ANNALES
POLONICI MATHEMATICI
91.1 (2007)

On reconstructing algebraic sets and ideals

by Paweł Gniadek (Kraków)

Abstract. We generalize some results on reconstructing sets to the case of ideals of $\mathbb{k}[X_1, \dots, X_n]$. We show that reconstructing sets can be approximated by finite subsets having the property of reconstructing automorphisms of bounded degree.

1. Introduction. This paper deals with the question of reconstructing polynomial automorphisms from their restrictions. The first problem of this type was the problem of reconstructing a polynomial automorphism in $\mathbb{C}^n$ from its restriction to the coordinate hyperplanes. The solution for $n = 2$ was found by J. McKay and S. Wang [11] in 1988. However, their resultant based formula could not be generalized to higher dimensions.

Several years later A. van den Essen and M. Kwieciński [6] approached the problem with the Gröbner bases theory and found an algorithm for reconstructing automorphisms in the case $n > 2$. In his next paper [10] M. Kwieciński simplified the algorithm reducing computations to finding only two Gröbner bases.

In [7] the present author described a large family of algebraic sets for which the algorithm of Kwieciński could be used for reconstructing automorphisms. We generalize some of those results to ideals of $\mathbb{k}[X_1, \dots, X_n]$ and we show that reconstructing sets can be in some sense approximated by finite sets of points having the property of reconstructing automorphisms of a bounded degree (see Theorem 16).

2. Notations. In what follows, $\mathbb{k}$ denotes an arbitrary field of characteristic 0 and $X = (X_1, \dots, X_n)$, $Y = (Y_1, \dots, Y_m)$ $(n, m \in \mathbb{N})$.

For any $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ let $|\alpha| := \alpha_1 + \cdots + \alpha_n$. We often identify a multi-index $\alpha \in \mathbb{N}^n$ with the monomial $X^\alpha := X^{\alpha_1} \cdots X^{\alpha_n}$ of degree $|\alpha|$ via the isomorphism of monoids

$$j : \mathbb{N}^n \ni \alpha \mapsto X^\alpha \in T(X) := \{X^\alpha : \alpha \in \mathbb{N}^n\}.$$

2000 *Mathematics Subject Classification*: Primary 14Q20; Secondary 13P10, 14J50.
Key words and phrases: polynomial automorphisms, Gröbner bases.

We introduce the natural partial ordering on $\mathbb{N}^n$ by the formula $\alpha \sqsubseteq \beta \Leftrightarrow \alpha_i \leq \beta_i$ for $i = 1, \ldots, n$. The same symbol will denote the isomorphic ordering on $T(X)$.

For $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha X^\alpha \in \Bbbk[X]$ the set $\operatorname{supp}(f) := \{\alpha \in \mathbb{N}^n : c_\alpha \neq 0\}$ is called the *support* of f, and the number $\deg(f) := \max\{|\alpha| : \alpha \in \operatorname{supp}(f)\}$ is the *degree* of f. For a polynomial mapping $F = (F_1, \ldots, F_m) : \Bbbk^n \to \Bbbk^m$ we define $\deg(F) := \max\{\deg(F_i) : i = 1, \ldots, m\}$.

We now introduce some notions and notation from the theory of Gröbner bases. We assume that the reader is familiar with basic notions of this theory. For a comprehensive introduction see [3, 4, 8].

We will make use of two special types of admissible orderings: eliminating orderings and string-type orderings.

An admissible ordering $\prec$ on $T(X, Y)$ is called X-*eliminating* if for any $t \in T(Y)$ and $s \in T(X) \setminus \{1\}$ we have $t \prec s$.

An admissible ordering $\prec$ on $T(X)$ is called a *string-type* ordering if for any $\alpha \in \mathbb{N}^n$ the set $\{\beta \in \mathbb{N}^n : \beta \prec \alpha\}$ is finite.

Let us fix an admissible ordering $\prec$ on $T(X)$ (or equivalently on $\mathbb{N}^n$) and let $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha X^\alpha \neq 0$ in $\Bbbk[X]$. We will use the following notation:

$$\operatorname{mdeg}(f) := \max \operatorname{supp}(f), \qquad \operatorname{LT}(f) = c_{\operatorname{mdeg}(f)} X^{\operatorname{mdeg}(f)},$$
$$\Delta(f) := \operatorname{mdeg}(f) + \mathbb{N}^n = \{\operatorname{mdeg}(f) + \alpha : \alpha \in \mathbb{N}^n\}.$$

For any subset $A \subset \Bbbk[X]$ we also define

$$\Delta(A) := \bigcup_{f \in A \setminus \{0\}} \Delta(f), \qquad D(A) := \mathbb{N}^n \setminus \Delta(A),$$
$$\mathcal{M}(A) := \{X^\alpha : \alpha \in D(A)\}.$$

For any $\mu \in \mathbb{N}$ we let $D^{(\mu)}(A)$ denote the set of the first μ elements of $D(A)$ with respect to the chosen admissible ordering. Let us remark that the equality $\bigcup_{\mu \in \mathbb{N}} D^{(\mu)}(A) = D(A)$ holds true for string-type orderings, although it may fail for an arbitrary admissible ordering.

For any polynomial $f \in \Bbbk[X]$ and any subset $G \subseteq \Bbbk[X]$ let $\operatorname{NF}(f, G)$ denote the normal form of F with respect to the set G (under a fixed admissible ordering).

3. Reconstructing ideals and sets. The following theorem due to A. van den Essen [5] provides a useful method of deciding whether a given polynomial mapping is a polynomial automorphism and finding its inverse.

THEOREM 1 (A. van den Essen [5]). *Let $F = (F_1, \ldots, F_n) : \Bbbk^n \to \Bbbk^n$ be a polynomial mapping and denote by $\mathcal{B}$ the reduced Gröbner basis of the ideal $I = \langle Y_1 - F_1(X), \ldots, Y_n - F_n(X)\rangle$ with respect to a fixed admissible*

X-eliminating ordering. Then F is a polynomial automorphism if and only if $\mathcal{B} = \{X_1 - G_1(Y), \dots, X_n - G_n(Y)\}$ for some $G_i \in \Bbbk[Y]$. In this case, the mapping $G = (G_1, \dots, G_n)$ is the inverse of F.

A generalization of this result due to M. Kwieciński [9] gives an effective criterion for checking if a polynomial mapping from an algebraic subset is an isomorphism onto the Zariski closure of its image.

THEOREM 2 (M. Kwieciński [9]). *Let $F = (F_1, \dots, F_n) : \Bbbk^n \to \Bbbk^n$ be a polynomial mapping, let V be a non-empty algebraic subset of $\Bbbk^n$, and let $\{P_1(X), \dots, P_s(X)\} \subset \Bbbk[X]$ be generators of the ideal $I(V)$. Let $\mathcal{B}$ be the reduced Gröbner basis of the ideal*

$$J = \langle Y_1 - F_1(X), \dots, Y_n - F_n(X), P_1(X), \dots, P_s(X)\rangle$$

with respect to a fixed X-eliminating ordering. Then $F|_V : V \to \overline{F(V)}$ is an isomorphism if and only if $\mathcal{B} = \mathcal{B}_{\mathrm{inv}} \cup \mathcal{B}_{\mathrm{im}}$ where $\mathcal{B}_{\mathrm{inv}} = \{X_1 - G_1(Y), \dots, X_n - G_n(Y)\}$ for some $G_i \in \Bbbk[Y]$ and either $\mathcal{B}_{\mathrm{im}} = \emptyset$ or $\mathcal{B}_{\mathrm{im}} = \{Q_1(Y), \dots, Q_r(Y)\}$ for some $Q_i \in \Bbbk[Y]$. In this case $\mathcal{B}_{\mathrm{im}}$ is the reduced Gröbner basis of the ideal $I(F(V))$ and the mapping $G = (G_1, \dots, G_n)|_{\overline{F(V)}}$ is the inverse of $F|_V$.

Now we describe the reduced Gröbner basis of the ideal J from the previous theorem in the case when I is an arbitrary ideal, not necessarily radical.

Let $F = (F_1, \dots, F_n) : \Bbbk^n \to \Bbbk^n$ be a polynomial automorphism and let $I = \langle R_1(X), \dots, R_s(X)\rangle$ be an ideal in $\Bbbk[X]$. The automorphism F induces a $\Bbbk$-algebra isomorphism $F^* : \Bbbk[Y] \to \Bbbk[X]$ given by the formula $F^*(P) = P \circ F$ for any $P \in \Bbbk[Y]$.

THEOREM 3. *If $I \neq \Bbbk[X]$ then the reduced Gröbner basis $\mathcal{B}$ of the ideal*

$$J = \langle Y_1 - F_1(X), \dots, Y_n - F_n(X), R_1(X), \dots, R_s(X)\rangle$$

with respect to a fixed X-eliminating ordering $\prec$ has the form

$$\{X_1 - \widetilde{G}_1(Y), \dots, X_n - \widetilde{G}_n(Y), Q_1(Y), \dots, Q_t(Y)\}$$

for some $\widetilde{G}_1(Y), \dots, \widetilde{G}_n(Y), Q_1(Y), \dots, Q_t(Y) \in \Bbbk[Y]$.

Moreover $\{Q_1(Y), \dots, Q_t(Y)\}$ is the reduced Gröbner basis of the ideal $G^*(I) \subseteq \Bbbk[Y]$ and $\widetilde{G}_i(Y) - G_i(Y) \in G^*(I)$ for $i = 1, \dots, n$.

Proof. Since the polynomials $X_1 - G_1(Y), \dots, X_n - G_n(Y)$ belong to $\langle Y_1 - F_1(X), \dots, Y_n - F_n(X)\rangle$ which is the ideal of the graph of F, they also belong to J. The ordering $\prec$ is X-eliminating, hence $\mathrm{LT}(X_i - G_i(Y)) = X_i$. Suppose that $0 \in \Delta(J)$. Then $1 \in J$ and

$$\begin{aligned} 1 = {} & h_1(X,Y)(Y_1 - F_1(X)) + \dots + h_n(X,Y)(Y_n - F_n(X)) \\ & + h_{n+1}(X,Y)R_1(X) + \dots + h_{n+s}(X,Y)R_s(X) \end{aligned}$$

for some $h_1, \dots, h_{n+s} \in \Bbbk[X, Y]$. Substituting $Y_i = F_i(X)$ we get

$$1 = h_{n+1}(X, F(X))R_1(X) + \cdots + h_{n+s}(X, F(X))R_s(X),$$

which contradicts our assumption that $I \neq \Bbbk[X]$. Therefore, $0 \notin \Delta(I)$, which implies that the multi-indices $\operatorname{mdeg}(X_i)$ for $i = 1, \dots, n$ belong to the minimal basis of the set $\Delta(J)$. Consequently, the reduced Gröbner basis of J consists of polynomials of the form $X_i - \widetilde{G}_i(Y)$ $(i = 1, \dots, n)$ and a number of polynomials $Q_1(Y), \dots, Q_t(Y) \in \Bbbk[Y]$, so the basis has the form

$$\{X_1 - \widetilde{G}_1(Y), \dots, X_n - \widetilde{G}_n(Y), Q_1(Y), \dots, Q_t(Y)\}.$$

Since the ordering $\prec$ is X-eliminating, $\{Q_1(Y), \dots, Q_t(Y)\} = \mathcal{B} \cap \Bbbk[Y]$ is the reduced Gröbner basis of the ideal $J \cap \Bbbk[Y]$ with respect to the restriction of $\prec$ to $T(Y)$. Now we show that $J \cap \Bbbk[Y] = G^*(I)$.

Let $Q(Y) \in J \cap \Bbbk[Y]$. We have

$$\begin{aligned} Q(Y) = {} & k_1(X, Y)(Y_1 - F_1(X)) + \cdots + k_n(X, Y)(Y_n - F_n(X)) \\ & + l_1(X, Y)R_1(X) + \cdots + l_s(X, Y)R_s(X) \end{aligned}$$

for some $k_1, \dots, k_n, l_1, \dots, l_s \in \Bbbk[X, Y]$. Substituting $G_i(Y)$ for X_i we get

$$Q(Y) = l_1(G(Y), Y)R_1(G(Y)) + \cdots + l_s(G(Y), Y)R_s(G(Y)) \in G^*(I),$$

which implies that $J \cap \Bbbk[Y] \subseteq G^*(I)$.

To prove the opposite inclusion notice that

$$\{X_1 - G_1(Y), \dots, X_n - G_n(Y), Q_1(X), \dots, Q_t(Y)\}$$

is also a (not necessarily reduced) Gröbner basis of J. In particular, this set generates the ideal J, hence for $j = 1, \dots, s$ we have

$$\begin{aligned} R_j(X) = {} & k_1(X, Y)(X_1 - G_1(Y)) + \cdots + k_n(X, Y)(X_n - G_n(Y)) \\ & + l_1(X, Y)Q_1(Y) + \cdots + l_t(X, Y)Q_t(Y) \end{aligned}$$

for some $k_1, \dots, k_n, l_1, \dots, l_t \in \Bbbk[X, Y]$. Substituting once more $G_i(Y)$ for X_i we obtain

$$R_j(G(Y)) = l_1(G(Y), Y)Q_1(Y) + \cdots + l_t(G(Y), Y)Q_t(Y) \in J.$$

Thus, $G^*(I) = \langle G^*(R_1), \dots, G^*(R_s) \rangle \subseteq J \cap \Bbbk[Y]$.

To complete the proof it is sufficient to notice that

$$\widetilde{G}_i(Y) - G_i(Y) = (X_i - G_i(Y)) - (X_i - \widetilde{G}_i(Y)) \in J \cap \Bbbk[Y] = G^*(I). \blacksquare$$

Definition 4. An ideal $I \subseteq \Bbbk[X]$ is said to be *reconstructing for an automorphism* $F = (F_1, \dots, F_n) : \Bbbk^n \to \Bbbk^n$ with respect to a fixed admissible ordering $\prec$ if the reduced Gröbner basis of $I + \langle Y_1 - F_1(X), \dots, Y_n - F_n(X) \rangle$ has the form $\{X_1 - G_1(Y), \dots, X_n - G_n(Y), Q_1(Y), \dots, Q_s(Y)\}$, where $G = (G_1, \dots, G_n)$ is the inverse of F.

An ideal $I \subseteq \Bbbk[X]$ is said to be *d-reconstructing* with respect to $\prec$ if it is reconstructing for any automorphism $F : \Bbbk^n \to \Bbbk^n$ of degree not greater than d.

An ideal $I \subseteq \Bbbk[X]$ is said to be *reconstructing* with respect to $\prec$ if it is reconstructing for any automorphism $F : \Bbbk^n \to \Bbbk^n$.

Definition 5. An algebraic set $V \subseteq \Bbbk^n$ is said to be *reconstructing for an automorphism* F (respectively: *d-reconstructing*, *reconstructing*) if the ideal $I(V) \subseteq \Bbbk[X]$ is reconstructing for an automorphism F (respectively: d-reconstructing, reconstructing).

If $I \subseteq \Bbbk[X]$ is a reconstructing ideal for an automorphism $F = (F_1, \ldots, F_n)$ then there exists an effective algorithm for finding F knowing only its "restriction" to I, i.e. knowing the ideal $\langle Y_1 - F_1(X), \ldots, Y_n - F_n(X)\rangle + I$.

Indeed, let $\widetilde{F} = (\widetilde{F}_1, \ldots, \widetilde{F}_n) : \Bbbk^n \to \Bbbk^n$ be a polynomial mapping such that $F_i - \widetilde{F}_i \in I$ for $i = 1, \ldots, n$ and let $R_1, \ldots, R_s \in \Bbbk[X]$ be generators of the ideal I. Then the ideals

$$\langle Y_1 - F_1(X), \ldots, Y_n - F_n(X), R_1(X), \ldots, R_s(X)\rangle$$

and

$$\langle Y_1 - \widetilde{F}_1(X), \ldots, Y_n - \widetilde{F}_n(X), R_1(X), \ldots, R_s(X)\rangle$$

in $\Bbbk[X, Y]$ are equal.

Knowing the generators we can determine the reduced Gröbner basis of this ideal with respect to an X-eliminating admissible ordering on $T(X, Y)$. From the definition of a reconstructing ideal it follows that the basis has the form $\{X_1 - G_1(Y), \ldots, X_n - G_n(Y), Q_1(Y), \ldots, Q_t(Y)\}$, where $G = (G_1, \ldots, G_n)$ is the inverse of F. Having determined $G_1, \ldots, G_n$ we can now calculate the Gröbner basis of $\langle X_1 - G_1(Y), \ldots, X_n - G_n(Y)\rangle$ with respect to any Y-eliminating ordering on $T(X, Y)$. By Theorem 1 we will get the set $\{Y_1 - F_1(X), \ldots, Y_n - F_n(X)\}$ obtaining in this way the automorphism $F = (F_1, \ldots, F_n)$.

In what follows, we will need a criterion for deciding if an ideal is reconstructing for an automorphism F.

Proposition 6. *Let $F = (F_1, \ldots, F_n) : \Bbbk^n \to \Bbbk^n$ be a polynomial automorphism and let $G = (G_1, \ldots, G_n) = F^{-1}$ be the inverse of F. The ideal $I \subseteq \Bbbk[X]$ is reconstructing for F if and only if all components G_i are reduced modulo the ideal $G^*(I)$.*

Proof. Assume that $I \subseteq \Bbbk[X]$ is a reconstructing ideal for an automorphism F. By Definition 4 and Theorem 3 the reduced Gröbner basis of the ideal $I + \langle Y_1 - F_1(X), \ldots, Y_n - F_n(X)\rangle \subseteq \Bbbk[X, Y]$, calculated with respect to an X-eliminating admissible ordering, has the form

$$\{X_1 - G_1(Y), \ldots, X_n - G_n(Y), Q_1(Y), \ldots, Q_s(Y)\}$$

where $\{Q_1(Y),\dots,Q_s(Y)\}$ is the reduced Gröbner basis of $G^*(I)$. Thus, all the polynomials $X_i - G_i(Y)$, and consequently $G_i(Y)$, are reduced modulo $G^*(I)$.

Assume now that the components G_i of the automorphism $G = F^{-1}$ are reduced modulo $G^*(I)$. By Theorem 3 we know that the reduced Gröbner basis of I is equal to

$$\{X_1 - \widetilde{G}_1(Y),\dots,X_n - \widetilde{G}_n(Y), Q_1(Y),\dots,Q_s(Y)\},$$

where $\widetilde{G}_1(Y),\dots,\widetilde{G}_n(Y) \in \Bbbk[Y]$. Thus the polynomials $\widetilde{G}_i(Y)$, $i = 1,\dots,n$, are reduced modulo $G^*(I)$. By assumption, so are all $G_i(Y)$, and hence $G_i(Y) - G^*(I)$ is reduced. Consequently, $\mathrm{NF}(G_i(Y) - \widetilde{G}_i(Y), G^*(I)) = G_i(Y) - \widetilde{G}_i(Y)$. On the other hand, by Theorem 3, $G_i(Y) - G^*(I) \in G^*(I)$, which implies that $\mathrm{NF}(G_i(Y) - \widetilde{G}_i(Y), G^*(I)) = 0$. Thus $G_i(Y) = \widetilde{G}_i(Y)$, which completes the proof. ∎

4. Sequences of reconstructing ideals and sets. Let $I_1 \supseteq I_2 \supseteq \cdots$ be a decreasing sequence of ideals of $\Bbbk[X_1,\dots,X_n]$, and $I = \bigcap_{i=1}^{\infty} I_i$. The following example, which is a modification of an example from [1], shows that I may be a reconstructing ideal for an automorphism F although none of I_i shares this property.

Example 7. Equip $T(X_1, X_2, Y_1, Y_2)$ with a lexicographic ordering such that $X_1 > X_2 > Y_1 > Y_2$ and choose a sequence of natural numbers ϱ_ν such that $\varrho_{\nu+1} > \nu\varrho_\nu$ for $\nu \in \mathbb{N}$. Let $F : \Bbbk^2 \to \Bbbk^2$ be the automorphism $F(X_1, X_2) = (X_1 - X_2, X_2)$ and define a decreasing sequence of ideals

$$I_\nu = \Big\langle X_1 - \sum_{\mu<\nu} c_\mu X_2^{\varrho_\mu}, X_2^{\varrho_\nu} \Big\rangle \subseteq \Bbbk[X]$$

for $\nu \in \mathbb{N}$. We will show that for any $\nu \in \mathbb{N}$ the ideal I_ν is not reconstructing for F, but I is.

Proof. In [1] it was shown that the sequence $(I_\nu)_{\nu\in\mathbb{N}}$ is decreasing and $I = \bigcap_{i=1}^{\infty} I_i = \emptyset$. The empty set is obviously a reconstructing set.

Let $G(Y_1, Y_2) := (Y_1 + Y_2, Y_2) = F^{-1}$. The ideal I_ν is not reconstructing for F because $X_1 - G_1(Y_1, Y_2) = X_1 - Y_1 - Y_2$ is not reduced modulo $G^*(X_1 - \sum_{\mu<\nu} X_2^{\varrho_\mu}) = Y_1 + Y_2 - \sum_{\mu<\nu} Y_2^{\varrho_\mu}$. ∎

Our goal is to show that, under some assumptions on the ordering, any d-reconstructing set V can be approximated by a sequence of finite subsets of V which are also d-reconstructing.

Let $\mathcal{P} = \{P_1,\dots,P_r\} \subseteq \Bbbk^n$, $\mathcal{D} = \{\alpha^{(1)},\dots,\alpha^{(s)}\} \subseteq \mathbb{N}^n$ and assume that $\alpha^{(i)} \prec \alpha^{(j)}$ $(i < j)$, where $\prec$ is a fixed admissible ordering. Set

$$M(\mathcal{D},\mathcal{P}) = \begin{pmatrix} P_1^{\alpha^{(1)}} & \dots & P_1^{\alpha^{(s)}} \\ \vdots & \ddots & \vdots \\ P_r^{\alpha^{(1)}} & \dots & P_r^{\alpha^{(s)}} \end{pmatrix}.$$

In [2] the following theorem was proved.

THEOREM 8 ([2]). *Let $I = I(V) \subseteq \Bbbk[X]$ be the ideal of an algebraic set $V \subseteq \Bbbk^n$ and let $\mathcal{P} = \{P_1, \dots, P_\mu\} \subseteq V$ be a sequence of pairwise different points. Then for any fixed admissible ordering $\prec$ we have*

$$D(I(\mathcal{P})) = D^{(\mu)}(I) \;\Leftrightarrow\; \det M(D^{(\mu)}(I), \mathcal{P}) \neq 0.$$

We have the following corollary from Theorem 8:

COROLLARY 9. *Let $I = I(V) \subseteq \Bbbk[X]$ be the ideal of an algebraic set $V \subseteq \Bbbk^n$, and $\mathcal{P} = (P_i)_{i\in\mathbb{N}}$ a sequence of pairwise different points of V. Fix an admissible ordering on $T(X)$ and assume that there exists $\mu \in \mathbb{N}$ such that $D^{(\mu+1)}(I) \setminus D(I(\mathcal{P})) \neq \emptyset$. Then for any subset $\mathcal{P}'$ of $\mathcal{P}$ consisting of $\mu+1$ elements we have*

$$\det M(D^{(\mu+1)}(I), \mathcal{P}') = 0.$$

Proof. Suppose that there exists a subset $\mathcal{P}' \subseteq \mathcal{P}$ consisting of $\mu+1$ elements such that $\det M(D^{(\mu+1)}(I), \mathcal{P}') \neq 0$. By Theorem 8 we have $D^{(\mu+1)}(I) = D(I(\mathcal{P}')) \subseteq D(I(\mathcal{P}))$, which contradicts our assumption. ∎

The following technical lemma is the base of the proof of Theorem 16 below.

LEMMA 10. *For any admissible string-type ordering $\prec$ on $T(X)$ there exists an increasing function $\varphi_\prec : \mathbb{N} \to \mathbb{N}$ such that for any ideal $I \subseteq \Bbbk[X]$ and any polynomial $f \in \Bbbk[X] \setminus I$ there exists $\alpha \in D(I) \setminus D(I + (f))$ such that $|\alpha| \leq \varphi_\prec(\deg(f))$.*

Proof. Fix a string-type admissible ordering $\prec$ on $T(X)$. Let $\psi_\prec(\beta) := \max\{|\alpha| : \alpha \preceq \beta\}$ for $\beta \in \mathbb{N}^n$. This function is well defined because $\prec$ is a string-type ordering. We will show that one can take $\varphi_\prec(d) := \max\{\psi_\prec(\beta) : |\beta| \leq d\}$.

Indeed, let $h = \mathrm{NF}(f, I)$ be the reduced form of a polynomial f with respect to the ideal I. We know that $h \in I + (f)$, so $\mathrm{mdeg}(h) \notin D(I + (f))$. On the other hand, $\mathrm{mdeg}(h) \in D(I)$, so $\mathrm{mdeg}(h) \in D(I) \setminus D(I + (f))$.

It is clear that $\mathrm{mdeg}(h) \preceq \mathrm{mdeg}(f)$, hence $|\mathrm{mdeg}(h)| \leq \psi_\prec(\mathrm{mdeg}(f))$. On the other hand, $|\mathrm{mdeg}(f)| \leq \deg(f)$, which implies $\psi_\prec(\mathrm{mdeg}(f)) \leq \varphi_\prec(\deg(f))$ and $|\mathrm{mdeg}(h)| \leq \varphi_\prec(\deg(f))$.

To complete the proof, notice that the function $\psi_\prec$, and hence $\varphi_\prec$, is increasing. ∎

LEMMA 11. *Let $\mathcal{P} = \{P_1, \dots, P_\nu\}$ be a finite subset of an algebraic set $V \subseteq \Bbbk^n$ and fix an admissible ordering $\prec$. If there exists $\mu \leq \nu$ such that $D^{(\mu)}(I(V)) \subseteq D(I(\mathcal{P}))$, then there exists a subset $\mathcal{P}'$ of $\mathcal{P}$ consisting of μ elements such that*

$$\det M(D^{(\mu)}(I(V)), \mathcal{P}') \neq 0.$$

Proof. The set $\{X^\alpha : \alpha \in D(I(\mathcal{P}))\}$ is a base of the vector space $\Bbbk[X]/I(\mathcal{P})$ over $\Bbbk$, thus $\det M(D(I(\mathcal{P})), \mathcal{P}) \neq 0$. The columns of this matrix are linearly independent over $\Bbbk$ and contained in $M(D^{(\mu)}(I(V)), \mathcal{P})$, hence the rank of the latter matrix is μ. We can define $\mathcal{P}'$ to consist of those μ points which correspond to μ linearly independent rows of that matrix. ∎

In [2] a notion of a special system of points *admissible for interpolation* was introduced. This notion will be crucial in our considerations.

DEFINITION 12 ([2]). Let $V \subseteq \Bbbk^n$ be an algebraic set. Denote by $I = I(V)$ the ideal of V and fix an admissible ordering $\prec$. A finite subset $\mathcal{P} \subseteq V$ is said to be *admissible for interpolation on V* (with respect to the ordering $\prec$) if $D(I(\mathcal{P})) = D^{(\mu)}(I)$, where $\mu = \#\mathcal{P}$.

DEFINITION 13. Let $V \subseteq \Bbbk^n$ be an algebraic set. Denote by $I = I(V)$ the ideal of V and fix an admissible ordering $\prec$. An infinite sequence $P_1, P_2, \dots$ of pairwise different points $P_i \in V$ is said to be *admissible for interpolation on V* (with respect to the ordering $\prec$) if for any $r \in \mathbb{N}$ the finite set $\{P_1, \dots, P_r\}$ is admissible for interpolation on V.

In [2] one can find the following proposition.

PROPOSITION 14 ([2]). *Fix an admissible ordering on $T(X)$. Then every infinite algebraic subset $V \subseteq \Bbbk^n$ contains an infinite admissible sequence of pairwise different points $P_1, P_2, \dots$.*

The next proposition is a key step in the proof of Theorem 16.

PROPOSITION 15. *Fix a string-type ordering $\prec$ and let $I = I(V) \subseteq \Bbbk[X]$ be the ideal of an algebraic set $V \subseteq \Bbbk^n$. Let $\mathcal{P} = \{P_1, P_2, \dots\}$ be a sequence of points admissible for interpolation on V, and let $I(\mathcal{P}) \subseteq \Bbbk[X]$ be its ideal. Let $F : \Bbbk^n \to \Bbbk^n$ be a polynomial automorphism and define $J = F^*(I)$, $J_\nu = I(\{F(P_1), \dots, F(P_\nu)\})$ for $\nu = 1, 2, \dots$. If $\bigcap_{\nu=1}^{\infty} I(\{P_1, \dots, P_\nu\}) = I$ then for any $m \in \mathbb{N}$ there exists $\mu_m \in \mathbb{N}$ (depending on $\deg F$) such that $D^{(m)}(J) \subseteq D(J_\nu)$ for $\nu \geq \mu_m$.*

Proof. We will use induction on m. For $m = 1$ we can take $\mu_1 = 1$.

Assume that the statement is true for m. Thus $D^{(m)}(J) \subseteq D(J_\nu)$ for $\nu \geq \mu_m$. Let α_{m+1} be the $(m+1)$-st element of $D(J)$ (in the fixed admissible ordering) and define $\gamma := \max\{\deg(F(X)^{\alpha_i}) : i = 1, \dots, m+1\} \in \mathbb{N}$ and $\beta := \max_\prec\{\alpha \in \mathbb{N}^n : |\alpha| \leq \varphi_\prec(\gamma)\} \in \mathbb{N}^n$ (β is well defined because $\prec$ is a

string-type ordering). We will show that we can take $\mu_{m+1} := \#\{\alpha \in \mathbb{N}^n : \alpha \prec \beta\} + 1$.

Suppose this is not true, hence $\alpha_{m+1} \notin D(J_\nu)$ for some $\nu \geq \mu_{m+1}$. Because $D^{(m)}(J) \subseteq D(J_\nu)$ for $\nu \geq \mu_m$, Lemma 11 implies that we can choose a subset $\mathcal{P}' \subseteq \{P_i : i = 1, \ldots, \nu\}$ consisting of m elements and such that $\det M(D^{(m)}(J), F(\mathcal{P}')) \neq 0$. Notice that

$$\det \begin{pmatrix} M(D^{(m)}(J), F(\mathcal{P}')) & M(\alpha_{m+1}, F(\mathcal{P}')) \\ M(D^{(m)}(J), F(P_i)) & F(P_i)^{\alpha_{m+1}} \end{pmatrix} = 0$$

for $i = 1, \ldots, \nu$. This is clear for $P \in \mathcal{P}'$ and it follows from Corollary 9 for the other points.

This implies that all P_i are roots of the polynomial $h(F(X)) \in \Bbbk[X]$ of degree not greater than γ, where $h \in \Bbbk[Y]$ is defined by

$$h(Y) = \det \begin{pmatrix} M(D^{(m)}(J), F(\mathcal{P}')) & M(\alpha_{m+1}, F(\mathcal{P}')) \\ M(D^{(m)}(J), Y) & Y^{\alpha_{m+1}} \end{pmatrix}.$$

The coefficient of the term $Y^{\alpha_{m+1}}$ of h is $M(D^{(m)}(J), F(\mathcal{P}')) \neq 0$, so $h \neq 0$. Notice that $\operatorname{supp}(h) \subseteq D^{(m+1)}(J) \subseteq D(J)$, thus $h \notin J$, and consequently $h(F) \notin I$. By Lemma 10 this implies that there exists a polynomial $g \notin I$ such that $h - g \in I$ and

$$|\operatorname{mdeg}(g)| \leq \varphi(\deg(h(F))) \leq \varphi(\gamma).$$

The ordering $\prec$ is string-type, hence we can arrange the elements of $D(I)$ into an increasing sequence ordered by $\prec$. Let k be the position of the element $\operatorname{mdeg}(g)$ in this sequence. We have $k \leq \mu_{m+1}$. On the other hand, $\mathcal{P}$ is admissible for interpolation on V, which implies $D(I_k) = D^{(k)}(I)$, where $I_k = I(\{P_1, \ldots, P_k\})$. Thus $g \in I_k$ and $I \cup \langle g \rangle \subseteq I_k$. But $\operatorname{mdeg}(g) \in D(I_k) \subseteq D(I \cup \langle h \rangle)$, which leads to a contradiction. ∎

We are in a position to prove the main theorem.

THEOREM 16. *Let $I = I(V)$ be a d-reconstructing ideal, and $P_1, P_2, \ldots \in V$ a sequence of points admissible for interpolation such that $I = \bigcap_{\nu=1}^{\infty} I_\nu$, where $I_\nu = I(P_1, \ldots, P_\nu)$. Fix a string-type admissible ordering on $T(Y)$. Then there exists $\mu \in \mathbb{N}$ such that the ideal I_ν is d-reconstructing for any $\nu > \mu$.*

Proof. Let $F = (F_1, \ldots, F_n)$ be a polynomial automorphism of degree not greater than d. Let $H = (H_1, \ldots, H_n) = F^{-1}$ be the inverse of F. It is known that $\deg(H) \leq d^{n-1}$. Moreover, we know that the components of the automorphism H are reduced modulo $H^*(I)$, where $H^* : \Bbbk[X] \to \Bbbk[Y]$ is the isomorphism of rings given by

$$H^*(F) = F \circ H = F(H_1, \ldots, H_n).$$

Setting $J = H^*(I)$ and $J_\nu = H^*(I_\nu)$ we have

$$J = \bigcap_{\nu=1}^{\infty} J_\nu.$$

Let $e = d^{n-1}$ and let $D_e = \{\alpha \in \mathbb{N}^n : |\alpha| \leq e\}$. To prove the theorem it suffices to find μ such that for any $\nu \geq \mu$ we have $D_{J_\nu} \cap D_e = D_J \cap D_e$. Let β be the greatest element of the set $D(J) \cap D_e$ with respect to the ordering $\prec$. By Proposition 15 we can take $\mu = \mu_m$, where $m = \#\{\alpha \in D_J : \alpha \preceq \beta\}$. ∎

References

[1] J. Apel, J. Stückrad, P. Tworzewski, and T. Winiarski, *Intersection of sequences of ideals generated by polynomials*, J. Pure Appl. Algebra 131 (1998), 1–12.

[2] —, —, —, —, *Term bases for multivariate interpolation of Hermite type*, Univ. Iagel. Acta Math. 37 (1999), 37–49.

[3] T. Becker, H. Kredel, and V. Weispfenning, *Gröbner Bases. A Computational Approach to Commutative Algebra*, Springer, 1993.

[4] D. Cox, J. Little, and D. O'Shea, *Ideals*, *Varieties*, *and Algorithms*, Springer, 1992.

[5] A. van den Essen, *A criterion to decide if a polynomial map is invertible and to compute its inverse*, Comm. Algebra 18 (1990), 3183–3186.

[6] A. van den Essen and M. Kwieciński, *On the reconstruction of polynomial automorphisms from their face polynomials*, J. Pure Appl. Algebra 80 (1992), 327–336.

[7] P. Gniadek, *On reconstruction of polynomial automorphisms*, Ann. Polon. Math. 61 (1996), 61–69.

[8] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra*, Springer, 2000.

[9] M. Kwieciński, *A Gröbner basis criterion for isomorphisms of algebraic varieties*, J. Pure Appl. Algebra 74 (1991), 275–279.

[10] —, *Automorphisms from face polynomials via two Gröbner bases*, ibid. 82 (1992), 65–70.

[11] J. McKay and S. Wang, *An inversion formula for two polynomials in two variables*, ibid. 52 (1988), 103–119.

[12] K. Rusek and T. Winiarski, *Polynomial automorphisms of* $\mathbb{C}^n$, Univ. Iagel. Acta Math. 24 (1984), 143–149.

Institute of Mathematics
Jagiellonian University
Reymonta 4
30-059 Kraków, Poland
E-mail: Pawel.Gniadek@im.uj.edu.pl

Received 11.4.2006
and in final form 24.1.2007 (1568)