Journal of Algebra **227,** 633–644 (2000)
doi:10.1006/jabr.1999.8243, available online at http://www.idealibrary.com on IDEAL®

On the Number of Sets Definable by Polynomials

Gabriela Jeronimo[1] and Juan Sabia[1]

Communicated by Leonard Lipshitz

Received May 11, 1999

We show that the known algorithms used to re-write any first order quantifier-free formula over an algebraically closed field into its normal disjunctive form are essentially optimal. This result follows from an estimate of the number of sets definable by equalities and inequalities of fixed polynomials. Finally we apply our results to obtain similar estimates in the real case. © 2000 Academic Press

Key Words: polynomial-definable sets; algorithms; algebraic complexity.

1. INTRODUCTION

One of the problems that computational algebra has to face is related to time: many algorithms to solve different problems are known but so much time to run them is necessary (in one or even in several computers) that they are useless. A way to estimate the time an algebraic algorithm takes is its *algebraic complexity*: if an algorithm is a directed acyclic graph, its complexity is the number of nodes of the graph.

Sometimes, it is impossible to obtain a better algorithm (that is, an algorithm of lower algebraic complexity) than the known ones to solve a fixed problem. In this case, the principal aim of computational algebra is to obtain lower complexity bounds to show that the running time of the known algorithms cannot be improved.

A basic problem that appears when designing algebraic algorithms is re-writing an arbitrary first order quantifier-free formula over an algebraically

[1] Partially supported by the following Argentinian research grants: CONICET: PIP'97 4571; UBACyT: EX TW80 (1998); ANPCyT: PICT 03-0000001593 (1998).

0021-8693/00 $35.00

closed field (i.e., a formula involving multivariate polynomials, equalities and inequalities, and the logical connectives $\wedge$, $\vee$, $\neg$) into an equivalent formula written in some standard way. The standard way we are going to consider is called the *normal disjunctive form* of the given formula.

Let Φ be an arbitrary quantifier-free formula and let $\{f_1, \ldots, f_s\}$ be the set of polynomials involved in Φ. The normal disjunctive form of Φ is a formula equivalent to Φ of the type

$$\bigvee_{I \in \mathscr{S}} \Big(\bigwedge_{i \in I} f_i = 0 \ \wedge \bigwedge_{j \in \{1,\ldots,s\}-I} f_j \neq 0 \Big),$$

where $\mathscr{S}$ is a set of subsets of $\{1, \ldots, s\}$ and the sets defined by

$$\bigwedge_{i \in I} f_i = 0 \ \wedge \bigwedge_{j \in \{1,\ldots,s\}-I} f_j \neq 0 \tag{1}$$

are nonempty. This last condition not only provides the uniqueness of the normal disjunctive form but also allows one to design better elimination algorithms in terms of complexity (see [1]).

The algorithm to get the normal disjunctive form of any given formula Φ used in [1] consists of two steps. In the first step, it determines all the formulas of type (1) defining nonempty sets. In the second step, it decides which of these appear in the normal disjunctive form of Φ. The algebraic complexity of this algorithm depends on the number of formulas of type (1) which define nonempty sets.

Heintz (see [3]) proved that, for any set of s n-variate polynomials with total degrees bounded by d, the number of nonempty sets defined by conjunctions of type (1) is less or equal to $(1 + sd)^n$.

In this paper we improve the upper bound obtained by Heintz. We also obtain a lower bound on the maximum number of these sets. This bound allows us to show a lower bound for the algebraic complexity of *any* algorithm that re-writes a given formula into its normal disjunctive form. We also show that the upper and the lower bounds obtained have the same asymptotical behavior. This implies that the algorithm described in [1] cannot be essentially improved.

Finally, we apply our results in order to obtain lower bounds on the real case and show that they have the same asymptotical behavior as the upper bounds obtained in [4].

2. DEFINITIONS AND NOTATIONS

Let k be an arbitrary field and let $X_1, \ldots, X_n$ be indeterminates over k. As usual, we denote by $k[X_1, \ldots, X_n]$ the polynomial ring in $X_1, \ldots, X_n$

with coefficients in k. Let $\bar{k}$ be an algebraic closure of k. $\mathbb{A}^n(\bar{k})$ (or simply, $\mathbb{A}^n$) will be the affine space $\bar{k}^n$ equipped with its Zariski topology.

Given a closed set $V \subseteq \mathbb{A}^n$, we will consider two intrinsic numbers related to V:

The *dimension* of V (denoted by $\dim V$) is the Krull dimension of its coordinate ring, as usual.

If V is an irreducible closed set of dimension r we define the *degree* of V as

$$\deg V := \sup\{\#H_1 \cap \cdots \cap H_r \cap V \ ; \ H_1, \ldots, H_r \text{ affine hyperplanes in } \mathbb{A}^n \text{ such that } H_1 \cap \cdots \cap H_r \cap V \text{ is a finite set}\}.$$

For an arbitrary closed set $V \subseteq \mathbb{A}^n$, we define $\deg V$ as the sum of the degrees of all the irreducible components of V.

DEFINITION 1. Let $f_1, \ldots, f_s$ be polynomials in $k[X_1, \ldots, X_n]$. A set $Z \subseteq \mathbb{A}^n$ is called an $(f_1, \ldots, f_s)$-*cell* if:

- There exists $I \subseteq \{1, \ldots, s\}$ such that

$$Z = \{x \in \bar{k}^n : f_i(x) = 0 \ \forall i \in I \text{ and } f_j(x) \neq 0 \ \forall j \in \{1, \ldots s\} - I\}.$$

- $Z \neq \emptyset$.

Note that, according to this definition, an $(f_1, \ldots, f_s)$-cell is a nonempty intersection of sets of the type $\{x \in \bar{k}^n : f_i(x) = 0\}$ and $\{x \in \bar{k}^n : f_i(x) \neq 0\}$ over all indices i, $1 \leq i \leq s$.

3. AN UPPER BOUND FOR THE NUMBER OF CELLS

In this section we will give an upper bound for the number of cells determined by a set of multivariate polynomials. The bound, stated in the following theorem, depends on the number of variables, the number of polynomials involved, and their degrees. We will consider $\binom{s}{k} = 0$ whenever $k > s$.

THEOREM 2. *Let $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ be s polynomials in n variables. Let d be a non-negative integer such that $\deg f_i \leq d$ for all $1 \leq i \leq s$. Then the number of $(f_1, \ldots, f_s)$-cells of $\mathbb{A}^n$ is at most $\sum_{k=0}^{n} \binom{s}{k} d^k$.*

The idea of the proof of Theorem 2 is to obtain our bound by means of a bound for the number of irreducible components of the Zariski closures of the cells. To estimate this number we apply the following Bezout inequality (see [3]):

Bezout inequality. Let $X, Y \subseteq \mathbb{A}^n$ be closed sets. Then

$$\deg(X \cap Y) \leq \deg X . \deg Y.$$

The proof of Theorem 2 is based on two previous lemmas.

Let $f_1, \ldots, f_s$ be polynomials in $k[X_1, \ldots, X_n]$.

For each $(f_1, \ldots, f_s)$-cell Z, we consider its Zariski closure $\overline{Z}$ and the decomposition of $\overline{Z}$ into irreducible components. We define

$$\mathcal{I}(Z) := \{C \subseteq \mathbb{A}^n : C \text{ is an irreducible component of } \overline{Z}\}.$$

If $Z = \{x \in \bar{k}^n : f_i(x) = 0 \ \forall i \in I \text{ and } f_j(x) \neq 0 \ \forall j \in \{1, \ldots, s\} - I\}$, it can be shown that

$$\mathcal{I}(Z) = \{C \subseteq \mathbb{A}^n : C \text{ is an irreducible component of } \bigcap_{i \in I}\{f_i = 0\},\ C \cap Z \neq \emptyset\} \tag{2}$$

(when $I = \emptyset$, $\bigcap_{i \in I}\{f_i = 0\} = \mathbb{A}^n$).

We denote by $\mathcal{I}$ the set of all irreducible components of the Zariski closures of all the $(f_1, \ldots, f_s)$-cells in $\mathbb{A}^n$, that is,

$$\mathcal{I} := \bigcup \mathcal{I}(Z),$$

where the union ranges over the set of all $(f_1, \ldots, f_s)$-cells.

The following lemma, which can be easily proved from (2), provides a characterization for the elements of $\mathcal{I}$. To make notation shorter, $\{f_i = 0\}$ will denote the set $\{x \in \bar{k}^n : f_i(x) = 0\}$.

LEMMA 3. *Let $f_1, \ldots, f_s$ be polynomials in $k[X_1, \ldots, X_n]$ and let $\mathcal{I}$ be defined as above. Then*

$$\mathcal{I} = \Big\{C \subseteq \mathbb{A}^n : \exists I \subseteq \{1, \ldots, s\}/C \text{ is an irreducible component of } \bigcap_{i \in I}\{f_i = 0\}\Big\}.$$

The next result allows us to estimate the number of cells from the cardinality of $\mathcal{I}$. We skip the proof because it is straightforward.

LEMMA 4. *Let $f_1, \ldots, f_s$ be polynomials in $k[X_1, \ldots, X_n]$ and let Z_1 and Z_2 be two different $(f_1, \ldots, f_s)$-cells. Then $\mathcal{I}(Z_1) \cap \mathcal{I}(Z_2) = \emptyset$.*

Now, we are going to prove Theorem 2:

Proof of Theorem 2. As an immediate consequence of Lemma 4, the number of $(f_1, \ldots, f_s)$-cells of $\mathbb{A}^n$ is bounded by the number of irreducible components of their Zariski closures, denoted by $\#\mathcal{I}$.

As every nonempty closed set has positive degree,

$$\#\mathcal{I} \leq \sum_{C \in \mathcal{I}} \deg C.$$

Therefore, it suffices to prove that

$$\sum_{C\in\mathcal{I}} \deg C \le \sum_{k=0}^{n} \binom{s}{k} d^k.$$

For each $0 \le k \le n$, let

$$\mathcal{I}_k := \{C \in \mathcal{I} : \operatorname{codim} C = k\}$$

and let

$$c_k := \sum_{C\in\mathcal{I}_k} \deg C.$$

We are going to prove that $c_0, \dots, c_n$ verify a recursive relation.

Since $\mathcal{I}_0 = \{\mathbb{A}^n\}$, it follows that $c_0 = 1$.

Fix $1 \le k \le \max\{s, n\}$ and let $C \in \mathcal{I}_k$ be an irreducible component of codimension k of the closure of a cell. From Lemma 3, there exists a subset $I \subseteq \{1, \dots, s\}$ such that C is an irreducible component of $\bigcap_{i\in I}\{f_i = 0\}$. Take I minimal in this sense, i.e., such that C is not an irreducible component of $\bigcap_{i\in J}\{f_i = 0\}$ for any proper subset J of I. Note that $\#I$ (the number of elements of I) is at least k.

For each $j \in I$, there exists an irreducible closed set $C^{(j)}$ of codimension $k-1$ which is an irreducible component of $\bigcap_{i\in I-\{j\}} \{f_i = 0\}$ (i.e., $C^{(j)}$ is an element of $\mathcal{I}_{k-1}$) such that $C \subset C^{(j)}$.

It is easy to see that, if j_1, j_2 are different elements of I, $C^{(j_1)} \ne C^{(j_2)}$.

Therefore, we have that, for each $C \in \mathcal{I}_k$, there exist at least k polynomials $f_{j_1}, \dots, f_{j_k}$ and k elements $C^{(j_1)}, \dots, C^{(j_k)}$ in $\mathcal{I}_{k-1}$ such that for every $1 \le l \le k$, C is an irreducible component of the variety $C^{(j_l)} \cap \{f_{j_l} = 0\}$.

Let us now consider the degrees of the closed sets involved.

Let $\mathcal{D}_k$ be the set

$$\mathcal{D}_k := \big\{(D, f_j) : D \in \mathcal{I}_{k-1},\ j \in \{1, \dots, s\},\ \operatorname{codim}(D \cap \{f_j = 0\}) = k\big\}.$$

From the previous considerations and the definition of degree we have

$$kc_k = \sum_{C\in\mathcal{I}_k} k \deg C \le \sum_{(D,f_j)\in\mathcal{D}_k} \deg(D \cap \{f_j = 0\}). \tag{3}$$

For every $D \in \mathcal{I}_{k-1}$ we have

$$\#\{j \in \{1, \dots, s\} / (D,\ f_j) \in \mathcal{D}_k\} \le s - (k-1). \tag{4}$$

Applying the Bezout inequality to (3) and combining it with (4) we deduce that the following recursive relation holds:

$$\begin{aligned} c_0 &= 1 \\ c_k &\le \frac{s-k+1}{k}\, d\, c_{k-1} \qquad (k = 1, \dots, n). \end{aligned} \tag{5}$$

Therefore, for every $0 \leq k \leq n$,

$$c_k \leq \binom{s}{k} d^k$$

and then

$$\sum_{C \in \mathcal{F}} \deg C = \sum_{k=0}^{n} c_k \leq \sum_{k=0}^{n} \binom{s}{k} d^k.$$

As the number of $(f_1, \ldots, f_s)$-cells is less or equal to $\sum_{C \in \mathcal{F}} \deg C$, as stated before, the theorem follows. ∎

4. LOWER BOUNDS

In Section 3 we obtained an upper bound for the number of cells of $\mathbb{A}^n$ determined by s polynomials in n variables of degrees bounded by d. The question that arises now is whether this bound is optimal or it can be improved. The present section is devoted to the analysis of this problem.

In the sequel, k will always denote an infinite field.

4.1. *Examples*

We are going to construct families of polynomials (first in one variable, and then in several variables), trying to obtain as many cells as possible. These families will allow us to get lower bounds for the general case as will be stated afterwards.

The first example is an intermediate step in our construction. We will consider a family of d univariate polynomials $f_1, \ldots, f_d \in k[X]$ of degree d.

Note that, when the polynomials are univariate, a cell is either the set of points which are not zeroes of any polynomial (the cell defined by $f_j \neq 0$ for every j) or a finite number of points, which are common zeroes of some of the polynomials (in fact, they are common zeroes of the polynomials which appear equal to 0 in the definition of the cell). In order to control the degrees of the polynomials involved, we shall deal only with cells which correspond to zeroes of at most two polynomials.

EXAMPLE 5. We consider polynomials $f_1, \ldots, f_d \in k[X]$ with all their zeroes in k and no multiple zeroes, which satisfy the following conditions:

1. Each polynomial has only one zero which is not a zero of any of the others.

2. Given two polynomials, they have only one common zero that is not a zero of any of the others.

3. The zeroes involved in items 1 and 2 are the only zeroes of the polynomials $f_1, \ldots, f_d$.

Note that, as k is infinite, for every positive integer d, there exists a family $f_1, \ldots, f_d$ of polynomials in $k[X]$ satisfying these conditions. Moreover, we can easily see that $\deg f_i = d$ for every $1 \leq i \leq d$.

Let us compute the number of cells determined by a family of polynomials which satisfies 1, 2, and 3:

Fix i and j, $i \neq j$. Because of conditions 1 and 2

$$Z_i = \{x \in \bar{k}^n : f_i(x) = 0 \text{ and } f_\ell(x) \neq 0 \ \forall \ell \neq i\}$$

$$Z_{ij} = \{x \in \bar{k}^n : f_i(x) = 0, f_j(x) = 0 \text{ and } f_\ell(x) \neq 0 \ \forall \ell \neq i, j\}$$

are nonempty sets and, therefore, $(f_1, \ldots, f_d)$-cells.

The set

$$Z = \{x \in \bar{k}^n : f_k(x) \neq 0 \ \forall 1 \leq k \leq d\}$$

is also an $(f_1, \ldots, f_d)$-cell.

On the other hand, condition 3 guarantees that there are no other cells.

Then the number of $(f_1, \ldots, f_d)$-cells is

$$d + \binom{d}{2} + 1 = \frac{d + d^2}{2} + 1.$$

Note that these cells are either a point or the complement of a finite set.

In the next example we show a family of multivariate polynomials which provides a lower bound for the maximum number of cells depending on the number of variables involved, the quantity of polynomials, and their degrees.

The polynomials we are going to consider are those we have constructed in the case of a single variable slightly modified. To obtain polynomials in n variables without increasing their degrees, we will specialize the univariate polynomials in suitably chosen linear forms.

EXAMPLE 6. Let s and d be positive integers. Let m and r be the quotient and the remainder of the division of s by d.

Let $f_1, \ldots, f_d \in k[X]$ be as in Example 5 and let $\alpha_1, \ldots, \alpha_c$ be their different zeroes. We will consider a family of $m + 1$ homogeneous linear forms $l_1, \ldots, l_{m+1} \in k[X_1, \ldots, X_n]$ satisfying

1. Every subset of n linear forms of $\{l_1, \ldots, l_{m+1}\}$ is a linearly independent set.

2. Every linear system involving $n + 1$ different linear forms, of the type

$$\begin{aligned} l_{j_1}(x) &= \alpha_{i_{j_1}} \\ l_{j_2}(x) &= \alpha_{i_{j_2}} \\ &\vdots \qquad \vdots \\ l_{j_{n+1}}(x) &= \alpha_{i_{j_{n+1}}}, \end{aligned}$$

has no solution in k^n.

The first condition is equivalent to the fact that the determinants of all matrices of size $n \times n$, whose rows are the coefficients of n of the linear forms, are different from zero. Once this condition is stated, the second one is equivalent to the fact that the determinants of the augmented matrices of all the $(n+1) \times (n+1)$ systems considered are different from zero.

Therefore, conditions 1 and 2 are equivalent to a nonempty open condition over the coefficients of the linear forms. Then, the existence of such linear forms follows from the fact that k is an infinite field.

For each pair (i, j), $1 \leq i \leq d, 1 \leq j \leq m$, let $f_{ij} := f_i(l_j)$ be the polynomial of degree d obtained by specializing the polynomial f_i in the linear form l_j. If $j = m+1$, we only consider the polynomials $f_{ij} := f_i(l_j)$ for $1 \leq i \leq r$.

We are going to determine all the cells defined by the polynomials f_{ij}. If Z is such a cell, then

$$Z = Z_1 \cap \ldots \cap Z_m \cap Z_{m+1}, \tag{6}$$

where, for each $1 \leq j \leq m$, Z_j is an $(f_{ij})_{1 \leq i \leq d}$-cell and Z_{m+1} is an $(f_{i\,m+1})_{1 \leq i \leq r}$-cell. From the construction of the polynomials $f_1, \ldots, f_d$ (see Example 5), we have that, for a fixed $1 \leq j \leq m$, an $(f_{ij})_{1 \leq i \leq d}$-cell is an hyperplane in $\mathbb{A}^n$ (given by an equation of the form $l_j = \alpha_{i_j}$ for some $1 \leq i_j \leq c$) or it is the complement of a finite union of hyperplanes (this happens when the cell is defined by $f_{ij} \neq 0 \ \forall 1 \leq i \leq d$). Similarly, if $\{\beta_1, \ldots, \beta_{c'}\} \subseteq \{\alpha_1, \ldots, \alpha_c\}$ is the set of the different zeroes of the polynomials $f_1, \ldots, f_r$, an $(f_{i\,m+1})_{1 \leq i \leq r}$-cell is a finite union of hyperplanes (of equations of type $l_{m+1} = \beta_k$) or it is the complement of a finite union of hyperplanes.

Suppose first that

$$Z_{m+1} = \{x \in \bar{k}^n : f_{i\,m+1}(x) \neq 0 \ \forall 1 \leq i \leq r\} = \{x \in \bar{k}^n : l_{m+1}(x) \neq \beta_k \ \forall 1 \leq k \leq c'\}.$$

Let $Z_{j_1}, \ldots, Z_{j_t}$ be the sets appearing in (6) which are hyperplanes. We consider the set $W = \bigcap_{h=1}^{t} Z_{j_h}$. Note that W is an irreducible closed set defined by a linear system of equations

$$\begin{aligned} l_{j_1}(x) &= \alpha_{i_{j_1}} \\ l_{j_2}(x) &= \alpha_{i_{j_2}} \\ &\vdots \qquad \vdots \\ l_{j_t}(x) &= \alpha_{i_{j_t}} \end{aligned}$$

and that we have

$$Z = W \cap U,$$

where U is an open set in $\mathbb{A}^n$.

From condition 2 in the choice of the linear forms $l_1, \ldots, l_{m+1}$, as W is a nonempty set, it follows that $t \leq n$.

We are going to show that, whenever $t \leq n$, if $\{j_1, \ldots, j_t\} \subseteq \{1 \ldots, m\}$ and

$$W = \{x \in \bar{k}^n \ : l_{j_1}(x) = \alpha_{i_{j_1}} \wedge l_{j_2}(x) = \alpha_{i_{j_2}} \wedge \cdots \wedge l_{j_t}(x) = \alpha_{i_{j_t}}\}$$

$$U = \{x \in \bar{k}^n : l_j(x) \neq \alpha_h\,;\, 1 \leq j \leq m,\ j \notin \{j_1, \ldots, j_t\}\,,$$

$$1 \leq h \leq c \ \wedge \ l_{m+1} \neq \beta_k\,;\, 1 \leq k \leq c'\}$$

then $Z := W \cap U$ is a nonempty set and, therefore, a cell.

First, note that, as a consequence of the linear independence of every subset of n linear forms of $\{l_1, \ldots, l_{m+1}\}$, W is a nonempty linear affine variety of codimension t. Consider

$$W \cap U^c = \left(\bigcup_{\substack{1 \leq j \leq m \\ j \notin \{j_1, \ldots, j_t\}}} \ \bigcup_{1 \leq h \leq c} W \cap \{l_j = \alpha_h\} \right) \cup \left(\bigcup_{1 \leq k \leq c'} W \cap \{l_{n+1} = \beta_k\} \right). \tag{7}$$

If $t < n$, because of condition 1 stated before, each of the sets appearing in the union above is a linear affine variety of codimension $t+1$. As $\operatorname{codim}(W) = t$, it follows that $W \neq W \cap U^c$ and therefore $W \cap U \neq \emptyset$.

If $t = n$, condition 2 assures that all the sets appearing in the union (7) are empty and then $W \cap U = W$, which is nonempty.

If $Z_{m+1} = \bigcup_{k=1}^{\ell} \{l_{m+1} = \beta_{i_k}\}$, $Z = W \cap U$ with U an open set and

$$W = \bigcup_{k=1}^{\ell} W_k,$$

where $W_1, \ldots, W_\ell$ are linear affine varieties of the same dimension. Applying our previous arguments to each of the sets $W_1 \cap U, \ldots, W_\ell \cap U$ we obtain that there are at most $n-1$ indices $j \in \{1, \ldots, m\}$ such that l_j is involved in the definition of W. The converse follows in the same way as before (once again, considering the irreducible decomposition of W).

Summarizing, we have that the cells determined by the s polynomials considered are all intersections of the form

$$Z = Z_1 \cap \ldots \cap Z_{m+1},$$

where, for each $1 \leq j \leq m$, Z_j is an $(f_{ij})_{1 \leq i \leq d}$-cell and Z_{m+1} is an $(f_{i\,m+1})_{1 \leq i \leq r}$-cell and, at most n of the sets $Z_1, \ldots, Z_{m+1}$ are hyperplanes or, in the case of Z_{m+1}, a finite union of hyperplanes.

It is immediate that the number of these sets is

$$\sum_{k=0}^{n}\binom{m}{k}\left(\frac{d^2+d}{2}\right)^k+\sum_{k=0}^{n-1}\binom{m}{k}\left(\frac{r^2+r}{2}\right)\left(\frac{d^2+d}{2}\right)^k$$

and therefore this is the number of cells determined by the $s = md + r$ polynomials.

4.2. *A Lower Bound for the Maximum Number of Cells*

From the examples given in Section 4.1, we can obtain a lower bound for the maximum number of cells determined by s polynomials in n variables with coefficients in an infinite field k, whose degrees are bounded by a positive integer d.

Let s, n, and d be positive integers and let m and r be the quotient and the remainder of the division of s by d. From Example 6, there exists a family of s polynomials in n variables which determines

$$\sum_{k=0}^{n}\binom{m}{k}\left(\frac{d^2+d}{2}\right)^k+\sum_{k=0}^{n-1}\binom{m}{k}\left(\frac{r^2+r}{2}\right)\left(\frac{d^2+d}{2}\right)^k \tag{8}$$

cells in $\bar{k}^n$. Considering m as a variable, for each $0 \le k \le n$, $\binom{m}{k}$ is a polynomial of degree k in m. Then, if d and n are fixed integers, when $s \to \infty$, the sum in (8) is a number of order $\frac{s^n d^n}{n!\,2^n}$.

Let $\sigma(s, n, d)$ be the maximum number of cells which can be determined by s polynomials of degrees at most d in n variables with coefficients in an infinite field k.

Recalling the upper bound

$$\sigma(s, n, d) \le \sum_{k=0}^{n}\binom{s}{k}d^k$$

we have found in Section 3, and considering as in the previous case the numbers d and n fixed and s as a variable, we obtain the following result.

Let s, n, and d be positive integers. Let $\sigma(s, n, d)$ be the maximum number of cells which can be determined by a set of s polynomials in n variables of degrees bounded by d with coefficients in an infinite field k. Then, as $s \to \infty$,

$$O\left(\frac{s^n d^n}{n!\,2^n}\right) \le \sigma(s, n, d) \le O\left(\frac{s^n d^n}{n!}\right).$$

REMARK 7. Let f_{ij}, $1 \le i \le d$ if $1 \le j \le m$ and $1 \le i \le r$ if $j = m + 1$ be the polynomials defined in Example 6. Let Φ be any first order quantifier-free formula involving them and let

$$\Psi : f_{11} = 0 \vee f_{11} \neq 0 \vee \Phi.$$

Consider any general algorithm that, from a given formula, obtains its normal disjunctive form. As the set defined by Ψ is $\mathbb{A}^n$, when the input of this algorithm is Ψ, the output must necessarily be the disjunction of all the conjunctions defining the cells given by the polynomials. Then, the complexity of the algorithm must be a number greater or equal to $O\left(\frac{s^n d^n}{n!\,2^n}\right)$. This is another example of the fact that general algorithms (i.e., algorithms solving all possible instances) in computational algebra are usually of great complexity.

5. ON THE NUMBER OF CELLS IN THE REAL CASE

Many problems over a real closed field (for example, real quantifier elimination) are solved by algorithms whose algebraic complexity has to do with the number of real cells defined by the polynomials involved.

We are now going to apply the lower bound for the maximum number of cells obtained in the previous section in order to estimate the number of cells in the real case.

DEFINITION 8. Let R be a real closed field. Let $f_1, \ldots, f_s \in R[X_1, \ldots, X_n]$. A *real* $(f_1, \ldots, f_s)$*-cell* is a nonempty semialgebraic set of the form

$$\left\{x \in R^n : \bigwedge_{i\in I} f_i(x) = 0 \wedge \bigwedge_{i_1\in I_1} f_{i_1}(x) > 0 \wedge \bigwedge_{i_2\in I_2} f_{i_2}(x) < 0\right\},$$

where $I \cup I_1 \cup I_2 = \{1, \ldots, s\}$.

This definition of a real cell follows [2, 3] but differs from the definition used in [4].

In [2], Grigor'ev obtains, from the bound of Heintz in the algebraically closed field case, an upper bound for the number of connected components of real cells (defined by s n-variate polynomials of total degree bounded by d) of order $O(sd)^{2n}$. Later, Pollack and Roy (see [4]), following [5], obtained in the same case an upper bound of order $O\left(\frac{sd}{n}\right)^n$.

We assert that this last bound is asymptotically optimal, not only for the number of connected components of real cells but for the number of real cells as well.

Let $\bar{k}$ be an algebraic closure of R. Given $f_1, \ldots, f_s \in R[X_1, \ldots, X_n]$, the following equality holds:

$$R^n \bigcap \{x \in \bar{k}^n : \bigwedge_{i\in I} f_i(x) = 0 \wedge \bigwedge_{j\in\{1,\ldots,s\}-I} f_j(x) \neq 0\}$$

$$= \bigcup_{I_1\cup I_2=\{1,\ldots,s\}-I} \left\{x \in R^n : \bigwedge_{i\in I} f_i(x) = 0 \wedge \bigwedge_{i_1\in I_1} f_{i_1}(x) > 0 \wedge \bigwedge_{i_2\in I_2} f_{i_2}(x) < 0\right\}.$$

If we consider $k = R$ and the polynomials defined in Example 6, the intersection of R^n with each cell (in the algebraically closed sense) is a nonempty set.

Therefore, in this case, the number of real cells is greater or equal to the number of cells (in the algebraically closed sense). From our lower bound on the maximum number of cells, applying the Stirling formula, we conclude that the maximum number of real cells (and, therefore, the maximum number of connected components of real cells) defined by a set of s polynomials in n variables of degrees bounded by d is at least $O\left(\frac{sd}{n}\right)^n$, which matches the upper bound in [4].

Again, this gives a lower estimate to the complexity of any algorithm computing a real normal disjunctive form (see Remark 7).

ACKNOWLEDGMENT

The authors acknowledge the referee for some helpful remarks.

REFERENCES

1. 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** (1990), 1–14.
2. D. Yu Grigor'ev, Complexity of deciding Tarski algebra, *J. Symbolic Comput.* **5** (1988), 65–108.
3. J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, *Theoret. Comput. Sci.* **24** (1983), 239–277.
4. R. Pollack and M.-F. Roy, On the number of cells defined by a set of polynomials, *C. R. Acad. Sci. Paris* **316** (1993), 573–577.
5. H. E. Warren, Lower bounds for approximation of nonlinear manifolds, *Trans. Amer. Math. Soc.* **133** (1968), 167–178.