$$

trivial ideal or form a regular sequence in the localized $\mathbb{Q}$ -algebra $\mathbb{Q}[X_1,\dots,X_n]_g$. In either case the ideal generated by $f_1,\dots,f_p,M_p,\dots,M_{p+i-1}$ in $\mathbb{Q}[X_1,\dots,X_n]_g$ is radical and defines a complex variety that is empty or of degree

$$\deg(\overline{W_i\setminus V(g)})\le \deg(\overline{W_i\setminus SingW_0})=\deg \widetilde{W}_i\le\delta.$$

Moreover, by assumption, the polynomials $f_1,\dots,f_p$ form a regular sequence in $\mathbb{Q}\ [X_1,\dots,X_n]_g$ and for each $1\le k\le p$ the ideal generated by $f_1,\dots,f_k$ in $\mathbb{Q}[X_1,\dots,X_n]_g$ is radical and defines a complex variety of degree

$$\deg \overline{V_k\setminus V(g)}\le \deg \widetilde{V}_k\le\delta.$$

One sees easily that the polynomials $f_1,\dots,f_p,M_p,\dots,M_{n-1}$ and g can be evaluated by a division–free arithmetic circuit of size $O(L+n^5)$ and nonscalar depth $O(\log n+\ell)$. Applying now, for each $1\le i\le n-p$, the algorithm underlying [30], Proposition 18 in its rational version [31], Theorem 19 to the system

$$f_1=0,\dots,f_p=0,\ M_p=0,\dots,M_{p+i-1}=0,g\neq 0$$

we are able to check whether the particular system

$$f_1=0,\dots,f_p=0,\ M_p=0,\dots,M_{n-1}=0,g\neq 0$$

has a solution in $\mathbb{C}^n$. If this is the case, then this system defines a zero–dimensional algebraic set, namely $W_{n-p}\setminus V(g)$, and the algorithm produces an arithmetic circuit $\bar\gamma$ in $\mathbb{Q}$ that represents the coefficients of $n+1$ univariate polynomials $\bar q,\bar p_1,\dots,\bar p_n\in\mathbb{Q}[X_n]$ satisfying the following conditions:

$$\deg\bar q=\#\ (W_{n-p}\setminus V(g)),$$

$$\max\{\deg\bar p_k|1\le k\le n\}<\deg\bar q,$$

$$W_{n-p}\setminus V(g)=\{(\bar p_1(u),\dots,\bar p_n(u))|u\in\mathbb{C},\bar q(u)=0\}.$$

The algorithm is represented by an arithmetic network of size $L(nd\delta)^{O(1)}$ and nonscalar depth $O(n(\log nd+\ell)\log\delta)$, and the circuit $\bar\gamma$ has asymptotically the same size and nonscalar depth. Running this procedure for each selection $1\le i_1<\cdots<i_p\le n$ and $1\le j,k\le p$ we obtain an arithmetic network $\mathcal{N}_0$ of size $p^2\binom{n}{p}L(nd\delta)^{O(1)}=\binom{n}{p-1}L(nd\delta)^{O(1)}$ and nonscalar depth $O(n(\log nd+\ell)\log\delta)$, which decides whether $\widetilde{W}_{n-p}=W_{n-p}\setminus SingW_0$ is empty. Suppose that this is not the case. Then $\mathcal{N}_0$ describes locally the variety $\widetilde{W}_{n-p}$, which is now zero-dimensional. Each local description of $\widetilde{W}_{n-p}$ contains an arithmetic circuit representation of the coefficients of the minimal polynomial of the variable X_n with respect to the corresponding local piece of $\widetilde{W}_{n-p}$. Moreover, one easily obtains the same type of information for any linear form X_i+X_n and any variable X_i with $1\le i<n$. One multiplies now all minimal polynomials of the variable X_n obtained in this way. Making this product squarefree (see e.g [45], Lemma 12) one obtains the polynomial q of the statement of Theorem 11. Doing the same thing for the minimal polynomials of each linear form X_i+X_n and each variable X_i with $1\le i<n$, yields by means of [45], Lemma 26, the polynomials $p_1,\dots,p_n$ of the statement of Theorem 11. All this can be done

The Jacobian of $G_1,\dots,G_p$ has the form

$$J(G_1,\dots,G_p):=\left[\frac{\partial G_k}{\partial Y_j}\right]_{\substack{1\le k\le p\\1\le j\le n}}=J(f_1,\dots,f_p)A.$$

Using a similar notation as before, we denote by

$$\widetilde{M}(i_1,\dots,i_p)$$

the p–minor of the new Jacobian $J(G_1,\dots,G_p)$ that corresponds to the columns $1\le i_1<\cdots<i_p\le n$.

Moreover, we denote by $\widetilde{M}_j$ the $p-$ minor $\widetilde{M}(1,\dots,p-1,j)$ determined by the fixed first $p-1$ columns of $J(G_1,\dots,G_p)$ and the column $j\in\{p,\dots,n\}$.

For $p\le r,t\le n$ let $Z_{r,t}$ be a new indeterminate. Using the following regular $(n-p+1)\times(n-p+1)$–parameter matrix

$$Z:=\begin{bmatrix}
1 & 0 & & 0 & & & \cdots & 0\\
Z_{p+1,p} & 1 & & & & & & \\
\vdots & \vdots & \ddots & & \text{O} & & & \vdots\\
Z_{p+i-1,p} & Z_{p+i-1,p+1} & \cdots & 1 & & & & \\
Z_{p+i,p} & Z_{p+i,p+1} & \cdots & Z_{p+i,p+i-1} & 1 & & & \\
\vdots & \vdots & & \vdots & \vdots & \ddots & & 0\\
Z_{n,p} & Z_{n,p+1} & \cdots & Z_{n,p+i-1} & Z_{n,p+i} & Z_{n,p+i+1} & \cdots & 1
\end{bmatrix},$$

we construct an $(n\times n)$–coordinate transformation matrix $A:=A(Z)$, which will enable us to prove the statement at the beginning of this subsection.

For the moment, let us fix an index $1\le i\le n-p$. We consider the formal polar variety W_i outside of the hypersurface $V(m)$. Corresponding to our choice of i, the matrix Z may be subdivided into submatrices as follows:

$$Z=\begin{bmatrix} Z_1^{(i)} & O_{i,n-p-i+1}\\ Z^{(i)} & Z_2^{(i)}\end{bmatrix}.$$

Here the matrix $Z^{(i)}$ is defined as

$$Z^{(i)}:=\begin{bmatrix} Z_{p+i,p} & \dots & Z_{p+i,p+i-1}\\ \dots & \dots & \dots\\ Z_{np} & \dots & Z_{n,p+i-1}\end{bmatrix},$$

and $Z_1^{(i)}$ and $Z_2^{(i)}$ denote the quadratic lower triangular matrices bordering $Z^{(i)}$ in Z, and $O_{i,n-p-i+1}$ is the $i\times(n-p-i+1)$ zero matrix. Let

$$A := A(Z) := \begin{bmatrix} I_{p-1} & O_{p-1,i} & O_{p-1,n-p-i+1} \\ O_{i,p-1} & Z_1^{(i)} & O_{i,n-p-i+1} \\ O_{n-p-i+1,p-1} & Z^{(i)} & Z_2^{(i)} \end{bmatrix}.$$

Here the submatrices I_r and $O_{r,s}$ are unit or zero matrices, respectively, of corresponding size, and $Z^{(i)}, Z_1^{(i)}$, and $Z_2^{(i)}$ are the submatrices of the parameter matrix Z introduced before. Thus, A is a regular, parameter dependent $(n\times n)$–coordinate transformation matrix.

Like the matrix Z, the matrix A contains

$$s := \frac{(n-p)(n-p+1)}{2}$$

parameters $Z_{r,t}$ which we may specialize into any point z of the affine space $\mathbb{C}^s$. For such a point $z\in\mathbb{C}^s$ we denote the corresponding specialized matrices by $A(z)$, $Z_1^{(i)}(z)$, $Z_2^{(i)}(z)$ and $Z^{(i)}(z)$.

We consider now the coordinate transformation given by $X = AY$ with $A = A(Z)$ and calculate the Jacobian $J(G_1,\ldots,G_p)$ with respect to the new polynomials $G_1,\ldots,G_p$. Recall that the coordinate transformation matrix A depends on our previous choice of the index $1\le i\le n-p$.

According to the structure of the coordinate transformation matrix $A = A(Z)$ we subdivide the Jacobian $J(f_1,\ldots,f_p)$ into three submatrices

$$J(f_1,\ldots,f_p) = \begin{bmatrix} U & V & W \end{bmatrix},$$

with

$$U := \left[\frac{\partial f_k}{\partial X_j}\right]_{\substack{1\le k\le p\\ 1\le j\le p-1}},\quad V := \left[\frac{\partial f_k}{\partial X_j}\right]_{\substack{1\le k\le p\\ p\le j\le p+i-1}},\quad W := \left[\frac{\partial f_k}{\partial X_j}\right]_{\substack{1\le k\le p\\ p+i\le j\le n}}.$$

¿From the identity $J(G_1,\ldots,G_p) = J(f_1,\ldots,f_p)\,A$ we deduce that our new Jacobian is of the form:

$$J(G_1,\ldots,G_p) = \left[\frac{\partial G_k}{\partial Y_j}\right]_{\substack{1\le k\le p\\ 1\le j\le n}} = \begin{bmatrix} U & VZ_1^{(i)} + WZ^{(i)} & WZ_2^{(i)}\end{bmatrix}.$$

We are interested in a local description of the i–th formal polar variety $W_i = W_0\cap\Delta_i$ outside of the hypersurface $V(m)$, where m is the fixed upper left $(p-1)$– minor of the Jacobian $J(f_1,\ldots,f_p)$ (and also of its submatrix U). Since the coordinate transformation $X = AY$ leaves the submatrix U unchanged, the $(p-1)$–minor m remains fixed under this transformation. ¿From Proposition 5 we know that the localized determinantal variety $(\Delta_i)_m$ is described by the i equations

$$M_p = 0,\ldots,M_{p+i-1} = 0,$$

(iv) the specialized Jacobian $J(f_1,\ldots,f_p)(x)$ has maximal rank in any point x of $S_0 := W_0\cap\mathbb{R}^n = \{x\in\mathbb{R}^n | f_1(x) = \cdots = f_p(x) = 0\}$ and S_0 is a bounded semialgebraic set (hence, S_0 is empty or a smooth, compact real manifold of dimension $n-p$; see Section 2 for details).

Theorem 11. *Let n,p,d,δ,L and ℓ be natural numbers with $d\ge 2$ and $p\le n$. There exists an arithmetic network $\mathcal{N}$ over $\mathbb{Q}$ of size $\binom{n}{p-1}L(nd\delta)^{O(1)}$ and nonscalar depth $O(n(\log nd+\ell)\log\delta)$ with the following property: Let $f_1,\ldots,f_p$ be a family of n–variate polynomials of a degree at most d and assume that $f_1,\ldots,f_p$ are given by a division-free arithmetic circuit β in $\mathbb{Q}[X_1,\ldots,X_n]$ of size L and nonscalar depth ℓ. Suppose that the polynomials $f_1,\ldots,f_p$ satisfy the conditions (i), (ii), (iii) and (iv) above. Further, suppose that the degree of the real interpretation of the polynomial system $f_1,\ldots,f_p$ is bounded by δ (let us now freely use the notations just introduced before).*

The algorithm represented by the arithmetic network $\mathcal{N}$ starts from the circuit β as input and decides first whether the complex variety $\widetilde{W}_{n-p}$ is empty. If this is not the case, then $\widetilde{W}_{n-p}$ is a zero–dimensional complex variety and the network $\mathcal{N}$ produces an arithmetic circuit in $\mathbb{Q}$ of asymptotically the same size and nonscalar depth as $\mathcal{N}$, which represents the coefficients of $n+1$ univariate polynomials $q,p_1,\ldots,p_n\in\mathbb{Q}[X_n]$ satisfying the following conditions:

$$\deg q = \#\,\widetilde{W}_{n-p},$$

$$\max\{\deg p_k | 1\le k\le n\} < \deg q,$$

$$\widetilde{W}_{n-p} = \{(p_1(u),\ldots,p_n(u)) | u\in\mathbb{C}, q(u) = 0\}.$$

Moreover, the algorithm represented by the arithmetic network $\mathcal{N}$ decides whether the set $\widetilde{W}_{n-p}\cap\mathbb{R}^n$ is empty. If this is not the case, then $\mathcal{N}$ produces at most $\#\,\widetilde{W}_{n-p}\le\delta$ sign sequences belonging to the set $\{-1,0,1\}$ such that these sign sequences encode the real zeros of the polynomial q "à la Thom" ([18]). In this way $\mathcal{N}$ describes the finite, non-empty set $\widetilde{W}_{n-p}\cap\mathbb{R}^n$, which contains at least one representative point for each connected component of the real variety $S_0 = \{x\in\mathbb{R}^n | f_1(x) = \cdots = f_p(x) = 0\}$.

Proof

We shall freely use the notations of Section 2. Any selection of indices $1\le i_1<\cdots< i_p\le n$ and $1\le j,k\le p$ determines a p– minor $M(i_1,\ldots,i_p)$ and a $(p-1)$– minor $m(i_1,\ldots,i_p;j,k)$ of the Jacobian $J(f_1,\ldots,f_p)$ in the following way: $M(i_1,\ldots,i_p)$ is the determinant of the $(p\times p)$– submatrix of $J(f_1,\ldots,f_p)$ with columns $i_1,\ldots,i_p$, and $m(i_1,\ldots,i_p;j,k)$ is the determinant of the matrix obtained from the former one deleting the row number j and the column number i_k. There are $p^2\binom{n}{p}$ such possible selections. Let us fix one of them, say $i_1 := 1,\ldots,i_p := p; j := p, k := p$. Then, using the notations of Section 2, we have $m(i_1,\ldots,i_p;j,k) = m$, $M(i_1,\ldots,i_p) = M_p$. Let us abbreviate $g := mM_p$. ¿From our assumptions on $f_1,\ldots,f_p$ and Theorem 8 and Theorem 10 of Section 2 we deduce the following facts: For any $1\le i\le n-p$ the polynomials $f_1,\ldots,f_p,M_p,\ldots,M_{p+i-1}$ have degree at most pd. They generate the

A (division-free) arithmetic network over $\mathbb{Q}$ is nothing else but an arithmetic circuit that additionally contains decision gates comparing rational values or checking their equality, and selector gates depending on these decision gates.
Arithmetic circuits and networks represent non–uniform algorithms, and the complexity of executing a single arithmetic operation is always counted at unit cost. Nevertheless, by means of well known standard procedures our algorithms will always be transposable to the uniform *random* bit model and they will be practically implementable as well. All this can be done in the spirit of the general asymptotic complexity bounds stated in Theorem 11 below.
Let us also remark that the depth of an arithmetic circuit (or network) measures the *parallel* time of its evaluation, whereas its size allows an alternative interpretation as "number of processors". In this context we would like to emphasize the particular importance of counting only *nonscalar* arithmetic operations (i.e.,only essential multiplications), taking $\mathbb{Q}$-linear operations (in particular, additions/subtractions) for cost–free. This leads to the notion of nonscalar size and depth of a given arithmetic circuit or network β. It can be easily seen that the nonscalar size determines essentially the total size of β (which takes into account all operations) and that the nonscalar depth dominates the degree and height of the intermediate results of β.

An arithmetic circuit (or network) becomes a sequential algorithm when we play a so–called *pebble game* on it. By means of pebble games we are able to introduce a natural space measure in our algorithmic model and along with this, a new, more subtle sequential time measure. If we play a pebble game on a given arithmetic circuit, we obtain a so–called *straight line program (slp)*. In the same way we obtain a *computation tree* from a given arithmetic network. For more details on our complexity model we refer to [11], [25], [26], [45], [53], [38] and especially to [33] (where also the implementation aspect is treated).

In the next Theorem 11 we are going to consider families of polynomials $f_1,\dots,f_p$ belonging to $\mathbb{Q}\,[X_1,\dots,X_n]$, for which we arrange the following assumptions and notations:

(i) $f_1,\dots,f_p$ form a regular sequence in $\mathbb{Q}\,[X_1,\dots,X_n]$,
(ii) for every $1\le k\le p$ the ideal $(f_1,\dots,f_k)$ generated by $f_1,\dots,f_k$ in $\mathbb{Q}\,[X_1,\dots,X_n]$ is radical and defines a subvariety of $\mathbb{C}^n$ of dimension $n-k$ that we denote by $V_k:=V(f_1,\dots,f_k)$.
(iii) the variables $X_1,\dots,X_n$ are in generic position with respect to the polynomials $f_1,\dots,f_p$.

Let $W_0:=\{x\in\mathbb{C}^n|f_1(x)=\dots=f_p(x)=0\}$ and denote by $SingW_0$ the singular locus of W_0. For $1\le i\le n-p$ let W_i be the i–th formal polar variety associated with W_0 and the variables $X_{p+i},\dots,X_n$, and let $\widetilde{W}_i:=\overline{W_i\setminus SingW_0}$ be the i–th polar variety of W_0 in the usual sense (see Section 2 for precise definitions). Further, for $1\le k\le p$ we shall write $\widetilde{V}_k:=\overline{V_k\setminus SingW_0}$. We call

$$\delta:=\max\{\max\{\deg\widetilde{V}_k|1\le k\le p\},\max\{\deg\widetilde{W}_i|1\le i\le n-p\}\}$$

the *degree* (of the real interpretation) *of the polynomial equation system* $f_1,\dots,f_p$.
Finally, let us make the following assumption:

and by the condition $m\neq 0$. The p– minors $M_p,\dots,M_{p+i-1}$ defining these equations are built up by the submatrix $[\,U\;\;V\,]$ of the Jacobian $J(f_1,\dots,f_p)$. Under the coordinate transformation $A(Z)$ the matrix $[\,U\;\;V\,]$ is changed into the submatrix

$$\left[\,U\;\;VZ_1^{(i)}+WZ^{(i)}\right]$$

of the Jacobian $J(G_1,\dots,G_p)$ and the p–minors $M_p,\dots,M_{p+i-1}$ are changed into the p– minors

$$\widetilde{M}_p,\dots,\widetilde{M}_{p+i-1}$$

of the matrix $\left[\,U\;\;VZ_1^{(i)}+WZ^{(i)}\right]$. This implies the matrix identity

$$(**)\qquad \left[\widetilde{M}_p,\dots,\widetilde{M}_{p+i-1}\right]=[M_p,\dots,M_{p+i-1}]\;Z_1^{(i)}+[M_{p+i},\dots,M_n]\;Z^{(i)}.$$

For the previously chosen index $1\le i\le n-p$, the coordinate transformation $X=A(Z)Y$ induces the following morphism of affine spaces:

$$\Phi_i:\;\mathbb{C}^n\times\mathbb{C}^s\to\mathbb{C}^p\times\mathbb{C}^i,$$

defined by

$$(x,z)\longmapsto\Phi_i(x,z):=\Big(\,f_1(x),\dots,f_p(x),\widetilde{M}_p(x,z),\dots,\widetilde{M}_{p+i-1}(x,z)\,\Big).$$

Consider an arbitrary point $z\in\mathbb{C}^s$. We denote by Δ_i^z the determinantal subvariety of $\mathbb{C}^n$ defined by all p–minors of the matrix $\left[\,U\;\;VZ_1^{(i)}(z)+WZ^{(i)}(z)\right]$ (which is a submatrix of the new Jacobian obtained by specializing the coefficients of the polynomials $G_1,\dots,G_p$ into the point $z\in\mathbb{C}^s$). Writing $W_i^z:=W_0\cap\Delta_i^z$, one sees immediately that the zero fiber $\Phi_i^{-1}(0)$ of the morphism Φ_i contains the set

$$(W_i^z)_m:=W_0\cap(\Delta_i^z)_m.$$

In other words, for any arbitrarily chosen point $z\in\mathbb{C}^s$, the zero fiber $\Phi_i^{-1}(0)$ of the morphism Φ_i contains the transformed formal polar variety W_i^z, localized in the hypersurface $V(m)$ and expressed in the old coordinates.

We are going now to analyze the rank of the Jacobian of the morphism Φ_i in an arbitrary point $(x,z)\in\mathbb{C}^n\times\mathbb{C}^s$ with $x\in(W_i^z)_m$. Using the subdivision of the parameter matrix Z into the parts $Z^{(i)}$, $Z_1^{(i)}$ and $Z_2^{(i)}$, the Jacobian $J(\Phi_i)$ of the morphism Φ_i can be written symbolically as

$$J(\Phi_i)=\left[\frac{\partial\Phi_i}{\partial X}\quad\frac{\partial\Phi_i}{\partial Z^{(i)}}\quad\frac{\partial\Phi_i}{\partial Z_1^{(i)}}\quad\frac{\partial\Phi_i}{\partial Z_2^{(i)}}\right].$$

We have

$$\left[\frac{\partial\Phi_i}{\partial X}\quad \frac{\partial\Phi_i}{\partial Z^{(i)}}\right] =$$

$$= \begin{bmatrix} J(f_1,\dots,f_p) & O_{p,n-p-i+1} & \cdots & O_{p,n-p-i+1} \\ * & \left[\frac{\partial\widetilde{M}_p}{\partial Z_{p+i,p}},\dots,\frac{\partial\widetilde{M}_p}{\partial Z_{np}}\right] & \cdots & O_{1,n-p-i+1} \\ \vdots & \vdots & \ddots & \vdots \\ * & O_{1,n-p-i+1} & \cdots & \left[\frac{\partial\widetilde{M}_{p+i-1}}{\partial Z_{p+i,p+i-1}},\dots,\frac{\partial\widetilde{M}_{p+i-1}}{\partial Z_{n,p+i-1}}\right] \end{bmatrix},$$

where the columns correspond to the partial derivatives of Φ_i with respect to the variables

$$X_1,\dots,X_n, Z_{p+i,p},\dots,Z_{n,p},\dots,Z_{p+i,p+i-1},\dots,Z_{n,p+i-1}$$

(in this order). The entries $O_{r,t}$ denote here zero matrices of corresponding size and the row matrices labeled by "$*$" represent the partial derivatives with respect to the variables $X_1,\dots,X_n$ of the minors $\widetilde{M}_p,\dots,\widetilde{M}_{p+i-1}$. These row matrices will be irrelevant for our considerations.

Furthermore, the third submatrix $\left[\frac{\partial\Phi_i}{\partial Z_1^{(i)}}\right]$ of $J(\Phi_i)$ can be written as

$$\begin{bmatrix} O_{p,i-1} & O_{p,i-2} & \cdots & 0 \\ \left[\frac{\partial\widetilde{M}_p}{\partial Z_{p+1,p}},\dots,\frac{\partial\widetilde{M}_p}{\partial Z_{p+i-1,p}}\right] & O_{1,i-2} & \cdots & 0 \\ O_{1,i-1} & \left[\frac{\partial\widetilde{M}_{p+1}}{\partial Z_{p+2,p+1}},\dots,\frac{\partial\widetilde{M}_p}{\partial Z_{p+i-1,p+1}}\right] & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ O_{1,i-1} & O_{1,i-2} & \cdots & \left[\frac{\partial\widetilde{M}_{p+i-1}}{\partial Z_{p+i-1,p+i-2}}\right] \\ O_{1,i-1} & O_{1,i-2} & \cdots & 0 \end{bmatrix}$$

and the last submatrix $\left[\frac{\partial\Phi_i}{\partial Z_2^{(i)}}\right]$ of $J(\Phi_i)$ is a zero matrix since the $p-$ minors $\widetilde{M}_p,\dots,\widetilde{M}_{p+i-1}$ are indepedent of the parameters $Z_{r,t}$ occurring in the submatrix $Z_2^{(i)}$ of the coordinate transformation matrix $A(Z)$.

Therefore, the Jacobian $J(\Phi_i)$ is of full rank $p+i$ wherever the submatrix

$$\widetilde{J}(\Phi_i) := \left[\frac{\partial\Phi_i}{\partial X}\ \frac{\partial\Phi_i}{\partial Z^{(i)}}\right]$$

is of full rank $p+i$. On the other hand, considering the i row matrices contained in $\widetilde{J}(\Phi_i)$ for $p\le j\le p+i-1$

$$\left[\frac{\partial\widetilde{M}_j}{\partial Z_{p+i,j}},\dots,\frac{\partial\widetilde{M}_j}{\partial Z_{n,j}}\right],$$

$$\det\begin{bmatrix} \frac{\partial f_1}{\partial X_1}(b) & \cdots & \frac{\partial f_1}{\partial X_{p-1}}(b) & \frac{\partial f_1}{\partial X_j}(b) \\ \dots & \dots & \dots & \dots \\ \frac{\partial f_p}{\partial X_1}(b) & \cdots & \frac{\partial f_p}{\partial X_{p-1}}(b) & \frac{\partial f_p}{\partial X_j}(b) \end{bmatrix} = 0 \tag{4}$$

holds for every $p\le j\le n-1$. Using our notations for the p–minors of the Jacobian $J(f_1,\dots,f_p)$, we reinterprete now the equations (4) as

$$M_p\,(b) = \ldots = M_{n-1}\,(b) = 0.$$

Since $m(b)\neq 0$ holds by assumption, Proposition 5 implies that b belongs to the localized determinantal variety $(\Delta_{n-p})_m$. Therefore, we have $b\in W_0\cap(\Delta_{n-p})_m$, i.e., the last formal polar variety W_{n-p} contains the point b. On the other hand, b is a nonsingular point of W_0 and belongs therefore to $\widetilde{W}_{n-p} = \overline{W_{n-p}\setminus SingW_0}$. Thus $\widetilde{W}_{n-p}$ is a non–empty set of dimension zero that contains the real point b of the arbitrarily chosen connected component C of the real variety S_0. In particular, $b\in\widetilde{W}_{n-p}\cap\mathbb{R}^n\subset W_i\cap\mathbb{R}^n = S_i$ holds for any $1\le i\le n-p$.

These considerations imply the following result:

Theorem 10. *Let $W_0 := V(f_1,\dots,f_p)$ be as in Theorem 8. If the real variety $S_0 := W_0\cap\mathbb{R}^n$ is non–empty, bounded and smooth, and if the variables $X_1,\dots,X_n$ are in generic position with respect to $f_1,\dots,f_p$, then every real formal polar variety $S_i = W_i\cap\mathbb{R}^n$, $1\le i\le n-p$, is a non–empty, smooth manifold of dimension $n-(p+i)$ and contains at least one representative point of each connected component of the real variety S_0.*

3. Real Equation Solving

The geometric results of Section 2 allow us to design a new efficient procedure that finds at least one representative point in each connected component of a given smooth, compact, real complete intersection variety.

This procedure will be formulated in the algorithmic (complexity) model of (division-free) arithmetic circuits and networks (arithmetic-boolean circuits) over the rational numbers $\mathbb{Q}$.

Roughly speaking, a division-free arithmetic circuit β over $\mathbb{Q}$ is an algorithmic device that supports a step by step evaluation of certain (output) polynomials belonging to $\mathbb{Q}\,[X_1,\dots,X_n]$, say $f_1,\dots,f_p$. Each step of β corresponds either to an input from $X_1,\dots,X_n$, to a constant (circuit parameter) from $\mathbb{Q}$ or to an arithmetic operation (addition/subtraction or multiplication). We represent the circuit β by a labelled *directed acyclic graph (dag).* The size of this dag measures the sequential time requirements of the evaluation of the output polynomials $f_1,\dots,f_p$ performed by the circuit β.

holds for any $x = (x_p, \ldots , x_{n-1}) \in \mathcal{U}$. With respect to this local parametrization, the polynomials f_k, $1 \le k \le p$, induce real valued functions of the form:

$$\tilde{f}_k(X_p, \ldots , X_{n-1}) :=$$

$$f_k(\varphi_1(X_p, \ldots , X_{n-1}), \ldots , \varphi_{p-1}(X_p, \ldots , X_{n-1}),$$

$$X_p, \ldots , X_{n-1}, \varphi_n(X_p, \ldots , X_{n-1})).$$

For every $1 \le k \le p$, and every $p \le j \le n-1$, one has the identity

$$\frac{\partial \tilde{f}_k}{\partial X_j} = \frac{\partial f_k}{\partial X_j} + \frac{\partial f_k}{\partial X_1}\frac{\partial \varphi_1}{\partial X_j} + \cdots + \frac{\partial f_k}{\partial X_{p-1}}\frac{\partial \varphi_{p-1}}{\partial X_j} + \frac{\partial f_k}{\partial X_n}\frac{\partial \varphi_n}{\partial X_j} = 0 \tag{1}$$

in the open set $\mathcal{U}$.
Considering the $(p \times p)$–matrix

$$B := \begin{bmatrix} \dfrac{\partial f_1}{\partial X_1} & \cdots & \dfrac{\partial f_1}{\partial X_{p-1}} & \dfrac{\partial f_1}{\partial X_n} \\ \cdots & \cdots & \cdots & \cdots \\ \dfrac{\partial f_p}{\partial X_1} & \cdots & \dfrac{\partial f_p}{\partial X_{p-1}} & \dfrac{\partial f_p}{\partial X_n} \end{bmatrix},$$

and observing that B is regular in $\mathcal{U}$, we obtain from (1) that

$$-\det B(x) \begin{bmatrix} \dfrac{\partial \varphi_1}{\partial X_j} \\ \vdots \\ \dfrac{\partial \varphi_{p-1}}{\partial X_j} \\ \dfrac{\partial \varphi_n}{\partial X_j} \end{bmatrix} = (Adj\ B)(x) \begin{bmatrix} \dfrac{\partial f_1}{\partial X_j}(x) \\ \vdots \\ \dfrac{\partial f_{p-1}}{\partial X_j}(x) \\ \dfrac{\partial f_p}{\partial X_j}(x) \end{bmatrix} \tag{2}$$

holds for any $x \in \mathcal{U}$ (here $Adj\ B$ denotes the adjoint matrix of the matrix B). As b is a locally maximal point of X_n, we have that

$$\frac{\partial \varphi_n}{\partial X_j}(a) = 0$$

holds for every $p \le j \le n-1$. Thus, equation (2) implies

$$B(n,1)\ (b)\ \frac{\partial f_1}{\partial X_j}\ (b) + \cdots + B(n,p)\ (b)\ \frac{\partial f_p}{\partial X_j}\ (b) = 0 \tag{3}$$

for every $p \le j \le n-1$ (here for $1 \le k \le p$ we denote the entry of the adjoint matrix $Adj\ B$ at the cross point of the k–th column and the last row by $B(n,k)$). Taking into account the particular form of the matrix B, the equation system (3) means that

we see that the representation $(**)$ of the transformed p–minors $\widetilde{M_j}$ implies the identity

$$\left[\frac{\partial \widetilde{M_j}}{\partial Z_{p+i,j}}, \ldots , \frac{\partial \widetilde{M_j}}{\partial Z_{n,j}}\right] = [\ M_{p+i}, \ldots , M_n].$$

Thus, we obtain the representation

$$\widetilde{J}(\Phi_i) = \begin{bmatrix} J(f_1, \ldots , f_p) & O_{p,n-p-i+1} & \cdots & O_{p,n-p-i+1} \\ * & [M_{p+i}, \ldots , M_n] & \cdots & O_{1,n-p-i+1} \\ \vdots & \vdots & \ddots & \vdots \\ * & O_{1,n-p-i+1} & \cdots & [M_{p+i}, \ldots , M_n] \end{bmatrix}.$$

Since all entries of the submatrix $\widetilde{J}(\Phi_i)$ of the Jacobian $J(\Phi_i)$ belong to the polynomial ring $\mathbb{Q}\,[X_1, \ldots , X_n]$, we see that the rank of the matrix $J(\Phi_i)$ in a given point $(x,z) \in \mathbb{C}^n \times \mathbb{C}^s$ with $x \in (W_i^z)_m$ depends only on the choice of x. According to our localization outside of the hypersurface $V(m)$, let us consider an arbitrary smooth point $\tilde{x}$ of $W_0 = V(f_1, \ldots , f_p)$ satisfying the condition $m(\tilde{x}) \neq 0$. Suppose that the submatrix $\widetilde{J}(\Phi_i)(\tilde{x})$ is not of full rank, i.e., that

$$rk\ \widetilde{J}(\Phi_i)(\tilde{x}) < p + i$$

holds. This latter inequality is valid if and only if all p-minors $M_{p+i}, \ldots , M_n$ of the Jacobian $J(f_1, \ldots , f_p)$ vanish at $\tilde{x}$. Let $\tilde{z} \in \mathbb{C}^s$ be any parameter point such that the pair $(\tilde{x}, \tilde{z})$ belongs to the fiber $\Phi_i^{-1}(0)$ of the morphism Φ_i. Since the p-minors $\tilde{M}_p, \ldots , \tilde{M}_{p+i-1}$ of the transformed Jacobian $J(G_1, \ldots , G_p)$ must vanish at $(\tilde{x}, \tilde{z})$, we deduce from $(**)$ that

$$[0, \ldots , 0] = [M_p(\tilde{x}), \ldots , M_{p+i-1}(\tilde{x})]\ Z_1^{(i)}(\tilde{z})$$

holds (here $Z_1^{(i)}(\tilde{z})$ denotes again the matrix obtained by specializing the entries of $Z_1^{(i)}$ into the corresponding coordinates of the point $\tilde{z} \in \mathbb{C}^s$). Because of the lower triangular form of the regular matrix $Z_1^{(i)}$, the latter matrix equation holds if and only if the conditions

$$M_{p+i-1}(\tilde{x}) = \cdots = M_p(\tilde{x}) = 0.$$

are satisfyied. Therefore, our assumptions on $\tilde{x}$ and $\tilde{z}$ imply $m(\tilde{x}) \neq 0$ and $M_p(\tilde{x}) = \cdots = M_n(\tilde{x}) = 0$. However, by Remark 7 this means that the Jacobian $J(f_1, \ldots , f_p)(\tilde{x})$ is singular. Hence, $\tilde{x}$ is not a smooth point of W_0, i.e., $\tilde{x} \in Sing\, W_0$, which contradicts our assumption on $\tilde{x}$.

Now, suppose that we are given a point $(\bar{x}, z) \in \mathbb{C}^n \times \mathbb{C}^s$ that belongs to the fiber $\Phi_i^{-1}(0)$. Then $\bar{x}$ belongs to W_0. Further, suppose that $\bar{x}$ is a smooth point of W_0 outside of the hypersurface $V(m)$. Let us consider the Zariski–open neighbourhood

$\tilde{U}$ of $\bar{x}$ consisting of all points $x \in \mathbb{C}^n$ with $m(x) \neq 0$ and $rk\ J(f_1, \dots, f_p) = p$, i.e., we consider

$$\widetilde{U} := \mathbb{C}^n \setminus (Sing\ W_0 \cup V(m)).$$

We are going to show that the restricted morphism

$$\Phi_i : \tilde{U} \times \mathbb{C}^s \to \mathbb{C}^p \times \mathbb{C}^i$$

is transversal to the origin $0 \in \mathbb{C}^p \times \mathbb{C}^i$.

In order to see this, consider an arbitrary point (x, z) of $\tilde{U} \times \mathbb{C}^s$ that satisfies the equation $\Phi_i(x, z) = 0$. Thus, x belongs to $\tilde{U} \cap W_0$ and is, therefore, a smooth point of W_0, which is outside of the hypersurface $V(m)$. By the preceding considerations on the rank of the Jacobian $J(\Phi_i)$ it is clear that $J(\Phi_i)$ has the maximal rank $p+i$ at (x, z). This means that (x, z) is a regular point of Φ_i. Since (x, z) was an arbitrary point of $\Phi_i^{-1}(0) \cap (\tilde{U} \times \mathbb{C}^s)$, the claimed transversality has been shown.

Now, applying the Weak–Transversality–Theorem of Thom–Sard (see e.g. [22]) to the diagram

$$\begin{array}{ccc} \Phi_i^{-1}(0) \cap (\tilde{U} \times \mathbb{C}^s) & \hookrightarrow & \mathbb{C}^n \times \mathbb{C}^s \\ & \searrow & \downarrow \\ & & \mathbb{C}^s \end{array}$$

one concludes that there is a residual dense set Ω_i of parameters $z \in \mathbb{C}^s$ for which transversality holds. This implies that, for every fixed $z \in \Omega_i$, the transformed and localized formal polar variety

$$W_i^z \setminus (Sing\ W_0 \cup V(m))$$

is either empty or a smooth variety of codimension $p+i$. This variety can be described locally by the polynomials

$$(***) \qquad f_1(X), \dots, f_p(X),\ \widetilde{M}_p(X, z), \dots, \widetilde{M}_{p+i-1}(X, z)$$

that form a regular sequence outside of $SingW_0 \cup V(m)$. Up to now, our considerations concerned only the change of coordinates for an arbitrarily *fixed* $1 \leq i \leq n-p$. However, $\Omega := \bigcap_{i=1}^{n-p} \Omega_i$ is a dense residual parameter set in $\mathbb{C}^s$ from which we can choose a simultaneous change of coordinates for all $1 \leq i \leq n-p$. For every choice $z \in \Omega$ and $1 \leq i \leq n-p$ the transformed formal polar variety W_i^z is, outside of the closed set $SingW_0 \cup V(m)$, a smooth complete intersection variety described by the (local) regular sequence $(***)$. One sees now easily that the affine space $\mathbb{R}^s$ contains a non–empty residual dense set of parameters z such that the conclusions above apply to the coordinate transformation $X = A(z)Y$. Moreover, z can be chosen from $\mathbb{Q}^s$.

Taking into account Proposition 5 and Remark 7, we deduce the following result from our argumentation:

Theorem 8. *Let $W_0 = V(f_1, \dots, f_p)$ be a reduced complete intersection variety given by polynomials $f_1, \dots, f_p$ in $\mathbb{Q}[X_1, \dots, X_n]$ and suppose that the variables $X_1, \dots, X_n$ are in generic position with respect to $f_1, \dots, f_p$. Further, let m be the upper left $(p-1)$–minor of the Jacobian $J(f_1, \dots, f_p)$. Then, every formal polar variety W_i, $1 \leq i \leq n-p$, localized with respect to the closed set $SingW_0 \cup V(m)$, is either empty or a smooth variety of codimension $p+i$ that can be decribed by the equations*

$$f_1, \dots, f_p, M_p, \dots, M_{p+i-1},$$

where M_j, $p \leq j \leq p+i-1$, is the p– minor of the Jacobian $J(f_1, \dots, f_p)$ given by the columns $1, \dots, p-1, j$. Then the polynomials

$$f_1, \dots, f_p, M_p, \dots, M_{p+i-1}$$

form a regular sequence outside of $SingW_0 \cup V(m)$.

Remark 9. *Taking into account that the argumentation on the localization with respect to the fixed $(p-1)$-minor m remains valid mutatis mutandis for any other $(p-1)$-minor $\tilde{m}$ of the Jacobian $J(f_1, \dots, f_p)$, Theorem 8 can be restated for any fixed $(p-1)$–minor just by reordering of columns and rows of the Jacobian $J(f_1, \dots, f_p)$.*

2.4. **Existence of Real Points in the Polar Varieties.** Let $f_1, \dots, f_p$ be a reduced regular sequence in $\mathbb{Q}[X_1, \dots, X_n]$ and let again $W_0 := V(f_1, \dots, f_p)$ be the affine variety defined by $f_1, \dots, f_p$. Consider the real variety $S_0 := W_0 \cap \mathbb{R}^n$ and suppose that

(i) S_0 is nonempty and bounded (and hence compact),
(ii) the Jacobian $J(f_1, \dots, f_p)(x)$ is of maximal rank in all points x of S_0 (i.e., S_0 is a smooth subvariety of $\mathbb{R}^n$ given by the reduced regular sequence $f_1, \dots, f_p$),
(iii) the variables $X_1, \dots, X_n$ are in generic position with respect to the polynomials $f_1, \dots, f_p$.

Further, let C be any connected component of the compact set S_0, and let $b := (a_1, \dots, a_{p-1}, a_p, \dots, a_{n-1}, a_n) \in C$ be a locally maximal point of the last coordinate X_n in the non–empty compact set $C \subset S_0$. Without loss of generality we may assume that the upper left $(p-1)$–minor m of the Jacobian $J(f_1, \dots, f_p)$ does not vanish in b (by our assumptions there must be a $(p-1)$–minor of $J(f_1, \dots, f_p)$ not vanishing at b). In any local parametrization of S_0 at b the variable X_n cannot be an independent variable, since X_n attains a local maximum in b (a_n is this local maximum). Hence, without loss of generality we may assume that the local parametrization of S_0 in b has the following form: there exists an open set $\mathcal{U} \subset \mathbb{R}^{n-p}$ containing the point $a := (a_p, \dots, a_{n-1})$, and a continuously differentiable function

$$\varphi : \mathcal{U} \to \mathbb{R}^p,\ \varphi := (\varphi_1, \dots, \varphi_{p-1}, \varphi_n)$$

such that

$$x_1 = \varphi_1(x_p, \dots, x_{n-1}), \dots, x_{p-1} = \varphi_{p-1}(x_p, \dots, x_{n-1}),$$

$$x_n = \varphi_n(x_p, \dots, x_{n-1})$$