Computing Dimension and Independent Sets for Polynomial Ideals

HEINZ KREDEL* AND VOLKER WEISPFENNING†

Universität Passau, D-8390 Passau, FRG

(Received 5 November 1986, and in revised form 8 April 1988)

We present an algorithm that computes the dimension and maximal independent sets for a polynomial ideal I from a Gröbner basis for I with respect to a lexicographical term order, and extends Buchberger's test for zero-dimensionality. The algorithm is (for a given lexicographical Gröbner basis) faster than the method of Möller & Mora (1983) using the computation of the Hilbert polynomial, and yields important additional information on independent sets and associated prime ideals. Its verification involves the new concept of strong independence modulo an ideal with respect to an admissible term order. The algorithm is implemented in the ALDES/SAC-2 system of Collins & Loos (1980), and has been tested successfully on the examples from Böröczky et al. (1986) and other examples.

Introduction

Among the basic problems of the algorithmic theory of polynomial ideals, the computation of the dimension $\dim(I)$ of an ideal $I$ in a polynomial ring $\mathbb{R} = \mathbb{K}[X_1, \ldots, X_n]$ occupies a prominent place. The geometric definition of $\dim(I)$ as the maximal dimension of all isolated prime ideals $J$ associated with $I$ is unfavourable for computation, since it involves the primary decomposition of $I$. Instead, $\dim(I)$ can be described more directly as the largest number of elements in $\mathbb{R}$ that are independent modulo $I$ in a natural sense (see Gröbner, 1968/1970). A third approach characterizes $\dim(I)$ as the degree of the Hilbert polynomial of $I$, that can be computed from the vector space dimension of the $\mathbb{K}$-linear spaces $S_m = \{ f + I | \deg(f) \leq m \} \subseteq \mathbb{R}/I$.

This last characterization has been combined successfully with the algorithmic technique of Gröbner bases introduced by Buchberger (1965), Möller & Mora (1983). The resulting algorithms are applicable to non-trivial cases. (The special problem to test whether $\dim(I) \leq 0$ can be handled more easily by Buchberger's criterion (Method 6.9 in Buchberger, 1985).

The Gröbner basis method can also be combined with the second characterization of $\dim(I)$: Consider all pure lexicographical orderings $<_L$ of terms in $\mathbb{R}$ induced by permutations of the variables $X_i$. Compute a Gröbner basis $G = G(<_L)$ of $I$ with respect to $<_L$, and let $S = S(<_L)$ be the largest initial segment of the set of variables, such that no head term of a polynomial in $G$ contains only variables from $S$. Then each $S$ is independent modulo $I$ and the largest $S$ determines the dimension of $I$ (see Kandri-Rody, * Formerly: Gesellschaft für Schwerionenforschung, D-6100 Darmstadt, FRG.
† Formerly: Universität Heidelberg, D-6900 Heidelberg, FRG.
1985), compare also Kutzler & Stifler (1985), Lemma 5. The advantage of this method is that it determines besides \textit{dim}(I) also sets of variables independent modulo \textit{I}. On the other hand, the number of Gröbner basis calculations involved in this method renders it useless for practical purposes in most cases. Further related methods for computing the dimension of a polynomial ideal appear in Giusti (1984) and Carra-Ferro (1986). The application of resultant calculus to this problem has been described in Kredel (1985).

In this paper, we present an algorithm that computes both the dimension of \textit{I} and maximal independent sets of variables modulo \textit{I} from a single Gröbner basis of \textit{I}. We verify the correctness for the case of a pure lexicographical term order and a few other cases. A recent theorem of Carra-Ferro (1987) implies that the algorithm is correct for an arbitrary admissible term order. The algorithm is significantly faster than the algorithms in Möller & Mora (1983) using the Hilbert polynomial. It also provides considerable additional information on independent sets and dimensions of isolated prime ideals associated with \textit{I}. Thus, it is particularly suitable to the method of geometrical theorem proving developed in Kutzler & Stifter (1985/86). The method provides parametrizations of affine algebraic sets. Thus it may be helpful in determining the spatial structure of molecules from algebraic equations describing this structure (compare example 4.6).

The verification of the algorithm employs the novel notion of strong independence modulo an ideal \textit{I}, a concept that correlates well with Gröbner bases and may be of independent interest.

The algorithm is implemented in the ALDES/SAC-2 system of Collins & Loos (1980), and has been tested successfully on substantial examples, including those studies in Böge et al. (1986).

The plan of the paper is as follows: Section 1 introduces strong independence modulo a polynomial ideal \textit{I}, and studies its properties and relations to the traditional concept of independence modulo \textit{I}. Section 2 relates strong independence with Gröbner bases and provides the theoretical basis for our algorithm. Section 3 presents the algorithm and its implementation. Section 4 gives an overview of the performance of the algorithm for a number of examples.

1. Independence Modulo an Ideal

Let \textit{K} be a field, \textit{R} = \textit{K}[X_1, \ldots, X_m] a polynomial ring over \textit{K}, and let \textit{X} = \{X_1, \ldots, X_n\}. For any subset \textit{S} = \{X_{i_1}, \ldots, X_{i_r}\} \subseteq \textit{X}, we let \textit{T(S)} be the set of all terms (power products) of variables in \textit{S}, and we let \textit{K}[S] = \textit{K}[X_{i_1}, \ldots, X_{i_r}]. An ideal \textit{I} of \textit{R} is proper, if \textit{I} \neq \textit{R}, or equivalently \textit{I} \neq \textit{R}. Guided by the concept of algebraic dependence in fields (see Zariski & Samuel, 1958/60), the following notions of independence and dependence (appearing in Gröbner (1968/70)) seem to be the most natural: Let \textit{I} be a proper ideal in \textit{R}, let \textit{S} \subseteq \textit{X}, \textit{x} \in \textit{X}\setminus\textit{S}. Then \textit{S} is \textit{independently modulo} \textit{I} if \textit{K}[S] \cap \textit{I} = \{0\}; otherwise \textit{S} is \textit{dependent modulo} \textit{I}. \textit{X} is \textit{dependent on} \textit{S} \textit{modulo} \textit{I} if there exists \textit{f} \in \textit{K}[S][X] \cap \textit{I} such that \textit{f} has positive degree in \textit{X}. For the case of a prime ideal \textit{I}, these concepts coincide essentially with algebraic independence and dependence in the quotient field of the residue ring \textit{R}/\textit{I}:

\textbf{LEMMA 1.1.} Suppose \textit{I} is a prime ideal in \textit{R}. Denote the residue class \textit{f} + \textit{I} \in \textit{R}/\textit{I} by \textit{f} and let \textit{K}' be the quotient field of \textit{R}/\textit{I}, so that \textit{K} \subseteq \textit{R}/\textit{I} \subseteq \textit{K}'. Then the following hold for \textit{S} \subseteq \textit{X}, \textit{x} \in \textit{X}\setminus\textit{S}.  

\textbf{LEMMA 1.1.} Suppose \textit{I} is a prime ideal in \textit{R}. Denote the residue class \textit{f} + \textit{I} \in \textit{R}/\textit{I} by \textit{f} and let \textit{K}' be the quotient field of \textit{R}/\textit{I}, so that \textit{K} \subseteq \textit{R}/\textit{I} \subseteq \textit{K}'. Then the following hold for \textit{S} \subseteq \textit{X}, \textit{x} \in \textit{X}\setminus\textit{S}.
Computing Dimension and Independent Sets

(1) $S$ is independent mod $I$ iff $S = \{\bar{Y} | Y \in S\}$ is algebraically independent in $K'$ over $K$ and $|S| = |\bar{S}|$.

(2) If $S$ is independent mod $I$, then $X$ is dependent on $S$ mod $I$ iff $\bar{X}$ is algebraically dependent on $\bar{S}$ in $K'$ over $K$.

PROOF. Obvious □

For an arbitrary ideal $I$, the following properties hold:

LEMMA 1.2. Let $S \subseteq X, X \in X \setminus S$.

(1) $S \cup \{X\}$ is dependent mod $I$ iff $S$ is dependent mod $I$ or $X$ is dependent on $S$ mod $I$.

(2) $S$ is independent mod $I$ iff no $Y \in S$ is dependent on $S \setminus \{Y\}$ mod $I$.

(3) If $S' \subseteq S$ and $X$ is dependent on $S'$ mod $I$, then $X$ is dependent on $S$ mod $I$.

(4) (Steinitz exchange property) Let $Y \in S, S' = S \setminus \{Y\}$. If $X$ is dependent mod $I$ on $S$ but not on $S'$, then $Y$ is dependent on $S' \cup \{X\}$.

PROOF. (1)–(3) are obvious. (4) Let $f \in K[S'][Y][X] \cap I$ be of positive degree in $X$. Then $f$ is of positive degree in $Y$, since otherwise $f \in K[S'][X]$, contradicting the hypothesis. So we may construe $f$ as a polynomial in $K[S' \cup \{X\}][Y] \cap I$ of positive degree in $Y$. □

Recall that the dimension of a prime ideal $J$ in $R$, $\dim(J)$, is defined as the transcendence degree of the quotient field $K'$ of any $R/J$ over $K$. By lemma 1.1, $\dim(J)$ is the number of elements of any maximal set $S$ of variables independent mod $J$. For an arbitrary proper ideal $I$ in $R$, $\dim(I)$ is defined as the maximal dimension of an isolated prime ideal associated with $I$ (see Zariski & Samuel, 1958/60). $\dim(I)$ can be characterized more directly after Gröbner (1968/70) as follows:

LEMMA 1.3. Let $I$ be a proper ideal in $R$. Then $\dim(I)$ is the maximal number $d$ of elements in any set $S$ of variables independent mod $I$.

PROOF. Let $J$ be an isolated prime ideal associated with $I$ such that $\dim(J) = \dim(I)$ and let $S \subseteq X, |S| = \dim(J)$, be independent mod $J$. Then $S$ is also independent mod $I$, and so $|S| \leq d$. Conversely, if $S' \subseteq X, |S'| = d$, and $S'$ is independent mod $I$, then the set $M = K[S'] \setminus \{0\}$ is multiplicatively closed and disjoint to $I$. So there exists a prime ideal $J' \supseteq I$ disjoint to $M$. Let $J''$ be an isolated prime ideal associated with $I$ such that $J'' \subseteq J'$. Then $S'$ is independent mod $J''$, and so $\dim(I) \geq \dim(J'') \geq d$. □

Unfortunately, the transitivity of the dependence modulo an ideal fails, and so this is not an algebraic dependence relation in the axiomatic sense (see Zariski & Samuel, 1958/60). In fact, the most important property of an axiomatic algebraic dependence relation fails: There exist maximal sets of variables independent mod $I$ of different cardinalities.

EXAMPLE 1.4. Let $R = K[X, Y, Z], J = (X), J' = (Y, Z), I = J \cdot J' = (XY, XZ)$. Then $S = \{X\}$ is a maximal subset of $\{X, Y, Z\}$ independent mod $I$, since $XY, XZ \in I$. On the other hand, $S' = \{Y, Z\}$ is also independent mod $I$. Thus $|S| = 1 = \dim(J') < 2 = |S'| = \dim(J) = \dim(I)$.  

For a prime ideal $I$, however, all maximal sets of variables independent mod $I$ have the same cardinality by lemma 1.1.

It turns out that this natural concept of independence does not correlate well with Gröbner bases for the ideal $I$. This leads us to a more refined concept of independence mod $I$ that refers to a given admissible order $<_\tau$ of the set $T = T(X)$. Recall from Buchberger (1985) that a linear order $<_\tau$ of $T$ is admissible, if $1 < X$, and $t < t'$ implies $Xt < X't'$ for $X \in X$ and $t, t' \in T$. As a consequence, multiplication is monotonic with respect to $<_\tau$. Examples of admissible orders are the pure lexicographical ordering ($<_L$) and the total degree order ($<_d$) on $T$ induced by some linear order on $X$.

Characterizations of all admissible term orders can be found in Robbiano (1985) and Weispfenning (1987). For $S \subseteq T, t \in T$ we write $S <_\tau t$ if $s <_\tau t$ for all $s \in S, S <_\tau S'$ is defined similarly. For $f \in R, F \subseteq R$, we let $HT(f)$ denote the highest term of $f$ with respect to $<_\tau$, and let $HT(F) = \{HT(f) | f \in F\}$. So we may write $f \in R$ as $f = a \cdot HT(f) + r_f$ with $0 \neq a \in K^*$, $r_f \in R$, $r_f$ is called the reduct of $f$. We define $f >_\tau g$ iff $HT(f) >_\tau HT(g)$ or if $HT(f) = HT(g)$ and $r_f >_\tau r_g$.

The following definitions are fundamental for our study. Let $S$ and $A$ be disjoint subsets of $X$, and let $I$ be a proper ideal of $R$. Then $K[S/A]$ denotes the set of all non-zero polynomials $f \in K[S \cup A]$ such that $HT(f) \in K[S]$: $K[S/A] = \{f | 0 \neq f \in K[S \cup A] \text{ and } HT(f) \in K[S]\}$ (so for $S = \emptyset, K[S/A] = K^*$). We say $S$ is independent mod $I$ with respect to $A$, if $K[S/A] \cap I = \emptyset$. If $X \in X \setminus (S \cup A)$ we say $X$ is dependent on $S/A$ mod $I$, if there exists $f \in K[S \cup A\setminus X]/A \cap I$ such that $X$ occurs in $HT(f)$. This implies that there exists $f \in K[S \cup A\setminus X]/A \cap I$ such that the coefficient of some positive power of $X$ in $f$ is in $K[S/A]$. For $A = \emptyset$, these concepts coincide with those considered above. We say $S$ is strongly independent modulo $I$, if $S$ is independent mod $I$ with respect to $X \setminus S$. So any strongly independent set $S$ of variables is also independent mod $I$. The converse fails as the following easy example shows:

**Example 1.5.** Let $R = K[X, Y], I = (Y - X)$ and let $X <_\tau Y$. Then $S = \{Y\}$ is independent but not strongly independent mod $I$.

A much more delicate problem arises, when we consider maximal sets $S$ strongly independent mod $I$: Clearly, any such $S$ is independent mod $I$. Is it also maximal independent mod $I$? Using the interrelations between Gröbner bases and strongly independent sets, we are going to verify the following example in the next section.

**Example 1.6.** Let $R = K[X, Y, Z]$, where $<_\tau = <_L$ is the pure lexicographical order with $X <_\tau Y <_\tau Z$; let $J = (Z - X), J' = (X, Y), I = J, J' = (ZX - X^2, ZY - XY)$, and let $S = \{Z\}$. Then $S$ is maximal strongly independent mod $I$, but $S' = \{X, Y\}$ is independent mod $I$, and so $S$ is not maximal independent mod $I$.

Notice that in the example, $I$ is a product of two prime ideals of different dimensions 2 and 1.

In view of the results below we conjecture that for a prime ideal $I$ any maximal set of variables strongly independent mod $I$ is also maximal independent mod $I$ and hence determines the dimension of $I$. Some consequences of this conjecture will be discussed at the end of this section.
The results of this section will be concerned with sufficient conditions on a maximal set $S$ of variables strongly independent mod $I$ to be also maximal independent mod $I$.

We begin by relating strongly independent sets of variables modulo an arbitrary ideal $I$ to the corresponding sets modulo the isolated prime ideals associated with $I$.

**Lemma 1.7.** Let $I$ be a proper ideal in $R$, let $S \subseteq X$, and let $\prec$ be an arbitrary admissible term order on $T$.

1. If $S$ is (maximal) strongly independent mod $I$ with respect to $\prec$, then there exists an isolated prime ideal $J$ associated with $I$ such that $S$ is also (maximal) strongly independent mod $J$ with respect to $\prec$.
2. Let $U = \{S \subseteq X | S$ is strongly independent mod $I$ with respect to $\prec\}$, and $U' = \{S \subseteq X |$ there exists an isolated prime ideal $J$ associated with $I$ such that $S$ is strongly independent mod $J$ with respect to $\prec\}$, then $U = U'$.

**Proof.**

1. Let $S$ be strongly independent mod $I$ and let $A = X \setminus S$. Then $K[S/A]$ is a multiplicatively closed subset of $R$ disjoint to $I$. So there exists a prime ideal $J \supseteq I$ in $R$ disjoint to $K[S/A]$. Let $J'$ be an isolated prime ideal associated with $I$ such that $I \subseteq J' \subseteq J$. Then $S$ is strongly independent mod $J'$. Moreover, if $S$ is maximal strongly independent mod $I$, then for any $S \subseteq S' \subseteq X$ with $S'$ strongly independent mod $J'$, $S'$ is strongly independent mod $I$, and so $S' = S$.

2. By (1), $U \subseteq U'$, the converse, $U' \subseteq U$, is trivial. □

**Theorem 1.8.** Let $J$ be a prime ideal in $R$, let $\prec$ be an arbitrary admissible term order on $T$ and let $S \subseteq X$ be maximal strongly independent mod $J$ with respect to $\prec$. If $|S| \geq n - 2$, then $S$ is also maximal independent mod $J$, and so $|S| = \dim(J)$.

**Proof.** If $|S| = n - 1$ there is nothing to prove. So we may assume $S = X \setminus \{X, Y\}$ with $X \neq Y$. Pick $f \in K[S \cup \{X\}/\{Y\}] \cap J$ and $g \in K[S \cup \{Y\}/\{X\}] \cap J$. Then any irreducible factor of $f$ is also in $K[S \cup \{X\}/\{Y\}] \cap J$, and similar for $g$. So we assume without restriction that $f$ and $g$ are irreducible. Since $S$ is strongly independent mod $J$, $X$ occurs in $HT(f)$ and $Y$ occurs in $HT(g)$, and so $g$ is not a multiple of $f$. Consequently, the prime ideal $J'$ generated by $f$ is properly contained in $J$, and so by Zariski & Samuel (1958/60) chapter VII, theorem 20, $\dim(J) \leq n - 2$ and so $S$ is maximal independent mod $J$. □

The following somewhat technical theorem is the central result of this section. It requires the concept of an inessential set of variables: let $S \subseteq X, f \in R$, and let $\prec$ be an arbitrary term order on $T$. Then we denote by $f^S$ the polynomial resulting from $f$ by substituting 1 for all variables from $S$ in $f$. We say $S$ is inessential for $f$ if all terms $t$ occurring in $f$, $t^S \leq HT(f)^S$.

**Theorem 1.9.** Let $S \subseteq X$, $I$ a prime ideal in $R$ and let $\prec$ be an arbitrary admissible term order on $T$ and let $S \subseteq X$ be independent mod $I$ and that for any $X \subseteq X \setminus S$ there exists a polynomial $f_x \in K[S \cup \{X\}/X \setminus \{X\}] \cap I$ such that $S$ is inessential for $f_x$. Then $S$ is maximal independent mod $I$, and so $|S| = \dim(I)$.

**Proof.** For $X \in X \setminus S$, let $d_X$ be the degree of $HT(f_x)$ in $X$. Then $d_X > 0$; for otherwise $HT(f_x^S) = 1$, and so $t^S \leq 1$ for all terms $t$ occurring in $f$, and so $f \in K[S]$ which contradicts...
the independence of \( S \mod I \). Let \( T' \) be the set of all \( t \in T \) such that for every \( X \in X \setminus S \), the degree of \( t \) in \( X \) is \( \leq d_X \).

CLAIM. For every \( t \in T \setminus T' \) there exists \( 0 \neq p, p_1, \ldots, p_m \in K[S], t_1, \ldots, t_m \in T' \) and \( f \in I \) such that \( pt = p_1 t_1 + \cdots + p_m t_m + f \).

PROOF OF THE CLAIM. Assume for a contradiction that the claim fails for some \( t \in T \setminus T' \) and that \( t \) is \( \tau \)-minimal with this property. Choose \( X \in X \setminus S \) such that the degree \( d \) of \( t \) in \( X \) is greater than \( d_X \), and put \( u = t \cdot X^{-d} \in T \). By our hypothesis, \( f_x \) may be written in the form \( p X^{d_X} = p_1 t_1 + \cdots + p_m t_m \) with \( t_i \in T(X \setminus S), 0 \neq p_i \in K[S], X^{d_X} > t_j \) for \( 1 \leq i \leq m \).

So \( pt = X^{d_X} \cdot u \cdot f_x - p_1 t_1 X^{d_X} \cdot u + \cdots - p_m t_m X^{d_X} \cdot u \) with \( X^{d_X} \cdot u \cdot f_x \in I \) and \( t X^{d_X} < X^{d_X} \cdot X^{d_X} \cdot u = t \) for \( 1 \leq i < m \). So the claim is valid for all \( t_i \cdot X^{d_X} \cdot u \), and hence for \( t \) as well, a contradiction.

With the notation of lemma 1.1 we may now conclude that \( K \subseteq K(S) \subseteq K' \), the quotient field of \( R/I \), and that \( R/I \) is generated as a \( K(S) \)-vector space by the finite set \( T' \).

So each \( X \in X \setminus S \) is algebraic over \( K(S) \), and so \( K' = R/I \) is a finite algebraic extension of \( K(S) \), and so \( \dim(I) = |S| = |S| \).

Next we define a special type of maximal strongly independent set, the \textbf{left basic set} of an ideal \( I \).

Let \( \prec \tau \) be an arbitrary admissible order on \( T \) and let \( I \) be a proper ideal in \( R \). For \( 0 \leq k \leq n \) define \( S_k \subseteq X \) inductively by

\[
S_0 = \emptyset \\
S_k + 1 = \begin{cases} 
S_k \cup \{X_k\} & \text{if } S_k \cup \{X_k\} \text{ is strongly independent mod } I \text{ wrt. } \prec \tau, \\
S_k & \text{otherwise.}
\end{cases}
\]

Then we call \( S = S_n \) the \textbf{left basic set of } \( I \text{ with respect to } \prec \tau \). Notice that by definition \( S \) is maximal strongly independent modulo \( I \) with respect to \( \prec \tau \). We shall see in section 2 that \( S \) can be constructed from \( \prec \tau \) and an ideal basis for \( L \).

As an immediate consequence of the definition, we note:

\textbf{PROPOSITION 1.10.} Let \( I \) be an ideal in \( R \), let \( \prec \tau \) be an arbitrary admissible term order on \( T \), and let \( S \) be the left basic set of \( I \) with respect to \( \prec \tau \). Then \( S = \emptyset \) iff for all \( X \in S \) there exists a polynomial \( f_x \in K[\{X\}/(X \setminus \{X\})] \cap I \).

Combining 1.10 with 1.9 and 1.7 we obtain:

\textbf{THEOREM 1.11.} Let \( I \) be a proper ideal in \( R \), let \( \prec \tau \) be an arbitrary admissible term order on \( T \), and let \( S \) be the left basic set of \( I \) with respect to \( \prec \tau \). Then \( S = \emptyset \) iff \( \dim(I) = 0 \).

Specializing theorem 1.9 to a pure lexicographic term order, we get:

\textbf{COROLLARY 1.12.} Let \( I \) be a prime ideal in \( R \), let \( \prec_L \) be a pure lexicographic term order on \( T \) and let \( S \) be the left basic set of \( I \) with respect to \( \prec_L \). Then \( S \) is maximal independent mod \( I \) and so \( |S| = \dim(I) \).

\textbf{PROOF.} Since \( S \) is maximal strongly independent mod \( I \), we find for every \( X \in X \setminus S \) a polynomial \( f_x \in K[S \cup \{X\}/X(S \cup \{X\})] \cap I \). \( f_x \) contains no variable \( Y \in X \) with \( Y \prec_L X \).
moreover, for every term $t$ occurring in $f_x$, the degree of $t$ in $X$ is smaller or equal to the degree $d_x$ of $HT(f_x)$ in $X$. Consequently, $HT(f_x^s) = X^{d_x} \geq_L r^s$ for all terms $t$ occurring in $f_x$, and so $S$ is inessential for $f_x$. This verifies the hypothesis of theorem 1.9. □

The main application of 1.12 is as follows:

**THEOREM 1.13.** Let $I$ be a proper ideal in $R$, let $<_L$ be a pure lexicographic term order on $T$, and put

$$d = \max\{|S|: S \subseteq X, S \text{ is maximal strongly independent mod } I \text{ wrt. }<_L\}.$$

Then $d = \dim(I)$.

**PROOF.** By lemma 1.3, $\dim(I) \geq d$. Pick an isolated prime ideal $J$ associated with $I$ such that $\dim(J) = \dim(I)$, and let $S$ be the left basic set of $J$. Then $|S| = \dim(J) = \dim(I)$ and $S$ is strongly independent mod $J$ and hence mod $I$, and so $d \geq \dim(I)$. □

Recall that a proper ideal $I$ in $R$ is **unmixed** if all isolated prime ideals associated with $I$ have the same dimension. We call $I$ **weakly unmixed**, if all isolated prime ideals of positive dimension associated with $I$ have the same dimension.

**COROLLARY 1.14.** Let $I$ be a weakly unmixed ideal in $R$, let $<_L$ be a pure lexicographic term order on $T$, and let $S$ be the left basic set of $I$. Then $|S| = \dim(I)$.

**PROOF.** By theorem 1.11, it suffices to consider the case that $S \neq \emptyset$. By 1.7 there exists an isolated prime ideal $J$ associated with $I$ such that $S$ is strongly independent mod $J$. Then $S$ is also the left basic set of $J$ and so by 1.12, $|S| = \dim(J) = \dim(I)$. □

**REMARK 1.15.**

(i) In a recent preprint, Carra-Ferro (1987), states a combinatorial theorem (theorem 3.1 in Carro-Ferro, 1987), which together with our theorem 2.1 below implies that theorem 1.13 is valid for an arbitrary admissible term order $<_T$ on $T$.

(ii) Suppose our conjecture is valid, that for any prime ideal $J$ in $R$, an arbitrary admissible term order $<_T$ on $T$, and any maximal strongly independent set $S$ mod $J$, $|S| = \dim(J)$. Then we may conclude from 1.7: If $I$ is a proper ideal in $R$ and $S$ is maximal strongly independent mod $I$, then $S = \dim(J)$ for some isolated prime ideal $J$ associated with $I$.

### 2. Strong Independence and Gröbner Bases

In this section we establish the connection between Gröbner bases for polynomial ideals $I$ and strong independence modulo $I$. This will enable us to turn the main results of section 1 into algorithmic methods for computing maximal independent sets and dimensions for polynomial ideals. For the relevant information on Gröbner bases, we refer the reader to Buchberger (1985).

Let $<_T$ be an arbitrary but fixed admissible order on $T$, and let $F$ be a finite non-empty set of polynomials in $R$. Then $\rightarrow_T$ denotes the reduction on $R$ induced by $F$, and $\rightarrow_T^+$ denotes the reflexive-transitive closure of $\rightarrow_T$. $F$ is a Gröbner basis, if for all $f \in (F), f \rightarrow_T^+ 0$. 
THEOREM 2.1. Let \( <_T \) be an arbitrary admissible order on \( T \), let \( S \subseteq X \), and let \( G \) be a Gröbner basis in \( R \) with respect to \( <_T \). Then \( S \) is strongly independent modulo \( (G) \) with respect to \( <_T \) iff \( T(S) \cap HT(G) = \emptyset \).

PROOF. If \( g \in G \) with \( HT(g) \in T(S) \), then \( g \in K[S/(X \setminus S)] \cap (G) \), and so \( S \) is not strongly independent modulo \( (G) \). Conversely, assume \( f \in K[S/(X \setminus S)] \cap (G) \). Then \( f \rightarrow \bar{f} 0 \) say \( f \rightarrow f_1 \rightarrow \sigma f_2 \rightarrow \sigma f_3 \rightarrow \sigma \ldots \rightarrow \sigma \bar{f} 0 \). Pick \( k \) minimal such that \( HT(f_k) \geq_{\sigma} HT(f_{k+1}) \), and pick \( g \in G \) such that \( f_k \rightarrow \sigma f_{k+1} \). Then \( HT(g) \) divides \( HT(f_k) = HT(f) \) in \( T \), and so \( HT(g) \in T(S) \). \( \square \)

Using theorem 2.1, we can now verify the statements in example 1.6: First, one can observe that \( G = \{ ZX - X^2, ZY - XY \} \) is a Gröbner basis wrt. \( <_L \) with \( X <_L Y <_L Z \), since the \( S \)-polynomial of these two polynomials is zero (see Buchberger, 1985). \( S = \{ Z \} \) is now obviously a maximal subset of \( X \) satisfying \( T(S) \cap HT(G) = \emptyset \), and so by 2.1, \( S \) is maximal strongly independent mod \( I \). Next we reorder \( T \) by the pure lexicographical order with \( Y <_L Z <_L X \). Then \( G = \{ -X^3 + ZX, -XY + ZY \} \) is again a Gröbner basis with respect to the new order on \( T \). For \( S' = \{ X, Z \} \) we now have \( T(S') \cap HT(G) = \emptyset \). So by 2.1, \( S' \) is strongly independent, and hence independent mod \( I \).

COROLLARY 2.2. Let \( <_T \) be an arbitrary admissible order on \( T \), let \( G \) be a Gröbner basis in \( R \) with respect to \( <_T \), and put \( I = (G) \). Then the left basic set \( S \) of \( I \) can be constructed from \( G \) and \( <_T \) by the following algorithm LBS:

**Algorithm LBS(G)**

Left basic set of polynomial ideal from a Gröbner basis.

**Given:** \( <_T \) an admissible order on \( T \).

\( G = \) Gröbner basis for an ideal \( I \subseteq K[X_1, \ldots, X_n] \) with respect to \( <_T \).

**Find:** \( S = \) left basic set of \( (G) \) with respect to \( <_T \).

if \( \text{dim}(I) = -1 \) then \( S \) is undefined.

**comment** Initialise, and check dimension < 0.

if \( 1 \in G \) then return.

\( S \leftarrow \emptyset \). \( U \leftarrow \{ X_1, \ldots, X_n \} \).

repeat select \( x \) from \( U \). \( U \leftarrow U \setminus \{ x \} \).

if \( T(S \cup \{ x \}) \cap HT(G) = \emptyset \) then \( S \leftarrow S \cup \{ x \} \).

until \( U = \emptyset \).

return.

The combination of theorem 2.1 with 1.13 and 1.8 yields the following algorithmic result:

**THEOREM 2.3.** Let \( <_L \) be a pure lexicographic order on \( T \), let \( G \) be a Gröbner basis in \( R \) with respect to \( <_L \) such that \( G \cap K = \emptyset \), let \( I = (G) \), and let \( S \) be a subset of \( X \) such that

\[
T(S) \cap HT(G) = \emptyset,
\]

and such that \( S \) has the largest number of elements among all subsets of \( X \) satisfying (*)

Then \( S \) is maximal independent mod \( I \) and \( |S| = \text{dim}(I) \). The same condition holds for an arbitrary admissible term order \( <_T \) on \( T \) in case \( |S| \geq |X| - 2 \).

**Remark 2.4.**
(i) The easy special case of theorem 2.3, where \( S \) is an initial segment of \( X \) under the
order \(<_L\) was noted already in Kutzler & Stifter (1985/86) and in Kandri-Rodi (1985).

(ii) A recent result of Carra-Ferro (1987, theorem 3.1), states that theorem 2.3 is valid for an arbitrary admissible term order \(<_T\) on \(T\), provided \(G\) is a reduced Gröbner basis.

(iii) Let \(<_T\) be an arbitrary admissible term order on \(T\), let \(G\) be an arbitrary ideal basis in \(R\), and let \(S\) and \(I\) be as in theorem 2.3. Then \(G\) can be extended to a Gröbner basis \(G'\) of \(I\), and so \(|S| \geq \dim(I)|. This fact may be used to guess \(\dim(I)| from an "approximate" Gröbner basis for \(I\).

Condition (*) depends only on \(HT(G)\), which is obviously a Gröbner basis in \(R\). As a consequence, we have:

**Corollary 2.5.** Let \(<_L\) be a pure lexicographic term order on \(T\), and let \(G\) be a Gröbner basis in \(R\) with respect to \(<_L\). Then \(\dim(G) = \dim(HT(G))\).

Notice that Buchberger's criterion for deciding, whether a polynomial ideal is zero-dimensional, is an immediate consequence of 2.1 and 1.11.

**Corollary 2.6** (Buchberger, 1965, 1985). Let \(<_T\) be an admissible order on \(T\), and let \(G\) be a Gröbner basis in \(R\) with respect to \(<_T\), and let \(I = (G)\). Then \(I\) is zero-dimensional iff for all \(X \in X\), \(T(\{X\}) \cap HT(G) \neq \emptyset\).

**Proof.** By 2.3 and 1.11, \(I\) is zero-dimensional iff every singleton \(S = \{X\}\) violates condition (*). \(\Box\)

We have indicated in 1.15(ii) that if our conjecture on prime ideals holds then every maximal set \(S\) of variables satisfying \(T(S) \cap HT(G) = \emptyset\) for a Gröbner basis \(G\) in \(R\) is a maximal independent set for some isolated prime ideal \(J\) associated with \(I = (G)\); this is the case e.g. for \(|S| \geq |X| - 2\). So one may ask for a converse: Given some isolated prime ideal \(J\) associated with \(I\), and a maximal set \(S\) of variables independent mod \(J\), does \(S\) occur as a maximal set with \(T(S) \cap HT(G) = \emptyset\). The answer is no, for the simple reason that \(S\) may be a proper subset of a maximal set \(S'\) independent mod \(J'\) for another isolated prime ideal \(J'\) associated with \(I\):

**Example 2.7.** Let \(R = K[X, Y, Z]\), \(J = (X), J' = (X + 1, Y), I = J \cdot J' = (X^2 + X, XY)\). Then \(G = \{XY, X^2 + X\}\) is a Gröbner basis of \(I\) with respect to the pure lexicographical order on \(T\) with \(X < Y\). So by 2.1, \(S = \{Y, Z\}\) is the only maximal set of variables with \(T(S) \cap HT(G) = \emptyset\). Thus the only maximal set \(S' = \{Z\}\) of variables independent mod \(J'\) is 'hidden' by the larger set \(S\) belonging to \(J\).

Finally we give a new, constructive proof of a theorem proved in Giusti (1984) for homogeneous ideals.

**Theorem 2.8.** Let \(<_T = <_L\) be the pure lexicographical order on \(T\) with \(X_1 <_L \cdots <_L X_n\). For any finite ideal basis \(F\) of \(I\) in \(R\) one can construct a non-empty Zariski-open subset \(M\) of \(GL(n)\) (regarded as acting on \(X_1, \ldots, X_n\)) such that for all \(\varphi \in M\) the left basic set \(S^\varphi\) of the transformed ideal \(I^\varphi = (F^\varphi)\) equals some \(\{X_1, \ldots, X_s\}\) \((0 \leq s \leq n)\) and determines the dimension of \(I\): \(\dim(I) = \dim(I^\varphi) = |S^\varphi|\).
PROOF. First we compute a Gröbner basis $G$ of $I$ with respect to $<_r$ and a strongly independent set $S \subseteq X$ with maximal number of elements. Then $s = |S| = \text{dim}(I)$. Next we determine $\varphi \in G(n)$ permuting $X_1, \ldots, X_n$ such that $S^\varphi = \{X_1, \ldots, X_s\}$. Then $S^\varphi$ is independent modulo $I^\varphi$. Since $<_r$ is pure lexicographic, $S^\varphi$ is strongly independent modulo $I^\varphi$ and hence is the left basic set of $I^\varphi$. Compute a Gröbner basis $G'$ of $I^\varphi$. Then $HT(G') \cap T(S^\varphi) = \emptyset$. Next we apply theorem 2.1 in Weispfenning (1988) to determine for $G'$ a Zariski-open subset $M$ of $GL(n)$ such that for all $\psi \in M$ the reduced Gröbner basis $G''(\psi)$ of $(I')^\psi$ is computed uniformly in $\psi$; in particular the coefficients of the polynomials in $G''(\psi)$ are rational functions in the components of $\psi$. We claim that for all $\psi \in M, T(S^\varphi) \cap HT(G''(\psi)) = \emptyset$. This will prove the theorem.

Assume for a contradiction that for some $\psi \in M, HT(G''(\psi)) \cap T(S^\varphi) \neq \emptyset$. There is a Zariski-open subset $M'$ of $GL(n)$ such that for all $\rho \in M'$, $T(S^\rho) \cap HT(G''(\psi)^\rho) = \emptyset$. Pick $\rho \in M \cap M'$ and $\psi$. Then $G''(\sigma \circ \psi) = G''(\psi)^\sigma$, and so $T(S^\rho) \cap HT(G''(\sigma \circ \psi)) = \emptyset$. This contradicts the uniformity of the construction of $G''(\psi)$ and $G''(\sigma \circ \psi)$ from $G'$, by which also $HT(G''(\sigma \circ \psi)) \cap T(S^\rho) \neq \emptyset$. □

3. Algorithm Description

The following two algorithms $\text{DIMENSION}$ and $\text{DIMREC}$ compute the dimension $d$ of a polynomial ideal $I \subseteq K[X], X = \{X_1, \ldots, X_n\}$ from a given Gröbner basis $G$ of $I$ with respect to a pure lexicographic order on $T$. They compute a set $M$, whose elements $S \subseteq X$ are maximal strongly independent sets of variables mod $I$ with respect to $<_r$. Then $d = \max \{|S|: S \in M\}$.

The algorithm $\text{DIMENSION}$ first checks if $1 \in G$. Then it initializes the sets $S$, $U$ and $M$ and calls the recursive algorithm $\text{DIMREC}$. $\text{DIMREC}$ computes $M$ by testing if there is a header in $G$ in the variables of subsets $S$ of $X$. Thereafter $\text{DIMENSION}$ determines the element of $M$ with maximal number of variables.

Algorithm $\text{DIMENSION}(G, d, S, M)$

Dimension of a polynomial ideal from a Gröbner basis.

Given: $G = \text{Gröbner basis for an ideal } I \subseteq K[X_1, \ldots, X_n]$.

Find: $d = \text{dimension } \text{ideal}(G)$.

$S = \text{greatest maximal set of variables with } T(S) \cap HT(G) = \emptyset, \text{ if } d > 0$.

$M = \text{set of maximal sets of variables with } T(S) \cap HT(G) = \emptyset$.

comment Initialize, and check dimension $< 0$.

$M \leftarrow \emptyset$. $d \leftarrow -1$.

if $1 \in G$ then return.

$S \leftarrow \emptyset$. $U \leftarrow \{X_1, \ldots, X_n\}$.

comment Call of the recursive algorithm for the computation of $M$.

$M \leftarrow \text{DIMREC}(G, S, U, M)$.

comment Search for greatest $S \in M$

$M' \leftarrow M$.

repeat select $m$ from $M'$. $M' \leftarrow M' \setminus \{m\}$.

$d' \leftarrow |m|$.

if $d' > d$ then begin

$d \leftarrow d'$. $S \leftarrow m$ end

until $M' = \emptyset$

return.

Algorithm $M' \leftarrow \text{DIMREC}(G, S, U, M)$

Recursive computation of maximal sets $S'$ with $T(S') \cap HT(G) = \emptyset$. 

Given: \( G = \text{Gröbner basis for an ideal } I \subseteq K[X_1, \ldots, X_n] \).

\( S = \text{set of variables with } T(S) \cap HT(G) = \emptyset. \)

\( U = \text{the set of unprocessed variables, } U \subseteq \{X_1, \ldots, X_n\}. \)

\( M = \text{set of already computed maximal sets } S' \text{ with } T(S') \cap HT(G) = \emptyset. \)

Find: \( M' = \text{updated set of maximal sets } S' \text{ with } T(S') \cap HT(G) = \emptyset. \)

comment Loop until \( U \) becomes empty.

\[ M' \leftarrow M \]

while \( U \neq \emptyset \) do begin

select first \( u \) from \( U \).

\( U \leftarrow U \setminus \{u\}. \)

if \( T(S \cup \{u\}) \cap HT(G) = \emptyset \)

then \( M' \leftarrow \text{DIMREC}(G, S \cup \{u\}, U, M') \)

end

comment Test if \( S \) is already contained in some element of \( M' \).

\( M'' \leftarrow M'. \quad t \leftarrow \text{true}. \)

while \( M'' \neq \emptyset \) and \( t \neq \text{false} \) do begin

select \( m \) from \( M''. \quad M'' \leftarrow M'' \setminus \{m\}. \)

if \( S \subseteq m \) then \( t \leftarrow \text{false} \) end.

if \( t \) then \( M' \leftarrow M' \cup \{S\} \)

return.

3.1. NOTES ON THE CORRECTNESS

To test

\[ T(S \cup \{u\}) \setminus T(S) \cap HT(G) = \emptyset, \]

as requested by Theorem 2.3, it is sufficient to test

\[ T(S \cup \{u\}) \cap HT(G) = \emptyset, \]

since

\[ T(S) \cap HT(G) = \emptyset \]

by recursion assumption.

At the end of the while-loop in \( \text{DIMREC} \) at least \( S \) is independent mod \( F \) with respect to \( X \setminus S \). So if \( S \) is not already contained in some element of \( M \), \( S \) can correctly be added to \( M \).

Crucial for the correctness of the algorithm is the step when

\[ T(S \cup \{u\}) \cap HT(G) = \emptyset \]

and after return from the recursion in the next while-loop a variable \( v \) is found with \( S <_r u <_r v \) and

\[ T(S \cup \{v\}) \cap HT(G) = \emptyset. \]

We have to consider the two cases

\[ T(S \cup \{u\} \cup \{v\}) \cap HT(G) \begin{cases} \emptyset \\ \neq \emptyset \end{cases}. \]

Let \( A <_r v \) and \( A \subseteq X \setminus \{S \cup \{u\}\} \) in the following.

- the intersection is empty:
  In this case \( S' = S \cup \{u\} \cup \{v\} \) is independent mod \( J \) with respect to \( A \) and so \( S' \)
has become subset of an element in $M$ by the previous recursion. Then at the end of
the next recursion level it is tested if $S \cup \{v\}$ is a subset of an element in $M$ and since
this is true, $S \cup \{v\}$ is not entered into $M$.

- the intersection is not empty:
  
  Since $T(S \cup \{v\}) \cap HT(G) = \emptyset$ we know per definition that $S \cup \{v\}$ is independent
  mod $I$ with respect to $A \cup \{u\}$. And so $S \cup \{v\}$ correctly enters into $M$ as subset of
  some $S'$.

For an arbitrary admissible term order $<_\tau$, Buchberger's test for dimension zero is
included, since in this case for all $u \in U$:

$$T(\emptyset \cup \{u\}) \cap HT(G) \neq \emptyset,$$

and so the algorithm DIMREC finishes without any further recursion.

3.2. NOTES ON THE COMPLEXITY

The depth of recursion is equal to $d + 1$, since only when $T(S \cup \{u\}) \cap HT(G) = \emptyset$, a
new recursion level is entered. The while-loop in DIMREC is performed at most $|U| = n$
times. When a new recursion level is entered, $U$ is at least one element smaller than
before.

By this at most

$$\binom{n}{0} + \cdots + \binom{n}{d + 1}$$

subsets of $X$ are tested if there is a headterm in the Gröbner base. If $d = 0$ only $n$ subsets
of $X$ with one element are tested. If $d = n - 1$ then $2^n - 1$ subsets of $X$ are tested. (The
empty set is tested in DIMENSION, i.e. the test for $1 \in G$.)

The number of calls of the DIMREC algorithm is then at most

$$\binom{n}{0} + \cdots + \binom{n}{d},$$

i.e. if $d = 0$, DIMREC is only called once. In the case $d = n - 1$, DIMREC is called $2^n - 1$
times.

4. Examples for the Computation

In the following examples the ground field $K$ is always the field of the rational numbers.
To improve readability, only the headterms of the computed Gröbner bases are
displayed. Listings of the input ideal bases can be found in Böge et al. (1986).
The algorithms were coded in ALDES, and the computation was done using the
SAC-2 computer algebra system by Collins & Loos (1980) and the Buchberger Algorithm
System by Gebauer & Kredel (1983), on an IBM 3090-200 mainframe under MVS/XA at
GSI. The definitions of the used term orders can be found in Kredel (1988). If the
polynomial ring is $K[X_1, X_2, \ldots, X_n]$ we always assume that $X_1 <_\tau X_2 <_\tau \cdots <_\tau X_n$.
Although the algorithms are proved to be correct only in the case of the pure lexicographic term order, we include also examples with different term orders, to support the
evidence in these cases.

EXAMPLE 4.1 (HAIRER, RUNGE-KUTTAS 1). See example 1 in Boge et al. (1986).

Polynomial ring: $K[C_2, C_3, B_3, B_1, A_{21}, A_{32}, A_{31}]$

Term order is inverse lexicographic $<_L$. 

Computing Dimension and Independent Sets

Input: \( HT(G) = \{ C_3^2B_3, C_2B_2, B_1, A_3, C_2A_3, C_2C_3A_3, B_3A_3, C_3B_2A_3, A_3 \} \)

Output: \( d = 2 \)
\( S = \{ C_2, C_3 \} \)
\( M = \{ \{ C_2, C_3 \}, \{ C_2, B_1 \}, \{ C_3, A_3 \}, \{ B_3, B_2 \}, \{ B_2, A_3 \} \} \)

Statistics: Computing time = 20 ms, Used storage cells = 822

**EXAMPLE 4.2 (HAIRER, RUNGE-KUTTA 2). See example 2 in Boge et al. (1986).**

Polynomial ring: \( K[C_2, C_3, C_a, B_4, B_3, A_4, A_3, A_2, B_1] \)
Term order is inverse lexicographic \(<_L>\).

Input: \( HT(G) = \{ C_4, C_2B_3, C_3B_4, C_2A_4, C_3B_3, C_3A_4, C_2B_3A_4, C_3B_3A_4, C_2A_4 \} \)

Output: \( d = 2 \)
\( S = \{ C_2, C_3 \} \)
\( M = \{ \{ C_2, C_3 \}, \{ C_2, B_4 \}, \{ C_3, A_4 \}, \{ C_3, B_4 \}, \{ C_3, A_4 \}, \{ C_3, A_2 \}, \{ B_4, A_2 \}, \{ B_4, A_3 \}, \{ B_4, A_2 \}, \{ A_4, A_3 \} \} \)

Statistics: Computing time = 120 ms, Used storage cells = 6552.

**EXAMPLE 4.3 (BUTCHER, RUNGE-KUTTA, \( s = 3, \text{pt} = 4 \)). See example 5 in Böge et al. (1986).**

Gröbner base of the extension ideal containing the third factor \((B + 1)\) of the univariate polynomial in \( B: B^7 + 7/2B^6 + 14/3B^5 + 23/8B^4 + 97/144B^3 - 17/144B^2 - 13/144B - 1/144.\)

Polynomial ring: \( K[B, C_2, C_3, A, B_3, A_3, B_1] \)
Term order is inverse lexicographic \(<_L>\).

Input: \( HT(G) = \{ B, A, C_2B_3, C_3B_2, C_2A_3, C_3B_2A_3, B_1 \} \)

Output: \( d = 3 \)
\( S = \{ C_2, C_3, A_3 \} \)
\( M = \{ \{ C_2, C_3, A_3 \}, \{ C_2, B_3 \}, \{ C_3, B_2, A_3 \}, \{ B_3, B_2, A_3 \} \} \)

Statistics: Computing time = 20 ms, Used storage cells = 690

With a different lexicographical term order we get:

Polynomial ring: \( K[B_3, B_2, A_3, C_2, C_3, B, A, B_1] \)
Term order is inverse lexicographic \(<_L>\).

Input: \( HT(G) = \{ B_3A_3C_2, B_2A_3C_2, B_3A_3C_2, B_3A_3C_2, B_3A_3C_2, B_3A_3C_2, B, A, B_1 \} \)

Output: \( d = 3 \)
\( S = \{ B_3, B_2, A_3 \} \)
\( M = \{ \{ B_3, B_2, A_3 \}, \{ B_3, C_3 \}, \{ B_2, A_3, C_3 \}, \{ A_3, C_3 \} \} \)

Statistics: Computing time = 30 ms, Used Storage cells = 1509

With Buchberger's total degree term order we get:

Polynomial ring: \( K[B, C_2, C_3, A, B_3, A_3, B_1] \)
Term order is \(<_g>\).
Input: $HT(G) = \{B, A, B_1, C_2, B_3, C_2C_3B_1, C_2B_3A_2, C_3^2B_3, C_3B_2A_3\}$

Output: $d = 3$
$S = \{C_2, C_3, A_3\}$
$M = \{\{C_2, C_3, A_3\}, \{C_2, B_3\}, \{C_3, B_2, A_3\}, \{B_3, B_2, A_3\}\}$

Statistics: Computing time = 20 ms, Used storage cells = 855

With the inverse graduated term order we get:

Polynomial ring: $K[B, C_2, C_3, A, B_3, B_2, A_3, B_1]$
Term order is $\prec_{\sigma}$.

Input: $HT(G) = \{B, A, B_1, C_2, B_2, C_2B_3, C_2B_3A_3, C_3B_2A_3\}$

Output: $d = 3$
$S = \{C_2, C_3, A_3\}$
$M = \{\{C_2, C_3, A_3\}, \{C_2, B_3\}, \{C_3, B_2, A_3\}, \{B_3, B_2, A_3\}\}$

Statistics: Computing time = 20 ms, Used storage cells = 791

\textbf{Example 4.4. (GERDT).} See special example 1 in Böge et al. (1986).

Polynomial ring: $K[L_1, L_2, L_4, L_5, L_6, L_7]$
Term order is inverse lexicographic $\prec_L$.

Input: $HT(G) = \{L_1^3L_2, L_1^2L_2^2, L_1L_2L_4, L_1L_2L_5, L_1L_3L_4, L_1L_3L_5, L_1L_4L_5, L_1L_5L_6, L_1L_6L_7, L_2L_5, L_1L_2L_5, L_1L_3L_5, L_2L_3L_5, L_1L_5L_6L_7, L_1L_6L_7, L_2L_5, L_3L_5, L_1L_2L_5, L_1L_3L_5, L_2L_3L_5, L_1L_5L_6L_7, L_1L_6L_7, L_2L_5, L_3L_5\}$

Output: $d = 3$
$S = \{L_2, L_5, L_3\}$
$M = \{\{L_2, L_5\}, \{L_2, L_3\}, \{L_2, L_3\}\}$

Statistics: Computing time = 50 ms, Used storage cells = 2097

With a different lexicographical term order we get:

Polynomial ring: $K[L_2, L_3, L_1, L_4, L_5, L_6, L_7]$
Term order is inverse lexicographic $\prec_L$.

Input: $HT(G) = \{L_1L_2L_3, L_1L_2L_4, L_1L_2L_5, L_1L_3L_4, L_1L_3L_5, L_1L_4L_5, L_1L_5L_6, L_1L_6L_7, L_2L_3L_4, L_2L_3L_5, L_2L_4L_5, L_2L_5L_6, L_2L_6L_7, L_3L_5, L_3L_6, L_3L_7, L_4L_5, L_4L_6, L_4L_7, L_5L_6, L_5L_7, L_6L_7\}$

Output: $d = 3$
$S = \{L_2, L_3, L_5\}$
$M = \{\{L_2, L_3\}, \{L_2, L_3\}\}$

Statistics: Computing time = 30 ms, Used storage cells = 1782

With a different lexicographical term order we get:

Polynomial ring: $K[L_2, L_3, L_5, L_1, L_4, L_6, L_7]$
Term order is inverse lexicographic $\prec_L$.

Input: $HT(G) = \{L_1L_2L_3, L_1L_2L_4, L_1L_2L_5, L_1L_3L_4, L_1L_3L_5, L_1L_4L_5, L_1L_5L_6, L_1L_6L_7, L_2L_3L_4, L_2L_3L_5, L_2L_4L_5, L_2L_5L_6, L_2L_6L_7, L_3L_5, L_3L_6, L_3L_7, L_4L_5, L_4L_6, L_4L_7, L_5L_6, L_5L_7, L_6L_7\}$

Output: $d = 3$
$S = \{L_2, L_3, L_5\}$
$M = \{\{L_2, L_3\}, \{L_2, L_3\}\}$
EXAMPLE 4.5 (GEDDES). See special example 4 in Böge et al. (1986).

Polynomial ring: \( K \{ B_5, B_4, A_5, B_0, A_4, B_2, A_3, B_1, B_2, A_2, A_0, C_5, C_4, C_3, C_1, C_2, C_0 \} \)
Term order is inverse lexicographic \(<_L\).

Input: \( HT(G) = \{ B_0^3, B_2 B_4, B_3^3, B_5 A_3, B_2 A_4, B_3 A_5, B_4 A_4, A_2 A_4, A_2^2, B_3 B_3, A_3 B_3, \)
\( A_3 B_5, B_5^2, A_2 B_2, A_3 A_3, B_3 A_3, B_5 B_1, A_2 B_1, A_2 B_1, A_3 B_1, B_1 B_2, B_4 B_2, \)
\( A_2 B_2, A_2 B_3, B_3^2, B_4 A_2, A_2 A_2, A_2 A_2, B_3 A_2, A_3 A_2, B_1 A_2, B_2 A_2, C_5, C_4, C_3, \)
\( C_1, C_2, C_0 \} \)

Output: \( d = 3 \)
\( S = \{ B_0, A_3, A_0 \} \)
\( M = \{ \{ B_0, A_3, A_0 \}, \{ B_0, B_1, A_0 \}, \{ B_0, A_2, A_0 \} \} \)

Statistics: Computing time = 220 ms, Used storage cells = 8681

With a different lexicographical term order we get:

Polynomial ring: \( K \{ B_0, A_0, B_3, B_4, A_3, A_4, B_3, A_3, B_1, B_2, A_2, A_0, C_5, C_4, C_3, C_1, C_2, C_0 \} \)
Term order is inverse lexicographic \(<_L\).

Input: \( HT(G) = \{ B_0 A_3, B_3 A_3, B_2 A_4, B_1 A_3, A_3 A_3, B_3 A_3, B_3 B_1, A_2 B_1, A_2 B_1, A_3 B_1, B_1 B_2, B_4 B_2, \)
\( A_2 B_3, B_2 A_3, A_3 A_3, B_3 A_3, B_3 B_1, A_2 B_1, A_2 B_1, A_3 B_1, B_1 B_2, B_4 B_2, A_2 B_3, \)
\( B_2, B_4 A_2, A_3 A_2, A_3 A_2, B_3 A_2, A_3 A_2, B_1 A_2, B_2 A_2, C_5, C_4, C_3, C_1, C_2, C_0 \} \)

Output: \( d = 3 \)
\( S = \{ B_0, A_0, A_3 \} \)
\( M = \{ \{ B_0, A_0, A_3 \}, \{ B_0, A_0, B_1 \}, \{ B_0, A_0, A_2 \} \} \)

Statistics: Computing time = 250 ms, Used storage cells = 9545


Polynomial ring: \( K \{ X, Y, Z \} \)
Term order is inverse lexicographical \(<_L\).

Input: \( HT(G) = \{ X^2 Y^2, X^4 Z, Y Z, X^2 Z^2 \} \)

Output: \( d = 1 \)
\( S = \{ X \} \)
\( M = \{ \{ X \}, \{ Y \}, \{ Z \} \} \)

Statistics: Computing time = 4 ms, Used storage cells = 319

EXAMPLE 4.7 (MACAULAY'S CURVES, s = 10). See the examples in Möller and Mora (1983).

Polynomial ring: \( K \{ X_0, X_1, X_2, X_3 \} \)
Term order is inverse lexicographical \(<_L\).

Input: \( HT(G) = \{ X_0^2 X_2, X_0 Y_0, X_0^4 X_3, X_2^4 X_3, X_0^4 X_3, X_0^4 X_3, X_0^4 X_3, X_1 X_3, X_1^2 X_3, X_1 X_3 \} \)

Output: \( d = 2 \)
\( S = \{ X_0, X_1 \} \)
\( M = \{ \{ X_0, X_1 \}, \{ X_1, X_2 \}, \{ X_2, X_3 \} \} \)

Statistics: Computing time = 10 ms, Used storage cells = 484
EXAMPLE 4.8 (MACAULAY’S CURVES, \( s = 30 \)) See the examples in Möller and Mora (1983)

Polynomial ring: \( K[X_0, X_1, X_2, X_3] \)
Term order is inverse lexicographic \(<_L>\).

**Input:** \( HT(G) = \{X_0^{28}X_2, X_0, X_3, X_1^{28}X_3, X_1^{27}X_2, X_1^{26}X_3, X_1^{25}X_4, X_1^{24}X_5, X_1^{23}X_6, X_1^{22}X_7, \\
X_1^{21}X_8, X_1^{20}X_9, X_1^{19}X_{10}, X_1^{18}X_{11}, X_1^{17}X_{12}, X_1^{16}X_{13}, X_1^{15}X_{14}, X_1^{14}X_{15}, X_1^{13}X_{16}, \\
X_1^{12}X_{17}, X_1^{11}X_{18}, X_1^{10}X_{19}, X_1^9X_{20}, X_1^8X_{21}, X_1^7X_{22}, X_1^6X_{23}, X_1^5X_{24}, X_1^4X_{25}, \\
X_1^3X_{26}, X_1^2X_{27}, X_1X_{28}\} \)

**Output:** \( d = 2 \)
\( S = \{X_0, X_1\} \)
\( M = \{\{X_0, X_1\}, \{X_1, X_2\}, \{X_2, X_3\}\} \)

**Statistics:** Computing time = 20 ms, Used storage cells = 764
With different term orders, we get the following maximal strongly independent sets:

Polynomial ring: \( K[X_0, X_1, X_2, X_3] \)
Term order is inverse graduated \(<_G>\).

**Output:** \( d = 2 \)
\( S = \{X_0, X_1\} \)
\( M = \{\{X_0, X_1\}, \{X_1, X_2\}, \{X_2, X_3\}\} \)

**Statistics:** Computing time = 20 ms, Used storage cells = 764
Polynomial ring: \( K[X_0, X_1, X_2, X_3] \)
Term order is inverse total degree \(<_B>\).

**Output:** \( d = 2 \)
\( S = \{X_0, X_3\} \)
\( M = \{\{X_0, X_3\}\} \)

**Statistics:** Computing time = 20 ms, Used storage cells = 580
Polynomial ring: \( K[X_0, X_1, X_2, X_3] \)
Term order is inverse reverse exponent vector \(<_S>\).

**Output:** \( d = 2 \)
\( S = \{X_0, X_1\} \)
\( M = \{\{X_0, X_1\}, \{X_1, X_2\}, \{X_2, X_3\}\} \)

**Statistics:** Computing time = 20 ms, Used storage cells = 762

Research on this paper was carried out at the Gesellschaft für Schwerionenforschung, Darmstadt, and the University of Heidelberg, and was partially supported by a DFG-Heisenberg grant. We are indebted to B. Buchberger and H. Möller for helpful comments on an earlier version of the paper, to A. Kandri-Rody for valuable discussions on the subject, and to R. Loos and G. Hemion for providing us with example 4.6. We would also like to thank the GSI for providing computing time.

References


