comput complexity **3** (1993), 31–55 1016-3328/93/010031-25 $1.50+0.20

ALGORITHMIC ASPECTS OF SUSLIN'S PROOF OF SERRE'S CONJECTURE

LEANDRO CANIGLIA, GUILLERMO CORTIÑAS, SILVIA DANÓN, JOOS HEINTZ, TERESA KRICK AND PABLO SOLERNÓ
(WORKING GROUP NOAÏ FITCHAS)

Abstract. Let F be a unimodular $r \times s$ matrix with entries being n-variate polynomials over an infinite field K. Denote by $\deg(F)$ the maximum of the degrees of the entries of F and let $d = 1 + \deg(F)$. We describe an algorithm which computes a unimodular $s \times s$ matrix M with $\deg(M) = (rd)^{O(n)}$ such that $FM = [\mathbf{I}_r, \mathbf{0}]$, where $[\mathbf{I}_r, \mathbf{0}]$ denotes the $r \times s$ matrix obtained by adding to the $r \times r$ unit matrix $\mathbf{I}_r$ $s - r$ zero columns.

We present the algorithm as an arithmetic network with inputs from K, and we count field operations and comparisons as unit cost.

The sequential complexity of our algorithm amounts to $s^{O(r^2)} r^{O(n^2)} d^{O(n^2+r^2)}$ field operations and comparisons in K whereas its parallel complexity is $O(n^4 r^4 \log^2(srd))$.

The complexity bounds and the degree bound for $\deg(M)$ mentioned above are optimal in order. Our algorithm is inspired by Suslin's proof of Serre's Conjecture.

Key words. Serre's Conjecture, Quillen-Suslin Theorem, effective Nullstellensatz, linear equation systems over polynomial rings, complexity.
Subject classifications. 68C25.

1. Introduction

In this paper we consider Suslin's approach (see Lam 1978, Chapter III, §1) to solve Serre's Conjecture under a quantitative algebraic and algorithmic perspective.

By "Serre's Conjecture" we mean the following statement:

Any locally trivial algebraic vector bundle over an affine space is (globally) trivial.

(However, in his historical paper (FAC: Serre 1955) J. P. Serre was only pointing out that no example was known of a nontrivial algebraic vector bundle over an affine space.)

In FAC locally trivial algebraic vector bundles are interpreted as locally free coherent sheaves. This sheaf-theoretical interpretation of vector bundles allows us to reformulate Serre's Conjecture in the following purely algebraic way:

> *Let K be a field and $R = K[X_1, \ldots, X_n]$ the polynomial ring in the indeterminates $X_1, \ldots, X_n$ over K. Any finitely generated projective R-module is free.*

In view of a theorem due to Serre (see Lam 1978, Chapter II, Theorem 5.8) this form of Serre's Conjecture can be reduced to the following statement in terms of linear algebra over the polynomial ring R:

> *Let $F \in R^{r \times s}$ be a unimodular $r \times s$ matrix. There exists a unimodular square matrix $M \in R^{s \times s}$ such that $FM = [\mathbf{I}_r, \mathbf{0}]$, where $[\mathbf{I}_r, \mathbf{0}]$ denotes the $r \times s$ matrix obtained by adding to the $r \times r$ unit matrix $\mathbf{I}_r$ $s - r$ zero columns.*

Quillen and Suslin proved in 1976 independently by different methods this last statement, thus answering Serre's Conjecture positively. (See Lam 1978 and Kunz 1980 for a history of Serre's Conjecture, its motivations and applications.)

In the present article we consider Serre's Conjecture only in this ultimate form. From this point of view Serre's Conjecture represents a particular case of the more general problem of solving linear equation systems in the polynomial ring R.

The quantitative algebraic and algorithmic aspects of this problem were first studied in 1926 in a pioneering paper of G. Hermann (1926) and reconsidered later in (Seidenberg 1974) and in numerous research articles on Gröbner bases (see Buchberger 1985 and the references given there).

The general problem of solving linear equation systems in polynomial rings is exponential space complete and involves necessarily doubly exponential (in the number of variables) degree bounds for the polynomials appearing in the solutions (see Mayr & Meyer 1982, Bayer & Stillman 1988).

As a particular case let us consider the (general) representation problem for polynomial ideals:

> *Given polynomials $f, f_1, \ldots, f_s \in R = K[X_1, \ldots, X_n]$ such that f belongs to the ideal generated by $f_1, \ldots, f_s$ (in symbols: $f \in$*

$(f_1, \ldots, f_s)$), we consider the problem of finding a representation of f, $f = m_1 f_1 + \cdots + m_s f_s$, with $m_1, \ldots, m_s$ in R.

From (Mayr & Meyer 1982) it follows that $m_1, \ldots, m_s$ may have degrees not less than a lower bound which is doubly exponential in n. However, if $f = 1$, the corresponding triviality problem of finding a representation of 1 in R, $1 = m_1 f_1 + \cdots + m_s f_s$, admits a single exponential upper bound for the degrees of $m_1, \ldots, m_s$. More precisely, the following effective Nullstellensatz is true:

Let $f_1, \ldots, f_s \in R = K[X_1, \ldots, X_n]$, $d = \max_{1 \le i \le s} \{\deg(f_i)\}$, (where deg *denotes total degree), and suppose that $n > 1$ and $d \ge 3$. Then $1 \in (f_1, \ldots, f_s)$ if and only if there exist $m_1, \ldots, m_s \in R$ such that $1 = m_1 f_1 + \cdots + m_s f_s$ with $\max_{1 \le i \le s} \{\deg(m_i f_i)\} \le d^n$.*

(See the original papers Brownawell 1987, Caniglia *et al.* 1989, Kollár 1988 or the survey Teissier 1990 and the references given there. Elementary proofs of this theorem can be found in Fitchas & Galligo 1990, Philippon 1988 or Caniglia *et al.* 1990.)

The condition $1 \in (f_1, \ldots, f_s)$ means that the row vector $F = [f_1, \ldots, f_s] \in R^{1 \times s}$ with polynomial entries $f_1, \ldots, f_s$ is unimodular. The Quillen-Suslin Theorem (Lam 1978, Chapter III, Theorem 1.8 and Remark 1.10) says that under these circumstances there exists a unimodular matrix $M \in R^{s \times s}$ such that $FM = [1, 0, \ldots, 0]$. This implies that the first column $\begin{pmatrix} m_1 \\ \vdots \\ m_s \end{pmatrix}$ of M satisfies $1 = m_1 f_1 + \cdots + m_s f_s$.

In particular Suslin's proof of this theorem yields such a unimodular matrix M, thus solving the triviality problem for $(f_1, \ldots, f_s)$. However, the degree and complexity bounds which can be derived revising this proof from an algorithmic point of view are very coarse (see Chaqui 1983 and Logar & Sturmfels 1992 for this approach).

Using the fundamental ideas of Suslin's proof (see Lam 1978, Chapter III, §1) and applying the effective Nullstellensatz mentioned before, the authors of the present paper showed the following quantitative algebraic and algorithmic version of the Quillen-Suslin Theorem (Fitchas & Galligo 1990, Théorème 15):

Let K be an infinite field, let $f_1, \ldots, f_s \in R = K[X_1, \ldots, X_n]$, $d = 1 + \max_{1 \le i \le s} \{\deg(f_i)\}$, and assume that $F = [f_1, \ldots, f_s] \in R^{1 \times s}$ is a unimodular row vector. Then there exists a square matrix $M = [m_{ij}] \in R^{s \times s}$ such that:

(*i*) *M is unimodular,*

(*ii*) $FM = [1, 0, \ldots, 0] \in R^{1 \times s}$,

(*iii*) $\deg(M) = \max_{1 \leq i,j \leq s} \{\deg(m_{ij})\} = d^{O(n)}$, *and*

(*iv*) *M is a product of* $O(n^2 s^2 d^2)$ *matrices, each of them being elementary or having the form* $\begin{pmatrix} T & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{s-2} \end{pmatrix}$ *for some* $T \in SL_2(R)$.

A matrix fulfilling the properties $(i), \ldots, (iv)$ *can be computed in sequential time* $s^4 d^{O(n^2)}$ *and in parallel time* $O(n^4 \log^2 sd)$.

The degree and complexity bounds (item (*ii*) and conclusion) specify the usual form of the Quillen-Suslin Theorem (items (*i*) and (*ii*)). The main feature of these bounds is that they are polynomial in s and d and "only" simply exponential in n. The order of these bounds cannot be improved as is shown by a well-known example due to Mora, Lazard, Masser and Philippon (see Brownawell 1987).

It is now natural to ask whether the general solution of Serre's Conjecture (as introduced before) admits also single exponential degree and complexity bounds. In the present paper we answer this question affirmatively showing the following theorem which was already announced in (Caniglia *et al.* 1989) and (Fitchas & Galligo 1990):

Let K be an infinite field, let $R = K[X_1, \ldots, X_n]$ *and let* $F \in R^{r \times s}$ *be a unimodular matrix with polynomial entries. Let* $d = 1 + \deg(F)$. *Then there exists a square matrix* $M \in R^{s \times s}$ *such that:*

(*i*) *M is unimodular,*

(*ii*) $FM = [\mathbf{I}_r, \mathbf{0}] \in R^{r \times s}$,

(*iii*) $\deg(M) = (rd)^{O(n)}$, *and*

(*iv*) *M is a product of* $O(n^2 s^2 (rd)^{2n})$ *matrices, each of them being elementary or having the form* $\begin{pmatrix} T & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{s-r-1} \end{pmatrix}$ *for some* $T \in SL_{r+1}(R)$.

A matrix M fulfilling the properties $(i), \ldots, (iv)$ *can be computed in sequential time* $s^{O(r^2)} r^{O(n^2)} d^{O(n^2+r^2)}$ *and in parallel time* $O(n^4 r^4 \log^2(srd))$ *by an arithmetic network with entries from K.*

(See von zur Gathen 1986 or Fitchas *et al.* 1990 for the notion of arithmetic network.)

The reader should note that this result cannot be obtained just by iterating the quantitative algebraic and algorithmic version of the Quillen-Suslin Theorem we mentioned above (for this would imply bounds which are doubly exponential in r).

We interpret our result as a particular but relevant case of the general problem of solving linear equation systems in the polynomial ring R having the property that it admits single exponential degree and complexity bounds.

Finally let us observe that our result allows us to compute in single exponential (sequential) time a basis of a free R-module given as the kernel of a unimodular matrix over R (see Corollaries 3.2 and 3.4 below).

2. Preliminaries

NOTATION 2.1. *Let K be an infinite field having an algebraic closure $\overline{K}$ and let $R = K[X_1, \ldots, X_n]$ be the polynomial ring in the n indeterminates $X_1, \ldots, X_n$ over K. Let $Q = [q_{ij}]$ be a polynomial matrix with entries q_{ij} in R. We write:*

$$\deg(Q) = \max_{i,j}\{\deg(q_{ij})\}.$$

(Here, as usual, deg *denotes the total degree in $X_1, \ldots, X_n$.)*

By Q_j we denote the j-th column of Q. If Q has m columns, sometimes we will write $[Q_1, \ldots, Q_m]$. More generally, if $I = (i_1, \ldots, i_r)$ is a sequence of natural numbers with $1 \leq i_1 < \cdots < i_r \leq m$, Q_I denotes the matrix $Q_I = [Q_{i_1}, \ldots, Q_{i_r}]$.

From now on we will fix a matrix $F = [f_{ij}] \in R^{r \times s}$, where $r \leq s$. Let $d = 1 + \deg(F)$. We shall also denote by F the R-linear map

$$\begin{aligned} R^s &\to R^r \\ g &\mapsto g\,{}^tF \end{aligned}$$

where ${}^tF$ is the $s \times r$ matrix obtained by transposing the $r \times s$ matrix F.

REMARK 2.2. *The following conditions are equivalent:*

(*i*) *$F\colon R^s \to R^r$ is an epimorphism.*

(*ii*) *The ideal of R generated by all $r \times r$ subdeterminants of the matrix F is trivial (i.e., it contains the unit $1 \in R$).*

DEFINITION 2.3. *The matrix F is called unimodular if it fulfills the equivalent conditions (i) and (ii) of Remark 2.2.*

EXAMPLE 2.4. *In case $r = 1$ the row matrix $F = [f_1, \ldots, f_s] \in R^{1\times s}$ is unimodular if and only if the ideal $(f_1, \ldots, f_s)$ is trivial.*

EXAMPLE 2.5. *In case $r = s$ the square matrix $F \in R^{s\times s}$ is unimodular if and only if the determinant of F (denoted by $\det(F)$) belongs to $K \setminus \{0\}$; i.e., if and only if F is invertible in $R^{s\times s}$.*

NOTATION 2.6. *$\mathbf{I}_r$ denotes the $r \times r$ identity matrix. If A and B are square matrices, then $A \oplus B$ denotes the block diagonal matrix*

$$\begin{pmatrix} A & \mathbf{0} \\ \mathbf{0} & B \end{pmatrix}.$$

A square matrix is called elementary if it is equal to the identity matrix, except (eventually), for one nonzero entry outside the diagonal. $SL_m(R)$ is the submonoid of $R^{m\times m}$ consisting of all matrices T with $\det(T) = 1$.

REMARK 2.7. *Let $Z = [z_{ij}] \in R^{s\times r}$ be an $s \times r$ matrix. Then FZ is an $r \times r$ matrix which satisfies*

$$\det(FZ) = \sum_I \det(F_I)\det(({}^tZ)_I),$$

where I runs through all sequences of natural numbers $(i_1, \ldots, i_r)$ with $1 \leq i_1 < \cdots < i_r \leq s$. This identity is called the Binet-Cauchy Formula. For a proof see (Gantmacher 1977, Chapter I, §2).

We shall use the following consequence of the Binet-Cauchy Formula: Let $A = [a_{ij}]$ be the unimodular $s \times s$ matrix

$$A = \begin{pmatrix} X_n & 1 & & & & & & & \\ & X_n & 1 & & & & & & \\ & & X_n & \ddots & & & & & \\ & & & \ddots & 1 & & & & \\ & & & & X_n & 1 & & & \\ & & & & & 0 & 1 & & \\ & & & & & & 0 & \ddots & \\ & & & & & & & \ddots & 1 \\ 1 & & & & & & & & 0 \end{pmatrix}$$

i.e.,

$$a_{ij} = \begin{cases} X_n & \text{for } i = j \leq r \\ 1 & \text{for } j = i + 1 \\ 1 & \text{for } i = s,\ j = 1 \\ 0 & \text{in all other places.} \end{cases}$$

Let $F' = FA$ and suppose that $\deg(\det[F_1, \ldots, F_r]) \geq \deg(\det(F_I))$ for all sequences of natural numbers $I = (i_1, \ldots, i_r)$ with $1 \leq i_1 < \cdots < i_r \leq s$. Then $\deg(\det[F'_1, \ldots, F'_r]) > \deg(\det(F'_I))$ for all $I \neq (1, \ldots, r)$. Moreover $\deg(F') \leq d = 1 + \deg(F)$. We choose a product E of elementary matrices such that E permutes the columns of F in such a way that for $\tilde{F} = FE$ the following holds:

$$\deg(\det([\tilde{F}_1, \ldots, \tilde{F}_r]) \geq \deg(\det(\tilde{F}_I)) \quad \text{for all } I = (i_1, \ldots, i_r).$$

Since K is infinite, we may assume, after a suitable linear change of variables, that the polynomial $\det([\tilde{F}_1, \ldots, \tilde{F}_r])$ is monic in all indeterminates $X_1, \ldots, X_n$. Thus we see that replacing F by FEA and performing a linear change of variables, we may make the following assumption.

ASSUMPTION 2.8. *$D = \det[F_1, \ldots, F_r]$ is monic in all indeterminates $X_1, \ldots, X_n$, and $\deg(\det[F_1, \ldots, F_r]) > \deg(\det(F_I))$ for all sequences of natural numbers $I = (i_1, \ldots, i_r)$ with $1 \leq i_1 < \cdots < i_r \leq s$ and $I \neq (1, \ldots, r)$. (Note that this procedure may change d into $d + 1$.)*

3. Results

THEOREM 3.1. *Assume that $F \in R^{r \times s}$ is unimodular. Then there exists a square matrix $M \in R^{s \times s}$ such that:*

(i) M is unimodular,

(ii) $FM = [\mathbf{I}_r, \mathbf{0}] \in R^{r \times s}$,

(iii) $\deg(M) = (rd)^{O(n)}$, and

(iv) M is a product of $O(n^2 s^2 (rd)^{2n})$ matrices, each of them being elementary or having the form $T \oplus \mathbf{I}_{s-r-1}$ for some $T \in SL_{r+1}(R)$.

COROLLARY 3.2. *Assume that $F \in R^{r \times s}$ is unimodular and let $P \subset R^s$ be the kernel of the epimorphism $F\colon R^s \to R^r$. Let $M \in R^{s \times s}$ be a square matrix satisfying properties (i), (ii), (iii) of Theorem 3.1. Then the last $s - r$ columns $M_{r+1}, \ldots, M_s$ of M form a basis of the free R-module P. In particular, P has an R-basis involving only polynomials of degree $(rd)^{O(n)}$.*

THEOREM 3.3. *Assume that $F \in R^{r\times s}$ is unimodular. Then a square matrix $M \in R^{s\times s}$ satisfying properties $(i),\ldots,(iv)$ of Theorem 3.1 can be computed by an arithmetic network with inputs from K in*

$$\text{sequential time } r^{O(n^2)}s^{O(r^2)}d^{O(n^2+r^2)}$$

and

$$\text{parallel time } O(n^4r^4\log^2(srd)).$$

(See von zur Gathen 1986 or Fitchas *et al.* 1990 for the notion of arithmetic network.)

COROLLARY 3.4. *Assume that $F \in R^{r\times s}$ is unimodular. Then an R-basis of the kernel P of the epimorphism $F\colon R^s \to R^r$ involving only polynomials of degree $(rd)^{O(n)}$ can be computed by an arithmetic network within the time bounds of Theorem 3.3.*

The proofs of Corollaries 3.2 and 3.4 from Theorems 3.1 and 3.3 are immediate (see Fitchas & Galligo 1990, Corollaire 14, for details).

In the case that F is a unimodular row (i.e., $r = 1$) Theorems 3.1 and 3.3 correspond to (Fitchas & Galligo 1990, Théorème 15).

Note that Theorem 3.3 implies a constructive solution of Serre's Conjecture (see also Chaqui 1983, Fitchas & Galligo 1990 and Logar & Sturmfels 1992).

4. Proof of Theorem 3.1

For the proof of Theorem 3.1 it suffices to show the following.

PROPOSITION 4.1. *Assume that $F \in R^{r\times s}$ is unimodular. Then there exists a square matrix $M \in R^{s\times s}$ such that:*

(*i*) *M is unimodular,*

(*ii*) *$FM = [f_{ij}(X_1,\ldots,X_{n-1},0)]$ (i.e., FM is equal to the $r \times s$ matrix obtained by specializing the indeterminate X_n to zero in the matrix F),*

(*iii*) *$\deg(M) = (rd)^{O(n)}$, and*

(*iv*) *M is a product of $O(ns^2(rd)2n)$ matrices, each of them being elementary of the form $T \oplus \mathbf{I}_{s-r-1}$ for some $T \in SL_{r+1}(R)$.*

Theorem 3.1 follows then by successively applying Proposition 4.1 to F equal to the matrices:

$$[f_{ij}(X_1,\ldots,X_n)],$$
$$[f_{ij}(X_1,\ldots,X_{n-1},0)],$$
$$\vdots$$
$$[f_{ij}(X_1,\ldots,X_h,0,\ldots,0)],$$
$$\vdots$$
$$[f_{ij}(X_1,0,\ldots,0)].$$

(Here the reader should observe that specializing variables to 0 doesn't increase the degree of the polynomials involved and that unimodularity and Assumption 2.8 are preserved under this procedure. For details we refer to Lam 1978, Chapter III, §1.)

In Proposition 4.1 the indeterminate X_n plays a role different from the one played by $X_1,\ldots,X_{n-1}$. Thus it is convenient to introduce the following notation.

NOTATION 4.2. (*i*) $A = K[X_1,\ldots,X_{n-1}]$,

(*ii*) $t = X_n$ *(thus* $A[t] = R$*)*,

(*iii*) *for all* q, $b \in R$ *let* $q(b) = q(X_1,\ldots,X_{n-1},b)$,

(*iv*) *for any matrix* $Q = [q_{ij}]$ *with entries* $q_{ij} \in R$ *and for any* $b \in R$ *let* $Q(b) = [q_{ij}(b)]$, *and*

(*v*) *we write* $\mathbf{A}^{n-1}$ *for the* $(n-1)$*-dimensional affine space over* $\overline{K}$.

PROCEDURE 4.3. Let us now sketch the main steps of the proof of Proposition 4.1.

Step 1. We construct a sequence of polynomials $c_1,\ldots,c_N \in A$ of degree bounded by $(rd)^2$ and with $N \leq (1+rd)^{2n}$, having the following properties:

- $1 \in (c_1,\ldots,c_N)$; i.e., the ideal of A generated by $c_1,\ldots,c_N$ is trivial,
- for each $1 \leq k \leq N$ there exists a nonsingular $s \times s$ matrix Λ_k with entries from K (in symbols: $\Lambda_k \in GL_s(K)$) such that

$$c_k = \mathrm{Res}_t(\det[F_1^{(k)},\ldots,F_r^{(k)}],\ \det[F_1^{(k)},\ldots,F_{r-1}^{(k)},\ F_{r+1}^{(k)}])$$

where $F_1^{(k)},\ldots,F_s^{(k)}$ are the columns of $F^{(k)} = F\Lambda_k$, and Res_t denotes the resultant with respect to the indeterminate t.

Step 2. As a consequence of the effective Nullstellensatz (Fitchas & Galligo 1990, Théorème 1) one obtains a representation

$$t = a_1 c_1 + \cdots + a_N c_N \qquad \text{with} \quad a_k \in At \subset R$$

and with

$$\max_{1 \le k \le N} \{\deg(a_k c_k)\} \le (rd)^{2n} + 1.$$

Step 3. For each $1 \le k \le N$ we construct a unimodular matrix $M_k \in R^{s \times s}$ (in fact a product of $(r+1)(s-r-1)$ elementary matrices and one matrix of the form $T \oplus \mathbf{I}_{s-r-1}$, where $T \in SL_{r+1}(R)$) such that for $b_k = \sum_{1 \le h \le k} a_h c_h$, $b_{k-1} = \sum_{1 \le h \le k-1} a_h c_h$ and $F^{(k)} = F\Lambda_k$ the following equality holds:

$$F^{(k)}(b_k) M_k = F^{(k)}(b_{k-1}).$$

For $E_k = \Lambda_k M_k \Lambda_k^{-1}$ we therefore obtain $F(b_k)E_k = F(b_{k-1})$; E_k is unimodular, being a product of $(r+1)(r-s-1)+2s^2$ elementary matrices and one matrix of the form $T \oplus \mathbf{I}_{s-r-1}$, where $T \in SL_{r+1}(R)$. Moreover we have

$$\deg(E_k) \le \deg(M_k) \le rd(1+rd)\max\{\deg(b_k), \deg(b_{k-1})\} = (rd)^{O(n)}.$$

Step 4. By Steps 2 and 3 we have

$$\begin{aligned} F = F(t) &= F(b_N), \\ F(b_{N-1}) &= F(b_N)E_N, \\ &\vdots \\ F(b_{k-1}) &= F(b_k)E_k, \\ &\vdots \\ F(0) = F(b_0) &= F(b_1)E_1. \end{aligned}$$

Thus $M = \prod_{1 \le k \le N} E_k$ fulfills properties $(i), \ldots, (iv)$ of Proposition 4.1.

The following two lemmas correspond to (Lam 1978, Chapter III, Lemma 1.4 and Theorem 1.5). Their particular form is due to the circumstance that we need for the proofs of Theorems 3.1 and 3.3 arguments which are almost constructive and which involve only polynomials with controlled degrees. (See also Fitchas & Galligo 1990, Lemma 16 and Lemma 17 for the case where F is a unimodular row, i.e., $r = 1$.)

LEMMA 4.4. *For each $\xi \in \mathbf{A}^{n-1}$ there exists $\Lambda \in GL_s(K)$ such that the following holds: Let $F' = F\Lambda$, $D'_1 = \det[F'_1, \ldots, F'_r]$, $D'_2 = \det[F'_1, \ldots, F'_{r-1}, F'_{r+1}]$ and $c = \mathrm{Res}_t(D'_1, D'_2)$, the resultant of D'_1 and D'_2 with respect to the indeterminate t. Then $c(\xi) \neq 0$.*

PROOF. Let $\xi = (\xi_1, \ldots, \xi_{n-1}) \in \mathbf{A}^{n-1}$ be given; let $K[Y] = K[y_{ij};\ 1 \leq i, j \leq s]$ be the polynomial ring in the s^2 new indeterminates $y_{11}, \ldots, y_{ss}$ over K. By Y we denote the $s \times s$ matrix $[y_{ij}]$ with columns $Y_1, \ldots, Y_s$. We write Y' and Y'' for the $s \times r$ matrices $[Y_1, \ldots, Y_r]$ and $[Y_1, \ldots, Y_{r-1}, Y_{r+1}]$ respectively. Let $F' = FY \in (R \otimes_K K[Y])^{r \times s}$.

From the Binet-Cauchy Formula (Remark 2.7) we see that:

$$\begin{cases} D'_1 = \det[F'_1, \ldots, F'_r] = \sum_I \det(F_I) \det(({}^tY')_I), \text{ and} \\ D'_2 = \det[F'_1, \ldots, F'_{r-1}, F'_{r+1}] = \sum_I \det(F_I) \det(({}^tY'')_I) \end{cases} \tag{4.1}$$

where I runs through all sequences $(i_1, \ldots, i_r)$ such that $1 \leq i_1 < \cdots < i_r \leq s$.

Let $c = c(X_1, \ldots, X_{n-1}, Y) = \mathrm{Res}_t(D'_1, D'_2)$ be the resultant of D'_1 and D'_2 with respect to the indeterminate t.

Claim. $c(\xi, Y) = c(\xi_1, \ldots, \xi_{n-1}, Y) \neq 0$.

Proof of the Claim. By Assumption 2.8 we have $\deg_t(\det[F_1, \ldots, F_r]) > \deg_t(\det(F_I))$ for all sequences of natural numbers $I = (i_1, \ldots, i_r)$ with $1 \leq i_1 < \cdots < i_r \leq s$ and $I \neq (1, \ldots, r)$ (where $\deg_t$ denotes degree in t). Furthermore $\det[F_1, \ldots, F_r]$ is monic in t. Thus Proposition 4.1 implies that $c(\xi, Y) = c(\xi_1, \ldots, \xi_n, Y) = \mathrm{Res}_t(D'_1(\xi, t, Y'), D'_2(\xi, t, Y''))$.

Suppose now that $c(\xi, Y) = 0$. Then there exists $p \in \overline{K}[t, Y]$ with $\deg_t(p) \geq 1$ such that p divides both $D'_1(\xi, t, Y')$ and $D'_2(\xi, t, Y'')$. In particular we have $p \in \overline{K}[t, Y_1, \ldots, Y_{r-1}]$. Let $q \in \overline{K}[t, Y']$ such that

$$pq = D'_1 = \sum_I \det(F_I(\xi, t)) \det(({}^tY')_I). \tag{4.2}$$

Let $\mathcal{J} \subset \overline{K}[t][Y']$ be the ideal generated by all determinants $\det(({}^tY')_I)$. $\mathcal{J}$ is a homogeneous prime ideal. From (4.2) we see that p and q must be homogeneous in Y' and that $\deg_{Y'}(p) + \deg_{Y'}(q) = r$. The polynomial p doesn't belong to $\mathcal{J}$ since it is homogeneous in Y' and independent from Y_r. Since $D'_1 \in \mathcal{J}$ by (4.2) and $\mathcal{J}$ is prime, we conclude $q \in \mathcal{J}$ and $\deg_{Y'}(q) \geq r$. Thus $\deg_{Y'}(p) = 0$, i.e., $p \in \overline{K}[t]$. Now, again by (4.2), we see that p divides all $\det(F_I(\xi, t))$. Remark 2.2 (*ii*) implies that the ideal generated by all polynomials $\det(F_I(\xi, t))$ is trivial. Therefore $p \in \overline{K}$, which contradicts $\deg_t(p) \geq 1$. This finishes the proof of the Claim.

Since K is infinite and since $c(\xi, Y) \neq 0$ there exists $\Lambda = [\lambda_{ij}] \in K^{s\times s}$ such that:

- $\det \Lambda \neq 0$,
- $\det [\lambda_{ij}]_{1\leq i,j\leq r} \neq 0$, and
- $c(\xi, \Lambda) \neq 0$.

Taking into account Assumption 2.8 and (4.1) one verifies immediately that for this Λ the assertion of Lemma 4.4 is true. □

LEMMA 4.5. *Let $D_1 = \det[F_1, \ldots, F_r]$ and $D_2 = \det[F_1, \ldots, F_{r-1}, F_{r+1}]$. Let $c = \mathrm{Res}_t(D_1, D_2)$ be the resultant of D_1 and D_2 with respect to t. Then for all b, $b' \in R$ such that $b \equiv b' \pmod{cR}$ there exists a unimodular matrix $M \in R^{s\times s}$ satisfying:*

(*i*) $F(b)M = F(b')$,

(*ii*) $\deg(M) \leq rd(1 + 2rd)\max\{\deg(b), \deg(b')\}$, *and*

(*iii*) *M is a product of $(r+1)(s-r-1)$ elementary matrices and one matrix of the form $T \oplus \mathbf{I}_{s-r-1}$, where $T \in SL_{r+1}(R)$.*

PROOF. Let g, $h \in R$ such that

$$c = gD_1 + hD_2.$$

Without loss of generality we may assume that $\deg(g)$, $\deg(h)$, $\deg(c) \leq (rd)^2$.

Let b, $b' \in R$ be given with $b - b' \in cR$. There exists for each $r + 2 \leq j \leq s$ a column vector $G_j \in R^{r\times 1}$ such that $F_j(b') - F_j(b) = cG_j$. Let $\beta = \max\{\deg(b), \deg(b')\}$. Observe that $\deg(G_j) \leq d\beta$. Since c doesn't depend on t we have $c = g(b)D_1(b) + h(b)D_2(b)$. Therefore $F_j(b') - F_j(b) = D_1(b)G'_j + D_2(b)G''_j$, where $G'_j = g(b)G_j$ and $G''_j = h(b)G_j$. Observe that $\deg(G'_j)$, $\deg(G''_j) \leq (rd)^2\beta + d\beta$.

Let $B_1 = \mathrm{adj}[F_1(b), \ldots, F_r(b)]$ be the adjoint matrix of the $r \times r$ matrix $[F_1(b), \ldots, F_r(b)]$. Similarly, let B_2 be the adjoint of $[F_1(b), \ldots, F_{r-1}(b), F_{r+1}(b)]$. Thus:

$$D_1(b)G'_j = [F_1(b), \ldots, F_r(b)](B_1G'_j)$$

and

$$D_2(b)G''_j = [F_1(b), \ldots, F_{r-1}(b),\ F_{r+1}(b)](B_2G''_j).$$

From these equalities we conclude that

$$F_j(b') - F_j(b) = g_1 F_1(b) + \cdots + g_{r+1} F_{r+1}(b)$$

for suitable polynomials $g_1, \ldots, g_{r+1} \in R$ of degree bounded by $rd\beta + (rd)^2\beta$. This holds for all $r+2 \leq j \leq s$. Therefore there exists a unimodular matrix M' such that:

- $F(b)M' = [F_1(b), \ldots, F_{r+1}(b),\ F_{r+2}(b'), \ldots, F_s(b')]$,
- $\deg(M') \leq rd\beta + (rd)^2\beta$, and
- M' is a product of $(r+1)(s-r-1)$ elementary matrices.

Let T be the $(r+1) \times (r+1)$ matrix defined by

$$T = \frac{1}{c}\mathrm{adj}\begin{pmatrix} F_1(b) & \ldots & F_r(b) & F_{r+1}(b) \\ 0 & \ldots & -h(b) & g(b) \end{pmatrix}\begin{pmatrix} F_1(b') & \ldots & F_r(b') & F_{r+1}(b') \\ 0 & \ldots & -h(b') & g(b') \end{pmatrix}.$$

Since $b \equiv b' \pmod{cR}$ and $c = c(b) = c(b')$ it is easy to see that $T \in R^{(r+1)\times(r+1)}$ and $\det(T) = 1$. Therefore $T \in SL_{r+1}(R)$. Moreover we have $[F_1(b), \ldots, F_{r+1}(b)]T = [F_1(b'), \ldots, F_{r+1}(b')]$ and $\deg(T) \leq 2(rd)^2\beta + rd\beta$. One sees now easily that $M = M'(T \oplus \mathbf{I}_{s-r-1})$ satisfies $(i), (ii)$ and (iii). □

PROCEDURE 4.6. (**End of the proof of Proposition 4.1**) Since the proof of Proposition 4.1 (and Theorem 3.1) is straightforward linear algebra, we shall assume $\deg(F) \geq 2$. Thus $d \geq 3$.

Step 1. For each $\xi \in \mathbf{A}^{n-1}$ choose $\Lambda_\xi \in GL_s(K)$ as in Lemma 4.4. Let $F^{(\xi)} = F\Lambda_\xi$, $D_1^{(\xi)} = \det[F_1^{(\xi)}, \ldots, F_r^{(\xi)}]$, $D_2^{(\xi)} = \det[F_1^{(\xi)}, \ldots, F_{r-1}^{(\xi)}, F_{r+1}^{(\xi)}]$ and $c_\xi = \mathrm{Res}_t(D_1^{(\xi)}, D_2^{(\xi)})$. Thus $c_\xi(\xi) \neq 0$ and $\deg(c_\xi) \leq (rd)^2$.

The set $\{c_\xi : \xi \in \mathbf{A}^{n-1}\}$ is contained in the K-linear subspace $\mathbf{V}$ of A consisting of all polynomials in $X_1, \ldots, X_{n-1}$ of degree bounded by $(rd)^2$. Let $\{c_1, \ldots, c_N\} \subset \{c_\xi : \xi \in \mathbf{A}^{n-1}\}$ be a basis of the K-linear subspace of $\mathbf{V}$ generated by all c_ξ. One verifies easily:

(i) $1 \in (c_1, \ldots, c_N)$, i.e., the ideal of A generated by $c_1, \ldots, c_N$ is trivial. Moreover we have $\max\limits_{1\leq k\leq N} \{\deg(c_k)\} \leq (rd)^2$.

(ii) $N \leq \dim \mathbf{V} \leq (1+rd)^{2n}$.

(*iii*) For each $1 \leq k \leq N$ there exists $\Lambda_k \in GL_s(K)$ such that

$$c_k = \mathrm{Res}_t(\det[F_1^{(k)}, \ldots, F_r^{(k)}], \det[F_1^{(k)}, \ldots, F_{r-1}^{(k)}, F_{r+1}^{(k)}])$$

where $F^{(k)} = [F_1^{(k)}, \ldots, F_s^{(k)}] = F\Lambda_k$.

Step 2. From Step 1 (*i*) and from the effective Nullstellensatz (Fitchas & Galligo 1990, Théorème 1) we conclude that there exists a representation

$$t = a_1 c_1 + \ldots + a_N c_N \qquad \text{with} \quad a_k \in At$$

and with

$$\max_{1 \leq k \leq N} \{\deg(a_k c_k)\} \leq (rd)^{2n} + 1.$$

(Observe that $d \geq 3$.)

Steps 3 and 4. For $1 \leq k \leq N$ let

$$b_k = \sum_{1 \leq h \leq k} a_h c_h, \qquad b_{k-1} = \sum_{1 \leq h \leq k-1} a_h c_h \qquad \text{and} \quad F^{(k)} = F\Lambda_k.$$

Since by construction

$$c_k = \mathrm{Res}_t(\det[F_1^{(k)}, \ldots, F_r^{(k)}], \det[F_1^{(k)}, \ldots, F_{r-1}^{(k)}, F_{r+1}^{(k)}])$$

(see Step 1) and $b_k \equiv b_{k-1} \pmod{c_k R}$, we can apply Lemma 4.5 to this situation. Therefore there exists a unimodular matrix $M_k \in R^{s \times s}$ satisfying

- $F^{(k)}(b_k)M_k = F^{(k)}(b_{k-1})$,
- $\deg(M_k) \leq rd(1 + 2rd)\max\{\deg(b_k), \deg(b_{k-1})\} = (rd)^{O(n)}$ (see Step 2), and
- M_k is a product of $(r+1)(s-r-1)$ elementary matrices and one matrix of the form $T \oplus \mathbf{I}_{s-r-1}$, where $T \in SL_{r+1}(R)$.

For $E_k = \Lambda_k M_k \Lambda_k^{-1}$ we obtain then $F(b_k)E_k = F(b_{k-1})$.
Finally $M = \prod_{1 \leq k \leq N} E_k$ satisfies properties $(i), \ldots, (iv)$ of Proposition 4.1.

5. Proof of Theorem 3.3

(*i*) Using parallelizable linear algebra over K (see Berkowitz 1984, Chistov 1985, Mulmuley 1986, the survey von zur Gathen 1986 and interpolation techniques as described in Fitchas *et al.* 1990), one immediately deduces Theorem 3.3 if $\deg(F) = 1$ ($d = 2$) or if $s = 1$. Therefore we shall suppose from now on that $d \geq 3$ and $s \geq 2$. The case $r = s$ follows in the same way just by inverting the matrix F. Thus we shall also suppose that $r < s$.

(*ii*) Theorem 3.1 follows from an iterated (n-fold) application of Proposition 4.1 whose proof is almost algorithmic. Only Step 1 of this proof is nonconstructive (see Procedures 4.3 and 4.6). This step is based on Lemma 4.4. In the present section we are going to describe an algorithm which has as output data a finite family $(\Lambda_k, 1 \leq k \leq N)$ of $N = O((sr^2d^2)^r) = (sd)^{O(r^2)}$ matrices $\Lambda_k \in GL_s(K)$ such that for each $\xi \in \mathbf{A}^{n-1}$ there exists $1 \leq k \leq N$ with the following property:

Let $F^{(k)} = [F_1^{(k)}, \ldots, F_s^{(k)}] = F\Lambda_k$ and

$$c_k = \mathrm{Res}_t(\det[F_1^{(k)}, \ldots, F_r^{(k)}], \det[F_1^{(k)}, \ldots, F_{r-1}^{(k)}, F_{r+1}^{(k)}]).$$

Then $c_k(\xi) \neq 0$ (see Lemma 4.4). Thus $1 \in (c_1, \ldots, c_N)$.

Repeating now the arguments of the end of the proof of Proposition 4.1 (see Procedure 4.6), one obtains *constructively* a matrix $M \in R^{s \times s}$ satisfying properties $(i), \ldots, (iv)$ of Proposition 4.1.

Applying this algorithmic version of Proposition 4.1 iteratively (n times), to eliminate successively the variables $X_n, \ldots, X_1$, we obtain Theorem 3.3.

We use the notation introduced in Notations 2.1, 2.6 and 4.2. We make also use of the following additional notation.

NOTATION 5.1. *Let ℓ, m, p be natural numbers and let $Q \in R^{\ell \times m}$.*

(i) Assume $\ell \leq m$. For each sequence $I = (i_1, \ldots, i_p)$ such that $1 \leq i_1 < \cdots < i_p \leq \ell$, Q_I denotes the matrix $[Q_{i_1}, \ldots, Q_{i_p}]$ (see Notation 2.1).

(ii) Assume $\ell > m$. For each sequence $I = (i_1, \ldots, i_r)$ such that $1 \leq i_1 < \cdots < i_p \leq \ell$, Q_I denotes the $p \times m$ matrix whose rows are the rows $i_1 < \cdots < i_p$ of Q.

(iii) We simply say that Q is unimodular if Q or ${}^tQ$ is unimodular in the sense of Definition 2.3).

(iv) In the sequel I_1 will denote the sequence $I_1 = (1, \ldots, r)$ and I_2 the sequence $I_2 = (1, \ldots, r-1, r+1)$.

ASSUMPTION 5.2. *Following Assumption 2.8 we shall assume in the sequel that $\det(F_{I_1})$ is monic in all variables and in particular in t, and that $\deg_t(\det(F_{I_1})) = \deg(\det(F_{I_1})) > \deg(\det(F_I)) \geq \deg_t(\det(F_I))$ for all sequences of natural numbers $I = (i_1, \ldots, i_r)$ with $1 \leq i_1 < \cdots < i_r \leq s$ and $I \neq I_1$.*

ASSUMPTION 5.3. *For each $1 \leq i \leq r$ we choose a finite set $A_i \subset K \setminus \{0\}$ of cardinality*

$$\#(A_i) = \begin{cases} (r+1)d+1 & \text{for } i < r \\ 2r(s-r)d+1 & \text{for } i = r. \end{cases}$$

For each $1 \leq i \leq r-1$ we choose another finite set $B_i \subset K \setminus \{0\}$ such that $\#(B_i) = rsd + 1$.

For each $(\alpha;\beta) = (\alpha_1, \ldots, \alpha_r\,;\, \beta_1, \ldots, \beta_{r-1}) \in \prod_{1\leq i\leq r} A_i \times \prod_{1\leq i\leq r-1} B_i$ we consider the following $s \times s$ matrix :

$$\Lambda_{(\alpha;\beta)} = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \alpha_1 & 1 & \ldots & \cdot & \cdot & \cdot & & \cdot \\ \alpha_1\beta_1 & \alpha_2 & \ldots & \cdot & \cdot & \cdot & & \cdot \\ \cdot & \alpha_2\beta_2 & \ldots & \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \ldots & \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \ldots & 0 & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \ldots & 1 & 0 & \cdot & & \cdot \\ \cdot & \cdot & \ldots & \alpha_{r-1} & 1 & 0 & \ldots & \cdot \\ \cdot & \cdot & \ldots & \alpha_{r-1}\beta_{r-1} & 0 & 1 & \ldots & \cdot \\ \cdot & \cdot & \ldots & \cdot & \cdot & \alpha_r & \ldots & \cdot \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \alpha_1\beta_1^{s-2} & \alpha_2\beta_2^{s-3} & \ldots & \alpha_{r-1}\beta_{r-1}^{s-r} & 0 & \alpha_r^{s-r-1} & \ldots & 1 \end{pmatrix}. \tag{5.3}$$

Thus $\Lambda_{(\alpha;\beta)} = [\lambda_{ij}] \in K^{s\times s}$ is defined by

$$\lambda_{ij} = \begin{cases} 1 & \text{if } i = j \\ \alpha_j\beta_j^{i-j-1} & \text{if } j+1 \leq i \text{ and } j \leq r-1 \\ \alpha_r^{i-j} & \text{if } r+1 \leq j \leq i \\ 0 & \text{if } i < j \text{ or } i \neq j \text{ and } j = r. \end{cases}$$

Note that we have thus defined $N_i = \#(\prod_{1\leq i\leq r} A_i \times \prod_{1\leq i\leq r-1} B_i) = O((r^2sd^2)^r)$ many matrices $\Lambda_{(\alpha;\beta)}$.

NOTATION 5.4. *For the sake of expository simplicity we choose a fixed order of the set of all pairs $(\alpha;\beta)$ just introduced. Thus, if $(\alpha;\beta)$ is the k-th pair in this order, we shall write Λ_k instead of $\Lambda_{(\alpha;\beta)}$, where $1 \le k \le N = (O((r^2sd^2)^r)$. We shall write also $F^{(k)} = F\Lambda_k$.*

LEMMA 5.5. *Let $1 \le i \le r-1$. Then for each $\xi \in \mathbf{A}^{n-1}$ there exists $1 \le k \le N$ such that $F^{(k)}_{(1,\dots,i)}(\xi,t) \in (\overline{K}[t])^{r\times i}$ is unimodular.*

PROOF. We proceed by induction on i.

Case $i = 1$. For $\alpha \in A_1$ and $\beta \in B_1$ we consider the column vector $Q_{\alpha\beta}$ defined by

$$Q_{\alpha\beta} = F_1 + \alpha \sum_{0\le j\le s-2} \beta^j F_{j+2}.$$

Thus, if $(\alpha, \alpha_2, \dots, \alpha_r\,;\, \beta, \beta_2, \dots, \beta_{r-1})$ is the k-th pair in our ordering, we have $Q_{\alpha\beta}(\xi,t) = F^{(k)}_{(1)}$. Therefore it suffices to show the following.

Claim. For each $\xi \in \mathbf{A}^{n-1}$ there exist $\alpha \in A_1$ and $\beta \in B_1$ such that $Q_{\alpha\beta}(\xi,t)$ is unimodular.

Proof of the Claim. Assume that for some given $\xi \in \mathbf{A}^{n-1}$ all column vectors $Q_{\alpha\beta}(\xi,t)$ with $\alpha \in A_1$ and $\beta \in B_1$ are not unimodular. Then, for each $(\alpha;\beta) \in A_1 \times B_1$ there exists $a_{\alpha\beta} \in \overline{K}$ such that $Q_{\alpha\beta}(\xi, a_{\alpha\beta}) = 0$. For $\beta \in B_1$ let $Q_\beta = [F_1, \sum_{0\le j\le s-2} \beta^j F_{j+2}]$. Note that $Q_\beta = [F_1, \alpha^{-1}(Q_{\alpha\beta} - F_1)]$ for any $\alpha \in A_1$.

Let us fix an element $\beta \in B_1$ for the moment. We consider the matrix

$$[Q_\beta, F_2, \dots, F_{r-1}] \in R^{r\times r}.$$

We have

$$\det[Q_\beta, F_2, \dots, F_{r-1}] = \beta^{r-2} \det[F_1, F_r, F_2, \dots, F_{r-1}] + \sum_{r-1\le j\le s-2} \beta^j \det[F_1, F_{j+2}, F_2, \dots, F_{r-1}].$$

Therefore Assumption 5.2 implies that $\det[Q_\beta, F_2, \dots, F_{r-1}]$ is monic in t. Thus $\det[Q_\beta, F_2 \dots, F_{r-1}](\xi,t) \not\equiv 0$ and the Laplace expansion (see Gantmacher 1977, Chapter I, §4) along the two first columns of $[Q_\beta, F_2, \dots, F_{r-1}]$ shows that there exist two rows, say the i_1-th and the i_2-th ones, such that $\det(Q_\beta)_{(i_1,i_2)}(\xi,t) \not\equiv 0$.

Now we observe the following: For any $\alpha \in A_1$ our assumption on ξ says that $Q_{\alpha\beta}(\xi, a_{\alpha\beta}) = 0$ holds. Thus $\operatorname{rank}(Q_\beta(\xi, a_{\alpha\beta})) = \operatorname{rank}[F_1(\xi, a_{\alpha\beta}), \alpha^{-1}(Q_{\alpha\beta} -$

$F_1)(\xi, a_{\alpha\beta})] \leq 1$, where "rank" denotes the rank of the corresponding matrix. Therefore we have $\det((Q_\beta)_{(i_1,i_2)}(\xi, a_{\alpha\beta})) = 0$ for all $\alpha \in A_1$.

Since $\# A_1 \geq 2d+1$ and $\deg(\det((Q_\beta)_{(i_1,i_2)}(\xi,t)) \leq 2d$, we conclude by the pigeonhole principle that there exist two different elements α_1, $\alpha_2 \in A_1$ such that $a_\beta = a_{\alpha_1\beta} = a_{\alpha_2\beta}$. Thus

$$0 = Q_{\alpha_1\beta}(\xi, a_\beta) = F_1(\xi, a_\beta) + \alpha_1 \sum_{0\leq j\leq s-2} \beta^j F_{j+2}(\xi, a_\beta), \text{ and}$$

$$0 = Q_{\alpha_2\beta}(\xi, a_\beta) = F_1(\xi, a_\beta) + \alpha_2 \sum_{0\leq j\leq s-2} \beta^j F_{j+2}(\xi, a_\beta),$$

where $\alpha_1 \neq \alpha_2$ implies that $F_1(\xi, a_\beta) = 0$ and $\sum_{0\leq j\leq s-2} \beta^j F_j(\xi, a_\beta) = 0$.

Now let s vary β over B_1. For each $\beta \in B_1$ we choose an element $a_\beta \in \overline{K}$ such that $F_1(\xi, a_\beta) = 0$ and $\sum_{0\leq j\leq s-2} \beta^j F_j(\xi, a_\beta) = 0$. Let $\sim$ be the equivalence relation on B_1 defined by

$$\beta \sim \beta' \iff a_\beta = a_{\beta'} \qquad \text{for} \quad \beta, \beta' \in B_1.$$

Note that Assumption 5.2 implies $F_1(\xi, t) \neq 0$. On the other hand, we have $\deg(F_1(\xi,t)) \leq d$. Therefore $B_1/\sim$, the set of residue classes of B_1 modulo the equivalence relation $\sim$, satisfies

$$\#(B_1/\sim) \leq d.$$

Taking into account that $\# B_1 \geq (s-2)d + 1$ we see again by the pigeonhole principle that there exists an element $\bar{\beta} \in B_1$ such that $\#\{\beta \in B_1 : \beta \sim \bar{\beta}\} \geq s-1$. We choose now pairwise different elements $\beta_0, \ldots, \beta_{s-2} \in B_1$ such that $\bar{\beta} \sim \beta_i \sim \beta_j$ for $0 \leq i, j \leq s-2$. Let $a = a_{\beta_0} = \cdots = a_{\beta_{s-2}}$. We have

$$F_1(\xi, a) = 0 \qquad \text{and} \qquad \sum_{0\leq j\leq s-2} \beta_i^j F_{j+2}(\xi, a) = 0 \qquad \text{for} \quad 0 \leq i \leq s-2.$$

Since the Vandermonde matrix $[\beta_i^j]_{0\leq i,j\leq s-2}$ is nonsingular, we conclude

$$F_{j+2}(\xi, a) = 0 \qquad \text{for all} \quad 0 \leq j \leq s-2.$$

This conclusion and $F_1(\xi, a) = 0$ imply $F(\xi, a) = 0$ which contradicts the unimodularity of F. This finishes the proof of the Claim and settles the case $i = 1$.

Case $1 < i \leq r-1$. Let $\xi \in \mathbf{A}^{n-1}$. From the induction hypothesis we know that there exists $1 \leq k \leq N$ such that $F^{(k)}_{(1,\ldots,i-1)}(\xi, t)$ is unimodular. For each pair $(\alpha; \beta) \in A_i \times B_i$ let $Q_{\alpha\beta}$ be the $r \times i$ matrix

$$Q_{\alpha\beta} = [F^{(k)}_{(1,\ldots,i-1)}, F_i + \alpha \sum_{0\leq j\leq s-i-1} \beta^j F_{j+i+1}].$$

Thus if the k-th pair in our ordering of $\prod_{1\le i\le r} A_i \times \prod_{1\le i\le r-1} B_i$ has the form

$$(\alpha_1,\dots,\alpha_i,\dots,\alpha_r\,;\,\beta_1,\dots,\beta_i,\dots,\beta_{r-1})$$

we have by definition $Q_{\alpha_i\beta_i} = F^{(k)}_{(1,\dots,i)}$.

Suppose now that the assertion of Lemma 5.5 is wrong for i. Then there exists for each $(\alpha;\beta) \in A_i \times B_i$ an element $a_{\alpha\beta} \in \overline{K}$ such that all $i\times i$ subdeterminants of $Q_{\alpha\beta}(\xi, a_{\alpha\beta})$ are equal to zero, which implies that $\operatorname{rank}(Q_{\alpha\beta}(\xi, a_{\alpha\beta})) \le i-1$.

Let us fix for the moment an element $\beta \in B_i$. Let

$$Q_\beta = [F^{(k)}_{(1,\dots,i-1)},\, F_i\,,\, \sum_{0\le j\le s-i-1} \beta^j F_{j+i+1}].$$

Since $\operatorname{rank}(Q_{\alpha\beta}(\xi, a_{\alpha\beta})) \le i-1$, we have $\operatorname{rank}(Q_\beta(\xi, a_{\alpha\beta})) \le i$ for all $\alpha \in A_i$. Thus for each $\alpha \in A_i$, $\alpha_{\alpha\beta} \in \overline{K}$ is a common zero of all $(i+1)\times(i+1)$ subdeterminants of $Q_\beta(\xi,t)$, considered as elements of the polynomial ring $\overline{K}[t]$.

Now we are going to show that at least one $(i+1)\times(i+1)$ subdeterminant of $Q_\beta(\xi,t)$ is different from zero. We consider the matrix $[Q_\beta, F_{i+1},\dots,F_{r-1}] \in R^{r\times r}$. Since Λ_k has the lower triangular from (5.3), the multilinearity of the determinant function and the Binet-Cauchy Formula (Remark 2.7) imply that

$$\begin{aligned}\det[Q_\beta, F_{i+1},\dots,F_{r-1}] &= \beta^{s-i-1}\det[F_1,\dots,F_i,F_r,F_{i+1},\dots,F_{r-1}]\\ &\quad + \sum_{I\ne I_1} c_I \det(F_I)\end{aligned}$$

for some $c_i \in K$. By virtue of Assumption 5.2 this implies that $\det[Q_\beta, F_{i+1},\dots,F_{r-1}]$ is monic in t. Therefore $\det[Q_\beta, F_{i+1},\dots,F_{r-1}](\xi,t) \ne 0$. The Laplace expansion of this determinant along its $(i+1)$ first columns shows that there exists a sequence I of $i+1$ rows of Q_β such that $\det((Q_\beta)_I(\xi,t)) \ne 0$. Observe that $\deg(\det((Q_\beta)_I(\xi,t))) \le (i+1)d$ and that $\#A_i \ge (i+1)d+1$. Thus there exist by the pigeonhole principle two different elements $\alpha_1, \alpha_2 \in A_i$ such that $a_\beta = a_{\alpha_1\beta} = a_{\alpha_2\beta}$. Since by the induction hypothesis $F^{(k)}_{(1,\dots,i-1)}(\xi,t)$ is unimodular we conclude that $\operatorname{rank}(F^{(k)}_{(1,\dots,i-1)}(\xi,a_\beta)) = i-1$. On the other hand $F^{(k)}_{(1,\dots,i-1)}(\xi,a_\beta)$ is a submatrix of $Q_{\alpha_1\beta}(\xi,a_\beta)$ and of $Q_{\alpha_2\beta}(\xi,a_\beta)$, which have rank at most $i-1$. Hence

$$i-1 = \operatorname{rank}(F^{(k)}_{(1,\dots,i-1)}(\xi,a_\beta)) = \operatorname{rank}(Q_{\alpha_1\beta}(\xi,a_\beta)) = \operatorname{rank}(Q_{\alpha_2\beta}(\xi,a_\beta)).$$

This means that the column vectors

$$F_i(\xi,a_\beta) + \alpha_1 \sum_{0\le j\le s-i-1} \beta^j F_{j+i+1}(\xi,a_\beta)$$

and

$$F_i(\xi, a_\beta) + \alpha_2 \sum_{0 \le j \le s-i-1} \beta^j F_{j+i+1}(\xi, a_\beta)$$

are linearly dependent from the column vectors of $F^{(k)}_{(1,\ldots,i-1)}(\xi, a_\beta)$. Since $\alpha_1 \neq \alpha_2$ this implies that

$$\begin{aligned} \operatorname{rank}([F^{(k)}_{(1,\ldots,i-1)}, F_i](\xi, a_\beta)) &= \operatorname{rank}([F^{(k)}_{(1,\ldots,i-1)}, \sum_{0 \le j \le s-i-1} \beta^j F_{j+i+1}](\xi, a_\beta)) \\ &= i - 1. \end{aligned}$$

By an argument similar to the one just used, we conclude that at least one $i \times i$ subdeterminant of

$$[F^{(k)}_{(1,\ldots,i-1)}, F_i](\xi, t)$$

is different from zero. Since $\operatorname{rank}([F^{(k)}_{(1,\ldots,i-1)}, F_i](\xi, a_\beta)) = i - 1$, a_β is a zero of this nonvanishing $i \times i$ subdeterminant of $[F^{(k)}_{(1,\ldots,i-1)}, F_i](\xi, t)$, which has degree at most id. Thus, if β varies over B_i, we see that

$$\#\{a_\beta : \beta \in B_i\} \le id.$$

Since $\# B_i \ge i(s-i-1)d + 1$ we conclude by the pigeonhole principle that there exist pairwise different elements $\beta_0, \ldots, \beta_{s-i-1} \in B_i$ such that $a = a_{\beta_0} = \cdots = a_{\beta_{s-i-1}}$. Therefore the column vectors

$$F_i(\xi, a)$$

and

$$\sum_{0 \le j \le s-i-1} \beta_\ell^j F_{j+i+1}(\xi, a), \qquad \text{for} \quad 0 \le \ell \le s-i-1,$$

belong to the $\overline{K}$-linear vector space generated by $F_1^{(k)}(\xi, a), \ldots, F_{i-1}^{(k)}(\xi, a)$, the column vectors of $F^{(k)}_{(1,\ldots,i-1)}(\xi, a)$.

Since the Vandermonde matrix

$$[\beta_\ell^j]_{0 \le j, \ell \le s-i-1}$$

is regular we conclude that $F_i(\xi, a)$, $F_{i+1}(\xi, a), \ldots, F_s(\xi, a)$ belong to the $\overline{K}$ linear space generated by $F_1^{(k)}(\xi, a), \ldots, F_{i-1}^{(k)}(\xi, a)$. Hence

$$\begin{aligned} & \operatorname{rank}[F^{(k)}_{(1,\ldots,i-1)}, F_i, \ldots, F_s](\xi, a) \\ = \; & \operatorname{rank}[F_1^{(k)}(\xi, a), \ldots, F_{i-1}^{(k)}(\xi, a), F_i(\xi, a), \ldots, F_s(\xi, a)] \\ = \; & i - 1. \end{aligned}$$

On the other hand let $\Lambda \in K^{s\times s}$ be the matrix we obtain by taking the first $i-1$ column vectors of Λ_k and adding to them the last $s-i+1$ column vectors of the identity matrix $\mathbf{I}_s$, i.e.,

$$\Lambda = [(\Lambda_k)_1, \ldots, (\Lambda_k)_{i-1}, (\mathbf{I}_s)_i, \ldots, (\mathbf{I}_s)_s].$$

From (5.3) we see that Λ is regular. Thus $[F^{(k)}_{(1,\ldots,i-1)}, F_i, \ldots, F_s] = F\Lambda$ is unimodular. This implies $\operatorname{rank}[F^{(k)}_{(1,\ldots,i-1)}, F_i, \ldots, F_s](\xi, a) = r$. This leads to a contradiction, and thereby finishes the proof of Lemma 5.5. □

PROPOSITION 5.6. *(See Lemma 4.4.) For each $\xi \in \mathbf{A}^{n-1}$ there exists $(\alpha;\beta) \in \prod_{1\le i\le r} A_i \times \prod_{1\le i\le r-1} B_i$ with the following property. Let*

$$F' = F\Lambda_{(\alpha;\beta)}, \quad D'_1 = \det[F'_1, \ldots, F'_r], \quad D'_2 = \det[F'_2, \ldots, F'_{r-1}, F'_{r+1}]$$

and

$$c = \operatorname{Res}_t(D'_1, D'_2).$$

Then $c(\xi) \neq 0$.

PROOF. The Binet-Cauchy Formula (see Remark 2.7) and Assumption 5.2 imply that $\det(F^{(k)}_{I_1})$ is monic in t for all $1 \le k \le N$.

Suppose that there exists $\xi \in \mathbf{A}^{n-1}$ such that for all $1 \le k \le N$,

$$\operatorname{Res}_t(\det(F^{(k)}_{I_1}(\xi, t)), \det(F^{(k)}_{I_2}(\xi, t))) = 0.$$

From (5.3) we see that $F^{(k)}_{I_1}$ and $F^{(k)}_{I_2}$ have the form

$$F^{(k)}_{I_1} = [F^{(k)}_{(1,\ldots,r-1)}, F_r]$$

and

$$F^{(k)}_{I_2} = [F^{(k)}_{(1,\ldots,r-1)}, \sum_{0\le j\le s-r-1} \alpha_r^j F_{j+r+1}],$$

if the k-th pair of $\prod_{1\le i\le r} A_i \times \prod_{1\le i\le r-1} B_i$ is $(\alpha_1, \ldots, \alpha_r; \beta_1, \ldots, \beta_{r-1})$. By Lemma 5.5 there exists $1 \le k_0 \le N$ such that $F^{(k_0)}_{(1,\ldots,r-1)}(\xi, t)$ is unimodular.

Our assumptions imply now that for each $\alpha \in A_r$ there exists an element $a_\alpha \in \overline{K}$ such that

$$F_r(\xi, a_\alpha) \qquad \text{and} \qquad \sum_{0\le j\le s-r-1} \alpha^j F_{j+r+1}(\xi, a_\alpha)$$

belong to the $\overline{K}$-linear vector space generated by $F_1^{(k_0)}(\xi, a_\alpha), \ldots, F_{r-1}^{(k_0)}(\xi, a_\alpha)$, i.e., the column vectors of $F_{(1,\ldots,r-1)}^{(k_0)}(\xi, a_\alpha)$. In particular a_α is a root of

$$\det(F_{I_1}^{(k_0)}(\xi, t)) = \det([F_{(1,\ldots,r-1)}^{(k_0)}, F_r](\xi, t))$$

for each $\alpha \in A_r$. Since $\det(F_{I_1}^{(k_0)}(\xi, t))$ is a specialization of $\det(F_{I_1}^{(k_0)})$ which is monic in t and of degree at most rd, we conclude that

$$\#\{a_\alpha : \alpha \in A_r\} \leq rd.$$

Since $\# A_r \geq r(s-r)d + 1$, the pigeonhole principle implies that there exist pairwise different elements $\alpha_0, \ldots, \alpha_{s-r-1} \in A_r$ such that $a = a_{\alpha_0} = \cdots = a_{\alpha_{s-r-1}}$. Thus the column vectors

$$F_r(\xi, a)$$

and

$$\sum_{0 \leq j \leq s-r-1} \alpha_\ell^j F_{j+r+1}(\xi, a), \qquad \text{for} \quad 0 \leq \ell \leq s-r-1,$$

belong to the K-linear vector space generated by $F_1^{(k_0)}(\xi, a), \ldots, F_{r-1}^{(k_0)}(\xi, a)$, the column vectors of $F_{(1,\ldots,r-1)}^{(k_0)}(\xi, a)$.

Since the Vandermonde matrix

$$[\alpha_\ell^j]_{0 \leq j, \ell \leq s-r-1}$$

is nonsingular, this implies that

$$\operatorname{rank}\,[F_{(1,\ldots,r-1)}^{(k_0)}, F_r, \ldots, F_s](\xi, a) = r - 1.$$

This contradicts the unimodularity of $[F_{(1,\ldots,r-1)}^{(k_0)}, F_1, \ldots, F_s]$ which follows from the unimodularity of F and from (5.3). □

If we now replace Lemma 4.4 by Proposition 5.6 in the proof of Proposition 4.1 (see Procedure 4.6), we obtain an algorithm which constructs, for the given unimodular matrix $F \in R^{r \times s}$, a matrix $M^{s \times s}$ satisfying the properties $(i), \ldots, (iv)$ of Proposition 4.1.

Here we give only an overview of the complexity bounds of the main steps of this algorithm, which involves only parallelizable linear algebra over K (see Berkowitz 1984, Chistov 1985, Mulmuley 1986 and the survey von zur Gathen 1986) and interpolation techniques as described in (Fitchas *et al.* 1990). The verification of these bounds is straightforward but lengthy so we shall omit it.

FACT 5.7. **(Preparatory Step)** *(See Assumptions 2.8 and 5.2.) Multiplication by an $s \times s$ matrix and linear change of variables is executed in*

$$\begin{aligned} \textit{sequential time} &= s^2(rd)^{O(n)}, \quad \text{and} \\ \textit{parallel time} &= O(n^2 \log^2 srd). \end{aligned}$$

FACT 5.8. **Computation of** $c_1, \ldots, c_N$ *(see Proposition 5.6 and Procedure 4.3, Step 1) is executed in*

$$\begin{aligned} \textit{sequential time} &= s^{O(r^2)} r^{O(n^2)} d^{O(n^2+r^2)}, \quad \text{and} \\ \textit{parallel time} &= O(n^4 \log^2 srd). \end{aligned}$$

FACT 5.9. **Computation of** $a_1, \ldots, a_N$ *(see Procedure 4.3, Step 2) is executed in*

$$\begin{aligned} \textit{sequential time} &= s^{O(r^2)} r^{O(n^2)} d^{O(n^2+r^2)}, \quad \text{and} \\ \textit{parallel time} &= O(n^4 r^4 \log^2 srd). \end{aligned}$$

FACT 5.10. **Computation of** $E_1, \ldots, E_N$ *(see Procedure 4.3, Step 3 and Lemma 4.5) is executed in*

$$\begin{aligned} \textit{sequential time} &= s^{O(r^2)} r^{O(n^2)} d^{O(n^2+r^2)}, \quad \text{and} \\ \textit{parallel time} &= O(n^4 \log^2 srd). \end{aligned}$$

From the complexity bounds, Facts 5.7 to 5.10, we obtain finally the complexity of the algorithm corresponding to Proposition 4.1:

FACT 5.11. **Computation of** M *(see Procedure 4.3, Step 4) is executed in*

$$\begin{aligned} \textit{sequential time} &= s^{O(r^2)} r^{O(n^2)} d^{O(n^2+r^2)}, \quad \text{and} \\ \textit{parallel time} &= O(n^4 r^4 \log^2 srd). \end{aligned}$$

Applying the algorithm corresponding to Proposition 4.1 n times one obtains easily Theorem 3.3. The complexity bounds of Theorem 3.3 follow from Fact 5.11.

References

D. BAYER AND M. STILLMAN, On the complexity of computing syzygies, *J. Symbolic Comp.* **6** (1988), 135–147.

S. BERKOWITZ, On computing the determinant in small parallel time using a small number of processors, *Inform. Processing Letters* **18** (1984), 147–150.

W. D. BROWNAWELL, Bounds for the degree in the Nullstellensatz, *Ann. Math.* (Second Series) **126** (3) (1987), 577–591.

B. BUCHBERGER, Gröbner-Bases: an algorithmic method in polynomial ideal theory, in *Multidimensional Systems Theory*, N. K. Bose, ed., Reidel Publishing Company, Dordrecht, 1985, 184–232.

L. CANIGLIA, A. GALLIGO, AND J. HEINTZ, Some new effectivity bounds in computational geometry, in *Proc. 6-th Int. Conf. Applied Algebra, Algebraic Algorithmic and Error Correcting Codes (AAECC-6)*, T. Mora, ed., Springer LN Comp. Sci. **357** (1989), 131–151.

L. CANIGLIA, J. A. GUCCIONE, AND J. J. GUCCIONE, Local Membership Problems for Polynomial Ideals, in *Effective Methods in Algebraic Geometry*, T. Mora and C. Traverso, eds., Progress in Math. **94**, Birkhäuser (1991), 31–45.

F. CHAQUI, *Algorithme de calcul d'une base pour les modules projectifs sur* $K[X,Y]$ *et* $\mathbb{Z}[X]$, Thèse 3ème Cycle, Université Paris-Sud, Centre d'Orsay (1983).

A. CHISTOV, Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic, in *Proc. Int. Conf. FCT 1985*, Springer LN Comp. Sci. **199** (1985), 63–69.

N. FITCHAS AND A. GALLIGO, Nullstellensatz effectif et Conjecture de Serre (Théorème de Quillen-Suslin) pour le Calcul Formel, *Math. Nachr.* **149** (1990), 231–253.

N. FITCHAS, A. GALLIGO AND J. MORGENSTERN, Algorithmes rapides en séquentiel et en parallèle pour l'élimination des quantificateurs en géométrie élémentaire, in F. Delon, M. Dickmann, D. Gondard (eds.), *Séminaire Structures Algébriques Ordonnées : Sélection d'exposés 1986–1987.* Publ. Université Paris VII **32** (1990), 103–145.

F. R. GANTMACHER, *Teorya matrits.* English version: *The theory of matrices*, Volume I, Chelsea Publishing Company, New York (1977).

J. VON ZUR GATHEN, Parallel arithmetic computations: a survey, *Proc. 13-th Symp. MFCS 1986*, Springer LN Comp. Sci. **233** (1986), 93–112.

G. HERMANN, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, *Math. Ann.* **95** (1926), 736–788.

J. KOLLÁR, Sharp effective Nullstellensatz, *J. Am. Math. Soc.* **1** (1988), 963–975.

E. KUNZ, *Einführnug in die kommutative Algebra und algebraische Geometrie,*

F. Vieweg und Söhne, Braunschweig-Wiesbaden (1980).

T. Y. LAM, *Serre's Conjecture*, Springer LN Math. **635** Springer-Verlag (1978).

A. LOGAR AND B. STURMFELS, Algorithms for Quillen-Suslin Theorem, *J. Algebra* **145** (1992), 231–239.

E. MAYR AND A. MEYER, The complexity of the word problem for commutative semigroups and polynomial ideals, *Advances in Math.* **46** (1982), 305–329.

K. MULMULEY, A fast parallel algorithm to compute the rank of a matrix over an arbitrary field, *Proc. 18-th Ann. ACM Symp. Theory of Comput.* (1986), 338–339.

P. PHILIPPON, *Théorème des zéros effectif d'après J.Kollár*, Probl. Dioph. 1988-89, Publ. Math. Univ. Paris VI **88** (1988).

A. SEIDENBERG, Constructions in Algebra, *Trans. Amer. Math. Soc.* **197** (1974), 273–313.

J. P. SERRE, Faisceaux algébriques cohérents, *Amer. Math.* **61** (1955), 191–274.

B. TEISSIER, Résultats récents d'algèbre commutative effective, *Séminaire Bourbaki.* Volume 1989/90, Exposé 718, Astérisque **189–190** (1991), 107–131.

Manuscript received 20 November 1991

WORKING GROUP NOAÏ FITCHAS
Departamento de Matemáticas
Fac. de Ciencias Exactas. Univ. de Buenos Aires
(1428) Buenos Aires ARGENTINA
joos@mate.edu.ar
krick@mate.edu.ar