

# The Multivariate Resultant is NP-hard in any Characteristic

Bruno Grenet, Pascal Koiran, and Natacha Portier\*

LIP\*\*, École Normale Supérieure de Lyon, Université de Lyon  
and Department of Computer Science, University of Toronto  
{Bruno.Grenet,Pascal.Koiran,Natacha.Portier}@ens-lyon.fr

Rapport de Recherche RRLIP2009-34

**Abstract.** The multivariate resultant is a fundamental tool of computational algebraic geometry. It can in particular be used to decide whether a system of  $n$  homogeneous equations in  $n$  variables is satisfiable (the resultant is a polynomial in the system's coefficients which vanishes if and only if the system is satisfiable). In this paper we present several NP-hardness results for testing whether a multivariate resultant vanishes, or equivalently for deciding whether a square system of homogeneous equations is satisfiable. Our main result is that testing the resultant for zero is NP-hard under deterministic reductions in any characteristic, for systems of low-degree polynomials with coefficients in the ground field (rather than in an extension). We also observe that in characteristic zero, this problem is in the Arthur-Merlin class AM if the generalized Riemann hypothesis holds true. In positive characteristic, the best upper bound remains PSPACE.

## 1 Introduction

Given two univariate polynomials, their Sylvester matrix is a matrix built on the coefficients of the polynomials which is singular iff the polynomials have a common root. The determinant of the Sylvester matrix is known as the resultant of the polynomials. This determinant is easy to compute since the size of the Sylvester matrix is the sum of the degrees of the polynomials. The study of the possible generalizations to multivariate systems comes within the scope of the theory of elimination [32,26,9,31,10]. This theory proves that the only case where a unique polynomial can testify to the existence of a common root to the system is the case of  $n$  homogeneous polynomials in  $n$  variables: the resultant of a square system of homogeneous polynomials  $f_1, \dots, f_n \in \mathbb{K}[x_1, \dots, x_n]$  is a polynomial in the indeterminate coefficients of  $f_1, \dots, f_n$  which vanishes iff  $f_1, \dots, f_n$  have a nonzero common root in the algebraic closure of  $\mathbb{K}$ . The resultant of such a system is known as the *multivariate resultant* in the literature. This captures the case of two univariate polynomials *modulo* their homogenization. Furthermore, in many cases a system of more than  $n$  homogeneous polynomials in  $n$  variables can be reduced to a system of  $n$  homogeneous

---

\* A part of this work was done during visits to the Fields Institute and the University of Toronto. It was partially funded by the Fields Institute and the European Community (7th PCRD Contract: PIOF-GA-2009-236197).

\*\* UMR 5668 École Normale Supérieure de Lyon – CNRS – UCBL – INRIA.

polynomials, so that the square case is an important one. This result is sometimes known as Bertini's theorem (as explained toward the end of this section, we will use an effective version of this result in one of our NP-hardness proofs). In this paper, we focus on the multivariate resultant which we simply refer to as the resultant.

The resultant has been extensively used to solve polynomial systems [25,28,5,7] and for the elimination of quantifiers in algebraically or real-closed fields [29,15]. More recently, the multivariate resultant has been of interest in pure and applied domains. For instance, the problem of robot motion planning is closely related to the multivariate resultant [3,6], and more generally the multivariate resultant is used in real algebraic geometry [4,20]. Finally, in the domain of symbolic computation progress has been made for finding explicit formulations for the resultant [19,8,2,7,16], see also [18].

**Definition 1.** *Let  $\mathbb{K}$  be a field and  $f_1, \dots, f_n$  be  $n$  homogeneous polynomials in  $\mathbb{K}[x_1, \dots, x_n]$ ,  $f_i(\bar{x}) = \sum_{|\alpha|=d_i} \gamma_{i,\alpha} x^\alpha$ . The multivariate resultant  $R$  of  $f_1, \dots, f_n$  is an irreducible polynomial in  $\mathbb{K}[\overline{\gamma_{i,\alpha}}]$  such that*

$$R(\overline{\gamma_{i,\alpha}}) = 0 \iff \exists \bar{x} \in \overline{\mathbb{K}}, f_1(\bar{x}) = \dots = f_n(\bar{x}) = 0. \quad (1)$$

*The multivariate resultant is unique up to a constant factor.*

The problem we are interested in is testing the resultant for zero. This is the same as deciding whether a square system of homogeneous polynomials (that is  $n$  polynomials in  $n$  variables) has a non-trivial root. This is closely related to the decision problem for the existential theory of an algebraically closed field. This problem is sometimes called the *Hilbert Nullstellensatz* problem:

**Definition 2.** *Let  $\mathbb{K}$  be a field and  $\overline{\mathbb{K}}$  be an algebraic closure of  $\mathbb{K}$ . The Hilbert Nullstellensatz problem over  $\mathbb{K}$ ,  $\text{HN}(\mathbb{K})$ , is the following: Given a system  $f$  of  $s$  polynomials in  $\mathbb{K}[x_0, \dots, x_n]$ , does there exist a root of  $f$  in  $\overline{\mathbb{K}}^{n+1}$ ?*

*Let us now assume that the  $s$  components of  $f$  are homogeneous polynomials. Then the homogeneous Hilbert Nullstellensatz problem over  $\mathbb{K}$ ,  $\text{H}_2\text{N}(\mathbb{K})$ , is to decide whether a non trivial (that is, nonzero) root exists in  $\overline{\mathbb{K}}$ .*

*If  $f$  is supposed to contain as many homogeneous polynomials as variables, the problem is called the square homogeneous Hilbert Nullstellensatz over  $\mathbb{K}$ ,  $\text{H}_2\text{N}^\square(\mathbb{K})$ .*

In the case of the field  $\mathbb{Q}$ , it is more natural to have coefficients in  $\mathbb{Z}$ . We shall use the notations  $\text{HN}$ ,  $\text{H}_2\text{N}$  and  $\text{H}_2\text{N}^\square$  for this case where the system is made of integer polynomials. In the sequel, for any prime number  $p$ , the finite field with  $p$  elements is denoted by  $\mathbb{F}_p$ . The notation is extended to characteristic zero, and  $\mathbb{F}_0 = \mathbb{Q}$ .

In the case of polynomials with coefficients in  $\mathbb{Z}$ , Canny [3] gave in 1987 a PSPACE algorithm to compute the resultant. To the authors' knowledge, this is the best known upper bound. In this paper we show that testing the resultant for zero is NP-hard in any characteristic. In other words,  $\text{H}_2\text{N}(\mathbb{K})$  is NP-hard for any field  $\mathbb{K}$ .

## Main results and proof techniques

In Sect. 2 we observe that for polynomials with integer coefficients, testing the resultant for zero is a problem in the Arthur-Merlin (AM) class. This result assumes the generalized Riemann hypothesis, and follows from a simple reduction to the Hilbert Nullstellensatz. For this problem, membership in AM assuming GRH was established in [21]. The remainder of the paper is devoted to hardness results.

In characteristic zero, it seems to be a "folklore" result that testing the resultant for zero is NP-hard. We give a proof of this fact in Sect. 3 since we have not been able to find one in the literature. In fact, we give two proofs of two results of incomparable strength. The first proof is based on a reduction from the **Partition** problem [13, problem SP12]. The second

proof is based on a result of Plaisted [27] and shows that the problem remains NP-hard for systems of only two homogeneous polynomials. For the latter result to be true, we need to use a sparse encoding for our two polynomials (their degree can therefore be exponential in the input size).

The first proof does not carry over to positive characteristic since the NP-hardness of **Partition** relies in an essential way on the fact that the data are integers (in fact, in any finite field the analogue problem can be solved in polynomial time by dynamic programming).

Plaisted’s result can be adapted to positive characteristic [33,17] but this requires randomization. By contrast, our ultimate goal is NP-hardness for deterministic reductions and low degree polynomials. We therefore need to use different techniques. Our starting point is a fairly standard encoding of **3 – SAT** by systems of polynomial equations. Using this encoding we show at the beginning of Sect. 4 that deciding the existence of a nontrivial solution to a system of homogeneous equations is NP-hard in any characteristic. The resulting system has in general more equations than variables. In order to obtain a square system we explore these two basic strategies:

- (i) Decrease the number of equations.
- (ii) Increase the number of variables.

In Sect. 4.1 we give a randomized NP-hardness result based on the first strategy. The idea is to replace the initial system by a random linear combinations of the system’s equations (the fact this does not change the solution set is sometimes called a “Bertini’s theorem”). In Sect. 4.2 we use the second strategy to obtain two NP-hardness results for deterministic reductions. The main difficulty is to make sure that the introduction of new variables does not create spurious solutions (we do not want to turn an unsatisfiable system into a satisfiable system). Our solution to this problem can be viewed as a derandomization result. Indeed, it can be shown that the coefficients of the monomials where the new variables occur could be chosen at random. It would be interesting to find out whether the proof based on the first strategy can also be derandomized.

## 2 The resultant lies in AM

In this section we show that testing the resultant for zero is reducible to  $\text{HN}(\mathbb{K})$ . In the case  $\mathbb{K} = \mathbb{Z}$ , this allows us to conclude (under the Generalized Riemann Hypothesis) that our problem is in the polynomial hierarchy, and more precisely in the Arthur-Merlin class. In fact, we show that this applies more generally to the satisfiability problem for homogeneous systems (recall that testing the resultant for zero corresponds to the square case).

**Proposition 1.** *For any field  $\mathbb{K}$ , the problem  $\text{H}_2\text{N}(\mathbb{K})$  is polynomial-time many-one reducible to  $\text{HN}(\mathbb{K})$ .*

*Proof.* Consider an instance  $\mathcal{S}$  of  $\text{H}_2\text{N}(\mathbb{K})$ , that is  $s$  homogeneous polynomials  $f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$ . The polynomials  $f_1, \dots, f_s$  can be viewed as elements of  $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_n]$  where  $y_1, \dots, y_n$  are new variables which do not appear in the  $f_i$ . Let  $\mathcal{T}$  be the system containing all the  $f_i$  and the new (non-homogeneous) polynomial  $\sum_{i=1}^n x_i y_i - 1$ . This is an instance of the problem  $\text{HN}(\mathbb{K})$ . It remains to prove that  $\mathcal{S}$  and  $\mathcal{T}$  are equivalent.

Given a root  $(a_1, \dots, a_n, b_1, \dots, b_n)$  of  $\mathcal{T}$ , the new polynomial ensures that there is at least one nonzero  $a_i$ . So  $(a_1, \dots, a_n)$  is a non trivial root of  $\mathcal{S}$ . Conversely, suppose that  $\mathcal{S}$  has a non trivial root  $(a_1, \dots, a_n)$ , and let  $i$  be such that  $a_i \neq 0$ . Then the tuple  $(a_1, \dots, a_n, 0, \dots, 0, a_i^{-1}, 0, \dots, 0)$  where  $a_i^{-1}$  corresponds to the variable  $y_i$  is a root of  $\mathcal{T}$ . Thus  $\text{H}_2\text{N}(\mathbb{K})$  is polynomial-time many-one reducible to  $\text{HN}(\mathbb{K})$ .

Koiran [21] proved that  $\text{HN} \in \text{AM}$  under the Generalized Riemann Hypothesis. We denote here by **AM** the Arthur-Merlin class, defined by *interactive proofs with public coins* (see [1]). Thereby,

**Corollary 1.** *Under the Generalized Riemann Hypothesis,  $\mathsf{H}_2\mathbb{N}$  is in the class AM.*

In positive characteristic, the best upper bound on the complexity of the Hilbert Nullstellensatz known to this day remains PSPACE (in particular it is not known whether the problem lies in the polynomial hierarchy, even assuming some plausible number-theoretic conjecture such as the generalized Riemann hypothesis).

### 3 The resultant is NP-hard in characteristic 0

We now give our first NP-hardness result, for the satisfiability of square systems of homogeneous polynomial equations. As explained in the introduction, this seems to be a “folklore” result. We give the (short) proof since finding an explicit statement (and proof) of this result in the literature appears to be difficult. The second part of the theorem shows that the problems remains NP-hard even for systems with small integer coefficients (i.e., coefficients bounded by 2). This is achieved by a standard trick: we introduce new variables in order to “simulate” large integers coefficients. It is interesting to note, however, that a similar trick for reducing degrees does not seem to apply to the resultant problem (more on this after Theorem 2).

**Theorem 1.** *The problem  $\mathsf{H}_2\mathbb{N}^\square$  of deciding whether a square system of homogeneous polynomials with coefficients in  $\mathbb{Z}$  has a non trivial root is NP-hard.*

*The problem remains NP-hard even if no polynomial has degree greater than 2 and even if the coefficients are bounded by 2.*

*Proof.* The reduction is done from **Partition** which is known to be NP-hard [13, problem SP12]: Given a finite set  $S$  and a non negative integer weight  $w(s)$  for each  $s \in S$ , the problem is to decide the existence of subset  $S'$  such that  $\sum_{s \in S'} w(s) = \sum_{s \notin S'} w(s)$ . That is, the aim is to cut  $A$  into two subsets of same weights.

Given such an instance of **Partition** where  $S = \{s_1, \dots, s_n\}$ , let us define a system of polynomials. For  $1 \leq i \leq n$ ,  $f_i(\bar{x}) = x_0^2 - x_i^2$ . And

$$f_0(x_0, \dots, x_n) = w(s_1)x_1 + w(s_2)x_2 + \dots + w(s_n)x_n. \quad (2)$$

A tuple  $(a_0, \dots, a_n)$  has to verify  $a_i = \pm a_0$  for each  $i$  to be a solution, hence the only case to consider is  $a_0 = 1$  and  $a_i = \pm 1$  for  $i \geq 1$ . Then it is clear that the system has a non trivial solution iff  $S$  may be split into two subsets of equal weights.

For the second part of the theorem, it remains to show that the coefficients in the system can be bounded by 2. As the  $w(s_i)$  may be big integers, they have to be replaced by variables. Let us write  $w(s_i) = \sum_{j=0}^p w_{ij}2^j$ . For each  $w_{ij}$ , a new variable  $W_{ij}$  is introduced. For every  $i$ , the values of the  $W_{ij}$  are defined by a descending recurrence:

$$\begin{cases} W_{ip} - w_{ip}x_0 & = 0 \\ W_{ij} - (2W_{i,j+1} + w_{ij}x_0) & = 0 \quad \text{for all } j < p \end{cases} \quad (3)$$

These equalities imply that for every  $i, j$  we have  $W_{ij} = \sum_{l=j}^p w_{il}2^{j-l}x_0$ . Then  $f_0$  is replaced by  $W_{1,0}x_1 + W_{2,0}x_2 + \dots + W_{n,0}x_n$ . Doing so, the number of polynomials remains the same as the number of variables. Hence, this algorithm build a new homogeneous system where the polynomials have their coefficients bounded by 2 and their degrees too. One can readily check that the new system has a non trivial solution iff the original one has. In particular, if  $x_0$  is set to zero, then all other variables have to be zero too.  $\square$

A related result is Plaisted’s [27] on the NP-hardness of deciding whether the gcd of two sparse univariate polynomials has degree greater than one. By homogenization of the polynomials, this is the same problem as in Theorem 1 for only two bivariate polynomials. Note that the polynomials are sparse and can be of very high degree since exponents are

written in binary (this polynomial representation is sometimes called “supersparse” [17]). If both polynomials were dense, the resultant could be computed in polynomial time since it is equal to the determinant of their Sylvester matrix. Plaisted’s theorem stated in the same language as Theorem 1 is the following:

**Theorem 2.** *Given two sparse homogeneous polynomials in  $\mathbb{Z}[x, y]$ , it is NP-hard to decide whether they share a common root in  $\mathbb{C}^2$ .*

We briefly sketch Plaisted’s reduction since it will help understand the discussion at the end of this section. For a full proof (including a correctness proof), see [27, Theorem 5.1].

*Proof (sketch).* The idea is to turn a 3 – SAT instance into a system of two univariate polynomials which share a common root iff the 3-CNF formula is satisfiable.

To every variable  $X_j$  is associated a prime  $p_j$ , and  $M = \prod p_j$  is defined where the product ranges over all variables that appear in the formula. A formula  $\phi$  is turned into a polynomial  $P_\phi$  according to the following rules. A non negated variable  $X_j$  is turned into  $P_{X_j}(x) = x^{M/p_j} - 1$  and a negated variable  $\neg X_k$  into  $P_{\neg X_k}(x) = 1 + x^{M/p_k} + \dots + x^{(p_k-1)M/p_k}$ . Then a formula  $\phi \vee \psi$  is turned into  $P_{\phi \vee \psi} = \text{lcm}(P_\phi, P_\psi)$ . A conjunction  $\phi = \bigwedge_i \phi_i$  is turned into the polynomial

$$P_\phi(x) = x^M \sum_i P_{\phi_i}(x) P_{\phi_i}(1/x) \quad (4)$$

This defines the first polynomial  $P$ . The second polynomial is simply  $x^M - 1$ . The proof that those two polynomials share a common root iff  $\phi$  is satisfiable is omitted.

To obtain the result in the way we stated it, it is sufficient to homogenize  $P(x)$  and  $x^M - 1$  with the second variable  $y$ .  $\square$

Theorems 1 and 2 seem to be incomparable. In particular, it is not clear how to derive Theorem 1 from Theorem 2. A natural idea would be to introduce new variables and use the repeated squaring trick to reduce the degrees of the polynomials occurring in Plaisted’s result. However, as we now explain this can lead to the creation of unwanted roots at infinity in the resulting polynomial system.

Assume for instance that we wish to get rid of all occurrences of  $x^2$  in a polynomial. One can add a new variable  $x_2$ , replace the occurrences of  $x^2$  by  $x_2$  and add a new polynomial  $x_2 - x^2$ . In order to keep the system homogeneous, the idea is to homogenize the latter polynomial:  $x_0 x_2 - x^2$ . The problem with this technique is that it adds some new roots with all variables but  $x_2$  set to 0, and in particular the homogenization variable  $x_0$ .

To give an explicit example of the problem mentioned above, let us consider the formula

$$(X \vee Y) \wedge (\neg X) \wedge (\neg Y). \quad (5)$$

Let us associate the prime number 2 to the variable  $X$ , and 3 to  $Y$  ( $M$  in the previous proof is therefore 6). By Plaisted’s construction,  $X$  is turned into  $x^{M/2} - 1 = x^3 - 1$  and  $Y$  into  $x^2 - 1$ . Their negations  $\neg X$  and  $\neg Y$  are respectively turned into  $1 + x^3$  and  $1 + x^2 + x^4$ . The disjunction of  $X$  and  $Y$  is turned into the lcm of  $x^3 - 1$  and  $x^2 - 1$ , that is  $(x^2 - 1)(x^2 + x + 1)$ . Finally, we have to apply formula (4) with the latter polynomial,  $1 + x^3$  and  $1 + x^2 + x^4$ . Therefore, the two polynomials of Plaisted’s construction are  $x^M - 1 = x^6 - 1$  and  $-x^3 + x^4 + 2x^5 + 9x^6 + 2x^7 + x^8 - x^9$ . It can be checked that as expected, those two polynomials do not share any common root.

Applying the repeated squaring trick with homogenization on this example gives the following system where the two first polynomials represent the original ones and the other ones are new ones:

$$\begin{cases} -x_3 + x_4 + 2x_5 + 9x_6 + 2x_7 + x_8 - x_9 = 0 \\ x_6 - x_0 = 0; \quad x_0 x_2 - x^2 = 0; \quad x_0 x_3 - x_2 x = 0 \\ x_0 x_4 - x_2^2 = 0; \quad x_0 x_5 - x_4 x = 0; \quad x_0 x_6 - x_2 x_4 = 0 \\ x_0 x_7 - x_4 x_3 = 0; \quad x_0 x_8 - x_4^2 = 0; \quad x_0 x_9 - x_8 x = 0 \end{cases} \quad (6)$$

But in that example, one can easily check that solutions with  $x_0 = 0$  exist. Namely if we set  $x_8$  and  $x_9$  to the same nonzero value and all other variables to 0, this defines a solution to the system.

To the authors' knowledge, there is no solution to avoid these unwanted roots. Furthermore, Plaisted's result works well with fields of characteristic 0, but as it uses the fact that a sum of non negative terms is zero iff every term is zero, this generalizes not so well to positive characteristic. In particular, generalizations to positive characteristic require randomization (see [17] and [33]). By contrast, two of the reductions given in the next section are deterministic and they yield systems with polynomials of low degree (i.e., of linear or even constant degree).

## 4 The resultant is NP-hard in arbitrary characteristic

In this section we give three increasingly stronger NP-hardness results for testing the resultant. As explained in the introduction, we first provide in Sect. 4.1 a NP-hardness proof for randomized reductions. We then give in Sect. 4.2 two NP-hardness results for deterministic reductions: the first one applies to systems with coefficients in an extension of the ground field, and the second (stronger) result to systems with coefficients in the ground field only. The starting point for these three NP-hardness results is the following lemma.

**Lemma 1 ([23]).** *Given a field  $\mathbb{K}$  of any characteristic, it is NP-hard to decide whether a system of  $s$  homogeneous polynomials in  $\mathbb{K}[x_0, \dots, x_n]$  has a non trivial root. That is,  $\text{H}_2\text{N}(\mathbb{K})$  is NP-hard.*

In [23],  $\text{H}_2\text{N}(\mathbb{K})$  was proven NP-hard by reduction from **Boolsys**. An input of **Boolsys** is a system of boolean equations in the variables  $X_1, \dots, X_n$  where each equation is of the form  $X_i = \text{True}$ ,  $X_i = \neg X_j$ , or  $X_i = X_j \vee X_k$ . The question is the existence of a valid assignment for the system, that is an assignment of the variables such that each equation is satisfied. This problem is easily shown NP-hard by reduction from 3-SAT. We now give a proof of this lemma since the specific form of the systems that we construct in the reduction will be useful in the sequel. This proof is a slight variation on the proof from [23].

*Proof.* Let  $\mathbb{K}$  be a field of any characteristic  $p$ ,  $p$  being either zero or a prime number. At first,  $p$  is supposed to be different from 2. The proof has to be slightly changed in the case  $p = 2$  and this case is explained at the end of the proof.

Let  $\mathcal{B}$  be an instance of **Boolsys**. Let us define a system of homogeneous polynomials from this instance with the property that  $\mathcal{B}$  is satisfiable iff the polynomial system has a non trivial common root. The variables in the system are  $x_0, \dots, x_n$  where  $x_i$ ,  $1 \leq i \leq n$ , corresponds to the boolean variable  $X_i$  in **Boolsys**, and  $x_0$  is a new variable. The system contains four kinds of polynomials:

- $x_0^2 - x_i^2$ , for each  $i > 0$ ;
- $x_0 \cdot (x_i + x_0)$ , for each equation  $X_i = \text{True}$  in **Boolsys**;
- $x_0 \cdot (x_i + x_j)$ , for each equation  $X_i = \neg X_j$ ;
- $(x_i + x_0)^2 - (x_j + x_0) \cdot (x_k + x_0)$ , for each equation  $X_i = X_j \vee X_k$ .

Let us denote by  $f$  the polynomial system obtained from  $\mathcal{B}$ . The first kind of polynomials ensures that if  $(a_0, \dots, a_n)$  is a non trivial root of  $f$ , then  $a_0^2 = a_1^2 = \dots = a_n^2$ . Now if  $f$  has a non trivial root  $(a_0, \dots, a_n)$ , then one can readily check that the assignment  $X_i = \text{True}$  if  $a_i = -a_0$  and  $X_i = \text{false}$  if  $a_i = a_0$  satisfies  $\mathcal{B}$ . Conversely, if there is a valid assignment  $X_1, \dots, X_n$  for  $\mathcal{B}$ , any  $(n+1)$ -tuple  $(a_0, \dots, a_n)$  where  $a_0 \neq 0$  and  $a_i = -a_0$  if  $X_i = \text{True}$  and  $a_i = a_0$  if  $X_i = \text{false}$  is a non trivial root of  $f$ .

This proof works for any field of characteristic different from 2. The problem in characteristic 2 is the implementation of **Boolsys** in terms of a system of polynomials. Indeed, for the other characteristics, the truth is represented by  $-a_0$  and the falseness by  $a_0$ . In characteristic 2, those values are equal. Yet, one can just change the polynomials and define in the case of characteristic 2 the following system:

- $x_0x_i - x_i^2$ , for each  $i > 0$ ;
- $x_0(x_i + x_0)$ , for each equation  $X_i = \text{True}$  in **Boolsys**;
- $x_0(x_i + x_j + x_0)$ , for each equation  $X_i = \neg X_j$ ;
- $x_i^2 + x_jx_k + x_0 \cdot (x_j + x_k)$ , for each equation  $X_i = X_j \vee X_k$ .

Now, given any nonzero value  $a_0$  for  $x_0$ , the truth of a variable  $X_i$  is represented by  $x_i = a_0$  whence the falseness is represented by  $x_i = 0$ . A root of the system is in particular a root of the polynomials defined by the first item. Therefore each  $x_i$  has to be set either to  $a_0$  or to 0. The system has a non trivial root iff the instance of **Boolsys** is satisfiable.  $\square$

#### 4.1 A randomized reduction

We now give the first of our three NP-completeness results in positive characteristic. The proof also applies to characteristic zero, but in this case Theorem 1 is preferable (its proof is simpler and the NP-hardness result stronger since it relies on deterministic reductions). For more on randomized reductions, see [1].

**Theorem 3.** *Let  $p$  be either zero or a prime number. The following problem is NP-hard under randomized reductions:*

- *INPUT: a square system of homogeneous equations with coefficients in a finite extension of  $\mathbb{F}_p$ .*
- *QUESTION: is the system satisfiable in the algebraic closure of  $\mathbb{F}_p$ ?*

*In the case  $p = 0$ , the results also holds for systems with coefficients in  $\mathbb{Z}$ .*

*Proof.* Lemma 1 shows that it is NP-hard to decide whether a non square polynomial system  $f$  with coefficients in  $\mathbb{F}_p$  has a non trivial root. From  $f$ , a square system  $g$  is built in randomized polynomial time.

Let us denote by  $f_j$ ,  $1 \leq j \leq s$ , the components of  $f$ . They are homogeneous polynomials in  $\mathbb{F}_p[x_0, \dots, x_n]$ . The components of  $g$  are defined by

$$g_i = \sum_{j=1}^s \alpha_{ij} f_j \quad (7)$$

for  $0 \leq i \leq n$ . In the sequel, we explain how to choose the  $\alpha_{ij}$  for  $f$  and  $g$  to be equivalent. For any choice of the  $\alpha_{ij}$ , a root of  $f$  is a root of  $g$ . Thus it is sufficient to show how to choose the  $\alpha_{ij}$  so that  $g$  has no non trivial root if the same is true for  $f$ .

The property the  $\alpha_{ij}$  have to verify is expressed by a first-order formula:

$$\Phi(\bar{\alpha}) \equiv \forall x_0 \dots \forall x_n \left( \bigwedge_{j=1}^s f_j(\bar{x}) = 0 \right) \vee \left( \bigvee_{i=0}^n \sum_{j=1}^s \alpha_{ij} f_j(\bar{x}) \neq 0 \right). \quad (8)$$

The formula  $\Phi$  belongs to the language of the first-order theory of the algebraically closed field  $\overline{\mathbb{F}_p}$ . This theory eliminates quantifiers and  $\Phi(\bar{\alpha})$  is therefore equivalent to a quantifier-free formula of the form

$$\Psi(\bar{\alpha}) \equiv \bigvee_k \left( \bigwedge_l P_{kl}(\bar{\alpha}) = 0 \wedge \bigwedge_m Q_{km}(\bar{\alpha}) \neq 0 \right), \quad (9)$$

where  $P_{kl}, Q_{km} \in \mathbb{F}_p[\bar{\alpha}]$ . As a special case of [11, Theorem 2], one can bound the number of polynomials in  $\Psi$  as well as their degrees by  $2^{P(n, \log(s+n))}$  where  $P$  is a polynomial independent from  $\Phi$ .

The proof of Theorem 6 (in Appendix) shows that the set  $A$  of tuples satisfying  $\Phi$  is Zariski-dense in  $\overline{\mathbb{F}_p}^{s(n+1)}$ . Since  $A$  is dense, and  $A$  is also defined by  $\Psi$ , one of the clauses of  $\Psi$  must define a Zariski dense subset of  $\overline{\mathbb{F}_p}^{s(n+1)}$ . This clause is of the form  $\bigwedge_m Q_m(\bar{\alpha}) \neq 0$ .

To satisfy  $\Phi$ , it is sufficient for the  $\alpha_{ij}$  to avoid the roots of a polynomial  $Q = \prod_m Q_m$ . As mentioned before, it is known that  $\Psi$  contains at most  $2^{P(n, \log(s+n))}$  polynomials of degree at most  $2^{P(n, \log(s+n))}$ . Thus,  $Q$  is a polynomial of degree at most  $2^{2P(n, \log(s+n))}$ . Consider now a finite extension  $\mathbb{K}$  of  $\mathbb{F}_p$  with at least  $2^{2+2P(n, \log(s+n))}$  elements (that is, of polynomial degree). If we choose the  $\alpha_{ij}$  uniformly at random in  $\mathbb{K}$ , then with probability at least  $3/4$  they are not a root of  $Q$  (by the Schwartz-Zippel Lemma). Thus with the same probability, they satisfy  $\Phi$ . Note that  $\mathbb{K}$  can be built in polynomial-time with Shoup's algorithm [30] when  $p$  is prime (for  $p = 0$ , we take of course  $\mathbb{K} = \mathbb{Q}$ ).

To sum up, we build from  $f$  a square system  $g$  defined by random linear combinations of the components of  $f$ . If  $f$  has a non trivial root, then it is a root of  $g$  too. Conversely, if  $f$  has no non trivial root, then with probability at least  $3/4$  it is also the case that  $g$  has no nontrivial root.  $\square$

In characteristic zero the bounds in the above proof can be sharpened: instead of appealing to the general-purpose quantifier elimination result of [11] we can use a result of [24]. Indeed, it follows from section 4.1 of [24] that there exists a polynomial  $F$  of degree at most  $3^{n+1}$  such that  $F(\bar{\alpha}) \neq 0$  implies that  $g$  has no non trivial root as soon as it is true for  $f$ . This polynomial plays the same role as  $Q$  in the previous proof but the bound on its degree is sharper.

## 4.2 Deterministic Reductions

We now improve the NP-hardness result of Sect. 4.1: we show that the same problem is NP-hard for *deterministic reductions*. This result is not only stronger, but also the proof is more elementary (there is no appeal to effective quantifier elimination).

**Theorem 4.** *Let  $p$  be either zero or a prime number. The following problem is NP-hard under deterministic reductions:*

- *INPUT: a square system of homogeneous equations with coefficients in a finite extension of  $\mathbb{F}_p$ .*
- *QUESTION: is the system satisfiable in the algebraic closure of  $\mathbb{F}_p$ ?*

*In the case  $p = 0$ , the results also holds for systems with coefficients in  $\mathbb{Z}$ .*

*Proof.* The proof of Lemma 1 gives a method to implement an instance of **Boolsys** with a system  $f$  of  $s$  homogeneous polynomials in  $n+1$  variables with coefficients in  $\mathbb{F}_p$ . It remains to explain how to construct a square system  $g$  that has a non trivial root iff  $f$  does. Let us denote by  $f_1, \dots, f_s$  the components of  $f$ , with for each  $i = 1, \dots, n$ ,  $f_i = x_0^2 - x_i^2$  if  $p \neq 2$  and  $f_i = x_0 x_i - x_i^2$  if  $p = 2$ . A new system  $g$  of  $s$  polynomials in  $s$  variables is built. The  $s$  variables are  $x_0, \dots, x_n$  and  $y_1, \dots, y_{s-n-1}$ , that is  $(s - n - 1)$  new variables are added. The system  $g$  is the following:

$$g(\bar{x}, \bar{y}) = \begin{pmatrix} f_1(\bar{x}) \\ \vdots \\ f_n(\bar{x}) \\ f_{n+1}(\bar{x}) & & +\lambda y_1^2 \\ f_{n+2}(\bar{x}) & -y_1^2 & +\lambda y_2^2 \\ & \vdots & \\ f_{n+i}(\bar{x}) & -y_{i-1}^2 & +\lambda y_i^2 \\ & \vdots & \\ f_{s-1}(\bar{x}) & -y_{s-n-2}^2 & +\lambda y_{s-n-1}^2 \\ f_s(\bar{x}) & -y_{s-n-1}^2 & \end{pmatrix} \quad (10)$$

The parameter  $\lambda$  is to be defined later. Clearly, if  $f$  has a non trivial root  $\bar{a}$ , then  $(\bar{a}, \bar{0})$  is a non trivial root of  $g$ . Let us now prove that the converse also holds true for some  $\lambda$ : if  $g$

has a non trivial root, then so does  $f$ . Note that a suitable  $\lambda$  has to be found in polynomial time.

Let  $(a_0, \dots, a_n, b_1, \dots, b_{s-n-1})$  be any non trivial root of  $g$ . Since  $\bar{a}$  must be a common root of  $f_1, \dots, f_n$ , we have  $a_0^2 = \dots = a_n^2$  if  $p \neq 2$ , and  $a_i \in \{0, a_0\}$  for every  $i$  if  $p = 2$ . Now, either  $a_0 = 0$  and  $f_i(\bar{a}) = 0$  for every  $i$ , or  $a_0$  can be supposed to equal 1. Therefore, if  $p \neq 2$  either  $\bar{a} = \bar{0}$  or  $a_i = \pm 1$  for every  $i$ , and if  $p = 2$  either  $\bar{a} = \bar{0}$  or  $a_i \in \{0, 1\}$  for every  $i$ . Let us define  $\epsilon_i = f_{n+i}(\bar{a}) \in \mathbb{F}_p$ . As  $(\bar{a}, \bar{b})$  is a root of  $g$ , the  $b_i^2$  satisfy the linear system

$$\begin{cases} \epsilon_1 & & + & \lambda Y_1 & = & 0, \\ \epsilon_2 & - & Y_1 & + & \lambda Y_2 & = & 0, \\ & & & \vdots & & & \\ \epsilon_{s-n-1} & - & Y_{s-n-2} & + & \lambda Y_{s-n-1} & = & 0, \\ \epsilon_{s-n} & - & Y_{s-n-1} & & & = & 0. \end{cases} \quad (11)$$

This system can be homogenized by replacing each  $\epsilon_i$  by  $\epsilon_i Y_0$  where  $Y_0$  is a fresh variable. This gives a square homogeneous linear system. The determinant of the matrix of this system is equal to  $(-1)^{s-n-1} (\epsilon_1 + \epsilon_2 \lambda + \dots + \epsilon_{s-n} \lambda^{s-n-1})$ .

Let us consider this determinant as a polynomial in  $\lambda$ . This polynomial vanishes identically iff all the  $\epsilon_i$  are zero. In that case, the only solutions satisfy  $Y_i = 0$  for  $i > 0$ , that is  $(\bar{a}, \bar{0})$  is a root of  $g$  and therefore  $\bar{a}$  is a root of  $f$ . If some  $\epsilon_i$  are nonzero, this is a nonzero polynomial of degree  $(s-n-1)$ . If  $\lambda$  can be chosen such that it is not a root of this polynomial (for any possible nonzero value of  $\bar{a}$ ), then the only solution to the linear system is the trivial one. This means that the only non trivial root of  $g$  is  $(\bar{a}, \bar{0})$  where  $\bar{a}$  is a root of  $f$ .

If the polynomials have coefficients in  $\mathbb{Z}$ ,  $\lambda = 3$  (or any other integer  $\lambda > 2$ ) satisfies the condition. Indeed, one can check that  $\epsilon_i = f_{n+i}(\bar{a}) \in \{-4, 0, 2, 4\}$  when  $a_0 = 1$ . The determinant is zero iff  $\epsilon'_1 + \epsilon'_2 \lambda + \dots + \epsilon'_{s-n} \lambda^{s-n-1} = 0$  where  $\epsilon'_i = \epsilon_i / 2 \in \{-2, 0, 1, 2\}$ . For each  $i$ , let  $\epsilon_i^+ = \max\{\epsilon'_i, 0\}$  and  $\epsilon_i^- = \max\{-\epsilon'_i, 0\}$ . Then  $\epsilon'_i = \epsilon_i^+ - \epsilon_i^-$ , and  $0 \leq \epsilon_i^+, \epsilon_i^- \leq 2$ . Now the determinant is zero iff  $\sum_i \epsilon_i^+ 3^i = \sum_i \epsilon_i^- 3^i$ . By the unicity of base-3 representation, this means that for all  $i$ ,  $\epsilon_i^+ = \epsilon_i^-$ , and so  $\epsilon'_i = 0$ .

For a field of positive characteristic, this argument cannot be applied. The idea is to find a  $\lambda$  that is not a root of any polynomial of degree  $(s-n-1)$ . Nothing else can be supposed on the polynomial because if  $\mathbb{F}_p = \mathbb{F}_3$  for example, any polynomial of  $\mathbb{F}_p[\lambda]$  can appear. This also shows that  $\lambda$  cannot be found in the ground field. Suppose an extension of degree  $(s-n)$  is given as  $\mathbb{F}_p[X]/(P)$  where  $P$  is an irreducible degree- $(s-n)$  polynomial with coefficients in  $\mathbb{F}_p$ . Then a root of  $P$  in  $\mathbb{F}_p[X]/(P)$  cannot be a root of a degree- $(s-n-1)$  polynomial with coefficients in  $\mathbb{F}_p$ . Thus, if one can find such a  $P$ , taking for  $\lambda$  the indeterminate  $X$  is sufficient. For any fixed characteristic  $p$ , Shoup gives a deterministic polynomial-time algorithm [30] that given an integer  $N$  outputs a degree- $N$  irreducible polynomial  $P$  in  $\mathbb{F}_p[X]$ . Thus, the system  $g$  is now a square system of polynomials in  $(\mathbb{F}_p[X]/(P))[\bar{x}, \bar{y}]$  and this system has a non trivial root iff  $f$  has a non trivial root. And Shoup's algorithm allows us to build  $g$  in polynomial time from  $f$ .

For any field  $\mathbb{F}_p$ , it has been shown that from an instance  $\mathcal{B}$  of **Boolsys** a square system  $g$  of polynomials with coefficients in an extension of  $\mathbb{F}_p$  (in  $\mathbb{Z}$  for integer polynomials) can be built in deterministic polynomial time such that  $g$  has a non trivial root iff  $\mathcal{B}$  is satisfiable. This shows that the problem is NP-hard.  $\square$

The previous result is somewhat unsatisfactory as it requires, in the case of positive characteristic, to work with coefficients in an extension field rather than in the ground field. A way to get rid of this limitation is now shown. Yet, a property of the previous result is lost. Instead of having constant-degree (even degree-2) polynomials, our next result uses linear-degree polynomials. It is not clear whether the same result can be obtained for degree-2 polynomials (for instance, as explained at the end of Sect. 3 reducing the degree by introducing new variables can create unwanted solutions at infinity).

The basic idea behind Theorem 5 is quite simple (we put the irreducible polynomial used to build the extension field into the system), but some care is required in order to obtain an equivalent homogeneous system.

Recall from the introduction that  $\mathbb{H}_2\mathbb{N}^\square(\mathbb{F}_p)$  is the following problem:

- INPUT: a square system of homogeneous equations with coefficients in  $\mathbb{F}_p$ .
- QUESTION: is the system satisfiable in the algebraic closure of  $\mathbb{F}_p$ ?

**Theorem 5.** *For any prime  $p$ ,  $\mathbb{H}_2\mathbb{N}^\square(\mathbb{F}_p)$  is NP-hard under deterministic reductions.*

*Proof.* The idea for this result is to turn coefficient  $\lambda$  in the previous proof into a variable and to add the polynomial  $P$  as a component of the system. Of course, considering  $\lambda$  as a variable implies that the polynomials are not homogeneous anymore. Thus, it remains to explain how to keep the system homogeneous.

First, the polynomial  $P$  needs to be homogenized. This is done through the variable  $x_0$  in the canonical way. As  $P(\lambda)$  is irreducible, it is in particular not divisible by  $\lambda$ . Hence, the homogenized polynomial  $P(\lambda, x_0)$  contains a monomial  $\alpha\lambda^d$  and another one  $\beta x_0^d$  where  $d$  is the degree of  $P$ . Hence  $x_0$  is zero iff  $\lambda$  is.

The other polynomials have the form  $f_{n+i}(\bar{x}) - y_{i-1}^2 + \lambda y_i^2$ . It is impossible to homogenize those polynomials by multiplying  $f_{n+i}$  and  $y_{i-1}^2$  by  $x_0$  (or any other variable) because then the variable  $y_{i-1}$  never appears alone in a monomial, and a  $s$ -tuple with all variables set to 0 but  $y_{i-1}$  would be a non trivial solution. Moreover, in the previous proof, the fact that the  $y_i$  all appear with degree 2 is used to consider the system as a linear system in the  $y_i^2$ . Thus replacing the monomial  $\lambda y_i^2$  by  $\lambda y_i$  does not work either. Instead, we construct the slightly more complicated homogeneous system:

$$g_h(\bar{x}, \bar{y}, \lambda) = \begin{pmatrix} f_1(\bar{x}) \\ \vdots \\ f_n(\bar{x}) \\ x_0^{s-n-1} f_{n+1}(\bar{x}) & & + \lambda y_1^{s-n} \\ x_0^{s-n-2} f_{n+2}(\bar{x}) & -y_1^{s-n} & + \lambda y_2^{s-n-1} \\ & \vdots & \\ x_0^{s-n-i} f_{n+i}(\bar{x}) & -y_{i-1}^{s-n-i+2} + \lambda y_i^{s-n-i+1} \\ & \vdots & \\ x_0 f_{s-1}(\bar{x}) & -y_{s-n-2}^3 + \lambda y_{s-n-1}^2 \\ f_s(\bar{x}) & -y_{s-n-1}^2 \\ P(\lambda, x_0) \end{pmatrix} \quad (12)$$

Contrary to the previous proof, the  $y_i$  do not appear all at the same power. Yet, all the occurrences of each  $y_i$  have the same degree, and we shall prove that this is sufficient.

Let us prove that if  $f$  does not have any non trivial root, then neither does  $g_h$ . Some of the observations made for  $g$  in the previous proof remain valid. Hence, it is sufficient to prove that a non trivial  $(s+1)$ -tuple  $(\bar{a}, \bar{b}, \ell)$  cannot be solution of  $g_h$  whenever  $a_0 = 1$ ,  $\bar{b} \neq \bar{0}$  and  $a_0^2 = \dots = a_n^2$  if  $p \neq 2$  or  $a_i \in \{0, a_0\}$  if  $p = 2$ . By a previous remark on the polynomial  $P$ ,  $\ell$  can also be supposed to be nonzero.

So, similarly as in the previous proof, let us define  $\epsilon_i = a_0^{s-n-i} f_{n+i}(\bar{a}) \in \mathbb{F}_p$ . In the system  $g_h$ , the variable  $y_i$  only appears at the power  $(s-n-i+1)$ . Therefore, given a value of  $\bar{a}$  and  $\ell$ , the tuple  $(\bar{a}, \bar{b}, \ell)$  is a root of  $g_h$  iff the  $b_i^{s-n-i+1}$  satisfy the linear system

$$\begin{cases} \epsilon_1 & & + & \ell Y_1 & = & 0 \\ \epsilon_2 & - & Y_1 & + & \ell Y_2 & = & 0 \\ & & & \vdots & & & \\ \epsilon_{s-n-1} & - & Y_{s-n-2} & + & \ell Y_{s-n-1} & = & 0 \\ \epsilon_{s-n} & - & Y_{s-n-1} & & & = & 0 \end{cases} \quad (13)$$

This is the same system as in the previous proof. Now if  $(\ell, 1)$  is supposed to be a root of  $P$ , as  $P$  is an irreducible polynomial of degree  $(s - n)$ ,  $\ell$  cannot be a root of a univariate polynomial of degree less than  $(s - n)$  with coefficient in  $\mathbb{F}_p$ . But the determinant of the linear system is such a polynomial, and thus cannot be zero. This determinant is then 0 iff all the  $\epsilon_i = 0$ . The same arguments as in the previous proof can be used to conclude that  $(\bar{a}, \bar{b}, \ell)$  can be a root of  $g_h$  iff  $\bar{a}$  is a root of  $f$ .

Thus, from an instance  $\mathcal{B}$  of **Boolsys**, a square homogeneous system  $g_h$  of polynomials with coefficients in the ground field  $\mathbb{F}_p$  is built in deterministic polynomial time. This system has a non trivial root iff  $\mathcal{B}$  is satisfiable. The result is proved.  $\square$

## 5 Final remarks

In characteristic zero, the upper and lower bounds on  $\mathbb{H}_2\mathbb{N}^\square$  are in a sense close to each other. Indeed,  $\text{NP} = \Sigma_1\text{P} \subseteq \text{AM} \subseteq \Pi_2\text{P}$ , that is, AM lies between the first and the second level of the polynomial hierarchy. Furthermore, “under plausible complexity conjectures,  $\text{AM} = \text{NP}$ ” [1, p157]. Improving the NP lower bound may be challenging as the proof of Proposition 1 shows that this would imply the same lower bound for *Hilbert’s Nullstellensatz*.

In positive characteristic, the situation is quite different. Indeed, the best known upper bound for *Hilbert’s Nullstellensatz* as well as for the resultant is PSPACE. As in characteristic zero, the known upper and lower bounds are therefore the same for both problems. But as the gap between the NP lower bound and the PSPACE upper bound is rather big, these problems might be of widely different complexity (more precisely, testing the resultant for zero could in principle be much easier than deciding whether a general polynomial system is satisfiable). Canny’s algorithm for computing the resultant [3] involves the computation of the determinants of exponential-size matrices, known as Macaulay matrices, in polynomial space. Those matrices admit a succinct representation (in the sense of [12]). One can prove that computing the determinant of a general succinctly represented matrix is FPSPACE-complete (and even testing for zero is PSPACE-complete) [14]. It follows that the FPSPACE upper bound could be improved only by exploiting the specific structure of the Macaulay matrices in an essential way, or by finding an altogether different (non Macaulay-based) approach to this problem. As pointed out in Sect. 2, in characteristic zero a different approach is indeed possible for *testing whether the resultant vanishes* (rather than for computing it). This problem is wide open in positive characteristic.

Finally, an interesting open question is whether the randomized reduction of Theorem 3 can be derandomized.

**Acknowledgments.** We thank Bernard Mourrain and Maurice Rojas for sharing their insights on the complexity of the resultant in characteristic 0.

## References

1. S. Arora and B. Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 1st edition, 2009.
2. L. Busé and C. D’Andrea. On the irreducibility of multivariate subresultants. *CR Math.*, 338(4):287–290, 2004.
3. J. F. Canny. *The complexity of robot motion planning*, volume 1987 of *ACM Doctoral Dissertation Award*. MIT Press, 1988.
4. J. F. Canny. Some algebraic and geometric computations in PSPACE. In *Proc. STOC’88*, pages 460–469, 1988.
5. J. F. Canny, E. Kaltofen, and L. Yagati. Solving systems of nonlinear polynomial equations faster. In *Proc. SIGSAM’89*, pages 121–128, 1989.

6. J. F. Canny and J. H. Reif. New lower bound techniques for robot motion planning problems. In *Proc. FOCS'87*, pages 49–60, 1987.
7. E. Cattani and A. Dickenstein. Introduction to residues and resultants. In A. Dickenstein and I. Emiris, editors, *Solving polynomial equations*, pages 1–61. Springer, 2005.
8. C. D'Andrea and A. Dickenstein. Explicit formulas for the multivariate resultant. *J. Pure Appl. Algebra*, 164(1-2):59–86, 2001.
9. A. Dixon. The eliminant of three quantics in two independent variables. *Proc. Lond. Math. Soc.*, 6:468–478, 1908.
10. I. Emiris and B. Mourrain. Matrices in elimination theory. *J. Symb. Comput.*, 28(1-2):3–43, 1999.
11. N. Fitchas, A. Galligo, and J. Morgenstern. Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields. *J. Pure Appl. Algebra*, 67(1):1–14, 1990.
12. H. Galperin and A. Wigderson. Succinct representations of graphs. *Inform. Control*, 56(3):183–198, 1984.
13. M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. Series of Books in the Mathematical Sciences. W. H. Freeman, 1979.
14. B. Grenet. Difficulté du résultant et des grands déterminants. Technical report, RRLIP2009-32, LIP, 2009. <http://prunel.ccsd.cnrs.fr/ensl-00431714/>.
15. D. Ierardi. Quantifier elimination in the theory of an algebraically-closed field. In *Proc. STOC'89*, pages 138–147, 1989.
16. G. Jeronimo and J. Sabia. Computing multihomogeneous resultants using straight-line programs. *J. Symb. Comput.*, 42(1-2):218–235, 2007.
17. E. Kaltofen and P. Koiran. On the complexity of factoring bivariate supersparse (lacunary) polynomials. In *Proc. ISSAC'05*, pages 208–215. ACM, 2005.
18. E. Kaltofen and P. Koiran. Expressing a fraction of two determinants as a determinant. In *Proc. ISSAC'08*, pages 141–146, 2008.
19. D. Kapur and T. Saxena. Comparison of various multivariate resultant formulations. In *Proc. ISSAC'95*, pages 187–194, 1995.
20. D. Kapur, T. Saxena, and L. Yang. Algebraic and geometric reasoning using Dixon resultants. In *Proc. ISSAC'94*, pages 99–107, 1994.
21. P. Koiran. Hilbert's Nullstellensatz is in the polynomial hierarchy. *J. Complexity*, 12(4):273–286, 1996.
22. P. Koiran. Circuits versus trees in algebraic complexity. In *Proc. STACS'00*, pages 35–54, 2000.
23. P. Koiran. The complexity of local dimensions for constructible sets. *J. Complexity*, 16(1):311–323, 2000.
24. T. Krick, L. Pardo, and M. Sombra. Sharp estimates for the arithmetic Nullstellensatz. *Duke Math. J.*, 109(3):521–598, 2001.
25. D. Lazard. Résolution des systèmes d'équations algébriques. *Theor. Comput. Sci.*, 15(1):77 – 110, 1981.
26. F. Macaulay. Some formulae in elimination. *Proc. Lond. Math. Soc.*, 1(1):3, 1902.
27. D. A. Plaisted. New NP-hard and NP-complete polynomial and integer divisibility problems. *Theor. Comput. Sci.*, 31(1-2):125–138, 1984.
28. J. Renegar. On the worst-case arithmetic complexity of approximating zeros of systems of polynomials. *SIAM J. Comput.*, 18:350, 1989.
29. A. Seidenberg. A new decision method for elementary algebra. *Ann. Math.*, 60(2):365–374, 1954.
30. V. Shoup. New algorithms for finding irreducible polynomials over finite fields. *Math. Comput.*, 54(189):435–447, 1990.
31. B. Sturmfels. Sparse elimination theory. In *Proc. Comput. Algebr. Geom. Commut. Algebra*. D. Eisenbud and L. Robbiano, eds., 1991.

- 32. B. L. van der Waerden. *Modern Algebra*. (third ed.) F. Ungar Publishing Co., New York, 1950.
- 33. J. von zur Gathen, M. Karpinski, and I. Shparlinski. Counting curves and their projections. *Comput. Complex.*, 6(1):64–99, 1996.

## A Appendix

The following result is used in the proof of Theorem 3.

**Theorem 6.** *Let  $\mathbb{K}$  be an algebraically closed field and  $V$  an algebraic variety of  $\mathbb{K}^{n+1}$  defined by a set of homogeneous degree- $d$  polynomials  $f_1, \dots, f_s \in \mathbb{K}[x_0, \dots, x_n]$ . This variety can be defined by  $(n + 1)$  homogeneous degree- $d$  polynomials  $g_1, \dots, g_{n+1} \in \mathbb{K}[x_0, \dots, x_n]$ . Moreover, suitable  $g_i$ 's can be obtained by taking generic linear combinations of the  $f_i$ . That is, we can take  $g_i = \sum_{j=1}^s \alpha_{ij} f_j$  where  $(\alpha_{ij})$  is a matrix of elements of  $\mathbb{K}$ , and the set of suitable matrices is Zariski-dense in  $\mathbb{K}^{s(n+1)}$ .*

*Proof.* A similar result is established in [22, Proposition 1] for arbitrary (possibly non-homogeneous) polynomials: Any algebraic variety of  $\mathbb{K}^n$  can be defined by taking  $n + 1$  generic linear combinations of the original equations. In Theorem 6 the polynomials are assumed to be of same degree to ensure that the linear combinations  $g_i$  are homogeneous. If the  $f_i$  are not of the same degree, the system can be transformed into an equivalent system where the degree of all polynomials is equal to the least common multiple of the degrees of the polynomials in the original system (in the application to Theorem 3, this transformation is not necessary since the input system is made of polynomials of equal degree).

Let  $V_\alpha$  be the variety defined by the  $g_i$ . Clearly,  $V \subseteq V_\alpha$  for any matrix  $\alpha$ . We need to show that there is a Zariski-dense set of matrices  $\alpha$  such that  $V_\alpha \subseteq V$ .

Consider a point  $(a_0, \dots, a_n) \in \mathbb{K}^{n+1}$ . If  $a_0 = 0$ , then one can define new polynomials  $\tilde{f}_j$  and  $\tilde{g}_i$  by setting  $\tilde{f}_j(x_1, \dots, x_n) = f_j(0, x_1, \dots, x_n)$  and  $\tilde{g}_i(x_1, \dots, x_n) = g_i(0, x_1, \dots, x_n)$ . The new polynomials satisfy the same linear relations, namely, we have  $\tilde{g}_i = \sum_{j=1}^s \alpha_{ij} \tilde{f}_j$ . By [22, Proposition 1], there is a Zariski-dense set of matrices  $\alpha$  such that for any tuple  $(a_1, \dots, a_n)$ , if the  $\tilde{g}_i$  vanish on  $(a_1, \dots, a_n)$  the same is true of the  $\tilde{f}_j$ . In this case the  $f_j$  vanish on  $(0, a_1, \dots, a_n)$ , and therefore  $(a_0, \dots, a_n) \in V$ .

It remains to examine the case  $a_0 \neq 0$ . In this case, for any tuple  $(a_0, a_1, \dots, a_n) \in V_\alpha$ , we have  $(1, a_1/a_0, \dots, a_n/a_0) \in V_\alpha$  since the polynomials are homogeneous. The same argument as for the case  $a_0 = 0$  shows that we will have  $(1, a_1/a_0, \dots, a_n/a_0) \in V$  for  $\alpha$  in a Zariski-dense set (we now apply [22, Proposition 1] to the polynomials  $\tilde{f}_j(x_1, \dots, x_n) = f_j(1, x_1, \dots, x_n)$  and  $\tilde{g}_i(x_1, \dots, x_n) = g_i(1, x_1, \dots, x_n)$ ). By appealing again to homogeneity, we can conclude that  $(a_0, \dots, a_n) \in V$ .

From the above analysis it follows that any matrix  $\alpha$  belonging to the intersection of two Zariski-dense sets (corresponding to the two cases  $a_0 = 0$  and  $a_0 \neq 0$ ) is suitable. This concludes the proof since a finite intersection of Zariski-dense sets is Zariski-dense.  $\square$