Canonical Bases: Relations with Standard Bases, Finiteness Conditions and Application to Tame Automorphisms⋆

François Ollivier

Laboratoire d'Informatique de l'X (LIX) ∗
École Polytechnique
F-91128 Palaiseau Cedex (France)

cffoll@frpoly11.BITNET
ollivier@cmep.polytechnique.fr

February, 3rd 1994

Abstract: Canonical bases for k-subalgeras of $k[x_1, \ldots, x_n]$ are analogs of standard bases for ideals. They form a set of generators, which allows to answer the membership problem by a reduction process. Unfortunately, they may be infinite even for finitely generated subalgeras. We redefine canonical bases, and for that we recall some properties of monoids, k-algebras of monoids and "binomial" ideals, which play an essential role in our presentation and the implementation we made in the IBM computer algebra system Scratchpad II. We complete the already known relations between standard bases and canonical bases by generalizing the notion of standard bases for ideals of any k-subalgebra admitting a finite canonical basis. We also have a way of finding a set of generators of the ideal of relations between elements of a canonical basis, which is a standard basis for some ordering.

We then turn to finiteness conditions, and investigate the case of integrally closed subalgebras. We show that if some integral extension B of a subalgebra A admits a finite canonical basis, we have an algorithm to solve the membership problem for A, by computing the generalized standard basis of a B-ideal. We conjecture that any integrally closed subalgebra admits a finite canonical basis, and provide partial results.

There is a simple case, but of special interest, where the complexity of computing a canonical basis is known: the case where $k[f_1, \ldots, f_n] = k[x_1, \ldots, x_n]$. We show that the canonical bases procedure give more information than previously known methods and may provide a tool for the tame generators conjecture.

0. Introduction

Standard bases first appeared in the work of Hironaka and became one of the main tools in computer algebra for solving systems of algebraic equations. This notion is very natural, and Janet in 1920, working on partial differential equations, described particular sets of generators of an ideal, which are not far from standard bases theory. Canonical bases seem to have a much shorter history.

Indeed, previously known methods like that of Shannon and Sweedler (see [SS]) for solving the membership problem in the case of an k-subalgebra $k[f_1, \ldots, f_m]$, uses the ideal defining the graph of the polynomial map f associated to $f_1, \ldots, f_m$, and standard bases. Nearly at the same time, in 1986, Kapur and Madlener discovered a direct approach, introducing canonical bases (see [KM]). Independently, Robbiano and Sweedler defined the same objects, which they called SAGBI, standing for subalgebra analog of Groebner bases of ideals (see [RS]). They have shown that it is possible to translate many properties of standard bases in the vocabulary of canonical bases.

We will complete those works, by a description of a first implementation of canonical bases, which is an essential step to have a precise idea of their efficiency, and new relations with standard bases, who belong to the folklore but also have practical consequences. The main difference is that k-subalgebras of $k[n]$ do not satisfy the ascending chain condition. As a consequence, there exist finitely generated k-subalgebras with

⋆ Partially supported by GDR G0060 *Calcul Formel, Algorithmes, Langages et Systèmes* and PRC *Mathématiques et Informatique*.

∗ Équipe Algèbre et Géométrie Algorithmiques, Calcul Formel, SDI CNRS n° 6176 et Centre de Mathématiques, Unité de Recherche Associée au CNRS n° D0169 infinite canonical basis already in 2 variables, as proved by ROBBIANO. This serious drawback apparently discouraged Kapur and Madlener to publish their work earlier.

Anyway, it is easy to provide examples where the canonical basis computation is almost free whereas it is impossible to compute the standard basis of Shannon and Sweedler's method on any existing computer. In the worst cases, standard bases calculations may have a double exponential complexity, and for a practical point of view, it is the same as if it would never stop. It is one of the major issues in that field to determine "good cases", with reasonable complexity, starting with the works of Lazard on -1 or 0-dimensional cases (see [L] and [G]). We may think that there is a strong relation with good complexity and "nice" algebraic properties of the ideal.

For canonical bases, nothing is known yet. If we analyse the examples given by ROBBIANO of finitely generated k-subalgebras with infinite canonical bases, we can remark that they are not integrally closed. This situation led us to conjecture that the canonical basis is finite for any integrally closed k-subalgebra (see [O2]). At least, we can prove a general relation between the canonical basis of a subalgebra and that of its integral closure. We will provide partial results and illustrate the practical consequences of a positive answer to our conjecture.

Investigating the simple case $k[f_1, \ldots, f_n] = k[x_1, \ldots, x_n]$, we show that we have a bound on the complexity of the standard basis computation, which is of the same order—simple exponential—as for the graph method, but yet smaller (see [O1]). If $f_1, \ldots, f_n$ determine a "generic" tame automorphism, the complexity is even better for canonical bases. This gives new interest to the tame generator conjecture, and canonical bases are shown to split any generic tame automorphism into a composition of elementary generators.

1. Monoids and Standard Bases

If not stated otherwise, k will denote a field of arbitrary characteristic, $k[n]$ the k-algebra of polynomials in n variables $k[x_1, \ldots, x_n]$ and M an abelian monoid with additive law. If E is a subset of M, $\mathrm{Mon}E$ *will denote the submonoid generated by E.*

1.1. Abelian Monoids and Algebras of Monoids

Before coming to canonical bases, we need first some results about abelian monoids. Although they are "well known", it is best to introduce them explicitly. The reader can refer to the work of JOUANOLOU in [Jo] for a complete exposition. As we will only consider abelian monoids, we will denote them simply by monoids, and monoideals will be both right and left monoideals.

We recall that an abelian monoid M been given, any subset I of M such that $x \in I$ implies $yx \in I$ for all $y \in M$ is called a monoideal. Any monoid has a natural structure of poset, with a partial ordering defined by $x \leq y$ if there exists z such that $x + z = y$. This ordering is admissible for the monoid structure, i.e. $x \leq y$ implies that $zx \leq zy$. For any admissible partial ordering $\prec$, we may define the *e-set* generated by a subset S of M to be the set $\mathcal{E}(E) = \{x \in M \mid \exists y \in S\ x \succeq y\}$. For $\leq$, e-sets are monoideals.

It is known that we can associate to any abelian monoid M an abelian k-algebra $k[M]$; the polynomial algebra $k[n]$ is $k[\mathbf{N}^n]$. If M is a submonoid of $\mathbf{N}^n$, we can consider $k[M]$ as a k-subalgebra of $k[n]$. In general, denoting by $\mathbf{N}^{(S)}$ the free abelian monoid generated by a set S, the polynomial algebra $k[S]$ is the monoid algebra $k[\mathbf{N}^{(S)}]$. There are close relations between properties of the monoids and properties of their k-algebras. For example, any finitely generated monoid is coherent for the ordering coming from its monoid structure, which means that every e-set, or monoideal in this case, is finitely generated. This property implies that for any finitely generated monoid M, the ring $k[M]$ is noetherian as it is the case for $k[n]$. The situation is not so good when submonoids of $\mathbf{N}^n$ are considered. They may be of infinite type, except for $n = 1$. As a consequence, there exist k-subalgebras of $k[n]$ of infinite type.

There is a natural bijection between admissible orderings on monomials of $k[n]$ and admissible orderings on $\mathbf{N}^n$. An admissible ordering $\prec$ being chosen, we can associate to any non-zero polynomial $P = cx_1^{\alpha_1} \cdots x_n^{\alpha_n} + \cdots$ in $k[n]$ its multidegree $\mathrm{mdeg}P = (\alpha_1, \ldots, \alpha_n) \in \mathbf{N}^n$. Then, for any ideal I (resp k-subalgebra A) of $k[n]$, the set $\{\mathrm{mdeg}P | P \in I\}$ (resp. $\{\mathrm{mdeg}P | P \in A\}$) is a monoideal (resp. submonoid) of $\mathbf{N}^n$.

PROPOSITION 1. *Let $\prec$ be an admissible ordering on $\mathbf{N}^n$, then any chain*

$$x_0 \succ x_1 \succ \cdots \succ x_k \succ x_{k+1} \succ \cdots$$

is finite. ∎

COROLLARY 2. *Any submonoid M of $\mathbf{N}^n$ admits a minimal set of generators.*

PROOF. We only have to consider the set of minimal elements for the natural ordering $<$, which is the wanted set. ∎

1.2. The Graph Method for Monomial Ideals

We will give relations between congruences on a monoid M and binomial ideals of $k[M]$. A binomial ideal of $k[M]$ is an ideal generated by polynomials of the form $m - m'$ where m and m' are primitive monomials. A congruence on a monoid M is an equivalence relation $\equiv$ between elements of M such that $\forall (x, y, z) \in M^3 \quad x \equiv y \Rightarrow zx \equiv zy$. The monoid structure of M induces then a unique monoid structure on the set of equivalence classes $M/\equiv$.

PROPOSITION 1. *An equivalence relation $\equiv\ \subset M \times M$ on a monoid M is a congruence iff $\equiv$ is a submonoid of $M \times M$.*

PROOF. See [Jo 1.4.1 p. 14]. ∎

PROPOSITION 2. *Let R be an integral domain and $\equiv$ a congruence on the monoid M, we associate to it the binomial ideal of $R[M]$ generated by the polynomials of the form $m - m'$ such that $m \equiv m'$. Then, for any two elements m, m' of M, $m \equiv m' \Leftrightarrow m - m' \in I$.*

PROOF. See [MM lemmas 1 and 2 p. 311], where a proof is given for $R = \mathbf{Z}$, which generalizes to any integral domain. ∎

We will need the following proposition, which allows to build a "standard basis" for a congruence by computing a standard basis for the associated ideal.

PROPOSITION 3. *Let $\equiv$ be a congruence on $\mathbf{N}^n$ and I the binomial ideal associated to $\equiv$ as in the previous proposition, then for any total compatible ordering on monomials of $k[n]$ the polynomials in the standard basis G of I are differences of monomials and the set $\{(m, m') | m - m' \in G\}$ generates the congruence.*

PROOF. It is easy to see that the polynomials in G are differences of monomials, for I is binomial and any S-polynomial coming from a syzygy between $x - y$ and $z - t$ is of the form $my - m't$, so that it is still a difference of monomials.

The last part is true by the proof of [Jo cor. 1.6.6.2. p. 34]. ∎

COROLLARY 4. *(Theorem of Redei) Every congruence in $\mathbf{N}^n$ is finitely generated.* ∎

COROLLARY 5. *Let $\phi : \mathbf{N}^n \mapsto \mathbf{N}^m$ and $\psi : \mathbf{N}^\ell \mapsto \mathbf{N}^m$ be two morphisms of monoids and M the subset of $\mathbf{N}^n \times \mathbf{N}^\ell$ defined by $M = \{(x, y) | \phi(x) = \psi(y)\}$, then M is a finitely generated monoid.* ∎

REMARK 6. It is known (see [R1]) that every admissible preordering in $\mathbf{N}^n$ is induced by a morphism of monoid $\phi : \mathbf{N}^n \mapsto \mathbf{R}^m$, where $\mathbf{R}^m$ is ordered by the pure lexicographic ordering. Such orderings were already used by RIQUIER and JANET. ROBBIANO has given a complete description of those orderings and shown that we can take $m \leq n$. If we consider a subset S of $k[n]$, and the k-algebra morphism $\psi : k[\mathbf{N}^{(S)}] \mapsto k[n]$ defined by $\psi(R) = R(S)$, any admissible ordering on $k[n]$ induces an admissible preordering of $k[\mathbf{N}^{(S)}]$, and so a graduation of $k[\mathbf{N}^{(S)}]$.

THEOREM 7. *Let $A = k[P_1, \ldots, P_m]$ be a k-subalgebra of $k[x_1, \ldots, x_n]$ and G be the standard basis of the ideal $I = (P_i - y_i)_{k[x_1,\ldots,x_n,y_1,\ldots,y_m]}$ for an admissible ordering which eliminates the x_i, then $Q \in A$ iff $Q \xrightarrow{G^\star} R(y)$.*

Furthermore the subset of G of polynomials which do not involve any x_i is a standard basis of $I \cap k[y] = \{R | R(P) = 0\}$.

PROOF. See [SS]. ∎

COROLLARY 8. *Let M be the submonoid of $\mathbf{N}^n$ generated by the finite set $\{\alpha_i;\ i \in [1,m]\}$. We define on $\mathbf{N}^n \times \mathbf{N}^m$ a congruence, associated to the morphism of monoid defined by $\phi(e_i) = m_i$, where e_i stands for the i^{th} elementary generator of $\mathbf{N}^m$, and $\phi(x) = x$ for any x in $\mathbf{N}^n$. We also denote by ϕ the associated morphism of k-algebra. Let $\prec$ denote an admissible ordering on $\mathbf{N}^n$, we extend it to $\mathbf{N}^n \times \mathbf{N}^m$ using ϕ, and complete it to an total ordering $\ll$, eliminating the n first variables. Let G be the standard basis for $\ll$ of the ideal $I = (x^{m_i} - y_i)_{k[x_1,\ldots,x_n,y_1,\ldots,y_m]}$. Then β belongs to M iff $x^\beta \xrightarrow{G} y^\gamma$, and this may be tested by computing only critical pairs up to the rank of β according to the graduation defined by $\prec$.*

The elements of $G \cap k[y]$ generate the congruence induced on $\mathbf{N}^m$ by ϕ.

PROOF. These are simple consequences of the last theorem and prop 3. The bound on the standard basis computation comes from the remark made above and classical considerations on homogeneous ideals, I being homogeneous for the graduation defined by $\prec$. ∎

2. Canonical Bases

We will denote by $k[n]$ the algebra of polynomials in n variables $x_1, \ldots, x_n$. We give ourselves an admissible ordering $\prec$ on monomials of $k[n]$. The leading coefficient of a polynomial P will be denoted by $\mathrm{lc}P$ and the leading primitive monomial of P by $\mathrm{lpm}P$. A will denote a k-subalgebra of $k[n]$. To avoid unuseful complications, we will suppose all polynomials to be monic, if not stated otherwise. It will be easy to think of the necessary modifications if it is not the case.

2.1. Definition

DEFINITION 1. *Let A be a k-subalgebra of $k[n]$ and E a subset of A, we denote by $\mathrm{Mon}E$ the submonoid of $\mathbf{N}^n$ generated by $\{\mathrm{mdeg}P | P \in A\}$. A subset E of A is said to be a canonical basis of A if $\mathrm{Mon}E = \mathrm{Mon}A$.*

Obviously, we have a similar definition for standard bases by replacing k-subalgebra by ideal and submonoid by e-set—or monoideal.

An admissible ordering being given, we can associate to any subset of a k-subalgebra a reduction relation, in the following way.

DEFINITION 2. *Let Q, and Q' be two polynomials of $k[n]$ and C a subset of $k[n]$, then we say that Q is reduced to Q' by C if $\mathrm{mdeg}Q \in \mathrm{Mon}C$ and*

$$Q' = Q - \prod_{i=1}^{k} R_i^{\alpha_i},$$

where the α_i and R_i are integers and elements of C such that $\mathrm{mdeg}Q = \sum_{i=1}^{k} \alpha_i \mathrm{mdeg}R_i$. This relation will be written

$$Q \xrightarrow{P} Q'.$$

We will denote by $\xrightarrow{C^\star}$ the inductive limit of the relation $\xrightarrow{C}$.

We say that P is reduced with respect to C if there is no Q such that $P \xrightarrow{C} Q$, and that P is strongly reduced if P is reduced and the reductum of P is strongly reduced, which means that no monomial of P belongs to $\mathrm{Mon}C$.

DEFINITION 3. *We say that C is a reduced canonical basis of A if C is a canonical basis, the polynomials in C are monic and each polynomial $P \in C$ is strongly reduced with respect to $C \setminus \{P\}$.*

As k is a field, any k-subalgebra A admits a unique reduced canonical basis, which is finite iff A admits a finite canonical basis. We will refer to the reduced canonical basis as *the* canonical basis of A.

Lemma 4. If P belongs to a k-subalgebra A of $k[n]$ and if C is a subset of A, then any polynomial Q such that $P \xrightarrow{C^\star} Q$ belongs to A. ∎

Lemma 5. *Any chain of reduction*

$$Q_0 \xrightarrow{C} Q_1 \ldots Q_{k-1} \xrightarrow{C} Q_k \xrightarrow{C} \ldots$$

has to be finite.

PROOF. This is only a translation of prop 1.1.1. ∎

DEFINITION 6. *If C is a subset of $k[n]$ we can extend any admissible ordering $\prec$ on monomials of $k[n]$ to a preordering on $k[\mathbf{N}^{(C)} \times \mathbf{N}^n]$ by setting $m \prec m' \Leftrightarrow m(C,x) \prec m'(C,x)$. That preordering will be used each time we will deal with polynomials in $k[\mathbf{N}^{(C)} \times \mathbf{N}^n]$ or $k[\mathbf{N}^{(C)}]$. The multidegree of a polynomial R will be then the maximal multidegree of $m(C)$, for all monomials m of R.*

Lemma 7. *If $P \xrightarrow{C^*} 0$, then there exists a polynomial $R \in [\mathbf{N}^{(C)}]$, of multidegree not greater than P, such that $R(C) = P$.*

PROOF. We can build R by reducing P, each step of reduction giving a monomial. The monomials appear then in strictly decreasing order according to $\prec$. ∎

The following notion is an analog of syzygies in the case of standard bases.

DEFINITION 8. *Let C be a subset of $k[n]$, $\{P_1, \ldots, P_\ell\}$ and $\{Q_1, \ldots, Q_m\}$ two finite subsets of C, whose elements are all different, let M be the submonoid of $\mathbf{N}^\ell \times \mathbf{N}^m$ whose elements $((\alpha_1, \ldots, \alpha_\ell), (\beta_1, \ldots, \beta_m))$ satisfy*

$$\sum_{i=1}^{\ell} \alpha_i \mathrm{mdeg} P_i = \sum_{i=1}^{m} \beta_i \mathrm{mdeg} Q_i .$$

Then, we call a superposition between elements of C a 4-uple $((P_1, \ldots, P_\ell), (Q_1, \ldots, Q_m), \alpha, \beta)$, such that (α, β) belongs to the minimal set of generators of M.

The polynomial

$$\prod_{i=1}^{\ell} P_i^{\alpha_i} - \prod_{i=1}^{m} Q_i^{\beta_i}$$

is called the S-polynomial associated to the superposition. The multidegree of the superposition is the common multidegree of both products in the formula above.

REMARK 9. With the same notations, the 2-uples of exponents $((\alpha_P), (\beta_Q))$ associated to all superpositions between elements of C, generate the congruence defined by

$$\sum_{P \in C} \alpha_P \mathrm{mdeg} P = \sum_{Q \in C} \beta_P \mathrm{mdeg} Q .$$

In this case, minimal sets of generators do not exist, but if C is finite, the construction of cor. 1.2.7. provide a finite set of superposition, generating the congruence, which is in general smaller than the set of all superpositions.

DEFINITION 10. *If $\mathcal{S}$ is a set of superpositions generating the congruence defined above, it is said to be a generating set of superpositions. It is said to be confluent if all the corresponding S-polynomials are reduced to 0 by C.*

Lemma 11. *If C is a subset of $k[n]$, m and m' two monomials of $k[\mathbf{N}^{(C)}]$ such that $m(C)$ and $m'(C)$ have the same leading monomial and $\mathcal{S}$ a generating set of superpositions, then there exist ℓ monomials M_i of $k[\mathbf{N}^{(C)}]$ and S-polynomials R_i associated to superpositions of $\mathcal{S}$ such that*

$$m(C) - m'(C) = \sum_{i=1}^{\ell} M_i(C) R_i .$$

∎

We have then a fundamental theorem, which also has an analog in the case of standard bases.

THEOREM 12. *Let A be a k-subalgebra of $k[n]$ and C a subset of A, then the three following propositions are equivalent:*

A) C is a canonical basis,

B) $\forall P \in A \;\; P \xrightarrow{C^*} 0$,

C) C generates A and there exists a generating confluent set $\mathcal{S}$ of superpositions between elements of C.

PROOF. A) $\Rightarrow$ B) For any element P of A, mdeg$P$ is in Mon$C$ so that P needs to be reduced by C if P is not 0. By lemmas 4 and 5, $P \xrightarrow{C^*} 0$.

B) $\Rightarrow$ C) As any polynomial in A is reduced to 0, it is obviously the case of any S-polynomial. This also implies that C generates A.

C) $\Rightarrow$ A) That will be the consequence of a more precise result.

PROPOSITION 13. *If $P = T(C)$ is a polynomial in A and if all superpositions between elements of C of multidegree not greater than the multidegree of T are reduced to 0 by C, then P is reduced to 0 by C.*

PROOF. We recall that we have extended $\prec$ to an ordering on monomials of $k[\mathbf{N}^{(C)}]$. We suppose the result is false and search a contradiction. Let us consider the non reducible $P = R(C)$ such that R is minimal according to $\prec$, we have $R \preceq T$. Then we can choose some P among them such that R has minimal number of monomials.

Let m be a maximal monomial of R, $m(C)$ is obviously reducible, and $R(C) - m(C)$ is reducible too, for its maximal monomials are not greater than m and $R - m$ has smaller number of monomials than R. $m(C)$ and $R(C) - m(C)$ have the same leading monomial and opposite leading coefficients, if not P would be reducible. Then $R(C) - m(C) \xrightarrow{C} Q(C)$, with $Q(C)$ reducible so that Q is smaller than $R - m$ according to lemma 7. Now $R(C) - m(C)$ is equal to $m'(C) + Q(C)$ where m' is a monomial greater than Q. $m(C)$ and $m'(C)$ have obviously opposite leading monomials and by lemma 11, $m(C) - m'(C)$ is of the form $\sum m_i S_i$, where the S_i are S-polynomials associated to superpositions in C and the $m_i S_i$ are smaller than R. We can then use the hypothesis on S-polynomials and apply again lemma 7 on each $m_i S_i$. So $m(C) + m'(C) = Q'(C)$ with Q' smaller than R.

The conclusion of this construction is that $P = Q(C) + Q'(C)$ and $Q + Q'$ is smaller than R, a contradiction. ∎

REMARK 14. We have no need in this proof to suppose that A is of finite type, nor that C is finite. Of course, we shall have to restrict ourselves to that case for effective applications.

2.2. Completion Procedure. Implementation

Using cor. 1.2.7, we can solve the membership problem for Mon$C$, and it is then easy to build a reduction procedure. The same standard basis construction will give a generating set of superposition, so that the construction of superpositions is also effective (see also [H]).

DEFINITION 1. *We say that a completion procedure is fair if all S-polynomials which are not discarded using some criteria have to be considered and reduced during the computation.*

For example, if we sort S-polynomials according to the multidegree of corresponding superposition the procedure is fair iff the ordering is archimedean.

We have then the following result.

THEOREM 2. *Let A be $k[P_1, \ldots, P_n]$, then if A admits a finite canonical basis, any fair procedure of the following form will stop and return a canonical basis:*

C := [P1,...,Pn]

(1) LS := *List-of-S-polynomials-not-considered-yet*(C)

if LS = [] *then* output C *fi*

Sp := *Choose*(LS); LS := LS - [Sp]

if *Red*(Sp) $\neq$ 0 *then* C := cons(*Red*(Sp),C) *fi*

goto (1).

If A admits no finite standard basis, the sets of polynomials C_i, returned at each loop are such that $\bigcup_{i=1}^{\infty} C_i$ is a standard basis.

PROOF. See [KM]. ∎

This way of computing a finite standard basis if there exists one, in a situation where finite standard bases do not exist in general, has already been intruced by F. Mora in [Mor] for a different situation, viz. non-commutative standard bases.

REMARK 3. We did not implement exactly a procedure of that type. Superpositions are determined, using a standard computation as described in 1.2.8. Each time a new element corresponding to a superposition is appended to the standard basis, its computation is suspended after returning the superposition to the canonical basis process. It computes the S-polynomial, reduces it, updates the list C as above and call the standard basis algorithm again. In this way, not all superpositions are found, but we still secure a generating set, which is enough, and better for efficiency. If a superposition corresponds to the reduction of a polynomial in C, we can discard it.

This algorithm is fair iff $\prec$ is archimedean. This is the case for the degree ordering, implemented in Scratchpad II. It would have been too complicated and inefficient to use the standard basis algorithm of the public system (implemented by Gebauer and Moeller), so that we have rewritten it in the case of binomial ideals and made it incremental. We use $\prec$, refined by the inverse lexicographical ordering on variables, sorted by "order of appearance". Indeed, for each element appended to C, a new variable appear in the standard basis computation. With such an ordering, we will never have to consider superpositions involving a polynomial which has been removed.

Two packages have been implemented, STANDMON computes standard bases for binomial ideals, monomials with suitable ordering been implemented in the domain MOFAM. The last package, BASECAN implements the canonical bases process.

REMARK 4. During the standard basis computation, some superpositions may be found, coming from the reduction of a syzygy between two superpositions—as in 1.2.8, superpositions are identified with binomials. In such a case, this superposition needs not to be considered, for it is generated by superpositions already treated and reduced. It seems that with the chosen ordering such a situation never occurs.

REMARK 5. Reducing to a generating set of superpositions is the canonical bases analog of the criterion of MOELLER allowing to reduced the set of syzygies to a generating set of the module of relations between leading monomials (see [Mo]).

3. Relations with Standard Bases

We will consider here a k-subalgebra A of $k[n]$ with a finite canonical basis C, according $\prec$. M will denote the submonoid Mon$A$.

3.1. A Generalization of Standard Bases

The generalized standard bases presented here are special cases of those described by SWEEDLER in [S] and ROBBIANO in [R2]. The connection made with canonical bases allows simpler definitions, and a more effective presentation. Moreover, canonical bases could be extended too, in the same way as SWEEDLER did for standard bases.

We first remark that if A is of finite type—it is obviously the case if A admits a finite canonical basis—then A is noetherian. So we may hope to generalize standard bases to A without much trouble. We will see it is indeed the case.

DEFINITION 1. *Let I be an ideal of A, M the submonoid* Mon$A$ *and E the e-set $\{\mathrm{mdeg}P | P \in I\}$ of M. Then we say that a subset G of I is a standard basis of I if the set $\{\mathrm{mdeg}P | P \in G\}$ generates E.*

REMARK 2. We have to notice that we must use the same ordering to define the canonical basis and the standard basis. In the case of $k[n]$, we do not have such a trouble for $\{x_1, \ldots, x_n\}$ is a canonical basis for all orderings. As shown in [RS], other algebras share this property, for example the elementary symmetrical polynomials form a standard basis of the subalgebra they generate, for all orderings.

Proposition 3. *All ideals of a k-subalgebra A admitting a finite canonical basis, admit a finite standard basis.*

proof. With the same notations as in the definition, M is of finite type so that it is coherent and E is of finite type. ∎

We will now generalize the notion of syzygy.

Definition 4. *Let $S = \{R_1, \ldots, R_q\}$ be a finite subset of a A, which admits a finite canonical basis $C = \{P_1, \ldots, P_\ell\}$, Q and R two elements of S, and E the set of 2-uple of monomials $(m, m') \in k[\ell] \times k[\ell]$ such that*

$$\mathrm{mdeg}(m(P)Q) = \mathrm{mdeg}(m'(P)R).$$

Denoting by M the submodule generated by E, we call syzygy between Q and R a 4-uple (R, S, m, m'), such that (m, m') belongs to the minimal subset of E which generates M. ∎

Remark 5. Such minimal elements are in finite number and we can again restrict ourselves to a generating set of syzygies, obtained in the following way. We consider the polynomial algebra $k[w, x, u, y]$, with 1 variable w, n variables x, q variables u associated to the polynomials R, and ℓ variables y associated to the polynomials P. We define weights on variables such that the weight of w and the u is 1, and the weight of the other variables 0. The binomial ideal $(\mathrm{lpm}P_i - y_i, w\mathrm{lpm}R_j - u_j)$ of $k[w, x, u, y]$, is homogeneous for this weight—this is why we need the extra variable w. Then, we compute the standard basis of this ideal up to weight 1, for an ordering which eliminates w and the x and then the u.

The elements of weight 1 in this basis whose leading monomial depends only of the variables u and y are of the form $\prod y^{\alpha_i} u_j - \prod y^{\beta_i} u_{j'}$. They are associated to a set of syzygies, generating the module of relations between leading monomials. As pointed out by P. Conti and C. Traverso in [CT], an efficient algorithm for standard bases of modules can be derived from an algorithm for ideals if we forget syzygies of weight 2 and more.

The considerations of remark 2.2.5 also apply in this case.

Remark 6. We have seen that in the case of canonical bases, superpositions involve in general more than two polynomials. Here, syzygies involve only two polynomials, but there can be more than just one syzygy between two given polynomials (see [S]).

We can define a notion of reduction with respect to a subset G of A in an obvious way and we get the usual theorem.

Theorem 7. *If A is a k-subalgebra of $k[n]$, I an ideal of A and G a subset of I, then the following properties are equivalent:*

A) G is a standard basis of I,

B) all elements of I are reduced to 0 by G,

C) G generates I and there exists a generating confluent set of syzygies between elements of G.

proof. We can adapt the proof of th. 2.1.12, or any proof for "usual" standard bases (see [Bu]). ∎

Again, we will have a completion procedure, relying on successive reduction of S-polynomials.

3.2. Ideal of Relations

Definition 1. *Let A be a k-subalgebra of $k[n]$ admitting a finite canonical basis $C = \{P_1, \ldots, P_m\}$, then we can define an ideal of relations between polynomials of C by $I = \{R \in k[m] | R(P) = 0\}$.*

Definition 2. *Let S be a superposition between elements of a finite canonical basis $C = \{f_1, \ldots, f_m\}$, P the S-polynomial associated to S. Reducing $P(f)$ to zero by C, we secure a polynomial $R(f)$, of smaller multidegree than P, such that $P - R \in I$. We denote $P - R$ by $R(S)$.*

Theorem 3. *With the same notations, if we consider the whole generating set of superpositions G determined by a standard basis computation, using some total ordering $\ll$ compatible with $\prec$ as described in cor. 1.2.7, then the the set of polynomials $R(G)$ associated by the previous construction form a standard basis of the ideal of relations I according to $\ll$.*

proof. It is easily seen using cor 1.28 and lemma 2.1.11 that all polynomials in I are reduced to 0 by $R(G)$. ∎

4. Finiteness Conditions

4.1. Examples

We will begin by two examples of ROBBIANO, which show that the canonical basis of a finitely generated k-subalgebra may be infinite.

EXAMPLE 1. Let $A = k[x, xy - x^2, xy^2] \in k[x, y]$. If k is of characteristic 0 and if we consider some ordering with $x > y$, then the reduced canonical basis of A is is

$$\{x, xy - y^2, xy^2, xy^3 - \frac{1}{2}y^4, xy^4, xy^5 - \frac{1}{3}y^6, \ldots\},$$

so that A admits no finite canonical basis. If we consider some ordering with $y > x$, then the canonical basis is finite.

If k is of positive characteristic p, then A admits a finite canonical basis for all orders, for then $y^{2p} \in A$.

It takes 11 s to compute the standard basis with $x > y$ up to degree 7, using Scratchpad II. Only two S-polynomials are reduced to 0 during this computation. As the degree increases, more and more unuseful and undetected superpositions are considered, coming from the particular structure of the algebra; $d-3$ well chosen superpositions would be enough to go up to degree d.

EXAMPLE 2. Let A be $k[x + y, xy, xy^2]$, where k is an arbitrary field, then the canonical basis of A for some ordering with $x > y$ is

$$\{x + y, xy, xy^2, xy^3, xy^4, \ldots\}.$$

If we take $y > x$ then the canonical basis is also infinite by symmetry.

REMARK 3. We can remark on those two examples that A is not integrally closed and that its integral closure is $k[x, y]$, which has a finite canonical basis.

In example 1, the extension $A[y^2]$ is an integral extension of A with finite canonical basis. Indeed, $y^2 = xy^2/x$ is in the integral closure, so that $I = xA$ is both a A ideal and a $A[y^2]$ ideal. Now, if we want to test that a polynomial P is in A, this can be done by computing a generalized standard basis for I in $A[y^2]$ and then test if xP belongs to I. In example 2, we can take $A[y] = k[x, y]$, and remarking that $y = xy^2/xy$ is in the integral closure, consider the ideal $xyA = xy\,A[y]$.

This method generalizes each time we know (by its generators) an integral extension B=$A[P_i/Q_i]$ of A in its fraction field, with finite canonical basis. The ideal $I = (\prod Q_i^{a_i - 1})\,A$, where a_i is the degree of a monic polynomial $R_i \in A[z]$ such that $A_i(P_i/Q_i) = 0$, is equal to $(\prod Q_i^{a_i-1})\,A[P_i/Q_i]$. This allows to reduce the membership problem for A to the membership problem for a the B ideal I, generated by a single element.

We can easily apply to those two examples the method of Shannon and Sweedler, but we can give some example where this method fails whereas the canonical basis method have a pretty good complexity.

EXAMPLE 4. If we consider the k-subalgebra A of $k[n]$ generated by the n polynomials

$$\begin{aligned} P_1 &= x_1 + \cdots + x_n \\ P_2 &= x_1x_2 + x_2x_3 + \cdots + x_nx_1 \\ &\vdots \\ P_n &= x_1x_2\cdots x_n, \end{aligned}$$

the standard basis of Shannon and Sweedler's method cannot be computed with the program Macaulay of BAYER and STILLMAN, already for $n = 7$. But the canonical basis of A for the degree ordering is $\{P_1, \ldots, P_n\}$. Indeed, there is no superposition between those polynomials, for their multidegrees are linearly independent. We can remark that the computation of a canonical basis for the ideal $(P_1, \ldots, P_{n-1}, P_n - 1)$ of $k[n]$ is itself a difficult problem, known as the Arnborg–Davenport problem. For the best of our knowledge it has been done only up to $n \leq 7$, using Macaulay, and $n = 8$ using the program of J. C. FAUGÈRE. It takes more than a week on ALLIANT FX40.

We could give many other examples of this kind, e.g. the polynomials of the Mayr–Meyer examples ([MM]), form a canonical basis for some ordering.

4.2. A Conjecture and Related Results

We have stated in [O2] the following conjecture, to which the remark 4.1.3 gives a particular interest.

CONJECTURE. *If A is a finitely generated integrally closed k-subalgebra of $k[n]$, then its canonical basis for any admissible ordering is finite.*

REMARK 1. The hypothesis that A is finitely generated is essential, for there exist integrally closed k-subalgebra of infinite type (consider for example $k[x, xy, xy^2, \dots] \subset k[x, y]$).

We will give some partial results relating the standard basis of A and that of its integral closure $\overline{A}$.

DEFINITION 2. *Let A be any k-subalgebra of $k[n]$, we call cone of A, the convex cone $\mathcal{C}A$ generated in $\mathbf{R}_+^n$ by $\mathrm{Mon}A \in \mathbf{N}^n$, with vertex at the origin.*

Lemma 3. If $P \in k[n]$ belongs to the integral closure $\overline{A}$ of A, then $\mathrm{mdeg}P \in \overline{\mathcal{C}A}$, which stands for the topological closure of $\mathcal{C}A$.

PROOF. P belongs to $\overline{A}$ so that $P = R/Q$ with $R \in A$ and $Q \in A$, and P satisfies some polynomial equation $P^k + a_1P^{k-1} + \cdots + a_k = 0$ where the a_i belong to A. Now, multiplying this equation by Q^k, we get $R^k + a_1QR^{k-1} + \cdots + a_kQ^k = 0$, so that R^{k+1}/Q belongs to A. We can now prove by induction that $R^kP^i = R^{k+i}/Q^i$ belongs to A for all positive integer i. The mutidegree of R^kP^i is $k\mathrm{mdeg}R + i\mathrm{mdeg}P$, hence the wanted result. ∎

THEOREM 4. *Let A be any k-subalgebra of $k[n]$, then*

$$\mathcal{C}A \subset \mathcal{C}\overline{A} \subset \overline{\mathcal{C}A}.$$

PROOF. The first inclusion is obvious and the second is a mere consequence of the lemma. ∎

REMARK 5. Our conjecture would imply that if A is finitely generated, $\mathcal{C}\overline{A} = \overline{\mathcal{C}A}$, for the canonical basis would be finite, so that its cone would be closed and generated by a finite number of points with integral coefficients. Of this, we would deduce that $\overline{\mathcal{C}A}$ is generated by a finite number of integral points for any k-subalgebra. We will see that this result can be proved for graded k-algebras of dimension 2.

4.3. Special Results for 2-dimensional Graded k-Algebras

We will first introduce some results, valid in general case.

PROPOSITION 1. *Let $A = k[P_1, \dots, P_n]$ be a finitely generated graded k-subalgebra of $k[n]$ of dimension μ, $I \in k[m]$ be the ideal of relations between polynomials P_i, $\Delta = \mathrm{lcm}(\mathrm{deg}P_i)$, $\delta = \mathrm{gcd}(\mathrm{deg}P_i)$, then if we denote by $H(d)$ the number of elements of degree d in $\mathrm{Mon}A$, there exist polynomials $R_i \in \mathbf{Q}[x]$ of common degree equal to $\mu - 1$, such that*

$$H(j\Delta + i\delta) = R_i(j),$$

for j great enough. Furthermore $H(j\delta + k) = 0$ for $0 < k < \delta$.

PROOF. The last part is obvious. Now, if we define a degree deg_p in $k[y_1, \dots, y_m]$ by $\mathrm{deg}_p(y_i) = \mathrm{deg}P_i$, we can remark that the number of elements of degree $\mathrm{deg}_p = d$ in $k[y_1, \dots, y_m]$ satisfies the wanted property. The ideal of relations I is obviously deg_p-homogeneous. This implies our result, for we have a finite free resolution of $A = k[m]/I$, which preserves the graduation deg_p. ∎

COROLLARY 2. *If A is a finitely generated k-algebra of dimension μ and $h(d)$ the number of points of degree less or equal to d in $\mathrm{Mon}A$, then there exists some polynomial $R \in \mathbf{Q}[x]$ of degree μ such that $h(d) \geq R(d)$.* ∎

DEFINITION 3. *Let A be a k-subalgebra, we call dimension of $\mathcal{C}A$, the maximal number of linearly independent points in $\mathcal{C}A$.*

PROPOSITION 4. *If A is a finitely generated k-subalgebra, the dimension of A is equal to the dimension of $\mathcal{C}A$.*

PROOF. The dimension of $\mathcal{C}A$ is the maximal number ℓ of linearly independent points in $\mathrm{Mon}A$. If $P_1, \dots, P_\ell$ are polynomials of A such that their multidegrees are linearly independent, then $k[P]$ is isomorphical to $k[\ell]$, so that $\dim A \geq \ell$. We also have $\dim A \leq \ell$ by cor. 2, hence the result. ∎

We will need the following simple lemma about submonoids of $\mathbf{N}^n$.

Lemma 5. If M is a submonoid of $\mathbf{N}^n$ and $p_1, \ldots, p_m$ points in $\mathcal{C}M$, then if we denote by G the subgroup of $\mathbf{Z}^n$ generated by M, there exist a point $q \in \mathcal{C}M$ such that the cone $\mathcal{C}'$ of vertex q generated by the points $p_i + q$ satisfies $M \cap \mathcal{C}' = G \cap \mathcal{C}'$. ∎

PROPOSITION 6. *If A is a 2-dimensional graded finitely generated k-subalgebra of $k[n]$, then for any ordering $\prec$, $\overline{\mathcal{C}A}$ is generated by 2 points in $\mathbf{N}^n$.*

PROOF. We will prove this result in $k[x, y]$, but the argument also applies in $k[n]$. We can remark that at most 2 canonical bases exist for A, one for orderings such that $x > y$ the other for $y > x$. We can consider only one of these cases, say $x > y$. Let $P_1, \ldots, P_m$ be homogeneous generators of A, $(\alpha_1, \beta_1), \ldots, (\alpha_m, \beta_m)$ their multidegrees, we choose P_j such that α_j/β_j is maximal—we consider it is the case if $\beta_j = 0$. It is easily seen that the S-polynomials coming from a superposition between the P_i have smaller slope than P_j. This implies that $p = (\alpha_j, \beta_j)$ generates the right border of $\mathcal{C}A$.

If the left border of $\mathcal{C}A$ is vertical, we have our result, if not we have to prove that its slope σ is rational. We denote by D the lcm of the degrees of P_i. By lemma 5, for any point $p' = (1, \sigma - \varepsilon) \in \mathcal{C}A$, the number $\mu(aD)$ of points of degree aD in $\mathcal{C}\{p, p'\} \cap \mathrm{Mon}A$ is asymptotically equivalent to the number of points in $G \cap \mathcal{C}'$. We denote by $\nu(aD)$ the number of points of degree aD in $\mathcal{C}\{p, (1, 1+\varepsilon)\} \cap G$. We can remark then that the number of points of degree aD in $G \cap \mathbf{R}^n_+$ is equivalent to aD/r for some integer r, so that

$$\frac{aD}{r}\left(\frac{\sigma + \varepsilon}{1 + \sigma + \varepsilon} - \frac{\beta}{\alpha + \beta}\right) \sim \nu(aD) \geq H(aD) \geq \mu(aD) \sim \frac{aD}{r}\left(\frac{\sigma - \varepsilon}{1 + \sigma - \varepsilon} - \frac{\beta}{\alpha + \beta}\right).$$

Now, by prop. 1, σ must be rational. ∎

This result is not sufficient to conclude, but it is still encouraging to prove—even in a special case—a consequence of the conjecture. Assume we can prove that the topological closure of the cone is finitely generated for any finitely generated algebra. An idea to go ahead would be to prove then that for any generator of the cone $(a_1, \ldots, a_n) \in \mathbf{N}^n$, one of the two following propositions is true:

i) there exists a polynomial in A, which multidegree is a multiple of $(a_1, \ldots, a_n)$,

ii) there exist a polynomial $P \in k[x_1, \ldots, x_n]$, with multidegree a multiple of $(a_1, \ldots, a_n)$, and a polynomial $R \in A$ such that $RP^p \in A$ $p \in \mathbf{N}$.

5. Application to Morphisms of $k[n]$

5.1. Complexity

If we consider an endomorphism of $k[n]$ defined by polynomials $f_1, \ldots, f_n$, it is an automorphism iff $k[f] = k[n]$, so that is can be tested using canonical bases. But, we need to secure a bound in order to stop the computation if $k[P]$ has an infinite canonical basis. That will be a consequence of a theorem of GABBER.

DEFINITION 1. *Let f be an endomorphism of $k[n]$ defined by polynomials f_i, we will call degree of f the maximum degree of the f_i.*

THEOREM 2. *If $f \in \mathbf{Aut}_k k[n]$ is of degree d, then the degree of f^{-1} is bounded by d^{n-1}.*

PROOF. See [BCW]. ∎

THEOREM 3. *If $A = k[f_1, \ldots, f_n] = k[n]$ and the maximal degree of polynomials f_i is d, then the canonical basis of A with respect to the degree ordering is $\{x_1, \ldots, x_n\}$ and may be computed by considering only superpositions of degree less or equal to d^n.*

PROOF. The first part is obvious, and the second is a simple consequence of prop. 2.1.13, using the theorem of Gabber. ∎

REMARK 4. Of that result, we can deduce a bound on the complexity of the canonical basis computation. It will be of the same order as the bound we can obtain for Shannon and Sweedler's method†, but yet smaller.

† In this special case the method has been introduced earlier by A. van den Essen in [E].

Indeed the computation of a canonical or standard basis may be considered as a linear algebra problem, once we have secured a bound on the degree of superpositions or syzygies. For the ideal of the graph the bound d^n has been proved in [O1]. For canonical basis, we have a system of $O(d^{n(n-1)})$ equations in $O(d^{n^2})$ variables; for the other method a system of $O(d^{2n^2})$ equations in $O(d^{2n^2})$ variables. Of this, we easily deduce a bound polynomial in d^{n^2} for both methods.

REMARK 5. If we consider the automorphism f of $k[n]$ defined by polynomials $x_1, x_2+x_1^d, \ldots, x_n+x_{n-1}^d$, then $\deg f^{-1} = d^{n-1}$. This shows that our bound is sharp, and that we will have to climb up to degree d^{n-1} at least using Shannon and Sweedler's method. But the canonical basis of $k[f]$ may be computed in degree d at most. We can obviously build examples where the canonical basis requires to consider superpositions of degree greater than d, but it seems difficult to reach d^n.

5.2. Tame Automorphism

We will now consider tame automorphisms of $k[n]$.

DEFINITION 1. *We say that an automorphism of $k[n]$ is tame if it is in the subgroup generated by elementary automorphisms which are:*
A) the automorphisms generated by the permutations of the variables,
B) de Jonquières' automorphisms:

$$f(x_1, \ldots, x_n) = (x_1, \ldots, x_{n-1}, cx_n + P(x_1, \ldots, x_{n-1})) \text{ with } c \neq 0.$$

It is known that all automorphisms of $k[2]$ are tame (see [Ju] and [Ku]). It is only a conjecture in more variables, see [BCW] and [N] for further details on the subject. We will see that we have a good bound on the degree of canonical bases for automorphisms of $k[2]$.

PROPOSITION 2. *If f is an automorphism of $k[2]$, we can be in the two following situations:*
A) there exists some integer a such that $\mathrm{mdeg} f_1 = a \mathrm{mdeg} f_2$ or $\mathrm{mdeg} f_2 = a \mathrm{mdeg} f_1$,
B) $\{f_1, f_2\}$ is a canonical basis of $k[2]$.

PROOF. Using the fact that f is tame we have $f = g_h \circ \cdots \circ g_1$ where the g_i are elementary. It is then easy to prove the result by induction on h. ∎

COROLLARY 3. *With the same notations, the canonical basis may be computed without considering any superposition of multidegree greater than* $\max(\mathrm{mdeg} f_1, \mathrm{mdeg} f_2)$.

PROOF. If we are in situation A), we can remark that the first superposition will be for example a reduction of $f_1 \xrightarrow{f_2} f_3$ of multidegree $\mathrm{mdeg} f_1$, so that we can delete f_1 and continue with f_2 and f_3. As the reduction corresponds to a de Jonquières' automorphism $k[f_1, f_2] = k[f_2, f_3]$ and we can iterate the argument untill we are in case B). Then we have secured a canonical basis, and the bound holds for the multidegrees of $f_1, f_2, \ldots$ are decreasing. ∎

REMARK 4. By the same proof, we see that the canonical basis algorithm will split f as a composition of elementary automorphisms.

It would be tempting to try to generalize prop 2. This can be done in the following way.

PROBLEM. *Let f be a tame automorphism of $k[n]$, does it exist $i \in [1, n]$ such that*

$$\mathrm{mdeg} f_i \in \mathrm{Mon} k[f_1, \ldots, \widehat{f_i}, \ldots, f_n]?$$

If we had a positive answer to that problem, we would be able to split f using canonical bases computations. But we would not have any more the bound of cor. 3, for we do not even know if the canonical basis of $k[f_1, \ldots, \widehat{f_i}, \ldots, f_n]$ is finite—as it is integrally closed, it would be a consequence of our conjecture.

The study of this problem has a special interest, for there is an automorphism of $k[x, y, z]$, given by NAGATA in [N], which does not match its conclusion, so that if the result holds anyway, the tame generators conjecture would be false in 3 variables.

EXAMPLE 5. (Nagata 1972) If we consider the automorphism

$$f: \begin{array}{rcl} x & \mapsto & x - 2y(y^2+xz) - z(y^2+xz)^2 \\ y & \mapsto & y + z(y^2+xz) \\ z & \mapsto & z, \end{array}$$

we can see that for all orderings, we cannot have $\mathrm{mdeg} f_i \in \mathrm{Mon} k[f_j, f_k]$ with all different indices. The consideration of this example convinced NAGATA that the tame generators conjecture is false.

We will conclude by giving a class of tame automorphism, for which the answer to our problem is yes.

DEFINITION 6. *We say that f is a generic tame automorphism of $k[n]$ if $f = g_h \circ \cdots \circ g_1$, where the g_i are elementary automorphisms such that:*
- *g_{2j+1} is de Jonquières and the polynomial P is a dense polynomial of degree a least 2,*
- *all coefficients are algebraically independent on the ground field of k,*
- *g_{2j} is a permutation which do not leave x_n invariant.*

PROPOSITION 7. *If f is a generic tame automorphism of $k[n]$, then the f_i form a canonical basis or there exist $i \in [1, n]$ such that $\mathrm{mdeg} f_i \in \mathrm{Mon}\{\mathrm{mdeg} f_j \,|\, j \neq i\}$.*

PROOF. If f is defined as in def. 6, this is easily proved by induction on h. ∎

COROLLARY 8. *If f is a generic tame automorphism, then it can be split into a composition of elementary automorphism by a canonical basis algorithm where no superposition of multidegree greater than $\max\{\mathrm{mdeg} f_i\}$ needs to be considered.*

PROOF. The proposition implies that if the f_i do not form themselves a canonical basis, then the canonical basis may be computed by successive reductions. ∎

Of course, in practice we will consider automorphism defined by polynomials in $\mathbf{Q}[n]$. But it seems, by trying many examples, that the "average" complexity will be the same, the computational time being of the same order than the time needed to build f as a composition of elementary automorphisms.

EXAMPLE 9. Consider the set of polynomials $\{x, y + x^{10}, z + y^{10}, t + z^{10}\}$. It determines a tame automorphism of $k[x, y, z, t]$ and that can be tested in 1.1s using Scratchpad on a IBM 4381. The computation of the standard basis of Shannon and Sweedler method takes 496.9 seconds using the pure lexicographical ordering.

Of course, in such an example where the inverse is of degree 1000, a method which determines it needs to get in some troubles. In cases where f and f^{-1} have the same degree, standard bases are more efficient in small examples, but canonical bases are better when the degree increases.

6. References

[BCW] H. BASS, E.H. CONNELL and D. WRIGHT, *The Jacobian Conjecture: Reduction of Degree and Formal Expansion of the Inverse*, Bull. of the A.M.S., v. 7, n° 1, 287–331, Sept 1982.

[Bu] B. BUCHBERGER, *Groebner bases: An algorithmic method in polynomial ideal theory*, in Multidimensional Systems Theory, N.K. Bose (ed.), Reidel, 184–232, 1985.

[CT] P. CONTI and C. TRAVERSO, *Computing the conductor of an integral extension*, preprint, 1989.

[E] A. van den ESSEN, *A Criterion to Decide if a Polynomial Map is Invertible and to Compute the Inverse*, Cath. Univ. Nijmegen, rep. 8653, 1986, to appear in Communications in Algebra, 1990.

[G] M. GIUSTI, *On the Castelnuovo regularity for curves*, proc. of ISSAC 1989, Portland, ACM press, 250–253.

[Ja] Maurice Janet, *Systèmes d'équations aux dérivées partielles*, J. de Math., 8ᵉ série, tome III, 1920.

[Jo] J.-P. JOUANOLOU, *Monoïdes*, publ. IRMA 297/P-162, Strasbourg, 1984.

[Ju] Heinrich W. E. JUNG, *Über ganze birationale Transformationen der Ebene*, J. Reine Agew. Math. 184, 1942.

[H] G. HUET, *An algorith to generate the basis of solutions to homogeneous linear diophantine equations*, Information Processing letters, 7, 3, 144–147, 1978.

[KM] Deepak KAPUR and Klaus MADLENER, *A Completion Procedure for Computing a Canonical Basis of a k-Subalgebra*, Computers and Mathematics, E. Kaltofen and S. M. Watt editors, Springer, 1989.

[Ku] W. van der KULK, *On polynomial rings in two variables*, Nieuw Arch. Wiskunde 1, 33-41, 1953.

[L] D. LAZARD, *Résolution des systèmes d'équations algébriques*, Theoretical Computer Science 15, 77–110, 1981.

[MM] E. W. MAYR and A. MEYER, *The Complexity of the Word Problems for Commutative Semigroups and Polynomial Ideals*, Advances in Math. 46, 305–329, 1982.

[Mo] H. M. MOELLER, *A reduction strategy for the Taylor resolution*, in proceedings of EUROCAL'85, Linz, 1985.

[Mor] F. MORA, *Groebner Bases for Non-Commutative Polynomial Rings*, in Proceeding of AAECC 3, Grenoble, 1985, Lecture notes in Comp. Science 229, Springer..

[N1] M. NAGATA, *On the automorphism group of k[x,y]*, Lect. Math. Kyoto University 1972.

[O1] François OLLIVIER, *Inversibility of Rational Mappings and Structural Indentifiability in Automatics*, prépublication du Centre de Mathématiques de l'École Polytechnique, appeared in the proceedings of ISSAC 1989, Portland, ACM press.

[O2] François OLLIVIER, *Inversibility of Rational Mappings and Structural Indentifiability in Control Theory*, prépublication du Centre de Mathématiques de l'École Polytechnique, expanded version of the previous paper, presented at AAECC 7, Toulouse, 1989.

[R1] L. ROBBIANO, *Terms ordering on the polynomial ring*, pr. of EUROCAL 1985, vol. 2, 513–517.

[R2] L. ROBBIANO, *On the Theory of Graded Structures*, J. Symb. Comp. 2, 1986.

[RS] L. ROBBIANO and M. SWEEDLER, *Subalgebra Bases*, preprint, Cornell Univ., 1989.

[S] M. SWEEDLER, *Ideals bases and valuation rings*, preprint, 1986.

[SS] D. SHANNON and M. SWEEDLER, *Using Groebner bases to determine algebra membership, split surjective algebra homomorphisms and determine birational equivalence*, , preprint, 1987, appeared in J. Symb. Comp. 6, 2–3.